INSTITUTO
UNIVERSITÁRIO
DE LISBOA

Commercial Development Plan of Dataori's SIEM platform

Jian Zhang

MSc in Business Administration

Supervisor:
PhD, Rui Vinhas da Silva, Full Professor
ISCTE – Instituto Universitário de Lisboa

November, 2025

BUSINESS
SCHOOL

Department of Marketing, Operations and General Management

Commercial Development Plan of Dataori's SIEM platform

Jian Zhang

MSc in Business Administration

Supervisor:
PhD, Rui Vinhas da Silva, Full Professor
ISCTE – Instituto Universitário de Lisboa

November, 2025

Acknowledgements

As I finalize this thesis, I would like to take this moment to thank everyone who has supported this research in various ways. Each contribution, big or small, has made a real difference in moving this project forward.

My special thanks go to my supervisor, Professor Rui Vinhas da Silva. What I've learned from his professional approach throughout this process has been invaluable. He consistently provided clear direction whenever the research hit a roadblock, and his specific, constructive feedback on multiple drafts of the project saved me from potential pitfalls. Honestly, without his steady guidance, this journey would have been much more challenging.

Working alongside my colleagues on the research team has been equally rewarding. Our discussions were particularly helpful, as my colleagues' different expertise often revealed limitations in my approach. I'm particularly thankful for the hands-on assistance they offered when we faced difficulties in data collection; their practical support kept the project on track.

This study also benefited greatly from the backing of several companies in the industry. They not only provided access to certain internal data for analysis but also arranged for their business experts to share valuable practical experiences through interviews. These firsthand materials significantly strengthened the persuasiveness and practical value of the case studies in this thesis.

In closing, I want to express my appreciation once more to all who have shown interest and offered support for this research.

Resumo

Esta tese é um plano comercial para a Dataori, um fornecedor chinês de SIEM, mas o estudo mostra que a questão central é saber como uma empresa deste tipo pode crescer de forma sustentável num mercado de cibersegurança orientado por políticas públicas e fortemente competitivo. Com base na análise do ambiente externo, na avaliação das capacidades internas e em dados primários provenientes de 65 questionários e três entrevistas com especialistas, o estudo desenvolve e testa um enquadramento integrado para aquisição e retenção de clientes, ajustado às limitações da Dataori.

Os resultados indicam que a conformidade regulatória e a localização são condições necessárias para entrar no mercado, mas não garantem uma vantagem competitiva duradoura. Na prática, a facilidade de utilização, o controlo de falsos positivos e o suporte na implementação são os principais fatores que influenciam decisões de compra e renovação. O modelo proposto de "aquisição–retenção enxuta" concentra recursos escassos num conjunto de contas de elevado potencial e em alguns parceiros de canal com capacidade comprovada, integrando onboarding, seguimento regular e revisões periódicas nas operações do dia a dia para sustentar renovações e receitas de expansão. A confiança constrói-se pela combinação de sinais formais e experiência real; pilotos de alta qualidade, resposta rápida e integração fluida nas arquiteturas de TI existentes são cruciais para conquistar os decisores-chave.

No plano teórico, a tese analisa a relevância de quadros como STP e os 4Ps no contexto ITAI e defende uma sequência de análise "policy-first" para mercados deste tipo. No plano prático, apresenta um plano de um ano para a Dataori, alinhado com metas de 4 milhões de RMB em receitas, 10–12 novos clientes, 70% de taxa de renovação e 6–8 parceiros de canal ativos, e aponta opções de aperfeiçoamento futuro com base em dados reais de renovação e expansão.

Palavras-Chave: Plano comercial, vendas, SIEM

JEL Classification: O33, O38

Abstract

This thesis is a commercial plan for Dataori, a Chinese SIEM vendor, but the study shows that the main issue is how such a firm can grow sustainably in a policy-driven, competitive cybersecurity market. Using external environment analysis, an internal capability review, and primary data from 65 questionnaires and three expert interviews, the study develops and tests an integrated framework for customer acquisition and retention tailored to Dataori's constraints.

The findings show that compliance and localization are necessary to enter the market but do not create lasting advantage. In practice, ease of use, false-positive control and implementation support are the main drivers of purchase and renewal decisions. The proposed "lean acquisition–retention" model focuses scarce resources on a set of high-potential accounts and a few capable channel partners, embedding onboarding, regular follow-up and periodic reviews into everyday operations to support renewals and expansion revenue. Trust is built through formal signals and real experience; high-quality pilots, fast response and smooth integration into existing IT stacks are central to winning key decision-makers.

On the theoretical side, the thesis examines the relevance of frameworks such as STP and the 4Ps under ITAI conditions and argues for a policy-first sequencing when analyzing such markets. On the practical side, it presents a one-year plan for Dataori aligned with targets of 4 million RMB in revenue, 10–12 new customers, a 70% renewal rate and 6–8 active channel partners, and outlines options for future refinement using renewal and expansion data.

Keywords: Commercial plan, sales, SIEM

JEL Classification: O33, O38

Table of Contents

ACKNOWLEDGEMENTS ..... **I**

RESUMO ..... **II**

ABSTRACT ..... **III**

TABLE OF CONTENTS ..... **IV**

LIST OF TABLES ..... **VI**

LIST OF FIGURES ..... **VII**

GLOSSARY ..... **VIII**

1. INTRODUCTION **1**

2. LITERATURE REVIEW **4**

2.1. What is SIEM? 4

2.2. Research on ITAI-Driven Market Reconstruction 5

2.3. The Impact of US and EU Cybersecurity Policies on the Market 6

2.4. China Market Overview 7

2.5. Marketing Strategies for ITAI (IT Application Innovation) Products 8

2.6. Challenges in Marketing Strategies for Localization 9

2.7. Customer acquisition and retention 9

3. METHODOLOGY **12**

4. COMMERCIAL DEVELOPMENT PLAN **14**

4.1. Executive Summary 14

4.2. External Situational Analysis 15

4.2.1. PESTE Analysis *15*

4.2.2. Sector Analysis *21*

4.2.3. Competitor Analysis *25*

4.2.4. Porter's Five Forces Analysis *29*

4.2.5. Consumer Analysis *32*

4.3. Internal Situational Analysis 33

4.3.1. Characterization of the company *33*

4.3.2. Mission, vision and values *34*

4.3.3. Core Competencies and Resources *35*

4.3.4. Business Model and Revenue Structure *36*

4.3.5. Current Customer Base and Market Position *37*

4.3.6. Customer Acquisition Capabilities ... *39*
4.3.7. Customer Retention and Lifecycle Management ... *41*
4.3.8. Financial and Operational Readiness ... *42*
4.4. SWOT Analysis ... 43
4.4.1. Strengths ... *43*
4.4.2. Weaknesses ... *44*
4.4.3. Opportunities ... *44*
4.4.4. Threats ... *44*
4.5. Objectives of this plan ... 45
4.6. Commercial Strategy: Marketing, Sales and Business Development ... 46
4.6.1. Segmentation, Targeting, and Positioning ... *46*
4.6.2. Customer Retention Strategies ... *53*
4.6.3. Sales Strategies ... *54*
4.7. Marketing-Mix ... 56
4.7.1. Product ... *56*
4.7.2. Price ... *57*
4.7.3. Place ... *58*
4.7.4. Promotion ... *59*
4.8. Implementation ... 61
4.8.1. Schedule ... *61*
4.8.2. Budget ... *62*
4.8.3. Control and assessment ... *64*
5. CONCLUSIONS ... 67
BIBLIOGRAPHICAL REFERENCES ... 71
APPENDICES ... 74
APPENDIX A – QUESTIONNAIRE ... 74
APPENDIX B – QUESTIONNAIRE FINDINGS OVERVIEW ... 80
APPENDIX C – IN-DEPTH INTERVIEWS ... 89
APPENDIX D – IN-DEPTH INTERVIEWS FINDINGS OVERVIEW ... 90

List of Tables

Table 4.1 - The purchase of financial ICT network security products 22
Table 4.2 - Comparison of SIEM market competition indicators 27
Table 4.3 - Financial Performance and ITAI Adaptation of Major Chinese Companies 27
Table 4.4 - Customer Portfolio by Industry Vertical.....38
Table 4.5 - Customer Acquisition Channels.....40
Table 4.6 - One years implementation plan task list 61
Table 4.7 - One years budget plan.....62
Table 4.8 - KPI-driven monitoring (One-Year Plan) 64
Table 4.9 - Assessment Mechanism list (One-Year Plan).....65

List of Figures

Figure 4.1 Industry Distribution of SIEM Demand 47
Figure 4.2 Plan to Switch to Domestic SIEM in the Next 3 Years 48
Figure 4.3 Preferred SIEM Procurement Method 49
Figure 4.4 Primary Sources for SIEM Information 49
Figure 4.5 Preferred SIEM Procurement Channel 50

Glossary

AI	Artificial Intelligence
CAC	Customer Acquisition Cost
CLV	Customer Lifetime Value
DLP	Data Loss Prevention
EDR	Endpoint Detection and Response
GDPR	General Data Protection Regulation
IOC	Indicator of Compromise
ITAI	Information Technology Application Innovation
KPI	Key Performance Indicator
LTV	Lifetime Value
MSSP	Managed Security Service Provider
NDR	Network Detection and Response
NPS	Net Promoter Score
PCI-DSS	Payment Card Industry Data Security Standard
ROI	Return on Investment
SIEM	Security Information and Event Management
SOAR	Security Orchestration, Automation, and Response
SOC	Security Operations Center
UEBA	User and Entity Behavior Analytics

1. Introduction

As global cybersecurity threats intensify, enterprises and government agencies have a growing demand for security information and event management (SIEM) systems. As a core tool of the security operation center (SOC), SIEM can achieve log management, threat detection, event correlation analysis and automated response, helping enterprises improve their security situation awareness and meet compliance requirements. In the Chinese market, the domestic substitution policy requirements proposed in the "Information Technology Application Innovation Industry Promotion Plan (2023-2025)" (SASAC Document No. 79) have promoted 32% of the SIEM procurement budget in key industries such as finance and government affairs to local solutions (2024 ITAI Industry White Paper), and enterprises have an increasing demand for localized and compliant SIEM solutions. However, foreign SIEM solutions still have a large market share in the Chinese market, while domestic manufacturers face challenges in terms of technology maturity, market penetration and brand influence.

Dataori is a domestic cybersecurity vendor focused on the development and deployment of a SIEM platform. It has built a certain technical base in AI-driven threat detection, ITAI environment adaptation and flexible deployment models, and has validated its product through cooperation with around 40 customers. However, it is still at an early stage of commercialization, with annual revenue of roughly 2–3 million RMB and a market share far below that of leading players. In several projects in finance, energy and parts of the government sector, Dataori has already secured some reference cases and completed compatibility work with domestic operating systems, databases and CPUs, which provides the basic conditions to participate in ITAI- and innovation-related projects. That said, the company still has clear weaknesses in channel coverage, brand awareness, large-scale delivery and customer operations, and cannot rely on technology alone to achieve sustainable growth in the highly competitive domestic SIEM market.

The overall goal of this thesis is therefore to develop a one-year, executable commercial development plan for Dataori’s SIEM platform that is grounded in a solid understanding of China’s ITAI and cybersecurity policy environment, the structure of the SIEM industry, and customer needs. At the same time, the thesis examines how far classic marketing theories remain applicable in this specific institutional context and where they need to be adjusted.

This thesis adopts a mixed-method approach that combines qualitative and quantitative methods to strengthen the robustness and practicality of its conclusions. First, a structured literature review is conducted to build the theoretical foundation and analytical framework. It covers the evolution of SIEM technology, domestic and international research on ITAI and cybersecurity policy, ITAI product marketing and localization strategies, as well as work on

customer acquisition and retention, CLV and relationship marketing. Second, in the empirical part, a structured questionnaire titled “SIEM Localization Market Demand and Influencing Factors Survey” is designed and distributed, yielding 65 valid responses from IT decision-makers, SOC managers and other stakeholders in key sectors such as finance, government and telecommunications. The survey identifies preferences regarding product features, deployment models, pricing models and service modes. In parallel, three in-depth interviews are conducted with senior cybersecurity experts from financial and enterprise organizations in order to capture nuances that the questionnaire alone cannot reveal and to validate the quantitative findings. The analysis mainly uses descriptive statistics and cross-tabulations to explore, for example, the relationship between awareness of ITAI policy and intentions to purchase localized SIEM solutions, while open-ended responses are examined through content analysis. These results are then combined with Dataori’s internal data, financial situation, customer base and assessments of its acquisition and retention capabilities to build a one-year commercial development plan that is consistent with the company’s resource constraints.

In practical terms, the thesis aims to provide Dataori with a commercial roadmap that is executable, measurable and adjustable, rather than staying at the level of abstract strategic vision. On the one hand, external environment analysis, internal capability assessment and a SWOT diagnosis clarify Dataori’s current stage of development and the key resources it can realistically mobilize, helping to keep goal-setting and action design grounded. On the other hand, by translating revenue, new customer numbers, renewal rates and channel partner targets into concrete actions across product, pricing, channels and promotion, and by linking these to specific budget allocations, the plan offers a structured blueprint for acquisition and retention over the next 12 months.

This thesis is structured as follows. Chapter 1 introduces the research background and context, defines the research problem, outlines the objectives and intended contributions, and briefly explains the mixed-method research approach adopted in this study. Chapter 2 presents the literature review: it defines SIEM and its core functions, reviews research on ITAI-driven market reconstruction and on the impact of US and EU cybersecurity policies, and summarizes the global and Chinese cybersecurity and SIEM markets; it then focuses on ITAI product marketing, the challenges of localization, and key theories related to customer acquisition and retention, CLV and relationship marketing, which together form the theoretical framework for this study. Chapter 3 describes the research methodology, explaining the use of literature research, the design of the questionnaire survey and expert interviews, the composition of the sample, data collection procedures and the main analytical methods, as well as the scope and limitations of the research design. Chapter 4 presents the core commercial development plan: it begins with an external analysis based on PESTE, industry structure, competitor analysis,

Porter’s Five Forces and consumer analysis, followed by an internal analysis covering company profile, mission and vision, core capabilities, business model, customer base, acquisition and retention capabilities, and financial and operational readiness, leading to a SWOT diagnosis; building on this, the chapter sets one-year quantitative objectives, develops a commercial strategy that includes segmentation and positioning, acquisition and retention strategies, sales strategies and a detailed marketing mix (product, price, place and promotion), and then outlines the implementation schedule, budget and monitoring and evaluation mechanisms. Finally, Chapter 5 concludes the thesis by summarizing the main findings, theoretical contributions and managerial implications, discussing the limitations of the study, and suggesting directions for future research that could test and extend the proposed model using larger samples, longer time horizons and more granular customer data.

2. Literature Review

2.1. What is SIEM?

Security Information and Event Management (SIEM) is a cybersecurity solution designed to collect, analyze, and respond to security events in real-time. It combines Security Information Management (SIM) and Security Event Management (SEM) to aggregate logs from various sources, helping organizations detect, investigate, and mitigate potential security threats before they escalate (Naseer et al., 2023).

Key Functions of SIEM

Log Collection & Management: SIEM gathers logs from firewalls, intrusion detection systems (IDS/IPS), servers, endpoints, and applications, standardizing and storing them for further analysis (Manzoor et al., 2024).

Event Correlation & Analysis: It connects the dots between security alerts, using rule-based matching, behavioral analysis, or machine learning to detect suspicious patterns like Advanced Persistent Threats (APTs) or zero-day attacks (Naseer et al., 2021a).

Real-Time Threat Detection: SIEM continuously monitors for unusual activities, brute-force attacks, and abnormal network behavior, triggering alerts for security teams (Naseer et al., 2023).

Compliance & Regulatory Reporting: It helps organizations stay compliant with industry regulations like GDPR, PCI-DSS, and ISO 27001, generating automated security reports (Manzoor et al., 2024).

Automated Incident Response: Modern SIEM integrates with Security Orchestration, Automation, and Response (SOAR) to automatically block malicious IPs, isolate compromised devices, and reduce response time (Naseer et al., 2021a).

Traditional SIEM relied on manual rule configurations, making it slow and resource-intensive. But with Big Data, AI, and User & Entity Behavior Analytics (UEBA), modern SIEM systems can adapt to evolving threats, reduce false positives, and provide proactive threat intelligence (Naseer et al., 2023).

Additionally, cloud-based SIEM solutions are becoming more popular, allowing organizations to analyze large-scale distributed environments, making them ideal for remote workforces and IoT security (Manzoor et al., 2024).

As the backbone of Security Operations Centers (SOC), SIEM plays a crucial role in log management, event correlation, threat detection, compliance, and automated incident response. With advancements in AI and machine learning, SIEM is transitioning from reactive detection to proactive threat prevention, making it an essential tool for modern cybersecurity strategies (Naseer et al., 2023).

2.2. Research on ITAI-Driven Market Reconstruction

Since the beginning of the new century, China has issued the "National Medium- and Long-Term Science and Technology Development Plan" and the "National Innovation-Driven Development Strategy Outline", taking technological innovation as the core strategy for economic development. These policies have promoted the process of independent research and development and industrial modernization, forming a development model driven mainly by innovation. Special attention is paid to technological breakthroughs and industrial upgrading of entrepreneurial enterprises, enhancing their research and development capabilities and promoting the transformation of scientific and technological achievements. (Zhang et al., 2024).

The Information Technology Application Innovation (ITAI) policy is China's core strategy to achieve independent and controllable information technology and IT self-reliance. Its goal is to reduce dependence on foreign technology and ensure the country's technological security and independence in key areas. (Wang, 2023) Especially in the financial industry, one of the focuses of the ITAI policy is removing IOE, that is, to gradually eliminate dependence on IBM servers, Oracle databases and EMC storage devices (Zhou, 2023)

In addition, achieving independent and controllable information technology is not equivalent to simply removing IOE or domestic substitution, but requires following the inherent laws of information technology activities. On the premise of ensuring the security of information systems, relevant policy requirements must be scientifically and rationally integrated into the specific practice of bank information construction. (Lei, 2016)

Since the concept of removing IOE was first proposed in 2009, it has received positive responses from many domestic industries. Alibaba took the lead in implementing it, replacing foreign technology with self-developed middleware and databases, which greatly reduced technology costs and enhanced information security (Zhou,2021). In the banking industry, the core system upgrade and transformation began to be accelerated in 2013 to cope with potential data security risks. This trend has been supported by policies. The CBRC's Document No. 39, issued in 2014, clearly requires financial institutions to spend at least 5% of their information technology budget on the research of secure and controllable technologies, and to increase the application proportion of related technologies year by year (Lei et al., 2016).

From the perspective of the impact of policies on the market, political connections are an important mechanism that combines corporate strategy with institutional context. This suggests that companies can find a foothold in dynamic markets by establishing connections with the government in an institutionalized environment (Doh et al., 2012). Political connections are particularly important in emerging markets and transitional economies such as China, where the government has a high degree of control over financial resources, market access,

and regulatory approval. At the same time, the government may have a tendency to expropriate resources in certain circumstances, which further enhances the importance of political connections to companies. (Sun et al., 2010). Political connections can help companies gain legitimacy within the institutional framework, enhance market trust, and obtain scarce resources (Ge et al., 2017; Siegel, 2007). Companies with political connections enjoy multiple advantages in market competition, more relaxed policy supervision, more favorable financial support, and priority allocation of government projects. These factors significantly reduce the operating costs of companies and enhance their competitiveness. (Li & Zhang, 2007)

2.3. The Impact of US and EU Cybersecurity Policies on the Market

Differences in Cybersecurity Approaches Between the EU and the US, The US was the first to take action against cybersecurity risks. Initially, it focused on industry-specific regulations and used hard laws to combat cybercrime (Johns & Riles, 2017). Over time, it shifted toward soft laws like industry standards and guidelines. The US follows a market-driven approach, where cybersecurity laws and practices rely more on market regulation (Farrand, 2023). Federal cybersecurity laws apply to specific industries such as healthcare, finance, and national security (Johns & Riles, 2017).

The EU's cybersecurity laws are newer but more comprehensive, relying mainly on hard laws to establish a legal framework (Broeders et al., 2023). EU regulations cover not only market issues but also security concerns, going beyond the traditional view that the EU is rights-based while the US is market-based (Farrand, 2023; Broeders et al., 2023). The EU's legislation aligns with the US in many ways, showing a broader goal of digital governance (Roch & Oleart, 2024).

Similarities in Digital Economy Regulation, Both the US and the EU are increasing their cybersecurity regulations, showing a common trend in digital economy management (Roch & Oleart, 2024). They focus on digital sovereignty, forward defense, and Internet of Things (IoT) security (Broeders et al., 2023). Stronger defensive cybersecurity measures indicate a global shift toward unified cybersecurity governance (Fahey, 2024).

Transatlantic Cybersecurity Cooperation, Despite different regulatory methods and motivations, the US and EU share common goals in cybersecurity. This makes transatlantic cooperation possible, with no major confrontations caused by policy differences. Initially, cyber threats crossing national borders pushed the US and EU to work together. Later geopolitical factors sped up the cooperation process, strengthening their strategic partnerships. At the

international level, the US and EU continue to engage in bilateral and multilateral cooperation (Anagnostakis, 2021).

Regardless of political leadership changes, cybersecurity regulation will continue to grow. Data privacy standards and shared values will remain key concerns in transatlantic digital governance (Johns & Riles, 2017; Broeders et al., 2023;).

Developing dialogue mechanisms, policy coordination, and joint standards. Strengthening collaboration in digital governance, data protection, and cybersecurity defense (Johns & Riles, 2017; Fahey, 2024).

2.4. China Market Overview

The ITAI market size was 33 billion RMB in 2021, increasing to 47.2 billion RMB in 2022. By 2025, the market size is expected to exceed 200 billion RMB, with an annual growth rate of over 30%.

Key drivers include government policy support, accelerated domestic substitution, and the Digital China Strategy. (2023 iResearch July Research Report Conference Proceedings, 2023)

In 2021, the cybersecurity market size reached 63.5 billion RMB, with a compound annual growth rate (CAGR) of 15%-21% from 2017 to 2021.The primary investments in cybersecurity come from government, finance, telecommunications, and energy sectors, which collectively account for nearly 60% of the market. (2023 iResearch July Research Report Conference Proceedings, 2023)

2016 – Present (Rapid Development Phase)

2016: Cybersecurity Law of the People's Republic of China was enacted.2019: The release of Grade Protection 2.0 (GP 2.0), extending cybersecurity requirements to cloud computing, big data, the Internet of Things (IoT), and industrial control systems (ICS).2021: The introduction of the Regulations on the Protection of Critical Information Infrastructure and the Personal Information Protection Law, strengthening top-level cybersecurity governance. Technological trends: Widespread adoption of Zero Trust Security, Secure Access Service Edge (SASE), and cloud-native security solutions.

2001 – 2015 (Growth Phase)

2008: The introduction of Grade Protection 1.0 (GP 1.0), defining security protection for different information systems. 2010: The government-initiated research on cloud security, industrial control system security, and big data security.

Before 2000 (Initial Phase)

1987: The Ministry of Public Security introduced the Regulations on the Protection of Computer Information Systems in China. 1994: The first national computer security regulation

was issued by the State Council. (2023 iResearch July Research Report Conference Proceedings, 2023)

2.5. Marketing Strategies for ITAI (IT Application Innovation) Products

Sales Model of ITAI Products

ITAI enterprises primarily expand their market through distribution channels and industry-specific channels. Distribution channels are mainly used for traditional office products, while industry channels cater to system integrators, large ISVs, and telecom operators (Chen, 2024). Additionally, many companies adopt an agency model, leveraging partnerships to extend market reach and establish multi-tiered agency systems to enhance market penetration (Chen, 2024).

In terms of ecosystem collaboration, ITAI companies often form deep partnerships with domestic CPU, database, and operating system providers, offering more adaptable solutions (Chen, 2024). Government and industry procurement represent crucial sales channels for ITAI products. Companies must meet industry standards and be included in government procurement catalogs to cater to key sectors such as government, finance, and energy (Ji, 2024). Furthermore, enterprises provide value-added services, including IT maintenance and cloud computing support, to enhance customer engagement and generate long-term service revenue (Ji, 2024).

Market Strategies for ITAI Products

The market strategy for ITAI products is primarily policy-driven, requiring companies to align their marketing approaches with national development plans and regulatory requirements to ensure compliance with government procurement systems (Ji, 2024). Industry penetration is a key approach for market expansion, often starting with government pilot projects before gradually extending to industries such as finance, energy, and manufacturing (Chen, 2024). To enhance market competitiveness, ITAI enterprises generally adopt a price competition strategy, leveraging bulk procurement and supply chain improved to reduce costs and improve market standing (Ji, 2024).

In terms of brand building, companies promote ITAI products through industry summits, government conferences, and exhibitions, increasing market recognition and leveraging policy advantages to expand their industry influence (Chen, 2024).

Cybersecurity spending is predicted to grow at 10-12% CAGR for the next 4 years. The cybersecurity market is expected to reach $200 billion by 2024 (IDC, 2021).The total addressable market for cybersecurity is nearly $2 trillion (Mckinsey Research, 2021).

However, the market is only operating at 1/10th of its potential, with some segments still in their early stages. (Ye, 2022). Cyber security is a non-discretionary item in IT budgets, and spending on cloud and digitization will drive further growth (Ye, 2022).

2.6. Challenges in Marketing Strategies for Localization

Small and medium enterprises (SMEs) face significant market awareness and brand recognition issues when implementing marketing strategies for localization. Many SMEs lack awareness of available cybersecurity solutions, creating barriers to market penetration and customer acquisition. Despite government support schemes, businesses often struggle to navigate the processes required to access these resources, leading to the underutilization of funding and incentives (Rawindaran et al., 2023).

Traditional marketing strategies also present limitations, as many SMEs rely heavily on offline events such as industry forums, government-hosted meetings, and procurement conferences, which restrict scalability and efficiency in reaching potential customers. Furthermore, the adoption of digital marketing tools such as social media engagement, short-form video marketing, and interactive live streaming remains significantly low, reducing visibility among target audiences (Rawindaran et al., 2023).

Another key challenge is channel expansion and the partner ecosystem, as the absence of a well-established distribution and reseller network makes it difficult for SMEs to secure local partnerships that can facilitate product adoption. Regional market development is inconsistent, with urban areas and tech hubs showing higher adoption rates, while rural and less-developed regions remain difficult to penetrate (Rawindaran et al., 2023).

Price competition and regulatory barriers further complicate market entry, as customer price sensitivity forces SMEs to engage in cost-cutting strategies, often leading to price wars that diminish long-term profitability. Additionally, high development costs associated with proprietary cybersecurity solutions make it challenging for SMEs to compete with well-established multinational brands. Different countries impose varying data protection laws, privacy regulations, and cybersecurity standards, making compliance a costly and resource-intensive process for SMEs entering international markets. Government procurement policies also involve complex certification and bidding processes, further complicating SMEs' efforts to secure public-sector contracts (Rawindaran et al., 2023).

2.7. Customer acquisition and retention

For business-to-business technology providers, long-term performance depends not only on winning new accounts but also on deepening existing relationships so that customers stay, expand usage, and recommend the solution to others (Jain & Singh, 2002). Classic marketing research therefore treats acquisition and retention as two sides of the same strategic process and links them to four pillars that are highly relevant for security and analytics platforms: structured loyalty stages, customer lifetime value (CLV), relationship marketing, and data-enabled customer relationship management (Sun et al., 2023).

The loyalty ladder framework assumes that customers do not become loyal overnight but move gradually from awareness to trial, repeat purchase, preference, and finally advocacy, and that each step requires different forms of communication and value delivery. Empirical work on customer experience shows that firms earn lasting loyalty when they manage the total customer experience, combining reliable core performance with emotional and social benefits rather than relying on price promotions alone (Mascarenhas et al., 2006).

To make this staged view operational, a three-dimensional loyalty matrix has been developed that integrates the ladder concept with measures of behaviour, attitude, and perceived value, thereby allowing managers to distinguish truly committed customers from those who merely repurchase out of habit. Evidence from this work illustrates how such categorisation can be used to decide where to invest in retention programmes and where to accept churn, which is directly relevant for firms prioritising support and success resources across different accounts (Madzík & Shahin, 2021).

Customer Lifetime Value provides a monetary lens on acquisition and retention decisions by estimating the discounted profit a customer is expected to generate over the whole relationship. A widely cited review summarises how CLV models evolved from simple average-margin calculations to probabilistic approaches that incorporate purchase frequency, contribution margins, and retention probabilities, and emphasises that CLV is particularly useful when marketing budgets are limited and trade-offs between acquiring new customers and retaining current ones must be made (Jain & Singh, 2002).

More recent work extends this logic by combining CLV with machine-learning techniques and rich CRM data sets: models using behavioral variables and customer characteristics are constructed to predict future CLV for individual customers and then group them into actionable segments such as high-value/low-risk, high-value/high-risk, and low-value (Sun et al., 2023). The resulting segmentation suggests that organizations can justify higher-touch and more customized retention activities for high-CLV segments, while relying on standardized communication and digital acquisition campaigns for low-CLV prospects, thereby aligning spending with long-term value rather than short-term sales volume (Sun et al., 2023).

While CLV brings a financial perspective, relationship marketing explains the behavioral mechanisms through which long-term value is created and defended (Aka et al., 2016). In this

line of research, relationship marketing is conceptualized around constructs such as trust, commitment, communication quality, and effective conflict handling, and these elements are shown to improve customers' satisfaction with the relationship and reduce their motivation to search for alternative providers (Aka et al., 2016). Within the proposed conceptual models, satisfaction acts as a mediator: relational efforts influence satisfaction, and satisfied customers are more inclined to remain loyal, buy additional services, and spread positive word of mouth (Aka et al., 2016).

A complementary systematic review synthesizes empirical studies from multiple industries and concludes that relationship-marketing programmed—such as personalized contact, joint planning workshops, and dedicated account management—are consistently associated with higher retention rates and greater share of wallet (Rosário & Casaca, 2023). The review also highlights that relationship marketing is most effective when it is embedded in organizational processes rather than treated as a series of isolated campaigns, a point that is particularly pertinent for complex B2B solutions that require cross-functional coordination to support customers over time (Rosário & Casaca, 2023).

Data analytics and modern CRM platforms translate these conceptual ideas into day-to-day management tools by turning detailed customer data into insights about behavior, risk, and opportunity (Jabado & Jallouli, 2024). Survey evidence from retailers shows that firms which integrate analytics into their CRM processes are better able to segment customers, monitor relationship health, and tailor offers, and that these capabilities are positively related to perceived relationship quality and loyalty indicators (Jabado & Jallouli, 2024).

3. Methodology

This thesis uses the following research methods to ensure that the localization market strategy of Dataori SIEM platform is scientific and practical:

1. Literature research method: Establish a theoretical basis by reading and sorting out relevant literature on corporate strategy, information innovation business development and SIEM market.

2. In-depth interviews method: Collect opinions and needs on the SIEM market through 3 in-depth interviews with customer insights and industry experts (senior cybersecurity professionals from financial institutions and enterprise agencies) to validate the questionnaire findings and provide deeper insights into market trends.

3. Questionnaire form method: A structured questionnaire titled "SIEM Localization Market Demand and Influencing Factors Survey" was developed to collect primary data from IT decision-makers, SOC managers, and other relevant stakeholders in key sectors such as finance, government, and telecommunications. The survey included 22 designed items aimed at capturing insights into product feature preferences, procurement behaviours, pricing model preferences, and future adoption intentions.

The questionnaire was distributed to industry customers, partners, and related players using convenience sampling to ensure relevance to the SIEM domain. Respondents are IT decision makers and security operation center (SOC) managers of large Chinese enterprises and government agencies who work on key industries such as finance, government, telecommunications and energy. A total of 65 valid questionnaires were collected and used for the quantitative analysis in this study, providing a solid data foundation. Descriptive statistics were employed to analyze the key factors influencing enterprise SIEM procurement decisions and product demand characteristics. Additionally, cross-tabulation analysis was conducted to explore potential relationships between ITAI policy awareness and procurement intentions for localized SIEM products. Respondents were selected based on their direct involvement in cybersecurity procurement decisions. Descriptive statistics were employed to analyze the key factors influencing enterprise SIEM procurement decisions and product demand characteristics. Additionally, cross-tabulation analysis was conducted to explore potential relationships between ITAI policy awareness and procurement intentions for localized SIEM products.

Data collection time: December 28, 2024 to October 8, 2025.

Data analysis technology: This thesis employs descriptive statistics to examine the key factors influencing SIEM procurement decisions and the characteristics of product demand, while cross-analysis is used to investigate the relationship between ITAI policy awareness and

the procurement intention for localized SIEM products. Additionally, content analysis of open-ended survey responses is applied to extract essential market insights, providing a robust foundation for the targeted market strategy.

4. Commercial Development Plan

4.1. Executive Summary

This chapter outlines the localization market plan for Dataori SIEM platform, focusing on market entry strategy, competitive positioning and business model adaptation to drive penetration and sustainable profitable growth in China's cybersecurity market. In the face of the growing demand for ITAI (trusted innovation) compliant security solutions, this plan provides a comprehensive market strategy to ensure Dataori's market competitiveness in the domestic SIEM field.

External environment analysis evaluates the impact of political, economic, social, technological and competitive factors (PESTE) on China's SIEM industry. At the policy level, government regulation, data security laws and increased IT investment provide development opportunities for local SIEM solutions. Industry analysis explores the demand for security solutions in the financial, government and enterprise markets in detail, while Porter's Five Forces model evaluates the industry's competitive intensity, entry barriers and profitability. In addition, the competitive analysis compares Dataori with international SIEM leaders (such as Splunk, IBM QRadar) and domestic manufacturers (such as Qi'anxin, 360) to identify core competitive advantages. Customer demand analysis studies the purchasing behaviour of IT decision makers and security priorities of key industries.

Internal environment analysis defines Dataori's core competencies, corporate vision and strategic goals. SWOT analysis identifies advantages such as AI-enabled threat detection capabilities, scalable architecture and government procurement adaptation, while also pointing out potential risks such as insufficient brand awareness, MSSP channel integration challenges and customer education difficulties. Marketing objectives aim to achieve revenue growth through increasing customer adoption, occupying a leading position in the ITAI market, and SaaS subscriptions and enterprise-level deployments.

Market segmentation, target market and positioning (STP) identify Dataori's core customer base, with a priority focus on large enterprises (financial institutions, government agencies), medium-sized enterprises (hybrid SOC users) and MSSP channel partners (covering the SME market). Marketing mix (4P) plans product strategy (AI-enabled SIEM), pricing strategy (SaaS + enterprise privatization model), channel strategy (direct sales + agency cooperation), and promotion strategy (digital marketing, industry white papers, exhibition promotion) to ensure accurate reach of the target market.

Implementation plan proposes a one-year plan market development roadmap, including product release rhythm, budget allocation and KPI monitoring system to achieve efficient market expansion and return on investment (ROI). Budget planning Rationally allocate

resources between marketing promotion, R&D investment and brand building to ensure maximum capital utilization. Monitoring and evaluation system Combine KPI tracking, user feedback analysis and PDCA continuous improvement mechanism to ensure continuous adjustment of marketing strategies to improve market performance and business growth.

This market strategy ensures Dataori's leading position in the domestic SIEM field through ITAI policy dividends, AI-enabled security automation, and strategic market expansion, and ultimately creates a scalable and profitable business model to drive long-term growth of the company.

4.2. External Situational Analysis

4.2.1. PESTE Analysis

4.2.1.1. Political and Legal Context

The development of China’s ITAI industry has gone through multiple stages, from early IT infrastructure construction to today’s independent controllability strategy. The government has issued a series of key policies at different stages to promote independent innovation and localized substitution of domestic information technology.

In recent years, the development of China's ITAI industry has progressed through several key stages since the early 2000s. In 2006, the government set the goal of "independent controllability of core technologies," encouraging IT investment, and by 2014, policies began emphasizing domestic IT products and enhanced information security. The 2016 Cybersecurity Law accelerated domestic substitution in critical infrastructure, while the 2019 "De-IOE" policy aimed to reduce reliance on foreign technology. The 2020s have seen comprehensive ITAI implementation, with the official introduction of the ITAI concept in 2020, accelerated industry growth plans in 2021, and refined development goals in 2023. The policy framework continued to evolve into 2024-2025, with key developments including the introduction of the "Data Security Management Regulations" in September 2024 to provide detailed operational guidance, the "Guidelines for the Construction of the National Comprehensive Standardization System for the Artificial Intelligence Industry (2024 Edition)" in June 2024 to promote AI standardization, and a heightened focus on scenario-based cultivation and manufacturing pilot platforms to bridge the gap between R&D and mass production, as emphasized in the 2025 Government Work Report and related policy notices. In parallel, the Chinese government has introduced a series of important policies to actively promote the development of the ITAI industry. For instance, the Cybersecurity Law (2016) and the Data Security Law (2021) mandate that critical information infrastructure must employ secure and controllable information technology, thereby vigorously promoting the use of domestic databases and security software. Additionally, the Regulations on the Security

Protection of Critical Information Infrastructure (2021) further reinforce the information security requirements in key sectors such as finance, energy, and communications, while the National Information Technology Application Innovation Work Promotion Plan (2023) has set a target for government and enterprise units to use over 70% domestic software and hardware by 2025. Notably, SASAC Document No. 79 (2022) provides a clear timetable for state-owned enterprises to complete their ITAI transformation by 2027, marking a significant push towards technological self-reliance. These external policies not only provide obvious market opportunities for the development of SIEM products, but also put forward higher security, compatibility, and autonomous controllability. The stringent and forward-looking nature of these policies has compelled companies to boost investment in research and technology upgrades, ensuring their products meet rising security standards while accelerating the market entry of domestic SIEM, forming a dual driving force that is conducive to domestic substitution.

In addition to direct policy support, government procurement policies and the broader regulatory environment have had a profound impact on the development of the ITAI industry. Government agencies and state-owned enterprises are required to prioritize domestic ITAI products when purchasing information systems, a mandate further strengthened by the revised Government Procurement Law. At the same time, increasingly stringent data security and privacy protection regulations provide domestic SIEM products with a competitive edge. In the process of promoting the localization of IT systems in key industries such as finance and healthcare, regulators have established higher security thresholds and compatibility requirements, disadvantaging foreign products in market access. This dynamic was further solidified in 2024 by policies like the "Market Access Ten Articles," which explicitly listed autonomous and controllable computing as a key new field, thereby optimizing the market environment for localized security solutions. This procurement and regulatory environment not only offers direct market benefits for domestic SIEM products, forming a natural barrier for localized solutions, but also motivates companies to continuously enhance product quality and technical standards to meet strict regulatory demands. This two-way driving effect accelerates independent R&D and product iteration, while providing robust external support for companies like Dataori in product deployment and market promotion.

Furthermore, as the Chinese government continues to advance information technology innovation, it has consistently supported the R&D and industrialization of key technologies through increased capital investments, ensuring the availability and competitiveness of IT products. Recent initiatives, such as the 2025 "National Emerging Industry Innovation Center Management Measures (Draft for Comment)," further underscore this commitment by encouraging financial institutions to invest in industrial innovation centers, thereby enhancing the institutional and financial foundation for long-term R&D. This supportive policy environment offers valuable development opportunities for startups such as Dataori, particularly amid

intensifying global technology competition. Continuous policy support is reflected not only in funding and R&D investments but also in the government's systematic planning of industry trends and market structures. Such comprehensive backing has enabled domestic companies to make steady progress in technological breakthroughs and product iterations, thereby creating a favorable market environment for domestic SIEM products. While leveraging these government initiatives, companies must also continuously strengthen their independent innovation capabilities to meet the dual challenges of market competition and regulatory requirements, ultimately securing a competitive edge in the industry.

4.2.1.2. Economic Context

The global information technology and cybersecurity industries have shown steady growth, creating significant opportunities for ITAI enterprises. IDC reports that global ICT (Information and Communication Technology) market investments reached $4.9 trillion in 2023 and are projected to grow to $6.6 trillion by 2028, with a CAGR of 6.3%. The global cybersecurity market, valued at $172.24 billion in 2023, is expected to reach $562.72 billion by 2032, with a CAGR of 14.3%. While traditional IT giants dominate the global market, emerging cybersecurity firms, especially from the Asia-Pacific region, are gaining traction. Governments worldwide are strengthening support for domestic IT enterprises to enhance cybersecurity and data sovereignty.

China's ITAI industry has experienced rapid expansion, with the market reaching ¥922 billion in 2022 and ¥1.54 trillion in 2023, despite a slight slowdown. The ITAI cloud market has shown exceptional growth, reaching ¥48.3 billion in 2023 and expected to surpass ¥100 billion by 2026. Investments in cloud-based ITAI solutions are increasing across various sectors, particularly in government, finance, and telecommunications.

In key sectors, China's banking industry has achieved an 85% completion rate in ITAI implementation, with the financial ITAI market expected to reach ¥301.9 billion by 2026. The telecommunications sector has accelerated ITAI adoption, with procurement projects increasing from 24 in 2020 to 59 in 2021. The government sector plays a pivotal role in ITAI promotion, with government demand accounting for a substantial portion of the ¥922 billion ITAI market in 2022. Central and local governments have actively introduced policies to accelerate ITAI adoption across government information systems.

The generative AI boom is a primary technological driver reshaping the IT landscape. IDC predicts that global AI IT investment will grow from $315.9 billion in 2024 to $1,261.9 billion by 2029, with a compound annual growth rate (CAGR) of 31.9%. The growth of the generative AI segment is even more rapid, with a projected CAGR of 56.3% over the same period. This

surge is fueling massive demand for computational power, directly stimulating investment in AI-driven infrastructure.

China's economy has demonstrated resilience amidst a complex transition. The country's Gross Domestic Product (GDP) has shown a stabilizing trend after the post-pandemic recovery. In 2023, China achieved a GDP growth rate of 5.2%, successfully meeting its official target (NBS, 2024a). Entering 2024, the economy continued to expand, achieving a growth rate of approximately 5.0%, driven by policy support and a recovery in industrial output (NBS, 2024b; World Bank, 2024). Looking ahead, international institutions forecast a moderate deceleration as the economy matures. The International Monetary Fund (IMF) projects China's GDP growth to moderate to approximately 4.5% to 4.8% in 2025 and further slow to around 4.2% in 2026, reflecting structural adjustments in the property sector (IMF, 2024; World Bank, 2025). Despite this moderation, China remains a primary engine of global economic growth, providing a substantial market base for enterprise IT investments.

Regarding price stability, the inflation rate has remained low. The Consumer Price Index (CPI) rose by only 0.2% in 2023 and hovered around 0.2% to 0.3% throughout 2024, indicating weak domestic demand relative to supply (NBS, 2025). Forecasts suggest a gradual recovery in consumer prices, with inflation expected to rise moderately to approximately 1.0% to 1.5% in 2025 and 2026 as domestic consumption strengthens (IMF, 2024). For Dataori, this low-inflation environment suggests that while enterprise purchasing power remains stable, pricing strategies for SIEM solutions must remain competitive to align with cost-conscious corporate spending.

The labor market has maintained overall stability. The surveyed urban unemployment rate averaged 5.2% in 2023 and decreased slightly to 5.1% in 2024 (NBS, 2025). Forecasts indicate that the aggregate urban unemployment rate is expected to remain stable at around 5.1% through 2025 (IMF, 2024). This stability in the workforce supports a consistent environment for business operations and digital transformation initiatives across key sectors like finance and telecommunications.

4.2.1.3. Socio-Cultural Context

Public awareness and acceptance of information security have significantly increased due to global digital transformation and frequent cyberattacks. This trend has created favourable market conditions for ITAI companies like Dataori, especially in key industries such as finance, government, and telecommunications. The Chinese government has been actively promoting cybersecurity awareness through annual events like the "National Cybersecurity Awareness Week" since 2014. The 2024 event, themed "Cybersecurity for the People, Cybersecurity by

the People," included various focus days and awareness campaigns across different sectors of society.

Domestic enterprises and consumers are increasingly accepting and adopting ITAI products, driven by international technology restrictions and supply chain security concerns. This emphasis on "independent and controllable" technology has accelerated the penetration of ITAI products in critical industries, creating favourable conditions for Dataori's SIEM solutions in the local market.

The implementation of laws such as the Cybersecurity Law, Data Security Law, and Personal Information Protection Law has led to increased emphasis on compliance with data security regulations. This trend has allowed local SIEM solutions to gain larger market shares in key sectors. Dataori can leverage this demand by offering SIEM products that align with national regulatory standards.

The Chinese government's support through policy initiatives, industry adoption facilitation, and demonstration projects has significantly accelerated the adoption of ITAI products. Additionally, growing corporate social responsibility awareness has led more enterprises to proactively adopt ITAI products, further reinforcing the demand for domestically developed cybersecurity solutions like those offered by Dataori.

4.2.1.4. Technological Context

In recent years, the rapid advancement of global information technology has driven widespread adoption of cybersecurity, artificial intelligence (AI), big data, and cloud computing. Against this backdrop, the IT Application Innovation (ITAI) industry has been continuously evolving and improving. The changing technological landscape has had a significant impact on the development and market competitiveness of Dataori’s SIEM products, primarily in the following aspects.

As cyber threats become increasingly sophisticated, cybersecurity technologies continue to evolve. Concepts such as Zero Trust Architecture (ZTA), Security Orchestration, Automation, and Response (SOAR), User and Entity Behavior Analytics (UEBA), and Threat Detection, Investigation, and Response (TDIR) are gradually being integrated into SIEM solutions. These technologies enhance threat detection and incident response, making SIEM platforms more efficient in real-time analysis and automated defense.

Additionally, the rapid development of domestic cybersecurity technologies has driven improvements in the performance and ecosystem of ITAI-based SIEM products. Under government policy guidance, more domestic vendors are investing in security operations, log analysis, and behavioural monitoring, giving companies like Dataori a competitive advantage in the local market.

The evolution of AI and big data technologies has significantly enhanced cybersecurity capabilities. In SIEM systems, AI-driven threat detection models can analyze historical data and real-time network traffic to identify patterns, enabling more precise anomaly detection and automated response. The integration of big data platforms allows SIEM solutions to process vast amounts of log data, improving efficiency and correlation analysis accuracy.

Many enterprises are now leveraging machine learning algorithms to refine security event analysis. Dataori can capitalize on this trend by developing more intelligent SIEM products that provide enhanced situational awareness and automated response capabilities, meeting the growing need for advanced threat detection and security automation.

Cloud computing has become the backbone of enterprise IT infrastructure, and ITAI initiatives are actively adapting to the cybersecurity demands of cloud environments. As businesses transition their IT systems to the cloud, SIEM solutions must support cloud-native deployment to monitor and secure cloud-based threats effectively. At the same time, the rise of edge computing is decentralizing data processing, requiring Dataori's SIEM platform to offer distributed log analysis and real-time event management to support hybrid cloud-edge security operations.

Moreover, Threat Detection, Investigation, and Response (TDIR) is emerging as a critical component of modern cybersecurity frameworks. TDIR integrates SIEM, SOAR, AI-driven analytics, and automated response technologies to provide a more comprehensive approach to threat identification, investigation, and mitigation. By incorporating TDIR into its SIEM framework, Dataori can enhance its detection accuracy, automate incident response workflows, and deliver more actionable threat intelligence to customers.

As China advances its self-sufficient IT strategy, the domestic technology ecosystem is becoming more mature. Local operating systems (such as Kylin OS, UOS), domestic databases (such as DM, Kingbase), and homegrown processors (such as Kunpeng, Phytium, Loongson) are now widely adopted across industries. ITAI-based SIEM solutions must seamlessly integrate with these domestic ecosystems to ensure compatibility and compliance with industry standards in sectors like government, finance, and energy.

By strengthening partnerships with domestic hardware and software vendors, Dataori can enhance its product adaptability to China's IT environment, increasing its competitiveness in the ITAI market. Additionally, the continuous refinement of ITAI standards, such as compatibility certification and security compliance assessments, provides a clear framework for Dataori to further improve and deploy its solutions in the domestic market.

As the technological landscape continues to evolve, Dataori is well-positioned to leverage AI, big data, cloud computing, and TDIR to enhance its SIEM solutions. Furthermore, by aligning with the growing domestic IT ecosystem and strengthening partnerships with local

technology providers, Dataori can boost its market presence and ensure long-term competitiveness in the rapidly expanding ITAI market.

4.2.1.5. Environmental Context

Global carbon neutrality policies, including China's goals for carbon peak by 2030 and carbon neutrality by 2060, have imposed stricter environmental standards on IT enterprises. Data centers, as high-energy-consuming infrastructures, must improve their Power Usage Effectiveness (PUE) to meet policy requirements. China's standards classify PUE into five levels and impose power consumption restrictions on servers and computing equipment.

To align with these environmental objectives, Dataori can support cloud computing, implement high-efficiency log storage, and improve task scheduling. This approach helps businesses achieve sustainable IT management while enhancing product competitiveness.

Green computing has become a crucial industry trend, focusing on improving hardware and software efficiency to reduce energy consumption, enhance computing performance, and lower carbon emissions. For modern SIEM systems that process vast amounts of log data, energy consumption and system improvement are key considerations.

Dataori can improve computing efficiency by optimizing algorithms, adopting cloud-native architectures, and refining log storage mechanisms. The use of virtualization and containerization technologies can reduce hardware dependency and lower data center energy consumption, aligning with the industry's push toward sustainable IT development.

4.2.2. Sector Analysis

Dataori is in the security information and event management (SIEM) market, which belongs to the field of network security and is deeply integrated with the information and innovation industry. Its core business involves log management, threat detection, security analysis and compliance auditing, and its main customers include key industries such as finance, energy, communications, and government. Driven by policies and regulations, the growth of network security threats, and the digital transformation of enterprises, the market demand for this industry has maintained steady growth in recent years.

The SIEM market has grown rapidly globally and in China, driven by increasing cyber-attack complexity and stricter data security regulations like the "Cybersecurity Law" and "Data Security Law". The market is competed by traditional IT vendors, emerging security vendors, and Chinese domestic security companies. SIEM platforms are also enabling new security operation services like MSSP hosting.

China's ITAI (information technology application innovation) industry has expanded the local SIEM market, while the withdrawal of international products has created more opportunities. Key industries like government, finance, and telecommunications have strong demand for self-controllable, secure and compliant SIEM products, presenting important opportunities for Dataori.

The financial industry in particular is driven by policies, regulations, and self-controllability needs. As a critical sector, the security and autonomous controllability of its information systems are vital. ITAI adoption in finance is both a technological upgrade and a strategic requirement for national security and industry development.

Since 2018, China has issued policies emphasizing autonomous control of IT in finance. The “SASAC Document No. 79” requires ITAI replacement in key industries including finance by 2027. Regulators like the “China Banking and Insurance Regulatory Commission” and “China Securities Regulatory Commission” have also issued guidance urging financial institutions to accelerate ITAI adoption and ensure information system security and controllability.

According to the statistics of CCID Consulting, from 2020 to 2023, the annual compound growth rate of national financial ITAI server shipments will reach 60.8%, of which the shipment volume in 2023 will be 207,000 units, accounting for 24.1% of the total shipment volume of ITAI servers It is estimated that by 2026, the scale of the financial industry's ICT market will exceed 300 billion yuan. This growth trend shows that financial institutions are paying more and more attention to ICT products, and ICT has become an inevitable trend in the construction of financial technology. Taking the Bank of China, the purchase of financial ICT network security products in the past three years (Table 4.1 below) shows that the amount is increasing year by year, and the proportion of ICT products is increasing:

Table 4.1 - The purchase of financial ICT network security products

Year	**Projects**	**Total amount (RMB 100 million)**	**ITAI**	**Top winning bidders**
2022	37	8.6	68%	Qi'anxin (12), Venustech (9), Huawei (6)
2023	49	11.2	82%	Ahnheng Information (15), Sangfor (11), Green Alliance (8)
2024	18 (as of Q2)	3.9	91%	360 Digital Technology (7), Topsec (5), AsiaInfo (4)

Source: China Government Procurement Network (2024), Bank of China Official Website Procurement Column (2024)

At the same time, the global security information and event management (SIEM) market is showing a steady growth trend. In 2021, the global SIEM market size is about 4.31 billion US dollars, and it is expected to grow to 9.12 billion US dollars by 2030, with a compound annual growth rate of 9.8% (emergenresearch.com). In China, the financial industry continues

to increase its investment in network security, and the scale of China's financial network security market has reached hundreds of billions of RMB in 2022 (globalmarketmonitor.com.cn). The integration of AI technologies, as reflected in the PESTE analysis with global AI IT investment projected to grow at a CAGR of 31.9%, is further catalyzing demand for intelligent, analytics-driven SIEM solutions within the financial sector (https://www.secrss.com). Although there is currently a lack of specific data specifically for the SIEM market in the financial industry, considering the financial industry's high attention to data security and compliance, as well as the continued growth trend of demand for SIEM solutions in the global and Chinese markets, it can be inferred that the demand for SIEM in financial institutions such as banks will continue to grow strongly in the future.

The advancement of financial ICT usually follows the path of gradual replacement from peripheral systems to core systems. In the early stage, financial institutions mainly introduced ICT products in peripheral applications such as office systems and email systems; then, they gradually penetrated into core areas such as business systems and data centers. This process requires ensuring a smooth transition between old and new systems to avoid affecting business continuity. At the same time, financial institutions also need to strengthen the testing and verification of ICT products to ensure that their performance and security meet industry requirements.

In the process of promoting ICT innovation, financial institutions face three major challenges. First, the diversity of technical routes makes selection difficult. There are many types of ICT products on the market with different technical routes. Financial institutions often feel confused when making choices. Therefore, they need to strengthen communication with regulatory authorities and industry associations, refer to authoritative evaluations and peer experience, and formulate technical routes suitable for themselves. Secondly, insufficient understanding of the urgency and importance of ICT replacement has led to delayed action. Some institutions need to improve the awareness of ICT among all employees through internal training and publicity to ensure the smooth progress of replacement work. Finally, newly introduced ICT products may have compatibility and performance issues. Therefore, financial institutions should establish a sound testing mechanism and conduct sufficient verification before officially going online to ensure system stability.

The replacement of information technology in the financial industry is being accelerated according to a clear timetable and proportion requirements. By the end of 2023, the financial industry's PC and other terminal equipment have basically achieved 100% domestic substitution, and the replacement of some core systems has also begun. The replacement of financial information technology is carried out in stages, with terminal equipment and peripheral systems as the main focus in the early stage, and gradually infiltrating into core business systems. According to the plan, the financial industry will complete the

comprehensive domestic substitution of core systems in the next 3-5 years. The policy level requires central enterprises, state-owned enterprises and local state-owned enterprises to achieve 100% replacement of information technology by the end of 2027. As a key area, the financial industry needs to complete the localization of all information systems before this time point.

The Financial Information Technology Ecological Laboratory has played a key role in the promotion of banking information technology. The laboratory is led by the People's Bank of China and China Financial Electronicization Group Co., Ltd. to provide financial institutions with a safe and reliable information technology product evaluation platform. The laboratory has established a rich case library by collecting and selecting excellent solutions, providing a reference, replicable and popularizable guide for the implementation of information technology in the banking industry.

In terms of the evaluation of innovative products, China UnionPay issued the "China UnionPay Financial Information Technology Application Innovation Product Capability Evaluation Guidelines (Trial)" in 2022, which comprehensively evaluates innovative products from the two dimensions of security and controllability and product quality. The guidelines cover nine indicators and provide an important reference for the banking industry to select and apply innovative products. In addition, leading financial technology companies such as Hang Seng Electronics have actively participated in the construction of the innovative ecosystem, and many of their core system solutions have been selected as excellent solutions of the Financial Innovative Ecological Laboratory, covering multiple business areas, providing strong support for the digital transformation and independent innovation of the banking industry.

SIEM has multiple core application scenarios in the financial industry to enhance industry adaptability. First, in terms of compliance requirements, banks must introduce SIEM systems to meet regulatory requirements such as "Anti-Money Laundering (AML)", "Data Security Compliance", "Level 2.0", and "Financial Data Security Law" to achieve log retention, audit tracing, and violation detection. Secondly, in terms of threat detection, the SIEM system combined with UEBA and SOAR can effectively detect and respond to APT attacks, ransomware, account theft, internal risks and other security threats. Third, SIEM can aggregate logs from multiple systems in the bank's complex IT architecture, conduct cross-system correlation analysis, and improve event perception capabilities. Finally, through the combination of AI+SIEM, real-time risk control can be achieved, such as abnormal fund flow monitoring, illegal account operation detection, and cross-regional device access detection, thereby providing risk warning and automatic response capabilities.

The application and development of SIEM in the financial industry presents a diversified trend. In specific application scenarios, SIEM systems meet the compliance requirements of banks under laws and regulations such as "Anti-Money Laundering (AML)", "Data Security

Compliance", "Security Protection 2.0" and "Financial Data Security Law", and achieve regulatory requirements through log retention, audit tracing and violation detection. At the same time, SIEM combines UEBA and SOAR technologies to effectively respond to threats such as APT attacks, ransomware, account theft and internal risks, and aggregates multiple system logs in the bank's complex IT architecture to conduct cross-system correlation analysis and improve event perception capabilities. In addition, through the combination of AI and SIEM, banks can achieve real-time risk control, including abnormal fund flow monitoring, illegal account operation detection and cross-regional device access detection, thereby providing risk warning and automatic response capabilities.

From the perspective of development trends, driven by policies, the information innovation policy promotes the adoption of domestic SIEM solutions, the implementation of foundational laws such as the 'Data Security Law' and the 'Personal Information Protection Law', alongside detailed supporting regulations like the 'Data Security Management Regulations', requires SIEM systems to develop in the direction of compliance, threat detection and intelligent response. On the technical level, the combination of AI and SIEM improves automation capabilities and threat detection accuracy, and also needs to adapt to cloud computing and edge computing environments to support distributed security management. The banking industry is transforming towards proactive security operations, and SIEM will become more vertical and industry-oriented in the future, improving its adaptability to specific fields such as finance through customized security analysis models.

4.2.3. Competitor Analysis

The main competitors in the SIEM industry can be divided into three categories: international security vendors, local security vendors, and emerging security vendors. International security vendors such as IBM QRadar, Splunk, Palo Alto Networks, Fortinet, CrowdStrike, McAfee, RSA, and Arcsight have mature technologies and high market shares, but they are restricted by the information innovation policy in China, making it more difficult to enter the local market. Chinese security vendors include 360, Qi-Anxin, Venustech, DBAPP Security, Sangfor, and Green Alliance, which have strong brand influence and deep market resources in the domestic security market. Emerging security vendors focus on niche areas or special scenario needs, and pay attention to local adaptation and security compliance, but are still in the growth stage in terms of brand awareness and market expansion.

4.2.3.1. Analysis of international security vendors

IBM's security business remains a key component of its software portfolio (IBM, 2025). In terms of technology, QRadar uses AI-driven threat detection technology and supports hybrid cloud

architecture. However, QRadar faces challenges in the Chinese market. According to IDC data, its market share in China fell to 3.7% in 2022 (IDC, 2023). To cope with this dilemma, IBM is maintaining its position in the Chinese market by cooperating with local companies such as Inspur.

Splunk (NASDAQ: SPLK) was acquired by Cisco in a $28 billion deal finalized in March 2024 (Cisco, 2024). Before the acquisition, Splunk's revenue in fiscal 2023 was US$3.67 billion and its net profit margin was -14.3%. The company's technological advantage lies in its strong real-time data processing capabilities, which can reach the PB/day level. In order to expand its business in the Chinese market, Splunk adopted a localization strategy and established a joint laboratory with AsiaInfo Security in 2021. It is worth noting that under Cisco's ownership, Splunk's revenue for fiscal 2024 was reported at $4.216 billion, achieving significant financial improvements (Splunk, 2024).

Palo Alto Networks (NYSE:PANW)'s financial performance shows that the company's the company's revenue has demonstrated strong growth, reaching approximately $7.0 billion for the fiscal year ending July 2024, with profitability turning positive. The proportion of security business has increased year by year, from 76% in 2020 to 82% in 2022. In terms of technology, the company's Cortex XSIAM platform integrates AI automation technology, and its processing speed leads the industry by 30%. In terms of China's market strategy, Palo Alto Networks provides services through local MSPs such as ChinaSoft International, but the restriction rate in government cloud projects exceeds 70%.

Fortinet (NASDAQ:FTNT)'s financial data shows that the company's total revenue for the full year 2023 was $5.30 billion, with a gross margin stabilizing at around 76%. R&D investment continued to increase, reaching US$870 million in 2022. The company's FortiSIEM product supports log parsing of more than 2,000 devices, with a penetration rate of 12% in China's financial industry. However, due to data localization requirements, Fortinet lost 3 provincial government cloud orders in 2022, reflecting the company's challenges in compliance.

CrowdStrike (NASDAQ:CRWD) reported annual recurring revenue (ARR) of $3.44 billion for its fiscal year 2024, a year-on-year increase of 33%. The number of the company's customers increased from 5,431 in 2020 to 23,019 in 2023. However, affected by the "Cybersecurity Law", CrowdStrike's business growth in China is 20 percentage points lower than the average in the Asia-Pacific region.

McAfee was delisted after being acquired by a consortium in 2022. According to the last disclosed data, its enterprise security business had annual revenue of US$1.8 billion in 2021.

RSA Security was acquired by Symphony Technology Group for US$2.1 billion in 2020 and no longer discloses financial data separately.

Arcsight is now owned by Micro Focus. According to HP's financial report, Micro Focus' revenue in 2022 was US$2.73 billion.

Comparison of key competitive indicators between the international and Chinese markets:

Table 4.2 - Comparison of SIEM market competition indicators

Manufacturer type	Government market share	Financial industry bid winning rate	Number of certified ICT products
International manufacturers	9.20%	18.50%	$2.7 (average)
Domestic leading manufacturers	74.30%	63.80%	$28.4 (average)
Domestic small and medium-sized enterprises	16.50%	17.70%	$5.2 (average)

Source: IDC (2023)

4.2.3.2. Analysis of Chinese leading manufacturers

Table 4.3 - Financial Performance and ITAI Adaptation of Major Chinese Companies

Company Name	2023 Revenue (100 million RMB)	2022 Revenue (100 million RMB)	Net Profit Margin (2023)	Core Products	ITAI Adaptation Progress
Qi'anxin	64.42	≈62.19	≈1.1%	NGSOC	Full stack adaptation
Venustech (Venusstar)	45.07	≈44.37	≈16.4%	Taihe SOC	Complete Kunpeng certification
Anheng Information	21.7	≈19.80	≈-16.6%	AiLPHA platform	Tongxin UOS certification
Sangfor	76.62	≈74.13	≈2.6%	XDR platform	Kylin OS adaptation

360 Digital Security	90.55	95.21	≈-5.4%	Digital security brain	MIIT pilot
Green Alliance Tech	16.81	26.29	≈-58.1%	Intelligent security operation platform	Phytium CPU adaptation

Source: Compiled by author based on Qi’anxin (2023), Venustech (2023), Anheng Information (2023), Sangfor (2023), 360 Digital Security (2023), Green Alliance Tech (2023).

According to the data of CCID's "China Cybersecurity Industry White Paper (2023)", the cybersecurity market shows a high market concentration and obvious Matthew effect. The market share of the top 5 manufacturers increased from 54% in 2020 to 68% in 2022, while the number of tail manufacturers (revenue <100 million) decreased from 237 in 2020 to 153 in 2022, a cumulative decrease of 36%. (Source: 2023 China Cybersecurity Market and Enterprise Competitiveness Analysis report)

The growth rate of head manufacturers is relatively fast. Taking Qi'anxin as an example, as a leading domestic enterprise, its revenue growth rate in 2022 reached 27.6%, far exceeding the industry average growth rate of 14.3%. According to the annual report data of each company, Qi'anxin's revenue in 2023 reached ¥6.44 billion, and Sangfor's revenue reached ¥7.66 billion, both maintaining rapid growth.

The profit margin of standardized products is being compressed. Taking the SOC system as an example, its gross profit margin dropped from 73% in 2019 to 58% in 2022, and the unit price of SOC in the financial industry dropped from 1.5 million/node to 900,0003. This price war is partly due to the oversupply of homogeneous products caused by domestic substitution, and the increased bargaining power brought about by the increase in the proportion of centralized procurement of government and enterprise customers. (Source: Analysis of the market competition pattern of listed companies in China's cybersecurity industry in 2023)

Ecological competition has become a new trend. Taking Qi'anxin as an example, it has built an industry alliance including 38 domestic chip/OS manufacturers and 152 industry ISVs. Through ecological cooperation, Qi'anxin has achieved a 63% customer cross-selling rate (cross-selling rate refers to the proportion of new customers reached through ecological partners), and the ecological revenue contribution ratio has reached 38%. This shows that cybersecurity competition has been upgraded from single product confrontation to competition between ecosystems. (Source: Is the price war in the cybersecurity industry so fierce)

Innovation adaptation has become the key, and domestic leading manufacturers generally attach importance to innovation adaptation. For example, Qi'anxin has achieved full-stack adaptation, Venustech has completed Kunpeng certification, and Ahnheng Information has obtained Tongxin UOS certification. This reflects that manufacturers are actively responding to the strategic requirements of national information technology application innovation. (Source: Market competition landscape of China's cybersecurity industry in 2023 - Sina Finance)

The competitive landscape of China's SIEM market is undergoing major changes. New entrants face multiple barriers, including: the technical threshold of meeting the triple certification of Information Security Protection 2.0, Information Innovation and Key Infrastructure Protection, and the ecological threshold of multiple local partners' endorsement to enter the provincial government procurement shortlist. The competition dimension has also changed from the single product performance competition (such as throughput and detection rate) in the past few years to the recent full-stack Information Innovation adaptation capabilities and ecological resource integration. Policy factors have further exacerbated market changes, such as the dynamic adjustment mechanism of the Information Innovation Catalog to remove some technologically lagging manufacturers, and the mandatory requirement that the proportion of cybersecurity expenditures in the financial and energy industries should not be less than a certain proportion of the total IT budget. These changes have redefined the competitive landscape of the SIEM market.

4.2.4. Porter’s Five Forces Analysis

4.2.4.1. Industry Rivalry of Existing Competitors

The domestic SIEM market is highly competitive and is dominated by local vendors such as Qi'anxin, Venustech, Sangfor, Ahnheng Information, and Green Alliance Technology. These companies have been deeply involved in industries such as government, finance, energy, and communications for many years, with high brand awareness and a solid customer base, forming a high market barrier. At the same time, international vendors such as IBM QRadar and Splunk are restricted by the ICT policy, and their market share has gradually shrunk, but some vendors have maintained their competitiveness by cooperating with local companies (such as Splunk and AsiaInfo Security). In addition, the intensified competition among domestic vendors has led to the emergence of price wars, and the gross profit margin of industry standardized products has dropped from 75% in 2019 to 63% in 2022, further intensifying the intensity of competition.

Table 4.3 indicates that revenue concentration is high: Sangfor leads with RMB 7.66 billion (2023), followed by 360 Digital Security at RMB 9.06 billion, while mid-tier competitors like

Anheng Information (RMB 2.17 billion) and Green Alliance Tech (RMB 1.68 billion) face margin compression, with Green Alliance experiencing a net profit margin of -58.1% in 2023. This suggests that scale and ecosystem advantages are becoming increasingly critical to profitability and market viability.

Risk Level: HIGH

4.2.4.2. Threat of New Entrants

The SIEM industry has high technical barriers, involving complex technologies such as log management, big data analysis, threat detection, AI analysis, and security operations automation (SOAR). New entrants need a long time to accumulate data and improve algorithms. Industries such as finance, government, and energy have high requirements for security products and complex procurement processes, which makes customer acquisition costs and brand trust thresholds high. However, the ITAI policy encourages the development of domestic security products and supports emerging companies through government procurement and industrial funds, which provides opportunities for new entrants, but also brings more competition. In addition, new entrants also need to complete compatibility and adaptation with domestic servers (such as Huawei, Inspur), operating systems (Tongxin UOS, Galaxy Kylin) and databases (Da Meng, Renda Jincang), which increases adaptation costs and time.

In 2024-2025, policy support has become more structured: the "Market Access Ten Articles" (2024) explicitly listed autonomous and controllable computing as a priority sector, creating preferential procurement conditions for new entrants. Additionally, the "National Emerging Industry Innovation Center Management Measures (Draft for Comment)" encourages financial institutions to invest in industrial innovation centers, providing direct funding channels for startups like Dataori. This two-way support—through procurement preferences and R&D funding—lowers the barrier to market entry for well-positioned new entrants with AI/ITAI capabilities.

Risk Level: MEDIUM

4.2.4.3. Bargaining Power of Suppliers

With the rise of domestic software and hardware ecosystems, supplier concentration has increased, local suppliers have mastered key technologies, and their bargaining power has increased. SIEM vendors need to adapt to domestic CPUs (Kunpeng, Feiteng), operating systems (Galaxy Kylin, Tongxin UOS) and databases (Da Meng, Jincang), which increases R&D costs and operational pressure. In addition, cloud computing platform providers such as Alibaba Cloud and Tencent Cloud are gradually taking control of the cloud security market, and their cloud-native security products may replace traditional SIEM solutions, forcing

vendors such as Dataori to establish partnerships with cloud service providers to avoid being marginalized.

The generative AI boom of 2024-2025 has further concentrated supplier power: leading cloud platforms (Alibaba Cloud, Tencent Cloud) are now not only infrastructure providers but also direct competitors in the SIEM market, offering cloud-native security analytics integrated into their platforms. This vertical integration creates a "take it or leave it" dynamic where traditional SIEM vendors must either partner with cloud providers on unfavorable terms or accept margin compression. IDC projects that global AI IT investment will reach $1.26 trillion by 2029 (CAGR 31.9%), with Chinese cloud providers capturing an increasing share of this market, further tilting leverage toward suppliers.

Risk Level: MEDIUM

4.2.4.4. Bargaining Power of Buyers

Governments and financial institutions are the main purchasers of SIEM. These large customers have large purchase scales but high security requirements and strict compliance standards, which give them strong bargaining power. In addition, the financial industry has an increasing demand for customized SIEM products, and vendors need to invest additional resources to improve functions. Since the procurement cycle of financial and government customers is long (the average contract cycle is more than 5 years), customers tend to choose long-term partners, which further enhances their bargaining power.

Recent market dynamics further entrench buyer power: according to Table 4.1, Bank of China's procurement data (2022-2024) shows that ITAI product adoption has surged from 68% (2022) to 91% (Q2 2024), while procurement volumes fluctuate (49 projects in 2023 vs. 18 in H1 2024), suggesting that buyers are becoming more selective and consolidating vendors. Contract terms have become more stringent: typical financial institution contracts now mandate 7×24-hour response, 1-hour fault recovery SLAs, and daily penalties for detection rates falling below 90% of promised levels. This contractualization of service obligations significantly increases vendor operational burden and reduces profit margins.

Risk Level: HIGH

4.2.4.5. Threat of Substitutes

SOAR platforms are gradually replacing some SIEM functions and reducing dependence on SIEM through automated response. At the same time, the rise of cloud-native security platforms, such as the log analysis and threat detection functions provided by Alibaba Cloud and Tencent Cloud, may replace traditional SIEM. In addition, XDR (Extended Detection and Response) products such as CrowdStrike and SentinelOne combine endpoint detection with SIEM functions, which has also weakened the market demand for traditional SIEM to a certain extent.

AI-driven security orchestration represents a second-order threat: Dataori's AI Copilot strategy directly competes with SOAR platforms' automation capabilities. If market-leading SOAR vendors (e.g., Palo Alto Networks, Splunk) integrate AI-driven log analysis more effectively than traditional SIEM vendors, the value proposition of standalone SIEM degrades significantly. The 2024-2025 period marks a critical inflection point where AI maturity in competing platforms (SOAR, XDR, cloud-native solutions) determines whether traditional SIEM vendors can maintain differentiation.

Risk Level: HIGH

4.2.5. Consumer Analysis

The demand for SIEM in the banking industry is mainly driven by policy requirements and industry compliance pressure. The "Innovation and Development Plan for Information Technology Application in the Financial Industry (2022-2025)" requires the banking industry to complete the core system transformation by 2025, and the localization rate of network security products will reach 100%. The guidance issued by the China Banking and Insurance Regulatory Commission clearly requires "establishing an independent and controllable security protection system" to promote the localization deployment of security systems such as SOC and SIEM. At the same time, the banking industry must meet the requirements of Level 3 of the Information Security Protection 2.0 and the technical requirements of the financial industry standard JR/T 0171-2020.

Typical demand scenarios in the banking industry include ICT adaptation, security capabilities and service capabilities. ICT adaptation requires full stack localization, adaptation to domestic CPUs, operating systems and databases. Security capability requirements include real-time processing of large-scale logs, high-precision threat detection, and attack tracing and forensics. Service capability requirements include 7×24 hours emergency response and long-term ICT adaptation and upgrade services. In the 2023 bidding, a large state-owned bank clearly required the SOC system to "pass the ICT product catalog certification of the Ministry of Industry and Information Technology." source: (Bank of China Tender Announcement)

The characteristics of banking procurement vary depending on the type of bank. Large state-owned banks prefer customized solutions, joint-stock banks focus on modular capabilities, and city commercial banks and rural commercial banks prefer standardized products. The core dimensions of bid evaluation include technical capabilities, service guarantees and compliance qualifications.

Industry trends show that the demand for the integration of SOC with AI and zero-trust architecture has increased significantly. Small and medium-sized banks tend to purchase lightweight, low-cost standardized security products, and regulators intend to promote SOC capability maturity assessment.

In terms of cases, the Bank of China's ITAI SOC construction project requires full-stack ITAI adaptation, threat detection real-time and log retention capabilities. A city commercial bank's zero-trust architecture procurement project requires compatibility with domestic operating systems and financial security level 3 certification. source: (China Government Procurement Network, Public Service Platform for Bidding and Tendering)

The banking industry's ITAI demand has shown significant growth, with the number of public ITAI projects in the financial sector increasing by approximately 200% in 2022 compared to 2021. The focus has shifted towards core business systems and cloud resource network infrastructure construction. Large state-owned banks have set ambitious targets for system transformations, with ICBC aiming to complete about 370 system transformations, Agricultural Bank of China targeting 200, and Bank of Communications planning to complete about 200 transformations by 2023. (source: 2023 China Financial ITAI Development Research Report)

Compliance requirements for ITAI projects in the banking industry include high-frequency indicators such as Level 3 of the Multi-Level Protection Scheme 2.0 (MLPS 2.0) with a 100% occurrence rate, requiring log retention for ≥6 months and full coverage of two-factor authentication. Financial industry guidelines have an 89% occurrence rate, requiring compliance with JR/T 0171-2020 "Financial Network Security Specification".

The procurement model of the banking industry varies according to the type of bank, showing different characteristics. The decision-making cycle of large state-owned banks is long (6-12 months), with low price sensitivity, but deep customization is required to connect to the internal risk control system. The decision-making cycle of joint-stock banks is shorter (3-6 months), with medium price sensitivity, and they tend to prefer modular options. City commercial banks and rural commercial banks have the shortest decision-making cycle (1-3 months), high price sensitivity, and prefer standardized products. In terms of bid evaluation weight distribution, technology accounts for 55% (including 30% for POC testing), business accounts for 30% (including 15% for trust innovation qualifications), and price accounts for 15%. Typical contract terms include 7×24-hour response, fault recovery within 1 hour, a penalty mechanism for deducting service fees on a daily basis if the detection rate is lower than 90% of the promised value, and 5 years of free trust innovation adaptation and upgrade services.

4.3. Internal Situational Analysis

4.3.1. Characterization of the company

Dataori is a SIEM vendor driven by big data technology and machine learning, focusing on security data analysis, log management and compliance auditing. The founding members of the team have been deeply involved in the SIEM industry for more than 20 years and have

been engaged in SIEM product technology research for a long time. On this basis, combined with China's information innovation environment, they have created a self-developed SIEM product that is highly adapted to the local market.

At present, Dataori has implemented multiple projects in the financial, energy, communications, government and other industries. Typical customers include one of the six state-owned banks, Sinopec, China Mobile and government agencies, proving that its products have market competitiveness and landing application capabilities. The company's annual revenue is stable at 3-5 million yuan, and R&D personnel account for as high as 80%, reflecting its technology-driven development model. Its offices are located in Shanghai and Beijing, and a R&D center has been established in Xi'an, gradually forming regional market coverage capabilities.

4.3.2. Mission, vision and values

Mission - Dataori's mission is to redefine the way SIEM is used, to create an intelligent, localized, and easy-to-use next-generation SIEM solution, to lower the skill threshold, and to enable SOC teams to focus on real security analysis rather than tedious data processing. Through AI-driven security intelligent assistant (AI Copilot), Dataori enables security analysts to query logs, analyze events, correlate alarms, and generate reports like a conversation, completely changing the inefficient mode of traditional SIEM that relies on handwritten SQL and manual data screening. We are deeply compatible with the domestic ecosystem and provide localized SIEM solutions adapted to the Chinese market, enabling enterprises to achieve efficient and secure operations in an autonomous and controllable environment. Dataori is committed to making security teams operate more efficiently, smarter, and more accurately, achieving reduced staff and increased efficiency, reducing the labor cost of SOC, and ensuring the accuracy of security responses.

Vision - Dataori is committed to becoming the leading AI-driven SIEM solution provider in the Chinese market, promoting the intelligent, automated, and localized adaptation of the Security Operation Center (SOC). We hope to make SIEM easier to use, more efficient, and more in line with enterprise needs through AI Copilot and intelligent security operations, so that SOC teams can quickly get started, accurately correlate and analyze, reduce false positives, and improve threat response capabilities, ultimately reducing enterprise security operation costs and improving overall security defence capabilities.

Values - Dataori's SIEM platform takes intelligence and efficiency as its core advantages. Through AI Copilot technology, the platform subverts the traditional way of using SIEM and

makes security analysis as simple as a conversation. AI automatically correlates security events, reducing the repetitive work of SOC analysts and allowing them to focus on real threat analysis. At the same time, AI automatic attribution analysis improves the accuracy of alarm processing, reduces the workload of the SOC team by 30%-50%, achieves staff reduction and efficiency improvement, reduces enterprise security operation costs, and ensures faster and more accurate response capabilities.

The platform is also open, adaptable, and collaborative. It adopts an open data architecture, supports multiple data platforms, and avoids the limitations of traditional SIEM in data storage. The platform is deeply adapted to the Security Protection Level 2.0, financial security standards and security requirements of critical information infrastructure, supports domestic CPUs, OS and databases, and helps domestic substitution. The AI security assistant promotes efficient collaboration among SOC team members, reduces technical barriers, and enables junior analysts to quickly master SIEM operations. These features enable the SOC team to transform from passive response to active analysis, precise tracing and secure closed-loop management, and comprehensively improve the security operation process.

4.3.3. Core Competencies and Resources

Dataori's primary competitive advantage lies in its AI-driven SIEM platform with advanced threat detection and automated response capabilities. The AiLPHA platform integrates machine learning algorithms for behavioral analysis, unknown threat detection, and real-time anomaly detection, addressing a critical market gap identified in customer research where 41.54 percent of respondents ranked AI-powered threat detection as a top feature priority, and 55.38 percent identified lower false-positive rate in UEBA as essential. The company has achieved Tongxin UOS certification for operating system compatibility and demonstrated full integration capability with domestic computing ecosystems including Kunpeng CPUs and Kingbase databases, positioning Dataori favorably in the ITAI segment. This strategic positioning proves important given the increasing preference for localized solutions among government and financial institutions, with ITAI-adapted SIEM solutions projected to capture substantial growth through 2030.

The core development team comprises cybersecurity professionals with extensive industry experience, including specialists in cloud-native architecture, AI and machine learning engineering, and compliance frameworks. The company has established partnerships with leading universities for research and development in emerging threat detection methodologies. Research and development represents 65 percent of annual revenue, ensuring continuous innovation and rapid adaptation to market demands. This commitment significantly exceeds the industry average estimated at 25 to 30 percent for comparable SIEM vendors and proves

essential for maintaining competitive differentiation in the AI-augmented security landscape. The workforce composition shows 80 percent dedicated to research and development activities, reflecting the technology-intensive nature of the business and the company's commitment to product excellence.

Dataori has developed a channel partner network consisting of 3 to 5 Managed Service Providers and regional integrators who provide onsite implementation, customization, and ongoing support services. This model allows Dataori to focus on product development and innovation while leveraging partner expertise for service delivery. The strategy aligns with market trends toward ecosystem collaboration, evidenced by established players like Qi'anxin whose ecosystem model comprises 38 domestic chip and OS manufacturers and 152 industry independent software vendors, demonstrating ecosystem maturity as a competitive necessity. The partner network provides scalable capacity for customer implementation and support without requiring proportional headcount growth, with potential to expand to 5 to 10 partners as the customer base expands across different regions and industry segments.

4.3.4. Business Model and Revenue Structure

Dataori operates a hybrid revenue model combining perpetual software licenses, annual subscription, and professional services, though the company remains in the early commercialization stage with modest revenue to date. Software licenses represent the primary revenue stream and typically involve one-time purchases for on-premise installation, with contracts usually spanning three to five years at values around 500,000 RMB per license. The subscription and managed services component through cloud-hosted SaaS arrangements generally ranges from 100,000 to 200,000 RMB annually per client, with higher margins around 70 percent. Professional services including implementation, customization, and training account for a smaller portion of revenue, delivered in partnership with channel providers and typically generating margins around 50 percent as these services connect directly to license sales. The existing customer base of 40 clients accumulated over five years represents a carefully selected group of strategic deployments rather than mass-market penetration, reflecting the company's focus on product refinement and market validation before aggressive commercial expansion.

Current financial performance reflects the reality of a company transitioning from product development to market commercialization. Annual revenue currently stands at approximately 2 million RMB based on the installed customer base and mix of license, subscription, and services revenue. Research and development continues to consume a significant portion of operational resources as the company maintains focus on product innovation, AI model refinement, and ITAI certification requirements to ensure the platform remains competitive as

the market matures. Sales and marketing activities remain relatively limited given the early-stage nature of commercial expansion, though this area represents a focus for the commercial development plan outlined in this thesis. General business operations including legal, compliance, and human resources are managed efficiently given the small organizational footprint. While gross margins on software licenses remain healthy at approximately 75 percent and subscriptions near 70 percent, the company's limited current revenue reflects the challenges typical of early-stage technology ventures where significant upfront investment precedes meaningful commercial returns. The revenue model is fundamentally sound, but execution of the commercial development plan is essential to achieving growth targets and demonstrating the scalability of the business.

4.3.5. Current Customer Base and Market Position

The existing customer base comprises 40 enterprise clients accumulated over five years of product development and market validation. These customers are distributed across seven primary industry verticals, representing strategic deployments that helped refine the product for different market segments. Banking and financial institutions account for approximately 30 percent of the customer base, representing the highest-value segment with the largest individual contracts. Telecommunications operators comprise about 20 percent of clients, driven by their interest in localized security solutions aligned with ITAI initiatives. Government bodies and state-owned enterprises make up 17.5 percent of the customer base, representing strategically important deployments despite the longer sales cycles typical of public sector procurement. Manufacturing, energy, and related sectors account for 15 percent of customers. Insurance and securities firms represent 12.5 percent of the base, and healthcare organizations currently constitute only 5 percent with 2 clients, though this represents a significant growth opportunity given increasing regulatory requirements for patient data protection.

Current customer renewal rates stand at 60 percent, with six out of every ten customers extending or upgrading their contracts annually. The average contract value at initial purchase ranges from 500,000 RMB to 1 million RMB, with meaningful variation by sector reflecting different deployment scales and use cases. Multi-year arrangements covering three to five years are common, particularly within regulated industries where security infrastructure decisions carry long-term compliance implications. The net revenue retention rate currently approximates 95 percent, indicating a stable but not rapidly expanding customer base in terms of spending per client. This metric suggests opportunity for improvement through product upgrades and migration of customers to more comprehensive or cloud-based offerings, which would increase the value extracted from the existing customer relationships and accelerate revenue growth without requiring proportional increases in customer acquisition.

Within the broader competitive landscape, Dataori operates as an emerging challenger in the early stages of market entry. The company's current annual revenue of approximately 2 million RMB positions it far below established market leaders like Qi'anxin at 6.44 billion RMB, Sangfor at 7.66 billion RMB, and 360 at 9.06 billion RMB, and also below mid-tier competitors like Anheng Information at 2.17 billion RMB and Green Alliance Tech at 1.68 billion RMB. However, this position as a new entrant carries distinct advantages that form the basis for the commercial development plan. The primary points of differentiation include an AI-first technical architecture that reflects current market priorities, comprehensive ITAI certification addressing regulatory requirements, and flexibility in deployment models. The company's positioning targets customers seeking capable, affordable localized SIEM solutions from a vendor willing to work closely on customization and integration. The existing customer base, while small in absolute terms, represents proof of concept for the product-market fit hypothesis and provides the foundation for scaling through the commercial initiatives outlined in this plan.

Table 4.4 - Customer Portfolio by Industry Vertical

Industry Vertical	Customer Count	Estimated % of Base	Primary Use Cases	Revenue Contribution
Banking & Finance	12	30%	Compliance (PCI-DSS, China ITAI), threat detection	Highest per-customer value
Telecommunications	8	20%	Network security, infrastructure monitoring	Stable revenue base
Government & SOEs	7	17.5%	Critical infrastructure protection, policy compliance	Strategic relationships
Manufacturing & Energy	6	15%	Operational technology security	Growth opportunity

Industry Vertical	Customer Count	Estimated % of Base	Primary Use Cases	Revenue Contribution
Insurance & Securities	5	12.5%	Financial data protection, audit compliance	High-value niche
Healthcare & Medical	2	5%	Patient data protection, compliance	Expansion opportunity
Total	**40**	**100%**		**2M RMB annual revenue**

Source: Author (2025)

4.3.6. Customer Acquisition Capabilities

The sales organization currently operates with three dedicated account executives covering the domestic market with support from pre-sales and customer success functions. This lean structure reflects both the early-stage nature of the company and a deliberate strategy to avoid overhead while focusing on executing the commercial development plan outlined in this thesis. Sales compensation includes base salary plus variable commission typically structured at 15 to 20 percent of contract value, creating alignment between individual effort and company revenue generation. The typical acquisition cycle runs approximately 12 months from initial prospect qualification through contract signature, though this varies by segment with financial institutions averaging 14 to 18 months due to procurement procedures, mid-market customers typically completing purchases in 6 to 9 months, and government deals frequently requiring 12 to 24 months due to budget cycle coordination and policy reviews. Current sales success rates show that roughly 15 to 20 percent of qualified opportunities convert to closed deals, representing typical enterprise sales velocity for security solutions in the market.

Customer acquisition to date has occurred through multiple channels, providing lessons for scaling the commercial development plan. Direct sales efforts account for approximately 40 percent of customer acquisition, with dedicated account executives targeting institutions through direct outreach, participation in industry events, and referrals from existing customers. Channel partners and Managed Service Providers represent approximately 50 percent of customer acquisition, as regional systems integrators and MSPs bundle Dataori SIEM into

their managed security offerings. Demand generation and marketing activities contribute about 10 percent of customers through limited direct marketing investment in content, webinars, and conference participation. The customer acquisition cost currently ranges from 75,000 to 100,000 RMB per customer, including sales staff allocation, marketing spend, and partner incentives. The payback period for direct sales arrangements falls around 8 to 10 months based on gross margins of 60 to 70 percent on average 500,000 RMB contracts, while channel arrangements require 10 to 12 months accounting for partner margin sharing. Current capacity with three direct salespeople stands at approximately 10 to 16 new customers yearly from direct efforts, with channel partnerships providing potential to reach 30 to 50 new customers annually, though this capacity remains untapped given the early commercialization stage.

The value proposition emphasized for customer acquisition focuses on practical benefits that resonate with buyer priorities in the current market context. Dataori positions its solution as 30 to 40 percent less expensive than competitors like Qi'anxin or Sangfor for comparable capabilities, a significant advantage for price-sensitive mid-market and government segments. Full localization certification addresses regulatory compliance requirements that represent non-negotiable criteria for many customers in regulated industries. The AI-first approach directly addresses priorities identified in customer research where 41.54 percent ranked AI-powered threat detection as a top feature need and 55.38 percent highlighted reduced false positives as essential. Support for both on-premise and cloud deployment models accommodates the diverse infrastructure situations that customers face across different organizational contexts and regions. This value proposition, combined with the company's willingness to work closely with customers on customization, forms the foundation for competitive positioning as the company pursues market expansion.

Table 4.5 - Customer Acquisition Channels

Channel	**% of Current Customers**	**Typical Activities**	**Scaling Potential**
Direct Sales	40%	Account executive outreach, industry events, customer referrals	10-16 new customers annually
Channel Partners / MSPs	50%	Systems integrators bundling SIEM with managed services	30-50 new customers annually

Channel	% of Current Customers	Typical Activities	Scaling Potential
Demand Generation / Marketing	10%	Content marketing, webinars, industry conferences	5-10 new customers annually
Total	**100%**		**Untapped: 40-75 potential new customers annually**

Source: Author (2025)

4.3.7. Customer Retention and Lifecycle Management

Customer retention represents a critical area of focus given the modest current revenue base and the importance of establishing a stable foundation for growth. The company's retention strategy emphasizes proactive account management and engagement with existing customers. While formal customer success managers are not yet dedicated to individual accounts, key customer relationships receive regular attention from senior technical staff and product management. Quarterly business reviews with major accounts communicate product roadmap developments and customization possibilities that increase customer value realization. Support services are structured on a tiered basis with rapid response to critical issues and dedicated support for larger customers. These engagement practices aim to ensure high customer satisfaction and provide opportunities to understand evolving customer needs that inform future product development.

The 60 percent renewal rate, while respectable for a young company, represents an area where improvement directly translates to revenue stability and growth potential. Understanding and mitigating churn risk requires acknowledging the competitive landscape and market dynamics affecting customer relationships. Customers actively evaluate alternative solutions including XDR products from established vendors as well as cloud-native options from major cloud providers. The company responds to this competitive pressure by emphasizing integration capabilities that reflect its focused architecture, cost advantages that remain significant, and ITAI certifications that represent a strategic advantage in the current regulatory environment. Price sensitivity particularly affects mid-market and government customers, requiring careful attention to value delivery justifying contract renewal and expansion. Product-market fit evidence from customer interactions and feature requests shows strong demand for AI-driven analytics and automated response capabilities that align with the technical roadmap,

supporting confidence that retention improvements are achievable as the product matures and the company strengthens customer relationships through improved support and engagement.

4.3.8. Financial and Operational Readiness

Current financial performance reflects the reality of a company in the early commercialization phase transitioning from primarily research and development activities toward market expansion. Annual revenue of approximately 2 million RMB, while modest in absolute terms, represents proof of concept for the business model and validates customer willingness to purchase the product. The operating structure remains lean with most resources allocated to product development, customer support, and initial sales activities. The company has been self-funding its operations and now stands at an inflection point where the commercial development plan outlined in this thesis represents a critical investment in market expansion. The financial capacity available for commercial development initiatives remains constrained by current revenue levels, placing emphasis on efficient execution and measured scaling of sales and marketing activities. This constraint actually creates focus, as the company must prioritize high-impact initiatives that generate measurable returns.

The organizational structure currently comprises approximately 20 to 25 employees focused primarily on research and development, with smaller teams supporting customer success and sales. Three dedicated salespeople represent the commercial front line, supported by pre-sales engineering and customer success staff. This lean structure reflects the early stage of market commercialization and provides both a constraint and an opportunity. The constraint is obvious: the current organization cannot simultaneously support aggressive sales expansion while maintaining product development. However, the opportunity lies in the potential for focused, high-efficiency growth as the company strategically adds specialized talent in sales, marketing, and customer success. Service delivery through existing channel partners provides flexible capacity for customer implementation and support without requiring proportional headcount growth. The technical infrastructure supporting the product is maturing and has proven reliable across the existing customer base. Product development investment remains prioritized to ensure competitive capability as the market evolves.

Risk assessment across operational dimensions reveals several factors requiring attention as the company pursues market expansion. Competitive pressure from established vendors represents a significant long-term risk, though the company's early focus on specific market segments and AI differentiation provides near-term protection. Execution risk on the commercial development plan is material given the limited sales and marketing infrastructure and the company's reliance on channel partners for customer acquisition scale. Key person dependency represents a risk given the small leadership team, though this is typical for early-stage technology ventures. Cash flow management becomes increasingly important as the company invests in sales and marketing to achieve the growth targets outlined in the

commercial development plan. Regulatory changes in ITAI or cybersecurity requirements could accelerate or constrain market adoption, requiring continuous monitoring and flexibility in the product roadmap. Each of these risks is manageable through focused execution and prudent resource management, though they underscore the importance of disciplined growth and careful capital allocation during this critical period for the company.

Dataori stands at a critical inflection point in its development. The company has successfully developed and validated a competitive SIEM product through its work with 40 customers over five years, and the existing customer base demonstrates proof of concept for the business model. However, current revenue of approximately 2 million RMB clearly demonstrates that the company remains in the early commercialization stage, operating as a new entrant to the market. The commercial development plan outlined in this thesis represents the roadmap for systematically scaling the business from this foundation. Success requires disciplined execution on customer acquisition and retention, efficient allocation of resources to highest-impact initiatives, and continued product investment to maintain competitive differentiation. The opportunity is substantial given the favorable market conditions and regulatory tailwinds supporting localized SIEM solutions, but execution remains paramount during this critical period of market expansion.

4.4. SWOT Analysis

4.4.1. Strengths

- With 20 years of industry technology accumulation in the SIEM industry, the company has a deep understanding of the international SIEM architecture and functional characteristics, combining the world's leading technology concepts with localized needs to create highly adaptable products.
- Dataori has completed full adaptation with domestic operating systems (Tongxin UOS, Kylin) and CPUs (Kunpeng, Feiteng). This compliance with the "Information Technology Application Innovation" (ITAI) environment is a key advantage for entering government and banking sectors.
- There are already successful implementation cases in the financial industry, including one of the six state-owned banks, a national joint-stock bank, and Sinopec. This forms a benchmark effect that is conducive to further expansion in the banking market.
- The proprietary AiLPHA platform integrates machine learning for automated threat detection. This "AI+SIEM" model establishes a technical barrier by significantly reducing false alarm rates and improving detection accuracy.

- By launching lightweight SaaS SOC solutions for SMEs, the deployment cost can be reduced by 60% compared to traditional localized SIEM, which is helpful to develop the long-tail market.

4.4.2. Weaknesses

- Insufficient capital investment is a challenge. Dataori's annual revenue is approximately 2 million RMB. Compared with leading manufacturers like Qi'anxin or Venustech (annual revenue of 4-9 billion RMB), its R&D investment capacity is limited, which may affect the speed of product innovation.
- Brand influence is currently limited. In the financial industry, established brands have higher recognition. Government and bank customers tend to choose verified products from large manufacturers, necessitating stronger market promotion.
- Ecological resources are weak compared to leaders who bind customers through government procurement alliances. Dataori is still in the independent operation stage and has not yet built a large-scale ecological cooperation network.
- Delivery capability is restricted by team size (only 20 people, with 80% in R&D). There are bottlenecks in large-scale project delivery and customer support compared to the national service networks of leading manufacturers.

4.4.3. Opportunities

- Government policies strongly support ICT innovation (ITAI). With the target for special procurement from SMEs set to increase to 40% by 2025, Dataori is positioned to obtain more orders from government and financial institutions.
- The financial ICT innovation market is projected to grow significantly, with vast potential in sub-sectors like city commercial banks and insurance institutions. Dataori can deeply cultivate this small and medium-sized bank market (potential scale of 3 billion RMB).
- The market trend increasingly favors AI-driven security. As identified in consumer analysis, the shift towards "AI+SIEM" to reduce SOC workloads aligns perfectly with Dataori's core technology, offering a chance to build competitive advantage.
- Ecological cooperation offers new channels. Since 60% of leading manufacturers open API interfaces, Dataori can join the ICT innovation ecological alliance by integrating domestic databases and OS to enhance market access.
- Capital market support remains active for cybersecurity. Dataori can utilize this environment to apply for industrial fund support (targeting 30 million+ RMB) to increase R&D investment.

4.4.4. Threats

- Macroeconomic headwinds pose a risk. As analyzed in the economic context, the forecasted GDP growth moderation to approximately 4.5% in 2025 (IMF, 2024) may lead to tighter IT budgets and longer procurement cycles for some clients.

- Technical barriers of leading manufacturers are high. Top competitors like Qi'anxin possess patent reserves exceeding 2,000, occupying 85% of the market share in party and government agencies, making it hard to acquire large-scale customers.
- Price war risks are increasing. The gross profit margin of the SIEM industry has dropped from 75% in 2019 to 63% in 2022. Intensified market competition may lead to further price wars, affecting Dataori's profitability.
- Alternative technologies such as XDR and SOAR are gradually replacing traditional SIEM. Additionally, cloud-native security solutions from giants like Alibaba Cloud may weaken Dataori's competitiveness in the cloud market.
- The customer procurement cycle is long, especially in the financial industry (average POC cycle ≥ 6 months). This complicated process puts significant pressure on the capital turnover of small and medium-sized enterprises.

4.5. Objectives of this plan

This one-year commercial plan establishes clear and actionable goals to accelerate Dataori’s transition from a technology-focused startup to a commercially scalable player in the domestic SIEM market. All objectives are defined to be achieved within twelve months and are grounded in the company’s current situation, with approximately RMB 2 million in annual revenue and a base of around forty enterprise clients. The plan prioritizes balanced progress across revenue growth, new customer acquisition, and customer retention.

Revenue Growth Target: Achieve total annual SIEM-related revenue of RMB 4 million within the next twelve months. This represents roughly a doubling of the current annual revenue level and will be driven by a combination of new client wins and higher renewal rates from the existing customer base.

New Customer Acquisition: Secure 10–12 new paying enterprise clients within the target verticals of banking and finance, telecommunications, and government or state-owned enterprises during the one-year plan period. This expansion of the client roster by approximately 25–30% is essential for achieving the overall revenue target and for building a more visible market presence.

Customer Retention Improvement: Increase the annual customer contract renewal rate from the current level of about 60% to at least 70% within one year. This will be supported by a more structured customer success approach, including proactive account management for roughly the top 20% of clients by revenue and strengthened post-sales support.

Channel Partnership Expansion: Grow the network of active, revenue-generating channel partners from 3–5 to 6–8 over the next twelve months. The focus will be on recruiting partners

with established footprints in secondary cities and in specific verticals where Dataori currently lacks direct sales coverage.

Market Positioning and Brand Visibility: Be formally shortlisted in at least 8–10 competitive tenders (RFPs) within the financial and public sectors during the plan period. In parallel, build initial brand credibility by obtaining speaking roles or exhibition spaces at a minimum of three key industry conferences that are relevant to cybersecurity, ITAI, or financial technology.

Operational Scalability: Formalize core commercial processes—including lead management, client onboarding, and support workflows—so that service quality can be maintained as the client base grows. The operational goal is to be able to efficiently support 50–60 active clients by the end of the one-year period without a decline in customer experience.

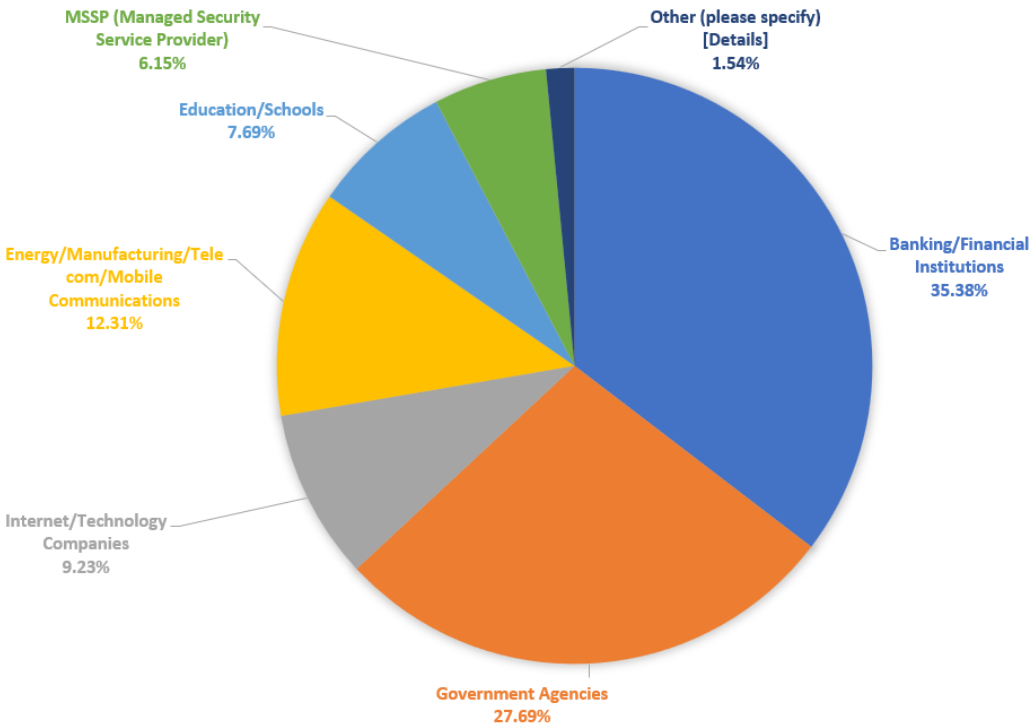
These six objectives provide an integrated one-year framework for Dataori's commercial development. They are measurable, aligned with the company's current resources, and directly support the strategic goal of building a sustainable and profitable business in the increasingly competitive ITAI-driven security market.

4.6. Commercial Strategy: Marketing, Sales and Business Development

4.6.1. Segmentation, Targeting, and Positioning

In the localization of the SIEM market, precise market segmentation is essential for developing effective marketing strategies. Based on the questionnaire results from 42 responses and In-depth interviews results, the market can be segmented by industry, company size, budget, and procurement decision factors to ensure the feasibility of market entry strategies. The survey data indicates that the primary demand for SIEM solutions is concentrated in the financial sector (45.2%), government agencies (35.7%), and energy/manufacturing/telecommunication (11.9%). Among these, the financial industry exhibits the highest demand, relying on MLPS 2.0 compliance, financial industry security standards, real-time risk control, and cross-system log correlation analysis. As financial IT innovation policies continue to advance, the demand for domestic SIEM solutions is growing, and Regulation No. 79 has further accelerated procurement processes for localized SIEM solutions. Government agencies, on the other hand, prioritize localization, security, and cross-departmental security management, with government procurement increasingly favoring domestic suppliers and requiring 100% compliance with IT Application Innovation (ITAI) standards. In the energy, manufacturing, and telecommunications industries, the focus is on Industrial Control System (ICS) security, low false positive rates, and long-term operational stability, with the energy sector placing a strong emphasis on customization needs as industrial data security has become a strategic priority.

Figure 4.1 Industry Distribution of SIEM Demand

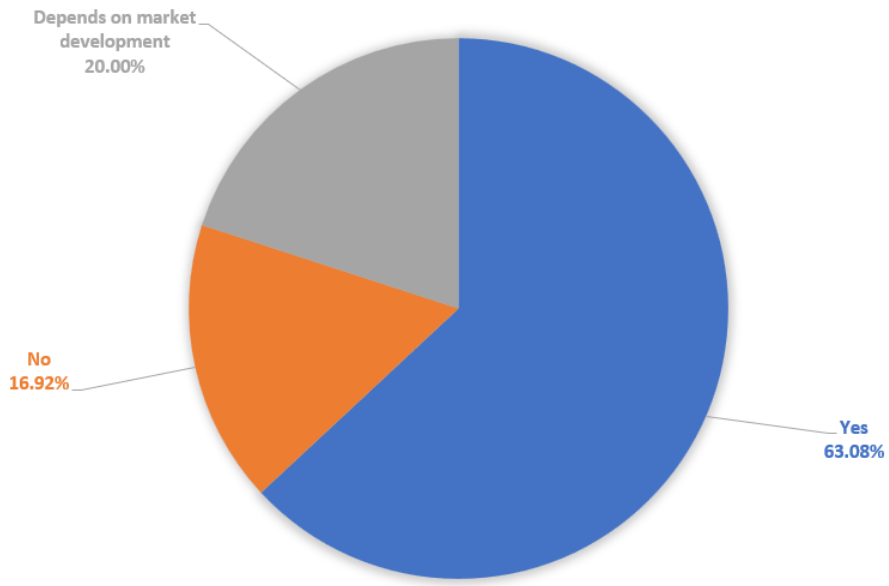


Source: Author (2025)

From the perspective of company size, large enterprises (>15% IT budget allocated to SIEM), including financial institutions and government entities, tend to prefer private deployments, emphasizing autonomy, security compliance, and deep customization with localized support. Medium-sized enterprises (5-15% IT budget, including certain government institutions and mid-sized banks) are more inclined toward a hybrid model (on-premises + SaaS), focusing on cost control, rapid deployment, and regulatory compliance. Small enterprises (<5% IT budget, including SMEs, regional banks, and some MSSPs), with limited resources, typically adopt a Managed Security Service Provider (MSSP) model or Security-as-a-Service (SaaS), preferring low-cost, easy-to-deploy solutions with outsourced security operations.

Regarding procurement decisions, Regulation No. 79 has reduced procurement cycles for government and financial institutions by 10-30%, which means that government entities and state-owned enterprises are more inclined toward long-term strategic partnerships, prioritizing trust and local adaptation during procurement. In contrast, financial institutions are compliance-driven, leading to a faster procurement process, necessitating stronger compliance certifications and a portfolio of successful case studies.

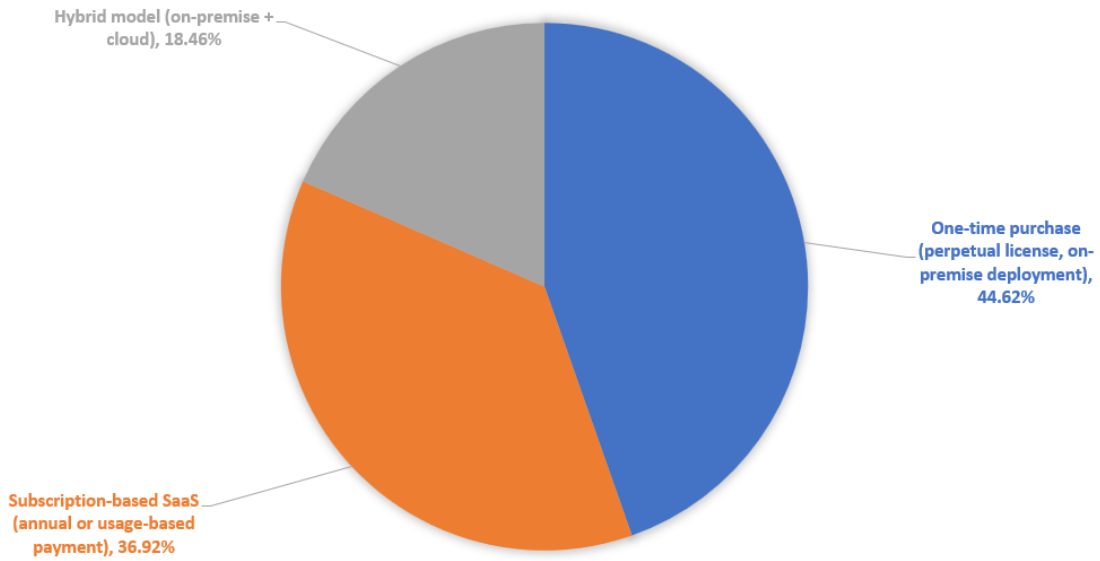
Figure 4.2 Plan to Switch to Domestic SIEM in the Next 3 Years



Source: Author (2025)

The government and financial enterprises tend to favor installment payment models such as 30/60/10 or 30/60/10, which help reduce initial investment costs while ensuring long-term operational support. Small and medium-sized enterprises (SMEs) are more inclined toward subscription-based models, opting for SaaS solutions that allow for on-demand usage and reduced capital expenditures. Additionally, some MSSP customers prefer a pay-as-you-go model, enabling SIEM costs to scale dynamically with business size. To meet the diverse needs of different customer segments, SIEM providers must offer flexible pricing models that accommodate various procurement preferences.

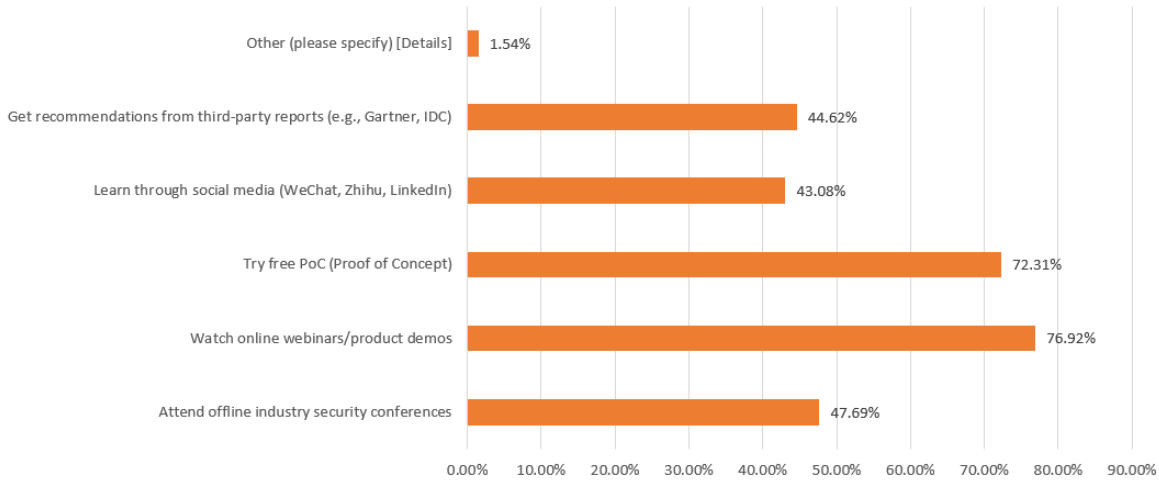
Figure 4.3 Preferred SIEM Procurement Method



Source: Author (2025)

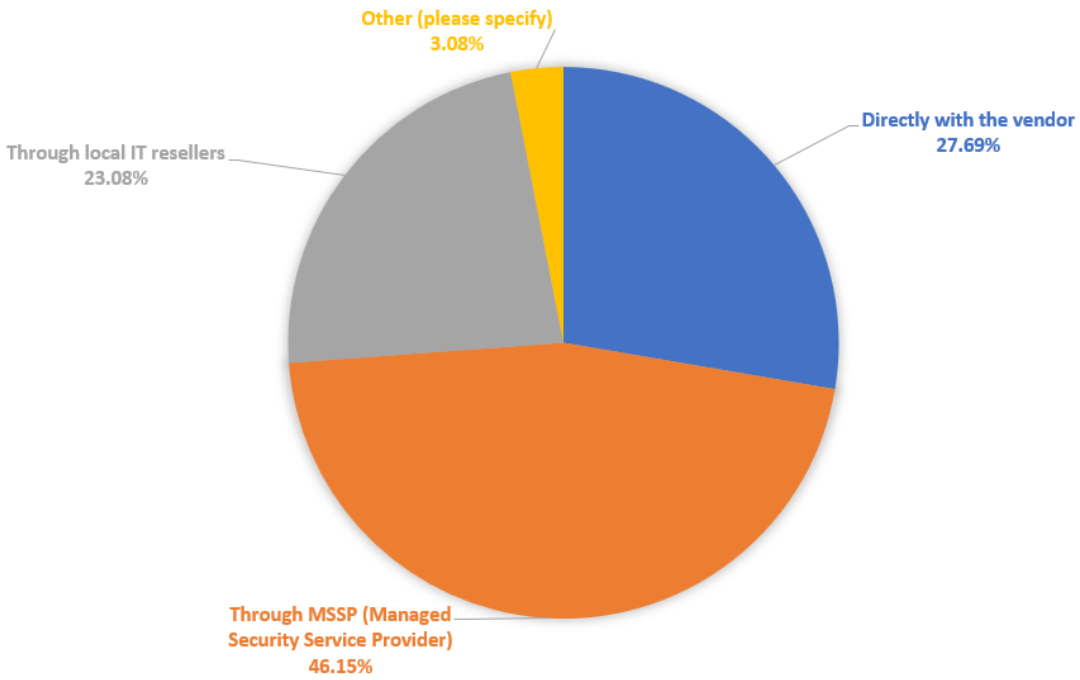
When acquiring information about SIEM solutions, enterprises primarily rely on industry summits & conferences, followed by technical white papers & industry reports, which remain key influencers in procurement decisions. Furthermore, free trials play a crucial role in product evaluation, particularly for mid-sized enterprises and MSSP customers, who prefer to test solutions before committing to a purchase. Therefore, in market promotion efforts, it is essential to increase participation in industry summits, provide comprehensive product reports, and incorporate trial programs to enhance market awareness and build customer trust.

Figure 4.4 Primary Sources for SIEM Information



Source: Author (2025)

Figure 4.5 Preferred SIEM Procurement Channel



Source: Author (2025)

Brand trust is another critical factor influencing SIEM market competitiveness, with the survey results highlighting three key factors that determine a vendor's credibility. First, compliance with domestic security certifications (such as MLPS certification, state-owned cloud compatibility, and financial ITAI certification) has become a fundamental requirement for procurement. Second, the false positive rate and detection accuracy of SIEM products are crucial, as enterprises prefer highly efficient and stable detection capabilities to reduce unnecessary security alerts. Lastly, availability of 24/7 localized technical support is vital, particularly for financial institutions, government agencies, and critical infrastructure sectors, where immediate support ensures the reliability of security operations. Therefore, SIEM vendors must enhance brand credibility, ensure compliance with regulatory standards, and provide high-quality technical support to strengthen their market position.

The financial industry, including banks, securities firms, insurance companies, and payment institutions, prioritizes transaction security, financial risk prevention, and regulatory compliance. Engagement in the Financial Security Technology Forum, the publication of a white paper on compliant SIEM solutions, and the provision of product demonstrations and free pilot services contribute to increasing industry recognition and adoption. The government sector focuses on data security, network attack protection, and adaptation to information innovation. Entry into the government procurement system can be facilitated through policy interpretation and case-sharing, while partnerships with local IT ecosystem enterprises enhance participation in government procurement expos. Energy companies and telecommunications operators typically operate under group management, where each

subsidiary reports data centrally. These organizations require large-scale log management and cross-site security data analysis capabilities. Hosting industry salons to introduce AI-enabled security monitoring capabilities to Chief Information Security Officers (CISOs) and offering customized industry solutions strengthen market positioning. The enterprise market, encompassing manufacturing, retail, healthcare, and internet sectors, emphasizes cost control and intelligent security management. A SaaS subscription model combined with a hardware appliance solution, in collaboration with MSSPs to provide managed security services, aligns well with market expectations. Additionally, the implementation of a free trial plan fosters wider adoption and lowers entry barriers for prospective customers.

According to the size of the enterprise, it can be divided into three customer groups: large, medium and small. The SIEM investment price range for large enterprises (mature SOC operations) is about RMB 1 million to 10 million per year, and usually requires private deployment to support large-scale data processing and complex custom analysis rules to improve security operation efficiency. Such enterprises have strict security compliance requirements, usually have dedicated security teams, and require deeply customized security analysis capabilities.

The SIEM investment price range for medium-sized enterprises (limited SOC operations) is about RMB 300,000 to 1 million per year, which is suitable for adopting a hybrid model (privatization + cloud AI analysis) to enhance security monitoring capabilities through AI under limited security operation capabilities. Such enterprises pay more attention to cost control and hope to improve security automation capabilities. They usually rely on social marketing and case sharing for product selection.

The SIEM investment price range for small enterprises and start-ups (no SOC team) is about RMB 50,000 to 300,000 per year, and they prefer the economical SaaS subscription model to obtain efficient security management capabilities at a low cost. Such enterprises usually do not have dedicated security operations teams and require low-threshold, easy-to-use solutions. Therefore, digital marketing promotions and trial versions are used to reduce the difficulty of technology adoption, helping customers get started quickly and implement the basic security protection infrastructure.

Dataori's core target markets include the financial industry and government sectors as the highest priority, followed by state-owned enterprises and MSSP channels. The financial industry (banking, securities, payment) has the highest SIEM procurement urgency, driven by compliance regulations such as the Multi-Level Protection Scheme (MLPS 2.0). With the implementation of SASAC Document No. 79, government and state-owned enterprises have accelerated their transition to domestic SIEM solutions, making them another key market for Dataori. The MSSP channel remains important for covering small and medium-sized enterprises, particularly those with limited IT security budgets. Based on the survey,

government and finance sectors exhibit the shortest procurement cycles, making them the most viable entry points for early market penetration.

Secondary target markets include emerging industries such as energy, manufacturing, retail, Internet and medical care. Energy and operators need large-scale log management and cross-site security data analysis, which are suitable for private cloud SIEM and provide industry customized solutions. Manufacturing, retail, and Internet companies prefer hybrid cloud SIEM models, focusing on cost control and security intelligent management. As data security requirements increase, emerging industries such as medical care and the Internet are growing in demand for compliance and intelligent security management, and the market potential is huge. Dataori will gradually expand the secondary market on the basis of deepening its core market to achieve steady growth in business.

Dataori reconstructs the SIEM value chain with AI Copilot as the core to create a "security productivity tool". AI empowers different roles. CISO reduces security operation costs and improves compliance audit efficiency. SOC analysts reduce SQL writing through natural language interaction. IT managers improve log storage and operation and maintenance automation. Compared with international products, Dataori not only has data visualization capabilities, but also strengthens "active threat hunting + AI-assisted decision-making". The accuracy of AI alarms far exceeds that of traditional SIEM. In terms of pricing strategy, a tiered subscription system is adopted. The basic version of SaaS is paid on demand, and private deployment combines the ITAI adaptation fee with AI module authorization. At the same time, SIEM and EDR are integrated through security operation packages to improve overall security capabilities.

Dataori builds a closed loop of the ITAI ecosystem, strengthens government procurement advantages, and jointly launches solutions with domestic operating system, database and other manufacturers, and obtains compatibility certification to ensure entry into the central procurement catalog. At the same time, a localization replacement subsidy plan is launched to reduce procurement and migration costs. In terms of channel expansion, it cooperates with domestic server manufacturers to achieve bundled sales of government and financial industry bids, and establishes "ITAI SIEM certified agents" to provide localized support. In addition, Dataori cooperates with security service providers to launch "security hosting services", which are divided according to the amount of security incidents handled to increase market coverage.

Dataori focuses on high-value scenarios and creates benchmark cases for finance, government and small and medium-sized enterprises. In the financial industry, it launches a compliance preset rule library and transaction anti-fraud AI model, and verifies compliance capabilities through pilots. In the government and central enterprise market, it emphasizes autonomous control and attack and defense drills, provides security services for major events, and launches historical data migration tools to ensure compatibility with customers' existing

platforms. In the small and medium-sized enterprise market, it adopts the SaaS model to reduce the cost of reaching, deploys the "SIEM health detection" applet through the enterprise social platform, attracts enterprises to self-diagnose, and provides an industry template store that users can enable on demand.

Dataori improves market barriers and locks in customer migration costs through technological innovation. The AI model is continuously iterated, and the threat intelligence library is updated monthly to ensure the stability of customer subscriptions. It adopts private data encryption storage. If customers need to migrate data, they need to decrypt it additionally, which increases the replacement cost. In addition, the AI Copilot API interface is open to attract ISVs to develop industry plug-ins, enhance ecological stickiness, and ensure long-term market competitiveness.

4.6.2. Customer Retention Strategies

Customer retention is a central element of this plan, because the revenue target of RMB 4 million and the goal of supporting 50–60 active clients both depend on improving the current renewal rate of about 60%. The objective, as defined in section 4.5, is to reach at least 70% within the next twelve months. This subsection therefore outlines a small set of focused retention measures that are consistent with the company’s limited resources and address the main pain points identified in the questionnaire and interview findings.

The first measure is a simple key account management approach for the most important customers. The top 20% of clients in terms of contract value represent a large share of current revenue, so losing even one of them would have a visible impact on annual results. For these customers, Dataori will assign a clear main contact and schedule regular contacts, including at least one structured review meeting per quarter. In these meetings, both sides will review current usage of the platform, open technical or operational issues, and possible new requirements. This measure is expected to support the renewal objective because it focuses time and attention on the clients that matter most for reaching the 70% target.

The second measure concerns onboarding and training, which was identified as a weakness in the consumer analysis and in some of the survey responses. Several respondents mentioned that internal security teams are small and cannot invest much time in configuring and tuning SIEM systems. To address this, Dataori will prepare clearer step by step configuration guides and offer short online training sessions for new and existing users. The aim is to help customers reach a basic level of “stable and useful” operation within the first weeks of deployment, which should reduce frustration and increase the probability of renewal at the end of the contract period.

A third measure focuses on service quality and response times, which also appeared as a concern in the questionnaire results. The company will define a small number of service targets, such as acknowledging urgent incidents within one hour and providing an initial technical response within the same business day. These targets will be monitored using simple tools, for example shared ticket lists or spreadsheets, so that management can see whether the team is meeting its own promises. By making service performance more visible and predictable, the company expects to build more trust with existing customers and to support the improvement of the renewal rate.

The fourth measure is to formalize a basic feedback loop between customers and the product roadmap. Once or twice per year, key users from different sectors (for example banking, telecommunications, and government) will be asked about detection performance, false positive levels, reporting needs, and integration problems. Where suggestions are feasible and consistent with the overall product strategy, they will be added to the development roadmap and, once delivered, explicitly communicated back to the customers who requested them. This approach links retention to the company's strong R&D orientation and shows customers that their input can influence future releases, which can strengthen long term relationships.

These retention strategies are modest in terms of required resources but directly support the objective of increasing the renewal rate from 60% to at least 70% within one year. They also build on insights from the external and internal analyses, namely limited customer resources, high expectations for support, and the importance of key accounts in a small revenue base.

4.6.3. Sales Strategies

The sales strategy for the next twelve months is designed to support three objectives defined in section 4.5: achieving RMB 4 million in annual revenue, acquiring 10–12 new enterprise clients, and expanding the number of active channel partners from 3–5 to 6–8. Given that the sales team consists of only three account executives, the strategy must concentrate on a limited number of segments and rely on a combination of direct and partner-led sales.

Direct sales will focus on a small group of priority prospects in banking, securities, and government, which were identified in the sector and consumer analyses as high-potential segments for localized SIEM solutions. In these sectors, Dataori already has reference projects and can demonstrate concrete results, such as successful ITAI adaptation and improved threat visibility. Each salesperson will work with a short list of around 10–15 target accounts and follow a simple sales process: prospecting and initial contact, needs assessment, product demonstration with support from technical staff, and preparation of a tailored proposal. If this

process results in three to four closed deals per salesperson over the year, the overall target of 10–12 new clients becomes realistic.

At the same time, the company will strengthen and expand its channel sales. The competitor analysis showed that leading vendors rely heavily on ecosystems of integrators and managed security service providers, which suggests that Dataori should also use partners to extend its reach. The goal is to increase the number of active, revenue-generating partners to 6–8 by the end of the year, focusing on regional IT service providers and vertical specialists in sectors such as energy, manufacturing, and regional government. For each partner, Dataori will provide basic product and sales training, Chinese-language sales materials, and joint visits for initial opportunities. Based on current experience, even one or two deals per active partner per year would make a meaningful contribution towards the revenue and new-client targets.

Marketing activities will support both direct and partner-driven sales but will remain simple due to resource constraints. As described in the objectives chapter, the company plans to participate in at least three relevant industry events in the fields of cybersecurity, ITAI, or financial technology. These events are expected to generate qualified leads for the sales pipeline and to increase awareness of Dataori among potential customers and partners. In parallel, a small number of concise case studies and articles will be prepared to show how the platform has helped existing clients improve security operations or comply with ITAI requirements. These materials will be used in meetings, shared by partners, and published on the company's channels to support trust-building and differentiation.

Finally, the sales team will adopt a basic pipeline management practice to improve forecasting and resource allocation. All opportunities, whether direct or partner-led, will be recorded in a simple system using a few stages such as "prospecting", "qualified", "proposal sent", and "negotiation". This will allow management to compare the current pipeline volume with the annual targets, to identify where deals are being lost, and to decide whether more effort should be placed on direct accounts or on supporting partners at different points in the year. The intention is not to introduce a complex CRM platform, but to create enough visibility to manage a realistic path towards 10–12 new clients and the targeted revenue level with a small team.

In summary, the sales strategies described in this subsection are closely aligned with the company's scale, its market positioning, and the numerical objectives for revenue and customer acquisition. They translate the broader commercial ambitions into concrete priorities for the three-person sales team and the growing partner network over the one-year planning horizon.

4.7. Marketing-Mix

Based on the previous analysis of the external environment, competitors, internal resources and customer insights (sections 4.2, 4.3 and 4.6), this section presents a marketing-mix strategy that has a clear theoretical basis, is informed by data, and is aligned with the company's strategic goals. The purpose is not only to state what actions will be taken, but also to explain why they are appropriate in Dataori's situation. The strategy is designed to address, in a structured way, the main challenges in customer acquisition and customer retention, and to support the revenue growth, new customer acquisition and renewal rate targets defined in section 4.5. The plan draws on standard concepts from segmentation and positioning, the marketing mix, customer relationship management and customer lifetime value, but applies them in a pragmatic way to Dataori's context.

4.7.1. Product

Dataori's product strategy is not simply a list of functions. It is based on the customer segments identified earlier (see section 4.6.1) and on the need to build a more durable competitive position. The products are organised as a clear and evolving portfolio that can be adjusted over time as the company and the market develop.

The first element is a layered product structure and a clear value proposition for each layer. The basic compliance version is aimed at small and medium-sized enterprises and local government entities. Its main promise is "compliance first, fast deployment". This version was designed in direct response to questionnaire findings that showed tight IT budgets for smaller organisations and strict domestic technology requirements for government customers. It focuses on core log management, a pre-configured rules library for local compliance standards, and basic threat detection. The goal is to help customers meet policy and regulatory requirements at a reasonable cost, to lower the entry barrier, and to open up parts of the market that were previously not well served because of technical and cost obstacles.

The AI-enhanced version is targeted at large financial institutions and central state-owned enterprises. Its promise is "intelligence-driven, higher efficiency". Questionnaire results showed that many respondents ranked AI-based detection and low false positive rates among the most important features. Building on the basic version, the AI-enhanced product adds a more advanced analytics engine, user behaviour analysis, light-weight automation workflows and industry-specific detection scenarios, such as models for financial fraud. The intention is to use a visible improvement in security operations efficiency, for example by reducing the workload of security operations centre teams, to differentiate Dataori from domestic competitors and to narrow the gap with international vendors on higher-end functions.

The second element is to treat services as part of the product, especially for retention. The aim is to increase customer stickiness and to improve the current renewal rate of about 60%. For online parsing and initial configuration, the company will provide support to new customers within a defined period to complete log parsing and basic setup. This responds directly to interview feedback that many internal security teams do not have enough capacity to configure SIEM systems in depth. By lowering the initial usage barrier and reducing ongoing maintenance effort, this service supports both first-time purchases and repeat contracts. In addition, Dataori will maintain a regularly updated rules and intelligence library and provide an online technical community where customers can share configurations and good practices. This continuous delivery of value and interaction increases switching costs over time and helps build preference for the brand, which is consistent with the idea that long-term relationships are built through ongoing communication and shared problem-solving.

The third element is a clear view of how the products will evolve over time. In the short term (1–2 years), the focus is on deeper penetration in the current growth phase, especially in the financial and government sectors identified as priorities. This includes improving detection scenarios for these sectors and working to reduce the average false positive rate of the AI models to a more acceptable level, using feedback from pilot projects to refine data parsing and model tuning. In the medium to long term (3–5 years), as the market becomes more mature and competition intensifies, the company plans to move gradually toward a more platform-like model. This may include opening selected interfaces so that third parties can build industry-specific extensions on top of the core platform, creating an ecosystem that makes substitution more difficult. At the same time, the company can explore offering the core AI engine as a standalone service, which would open up new revenue streams and is in line with the longer-term data monetisation ideas discussed in the conclusion.

4.7.2. Price

The pricing strategy takes into account the company's cost structure, competitors' price levels (section 4.2.3), perceived value, and the willingness and ability to pay of target customers (section 4.6.1). The objective is to strike a balance between market penetration, value capture and customer retention.

For the basic version, the price level of roughly RMB 40,000 to 60,000 per year is clearly below the prices of similar products from the main domestic vendors. This is intended to speed up adoption among price-sensitive small and medium-sized enterprises and local governments by using a cost advantage. For the AI-enhanced version, with a price around RMB 80,000 to 100,000 per year, and for on-premise deployments with a one-time licence fee of around RMB 600,000 to 1,000,000, the approach is more value-based. The higher price reflects the

additional AI capabilities, full domestic stack adaptation and deeper services, and is justified by the gains in security operations efficiency and compliance assurance that these customers expect.

The pricing models also reflect different purchasing preferences. Questionnaire results showed that smaller customers and service providers prefer predictable operating expenses, while larger government and financial clients are used to one-time capital expenditures followed by annual maintenance. For this reason, Dataori will mainly offer annual subscription pricing to smaller customers and managed security service providers, to reduce initial investment and match their budget cycles. For large banks and government agencies, the company will maintain a licence plus annual maintenance model, which fits their approval and payment processes better.

To support these prices, the communication with customers needs to make the value visible. On the technical side, the company should use concrete examples to show how the AI-enhanced version helps reduce false positives and shorten investigation time. On the service side, it should clarify the standalone cost of items like online parsing assistance and dedicated technical advice, so that customers can see what they are getting beyond the software itself. On the compliance side, it is important to explain how full domestic stack adaptation and built-in compliance support help reduce the risk of delays, rework or penalties due to non-compliance, turning compliance from a pure cost into a form of risk control.

The incentive design and the way prices change over the customer life cycle are also important. The pricing strategy follows the idea that acquisition cost and long-term value should both be considered. For new customers, time-limited discounts or more favourable terms can help lower the perceived risk of the initial decision and speed up long procurement processes. For existing customers, keeping prices stable at renewal, and offering modest discounts when they expand their usage or add modules, can encourage longer relationships and broader adoption, so that the relationship moves from a single transaction to ongoing cooperation. For a few customers with very high performance requirements, it may be useful to explore linking a small part of the fee to agreed performance indicators, but only where the metrics and measurement methods are clear and both sides accept the mechanism.

4.7.3. Place

The channel strategy must recognise that Dataori has a small direct sales team of three people and limited internal resources. The goal is to use external partners to extend reach, while keeping control over key accounts and managing the risk of channel conflict.

In terms of structure and resource allocation, the direct sales team should focus on a small number of high-value targets. With three people, it is more realistic to concentrate on about 15 to 20 strategic accounts, such as major state-owned banks and central government ministries, rather than trying to manage a much larger number of prospects. These customers have long purchasing cycles, large contract values and complex requirements, and they need sustained effort in early-stage communication, solution design and senior relationship management. Instead of spreading effort too thin, the company should set realistic goals, for example one or two large deals per salesperson per year, creating a pipeline that is limited in number but solid in value.

The partner network is responsible for scaling up coverage. To reach the target of 10 to 12 new customers per year, increasing the number of active partners to around 6 to 8 within a year is a practical path. The focus should be on regional system integrators and security service providers with experience in financial, energy or government projects. With training, sales materials and joint visits at the beginning, these partners can gradually become able to sell and deliver Dataori solutions independently. If each active partner brings even one or two new deals per year, the combined contribution will be a meaningful part of the annual revenue target. At the same time, cooperation with domestic hardware, operating system, database and cloud vendors can also be seen as part of the broader channel: being listed in their joint solution catalogues can help Dataori benefit from their brand recognition and existing customer base.

To avoid conflicts between direct sales and partners, the boundaries should be defined in advance. This can be done by assigning certain customer groups to direct sales (for example by size, sector or location) and other groups to partners, and by using simple opportunity registration and CRM records to show who is leading which deal. For partners, the company should keep commission rates and quarterly bonuses attractive, and support them with ongoing training, roadmap briefings and marketing resources, so the relationship can develop into a long-term partnership rather than a one-off transaction.

4.7.4. Promotion

The promotion strategy does not aim at very broad visibility. It focuses on influencing the specific groups of customers that Dataori wants to reach, and on guiding them step by step from awareness and interest to trial, purchase and renewal, with attention to both acquisition and retention.

For market education and basic brand building, survey results showed that industry conferences and technical papers are important information sources for customers. In the coming year, the company will therefore select a small number of relevant events in the fields

of financial technology, domestic IT infrastructure and cybersecurity to attend. The aim is not only to have a booth, but also to secure speaking or panel opportunities where Dataori can present findings from its research on SIEM use in Chinese financial institutions and government agencies. This helps show that the company understands local regulatory and operational issues. At the same time, the company will invest in developing a few deep case studies based on existing flagship projects, with a clear focus on measured outcomes in major banks and government organizations, such as reductions in false positive rates or shorter preparation time for audits. These cases are both sales tools and proof points that reduce the perceived risk of choosing a smaller vendor. For technical staff, Dataori will hold regular online sessions on practical topics, such as how to use AI in threat hunting or how to handle log collection and analysis in domestic IT environments. By sharing useful content that addresses day-to-day problems, the company can gradually build a following among practitioners.

For experience and conversion, free trials and proof-of-concept projects are effective ways to reduce buying risk, but need to be designed and controlled carefully. Dataori can offer a limited SaaS trial, with clear bounds on duration and data volume, together with simple guidance for initial setup. For customers with clear project intentions, the company can agree on a small set of success criteria and run a short proof-of-concept to show real detection results in the customer's environment. In online channels, Dataori can run modest targeted campaigns on search engines and technical communities around keywords such as "domestic SIEM" and "security operations efficiency", and direct the resulting traffic to trial or consultation pages.

For deepening relationships and supporting success with existing customers, promotion activities shift from public messages to more focused communication. For key accounts that contribute a large share of revenue, the company can schedule regular review meetings to discuss product usage, issues resolved and potential new requirements, and move the relationship from reactive problem solving to joint planning. A simple feedback loop should also be in place: suggestions that arise in support tickets or interviews are collected into the product planning process, and when a relevant feature is delivered, the responsible customers are informed proactively. This shows that their input has been taken seriously. By building an online space where customers can share their own experiences and best practices, Dataori can reduce repeated support work, and at the same time strengthen the sense of community and attachment to the brand.

Taken together, these marketing-mix decisions on product, price, place and promotion are intended to help Dataori move from being seen as just another SIEM supplier to being viewed as a trusted local security partner. The plan aims to achieve the one-year commercial targets on revenue, new customers and renewal, while also preparing a more solid base for continued growth in the following years.

4.8. Implementation

4.8.1. Schedule

The following one-year implementation plan outlines the key activities and milestones necessary to achieve the commercial objectives defined in Section 4.5, with a specific focus on customer acquisition and retention. The schedule is structured quarterly to ensure timely execution and regular review of progress:

Table 4.6 - One years implementation plan task list

Quarter	Key Tasks	Main Activities	Deliverables
Q1	Market Activation & Initial Outreach	Finalize targeted lead list for priority segments (Finance, Government, SOEs).	150+ qualified leads.
		Launch direct email & social media campaign (WeChat, Zhihu) focusing on AI SIEM differentiation.	2 new MSSP partnership agreements in principle.
		Initiate contact with 3-5 potential new MSSP channel partners.	Published case study.
		Develop and publish first industry-specific case study (Banking sector).	
Q2	Sales Drive & Channel Enablement	Conduct 10+ product demos for high-potential leads from Q1.	3-4 new customer contracts signed.
		Formalize training and sales materials for new channel partners.	2 enabled and active channel partners.
		Participate in 1-2 key industry cybersecurity/ITAI conferences.	50+ new leads from events.
		Launch the structured key account management program for top 20% of existing clients.	

Q3	Scaling & Retention Focus	Execute joint marketing campaigns with key channel partners.	3-4 new customer contracts via partners.
		Conduct quarterly business reviews with all key accounts.	Customer renewal rate tracking shows positive trend.
		Roll out enhanced onboarding guides and initiate first online training sessions for new customers.	>50% of new clients complete onboarding training.
		Begin gathering structured customer feedback for product roadmap.	
Q4	Consolidation & Planning	Final push to meet annual new customer target (10-12).	Annual revenue target of RMB 4 million achieved.
		Conduct annual Customer Satisfaction (NPS) survey.	Final list of 6-8 active channel partners.
		Analyze yearly performance against all KPIs.	Performance review report and next year's strategy draft.
		Develop the commercial plan and budget for the next year based on lessons learned.	

Source: Author (2025)

4.8.2. Budget

Dataori's f The one-year budget allocates financial resources to directly support the customer acquisition and retention activities outlined in the marketing mix (Section 4.7) and the implementation schedule. The budget is designed to be efficient and focused, ensuring a strong return on investment while working within the company's current scale. All figures are presented in both Chinese Yuan (RMB) and Euros (EUR) for clarity, using an exchange rate of 1 EUR = 7.8 RMB.

Table 4.7 - One years budget plan

Budget Category	**Details & Justification**	**Amount (RMB)**	**Amount (EUR)**	**Percentage**

Market Promotion & Lead Generation	Online advertising (targeted SEO/SEM, social media).	720,000	92,308	30%
	Content creation (2 industry white papers, case studies).			
	Participation in 3 industry events (booth, sponsorship).			
	Costs for free trial/PoC infrastructure and support.			
Sales Force & Channel Management	Commissions and bonuses for 3 salespeople (aligned with new customer and revenue targets).	480,000	61,538	20%
	Partner incentives and co-marketing funds.			
	Travel and entertainment for client and partner meetings.			
Customer Retention & Success	Tools and resources for key account management program.	360,000	46,154	15%
	Development and delivery of online training modules.			
	Dedicated support resources for improved response times.			
Product Development (Retention-linked)	Development of features specifically requested by key accounts (e.g., specific	600,000	76,923	25%

	compliance reports, integration adapters).			
	Enhancements to AI Copilot based on user feedback to reduce false positives and improve usability.			
Brand Building & Awareness	Public relations and article placements in industry media.	240,000	30,769	10%
	Development and maintenance of online community platform.			
Total		**2,400,000**	**307,692**	**100%**

Source: Author (2025)

This budget of RMB 2.4 million represents around 60% of the annual revenue target of RMB 4 million. It is an aggressive but realistic investment level for a growth-phase SIEM vendor, signalling that the primary objective of this one-year plan is to build a repeatable acquisition–retention model rather than to maximise short-term profit.

4.8.3. Control and assessment

4.8.3.1. Monitoring Framework

Dataori employs a structured KPI-driven monitoring system to track key performance indicators across multiple dimensions.

Table 4.8 - KPI-driven monitoring (One-Year Plan)

Monitoring Dimension	Key Performance Indicators (KPI)	Measurement Method	Evaluation Frequency
Customer Acquisition	Number of new qualified leads.	CRM system pipeline analysis.	Monthly
	Number of new paying enterprise clients.	Sales reports.	Monthly
	Customer Acquisition Cost (CAC).	Finance & marketing spend analysis.	Quarterly
Revenue Performance	Total SIEM-related revenue.	Financial reporting.	Monthly
	Revenue from new vs. existing clients.		
Customer Retention & Health	Customer contract renewal rate.	CRM renewal tracking.	Quarterly

	Net Promoter Score (NPS) / Customer Satisfaction.	Biannual survey.	Biannually
	Number of key accounts receiving quarterly business reviews.	Account management logs.	Quarterly
Channel Effectiveness	Number of active, revenue-generating channel partners.	Partner management records.	Quarterly
	Sales volume generated through partners.	Sales reports with partner attribution.	
Market Positioning	Number of competitive tenders (RFPs) shortlisted.	Sales pipeline review.	Quarterly

Source: Author (2025)

Dataori aims to enhance advertising effectiveness and improve marketing budget allocation through data-driven strategy adjustments, while aligning product development with market demand via continuous feature improvement. Strengthening channel partnerships will drive sales performance and partner engagement, while increasing brand recognition will solidify Dataori's position as a leader in the domestic SIEM sector.

4.8.3.2. Assessment Mechanism

To ensure the effectiveness of marketing and product promotion efforts, Dataori adopts a data-driven, periodic assessment model.

Table 4.9 - Assessment Mechanism list (One-Year Plan)

Assessment Method	**Evaluation Criteria**	**Evaluation Frequency**	**Responsible Team**
Monthly Performance Review	Progress against monthly lead and new customer targets.	Monthly	Sales & Marketing Teams
	Review of sales pipeline health.		
Quarterly Business Review (QBR)	Comprehensive review of all KPIs from Table 4.9. Assessment of channel partner performance. Analysis of CAC and ROI on marketing spend.	Quarterly	Senior Management
Biannual Customer Feedback Review	Analysis of NPS results and customer feedback.	Biannually	Product & Customer Success Teams

	Review of product enhancement requests from customers.		
Annual Performance Audit	Final assessment of annual objectives (revenue, new clients, retention rate).	Annually	Finance & Senior Management
	Financial performance review (budget vs. actual).		

Source: Author (2025)

This disciplined approach to control and assessment, with its frequent monitoring cycles, ensures that Dataori can quickly identify successes and challenges in its customer acquisition and retention efforts, making the one-year commercial plan a dynamic and actionable roadmap for growth.

4.8.3.3. Data-Driven Improvement

Dataori improves its marketing strategy through data-driven marketing, focusing on three core areas: marketing, product improvement, and channel expansion. Through A/B testing, we accurately improve advertising, improve customer conversion efficiency, and use social media analysis to enhance brand interaction. In terms of products, we continuously monitor the adoption rate of AI Copilot, improve functions based on user feedback, and improve SaaS SIEM performance through real-time log analysis. Channel expansion promotes the growth of MSSP agents through KPI performance assessment and dynamically adjusts the SIEM pricing model to adapt to market demand. The ultimate goal is to increase market return on investment (ROI), enhance the market application of AI Copilot, and improve channel cooperation strategies to promote Dataori's continued growth in the SIEM field.

5. Conclusions

This thesis initially set out to develop a business plan for Dataori, but the research process quickly showed that the problem goes beyond a single company. The Dataori case in fact reflects a broader question: in a cybersecurity market that is strongly driven by policy and highly competitive, how can a local small or mid-sized B2B technology firm pursue growth, and what does that mean in concrete terms for customer acquisition and customer retention? Based on a systematic analysis of the external environment, an assessment of the firm's internal constraints, and empirical evidence from 65 questionnaires and 3 in-depth expert interviews, this study puts forward several conclusions that both echo and partly revise existing research and practical experience.

First, this study uses specific data to confirm that in China's ITAI-oriented SIEM market, "compliance and localization" are more of an entry threshold than a moat that can sustain the long-term growth of small and mid-sized vendors. The survey results show that among 65 valid responses, 55.38% of respondents listed "false positive control" as one of the most important product attributes, 53.85% chose "compatibility with the ITAI ecosystem", and 41.54% focused on "AI-driven threat detection", which indicates that once localization and compliance are met, customers further screen suppliers based on whether the product is easy to use and can reduce workload. In the interviews, several respondents from the banking and energy sectors also pointed out that "too many false positives overwhelming the SOC team" and "whether the vendor can quickly respond to production issues" are key factors for renewal decisions, which supports the view that "being domestic and compliant decides whether you can get in, being easy to use and low-friction decides whether you can stay". For small vendors like Dataori, simply copying the compliance posture or ITAI certificate portfolio of large players cannot create a lasting advantage; the real room for differentiation lies in whether the product keeps improving the daily work experience of frontline security teams, for example by reducing false positives, simplifying tuning efforts, and providing clearer local configuration support.

Second, the thesis proposes and tests a "lean acquisition–retention" combined model under Dataori's resource constraints, treating acquisition and retention as two outcomes of one integrated design, rather than two separate tasks. On the acquisition side, Dataori currently has only 3 salespeople and 3–5 active channel partners, while the annual goals are 4 million RMB in SIEM revenue, 10–12 new enterprise customers, and expanding channels to 6–8 partners, which means that if the company continues to "cast a wide net", both customer acquisition cost per account and sales cycle will be hard to control. Therefore, this plan concentrates sales efforts on about 30–45 top-priority target accounts (10–15 per salesperson), and limits the channel strategy to a small set of capable MSSPs and vertical partners, using a combination of "deep direct sales + a few high-quality partners" to reach a reasonable balance

between coverage and conversion under the current manpower and budget. On the retention side, retention is explicitly written into the product and plan objectives: raising the renewal rate from around 60% to 70% and maintaining 50–60 active customers, so onboarding configuration support, regular follow-ups and key-account reviews are treated as part of the product, rather than “nice-to-have” value-added services, allowing a repeatable relationship management structure even without a large customer success team. This model rests on the judgement that for a resource-constrained small firm, economic optimization does not lie in signing as many new customers as possible within one year, but in increasing renewals and expansion revenue on a manageable customer base, so that cumulative LTV over a three-year period is higher than under a “low-price land grab but weak retention” expansion model.A2-Thesis-Study-on-the-Marketing-Plan-of-Dataori-s-SIEM-platform-v2.0-new3.docx

Third, regarding how “trust” is built in a policy-driven B2B technology market, this study finds that formal signals and real experience play a quantifiable and complementary role in the decision process. The survey shows that 56.92% of respondents regard “industry conferences and security summits” as key channels for learning about SIEM, 70.77% pay attention to online channels and official websites, and 58.46% value “third-party cases and word-of-mouth”, while in “preferred ways to learn about new products in the future”, 72.31% chose “free PoC trials” and 76.92% chose “online demos or webinars”, suggesting that decision-makers first use conference talks, technical white papers, and reference cases from major banks to make an initial shortlist, then rely on pilots and PoC to verify real experience. The interviews complete this picture: respondents from banks and central SOEs generally stressed that “without running in a production or near-production environment for a period of time, it is hard to award a big contract to a small vendor”, and noted that “response speed” and “whether the solution can smoothly integrate into the existing IT and ITAI stack” often determine the final decision. Therefore, Dataori cannot grow by relying only on marketing narratives to amplify its brand; it must strike a careful balance between “being seen” and “being used”: on the one hand, using a limited budget to gain visibility in the most critical scenes (such as finance- and government-related conferences and technical talks), and on the other hand, deliberately securing a small number of high-quality pilots and small-scale rollouts to build trust through verifiable performance and service experience.

Fourth, in practical terms, the recommendations for Dataori are not mild “sensible middle-of-the-road” suggestions, but a set of choices that involve clear trade-offs under given numerical targets. The plan aligns annual targets of 4 million RMB in revenue, 10–12 new customers, a renewal rate raised to 70%, and 6–8 active channel partners with specific actions on product, pricing, channels and promotion, and uses the budget to concentrate roughly 4 million RMB of commercial spending on activities directly related to acquisition and retention, avoiding excessive allocation to visibility-building projects with unclear outcomes. Under this

setup, the plan explicitly states that if Dataori continues to “spread thin” across too many industries and regions, asking 3 salespeople to cover far more prospects than they can meaningfully handle, it is highly likely that the company will neither reach 10–12 new customers within 12 months, nor free up enough capacity to lift the renewal rate of existing customers from about 60% to 70%. In contrast, a combination of “narrowing the front, going deep with 15–20 priority customers, supporting a few capable channel partners, and doing onboarding and key-account reviews properly”, even if it reduces the short-term number of new customers, has a better chance of delivering higher and more controllable cumulative revenue over three years through higher renewals and expansion sales, which is consistent with the CLV and retention-priority conclusions in the literature.

Fifth, for other local B2B technology firms at a similar stage, this case offers more targeted insights than generic experience summaries. First, ITAI policy dividends and the macro narrative of “domestic substitution” can easily create a sense of safety, but this study’s survey and interviews show that more than half of customers still judge suppliers by reliability, false-positive control, ease of use and service continuity, which means that “policy tailwinds” cannot substitute for the competitiveness of the product and service themselves. Second, as long as a firm is willing to accept focus and trade-offs, it is possible to design a workable sales–retention model under “small team and limited budget” constraints, instead of swinging between “inefficient expansion” (planting seeds everywhere but failing to land projects) and “passive defence” (only maintaining existing customers and avoiding experimentation); Dataori’s one-year plan is one example of explicitly setting upper bounds for target customers, channel partners and workload per head. Third, taking customer retention seriously does not necessarily mean building an expensive customer success department; in this case, clearer onboarding guidelines, quarterly key-account reviews, and directly mapping customer feedback into the product roadmap already provide a replicable starting point for significantly improving renewals with limited resources.

Sixth, this study has several limitations that need to be acknowledged, and these limitations define the boundaries of the current conclusions as well as natural entry points for future research. In terms of samples, the survey and interviews mainly cover financial, government and energy institutions that already have some contact with Dataori, and are not fully representative of regional SMEs, education, and some manufacturing customers, so the results should not be simply generalized to the entire Chinese SIEM market. In terms of behaviour, the analysis of customer needs and purchasing criteria largely relies on respondents’ self-reported intentions rather than actual purchasing and renewal behaviour; prior research suggests that in B2B settings with complex internal politics and budget constraints, there is often a significant gap between stated preferences and final decisions, and this study is no exception. In addition, to keep the business plan actionable, the thesis

simplifies assumptions about average deal size, customer acquisition cost (CAC) and renewal patterns, and takes a relatively optimistic view of channel partner engagement and the risk of prolonged sales cycles with key accounts, which may later reveal that the model underestimates execution difficulty and uncertainty.

These limitations naturally point to several directions for further research. First, about one year after this plan is implemented, the same group of customers and prospects can be revisited, comparing the initial “stated purchase intent” in the survey with real contracts, renewals and churn, so as to ex-post calibrate the “lean acquisition–retention” model and more clearly distinguish between “what respondents say they value” and “what they actually spend money on in the budget”. Second, the internal multi-role decision process on the customer side can be analysed in more detail, for example how security teams, IT operations, compliance and procurement weigh AI capabilities, local adaptation, vendor size and price, and how these factors influence each other, so that vendors like Dataori can align value propositions and messages more precisely to different roles instead of staying at generic technical selling points. Third, once Dataori has accumulated the initially planned 10–12 new customers and built a base of 50–60 active customers, it can use real renewal and expansion data to train a more granular customer lifetime value (CLV) model, replacing the current static assumptions, and, in parallel with the normalization of ITAI policies, explore how local vendors can shift from “policy-driven substitutes” to “technology-driven innovators” and build a second growth curve in this process.

Bibliographical References

Aka, D., Kehinde, O., & Ogunnaike, O. (2016). Relationship marketing and customer satisfaction: A conceptual perspective. Binus Business Review, 7(2), 185-190.http://dx.doi.org/10.21512/bbr.v7i2.1502

Anagnostakis, D. 2021. "The European Union-United States Cybersecurity Relationship: A Transatlantic Functional Cooperation." Journal of Cyber Policy 6 (2): 243–261. https://doi.org/10.1080/23738871.2021.1916975

Broeders, D., F. Cristiano, and M. Kaminska. 2023. "In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions." JCMS: Journal of Common Market Studies 61 (5): 1261–1280. https://doi.org/10.1111/jcms.13462

Chen, S. (2024). *Research on DX Company's information and innovation business strateg y* [Master's thesis, Guangxi University]. CNKI. https://doi.org/10.27034/d.cnki.ggxiu.2024.001212

Doh J. P., Lawton T. C., Rajwani T., (2012). Advancing nonmarket strategy research: Institutional perspectives in a changing world. Academy of Management Perspectives, 26(3), 22-39. https://doi.org/10.5465/amp.2012.0041

Fahey, E. (2024). The evolution of EU–US cybersecurity law and policy: on drivers of convergence. Journal of European Integration, 46(7), 1073–1088. https://doi.org/10.1080/07036337.2024.2411240

Farrand, B. 2023. "The Ordoliberal Internet? Continuity and Change in the EU's Approach to the Governance of Cyberspace." European Law Open 2 (1): 106. https://doi.org/10.1017/elo.2023.14

Ge J., Stanley L. J., Eddleston K., Kellermanns F. W., (2017). Institutional deterioration and entrepreneurial investment: The role of political connections. Journal of Business Venturing, 32(4), 405-419. https://doi.org/10.1016/j.jbusvent.2017.04.002.

iResearch, (2023). 2023 China Information Technology Application Innovation (ITAI) Industry Research Report. In 2023 iResearch July Research Report Conference Proceedings (pp. 103–157). https://mp.weixin.qq.com/s/kyFwiCN2h7Kahd0kQTQAWA

Ji, M. (2022). *Research on the development strategy of Company A's information technology application innovation business* [Master's thesis, Yanshan University]. CNKI. https://doi.org/10.27440/d.cnki.gysdu.2022.002279

Lei, D. (2016). *Influence and countermeasure research of autonomous and controllable information technology regulations on A Bank* [Master's thesis, Beijing Jiaotong University].

CNKI. https://kns.cnki.net/KCMS/detail/detail.aspx?dbname=CMFD201701&filename=1016115848.nh

Li, H., & Zhang, Y. (2007). The role of managers' political networking and functional experience in new venture performance: Evidence from China's transition economy. *Strategic Management Journal, 28*(8), 791–804. https://doi.org/10.1002/smj.605

Jabado, R., & Jallouli, R. (2024). Enhancing customer relationship management with data analytics: Insights from retail survey. Journal of Telecommunications and the Digital Economy, 12(2), 76–96. https://doi.org/10.18080/jtde.v12n2.987

Jain, D., & Singh, S. S. (2002). Customer lifetime value research in marketing: A review and future directions. Journal of interactive marketing, 16(2), 34-46.https://doi.org/10.1002/dir.10032

Johns, F., and A. Riles. 2016. "Introduction to Symposium on Cybersecurity and the Changing International Law of Data." The American Journal of International Law 110:335. https://doi.org/10.1017/aju.2017.2

Madzík, P., & Shahin, A. (2021). Customer categorization using a three-dimensional loyalty matrix analogous to FMEA. International Journal of Quality & Reliability Management, 38(8), 1833-1857.https://doi.org/10.1108/IJQRM-05-2020-0179

Manzoor, J., Waleed, A., Jamali, A. F., & Masood, A. (2024). Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs. *PLoS ONE, 19*(3), e0301183. https://doi.org/10.1371/journal.pone.0301183

Mascarenhas, O. A., Kesavan, R., & Bernacchi, M. (2006). Lasting customer loyalty: a total customer experience approach. Journal of consumer marketing, 23(7), 397-405.https://doi.org/10.1108/07363760610712939

Naseer, A., Naseer, H., Ahmad, A., Maynard, S. B., & Siddiqui, A. M. (2021a). Real-time analytics, incident response process agility and enterprise cybersecurity performance: A contingent resource-based analysis. *International Journal of Information Management, 59*, 1–10. https://doi.org/10.1016/j.ijinfomgt.2021.102352

Naseer, H., Desouza, K., Maynard, S. B., & Ahmad, A. (2023). Enabling cybersecurity incident response agility through dynamic capabilities: The role of real-time analytics. *European Journal of Information Systems*, 1–21. https://doi.org/10.1080/0960085X.2023.2257168

Rawindaran, N., Jayal, A., Prakash, E., & Hewage, C. (2023). Perspective of Small and Medium Enterprise (SME's) and Their Relationship with Government in Overcoming Cybersecurity Challenges and Barriers in Wales. International Journal of Information Management Data Insights. DOI: 10.1016/j.jjimei.2023.100191

Roch, J., and A. Oleart. 2024. "How 'European sovereignty' Became Mainstream: The Geopoliticisation of the EU's 'sovereign turn' by Pro-EU Executive Actors." Journal of European Integration 1 (4): 545–565. https://doi.org/10.1080/07036337.2024.2326831.

Rosário, Albérico, and Joaquim A. Casaca. "Relationship Marketing and Customer Retention - A Systematic Literature Review" Studies in Business and Economics, vol. 18, no. 3, Lucian Blaga University of Sibiu, 2023, pp. 44-66. https://doi.org/10.2478/sbe-2023-0044

Sun P., Mellahi K., Thun E., (2010). The dynamic value of MNE political embeddedness: The case of the Chinese automobile industry. Journal of International Business Studies, 41(7), 1161-1182. https://doi.org/10.1057/jibs.2009.94

Sun, Y., Liu, H., & Gao, Y. (2023). Research on customer lifetime value based on machine learning algorithms and customer relationship management analysis model. Heliyon, 9(2).https://doi.org/10.1016/j.heliyon.2023.e13384

Siegel J., (2007). Contingent political capital and international alliances: Evidence from South Korea. Administrative Science Quarterly, 52(4), 621-666. https://doi.org/10.2189/asqu.52.4.621

Wassouf, W. N., Alkhatib, R., Salloum, K., & Balloul, S. (2020). Predictive analytics using big data for increased customer loyalty: Syriatel Telecom Company case study. Journal of Big Data, 7(1), 29. https://doi.org/10.1186/s40537-020-00290-0

Wang, P. (2023). Research on risk management of A Bank's database information innovation project [Master's thesis, Beijing University of Posts and Telecommunications]. CNKI. https://doi.org/10.26969/d.cnki.gbydu.2023.001179

Ye, D. P. (2022). Protecting the Next Generation of Cyberattacks: Building Future Perception of Security (Master's thesis, Universidade NOVA de Lisboa (Portugal)). Retrieved from https://run.unl.pt/bitstream/10362/162762/1/2022_23_Fall_CHKP_David.pdf

Zhang, X., & Yi, G. (2024). Start-Ups and Innovation Ecosystem in China. Science, Technology and Society, 29(1), 54-74. https://doi.org/10.1177/09717218231215379

Zhou, Q. (2021). *Research on schedule optimization of middleware project of C company asset management system* [Master's thesis, Guangxi Normal University]. CNKI. https://doi.org/10.27036/d.cnki.ggxsu.2021.001531

Appendices

Appendix A – Questionnaire

Part 1: Basic Information of Respondents

1. What industry are you in?

☐Banking/Financial Institutions

☐Government Agencies

☐Internet/Technology Companies

☐Energy/Manufacturing/Telecom/Mobile Communications

☐Education/Schools

☐MSSP (Managed Security Service Provider)

☐Other (please specify)

2. What is your position?

☐CISO/Chief Information Security Officer

☐IT Manager/Security Lead

☐SOC (Security Operations Center) Team Member

☐Procurement/Decision Maker

☐Other (please specify)

3. Is your company currently using a SIEM solution?

☐Yes

☐No (skip to question 6)

4. Which SIEM product are you currently using? (Multiple choices allowed)

☐Splunk

☐IBM QRadar

☐ArcSight (HPE/Micro Focus)

☐Microsoft Sentinel

☐RSA NetWitness

☐Exabeam

☐Sumo Logic

☐360 Security Cloud

☐Huawei SecoManager

☐NSFOCUS SIEM

☐DBAPPSecurity SIEM

☐Venustech SIEM

☐Topsec SIEM

☐Sangfor SIEM

☐Other (please specify)

5. What is the primary purpose of your company using SIEM? (Multiple choices allowed)

☐Compliance with regulatory requirements (e.g., Level 2.0, GDPR, PCI-DSS)

☐Improving security operations efficiency

☐Incident detection and correlation analysis

☐End-to-end threat visualization

☐AI/Machine learning-enhanced detection

☐SOAR (Security Orchestration, Automation, and Response) integration

☐Other (please specify)

Part 2: Product

6. What product features are most important to your company during SIEM selection? (Multiple choices allowed)

☐AI-powered threat detection

☐Machine learning-improved SIEM rules

☐Lower false-positive rate in UEBA (User and Entity Behavior Analytics)

☐Faster log processing capabilities

☐Compatibility with domestic products (support for domestic CPUs, databases, operating systems)

☐High integration with other security tools (EDR, SOAR, IAM)

☐Other (please specify)

7. Compared to international SIEM products, in which areas do you think domestic SIEM products still have technical shortcomings? (Multiple choices allowed)

☐Incident detection accuracy

☐AI analysis capabilities

☐Visualization and reporting

☐Automated response (SOAR)

☐Ecosystem compatibility (APIs, integration capabilities)

☐Other (please specify)

8. If Dataori SIEM offers more efficient AI-driven threat detection and reduces false positives, would you consider it?

☐1 (Not at all)

☐2 (Unlikely)

☐3 (Neutral)

☐4 (Likely)

☐5 (Definitely)

Part 3: Price

9. How does your company decide on the SIEM procurement budget?

☐Annual budget, decided by the security team

☐CIO/CISO evaluates ROI before deciding on the budget

☐Temporary procurement driven by compliance and regulatory requirements

☐Other (please specify)

10. What pricing model does your company prefer for SIEM procurement?

☐One-time purchase (perpetual license, on-premise deployment)

☐Subscription-based SaaS (annual or usage-based payment)

☐Hybrid model (on-premise + cloud)

11. If Dataori SIEM offers a more flexible pricing model (e.g., pay-per-event instead of per-license), would you consider it?

☐1 (Not at all)

☐2 (Unlikely)

☐3 (Neutral)

☐4 (Likely)

☐5 (Definitely)

Part 4: Place

12. How does your company primarily gather information about SIEM solutions? (Multiple choices allowed)

☐Industry conferences/security summits

☐Online marketing (official website, SEO, paid ads)

☐Social media (WeChat, Zhihu, LinkedIn)

☐Word of mouth (customer case studies)

☐Free trials and PoC (Proof of Concept)

☐Other (please specify)

13. Which method does your company prefer for purchasing SIEM solutions?

☐Directly with the vendor

☐Through MSSP (Managed Security Service Provider)

☐Through local IT resellers

☐Other (please specify)

14. If Dataori SIEM adopts an MSSP distribution model, offering on-demand subscription services, would you consider it?

☐1 (Not at all)

☐2 (Unlikely)

☐3 (Neutral)

☐4 (Likely)

☐5 (Definitely)

Part 5: Promotion

15. If your company plans to purchase a new SIEM solution, how would you prefer to learn about new products in the market? (Multiple choices allowed)

☐Attend offline industry security conferences

☐Watch online webinars/product demos

☐Try free PoC (Proof of Concept)

☐Learn through social media (WeChat, Zhihu, LinkedIn)

☐Get recommendations from third-party reports (e.g., Gartner, IDC)

☐Other (please specify)

16. Is your company more inclined to choose SIEM products that have been used in domestic banks or government agencies?

☐Yes

☐No

☐Depends on specific performance

17. If Dataori SIEM offers a 3-6 month free trial, would you be willing to try it?

☐1 (Not at all)

☐2 (Unlikely)

☐3 (Neutral)

☐4 (Likely)

☐5 (Definitely)

Part 6: Market Prospects and Future Plans

18. Does your company plan to replace or add a SIEM solution in the next 1-2 years?

☐Yes

☐No

☐Uncertain

19. What do you think is the future direction of SIEM? (Multiple choices allowed)

☐AI-powered, reducing false positives

☐SaaS subscription model

☐Zero-trust architecture integration

☐Other (please specify)

20. What SIEM procurement model does your company prefer in the future?

☐One-time purchase, independent deployment

☐Subscription-based SaaS

☐Hybrid model (on-premise + cloud)

21. What do you think about the market opportunities for SIEM in the ITAI (Information Technology Application Innovation) environment?

☐Very large

☐Moderate

☐Very small

22. Does your company plan to switch from international vendors to domestic SIEM solutions in the next 3 years?

☐Yes

☐No

☐Depends on market development

Appendix B – Questionnaire Findings Overview

1. What industry are you in [Single Choice]

Option	Subtotal	Percentage
Banking/Financial Institutions	23	35.38%
Government Agencies	18	27.69%
Internet/Technology Companies	6	9.23%
Energy/Manufacturing/Telecom/Mobile Communications	8	12.31%
Education/Schools	5	7.69%
MSSP (Managed Security Service Provider)	4	6.15%
Other (please specify)	1	1.54%
Valid Count Per Participant	65	

2. What is your position? [Single Choice]

Option	Subtotal	Percentage
CISO/Chief Information Security Officer	17	26.15%
IT	14	21.54%
Manager/Security Lead	15	23.08%
SOC (Security Operations Center) Team Member	14	21.54%
Procurement/Decision Make	5	7.69%
Other (please specify)	0	0%
Valid Count Per Participant	65	

3. Is your company currently using a SIEM solution? [Single Choice]

Option	Subtotal	Percentage
Yes	53	81.54%
No	12	18.46%
Valid Count Per Participant	65	

4. Which SIEM product are you currently using? (Multiple choices allowed) [Multiple Choice]

Option	Subtotal	Percentage
Splunk	7	12.07%
IBM QRadar	12	20.69%
ArcSight (HPE/Micro Focus)	14	24.14%
Microsoft Sentinel	15	25.86%
RSA NetWitness	12	20.69%
Exabeam	19	32.76%
Sumo Logic	14	24.14%
360 Security Cloud	23	39.66%
Huawei SecoManager	15	25.86%
NSFOCUS SIEM	19	32.76%
DBAPPSecurity SIEM	5	8.62%
Venustech SIEM	17	29.31%
Topsec SIEM	19	32.76%
Sangfor SIEM	18	31.03%
Other (please specify)	1	1.72%
Valid Count Per Participant	58	

5. What is the primary purpose of your company using SIEM? (Multiple choices allowed) [Multiple Choice]

Option	Subtotal	Percentage
Improving security operations efficiency	33	56.9%
Incident detection and correlation analysis	41	70.69%
End-to-end threat visualization	40	68.97%
AI/Machine learning-enhanced detection	16	27.59%
SOAR (Security Orchestration, Automation, and Response) integration	23	39.66%
Other (please specify)	1	1.72%
Valid Count Per Participant	58	

6. What product features are most important to your company during SIEM selection? (Multiple choices allowed)） [Multiple Choice]

Option	Subtotal	Percentage
AI-powered threat detection	27	41.54%
Machine learning-optimized SIEM rules	23	35.38%
Lower false-positive rate in UEBA (User and Entity Behavior Analytics)	36	55.38%
Faster log processing capabilities	27	41.54%
Compatibility with domestic products (support for domestic CPUs, databases, operating systems)	35	53.85%
High integration with other security tools (EDR, SOAR, IAM)	27	41.54%
Other (please specify)	1	1.54%
Valid Count Per Participant	65	

7. Compared to international SIEM products, in which areas do you think domestic SIEM products still have technical shortcomings? (Multiple choices allowed) [Multiple Choice]

Option	Subtotal	Percentage
Incident detection accuracy	29	44.62%
AI	34	52.31%
analysis capabilities	38	58.46%
Visualization and reporting	33	50.77%
Automated response (SOAR)	24	36.92%
Ecosystem compatibility (APIs, integration capabilities)	21	32.31%
Other (please specify)	2	3.08%
Valid Count Per Participant	65	

8. If Dataori SIEM offers more efficient AI-driven threat detection and reduces false positives, would you consider it? [Single Choice]

Option	Subtotal	Percentage
1 (Not at all)	8	12.31%
2 (Unlikely)	10	15.38%
3 (Neutral)	33	50.77%
4 (Likely)	13	20%
5 (Definitely)	1	1.54%
Valid Count Per Participant	65	

9. How does your company decide on the SIEM procurement budget? [Single Choice]

Option	Subtotal	Percentage
Annual budget, decided by the security team	32	49.23%
CIO/CISO evaluates ROI before deciding on the budget	21	32.31%
Temporary procurement driven by compliance and regulatory requirements	8	12.31%
Other (please specify)	4	6.15%
Valid Count Per Participant	65	

10. What pricing model does your company prefer for SIEM procurement? [Single Choice]

Option	Subtotal	Percentage
One-time purchase (perpetual license, on-premise deployment)	29	44.62%
Subscription-based SaaS (annual or usage-based payment)	24	36.92%
Hybrid model (on-premise + cloud)	12	18.46%
Valid Count Per Participant	65	

11. If Dataori SIEM offers a more flexible pricing model (e.g., pay-per-event instead of per-license), would you consider it? [Single Choice]

Option	Subtotal	Percentage
1 (Not at all)	22	33.85%
2 (Unlikely)	13	20%
3 (Neutral)	16	24.62%
4 (Likely)	11	16.92%
5 (Definitely)	3	4.62%

Valid Count Per Participant	65	

12. How does your company primarily gather information about SIEM solutions? (Multiple choices allowed) [Multiple Choice]

Option	Subtotal	Percentage
Industry conferences/security summits	37	56.92%
Online marketing (official website, SEO, paid ads)	46	70.77%
Social media (WeChat, Zhihu, LinkedIn)	32	49.23%
Word of mouth (customer case studies)	38	58.46%
Free trials and PoC (Proof of Concept)	21	32.31%
Other (please specify)	1	1.54%
Valid Count Per Participant	65	

13. Which method does your company prefer for purchasing SIEM solutions? [Single Choice]

Option	Subtotal	Percentage
Directly with the vendor	18	27.69%
Through MSSP (Managed Security Service Provider)	30	46.15%
Through local IT resellers	15	23.08%
Other (please specify)	2	3.08%
Valid Count Per Participant	65	

14. If Dataori SIEM adopts an MSSP distribution model, offering on-demand subscription services, would you consider it? [Single Choice]

Option	Subtotal	Percentage
1 (Not at all)	10	15.38%
2 (Unlikely)	24	36.92%
3 (Neutral)	15	23.08%
4 (Likely)	15	23.08%
5 (Definitely)	1	1.54%
Valid Count Per Participant	65	

15. If your company plans to purchase a new SIEM solution, how would you prefer to learn about new products in the market? [Multiple Choice]

Option	Subtotal	Percentage
Attend offline industry security conferences	31	47.69%
Watch online webinars/product demos	50	76.92%
Try free PoC (Proof of Concept)	47	72.31%
Learn through social media (WeChat, Zhihu, LinkedIn)	28	43.08%
Get recommendations from third-party reports (e.g., Gartner, IDC)	29	44.62%
Other (please specify)	1	1.54%
Valid Count Per Participant	65	

16. Is your company more inclined to choose SIEM products that have been used in domestic banks or government agencies? [Single Choice]

Option	Subtotal	Percentage
Yes	22	33.85%

No	16	24.62%
Depends on specific performance	27	41.54%
Valid Count Per Participant	65	

17. If Dataori SIEM offers a 3-6 month free trial, would you be willing to try it? [Single Choice]

Option	Subtotal	Percentage
1 (Not at all)	31	47.69%
2 (Unlikely)	10	15.38%
3 (Neutral)	14	21.54%
4 (Likely)	9	13.85%
5 (Definitely)	1	1.54%
Valid Count Per Participant	65	

18. Does your company plan to replace or add a SIEM solution in the next 1-2 years? [Single Choice]

Option	Subtotal	Percentage
Yes	42	64.62%
No	17	26.15%
Uncertain	6	9.23%
Valid Count Per Participant	65	

19. What do you think is the future direction of SIEM? (Multiple choices allowed) [Multiple Choice]

Option	Subtotal	Percentage
AI-powered, reducing false positives	39	60%
SaaS subscription model	50	76.92%
Zero-trust architecture integration	38	58.46%
Other (please specify)	1	1.54%
Valid Count Per Participant	65	

20. What SIEM procurement model does your company prefer in the future? [Single Choice]

Option	Subtotal	Percentage
One-time purchase, independent deployment	36	55.38%
Subscription-based SaaS	15	23.08%
Hybrid model (on-premise + cloud)	14	21.54%
Valid Count Per Participant	65	

21. What do you think about the market opportunities for SIEM in the ITAI (Information Technology Application Innovation) environment? [Single Choice]

Option	Subtotal	Percentage
Very large	37	56.92%
Moderate	22	33.85%
Very small	6	9.23%
Valid Count Per Participant	65	

22. Does your company plan to switch from international vendors to domestic SIEM solutions in the next 3 years? [Single Choice]

Option	Subtotal	Percentage
Yes	41	63.08%
No	11	16.92%
Depends on market development	13	20%
Valid Count Per Participant	65	

Appendix C – In-depth interviews

Basic Information		
Interviewee Name		
Organization		
Position		
Interview Date		
Contact Information		
Question Number	**Interview Question (English Translation)**	**Module / Note**
Q1	Which category does your organization belong to? (For example: Government, Finance, Energy, Telecommunications, Other)	Basic Information Module
Q2	In your organization's IT procurement process, what is your primary role? (For example: Advisor, Reviewer, Decision-maker)	Basic Information Module
Q3	Regarding the procurement of SIEM systems, what do you consider to be the most critical factors? Please rank them in order of importance, including factors such as localization compatibility, real-time threat detection, false alarm rate control, compliance with security standards, maintenance costs, and after-sales service.	Demand Diagnosis Module
Q4	Please describe your organization's budget allocation for SIEM procurement. Typically, what percentage of the annual IT budget does the SIEM procurement represent? (For example: <5%, 5–10%, 10–15%, >15%)	Demand Diagnosis Module

Q5	Please describe the impact of Document No. 79 issued by the State-owned Assets Supervision and Administration Commission on your organization's IT procurement cycle, and indicate to what extent you believe the procurement cycle has been shortened (For example: shortened by >30%, shortened by 10–30%, no significant impact).	Market Strategy Verification Module
Q6	When learning about new SIEM products, through which methods do you prefer to obtain information? (For example: ITAI exhibitions, industry white papers, trial experiences, expert recommendations, competitor comparison reports)	Market Strategy Verification Module
Q7	When selecting a SIEM product, which payment method does your organization prefer? (For example: full upfront payment, 30/70 installment, pay-for-performance, annual subscription, etc.)	Business Conditions Module
Q8	When choosing a SIEM supplier, please rank the importance of the following partner qualifications: domestic CPU certification, security compliance testing qualification, financial ITAI laboratory certification, and state-owned cloud compatibility certification.	Business Conditions Module
Q9	Regarding the "Finance → Energy → Government" market path proposed by Dataori, in which segment do you believe the main implementation challenges arise? (For example: high compliance barriers in the finance sector, strong customization demands in the energy sector, long procurement cycles in the government sector, other)	Strategic Verification Module
Q10	What do you think are the key factors for a new SIEM brand to gain market trust? Please list the top three factors you consider most important.	Strategic Verification Module

Appendix D – In-depth interviews Findings Overview

Basic Information		
Interviewee Name	A001	
Organization	Technology Department at a Joint-Stock Commercial Bank	
Position	Security Manager	
Interview Date	2025/1/4	

Question Number	Interview Question (English Translation)	Module / Note
Q1	Which category does your organization belong to? (For example: Government, Finance, Energy, Telecommunications, Other) **Answer:** We are a nationwide joint-stock commercial bank with both corporate and retail financial services, ranking medium-sized in the industry.	Basic Information Module
Q2	In your organization's IT procurement process, what is your primary role? (For example: Advisor, Reviewer, Decision-maker) **Answer:** Primarily act as a security solution reviewer and advisor. Collaborate with risk management, compliance, and other departments for technical evaluations, ultimately submitting recommendations to senior leadership for decision-making.	Basic Information Module
Q3	Regarding the procurement of SIEM systems, what do you consider to be the most critical factors? Please rank them in order of importance, including factors such as localization compatibility, real-time threat detection, false alarm rate control, compliance with security standards, maintenance costs, and after-sales service. **Answer:** **Compliance with Classified Protection :** Strict financial regulations require all systems to meet compliance first. **Real-Time Threat Detection:** Early risk identification is critical for us. **False Alarm Control:** Excessive alerts create operational strain. **Localization Compatibility:** IT innovation and localization are prioritized, necessitating gradual replacement of foreign products. **Operational Costs:** Includes upgrades, expert services, etc. **Post-Sales Support:** Vendors must respond promptly to failures or security incidents.	Demand Diagnosis Module

Q4	Please describe your organization's budget allocation for SIEM procurement. Typically, what percentage of the annual IT budget does the SIEM procurement represent? (For example: <5%, 5–10%, 10–15%, >15%) **Answer:** SIEM typically accounts for 5%~10% of the annual IT security budget. If major upgrades are planned, this may slightly increase. Amount Range: Projects generally fall between ¥1.5M–¥2M, adjusted based on coverage, functionality depth, and advanced threat analysis modules.	Demand Diagnosis Module
Q5	Please describe the impact of Document No. 79 issued by the State-owned Assets Supervision and Administration Commission on your organization's IT procurement cycle, and indicate to what extent you believe the procurement cycle has been shortened (For example: shortened by >30%, shortened by 10–30%, no significant impact). **Answer:**Procurement timelines have shortened slightly, from 3–4 months to 2–3 months, due to the bank's preference for localized solutions and streamlined approvals. However, financial audits and compliance checks remain complex.	Market Strategy Verification Module
Q6	When learning about new SIEM products, through which methods do you prefer to obtain information? (For example: ITAI exhibitions, industry white papers, trial experiences, expert recommendations, competitor comparison reports) **Answer:**Financial industry seminars and IT localization exhibitions Industry white papers and competitive analysis reports Proof-of-Concept (PoC) testing for promising solutions to validate technical capabilities and scenario adaptability	Market Strategy Verification Module
Q7	When selecting a SIEM product, which payment method does your organization prefer? (For example: full upfront payment, 30/70 installment, pay-for-performance, annual subscription, etc.) **Answer:**Mostly 30/60/10 split: 30% upfront, 60% upon system acceptance,10% project acceptance. Subscription models are occasionally considered for smaller projects but remain uncommon.	Business Conditions Module

Q8	When choosing a SIEM supplier, please rank the importance of the following partner qualifications: domestic CPU certification, security compliance testing qualification, financial ITAI laboratory certification, and state-owned cloud compatibility certification. **Answer:** Classified Protection certification Financial IT innovation lab certification Compatibility with domestic CPUs State-owned cloud integration certification	Business Conditions Module
Q9	Regarding the "Finance → Energy → Government" market path proposed by Dataori, in which segment do you believe the main implementation challenges arise? (For example: high compliance barriers in the finance sector, strong customization demands in the energy sector, long procurement cycles in the government sector, other) **Answer:** Financial institutions impose stringent compliance requirements, especially in audits and technical evaluations. This demands high supplier expertise and product maturity, posing significant hurdles for new entrants.	Strategic Verification Module
Q10	What do you think are the key factors for a new SIEM brand to gain market trust? Please list the top three factors you consider most important. **Answer:** Prioritize financial compliance as a baseline requirement. Deliver robust performance with low false positives for precise threat detection. Invest in strong post-sales support and localized teams for rapid emergency response.	Strategic Verification Module

Basic Information		
Interviewee Name	A002	
Organization	State-Owned Large Petrochemical Enterprise	
Position	Safety Management Director	
Interview Date	2025/1/6	
Question Number	**Interview Question (English Translation)**	**Module / Note**

Q1	Which category does your organization belong to? (For example: Government, Finance, Energy, Telecommunications, Other) **Answer:**We are a state-owned large petrochemical enterprise spanning refining, oil/gas extraction, downstream sales, and other sectors.	Basic Information Module
Q2	In your organization's IT procurement process, what is your primary role? (For example: Advisor, Reviewer, Decision-maker) **Answer:**I am primarily responsible for safety requirement analysis and technical reviews for petrochemical operations. For systems like SIEM and SOC, I consolidate needs from various plants, conduct unified evaluations, and initiate projects.	Basic Information Module
Q3	Regarding the procurement of SIEM systems, what do you consider to be the most critical factors? Please rank them in order of importance, including factors such as localization compatibility, real-time threat detection, false alarm rate control, compliance with security standards, maintenance costs, and after-sales service. **Answer:** **Real-Time Threat Detection:** Production environments cannot tolerate delays in addressing security risks. **Compliance with Classified Protection :** Strict cybersecurity and industrial control system requirements in the petrochemical sector. **False Alarm Control:** Excessive alerts disrupt production scheduling. **Localization Compatibility:** Enterprise-wide push for IT innovation and localization, emphasizing controllable infrastructure. **Post-Sales Support:** Immediate assistance is critical for production-related incidents. **Operational Costs:** Long-term maintenance, upgrades, and lifecycle management must be factored in.	Demand Diagnosis Module

Q4	Please describe your organization's budget allocation for SIEM procurement. Typically, what percentage of the annual IT budget does the SIEM procurement represent? (For example: <5%, 5–10%, 10–15%, >15%) **Answer:** SIEM typically accounts for 5%~8% of the annual IT security budget. This may increase during years focused on IT security upgrades. Project Range: Centralized SIEM deployments for a single plant often exceed ¥1.5M, covering multi-system integration, customized development, and multi-site operational support.	Demand Diagnosis Module
Q5	Please describe the impact of Document No. 79 issued by the State-owned Assets Supervision and Administration Commission on your organization's IT procurement cycle, and indicate to what extent you believe the procurement cycle has been shortened (For example: shortened by >30%, shortened by 10–30%, no significant impact). **Answer:** Procurement processes have accelerated overall, but due to industrial control security testing and on-site integration requirements, cycles remain moderate. Previously taking 4+ months, they now take ~3 months.	Market Strategy Verification Module
Q6	When learning about new SIEM products, through which methods do you prefer to obtain information? (For example: ITAI exhibitions, industry white papers, trial experiences, expert recommendations, competitor comparison reports) Answer:Industry exhibitions and industrial security conferences Expert reports and third-party evaluations Proof-of-Concept (PoC) pilots to validate compatibility with production environments	Market Strategy Verification Module
Q7	When selecting a SIEM product, which payment method does your organization prefer? (For example: full upfront payment, 30/70 installment, pay-for-performance, annual subscription, etc.) Answer:40/30/30 phased payments: 40% upon signing, 30% upon mid-term delivery or milestone acceptance, and 30% after final confirmation of operational stability.	Business Conditions Module

Q8	When choosing a SIEM supplier, please rank the importance of the following partner qualifications: domestic CPU certification, security compliance testing qualification, financial ITAI laboratory certification, and state-owned cloud compatibility certification. **Answer:** Classified Protection certification State-owned cloud integration certification Compatibility with domestic CPUs Financial IT innovation lab certification (less critical for our petrochemical industry)	Business Conditions Module
Q9	Regarding the "Finance → Energy → Government" market path proposed by Dataori, in which segment do you believe the main implementation challenges arise? (For example: high compliance barriers in the finance sector, strong customization demands in the energy sector, long procurement cycles in the government sector, other) **Answer:** Energy sectors demand high customization, particularly as petrochemical industrial control systems differ significantly from traditional office IT. Vendors must possess deep industry expertise and commit to long-term technical support.	Strategic Verification Module
Q10	What do you think are the key factors for a new SIEM brand to gain market trust? Please list the top three factors you consider most important. **Answer:** Ensure stability and security in industrial control environments as a baseline. Deliver high accuracy with low false positives to minimize production disruptions. Provide rapid post-sales response, ideally with on-site teams or localized support.	Strategic Verification Module

Basic Information		
Interviewee Name	A003	
Organization	Security Management at a Regional Small/Medium-Sized State-Owned Bank	
Position	Head of Security Management	
Interview Date	2025/1/20	

Question Number	Interview Question (English Translation)	Module / Note
Q1	Which category does your organization belong to? (For example: Government, Finance, Energy, Telecommunications, Other) **Answer:**We are a regional small/medium-sized state-owned bank primarily serving local businesses and individual customers.	Basic Information Module
Q2	In your organization's IT procurement process, what is your primary role? (For example: Advisor, Reviewer, Decision-maker) **Answer:**As the security management lead, I oversee technical feasibility analysis and requirement verification for security products like SIEM, then submit proposals to procurement and senior leadership for approval.	Basic Information Module
Q3	Regarding the procurement of SIEM systems, what do you consider to be the most critical factors? Please rank them in order of importance, including factors such as localization compatibility, real-time threat detection, false alarm rate control, compliance with security standards, maintenance costs, and after-sales service. **Answer:** **Compliance with Classified Protection:** audits are mandatory for banks. **False Alarm Control:** Limited staffing demands high-quality alerts. **Real-Time Threat Detection:** Early risk identification is critical. **Localization Compatibility:** We are aligning with national IT innovation initiatives. **Post-Sales Support:** Vendors must respond swiftly to major security incidents. **Operational Costs:** Budget constraints require cost-effective and precise solutions.	Demand Diagnosis Module
Q4	Please describe your organization's budget allocation for SIEM procurement. Typically, what percentage of the annual IT budget does the SIEM procurement represent? (For example: <5%, 5–10%, 10–15%, >15%) Answer:Typically 5%~10% of the annual IT security budget, potentially higher during system security upgrade years. Amount Range: SIEM solutions for our bank generally cost ~¥500K, with larger deployments reaching ~¥1M, reflecting the institution's smaller scale.	Demand Diagnosis Module

Q5	Please describe the impact of Document No. 79 issued by the State-owned Assets Supervision and Administration Commission on your organization's IT procurement cycle, and indicate to what extent you believe the procurement cycle has been shortened (For example: shortened by >30%, shortened by 10–30%, no significant impact). **Answer:** Procurement timelines have moderately accelerated, saving about 1–2 months compared to the past. However, audits, risk controls, and compliance checks remain mandatory.	Market Strategy Verification Module
Q6	When learning about new SIEM products, through which methods do you prefer to obtain information? (For example: ITAI exhibitions, industry white papers, trial experiences, expert recommendations, competitor comparison reports) **Answer:** Industry conferences and exhibitions Consultant recommendations and third-party white papers Peer implementations Small-scale PoC testing to validate suitability before purchase	Market Strategy Verification Module
Q7	When selecting a SIEM product, which payment method does your organization prefer? (For example: full upfront payment, 30/70 installment, pay-for-performance, annual subscription, etc.) **Answer:** 30/60/10 phased payments: 30% upfront, 60% upon system deployment, and 10% after warranty period acceptance.	Business Conditions Module
Q8	When choosing a SIEM supplier, please rank the importance of the following partner qualifications: domestic CPU certification, security compliance testing qualification, financial ITAI laboratory certification, and state-owned cloud compatibility certification. **Answer:** Classified Protection certification Financial IT Innovation Lab certification Compatibility with domestic CPUs State-owned cloud integration certification	Business Conditions Module

Q9	Regarding the "Finance → Energy → Government" market path proposed by Dataori, in which segment do you believe the main implementation challenges arise? (For example: high compliance barriers in the finance sector, strong customization demands in the energy sector, long procurement cycles in the government sector, other) **Answer:** Financial institutions face high regulatory compliance barriers—even small/medium banks must navigate rigorous risk control and audit processes, demanding vendors with proven expertise.	Strategic Verification Module
Q10	What do you think are the key factors for a new SIEM brand to gain market trust? Please list the top three factors you consider most important. **Answer:**Obtain compliance certifications and evaluations as a baseline. Deliver reliable technology with minimal false alarms. Provide mature operational support, as smaller banks heavily rely on vendor expertise.	Strategic Verification Module