INSTITUTO
UNIVERSITÁRIO
DE LISBOA

Marketing Plan of Dataori's SIEM platform

Asen Zhang

Master in Applied Management

Supervisor:
Professor Doctor Rui Vinhas da Silva, Assistant Professor
ISCTE-IUL

March, 2025

iscte

BUSINESS
SCHOOL

Department of Marketing, Operations and General Management

Marketing Plan of Dataori's SIEM platform

Asen Zhang

Master in Applied Management

Supervisor:
Professor Doctor Rui Vinhas da Silva, Assistant Professor
ISCTE-IUL

March, 2025

Acknowledgements

The completion of this paper would not have been possible without the guidance and support of many mentors, colleagues, friends, and industry experts. Here, I would like to express my sincere gratitude to all the individuals and institutions who have provided their support.

First and foremost, I would like to extend my special thanks to my supervisors, Professor Rui Vinhas da Silva and Professor Sofia Lopes Portela, for their meticulous guidance, valuable advice, and continuous encouragement throughout the research process. Their professional expertise and academic insights were instrumental in shaping the direction and quality of this research, allowing me to continuously refine the paper's content and deepen my understanding of the research topic..

I am also grateful to my colleagues and friends for their constructive discussions during the research process, their valuable insights, as well as their encouragement and support during challenging times. Their assistance not only enriched the content of this paper but also deepened my perspective on the research issues.

Finally, I wish to thank the companies and experts who offered data support and professional insights for industry research. Their contributions enabled this paper to perform in-depth market analysis and ensured its practical value.

The completion of this paper owes much to everyone's help and contributions. Once again, I extend my heartfelt gratitude to everyone who has offered their support.

Abstract

With the escalation of cybersecurity threats and stricter government mandates for information security, Security Information and Event Management (SIEM) systems have become increasingly vital in enterprise security operations. Driven by China's Information Technology Application Innovation (ITAI) policy, the domestic demand for localized SIEM solutions has grown rapidly at a compound annual rate of 37%. As a domestic SIEM provider, Dataori faces significant challenges in market penetration, including technical compatibility issues, product localization difficulties, market entry barriers, and intense competition from international vendors dominating high-end segments and numerous domestic rivals competing aggressively on price and service.

Utilizing qualitative research methods—including comprehensive market analysis, competitive benchmarking, structured questionnaires with industry professionals, and expert interviews—this thesis explores critical success factors for localized SIEM solutions. The research identifies core opportunities such as AI-driven threat detection innovation, flexible SaaS subscription models tailored to local enterprise needs, targeted precision marketing strategies, and strategic ecosystem partnerships involving public-private collaboration.

Findings indicate that Dataori can leverage its advanced AI capabilities, localization advantages in compliance and technical adaptation, and adaptive business models to establish differentiated competitive positioning. The thesis recommends prioritizing targeted product refinement aligned with Chinese customer preferences, strategic channel development initiatives to enhance market reach, and precise brand differentiation efforts to clearly communicate Dataori's unique value proposition.

This thesis aims to assess Dataori's opportunities in the Chinese SIEM market and propose effective market expansion strategies to increase revenue.

Keywords: Security Information and Event Management (SIEM), Information Technology Application Innovation (ITAI), Cybersecurity Artificial Intelligence (AI), Localization, Marketing Strategy

JEL Classification: O33, O38

Resumo

Com a escalada de ameaças à cibersegurança e mandatos governamentais mais rigorosos para a segurança da informação, os sistemas de Gestão de Informação e Eventos de Segurança (SIEM) tornaram-se cada vez mais vitais nas operações de segurança empresarial. Impulsionada pela política de Inovação em Aplicações de Tecnologias de Informação (ITAI) da China, a procura interna por soluções SIEM localizadas cresceu rapidamente a uma taxa anual composta de 37%. Como fornecedor nacional de SIEM, a Dataori enfrenta desafios significativos na penetração no mercado, incluindo problemas de compatibilidade técnica, dificuldades de localização de produtos, barreiras à entrada no mercado e intensa concorrência de fornecedores internacionais que dominam segmentos de topo e vários rivais nacionais a competir agressivamente em preço e serviço.

Utilizando métodos de investigação qualitativa — incluindo análise de mercado abrangente, benchmarking competitivo, questionários estruturados com profissionais do setor e entrevistas com especialistas — este estudo explora fatores críticos de sucesso para soluções SIEM localizadas. A investigação identifica oportunidades importantes, como a inovação na deteção de ameaças orientada por IA, modelos flexíveis de subscrição de SaaS adaptados às necessidades empresariais locais, estratégias de marketing de precisão direcionadas e parcerias estratégicas de ecossistemas que envolvem colaboração público-privada.

As conclusões indicam que a Dataori pode alavancar as suas capacidades avançadas de IA, vantagens de localização em conformidade e adaptação técnica, e modelos de negócio adaptáveis para estabelecer um posicionamento competitivo diferenciado. O estudo recomenda a priorização do refinamento de produtos direcionados, alinhados com as preferências dos clientes chineses, iniciativas estratégicas de desenvolvimento de canais para aumentar o alcance do mercado e esforços precisos de diferenciação da marca para comunicar claramente a proposta de valor única da Dataori.

Palavras-Chave: Gestão de Informação e Eventos de Segurança (SIEM), Inovação em Aplicações de Tecnologias de Informação (ITAI), Inteligência Artificial (IA) de Cibersegurança, Localização, Estratégia de Marketing

JEL Classification: O33, O38

Table of Contents

List of Tables

List of Figures

Glossary

AI	Artificial Intelligence
CAC	Customer Acquisition Cost
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.

This thesis focuses on the challenges faced by Dataori SIEM platform in the localization promotion process in the Chinese market. Although Dataori has technical advantages such as AI empowerment, data adaptation, and automated threat detection, it still needs to be further improved in terms of market entry, channel expansion, and product localization adaptation. How to establish a differentiated competitive advantage in the fiercely competitive SIEM market? Based on Porter's value chain model, the research focuses on Dataori's strategic gaps in three dimensions: policy adaptation (trusted innovation certification), channel network (MSSP cooperation), and customer operation (financial industry improvement), which has become the core issue of this thesis.

The goal of this thesis is to analyze Dataori's SIEM development opportunities in the Chinese market and develop a feasible localized marketing plan. Specifically, this thesis will evaluate SIEM industry trends, target customer needs, and competitive landscape, and then design a market entry strategy suitable for Dataori, covering product improved, marketing, channel expansion, and brand building. In addition, the thesis will also explore business models such as SaaS subscription models, AI-enabled SIEM, and government and enterprise cooperation to enhance Dataori's sustainable development capabilities in the market.

This thesis employs a mixed-method approach combining qualitative and quantitative methods, including market research, competitive benchmarking through detailed comparative analysis of key domestic and international competitors, and case analysis to ensure the scientificity and feasibility of strategy formulation. First, the current status and future development trends of the Chinese SIEM market are analyzed through industry data. Secondly, the competitive strategies of major foreign and domestic SIEM suppliers are studied, and combined with successful market entry cases, to provide reference for Dataori. Finally, combined with expert interviews and user needs analysis, a targeted marketing plan is proposed, and a monitoring and evaluation mechanism is established to ensure the implementation of the market strategy.

This includes market research, competitive benchmarking and case analysis to ensure the scientific and feasibility of strategy formulation. First, the current status and future development trends of the Chinese SIEM market are analyzed through industry data. Secondly, the competitive strategies of major foreign and domestic SIEM suppliers are studied, and combined with successful market entry cases to provide reference for Dataori. Finally, through the collected 30 questionnaires and in-depth interviews with 3 experts, combined with user needs analysis, a targeted marketing plan is proposed, and a monitoring and evaluation mechanism is established to ensure the implementation of the market strategy.

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. Global Market Overvie

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).

2.5. 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)

2.6. 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).

2.7. 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).

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.

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 behaviors, pricing model preferences, and future adoption intentions.

The questionnaire was distributed to industry customers, partners, and related players using purposive sampling to ensure relevance to the SIEM domain. The target was to collect at least 30 valid responses from using purposive sampling from large enterprises within finance (45%), government (35%), and other sectors (20%). Additionally, three indepth-views expert interviews were conducted with senior cybersecurity professionals from financial institutions and enterprise agencies to validate questionnaire findings and provide deeper insights into market trends. 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.

Research subjects: IT decision makers and security operation center (SOC) managers of large Chinese enterprises and government agencies.

Contaminant method: The contaminant method is adopted to ensure that the samples are sampled in key industries such as finance, government, telecommunications and energy.

Data collection time: December 28, 2024 to March 15, 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 openended survey responses is applied to extract essential market insights, providing a robust foundation for the targeted market strategy.

4. Marketing 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 behavior 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 five-year 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 improvementmechanism 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. 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 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. 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 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.

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 favorable 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 favorable 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 behavioral 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 improvementare 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). 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, and the implementation of the "Data Security Law" and the "Personal Information Protection Law" 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 QRadar (NYSE: IBM) is IBM's SIEM product. From a financial perspective, IBM's security business revenue in 2022 was US$3.62 billion, accounting for 4.3% of the company's overall revenue, with a compound growth rate of -1.2% in the past three years. 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. 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 2023. 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 according to the latest financial report, Splunk achieved significant financial improvements in fiscal 2024, with net profit reaching US$264 million and operating income increasing to US$4.216 billion.

Palo Alto Networks (NYSE:PANW)'s financial performance shows that the company's revenue increased from US$3.40 billion in fiscal 2020 to US$5.42 billion in fiscal 2022, with net profit margins of -3.8%, -6.1% and -4.3% in the three years. 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 increased from US$2.59 billion in 2020 to US$4.42 billion in 2022, but the gross profit margin decreased slightly, from 77.2% in 2020 to 76.4% in 2022. 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) reached US$2.59 billion in annual recurring revenue (ARR) in fiscal 2023, a year-on-year increase of 54%. 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）

Souce: 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	2022 Revenue (100 million RMB)	Net Profit Margin	2021 Revenue	2020 Revenue	Core Products	ITAI adaptation progress
Qianxin	¥64.09	-18.20%	¥58.09	¥41.61	NGSOC	Full stack adaptation
Venusstar	¥43.63	12.10%	¥42.37	¥36.47	Taihe SOC	Complete Kunpeng certification
Anheng Information	¥19.8	-28.60%	¥18.2	¥13.23	AiLPHA platform	Tongxin UOS certification
Sangfor	¥74.12	10.60%	¥67.89	¥54.58	XDR platform	Kirin OS adaptation
360 Digital Technology	¥95.6	-6.80%	¥108.86	¥116.15	Digital security brain for the entire network	MIIT pilot
Green Alliance Technology	¥26.72	2.50%	¥26.09	¥20.1	Intelligent security operation platform	Feitian CPU adaptation

Source: Author (2025)

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 2022 reached 6.409 billion yuan, and Sangfor reached 7.412 billion yuan, both maintaining rapid growth. (Source: 2023 China Cybersecurity Industry Market Competition Pattern - Sina Finance)

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.

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.

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.

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.

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.

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 defense 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.

4.4. SWOT Analysis

Strengths

With 20 years of industry technology accumulation in the SIEM industry, we have a deep understanding of the international SIEM architecture and functional characteristics, and can combine the world's leading technology concepts with localized needs to create highly adaptable products.

Advantages of credible innovation adaptation. Dataori has completed the adaptation with domestic operating systems (UOS, Kylin), domestic databases (Da Meng, Renda Jincang) and domestic CPUs (Kunpeng, Feiteng), ensuring the compliance of products in the financial credible innovation environment, which is conducive to entering key industries such as government and banks.

There are already landing cases in the financial industry. Dataori has successfully landed in one of the six state-owned banks, a national joint-stock bank, Sinopec, government agencies and other projects, forming a benchmark effect, which is conducive to the expansion of the banking market.

Combination of AI+SIEM. Dataori plans to launch a SIEM+AI product model, combining AI automatic threat detection and intelligent incident response to establish technical barriers in reducing false alarm rates and improving detection accuracy.

Lightweight deployment, launching SaaS SOC solutions for small and medium-sized banks and enterprises, compared with traditional localized SIEM deployment, the cost can be reduced by 60%, which is helpful to develop the long-tail market.

Weaknesses

Insufficient capital investment. Dataori's annual revenue is only 3-5 million RMB. Compared with the leading manufacturers (Qi'anxin, Venustech, Sangfor, etc., with annual revenue of 4-9 billion RMB), its R&D investment capacity is limited. The average R&D investment of leading manufacturers accounts for 28%. Dataori's current R&D investment is insufficient, which may affect the speed of product innovation.

Limited brand influence. In the financial industry, Qi'anxin, Venustech and other brands have higher recognition. Government and bank customers tend to choose verified products from large manufacturers. Dataori needs to strengthen market promotion and improve brand recognition.

Weak ecological resources. Leading manufacturers bind customers through government procurement alliances, UnionPay ITAI ecology, etc. Dataori is still in the independent operation stage and has not yet built a large-scale ecological cooperation network.

Limited delivery capability. The Dataori team has only 20 people, 80% of whom are engaged in R&D. There are bottlenecks in large-scale project delivery, customer support, and operation and maintenance capabilities, and Dataori does not have the national delivery capability of the leading manufacturers.

Opportunities

Policy dividends for ICT innovation. Government procurement policies are tilted. The target of special procurement for small and medium-sized enterprises will be increased to 40% by 2025. Dataori is expected to obtain more orders from the government and financial institutions.

Growth in the sub-market. The financial ICT innovation market is expected to exceed 300 billion yuan in 2026. There are still a lot of undeveloped markets in the sub-scenarios (such as city commercial banks, rural credit cooperatives, and insurance institutions). Dataori can deeply cultivate the small and medium-sized bank market (potential scale of 3 billion yuan).

Ecological cooperation opportunities. 60% of the leading manufacturers open API interfaces. Dataori can join the ICT innovation ecological alliance by integrating domestic databases, OS, and ICT innovation clouds to enhance market access advantages.

AI+SIEM technology trend. AI+SIEM will become the core technology trend of the next generation of SIEM. Dataori can focus on AI to reduce false alarm rate and intelligent security operation, and build core competitiveness in technological innovation.

Capital market support. In recent years, the financing of the cybersecurity industry has been active. Dataori can consider applying for industrial fund support, raising RMB 30 million+, and increasing R&D investment.

Threats

Technical barriers of leading manufacturers. The average patent reserves of leading manufacturers such as Qi'anxin and Venustech exceed 2,000, and their technological advantages are obvious. The top three manufacturers in the industry occupy 85% of the market share of party and government agencies. Dataori faces challenges in acquiring large-scale customers.

Price war risk. The gross profit margin of the SIEM industry has dropped from 75% in 2019 to 63% in 2022. Intensified market competition may lead to price wars, affecting Dataori's profitability.

Alternative technology threats, emerging security technologies such as XDR (Extended Detection Response) and SOAR (Automated Orchestration Response) are gradually replacing traditional SIEM. The cloud-native security operation center solutions provided by cloud vendors (such as Alibaba Cloud and Tencent Cloud) may weaken Dataori's competitiveness in the cloud market.

The customer procurement cycle is long. The average POC test cycle for financial industry customers is ⩾ 6 months. The procurement process is complicated, which puts great pressure on the capital turnover of small and medium-sized enterprises.

4.5. Marketing Plan Objectives

Following in-depth interviews with the company’s CEO, the core strategic objective for the future development of the Dataori SIEM platform has been clearly defined: to achieve a 15%

market penetration rate in key industries—such as government, finance, and energy—and to exceed annual revenues of RMB 10 million. To attain this primary objective, the company will focus on four key strategic pillars, each with predetermined targets that support one another, as outlined below:

Product Innovation Strategy: The objective is to enhance the AI Copilot functionality, transforming the traditional SIEM operation model from one that relies on SQL queries to an interactive, AI-driven Q&A approach. This transformation is expected to reduce the technical barriers and learning curve associated with security operations. Simultaneously, the introduction of a “Security Data Lake” storage mode aims to improve data storage practices, targeting a 30% to 50% reduction in log storage costs while maintaining a false alarm rate below 8%. These product-level innovations are designed to improve user experience and product competitiveness, thereby driving a steady increase in market penetration.

Ecosystem Expansion Strategy: The goal here is to establish strategic partnerships with more than 10 leading domestic IT security vendors, MSSPs, and IT agents. By constructing a mutually beneficial security ecosystem, the company intends to broaden market channels and expand product coverage. This strategy will provide robust technical and channel support for the promotion of Dataori’s products across various sectors.

Financial Growth Strategy: The objective is to improve the SaaS subscription model and implement a tiered pricing strategy to enhance the average revenue from high-end customers and overall annual recurring revenue (ARR). Achieving these financial targets is expected to directly contribute to surpassing the RMB 10 million annual revenue mark, thereby laying a solid economic foundation for long-term growth.

Brand Recognition Strategy: This strategy aims to boost Dataori’s brand influence and market visibility within the domestic SIEM sector. The focus is on strengthening industry engagement and information dissemination through multi-channel marketing efforts, which will enhance market trust and brand competitiveness. Such improvements in brand recognition will provide sustained support for product promotion and channel expansion.

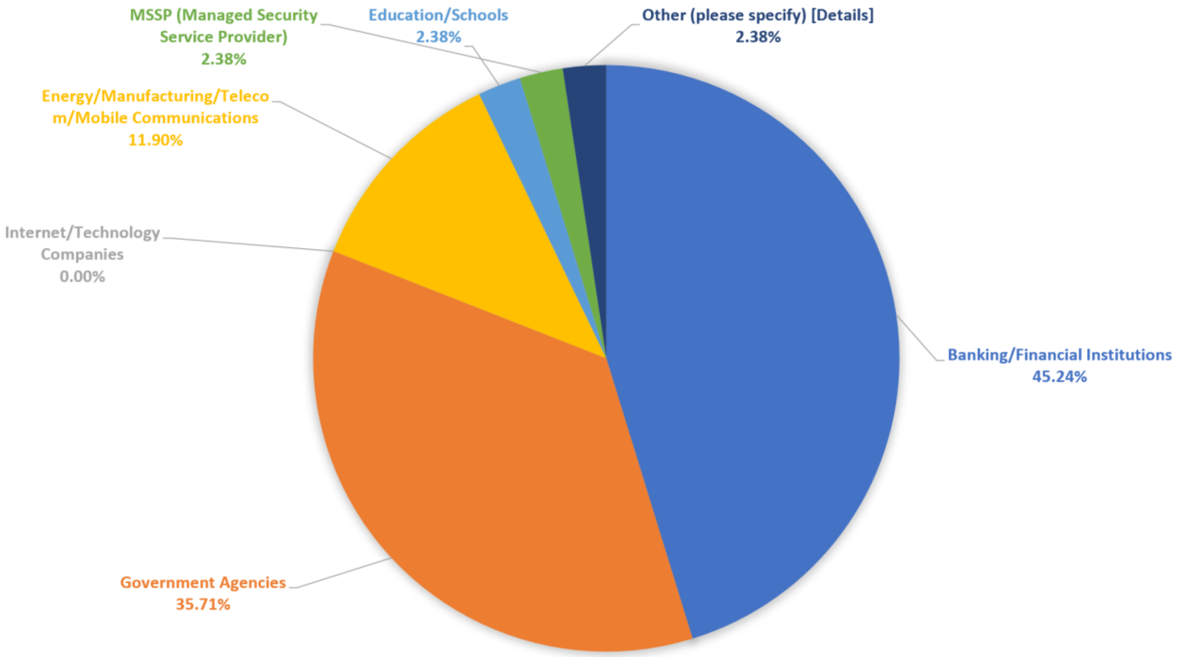
4.6. Segmentation, Targeting and Positioning

4.6.1. Segmentation

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

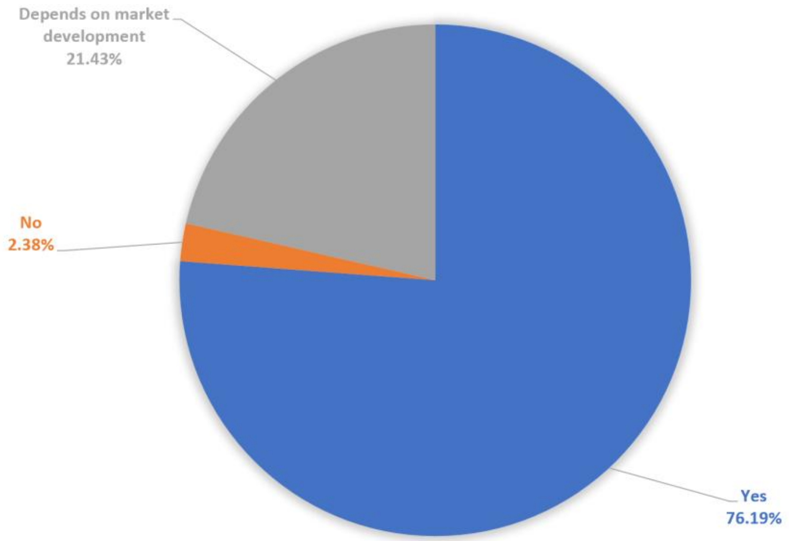


Source: Author (2025)

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.

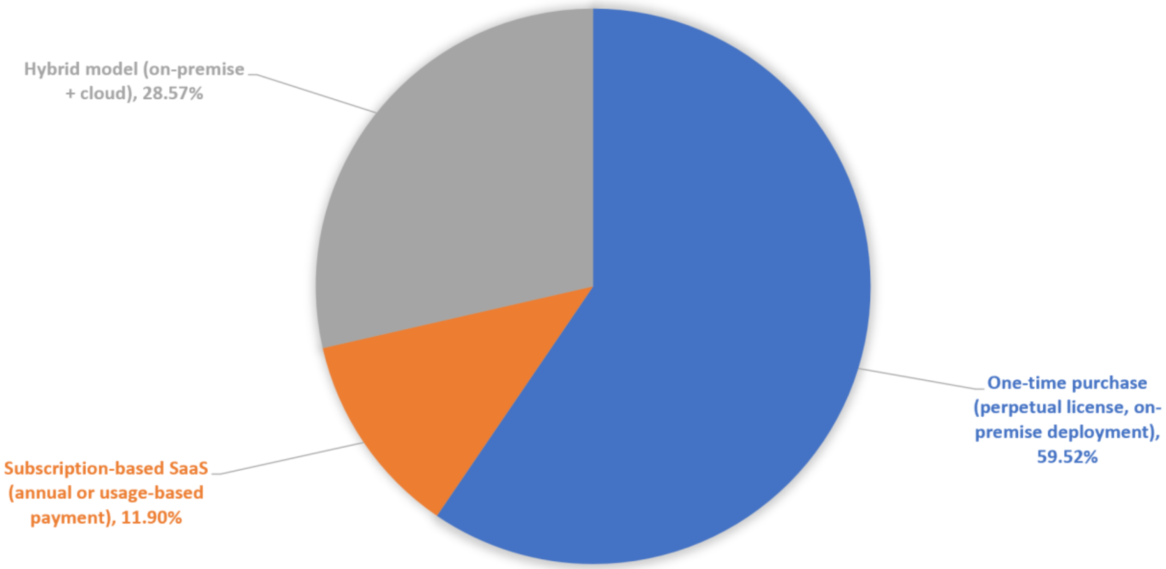
Figure 4.2 Plan to Switch to Domestic SIEM in the Next 3 Years



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.

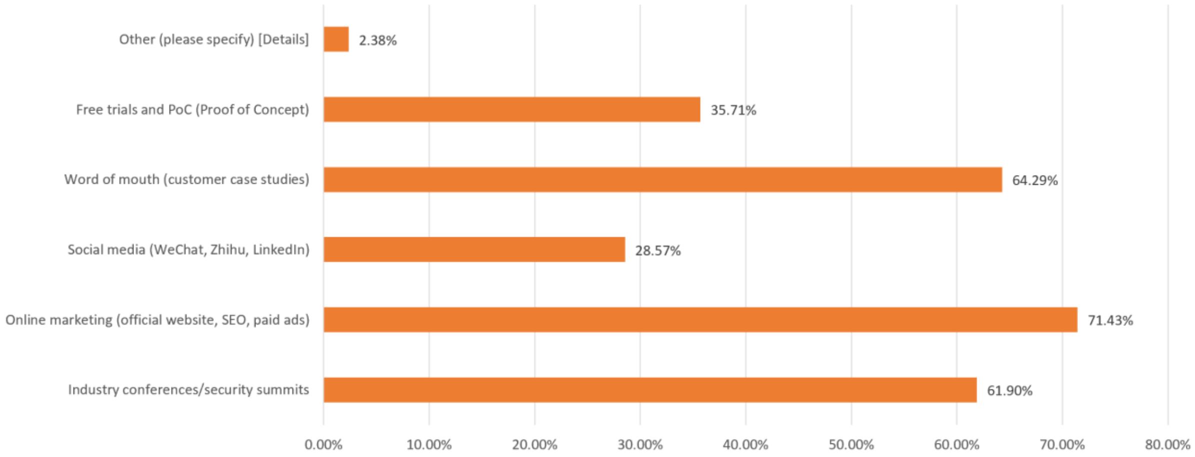
Figure 4.3 Preferred SIEM Procurement Method



Source: Author (2025)

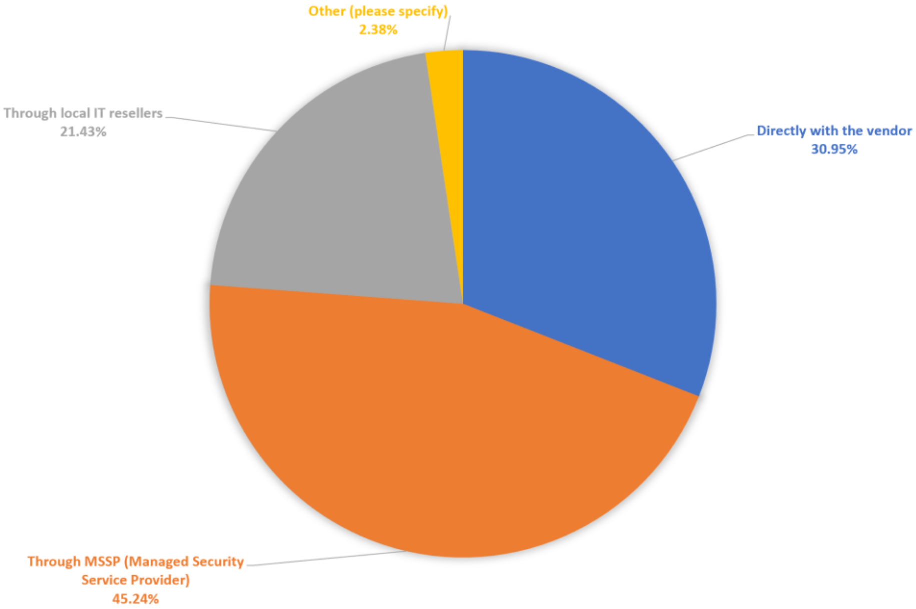
When acquiring information about SIEM solutions, enterprises primarily rely on industry summits & conferences, followed by technical white papers & industry reports, which remain key influencers in procurement decisions. Furthermore, free trials play a crucial role in product evaluation, particularly 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 Method



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.

4.6.2. Targeting

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.

4.6.3. Positioning

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.

4.7. Marketing-Mix

4.7.1. Product

The demand for domestic ICT adaptation has increased. With the advancement of the "Information Technology Application Innovation Industry Development Plan (2023-2025)" (SASAC Document No. 79), the government and key industries have continuously increased their demand for localization. Dataori SIEM's compatibility with domestic operating systems (UOS, Kylin OS) and domestic databases (DaMeng, Renda Jincang, OceanBase) can initially establish a foundation of trust in the fields of party and government, finance, energy, telecommunications, etc., and also open up a broader market for the company. According to the 2024 ICT Industry White Paper, domestic OS and database penetration in core industries has a CAGR of over 30%, and the scale of localized procurement in the next three years can reach 200 billion yuan (iResearch, 2023). This indirectly shows that Dataori is tapping into the potential of the "domestic substitution" trend. However, this also brings about the problems of high adaptation costs and immature ecology: there is a big gap between domestic operating systems and foreign Windows/Linux systems in kernel compatibility and driver adaptation, and Dataori must invest significant resources in testing and tuning; similar products sometimes lack large-scale log processing and distributed analysis capabilities, and need to continue to work closely with domestic operating system manufacturers to conduct stress testing and bug tracking. It is recommended that a dedicated team be established to perform regression testing on key functions when the operating system is upgraded or a new version appears, and to make the core testing process and data public to potential customers as endorsement.

Through AI empowerment and intelligent analysis, Dataori simplifies the operation process of log analysis, event correlation, and automated response by applying AI natural semantic conversion, which can significantly reduce the workload of security operators and improve detection accuracy. If SIEM products have AI correlation analysis capabilities, they can reduce false alarm rates and enhance the effectiveness of advanced threat detection; however, they also face challenges in data quality and computing power costs: training AI models requires huge and diverse security log data, and many domestic companies still lack standardized log management or are unwilling to share data due to sensitivity, which may lead to biased models; deep learning models also have high computing power requirements, and if customers choose local deployment, the cost of hardware upgrades cannot be ignored. Cloud resource investment likewise needs to be evaluated under the SaaS subscription model. For this reason, it is recommended that a ‘threat intelligence sharing platform’ be established in collaboration with industry associations or government departments, enabling multiple institutions to anonymously contribute security logs to build a large sample training set; and for small and medium-sized customers, lightweight models can be used first, lessening the need for high-performance hardware.

Based on the questionnaire results, it can be seen that AI-driven threat detection (Threat Detection) is the top concern for customers, and security operations combined with AI-enabled threat detection can significantly improve analysis efficiency. To this end, the Dataori SIEM platform uses AI as the core driver at the product level to build a TDIR (Threat Detection, Investigation & Response) integrated engine to achieve accurate threat detection, efficient investigation, and automated response. First, at the threat detection level, the platform uses a deep learning model based on the Transformer architecture to perform context-aware analysis on massive security data to more accurately identify both known and unknown threats. It builds a distributed threat intelligence network through federated learning technology, and each node can collaborate to train and improve detection models without sharing raw data, thereby sharing threat intelligence in real time and improving collaborative defense. It uses graph neural networks (GNNs) to model multi-dimensional elements such as network topology, user behavior, and asset information, and constructs an attack path map, which can quickly locate the source of the attack, predict potential targets, and evaluate the scope of impact, providing decision support for subsequent responses. It also leverages an adaptive threat detection mechanism to dynamically adjust detection strategies and parameters based on security operations and new attack types; once an unknown attack is discovered, it automatically learns its characteristics and generates new detection rules, continuously improving its threat identification level.

At the investigation level, an AI-assisted Threat Investigation function is added. Dataori SIEM introduces natural language query (NLQ) technology, which enables security analysts to describe security incidents in everyday language. The platform automatically converts this input into query statements and extracts information from massive data, significantly streamlining the investigation process. The system also employs AI technology for root cause analysis (RCA), automatically identifying intrusion paths, vulnerability details, and attack payloads, offering remediation suggestions and notably reducing troubleshooting time. Meanwhile, it can automatically extract IP addresses, domain names, malicious code features, and other elements from security incidents, correlating and analyzing them with other intelligence sources to continuously expand its threat intelligence library and bolster detection accuracy. It also integrates multiple data sources such as threat intelligence, vulnerability information, and asset data to enable multi-dimensional situational awareness, helping analysts gain a more comprehensive view of the attack’s background and potential impact range.

At the response level, an AI-enhanced Threat Response function is added. Dataori SIEM deeply integrates SOAR (Security Orchestration, Automation, and Response) capabilities, allowing for the customization of response workflows through a visual interface with automated execution, greatly improving the efficiency of security incident handling. For different attack types, impact magnitudes, and urgency levels, the platform automatically assesses and selects appropriate response strategies; for instance, in the face of DDoS attacks, traffic scrubbing and blacklist blocking measures are initiated automatically, reducing the need for manual intervention. The system also supports integration with security tools such as firewalls, intrusion detection systems (IDS/IPS), and EDR. Once a malicious IP is detected, it is immediately added to the firewall’s blacklist, thereby achieving rapid isolation and joint defense. By integrating threat deception technology, honeypots and honeynets can be deployed within the network to lure attackers into exposing TTPs (tactics, techniques, procedures), enabling the collection of genuine threat intelligence and early identification of potential attacks.

Promoting deep ecological integration and local cooperation, on the basis of localization and AI empowerment, Dataori SIEM further underscores an ecosystem-centric approach, seamlessly integrating with standard domestic SOC (security operation center) and an array of security tool platforms through plug-ins and API interfaces to deliver broader security operation collaboration: first, adopting standardized or modular methods to establish data interoperability with local SOC/SOAR vendors, combining visual analysis and threat intelligence sharing; second, forging close partnerships with domestic managed security service providers (MSSPs), where they share customer needs and log data, propelling the platform’s AI model iteration, allowing small and medium-sized businesses to benefit from advanced threat detection and rapid response; third, delivering flexible, customized configurations and services for industrial control protocols, regulatory compliance demands, or unique protection requirements in finance, government, and energy fields, thereby enhancing product adoption feasibility.

Formulating differentiated strategies and product lifecycle management, Dataori SIEM’s core differentiation lies in the dual benefits of "domestic compatibility + AI intelligence." On one hand, it uses localized adaptation to penetrate policy- and security-driven niches; on the other, it assists customers in enhancing security operation efficiency through advanced features such as intelligent analysis and automated response. This aligns with Porter’s (1985) notion of "differentiated competition," yet to truly capitalize on these advantages, it must sustain its edge through certifications, real-world proof points, and continuous technical upgrades—rather than a one-off promotional push. Referring to product lifecycle theory (Kotler & Keller, 2012), SIEM has reached a mature stage in global markets but remains in an early growth stage domestically, with the competitive landscape still unsettled; if Dataori increases market investment early, builds flagship success cases, and emphasizes brand-building, it can claim a larger share later on; in the mature stage, it must further channel resources into key differentiators like AI engines to guard against competitive pressures.

As for competing products in the global SIEM market, IBM QRadar and Splunk have long held top positions, yet their compatibility with domestic operating systems or CPUs is inadequate, and their pricing is high, making it tough to meet the government’s strict "100% localization" requirement in the near term. Currently, Splunk and IBM QRadar do not list any domestic OS support. By contrast, local companies such as 360, Qi'anxin, and Venustech have a long track record in network and endpoint security, maintain strong ties with government and major SOEs, and have gradually rolled out SIEM solutions, although further AI innovation and a fully localized stack remain needed. If Dataori is unable to quickly build successful cases and bolster brand visibility, it may be placed at a disadvantage in bidding. Nonetheless, in finance, telecom, and energy—sectors with strong compliance needs—the demand for "localized compliance + AI analysis capabilities" grows stronger, suggesting that Dataori’s product positioning is quite appealing, though additional empirical data is needed to validate the outcomes.

Even with the aforementioned product positioning, Dataori SIEM still faces multiple risks and challenges in practical deployment: first, if multi-source and diverse security log data are lacking, the AI model may show missed or false positives, necessitating a continuous iterative training mechanism in conjunction with MSSPs; second, in terms of complexity, SaaS and on-premises deployments each have pros and cons, and the preference for on-premises or private deployments in key industries will elevate operating and hardware costs, making it critical to reconcile compliance and cloud benefits through a hybrid approach; third, in terms of ecological integration, the absence of unified API standards adds technical strain to docking and version upgrades, requiring the joint creation of uniform interface standards with CAICT, the Financial Information Innovation Lab, or leading security vendors, alongside signing technical cooperation deals to improve interface efficiency.

Regarding product strategy, Dataori SIEM forms differentiated competitive barriers and sustainable collaboration. Harnessing in-depth localization and AI analytics (e.g., NLP, GNN, federated learning), it can be first to serve second- and third-tier financial institutions, municipal governments, certain energy SOEs, and other customers prioritizing cost-effectiveness and localization. The firm must invest significant resources—over 30% of its R&D budget—in localization and AI at the value chain level, partner with domestic OS/DB vendors for "joint key-project delivery," and build major-customer endorsements and brand awareness by actively joining government or finance security summits and innovation expositions. Additionally, under product lifecycle theory, with the domestic SIEM market possibly shifting from growth to maturity, Dataori should maintain advanced, AI-related differentiating features in later stages to reinforce its leading position.

To ensure strategic execution and bolster feasibility, Dataori SIEM has devised a phased deployment and metrics-based KPI: in the first phase (6–12 months), it will conduct in-depth compatibility testing with 2–3 domestic OS/DB vendors and pass official certifications, hold quarterly AI model simulations, and select provincial government or local banks for pilot adoption; in the second phase (1–2 years), it will improve API standardization with MSSP and SOAR vendors, accelerate SaaS promotion, and complete over five large-scale customer deployments, seeking a robust TDIR (Threat Detection, Investigation & Response) ecosystem in core industries; in the third phase (3–5 years), it will continuously iterate AI analytics, expand coverage and performance of automated responses, and strive to be among the top five in China's SIEM market. With respect to key indicators, the compatibility requirement is to achieve ≥95% pass rate for essential features on UOS/Kylin OS, an AI average false alarm rate below 5%, annual compound revenue growth above 30%, NPS ≥30, and at least 3–5 government/financial benchmark cases, along with increasing the AI team ratio from 10% to 25%. These benchmarks will serve as the basis for assessing product strategy success.

4.7.2. Price

Pricing Logic and Tiered Strategy: Dataori SIEM platform adopts a three-tier differentiated pricing model—"Basic Edition / Advanced Edition / Enterprise Edition"—to cater to customers of various sizes and scenarios. The Basic Edition (approximately RMB 200,000–500,000 per project) is primarily targeted at small and medium-sized enterprises, providing log collection, basic threat detection, and AI search at a relatively low price. This setup helps customers achieve initial security situational awareness and basic alert handling. The Advanced Edition (approximately RMB 500,000–2,000,000 per project) is geared toward mid-sized companies, featuring more comprehensive AI-enhanced analysis and automated response (SOAR), along with certain customizable integrations like deeper threat correlation or industrial control protocol extensions. Finally, the Enterprise Edition (approximately RMB 2,000,000–3,000,000 per project) is tailored for large enterprises, financial institutions, or those with strong localization requirements. It not only integrates deep AI analysis and automated response, but also provides full localization support—such as compatibility with domestic operating systems or databases—and professional consulting and custom development services. Compared with international vendors like Splunk and IBM QRadar, whose high-end solutions often reach RMB 3–4 million annually, Dataori's Enterprise Edition offers comparable functionality and performance at about a 30% lower cost, primarily due to reduced patent/license fees from localization, lower domestic R&D and operation costs, and a more focused allocation of resources on specific feature points to control total project expenses. Meanwhile, compared with domestic competitors such as 360, QiAnXin, Venustech, and Topsec, Dataori's "localization compatibility + AI value-added" model allows for a certain premium while still maintaining a high performance-to-price ratio. According to the survey, the preferred payment method varies by segment, with financial and government clients favoring the "30/70" split model, paying 30% upfront and 70% upon successful deployment to ensure long-term support and system stability. Mid-sized enterprises tend to prefer flexible hybrid models, combining a lower upfront payment with annual subscription fees for continuous upgrades, while smaller businesses and MSSP customers are more inclined toward annual subscriptions or usage-based pricing. In response to these findings, Dataori will expand its flexible payment options, offering subscription-based pricing for SaaS deployments while maintaining project-based pricing for private deployments, ensuring greater accessibility and alignment with diverse customer needs.

Cost Structure and Profitability Estimation: Dataori's main costs are divided among R&D investment, implementation and operations, as well as channel and marketing. On the R&D side, resources go into localization compatibility, AI engine algorithms, and automated testing; operational costs include SaaS cloud resources, engineering support, and onsite services for local deployments; and channels/marketing involve distributor commissions, tender fees, proofs of concept (POCs), and exhibition costs. Through a differentiated product positioning and moderate pricing, Dataori aims to maintain a 40–50% gross margin—slightly above the domestic security industry's average 30–40%—primarily relying on the premium and value-added services of the Advanced and Enterprise Editions. Balancing investments between

SaaS operations and large, one-off local deployment projects is also crucial to long-term profitability.

Different Customers and Budget Sensitivity: For small and medium-sized enterprises, Dataori recommends either the Basic Edition or a SaaS subscription—generally within RMB 200,000–500,000—and uses AI search to meet core detection needs. These customers tend to focus on cost-effectiveness and quick deployment, making monthly or annual subscription modes attractive. Mid-sized companies often gravitate toward the Advanced Edition (RMB 500,000–2,000,000), which can incorporate additional services such as industrial protocol parsing, NLP-assisted investigation, or custom reporting, thereby meeting higher security demands and providing room for incremental revenue via value-added services. Large enterprises, financial institutions, or key industries typically require the Enterprise Edition (RMB 2,000,000–3,000,000) to address more stringent compliance and data scale needs, featuring deeper AI analysis, fully localized integration, and specialized consulting. Such projects also generate significant contract values and branding effects for Dataori.

Bidding Model and Dynamic Adjustments: In government and financial tenders, there is usually a set budget cap and strict scoring criteria. With similar functionality yet 20–30% lower pricing than international competitors, Dataori can effectively increase its likelihood of winning bids. To accommodate evolving client demands, the company may set a 10–20% flexible component in project pricing tied to detection performance or AI training outcomes, adjusting quotes in response to real usage data and operational feedback. This approach helps balance compliance, competitiveness, and client interests, though it requires well-defined execution and auditing processes in contracts.

Pricing Implementation KPIs: In the short term (6–12 months), Dataori plans to refine the respective pricing ranges and feature sets for each edition and conduct cost and margin assessments in one or two pilot projects, thus ensuring offers that remain both competitive and profitable when bidding. Meanwhile, it will collaborate with domestic OS/DB vendors to release integration white papers to demonstrate that “with equivalent functionality, costs are more controllable.” In the medium term (1–2 years), Dataori will further improve its SaaS subscription framework—e.g., by charging based on log volume/EPS/node counts—and conduct joint marketing with MSSPs and other local ecosystem partners. It will also regularly track key performance metrics such as renewal rates, gross margins, and successful bids, fine-tuning its pricing model accordingly and aiming to complete 5–8 large-scale enterprise deployments (e.g. in finance/energy/government) for demonstrative effect. Over the long term (3–5 years), as the market matures and client needs evolve, Dataori will continue expanding the Enterprise Edition’s AI capabilities (e.g. TDIR, Zero Trust), recalibrating its pricing and value-added modules in response to market feedback to ensure annual compound revenue growth surpasses 30%, increasing market share in key domains, and stabilizing gross margins in the 40–50% range.

4.7.3. Place

In order to achieve more comprehensive and efficient coverage in the Chinese market and highlight the value of "localization + AI" products, Dataori adopts four models of direct sales, agents, MSSP (managed security service providers) and large-scale enterprise co-research and co-sales in its channel strategy, so as to achieve effective reach of different market segments and customer types and establish a more coordinated and competitive distribution network. However, in order to avoid the internal friction and conflicts that may be caused by multi-channel parallel operation, Dataori will further refine the target positioning, functional division and control mechanism in the design of the channel system, and make a layered layout based on the customer procurement process and market research data. 1. Direct sales: focus on key industry customers and deepen technical empowerment The direct sales team mainly provides solution consultation and sales support to high-end customer groups such as state-owned banks, headquarters of central enterprises, and government agencies, shortens the decision-making chain and ensures the accurate implementation of technical solutions. The direct sales model is more suitable for industry scenarios with highly customized security needs and strict localization compliance requirements. On the one hand, through one-on-one technical demonstrations and solution docking, Dataori can fully demonstrate the differentiated advantages of "localization + AI" and quickly respond to complex bidding processes. On the other hand, Dataori will introduce more sophisticated project management and after-sales delivery measures in the direct sales link to reduce customers' concerns about product stability and operation and maintenance services. To prevent conflicts with other channels, the direct sales team is mainly responsible for large projects at the headquarters level or above the provincial level, as well as customized projects with extremely complex requirements; regional or small and medium-sized requirements are followed up by agents or MSSPs.

Channel agents: hierarchical authorization to avoid overlapping conflicts In the field of regional markets or small and medium-sized customers, Dataori cooperates with core agents to improve market coverage and response speed through regional authorization or industry authorization. To prevent excessive competition between agents in the same region, Dataori will set up relatively clear regional divisions and industry franchises based on market capacity and customer characteristics; for the selection of agents, priority will be given to enterprises with a background in cooperation with the ITAI ecosystem or the ability to deepen traditional security products, so as to complement each other in marketing promotion and after-sales service. At the same time, Dataori has established a channel control mechanism, including a unified price policy, a bidding conflict handling process, and after-sales service quality assessment, to reduce mutual squeeze between channels, and strengthen the technical capabilities of agents and their awareness of Dataori products through regular training and joint marketing activities.

MSSP hosting: Lowering the threshold for security operation and maintenance for small and medium-sized enterprises The MSSP (hosted security service provider) model can provide 7×24 hours of remote security monitoring, threat intelligence sharing and incident response services for small and medium-sized enterprises with relatively weak technical and financial strength. Dataori and professional MSSPs have established joint solutions: Dataori provides SIEM software and AI detection models, and MSSPs are responsible for customers' daily security operations and maintenance. In this way, small and medium-sized enterprises do not have to build a large security operation and maintenance team or bear high software and hardware costs, and can also enjoy a higher level of threat detection and response capabilities. In order to ensure the interest separation between the MSSP channel and the agency channel, Dataori will guide them to the appropriate service model according to the size of the customer and the complexity of their needs. If the customer grows into a large customer in the later stage, it can be upgraded to a direct sales or enterprise customized solution to avoid poor coordination due to channel overlap.

Co-research and co-sales with large enterprises: Establish a joint brand and ecosystem For some central enterprises or large state-owned enterprises, Dataori adopts the "co-research and co-sales" model, jointly investing in product development and market promotion to create deeply customized SIEM and even a wider range of security operation solutions (such as integrated private cloud deployment, domestic operating system compatibility, etc.). Under this model, large enterprises can use their own perfect industry sales network to distribute Dataori solutions, which in turn enhances Dataori's brand influence and market share in the enterprise market. Regarding the ownership of intellectual property rights and technological achievements in the co-research process, Dataori has established a clear cooperation agreement and management system to ensure that key competitiveness such as product core algorithms and localized adaptation can still be retained in its own value chain. This model can not only quickly accumulate benchmark cases, but also help to form an ecosystem partnership, and continue to conduct joint research and development and external sales for subsequent upgraded functions or new products (such as TDIR, Zero Trust).

Control Mechanism and Conflict Resolution Multi-channel operation is prone to cross-competition in terms of region or customer type. Dataori has set up clear permissions and incentive policies for channel management: Unified prices and discounts: Through a systematic quotation strategy, ensure that there is no serious mismatch between the quotations of direct sales and agents. Project registration and exclusivity: Agents need to register potential projects in the enterprise CRM system. If they have been assigned to direct sales or other agents, Dataori must distinguish project-level permissions to prevent vicious competition. Performance evaluation and training: Regular performance evaluation, technical training and sales coaching are conducted for agents and MSSPs; for joint research projects with large enterprises, progress and input-output ratio are measured through phased acceptance. Customer stratification strategy: It is clear that direct sales will give priority to super-large or national customers; if a conflict occurs, the dominant channel will be determined based on the criterion of "who registered first and who has higher delivery capabilities".

4.7.4. Promotion

As an emerging domestic SIEM vendor, Dataori faces intense competition from both domestic and international players, as well as diverse customer needs. To stand out, Dataori must devise a systematic, actionable promotion strategy. Grounded in the procurement characteristics of the security software industry, this paper integrates academic perspectives with practical logic, follows the “positioning–planning–execution–evaluation” framework, and provides a detailed discussion of Dataori SIEM’s promotion strategies, aiming to enhance brand influence and drive market performance.

Procurement decisions in the security software industry are complex and diverse, with major differences in processes and key concerns across varying organizational sizes. Consequently, Dataori’s promotion strategies must be segmented by customer type, and a quantifiable promotion framework constructed around the classic AIDA model (Attention–Interest–Desire–Action). For large clients (e.g., state-owned/central enterprises), the procurement process is lengthy, requiring multi-level approval, compliance reviews, and budget planning; decision makers focus on product compliance, reliability, and long-term ROI. By contrast, small to medium-sized enterprises make decisions more quickly, prioritizing swift deployment, user-friendliness, and cost-effectiveness. Dataori’s promotion plan specifically includes: heightening brand awareness via industry summits and digital advertising (targeting 50,000 monthly brand exposures); fueling customer interest through technical white papers and online seminars (targeting 500 monthly technical document downloads); encouraging product experience through free trials and POC (proof of concept) offers (targeting 50 trial requests per month); and closing deals via sales follow-up and special offers (aiming for a 20% trial-to-purchase conversion rate).

Dataori categorizes its target customers into three groups: technology practitioners, SME owners, and core decision makers, each with distinct concerns and channels for information. For technology practitioners (e.g., CISOs and SecOps teams), emphasis lies on technological innovation, performance metrics, and real-world security outcomes. Accordingly, Dataori can publish technical articles in professional communities like CSDN and security forums, underscoring how “AI-driven threat detection” can cut false-positive rates below 5%, and sharing video demos of “localized adaptation” that reduce deployment time by 40%. For SME owners or security managers, who value rapid rollout, low O&M costs, and high cost-effectiveness, Dataori can create concise product intro videos via official WeChat accounts, Zhihu, Bilibili, etc., highlighting “30-minute deployment” and “20% lower O&M costs” compared to competitors. Meanwhile, for core decision makers (e.g., state-owned enterprise leaders, financial institution executives), who focus on compliance, ROI, and brand reliability, Dataori can leverage key industry summits and closed-door forums to illustrate “domestic certifications and compliance benefits,” and release a white paper detailing an ROI calculation model. To differentiate media strategies, Dataori can collaborate with industry KOLs on Zhihu for in-depth product reviews and produce a two-minute Bilibili video spotlighting streamlined deployment, thus visually distinguishing itself from competitors.

Industry summits and expos are integral to Dataori’s promotional activities, requiring clear prioritization and evaluation. At major security conferences (like Cybersecurity Conference and ITAI Conference), Dataori’s goal is direct competition with peers and showcasing “AI + localization” as its technical edge. Plans include interactive sessions (on-site AI threat detection demos, collecting customer pain points). Evaluation metrics include attendee count, retention rate (target 50%), and POC application rate (target 20%). For Dataori’s self-hosted “China Intelligent Security Operation Summit” themed “AI-driven Intelligent Security Operation,” the agenda features morning trend insights from industry experts, afternoon SIEM demos, and evening roundtables with key experts and flagship customers. Key performance indicators include total attendees (target 200), retention rate (target 50%), and trial application rate (target 20%). Afterward, Dataori will compile white papers and event videos for continued promotion on the official website and social media. To gauge effectiveness, Dataori will implement a CRM system to track lead conversions, periodically analyzing ROI and ensuring that promotional outcomes remain quantifiable.

Additionally, Dataori plans to form a systematic UseCase repository and tailor promotions to multiple industries via online seminars. Building and managing the repository involves collecting and labeling new cases through customer interviews and after-sales data, categorizing them by industry (e.g., finance, energy), threat types (e.g., ransomware, data leakage), and company size, and updating quarterly to ensure relevance. The online seminar component includes selecting topics such as “Best SIEM Practices in Finance,” inviting both flagship customers and internal technical experts, promoting it via WeChat group messages and email marketing (target 100 participants), and capturing feedback to refine future seminars.

Free trials and digital marketing are crucial for attracting customers, but boundaries must be defined to reduce risks and improve effectiveness. The free trial plan provides basic AI-driven threat detection features over a 30-day period with a 100GB data limit, restricting advanced functionality to paid tiers and limiting technical support to basic issues. A formal trial agreement specifies data security and support scope, preventing resource overconsumption. Digital marketing efforts concentrate on using WeChat ads for SMEs and Baidu SEM for technical keyword searches (e.g., “SIEM localization”), initially allocating 20% of the budget for testing, followed by 80% for subsequent optimization, while iterating based on click-through, registration, and trial conversion rates.

Finally, these promotional activities align with Dataori’s product positioning and channel system to deliver differentiated support for various channels. For direct sales, Dataori offers exclusive summit exposures and executive dialogues for high-end clients; for agents, it provides training and standardized marketing tools (e.g., case repositories, white papers) to ensure consistent messaging; for MSSPs, Dataori underscores “the feasibility and added value of managed services” and presents supporting data and success examples. The synergy lies in highlighting AI innovation through technical communities, underlining domestic compliance at summits, and maintaining promotional consistency with Dataori’s overall product positioning.

Dataori’s approach to promotion is underpinned by the AIDA model, IMC (integrated marketing communication) theory, and STP (segmentation, targeting, positioning). In practice, AIDA translates into capturing awareness via summits and digital ads, stimulating interest via technical resources and references, inspiring purchase desire through hands-on trials, and finalizing purchases via sales nurturing. Under IMC, online and offline channels are integrated to unify brand messaging and values, avoiding fragmented user experiences. Meanwhile, the STP model is applied by segmenting large vs. SME customers, positioning Dataori as a specialized security provider focusing on “AI + localization,” stressing compliance for larger clients and cost-performance for smaller ones.

4.8. Implementation

4.8.1. Schedule

A five-year plan was developed to ensure market penetration, compliance certification, channel expansion, and continuous improvement of the product. The following table outlines the key tasks and deliverables for each phase:

Table 4.3- 5 years implementation plan task list

Year	Key Tasks	Main Activities	Deliverables
Year 1	Market Research and	- Conduct SIEM industry analysis to assess Chinese market demand and regulatory requirements.	- Market analysis report

	Product Adaptation	- Study domestic and international competitors to refine product differentiation strategy.	- Competitor analysis
		- Complete ITAI certification and local compliance requirements assessment.	- Product compliance adaptation plan
		- Conduct user demand research to develop customized feature planning.	
Year 2	Product Improvementand Pilot Deployment	- Integrate AI security analysis to enhance localized intelligent threat detection capabilities.	- Pilot test feedback report
		- Conduct pilot deployments in government and financial institutions to collect real-world operational data.	- MSSP partnership agreements
		- Establish local partnerships (MSSPs, cloud service providers).	- Compliance certification documents
		- Apply for government and industry security certifications to enter procurement directories.	
Year 3	Market Expansion and Sales Network Development	- Participate in government procurement expos to expand industry influence.	- Market expansion strategy report
		- Increase brand awareness through online and offline promotions (exhibitions, seminars, digital marketing).	- Brand exposure data
		- Establish a nationwide sales and technical support network to improve customer acquisition and retention.	- National sales and service network
		- Enhance market acceptance through user training and implementation support.	
Year 4	Comprehensive Market Expansion and	- Expand into key sectors, including government, finance, energy, and manufacturing.	- Industry market penetration report

	Business Growth	- Improve SaaS model to meet SME demands and enhance profitability.	- SaaS user growth data
		- Expand localized security data lake to improve log storage costs and analysis efficiency.	- Security data lake improvementplan
		- Monitor market feedback and improve product features accordingly.	
Year 5	Continuous Improvementand Global Expansion	- Upgrade AI-driven security operations to enhance competitiveness in line with industry trends.	- Technology innovation white paper
		- Collaborate with the local IT ecosystem to drive joint innovation with domestic technology companies.	- Global market analysis report
		- Study feasibility of international expansion and formulate a global market entry strategy.	- New five-year growth str
		- Evaluate market objectives and develop a new five-year growth plan.	

Source: Author (2025)

4.8.2. Budget

Dataori's five-year budget plan for localizing SIEM products covers marketing, product development, channel expansion, and brand building. The plan ensures efficient allocation of resources and maximizes return on investment (ROI)

The budget is presented in RMB (Chinese Yuan) and EUR (Euros), assuming an exchange rate of 1 EUR = 7.8 RMB, with adjustments based on market fluctuations.

Table 4.4 - 5 years budget plan

Budget Category	**Year 1**	**Year 2**	**Year 3**	**Year 4**	**Year 5**	**Total (RMB)**	**Total (EUR)**	**Percentage**
Market Promotion	¥3,000,000 (€384,600)	¥3,500,000 (€448,700)	¥4,000,000 (€512,800)	¥4,500,000 (€576,900)	¥5,000,000 (€641,000)	¥20,000,000	€ 2,564,000	30%
Product Development	¥5,000,000 (€641,000)	¥6,000,000 (€769,200)	¥6,500,000 (€833,300)	¥7,000,000 (€897,400)	¥7,500,000 (€961,500)	¥32,000,000	€ 4,102,600	48%

Channel Expansion	¥2,000,000 (€256,400)	¥2,500,000 (€320,500)	¥3,000,000 (€384,600)	¥3,500,000 (€448,700)	¥4,000,000 (€512,800)	¥15,000,000	€ 1,923,000	22%
Brand Building	¥1,500,000 (€192,300)	¥1,800,000 (€230,800)	¥2,000,000 (€256,400)	¥2,200,000 (€282,000)	¥2,500,000 (€320,500)	¥10,000,000	€ 1,282,000	15%
Monitoring & Improvement	¥500,000 (€64,100)	¥800,000 (€102,600)	¥1,000,000 (€128,200)	¥1,200,000 (€153,800)	¥1,500,000 (€192,300)	¥5,000,000	€ 641,000	7%
Total	**¥12,000,000 (€1,538,500)**	**¥14,600,000 (€1,871,800)**	**¥16,500,000 (€2,115,400)**	**¥18,400,000 (€2,358,900)**	**¥20,500,000 (€2,628,200)**	**¥82,000,000**	**€ 10,512,800**	**100%**

Source: Author (2025)

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 4.5 - KPI-driven monitoring

Monitoring Dimension	**Key Performance Indicators (KPI)**	**Measurement Method**	**Evaluation Frequency**
Market Promotion	Growth in brand exposure (social media, short videos, forum visits)	Active user tracking, traffic analysis, follower growth	Quarterly
	Ad conversion rate (click-through rate, trial conversion rate)	Marketing analytics	Quarterly
	Number of customers attending conferences and exhibitions	Event registration data	Quarterly
Product Development	AI Copilot adoption rate	Client activation rate, feature usage data	Semi-Annually
	Growth in SaaS SIEM subscriptions	Paid subscription data	Quarterly

	Average security incident response time (SOC improvement)	Security event analysis	Semi-Annually
Channel Expansion	Number of MSSP partner agreements	Signed partnership contracts	Semi-Annually
	Sales growth from channel partners	Sales reports from partners	Quarterly
	Government procurement revenue	Contract value in government tenders	Annually
Brand Building	AI SIEM community active users	Registered users, engagement level	Semi-Annually
	Number of industry whitepaper downloads	Official website download data	Quarterly
	Customer satisfaction score (NPS - Net Promoter Score)	NPS survey analysis	Annually
Financial Performance	Annual revenue growth	Financial reports	Annually
	Reduction in Customer Acquisition Cost (CAC)	Sales/marketing expense ratio	Annually

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 4.6 - Assessment Mechanism list

Assessment Method	**Evaluation Criteria**	**Evaluation Frequency**	**Responsible Team**
Market Promotion Assessment	Assess advertising ROI, improve social media strategies	Quarterly	Marketing Team
Product Feedback Analysis	Analyze user feedback to enhance AI Copilot & SaaS product features	Semi-Annually	R&D Team

Channel Growth Monitoring	Evaluate MSSP and IT channel sales performance	Semi-Annually	Channel Expansion Team
Brand Influence Analysis	Track industry whitepaper downloads and forum discussions	Semi-Annually	Brand Operations Team
Customer Satisfaction Survey	Measure NPS score for user experience evaluation	Annually	Customer Support Team
Financial Performance Review	Calculate CAC, LTV (Lifetime Value) metrics	Annually	Finance Team

Source: Author (2025)

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

Software product adaptation is a complex and ongoing systematic process that requires continuous tracking of technological trends, in-depth analysis of user needs, and designing flexible and efficient functionalities based on these evolving factors. This ensures that the software product maintains strong adaptability across different environments and delivers an excellent user experience, ultimately securing its competitive edge in the market.

Dataori SIEM’s success in the Chinese market is built upon its robust localization adaptability, technological innovation, industry-proven applications, and extensive channel expansion resources, forming a clear and scalable revenue path. By securing stable cash flow in the short term, expanding market share in the mid-term, and achieving data monetization and value-added services in the long term, Dataori aims to establish a strong competitive moat in the SIEM sector. Its key strengths include full compatibility with domestic operating systems (Kylin, UnionTech) and databases (Dameng, Kingbase), which align with government procurement requirements. The platform is also equipped with AI-powered SIEM capabilities that provide threat intelligence, automated response mechanisms, and improved false-positive reduction, enhancing overall detection efficiency. Additionally, Dataori has successfully implemented a SaaS-based SIEM solution in one of China’s six largest banks, reinforcing its credibility and market acceptance. Leveraging Managed Security Service Provider (MSSP) partnerships, Dataori can rapidly extend its market influence and reach a broader audience. It also offers deeply improved SIEM solutions for key industries such as finance, energy, and government sectors, ensuring tailored security compliance. By obtaining MLPS 2.0 (Multi-Level Protection Scheme) certification and securing government procurement qualifications, Dataori strengthens its access to public sector and state-owned enterprise markets. These strategic advantages enable Dataori to formulate targeted monetization strategies at different market stages, ensuring sustained competitiveness and revenue growth.

In the short term, Dataori’s primary objective is to establish a stable cash flow foundation, which is essential for business expansion. Achieving this requires a dual approach of enterprise licensing sales and government procurement. First, by targeting high-demand industries such as banking, energy, and government agencies, Dataori employs a one-time licensing fee plus an annual maintenance model. A “trial-first, purchase-later” approach helps lower the adoption barrier for enterprises and improves the conversion rate. The annual maintenance fee for enterprise clients constitutes 15%-20% of the licensing cost, providing a recurring revenue stream. Simultaneously, securing inclusion in government procurement directories ensures long-term contract stability. Additionally, obtaining certification for trusted innovation strengthens Dataori’s positioning and access to lucrative government projects. To further enhance market penetration, Dataori offers tailored short-term consulting services, such as specialized security analysis and custom risk assessment reports, increasing the attractiveness of its offering. These tactics position Dataori to secure early-stage revenue streams despite intense market competition, laying the groundwork for future business expansion.

Once the market foothold is established, Dataori needs to leverage a SaaS subscription model and expand its channel partnerships to drive growth. The SaaS model capitalizes on its successful implementation in one of China’s six largest banks, boosting credibility and market acceptance. The company will offer tiered subscription plans, including Basic, Professional, and Enterprise editions, structured around an annual payment model to drive Annual Recurring Revenue (ARR) growth. The adoption of a progressive SaaS strategy allows businesses to start with fundamental functionalities and upgrade to premium features as their security needs evolve, improving customer retention and renewal rates. Simultaneously, through MSSP partnerships, Dataori can create long-term distribution channels, where MSSPs resell SIEM solutions in bulk. By implementing a combination of bulk licensing agreements and event-based usage billing, MSSPs are incentivized to scale their client base, accelerating Dataori’s market expansion. Additionally, Dataori can deepen its integration with domestic cloud providers and IT infrastructure providers, enabling broader industry adoption and enhancing its SaaS product’s reach, ensuring sustained subscription revenue growth and increasing its brand influence.

In the long run, Dataori must leverage AI-driven security analytics and data monetization to build a high-margin business model and achieve sustainable growth. AI-powered value-added services include premium threat intelligence subscription offerings that provide enterprises with predictive security insights. The introduction of automated compliance auditing enhances corporate regulatory adherence while reducing manual review costs. Furthermore, Dataori plans to develop an open API for its AI engine, allowing third-party developers and security operations centers to integrate Dataori’s SIEM capabilities, further expanding its market penetration. Additionally, verticalized industry-specific solutions, tailored for financial, healthcare, and energy sectors, will be developed in conjunction with domestic IT infrastructure, ensuring compliance and enhancing procurement attractiveness for government and enterprise clients. As Dataori’s data repositories grow, the company can further explore large-scale security intelligence analytics, offering real-time threat intelligence and industry-wide security posture analysis for external enterprises and governmental bodies. This shift toward data-driven monetization will introduce additional high-value revenue streams, ensuring long-term profitability.

Dataori must implement a phased execution strategy to improve revenue expansion while sustaining profitability. In the short term (1-2 years), the focus is on cash flow stability—

securing 5-10 major enterprise contracts, gaining entry into government procurement programs, and securing 2-3 high-value projects through licensing sales and maintenance fees to ensure sufficient early-stage capital. In the mid-term (3-5 years), the emphasis shifts toward channel expansion, establishing partnerships with 20+ MSSPs, scaling national market penetration, and increasing SaaS subscription revenues, targeting an ARR contribution exceeding 50%. Simultaneously, Dataori will deepen collaboration with domestic cloud, server, and database providers to enhance its market position. In the long term (5+ years), the primary focus will be data monetization and high-value AI analytics services. Establishing an SIEM + AI security intelligence platform, launching AI-driven risk prediction tools, developing a global threat intelligence network, and expanding API-driven revenue streams will solidify Dataori's industry leadership. The company's monetization strategy is built upon localization adaptability, technological innovation, validated SaaS implementations, government market penetration, and strategic channel partnerships—ensuring a structured transition from early-stage cash flow stability to large-scale revenue growth and ecosystem-driven monetization.

This research has several limitations. First, the sample size of the questionnaire (42 respondents) is relatively small, which may limit the generalizability of findings. Second, the qualitative nature of expert interviews might introduce subjective biases. Third, due to resource constraints, this thesis primarily focuses on financial institutions; thus, findings may not fully represent other industries such as government、telecommunications or energy.

Future research should focus on actionable strategies that align with policy-driven localization and market-specific needs in China's SIEM sector. First, studies could explore the impact of government procurement policies, such as SASAC Document No. 79, on domestic SIEM adoption rates and how localized compliance certifications influence buyer trust. This would provide insights into optimizing regulatory alignment for market penetration. Second, research could investigate effective channel strategies for expanding market reach, including partnerships with Managed Security Service Providers (MSSPs) and regional distributors to enhance coverage in underserved areas. Third, future work could examine the role of culturally tailored marketing approaches, such as leveraging local platforms like WeChat for targeted campaigns or co-branding initiatives with trusted domestic IT vendors, to improve brand recognition and customer engagement. Lastly, longitudinal studies on customer behavior in key industries like finance and government could reveal how procurement priorities evolve under ITAI policies, enabling more precise targeting of localized solutions. These directions would offer practical guidance for businesses navigating China's policy-driven and competitive cybersecurity landscape.

Bibliographical References

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

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.

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

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

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

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.

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

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

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

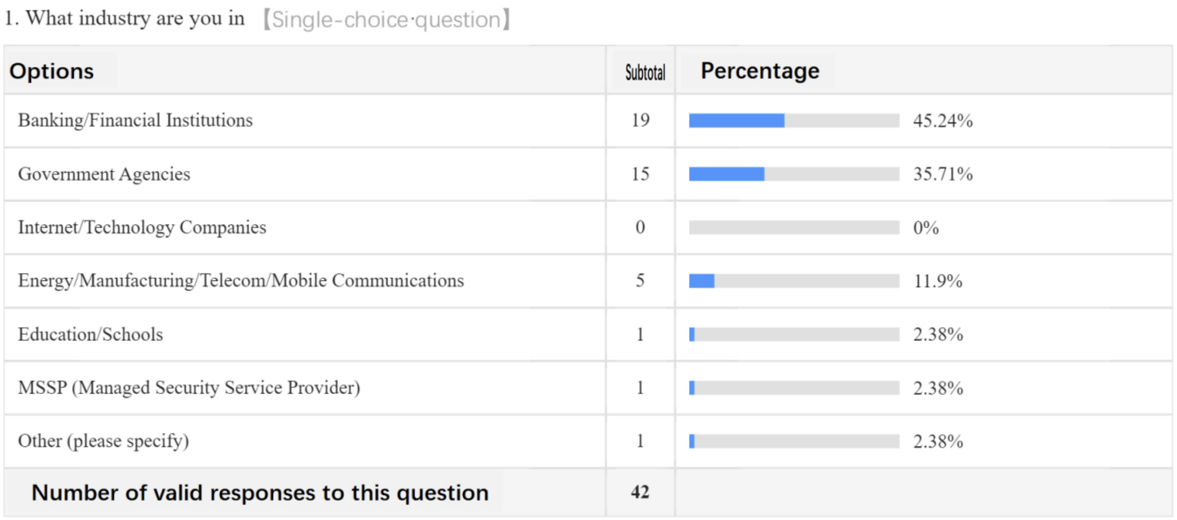
22. Does your company plan to switch from international vendors to domestic SIEM solutions in the next 3 years?

☐Yes

☐No

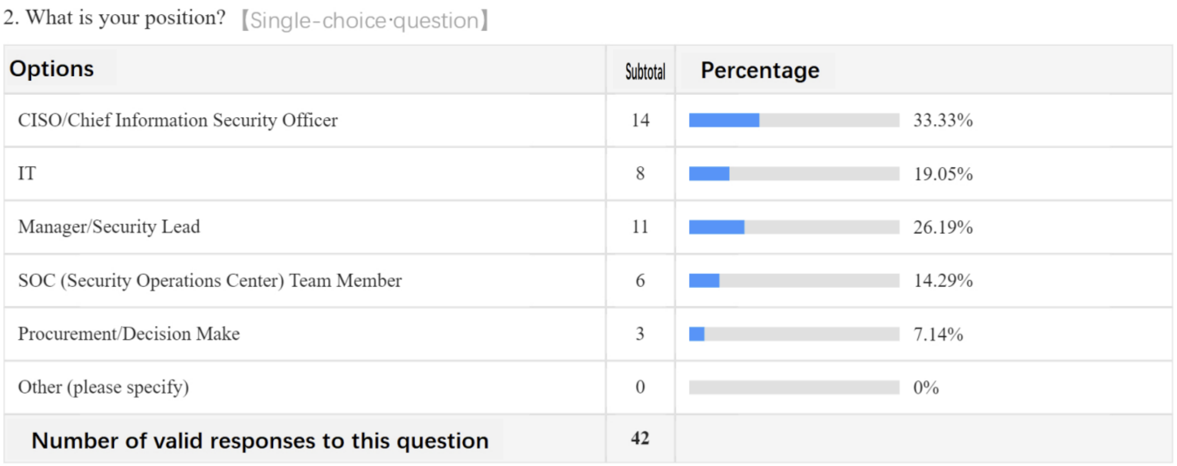
☐Depends on market development

Appendix B – Questionnaire Findings Overview



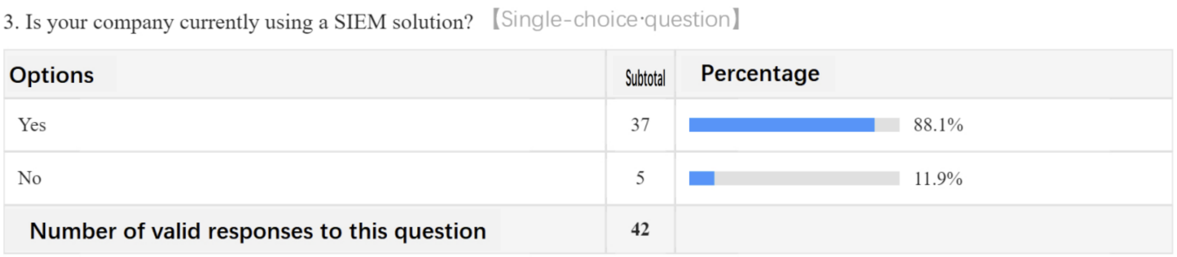
1. What industry are you in 【Single-choice·question】

Options	Subtotal	Percentage
Banking/Financial Institutions	19	45.24%
Government Agencies	15	35.71%
Internet/Technology Companies	0	0%
Energy/Manufacturing/Telecom/Mobile Communications	5	11.9%
Education/Schools	1	2.38%
MSSP (Managed Security Service Provider)	1	2.38%
Other (please specify)	1	2.38%
Number of valid responses to this question	42	



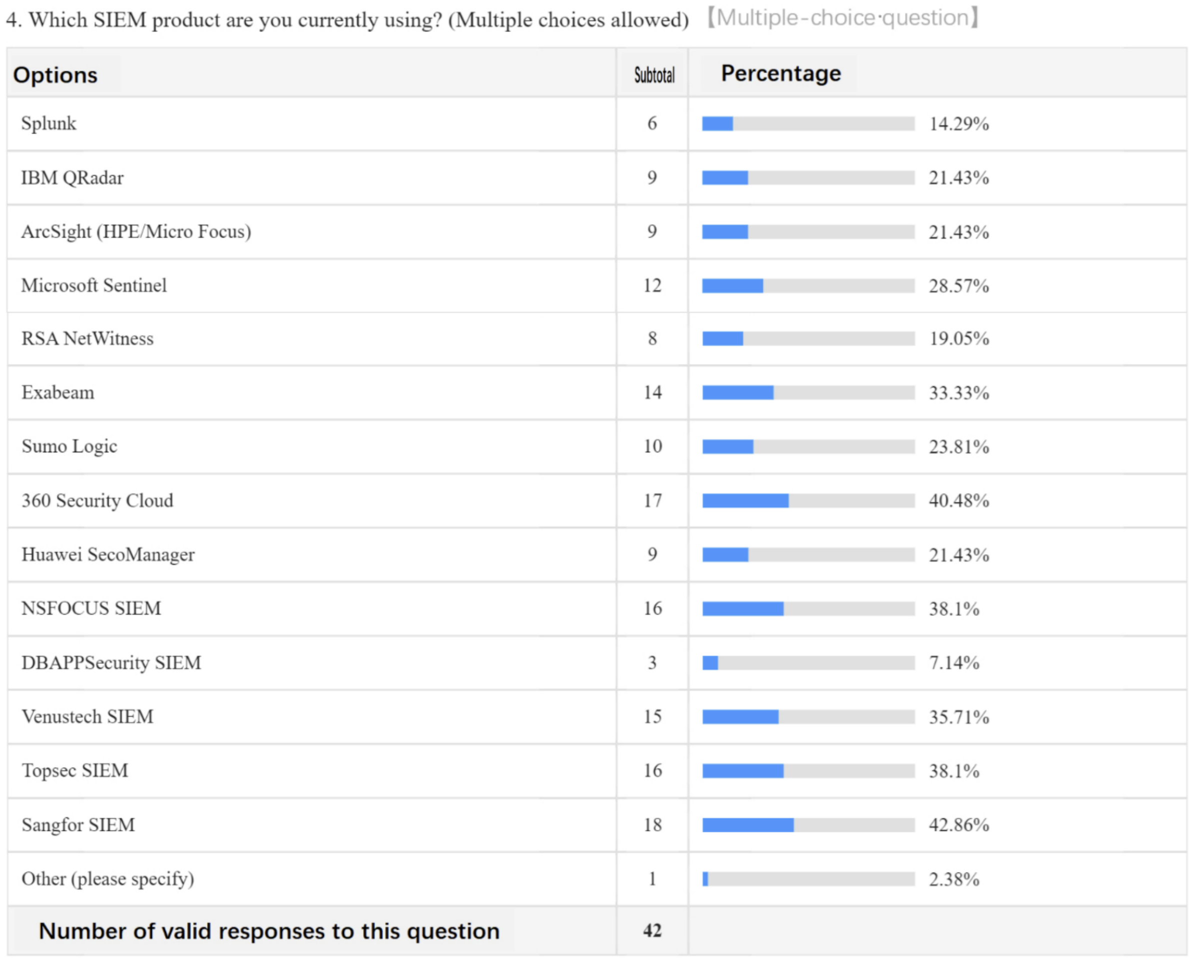
2. What is your position? 【Single-choice·question】

Options	Subtotal	Percentage
CISO/Chief Information Security Officer	14	33.33%
IT	8	19.05%
Manager/Security Lead	11	26.19%
SOC (Security Operations Center) Team Member	6	14.29%
Procurement/Decision Make	3	7.14%
Other (please specify)	0	0%
Number of valid responses to this question	42	



3. Is your company currently using a SIEM solution? 【Single-choice·question】

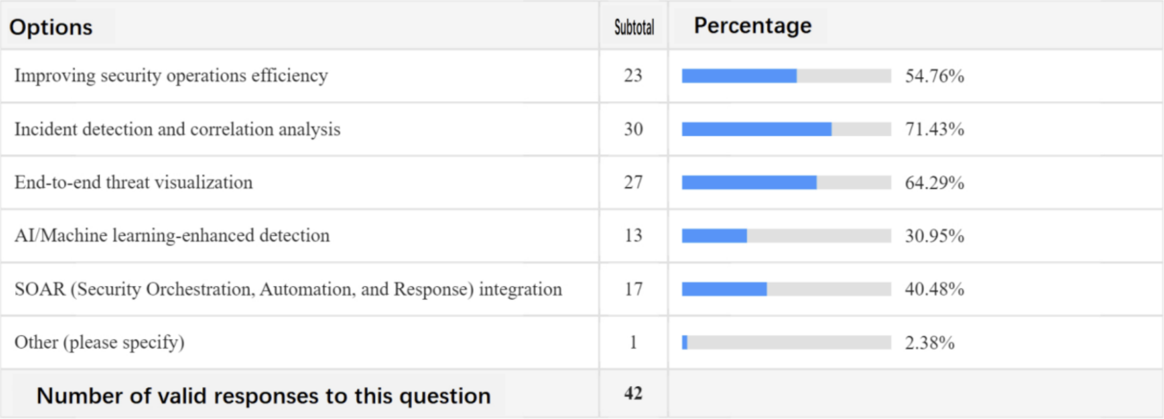
Options	Subtotal	Percentage
Yes	37	88.1%
No	5	11.9%
Number of valid responses to this question	42	



4. Which SIEM product are you currently using? (Multiple choices allowed) 【Multiple-choice·question】

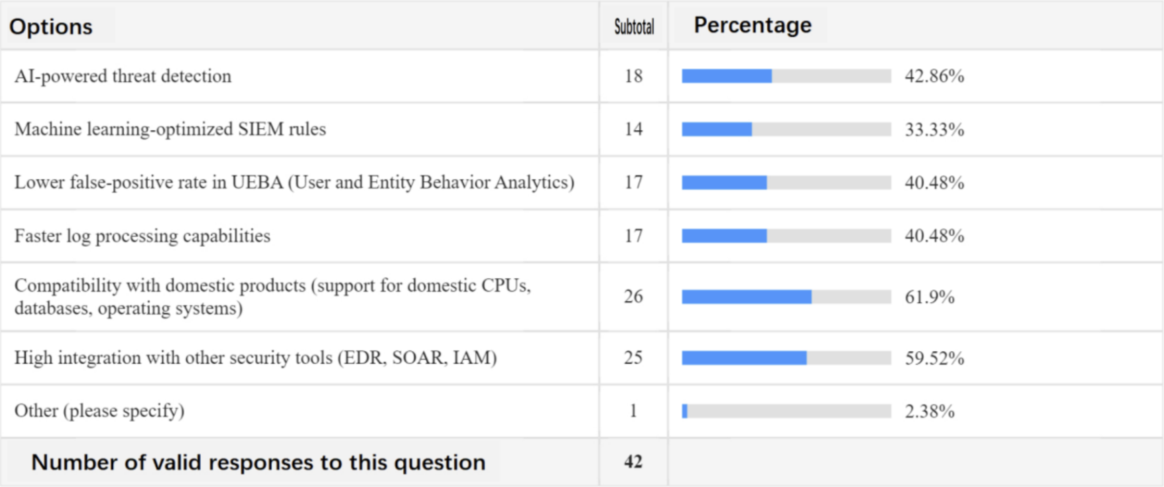
Options	Subtotal	Percentage
Splunk	6	14.29%
IBM QRadar	9	21.43%
ArcSight (HPE/Micro Focus)	9	21.43%
Microsoft Sentinel	12	28.57%
RSA NetWitness	8	19.05%
Exabeam	14	33.33%
Sumo Logic	10	23.81%
360 Security Cloud	17	40.48%
Huawei SecoManager	9	21.43%
NSFOCUS SIEM	16	38.1%
DBAPPSecurity SIEM	3	7.14%
Venustech SIEM	15	35.71%
Topsec SIEM	16	38.1%
Sangfor SIEM	18	42.86%
Other (please specify)	1	2.38%
Number of valid responses to this question	**42**	

5. What is the primary purpose of your company using SIEM? (Multiple choices allowed) 【Multiple-choice·question】

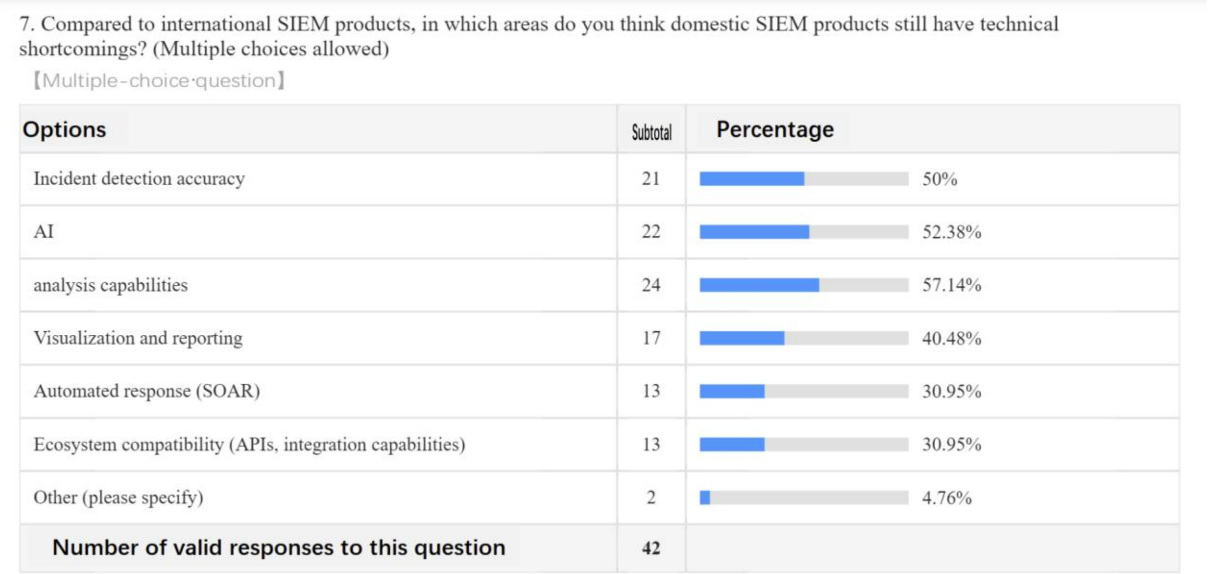


Options	Subtotal	Percentage
Improving security operations efficiency	23	54.76%
Incident detection and correlation analysis	30	71.43%
End-to-end threat visualization	27	64.29%
AI/Machine learning-enhanced detection	13	30.95%
SOAR (Security Orchestration, Automation, and Response) integration	17	40.48%
Other (please specify)	1	2.38%
Number of valid responses to this question	42	

6. What product features are most important to your company during SIEM selection? (Multiple choices allowed))
【Multiple-choice·question】

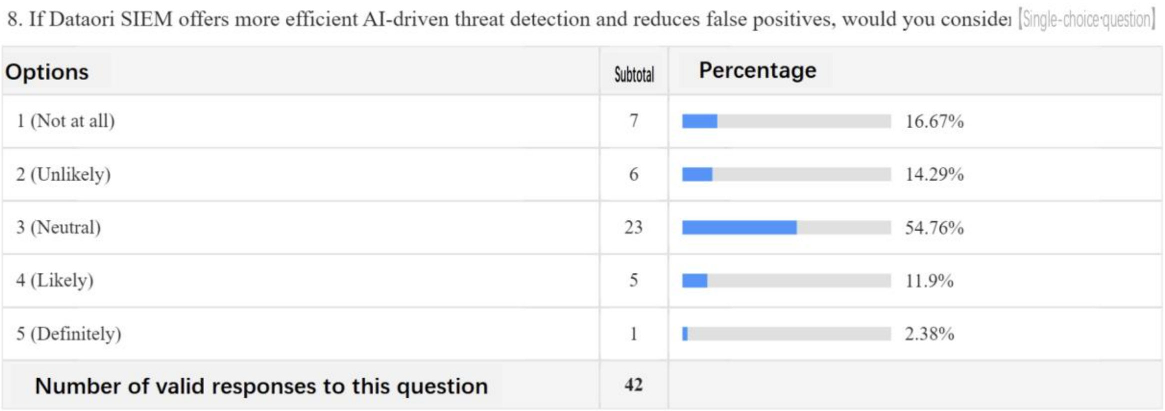


Options	Subtotal	Percentage
AI-powered threat detection	18	42.86%
Machine learning-optimized SIEM rules	14	33.33%
Lower false-positive rate in UEBA (User and Entity Behavior Analytics)	17	40.48%
Faster log processing capabilities	17	40.48%
Compatibility with domestic products (support for domestic CPUs, databases, operating systems)	26	61.9%
High integration with other security tools (EDR, SOAR, IAM)	25	59.52%
Other (please specify)	1	2.38%
Number of valid responses to this question	42	



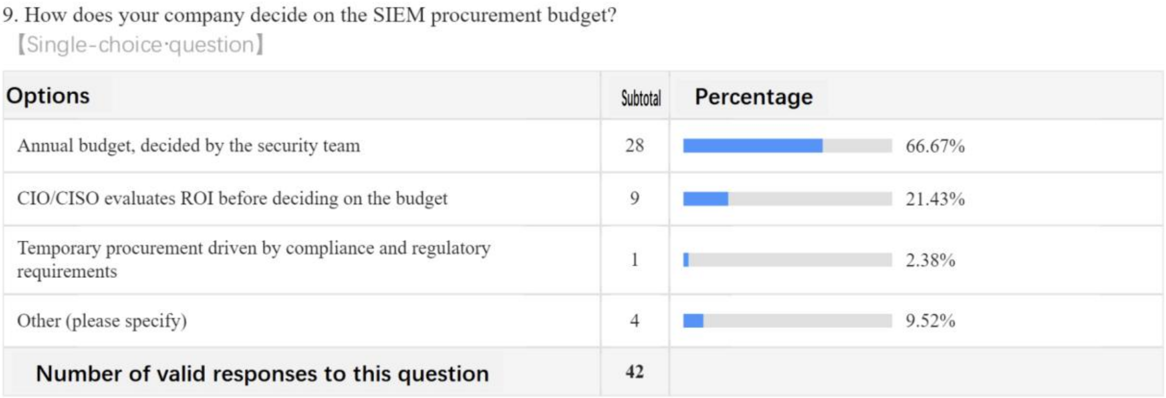
7. Compared to international SIEM products, in which areas do you think domestic SIEM products still have technical shortcomings? (Multiple choices allowed)
【Multiple-choice·question】

Options	Subtotal	Percentage
Incident detection accuracy	21	50%
AI	22	52.38%
analysis capabilities	24	57.14%
Visualization and reporting	17	40.48%
Automated response (SOAR)	13	30.95%
Ecosystem compatibility (APIs, integration capabilities)	13	30.95%
Other (please specify)	2	4.76%
Number of valid responses to this question	**42**	



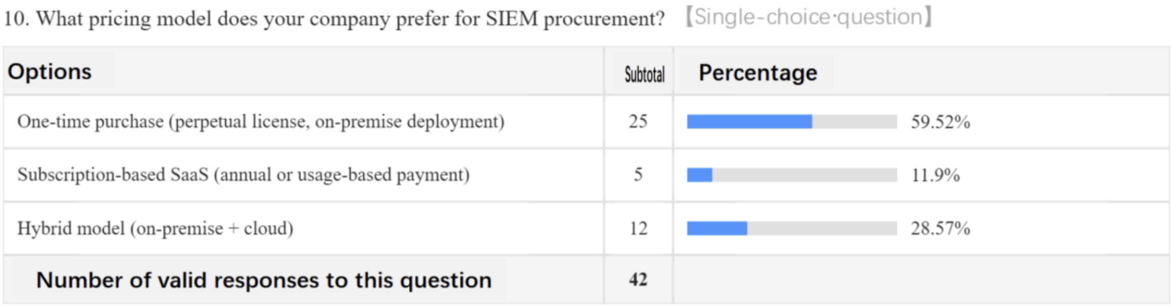
8. If Dataori SIEM offers more efficient AI-driven threat detection and reduces false positives, would you conside 【Single-choice·question】

Options	Subtotal	Percentage
1 (Not at all)	7	16.67%
2 (Unlikely)	6	14.29%
3 (Neutral)	23	54.76%
4 (Likely)	5	11.9%
5 (Definitely)	1	2.38%
Number of valid responses to this question	**42**	



9. How does your company decide on the SIEM procurement budget?
【Single-choice·question】

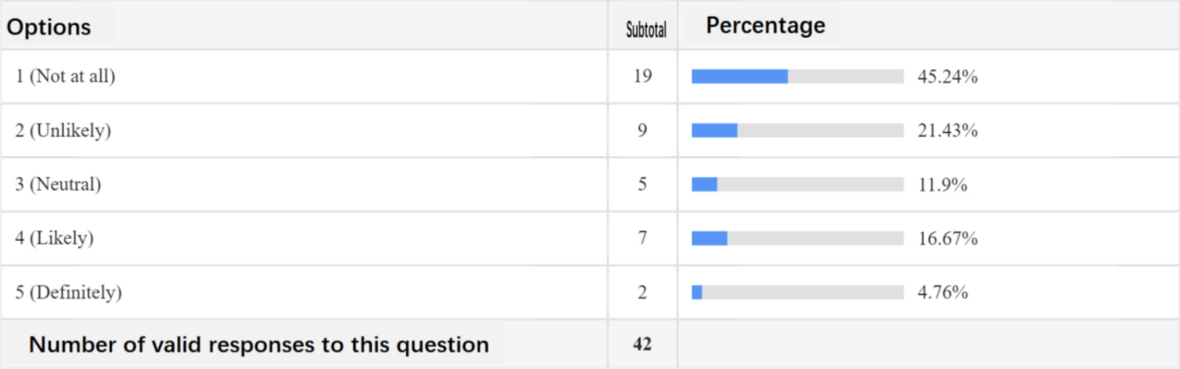
Options	Subtotal	Percentage
Annual budget, decided by the security team	28	66.67%
CIO/CISO evaluates ROI before deciding on the budget	9	21.43%
Temporary procurement driven by compliance and regulatory requirements	1	2.38%
Other (please specify)	4	9.52%
Number of valid responses to this question	**42**	



10. What pricing model does your company prefer for SIEM procurement? 【Single-choice·question】

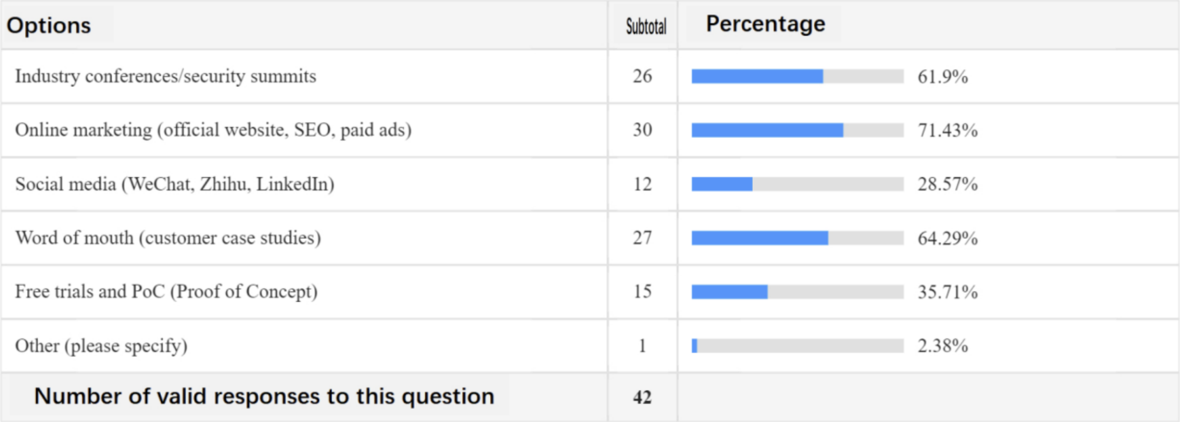
Options	Subtotal	Percentage
One-time purchase (perpetual license, on-premise deployment)	25	59.52%
Subscription-based SaaS (annual or usage-based payment)	5	11.9%
Hybrid model (on-premise + cloud)	12	28.57%
Number of valid responses to this question	**42**	

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 question】



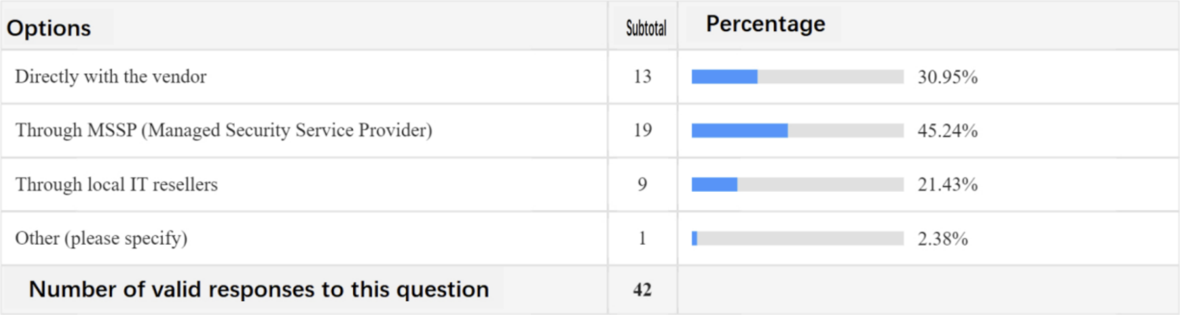
Options	Subtotal	Percentage
1 (Not at all)	19	45.24%
2 (Unlikely)	9	21.43%
3 (Neutral)	5	11.9%
4 (Likely)	7	16.67%
5 (Definitely)	2	4.76%
Number of valid responses to this question	42	

12. How does your company primarily gather information about SIEM solutions? (Multiple choices allowed) 【Multiple-choice question】



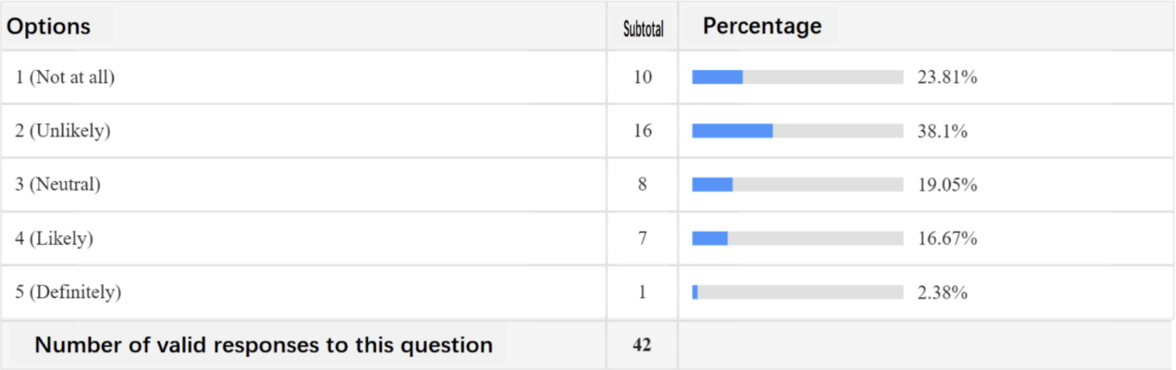
Options	Subtotal	Percentage
Industry conferences/security summits	26	61.9%
Online marketing (official website, SEO, paid ads)	30	71.43%
Social media (WeChat, Zhihu, LinkedIn)	12	28.57%
Word of mouth (customer case studies)	27	64.29%
Free trials and PoC (Proof of Concept)	15	35.71%
Other (please specify)	1	2.38%
Number of valid responses to this question	42	

13. Which method does your company prefer for purchasing SIEM solutions? 【Single-choice question】



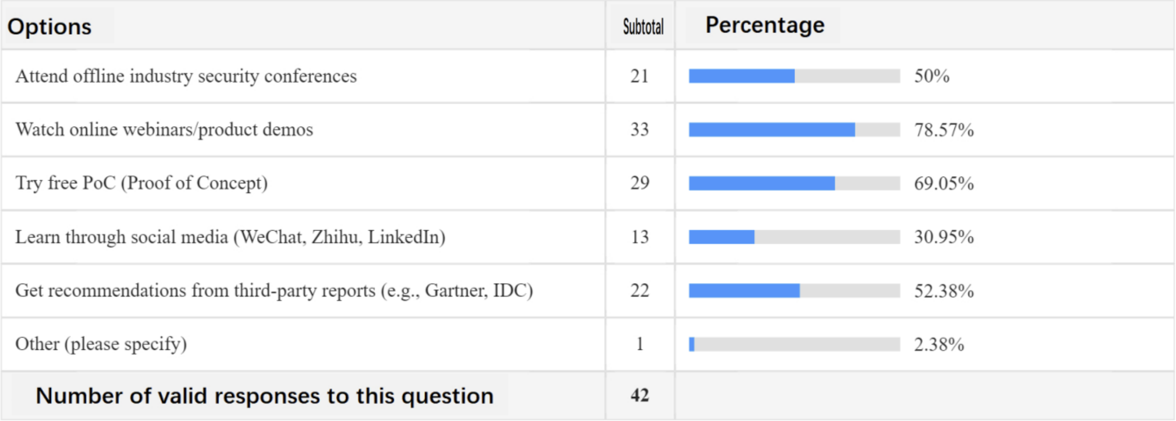
Options	Subtotal	Percentage
Directly with the vendor	13	30.95%
Through MSSP (Managed Security Service Provider)	19	45.24%
Through local IT resellers	9	21.43%
Other (please specify)	1	2.38%
Number of valid responses to this question	42	

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



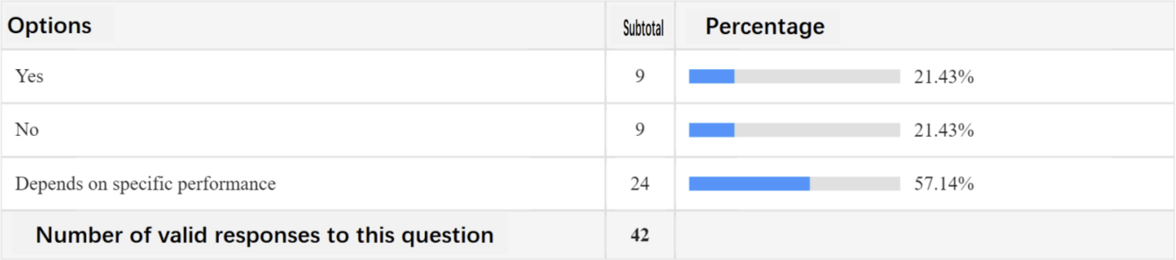
Options	Subtotal	Percentage
1 (Not at all)	10	23.81%
2 (Unlikely)	16	38.1%
3 (Neutral)	8	19.05%
4 (Likely)	7	16.67%
5 (Definitely)	1	2.38%
Number of valid responses to this question	42	

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) 【Multiple-choice·question】



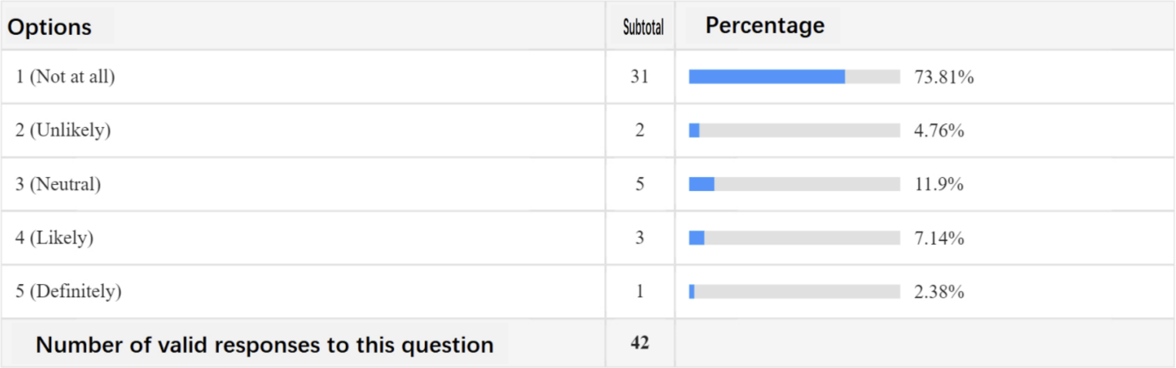
Options	Subtotal	Percentage
Attend offline industry security conferences	21	50%
Watch online webinars/product demos	33	78.57%
Try free PoC (Proof of Concept)	29	69.05%
Learn through social media (WeChat, Zhihu, LinkedIn)	13	30.95%
Get recommendations from third-party reports (e.g., Gartner, IDC)	22	52.38%
Other (please specify)	1	2.38%
Number of valid responses to this question	42	

16. Is your company more inclined to choose SIEM products that have been used in domestic banks or government agencies? 【Single--choice·question】



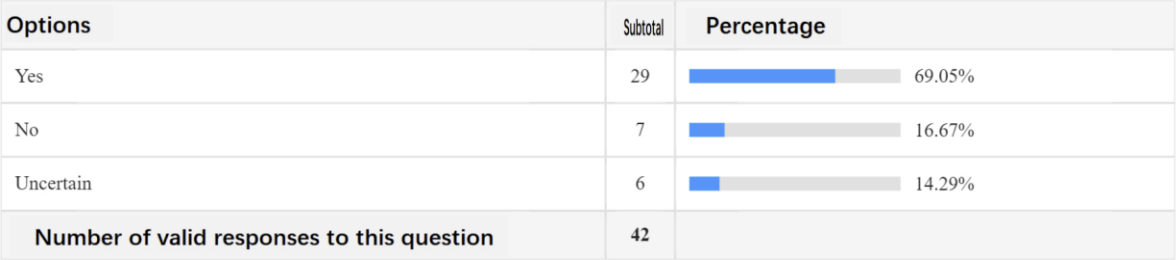
Options	Subtotal	Percentage
Yes	9	21.43%
No	9	21.43%
Depends on specific performance	24	57.14%
Number of valid responses to this question	42	

17. If Dataori SIEM offers a 3-6 month free trial, would you be willing to try it? 【Single-choice·question】



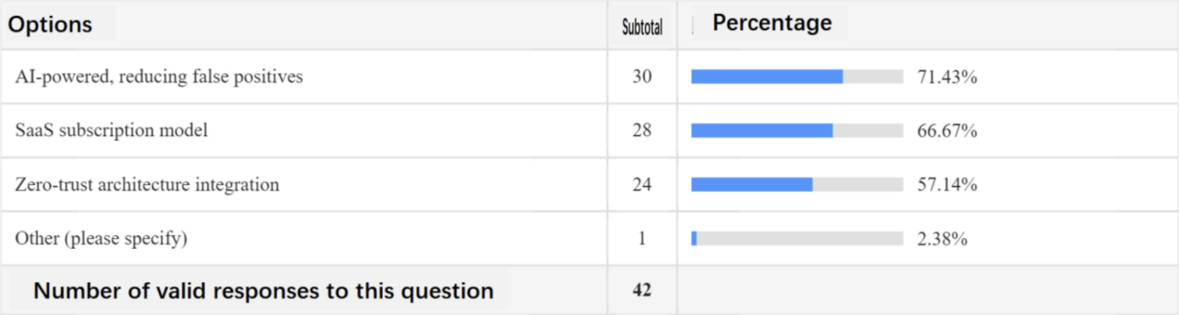
Options	Subtotal	Percentage
1 (Not at all)	31	73.81%
2 (Unlikely)	2	4.76%
3 (Neutral)	5	11.9%
4 (Likely)	3	7.14%
5 (Definitely)	1	2.38%
Number of valid responses to this question	42	

18. Does your company plan to replace or add a SIEM solution in the next 1-2 years? 【Single-choice·question】



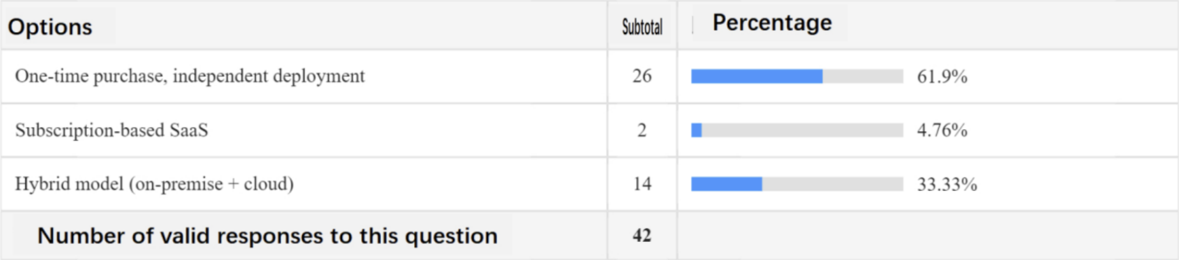
Options	Subtotal	Percentage
Yes	29	69.05%
No	7	16.67%
Uncertain	6	14.29%
Number of valid responses to this question	42	

19. What do you think is the future direction of SIEM? (Multiple choices allowed) 【Multiple-choice·question】



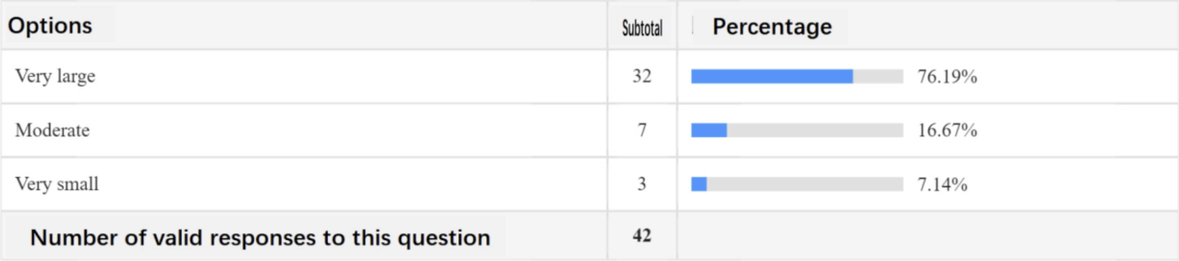
Options	Subtotal	Percentage
AI-powered, reducing false positives	30	71.43%
SaaS subscription model	28	66.67%
Zero-trust architecture integration	24	57.14%
Other (please specify)	1	2.38%
Number of valid responses to this question	**42**	

20. What SIEM procurement model does your company prefer in the future? 【Single-choice·question】



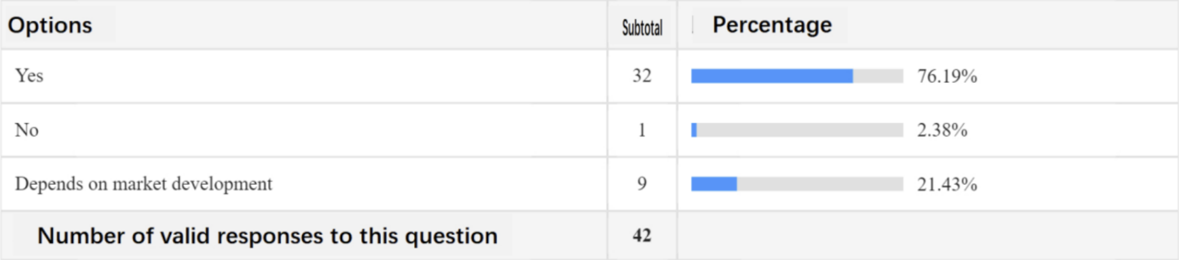
Options	Subtotal	Percentage
One-time purchase, independent deployment	26	61.9%
Subscription-based SaaS	2	4.76%
Hybrid model (on-premise + cloud)	14	33.33%
Number of valid responses to this question	**42**	

21. What do you think about the market opportunities for SIEM in the ITAI (Information Technology Application Innovation) environment? 【Single-choice·question】



Options	Subtotal	Percentage
Very large	32	76.19%
Moderate	7	16.67%
Very small	3	7.14%
Number of valid responses to this question	**42**	

22. Does your company plan to switch from international vendors to domestic SIEM solutions in the next 3 years? 【Single-choice·question】



Options	Subtotal	Percentage
Yes	32	76.19%
No	1	2.38%
Depends on market development	9	21.43%
Number of valid responses to this question	**42**	

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 C – 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 Verificati on 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 Verificati on 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 Conditio ns 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 Conditio ns 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