ISCTE IUL
REPOSITÓRIO
INSTITUTO UNIVERSITÁRIO DE LISBOA

Repositório ISCTE-IUL

Deposited in *Repositório ISCTE-IUL*:
2018-06-07

Deposited version:
Post-print

Peer-review status of attached file:
Peer-reviewed

Citation for published item:
Roldán-Molina, G., Almache-Cueva, M., Silva-Rabadão, C., Yevseyeva, I. & Basto-Fernandes, V. (2017). A decision support system for corporations cybersecurity management. In Reis L.P.,Rocha A.,Alturas B.,Costa C.,Cota M.P. (Ed.), 12th Iberian Conference on Information Systems and Technologies, CISTI 2017. Lisbon: IEEE.

Further information on publisher's website:
10.23919/CISTI.2017.7975826

Publisher's copyright statement:
This is the peer reviewed version of the following article: Roldán-Molina, G., Almache-Cueva, M., Silva-Rabadão, C., Yevseyeva, I. & Basto-Fernandes, V. (2017). A decision support system for corporations cybersecurity management. In Reis L.P.,Rocha A.,Alturas B.,Costa C.,Cota M.P. (Ed.), 12th Iberian Conference on Information Systems and Technologies, CISTI 2017. Lisbon: IEEE., which has been published in final form at https://dx.doi.org/10.23919/CISTI.2017.7975826. This article may be used for non-commercial purposes in accordance with the Publisher's Terms and Conditions for self-archiving.

Use policy

Creative Commons CC BY 4.0
The full-text may be used and/or reproduced, and given to third parties in any format or medium, without prior permission or charge, for personal research or study, educational, or not-for-profit purposes provided that:

- a full bibliographic reference is made to the original source
- a link is made to the metadata record in the Repository
- the full-text is not changed in any way

The full-text must not be sold in any format or medium without the formal permission of the copyright holders.

Serviços de Informação e Documentação, Instituto Universitário de Lisboa (ISCTE-IUL)
Av. das Forças Armadas, Edifício II, 1649-026 Lisboa Portugal
Phone: +(351) 217 903 024 | e-mail: administrador.repositorio@iscte-iul.pt
https://repositorio.iscte-iul.pt

A Decision Support System for Corporations Cybersecurity Management

Gabriela Roldán-Molina, Mario Almache-Cueva
Departamento de Ciencias de la Computación
Universidad de las Fuerzas Armadas ESPE
Sangolquí, Ecuador

Carlos Silva-Rabadão
School of Technology and Management
Computer Science and Communication Research Centre
Polytechnic Institute of Leiria
Leiria, Portugal

Iryna Yevseyeva
School of Computer Science and Informatics
Faculty of Technology, De Montfort University
Leicester, United Kingdom

Vitor Basto-Fernandes
Instituto Universitário de Lisboa (ISCTE-IUL)
University Institute of Lisbon, ISTAR-IUL
Lisboa, Portugal

Abstract — **This paper presents ongoing work on a decision aiding software intended to support cyber risks and cyber threats analysis of an information and communications technological infrastructure. The software will help corporations Chief Information Security Officers on cyber security risk analysis, decision-making, prevention measures and risk strategies for the infrastructure and information assets protection.**

Keywords – risk management; cybersecurity; decision-making.

I. INTRODUCTION

Recent reports have revealed the emergence of millions of computer security incidents per year and each year new records are reached. They refer that in 2014, 65% of companies, victim of intrusion and information theft, were notified after a late detection process that lasts 13 months on average [1].

This motivates the development of new technologies that can augment human understanding and decision-making abilities to create situation awareness in cyber environments. Situation awareness in cyber environments is made possible by the process of deriving context knowledge (awareness) from a multitude of information sources. Generally, it comprises three main levels, perception, comprehension and projection, which feeds the decision and action cycle.

Perception, involves sensory of significant information about the system itself and the environment it is operating in. This information can be obtained with the help of data collection tools related to the technological infrastructure of an organization (hardware, services, databases). Comprehension, encompasses more than simply sensing/perceiving data, it relates the meaning of the information with the system goal/purpose. It can be represented through an ontology for context knowledge representation. Projection, consists of predicting how system current state will evolve (in time) and how it will affect the future states of the operating environment.

Currently there are tools that comprise the different levels of situation awareness to help detect, prevent and recover from cyber incidents that could threaten the security of an organization. The present work shows a comparative analysis of the most popular and relevant tools in this area, and proposes a contribution in this domain.

The paper is organized as follows, section 2 presents a comparative analysis of a variety of tools for data collection about IT infrastructures and cybersecurity vulnerabilities. Section 3 describes the process followed to build and design cyber security context awareness. Section 4 addresses cybersecurity risk strategies and models adopted by popular vulnerability management software. Finally, section 5 presents the conclusions and future work.

II. IT INFRASTRUCTURE AND VULNERABILITY DATA COLLECTION

Nessus [2] [3] is one of the most popular vulnerability scanners, particularly for UNIX systems. A free "Nessus Home" version is available, although it is limited and only licensed for home network use. Reports generated by Nessus use standards such as CPE (Common Platform Enumeration) [4], CVE (Common Vulnerabilities and Exposures) [5], and CVSS (Common Vulnerability Scoring System) [6] which can be exported in different formats, e.g. CSV (Comma-separated values), HTML (Hypertext Markup Language), PDF (Portable Document Format) and NessusBD.

Each scan shows a vulnerabilities list, sorted by severity. It includes compliance checks, statistics and details, sorted by vulnerability severity. In addition, the results include remediation information with details, sorted by vulnerability number.

SAINT [3] is a suite of integrated products that perform vulnerability scanning, assessment, and validation on network devices, operating systems, databases, desktop applications, Web applications, and other targets. SAINTscanner not only detects weaknesses but also identifies remediations that can be applied to them before those weaknesses can be exploited by intruders. It provides information on how to implement those remediations, including pinpointing the most exploitable vulnerabilities for which remediations should be applied first. Besides, it reports the presence of exploits, the detected vulnerabilities' CVSS score, the identification of the vendor whose product is prone to the vulnerability, and other useful information.

Nmap (ZenMap) [7] known as Network Mapper is a free and open source (license) utility for network discovery and security auditing. Through the execution of commands in Nmap, you can obtain an XML (Extensible Markup Language) data file showing main information of the scan like: host name, address, open ports, services and CPE. This information is compared to CVE allowing to check system vulnerabilities. However, Nmap by itself doesn't tell us the existence of vulnerabilities on a system. By relating the scanning results, the knowledge of the computer networking, and the knowledge of the network baseline, it is possible to figure out what vulnerabilities exist, address these issues, and improve your security posture.

Retina Security Scanner enables to efficiently identify IT exposures and prioritize remediation enterprise-wide [8]. Retina Network vulnerability scanning is also offered in a free SaaS package, Retina Community, allows free vulnerability assessments and SCAP (Security Content Automation Protocol) [15] configuration compliance scans across the operating systems, applications, devices, and virtual environments at up to 32 target IP addresses, with reports generated in XML, CSV and PDF format [3]. In addition, Retina contains in its reports suggestions for remediating the security weaknesses. You can have the scan results sorted by machine (host), by vulnerability, or by CVE/IAV (Information Assurance Vulnerability Alerts) findings. Vulnerabilities can be sorted by name, risk, or severity code. You can also specify the level of detail and display options such as page breaks and optional job metrics or detailed audit status [9].

GFI LANguard [3] is a network security scanner and patch management solution that assists in patch management, vulnerability management, network and software auditing, asset inventorying, change management, risk and compliance analysis. GFI LanGuard supports machines across Microsoft®, MAC OS X® and Linux® operating systems as well as many third-party applications [10]. It includes its own vulnerability assessment database that includes checks for 2,000+ CVEs and SANS Top 20 vulnerabilities. The database is regularly updated with information from Bugtraq, SANS, CVE, Microsoft security updates, and GFI Software's and other community-based information repositories. Scan results can be exported in XML format. GFI also offers a freeware version, intended for personal use, and capable of scanning up to five IP addresses. The freeware version of GFI LANguard provides all functions found in the commercial version with the exception of patch management for non-Microsoft applications [3].

nCircle IP360 [3] is a component of nCircle's security risk and compliance management suite. Using agentless technology, IP360 profiles all networked devices and tests for the presence of more than 40,000 conditions (OSs, applications, vulnerabilities, configurations). IP360 [11] uses advanced analytics and a unique quantitative scoring algorithm based on several factors—including the vulnerability score and business-relevant asset value—to prioritize the vulnerabilities for remediation. The result is actionable data that enables IT security teams to focus on the tasks that will quickly and effectively reduce overall network risk with the fewest possible resources. Furthermore, IP360 has support for the following standards: SCAP (Security Content Automation Protocol), OVAL (Open Vulnerability and Assessment Language), CVE, CVSS.

Security System Analyzer 2.0 Beta (SSA) is free non-intrusive OVAL [12], FDCC (Federal Desktop Core Configuration) [13], XCCDF (Extensible Configuration Checklist Description Format) [14] and SCAP [15] scanner. It provides security testers and auditors with an advanced overview of the security policy level applied [16]. It can identify vulnerabilities and security discrepancies through its OVAL interpreter and large database of OVAL vulnerability definitions, and generate output in CSV [3] format. The main features of this tool are [16]:

a) Fully support of open security standards and initiatives (CVE, OVAL, CCE, CPE, CWE, SCAP, CVSS);
b) Perform Compliance and Security Checks using the XCCDF;
c) Configuration Checklist Description Format;
d) Qualifying the vulnerabilities using CVSS v2.0 scoring.

The Open Vulnerability Assessment System (OpenVas) [3] [17] is a framework of several services and tools. All clients run on Windows, Linux, and other OSs. For decision aiding purposes OpenVAS allows assessment of vulnerabilities, access control and intrusion, and risk assessment using the CVSS scoring system. It allows to analyze a desktop computer or a local/remote server and perform various types of reports on detected vulnerabilities. In addition, it adds a correlation engine to interlace everything that has been identified/detected and proposes associated solutions. The standard adopted for OpenVas is OVAL.

Nexpose [18] [19] is a vulnerability scanner that enables you to focus on risk that matters while greatly reducing the time required to run a successful vulnerability management program. NeXpose is offered in four versions: NeXpose Enterprise, NeXpose Consultant, NeXpose Express and NeXpose Community which is free. The Community version provides reporting in XML format. The tool also provides detailed remediation guidance that includes time estimates, exploit risk score, and asset criticality. Nexpose prioritizes mitigation tasks to reduce overall risk as quickly as possible. It categorizes vulnerabilities with a CVSS score. The standards adopted by Nexpose are CPE, CCE, SCAP, CVE and CVSS.

QualysGuard consists of an integrated suite of solutions to help organizations simplifying security operations and lowering the cost of compliance [20]. It includes Vulnerability Management (VM), a cloud service that gives you immediate, global visibility into where your IT systems might be vulnerable to the latest Internet threats and how to protect them [21]. Furthermore, Qualys separates reporting from scanning, enabling you to use a wide range of filters to explore your vulnerability findings. You can look for specific types of vulnerabilities and use criteria from Qualys's Knowledge Base such as severity, business risk, CVSS scores, existence of exploits or malware, and whether patches are available [22].

This section presents a comparative study identifying the main features of the most relevant tools for collecting

information on the IT infrastructure, in order to choose the most suitable and convenient for the development of a decision support system in the cybersecurity domain. The criteria established for the characterizations and evaluation of the tools are: The tool name (*Tool*); If the tool has a free version (*Free Version*); Type of license under which the tool is distributed (*License*), Commercial, Shareware, Open Source, or Freeware; If the Common Platform Enumeration standard is supported *(CPE)*; If the Common Configuration Enumeration standard is supported (*CCE*); Relevant standards to which the tool is compliant with (*Standards*), which includes only standards directly relevant to vulnerability analysis, i.e., SCAP, OVAL, CVE, CWE, and CVSS; The operating system(s) (OS) on which a software tool runs (*SO Support*); If the tool supports functionalities for vulnerability detection, identification and prioritization of remediation measures (*Decision Support*); Format to which the results can be exported (*Export Results*), e.g. information about the assets, exported to XML, CSV, etc.

For the selection of the most promising tool, each criteria is assigned a weight, according to its relevance in the context of our study. The criteria and their relevance are presented next.

Free Version:

As shown in the Table I, the value of "3" is assigned to the tool that has a free version available without a time limit, "2" for one that has a free version but has a limit number of days (usually 30 days) and "1" for one that does not have a free version.

TABLE I. TABLE WEIGHING FREE VERSION

Value	Weighting
No	1
Yes(Trial)	2
Yes	3

License:

The metric is defined according to the type of license (Table II), in the case of being open source the assigned value is "3", if it is freeware "2" and in case of being commercial the assigned value is "1".

TABLE II. TABLE WEIGHING LICENSE

Value	Weighting
Commercial	1
Freeware	2
Open Source	3

CPE, CCE, Decision Support:

In the case of the CCE, CPE and decision support criteria, value "2" or value "1" is assigned to indicate the corresponding tool compliance or not compliance, respectively (Table III).

TABLE III. TABLE WEIGHING CPE , CCE ,DECISION SUPPORT

Value	Weighting
No	1
Yes	2

Standards, SO Support, Export Results:

These criteria are quantified in Table IV, according to the number of standards used by the tool, the operating systems it supports or the number of formats available to export the results. Three is the highest value, for example in case a tool uses more than 3 security standards.

TABLE IV. TABLE WEIGHING STANDARDS,

SO SUPPORT, EXPORT RESULTS

Value	Weighting
One	1
More than 2	2
More than 3	3

Table V shows the results according to the established metrics.

TABLE V. RESULTS

Tool	Free Version	License	CPE	CCE	Standards	SO Support	Decision Support	Export Results	Total
Nexpose	3	1	2	2	3	3	2	3	19
Nessus Home	3	2	2	1	2	3	2	3	18
Security System Analyzer 2.0 Beta	3	3	2	1	3	1	2	1	16
OpenVas	3	3	1	1	1	2	2	3	16
Saint8	1	1	2	2	3	2	2	2	15
Nmap (ZenMap)	3	3	2	1	1	3	1	1	15
eEye Retina	2	1	2	1	3	1	2	2	14
QualysGuard	2	1	1	1	3	1	2	3	14
GFI LANguard	2	1	1	1	2	3	2	1	13
nCircle® IP360	1	1	2	1	3	1	2	2	13

As described previously, Nexpose is ranked first with a total of 19 points, followed by Nessus Home with 18 points. In this way, it can be concluded that Nexpose is the most promising tool in the context of our study, because it fulfills most criteria in comparison with the other tools. Among several properties, we can emphasize that this tool supports operating systems such as Windows and Linux. Furthermore, the representation of the results (vulnerability reports) is based on standards such as CPE, CVE and CVSS. This information can be exported in various formats such as XML and HTML, allowing developers to obtain these data for manipulation and integration with other applications.

Another important reason for choosing this tool is that it has several features for decision support, one of which is to get a full picture of risk across IT assets, encompassing vulnerabilities and configuration issues, presented in easy-to-use customizable reports. This enables better decision-making and increases the credibility of the security team across the organization.

III. DESIGNING AND BUILDING CYBER SECURITY CONTEXT AWARESSNESS

To implement the comprehension layer of our context aware system, we adopted an (OWL [23]) ontology based knowledge representation. The role of the ontology in our work is to represent not only the data captured at the perception layer by the tool described in previous section, but also to allow domain and corporations specific knowledge to be added by cyber security experts (e.g. CIO). Experts are allowed to introduce new specific knowledge into the ontology using Protége [24]

ontology editor. Assets characterization such as asset value and importance of each security dimension associated to that asset (privacy, integrity, availability) must be provided by experts and added to the ontology. This knowledge is essential to support corporation specific cyber risk analysis and management to be performed by the decision aiding software to be developed in our study.

A method to build/instantiate the initial (OWL) ontology automatically is proposed. The generation method is based on the XML-Schema of Nexpose [25] for the construction of the (OWL) ontology.

As shown in Fig. 1, the generation of OWL ontology from XML standards and data sources could be described in 3 steps:

1) From the XML-Schema the design of the base ontology is performed, using Protegé, a tool that provides a graphical interface for the construction of ontologies in OWL language.

2) The Nexpose results XML file is analyzed using the Document Object Model (DOM), an application programming interface for Java. In this way we can obtain Nexpose dynamically generated data that will be added in the ontology.

3) Finally, each of the individuals obtained from parsing the XML file is added in the base ontology, with the help of the OWL-API for java.

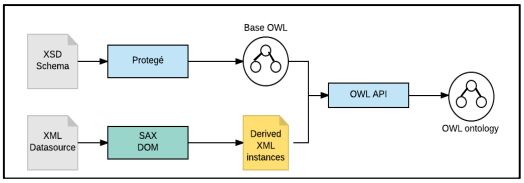

Figure 1. Generation process of OWL ontology.

A. XML to OWL Mapping

This section defines a notation to specify mappings between elements of Nexpose XML Schema and resources of an OWL ontology, which is mainly defined by classes, datatype and object properties [26] [27].

Three types of mappings are presented as follows:

- Class mapping: Maps an XML node to an OWL concept.
- Datatype property mapping: Maps an XML node to an OWL datatype property.
- Object property mapping: Relates two class mappings to an OWL object property.

In Table VI it is possible to observe the notation of the mapping of the vulnerability node in relation to the data of the XML schema.

TABLE VI. TABLE VULNERABILITY MAPPING

Mappings	**Schema Node XML**
Class	Vulnerability
Datatype property	id, title, severity, pciSeverity, cvssScore,cvssVector,published,added,modified, riskScore.
Object property	hasVulnerability (between Device and Vulnerability class)

The generated OWL ontology is shown in Fig. 2. In this ontology, there are eleven locals complex types defined within the Device, Software, OperatingSystem, VulnerabilityDefinitions, Vulnerability, Exploit, Tag, Reference, Description, Solution and Malware.

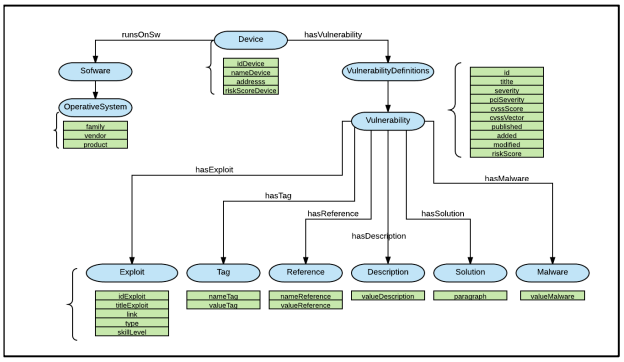

Figure 2. OWL ontology Structure.

IV. CIBERSECURITY RISK ANALYSIS

In this section, we address the context awareness projection layer and analyze how current tools deal with cyber security risk analysis and risk management.

Nexpose has a database certified to be compatible with the MITRE Corporation's Common Vulnerabilities and Exposures (CVE) index, which standardizes the data about vulnerabilities across diverse security products and vendors. The index rates vulnerabilities follow MITRE's Common Vulnerabilities Scoring System (CVSS) Version 2. Nexpose computes the CVSS score based on ease of exploit, remote execution capability, credentialed access requirement, and other criteria which range from 1.0 to 10.0 [27].

Nexpose uses CVSS metrics to compute the risk of a vulnerability on an asset. It defines different risk strategies which are based on different importance/weight of factors such as likelihood of compromise, impact of commitment, and asset importance, when computing risk. Each formula produces a different range of numeric values. For example, the Real Risk strategy produces a maximum score of 1,000, while the Temporal strategy has no upper bounds, with some high-risk vulnerability scores reaching the hundred thousand. This is important to keep in mind if you apply different risk strategies to different segments of scanned data [28].

Many of the available risk strategies use the same factors in assessing risk, each strategy evaluating and aggregating the

relevant factors in different ways. The common risk factors are grouped into three categories: vulnerability impact, initial exploit difficulty, and threat exposure. The factors that comprise vulnerability impact and initial exploit difficulty are the six base metrics employed in the Common Vulnerability Scoring System (CVSS) [29]. Nexpose environment metrics are associated to a site, which corresponds to a collection of assets that are targeted for a scan.

Nexpose applies levels of Criticality to assets to indicate their importance to the business or the negative impact resulting from an attack on them. A criticality level can be Very Low, Low, Medium, High, or Very High. Additionally, we can apply numeric values to criticality levels and use the numbers as multipliers that impact risk score. The importance level corresponds to a risk factor used to calculate a risk index for each site [28].

A. Risk Strategies

There are different types of risk strategies that help managing the uncertainty regarding a threat that can affect the assets of an organization. Some of the strategies used by Nexpose are described below [28]:

- Real Risk

"This strategy analyzes potential types of exposures associated with vulnerabilities to expand and deepen your understanding of real threats to your environment and the value of different mitigation approaches. The algorithm applies exploit and malware exposure metrics for each vulnerability to CVSS base metrics for asset impact (confidentiality, integrity, and availability) and likelihood of compromise (access vector, access complexity, and authentication requirements). It also indicates how time increases likelihood" [28]. Equation (1) is used to calculate the Real Risk scoring model:

$$\text{Risk}=\frac{\text{CVSS Impact Metrics}}{\text{CVSS Likelihood Metrics}}\times \text{Exposure}\left(\begin{matrix}\text{Malware Kits}\\ \text{Exploit Rank}\end{matrix}, \text{time}\right) \quad (1)$$

Calculating Real Risk utilizes both standard and environmental metrics for contextual insight.

- Temporal Plus

This strategy provides a more granular analysis of vulnerability impact, while indicating how time continuously increases likelihood of compromise. It applies a vulnerability's age as a multiplier of CVSS base metrics for likelihood (access vector, access complexity, and authentication requirements) and impact (confidentiality, integrity, and availability) [30].

Equation (2) is used to calculate the Temporal Plus scoring model:

$$\text{Risk}=\sqrt{t}\times\frac{(1+AV+C+I+A)}{(AC+Au)^2} \quad (2)$$

Where (t) is the time-based likelihood and represents the number of days since vulnerability publicly disclosed. The overall score increases with the number of days. The "CVSS" values refer to the various base component vectors of the CVSS version 2 which is broken down into 6 metrics, including: Access Vector (AV); Access Complexity (AC); Authentication Required (Au); Confidentiality Impact (C); Integrity Impact (I) and Availability Impact (A).

- Temporal

"This strategy indicates how time continuously increases likelihood of compromise. The calculation applies the age of each vulnerability, based on its date of public disclosure, as a multiplier of CVSS base metrics for likelihood (access vector, access complexity, and authentication requirements) and data impact (confidentiality, integrity, and availability)" [30]. Equation (3) is used to calculate the Temporal scoring model:

$$\text{Risk}=\text{time}\times\frac{\text{proximity-based impact}}{\text{exploit difficult}} \quad (3)$$

This equation can be broken down into its components as shown in (4):

$$\text{Risk}=\sqrt{t}\times\frac{(AV+C+I+A)!}{(AC+Au)^2} \quad (4)$$

This scoring model is the most effective means to track the risk associated with vulnerabilities over time.

- Weighted

"This strategy applies user-defined site importance to calculation of asset and vulnerability data to reflect corporations unique security priorities. The Weighted risk model is primarily based on asset data and vulnerability types, and it emphasizes the following factors" [27]:

a) Vulnerability severity, which is the number ranging from 1 to 10—that Nexpose calculates for each vulnerability;

b) Number of vulnerability instances;

c) Type of asset, such as a computer, router, or wireless access point (WAP);

d) Number and types of services on the asset; for example, a database has higher business value;

e) The level of importance, or weight, that you assign to a site when you configure it.

"Weighted risk scores scale with the number of vulnerabilities. A higher number of vulnerabilities on an asset means a higher risk score. The score is expressed in lower—usually single-digit—numbers with decimals" [30]. Equation (5) is used to calculate the Weighted scoring model:

$$\text{Risk}=\text{vulnSeverity}\times 0{,}02 \quad (5)$$

- PCI ASV 2.0 Risk strategy

"This strategy applies a score based on the Payment Card Industry Data Security Standard (PCI DSS) Version 2.0 to every discovered vulnerability. The scale ranges from 1 (lowest severity) to 5 (highest severity). With this scoring model, Approved Scan Vendors (ASVs) and other users can assess risk from a PCI perspective" [30].

V. Conclusions And Future Work

This paper presented a study for the development of a cyber security risk analysis and management system. The layered reference model for context aware system was followed, addressing the perception, comprehension, projection and decision/action layers. A detailed analysis was made on information technology infrastructure data collection tools, and one of the tools (Nexpose) was selected as the most suitable to support the perception layer of the decision support system to be developed.

OWL was selected as the standard to support the knowledge representation for the comprehension layer. An ontology design and a process of transforming the information provided by Nexpose to an OWL ontology was presented. Protége OWL ontology editor was also presented as one of the most suitable tools to allow cyber security experts to provide corporation specific assets value and security requirements characterization. Projection and decision layers were addressed by studying Nexpose currently supported risk strategies.

We intend to extend and specialize the risk analysis techniques of Nexpose, by using the knowledge management features supported by the OWL ontology and test new decision aiding techniques to take into account specific corporation needs. Specific data collection and inference by the means of ontology design and engineering, supported by experts knowledge and by new decision aiding models are promising research lines to be followed in our study.

Acknowledgment

The present study is carried out as part of the Master's Degree in Computer Engineering - Mobile Computing at the Polytechnic Institute of Leiria, thanks to the scholarship granted by the agreement SENESCYT-Leiria Polytechnic Institute. Vitor Basto-Fernandes acknowledges the support of the Portuguese republic national funds through Fundação para a Ciência e a Tecnologia under the project UID/CEC/4524/2016.

References

[1] A. Oltramari, L. Faith, C. R. J. Walls and P. McDaniel, "Building an Ontology of Cyber Security," November 2014. [Online]. Available: http://ceur-ws.org/vol-1304/stids2014_t08_oltramarietal.pdf.

[2] Tenable Network Security, "Nessus Home," 2017. [Online]. Available: https://www.tenable.com/products/nessus-home. [Accessed 2016].

[3] IATAC, "Vulnerability Assessment," 2 May 2011. [Online]. Available: https://www.csiac.org/wp-content/uploads/2016/02/vulnerability_assessment.pdf.

[4] The MITRE Corporation, "CPE Common Platform Enumeration," 28 November 2014. [Online]. Available: https://cpe.mitre.org/.

[5] The MITRE Corporation, "CVE Common Vulnerabilities and Exposures," 23 February 2017. [Online]. Available: https://cve.mitre.org/.

[6] FIRST.org, Inc., "Common Vulnerability Scoring System, V3 Development Update," 2017. [Online]. Available: https://www.first.org/cvss.

[7] NMap, "NMAP.ORG," 2016. [Online]. Available: https://nmap.org/.

[8] BeyondTrust,inc, "Retina Network Vulnerability Scanner," 2016. [Online]. Available: https://www.beyondtrust.com/products/retina-network-security-scanner/.

[9] D. Vitale, "Doug Vitale Tech Blog," 13 Frebruary 2012. [Online]. Available: https://dougvitale.wordpress.com/2012/02/13/retina-network-security-scanner.

[10] GFI Software, "Patch management for operating systems," 2016. [Online]. Available: http://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard/specifications/patch-management-for-operating-systems.

[11] NCircle, "Enterprise-Class Vulnerability and Risk Management.," 2010. [Online]. Available: http://www.base-camp.cc/wp-content/download/ncircle/nCircle-DS-IP360-1004-05.pdf.

[12] The Mitre Corporation, "OVAL Open Vulnerability and Assessment Language," 9 February 2016. [Online]. Available: https://oval.mitre.org/.

[13] Nist, "Federal Desktop Core Configuration," 21 September 2016. [Online]. Available: https://www.nist.gov/programs-projects/federal-desktop-core-configuration-fdcc.

[14] Nist, "XCCDF - The Extensible Configuration Checklist Description Format," 16 December 2016. [Online]. Available: https://scap.nist.gov/specifications/xccdf/.

[15] Nist, "The Security Content Automation Protocol (SCAP)," 16 December 2016. [Online]. Available: https://scap.nist.gov/.

[16] Google Code, "SA - Security System Analyzer 2.0," 2016. [Online]. Available: https://code.google.com/archive/p/ssa.

[17] OpenVas, "About OpenVAS Software," 2016. [Online]. Available: http://www.openvas.org/software.html.

[18] Rapid7, "Nexpose Free Vulnerability Scanner Trial," 2017. [Online]. Available: https://www.rapid7.com/products/nexpose/download.

[19] Rapid7Community, "Driving Risk Reduction through RealContext™ in Nexpose 5.9," 26 March 2014. [Online]. Available: https://community.rapid7.com/community/nexpose/blog/2014/03/26/driving-risk-prioritization-through-realcontext-in-nexpose-59.

[20] Qualys, Inc, "QualysGuard is the Qualys Cloud Platform," 2017. [Online]. Available: https://www.qualys.com/qualysguard.

[21] Qualys, Inc, "The Market Leader in Vulnerability Management," 2017. [Online]. Available: https://www.qualys.com/suite/vulnerability-management.

[22] Qualys, Inc, " Features," 2017. [Online]. Available: https://www.qualys.com/suite/vulnerability-management/features.

[23] W3C Semantic Web, "Web Ontology Language (OWL)," 11 December 2013. [Online]. Available: https://www.w3.org/OWL/.

[24] Stanford Center for Biomedical Informatics Research, "Protégé," 2016. [Online]. Available: http://protege.stanford.edu/.

[25] Rapid7Community, "Report_XML_Export_Schema_2.0.zip," 3 July 2013. [Online]. Available: https://community.rapid7.com/docs/DOC-2148. [Accessed 2017].

[26] T. Rodrigues, P. Rosa and J. Cardoso, "MAPPING XML TO EXISTING OWL ONTOLOGIES," Funchal,Portugal.

[27] Rapid7Community, "Nexpose User´s Guide," 3 February 2017. [Online]. Available: https://community.rapid7.com/docs/DOC-1387.

[28] Rapid 7, "Working with risk strategies to analyze threats," [Online]. Available: https://help.rapid7.com/nexpose/en-us/Files/Working_with_risk_strategies_to_analyze_threats.html. [Accessed 2017].

[29] N. Yahia, S. A. Mokhtar and A. Ahmed, "Automatic Generation of OWL Ontology from XML Data Source," IJCSI International Journal of Computer Science Issues, vol. 9, no. 2, pp. 77-83, 2012.

[30] Rapid7, "PCI, CVSS, & risk scoring frequently asked questions," 14 December 2016. [Online]. Available: https://help.rapid7.com/nexpose/en-us/Files/Risk_scoring_FAQ.html