Automation of Risk-Based Vulnerability Management Based on a Cyber Kill Chain Model

Thomas Devaux [1], Thomas Massip [1], Alexis Ulliac [1], Jean-Luc Simoni [1], and Paul Varela [1]

[1] *Thales SIX GTS France, 4 av. des Louvresses, 92230 Gennevilliers, France*

Abstract

Risk management and Vulnerability management are both essential cybersecurity domains. They are often managed independently without a proper interface to provide context information to each other's and share information. This paper proposes an approach to connect risk management and vulnerability management processes and provide automation in both ways to help to categorize and sort a large number of vulnerabilities and build operational risk scenarios relevant to the business. A four steps approach presents the process for connecting and adjusting information from Operational Scenario (OpeSce) and Vulnerabilities: STEP 1 Link Operational Scenarios and Vulnerabilities, STEP 2 Re-assessment scoring of the Operational Scenario, STEP 3 Re-assessment scoring of the Vulnerabilities.

Keywords

Vulnerability Management, Risk Management, Compliance, Automation, ATT&CK, CVSS, cyber kill chain, Triage

1. Introduction

The digitalisation and interconnexion of systems are increasing tremendously. The industry is facing a new challenge to manage risks and vulnerabilities at this scale. Systems become more and more complex and can be made of an aggregation of different sub-systems from several suppliers as well as legacy sub-systems. Risk management is done at high system level view when vulnerability management is done using the knowledge of assets at the field and sub systems level.

The Figure 1 shows this relationship where each sub-system can have its own risk assessment and own way of managing vulnerabilities.

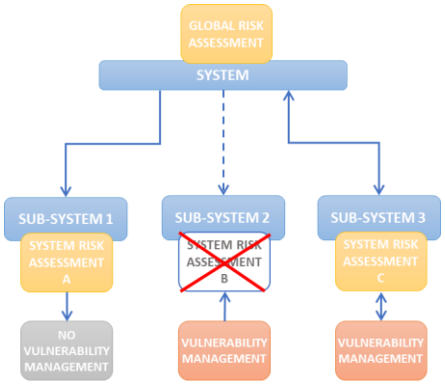

Figure 1: Risk management vs. Vulnerability management for system of systems

Therefore, interconnecting the vulnerability management to a high-level system risk management process can be challenging. This paper proposes an approach to connect risk management and

C&ESAR'21: Computer Electronics Security Application Rendezvous, November 16-17, 2021, Rennes, France
EMAIL: firstname.lastname@thalesgroup.com
ORCID: 0000-0003-1543-9473 (A. 2); 0000-0001-7936-316X (A. 3); 0000-0001-9028-8455 (A. 4); 0000-0001-9953-5360 (A. 5)

vulnerability management processes and provide automation in both ways to help to categorize and sort a large number of vulnerabilities and build operational risk scenarios relevant to the business.

In this paper, after the presentation of the problematic and associated challenges (§2), is presented the vulnerability management (§3) then risk management (§4) before presenting the interface between the two activities and how to provide automation to support the security analyst (§5).

2. Problematic

Risk management and Vulnerability management are both essential cybersecurity domains. Risk management is a framework to identify, evaluate and prioritize risks [1] from business analysis to identification of risks scenarios. The vulnerabilities management is the process of analysing and sorting vulnerabilities from audits and CSIRT[2] alerts in the most efficient way for treatment.

They are often managed independently without a proper interface to provide context information to each other and share information.

In the state of the art, publications have already been done on how to combine risk and vulnerability management. One approach is to try to use CVSS metrics for Information Security Risk Assessment as defined in [2]. The limit of this approach is the difficulty to establish an exhaustive mapping between all metrics used for vulnerably scoring with risk assessment metrics such as likelihood and impact.

A second approach is to combine CVSS, attack graphs and the network information to provide parameters to objectively reflects the risk represented by vulnerabilities regarding its network environment by using HIN (Heterogeneous Information Network) as defined in [3]. This approach provides a proposition of solution to the lack of additional values in CVSS Access Vector parameter (see Figure 3: CVSS v3.1 Score assessment) for Vulnerability assessment. It does not address the link with an actual risk management activity.

In addition, the usage of the Cyber Kill Chain® [5] (CKC) to organize vulnerabilities has been addressed by ENISA [6] with the outcome that vulnerabilities are not homogenously represented in the different CKC[3] steps. The advantage of using operational scenarios based on CKC, for vulnerability management, is to answer to attack-graph complexity that is explained in §2.2 bottom-up challenge. The BSI [7] proposes a mapping between elementary threats and security measures. They estimates [8] that an effective security baseline can cover up to 80% of basic attacks. Based on the EBIOS Risk Manager approach [9], operational scenarios are defined considering the compliance to the security baseline. It means that by mapping the operational scenarios, from risk management activities to vulnerabilities, the implementation of the security baseline and associated security controls is considered. This is not possible using only CVSS metrics following a traditional vulnerability management process. CVSS is not considering the actual security measures implemented.

A. Kuppa et al. [10] proposes an approach to match vulnerabilities and techniques of cyber kill chain with Natural Language Processing (NLP) techniques and Multi-Label Text Classification (MLTC) models. The lessons learned from this state-of-the-art analysis is that to avoid to add complexity to both processes, it is required to keep risk management and vulnerability management separated but complementary by defining an interface between them. The approach used by EBIOS Risk Manager with operational scenarios combined with the usage of the CKC for vulnerably organization can be used as an interface to provide automation in order to support the security analyst.

This publication focuses on proposing means to link Risk and Vulnerability Management activities, which are complementary, while keeping them independents.

[2] Computer Security Incident Response Team
[3] Cyber Kill Chain®

2.1. Top down challenges

The standard approach to perform a risk assessment is to use a top down approach to define what to protect, against who, what is feared and how it could occur. Top down challenges can be defined as:

- Architecture granularity: In most cases, the Risk Assessment is based on a High-Level Design (HLD) architecture which does not include the description of all assets (server, network, etc.). The vulnerabilities are assigned on technical assets. However, the link between the technical asset and the "higher level" assets of the Risk Assessment is not straightforward.
- Complex system risk assessment mapping: Risk Assessment starts at a high level for complex systems, in order to identify and justify security system requirements. However, as lower level systems can be developed and integrated by various stakeholders (industry, subcontractors, etc.), specific risk assessment can be done locally for sub systems. It is essential to tailor global risk assessment impacts to sub-systems.
- Likelihood evaluation: A consequence of the first above challenge is the difficulty to evaluate the likelihood of such risk scenario considering the lack of operational parameters and detail of lower level architecture.

The proposition to solve those challenges is to use vulnerabilities to help building risk scenarios using vulnerability management.

2.2. Bottom-up challenges

Vulnerability Management through the process of vulnerability disclosure is facing a huge number of vulnerabilities to deal with. It is essential to be able to perform a triage in order to keep only the relevant vulnerabilities for remediation decision by the management. Bottom-up challenge can be defined as:

- Asset valuation: Audits and penetration testing enable to report Vulnerabilities and Weaknesses (CVE vs CWE). In this situation, it is easy to link vulnerabilities to supporting assets, however, the lack of context with a pre-existing risk assessment makes them difficult to prioritize as it is difficult to define the importance of a supporting asset without the system context.
  The vulnerability scoring Common Vulnerability Scoring System CVSS version 3.1 [11], detailed later in this publication, reflects the challenge of bringing context to a vulnerability regarding the importance of a supporting asset for a system or the organization. Indeed, the CVSS score can be compared to a risk level as it is defined by the combination of the Exploitability and Impact metrics. Nevertheless, at the vulnerability level, only the associated supporting asset is known. All the context such as the importance of the asset regarding its environment and its mission is not known. The CVSS allows to apply a ponderation to the impact metrics regarding the vulnerability environment but at the vulnerability management level it is difficult to have access to such information.

- Attack-graph complexity: Many publications have been done to explain how to use attack-graph method to represent possible attack paths and associated vulnerabilities as explained in [3]. However, an issue with this approach is that attack graphs generation implies polynomial complexity and an exponential number of attack paths.

The proposition to solve these challenges is to use risk scenarios to help in the assessment of a vulnerability (including triage and prioritization).

2.3. Problematic of interfacing risk management and vulnerability management

As shown in Figure 2, this publication proposes a way to automatically interface risk management and vulnerability management in order to solve the top down (blue arrows) and bottom up (green arrows) challenges listed above.

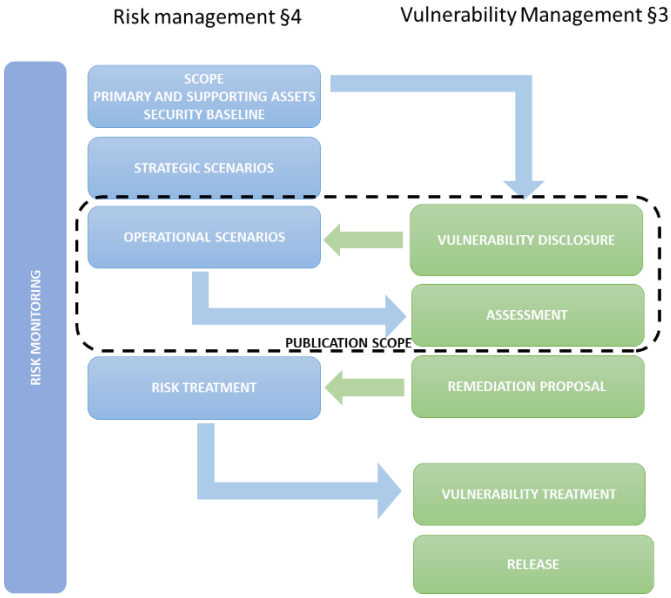

Figure 2: Risk and vulnerability management interaction

The current version of EBIOS Risk Manager [8] provides a detailed framework to define and describe operational scenarios as per the workshop 4.

3. Vulnerability management

3.1. Vulnerability handling and disclosure

In order to deal with vulnerabilities, a Vulnerability Management process needs to be defined in the organization. It can be defined as how to process and remediate potential vulnerability information reported by internal or external individuals or organizations.

ISO (International Standard Organization) provides terms, definitions, concepts and organization propositions to structure this activity through 2 complementary standards:

- ISO 30111 – Vulnerability handling process [12]. It deals with the investigation, triage, and remediation of internally or externally reported vulnerabilities.
- ISO 29147 – Vulnerability disclosure [13]. It deals with the interfaces between the different potential vulnerability reporting stakeholders (vendors, audits/penetration testing, etc.).

Vulnerability management can be defined by the following sub-activities:

- Vulnerability management policy and organization (Preparation): Development of a Vulnerability management policy, processes and capabilities. This includes the definition of roles and responsibilities such as an internal response team for Vulnerability management (PSIRT/CSIRT).

- Vulnerability disclosure (Receipt): Interactions with internal/external stakeholders to receive new potential vulnerability report from CVE (Common Vulnerabilities and Exposures)), audits and penetration testing results or security baseline non-compliance.

- Assessment (Verification): The internal PSIRT/CSIRT proceeds to an initial investigation in order to confirm that the potential vulnerability is applicable to the organization scope. A root cause analysis is then performed to identify the affected supporting assets and the related primary assets (information or processes). The vulnerability is assessed in order to define a prioritization. During the assessment, the importance of the supporting asset affected by the vulnerability can be defined in collaboration with the Chief Information Security Officer who is in charge of the risk management. This can be done by adjusting the Environmental score introduced below in 3.2 in accordance with the supporting asset owner (e.g. CISO).

- Remediation proposal & Vulnerability treatment (Remediation Development): The decision authority defines the remediation treatment option related to the vulnerability. The remediation is then produced and tested to ensure that the measure is efficient and does not introduce new vulnerabilities.

- Release (Release & Post Release): The remediation release is deployed on the related supporting assets. The post release ensures the maintenance and monitoring of the remediation.

3.2. Vulnerabilities assessment

Vulnerabilities scoring

Vulnerabilities can result from different type of inputs but it is important to share the same vulnerability scoring system and criteria in order to be able to make an assessment and prioritization.

Common Vulnerability Scoring System CVSS version 3.1 [4] allows to define an overall scoring of a vulnerability based on the following metric groups as defined in Figure 3:

- Basic: intrinsic qualities of a vulnerability that are constant over time and across user environments
- Temporal: characteristics of a vulnerability that change over time
- Environmental: characteristics of a vulnerability that are unique to a user's environment

It is the environmental metrics groups that will allow an organization to reassess the vulnerability overall scoring regarding its own environment (affected primary/supporting assets, etc.).

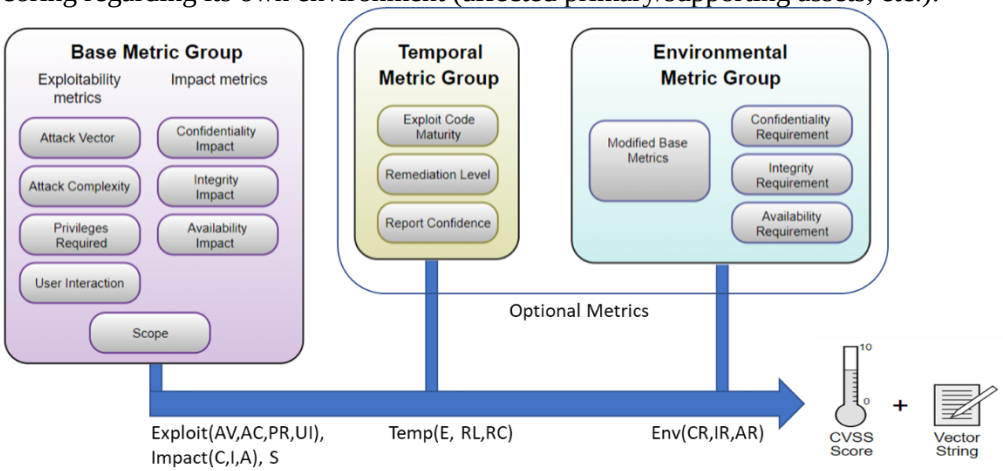

Figure 3: CVSS v3.1 Score assessment [4]

Vulnerability origin types

Vulnerabilities can be from different origin types and sources:

- Audits and penetration testing reports:

Vulnerabilities can result from security audits and penetration testing findings.

Depending on the scope and perimeter and type of audits, such as black box or crystal box, it is possible to identify non-identified vulnerabilities on the system. In order to be able to integrate those results in the vulnerability management process it is important to use the same scoring and metrics to be able to make an assessment using the same criteria.

Reports from security audits and penetration testing shall present the vulnerabilities identified using the CVSS scoring. Most of the time as the tests are done by external third parties, only the Base and Temporal Metric Group can be fulfilled in this situation.

- Publicly disclosed vulnerability – CVE:

Some vulnerabilities are publicly available. This is the case for CVEs [10] (Common Vulnerabilities and Exposures) which are computer security flaws, disclosed by CNAs (CVE Numbering Authorities) assigned to a specific CVE ID. Those software based CVE are assessed using the current Common Vulnerability Scoring System CVSS version 3.1 [4] and can be related to a CPE [14] (Common Platform Enumeration) which is a structured naming scheme for information technology systems, software, and packages. Those vulnerabilities are the most common to deal with in a vulnerability management process.

- Non-Compliance – Security baseline:

Vulnerabilities can also be expressed as a lack of security measure, or more specifically to a non-compliance to security requirements from the security baseline applicable to the system. The statement of compliance regarding the security requirements can be expressed as Covered/Partially covered / Not covered. Depending on this status it is possible to create a vulnerability issued from the non-compliance using the CVSS scoring.

In order to be able to use those vulnerabilities in risk scenarios definition, it is needed to use the same scoring metrics (such as CVSS). Further inputs can be found in [6]Figure 3.

4. Risk management

4.1. EBIOS Risk Manager

As per ISO 27005 [1] definition, the Information Security Risk Management process is a systematic approach to information security which is necessary to identify organisational need regarding information security requirements and to create an effective Information Security Management System (ISMS) in support to ISO 27001 [15].

Information risk management is a continuous process that enables to keep residual risks at an acceptable level for the organisation.

In this paper, the EBIOS Risk Manager [9] methodology is used as an information security risk assessment framework. The segregation of risk scenario into strategic and operational scenarios makes it suitable for this exercise.

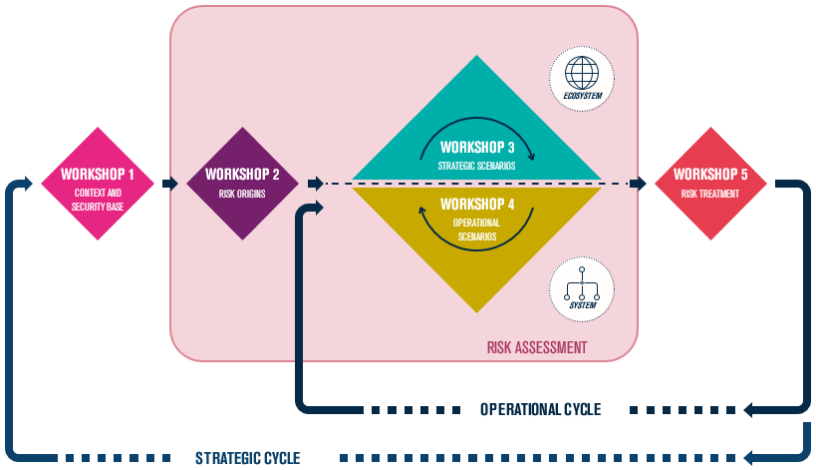

Figure 4: EBIOS Risk Manager Workshops

The methodology proposes a 5 steps workshop:

1. Scope and security baseline;
2. Risk origin and target objectives;
3. Strategic Scenarios (linked to Gravity value);
4. Operational Scenarios (linked to Likelihood value);
5. Risk treatment.

In this paper, the focus is on operational scenarios and how they can be:

- Used to build scenarios suitable for vulnerability management (2.1 top down challenge);
- Built from audit results from vulnerability management process, with limited prior knowledge of the sub-system architecture (2.2 bottom-up challenge).

4.2. Operational scenarios definition with Cyber Kill Chain

Operational scenarios are defined by different attack paths an attacker can realize to trigger a strategic scenario. Attack path are designed with the support of the Cyber Kill Chain® concept [5]. An attack path is composed of a sequence of steps, each of them composed of a technique (elementary actions also called elementary threats) and supporting asset (on which the technique is applied).

Various implementation of Cyber Kill Chain® knowledge base exists, the most well-known are the ATT&CK MITRE [11] or the Attack Kill Chain from Microsoft [16].

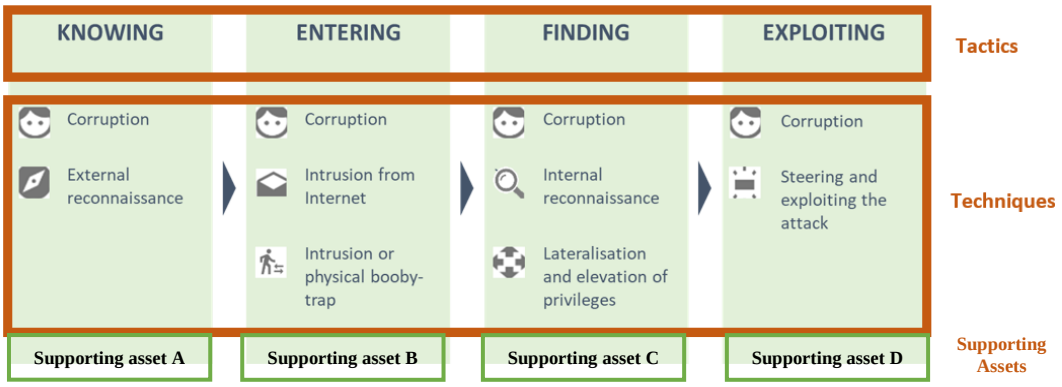

Figure 5: Simplified Cyber Kill Chain® [9]

In this paper, a simplified kill chain (proposed in EBIOS RM [9]) is used and composed of the following tactics in Figure 5:

1. Knowing: gather information on the targeted system (OSINT, Intelligence, etc.);

2. Entering: Find a way to enter into the targeted system (social engineering, USB key, fishing, existing channel, etc.);
3. Finding: recognition of internal assets and lateralization;
4. Exploiting: Exploitation of a malicious payload, maintaining on the system and exfiltration of the data.

The kill chain helps to understand the operational scenarios, by exploiting vulnerabilities to implement techniques on supporting assets and how to prevent it by interrupting it as soon as possible. Being able to identify the most likely paths of an attacker to reach its target objective is mandatory in order to identify where to breach for a greater efficiency to lower the risks at reasonable cost.

5. Interface between top-down and bottom-up challenges

5.1. General overview

The Figure 6 below presents the proposed STEPs for connecting and adjusting information from Operational Scenario (OpeSce) and Vulnerabilities.

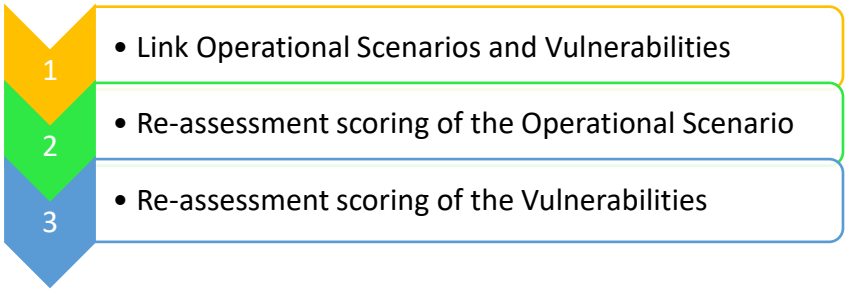

Figure 6: STEPS for connecting and adjusting information form Operational Scenario and Vulnerabilities

STEP 1 aims at establishing a link between OpeSce and Vulnerabilities. The objective is to define, for each vulnerability, on which attack path step (combination of a supporting asset and a technique) to associated it in an OpeSce. This can be done using different methods (manually, computer aided or fully automated). In this paper, the focus is done on the first 2 methods.

STEP 2 and STEP 3 are then to reassess the likelihood of the OpeSce and the CVSS scoring of the Vulnerability linked to OpeSce. The objective is to define if the new link has an influence on the valuation of the OpeSce and associated Vulnerabilities.

5.2. STEP 1: Link Operational Scenarios and Vulnerabilities

The objective of this STEP is to establish a link between vulnerabilities and the attack path step (combination of supporting asset and technique) of an OpeSce. The following scheme gives an overview of the method to realise this STEP.

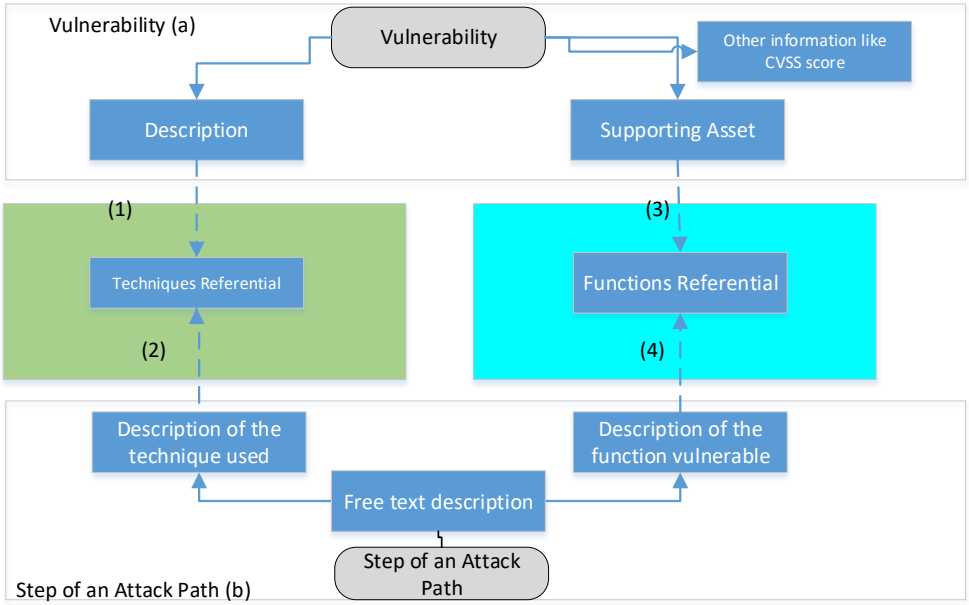

Figure 7: Solution to link OpeSce and vulnerabilities based on attributes

For a Vulnerability (a) (see Figure 7) the following attributes can be identified:

- Supporting asset;
- Description (of the vulnerability and how it can be exploited): Scoring like CVSS calculated in §3.2.

An OpeSce can contain one or several attack paths.

For every steps of an attack path (b) (see Figure 7) a free text description can be provided as no specific format has been adopted yet by the community. From that description the following information can be extracted and can be seen as attributes:

- Supporting asset function targeted by the attack;
- Technique used to do the attack.

2 attributes are being used in order to connect these 2 objects (Vulnerability and a step of an attack path):

- Technique (green in the figure);
- Function (blue in the figure).

On the general basis, theses 2 attributes are provided as a free text. The description does not follow any specific rules of writing or common referential. The objective is to propose multiple solutions for matching the 2 attributes.

Link the technique attribute

In order to link the "Technique" attribute, a referential as a way of establishing a common language is used. Such a referential can be e.g. ATT&CK matrix [17] or elementary threats from the BSI [7].

From Figure 7, in order to link the (1) and (2), multiple solutions exist, from manual to Assisted linkage:

1. The manual technique consists in the use of human knowledge.
   a. When describing a step of an attack path or a vulnerability referential of techniques shall be used.
   b. If it is not possible to categorize the description when producing the initial document then it can be done manually after. This is a very fastidious and time-consuming task.
2. Assisted linkage: It is a method based on texts alignment. The referential descriptions are inserted in a search engine. Using the Vulnerability description, as a question, the search engine ranks the possible techniques. Once validated by a human the Vulnerability description can be inserted in the technique description in the search engine. This feedback

loop starts to build a knowledge base and so improve the search engine results. Same process is done for the description of a step of an attack path (2) in Figure 7. Our results on linking the technique attribute are not homogenous and are very similar to the one in ENISA source [6]).

Link the function attribute

The link on "function attribute", it is now necessary to determine if the Vulnerability is impacting the function defined in the OpeSce. To establish this connection, we will rely on the logical architecture in the architecture document. This document describes with a top down approach and break the service into functions (and sub functions).
In the case of link (3) in Figure 6, the architecture document will help associating a supporting asset, linked to a vulnerability, to a supporting asset function.
For the link (4) in Figure 7, the function is associated to a function in the architecture document. And using the break down function the Vulnerability and the OpeSce step of attack path are connected.

This association can be done using similar technique as the one used for the *technique attribute* ie manually by a system engineer, or automated by using a database associating a supporting asset to its functions.

Automation based on non-compliance

As defined in 3.2, a vulnerability can have 3 origin types.

In case of non-compliance to the security baseline, it is possible to use the mapping from [7] to identify an elementary threat based on its related security control. This allows to automatically identify a technique (represented by an elementary threat using [7] wording) to an operational scenario based on a new vulnerability which is a non-compliance to a security control from the security baseline.

Using this approach allows to trigger updates of the associated attack paths and the risk assessment associated.

The limitation of the mapping proposed by [7] is that it requires an additional work to map each elementary threat to a tactic (step of the CKC) as defined in 4.2.

5.3. STEP 2: Re-assessment scoring of the Operational Scenario

Once some vulnerabilities have been linked to Operational scenarios, a process of likelihood assessment can start. The purpose is, knowing the existing associated vulnerabilities: does an attacker have more chance of reaching the objective?

Depending on the solution used to calculate the likelihood in the risk management process, the same solution needs to be replayed again for the re-assessment, this is in order to keep consistency. If the likelihood given to a scenario is validated by the management based on the experience of the security experts. For the re-assessment, this process needs to be replayed. The security experts will be gathered and their judgement will be used to re-evaluate the likelihood.

5.4. STEP 3: Re-assessment scoring of the vulnerabilities

In this step the objective is to re-assess the scoring of a vulnerability considering the information from the OpeSce. The gravity inherited by the OpeSce (through a strategic scenario) is used to prioritize the vulnerabilities remediation.

It is proposed to adjust the vulnerability scoring (defined in §3.2) by reflecting the gravity in the Environmental Metric Group. If a vulnerability is attached to multiple OpeSce then the max value of all gravity is taken.

6. Use case

This section is based on a Use Case that presents more concretely the proposed methodology. The Use Case is the following: A risk assessment has been already conducted. The system is in development phase and a penetration testing (pentest) has been conducted. The objective is then to assess how the vulnerabilities found during the pentest can affect Operational Scenarios. The data for the Operational Scenario and network architecture is part of the EBIOS RM training book [18].

6.1. Operational scenario (OpeSce)

This operational scenario describes a direct attack to the system in order to steal information. For the description of each step of the attack path, there are a technique used (in black) and an asset (in red).

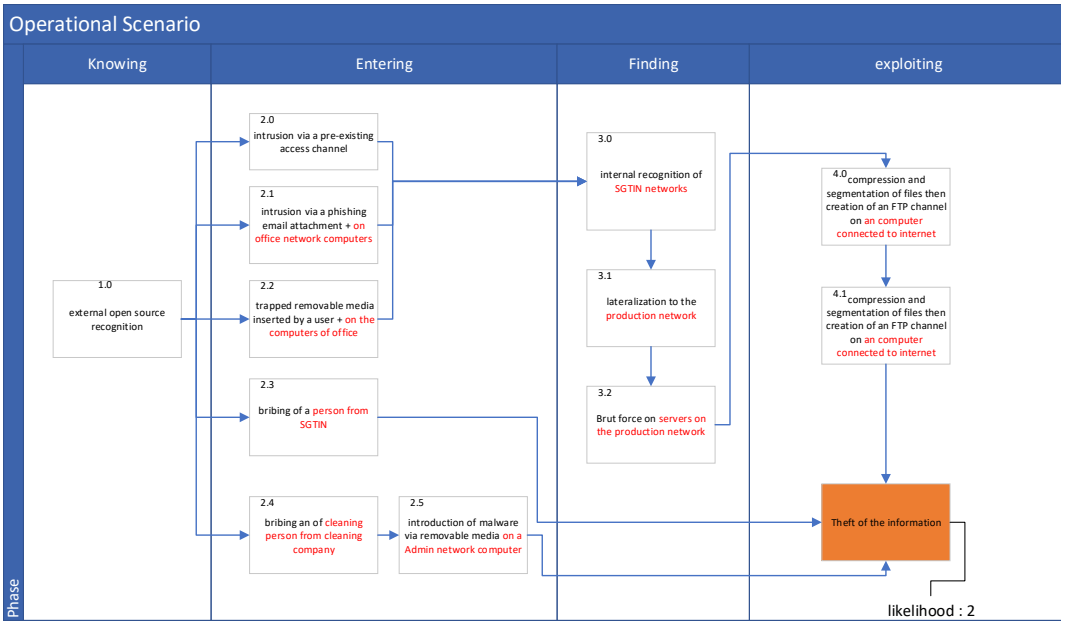

Figure 8: Example Operational Scenario

In order to be in a computational format, operational scenarios must be stored in an electronic format. They are saved in a database using the data model below (a simplified view).

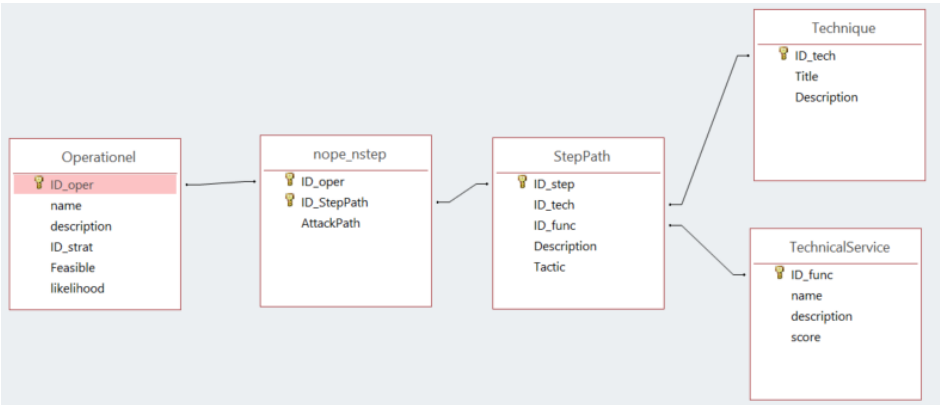

Figure 9: OpeSce Data model

6.2. Network architecture

This Network architecture describes the Information System of the example in Figure 10.

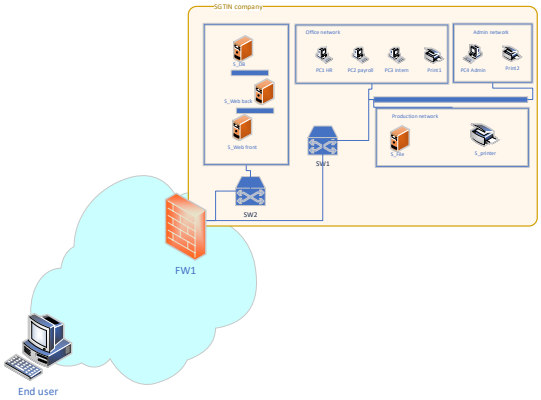

Figure 10: Example network architecture

In order to represent our architecture network in a computational format the concept of "CMDB" is used [19]. The CMDB model is made of different layers hardware, system, data, application, Service. The service layer contains entities to describe technical services (functions) and business services. The list of technical Service/Functions depends heavily on the modelling of the CMDB. In this example, "office Network" should not be seen just as a network but as a set of supporting assets that offer the technical service "office network".

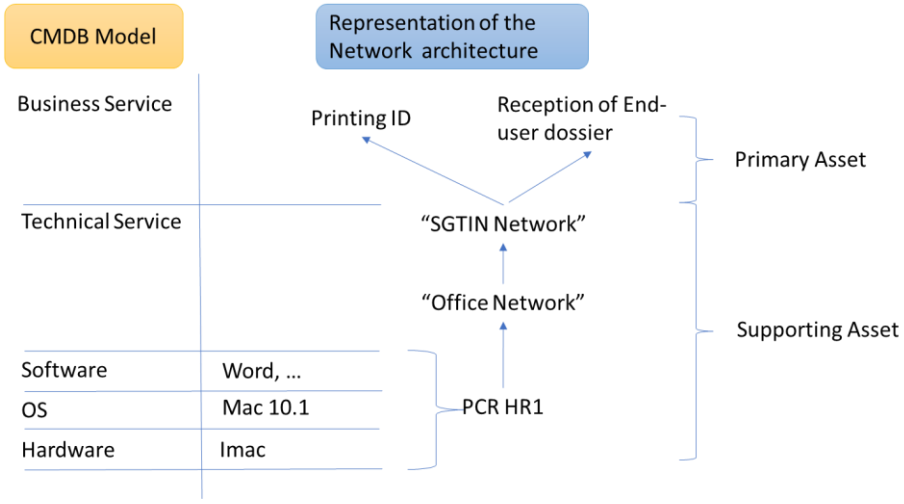

Figure 11: CMDB modelling of the architecture network

In the description of the operational scenario only items of the CMDB have to be used. The most used items are the one of the service layers.

6.3. Vulnerabilities

A list of vulnerabilities is built from several sources. For instance, the following vulnerabilities from Figure 12: Example list of vulnerabilities are identified as gathered from a pentest on the system.

name	description	constructor	product	firmware	CVSS
V1	SonicWall Analytics 2.5 On-Prem is vulnerable to Java Debug Wire Protocol (JDWP) interface security misconfiguration vulnerability which potentially leads to abuse of command and script interpreters to execute	sonicwall	tz500	6.2	10
V2	unauthorised port open on webserver	Microsoft	Windows server 2010		10
V4	weak Password policy, not in line with the security baseline. All Dell equipment impacted	Dell			10
CVE-2021-38539	NETGEAR with 1.6.0.4 firmware or before are vulnerable to privilege escalation due to code RCE.	netgear	ProSafe GS108PE	1.6.0.4	6
PT-08	NETGEAR switches with 1.6.0.4 firmware LAN (VLAN) switches allow remote attackers to inject 802.1q frames into another VLAN by forging the VLAN identifier in the trunking tag.	netgear		1.6.0.4	8
CVE-2021-1228	A vulnerability in the fabric infrastructure VLAN connection establishment of Netgear ProSafe Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to	netgear	ProSafe GS108PE	1.5.0.2	6
PT-16	Port lockdown missing on Mac equipment, the attacker may use this non lockdown to insert a non authorised removal media as USB key, CD...	Mac	iMac		10

Figure 12: Example list of vulnerabilities

6.1. STEP 1: Link Operational Scenarios and Vulnerabilities

The vulnerability PT16 from Figure 12, is used as an example in this step.

Identify the technique attribute

Using the description of PT16, it is needed to identify the associated techniques and the tactics. For that, the text search engine of the database (DB) is used (Figure 13). The DB proposes a list of possible techniques with associated tactic (Figure 14).

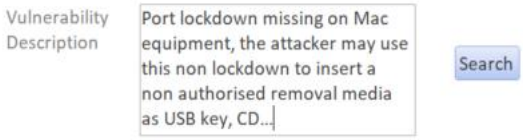

Figure 13: Example Vulnerability search box

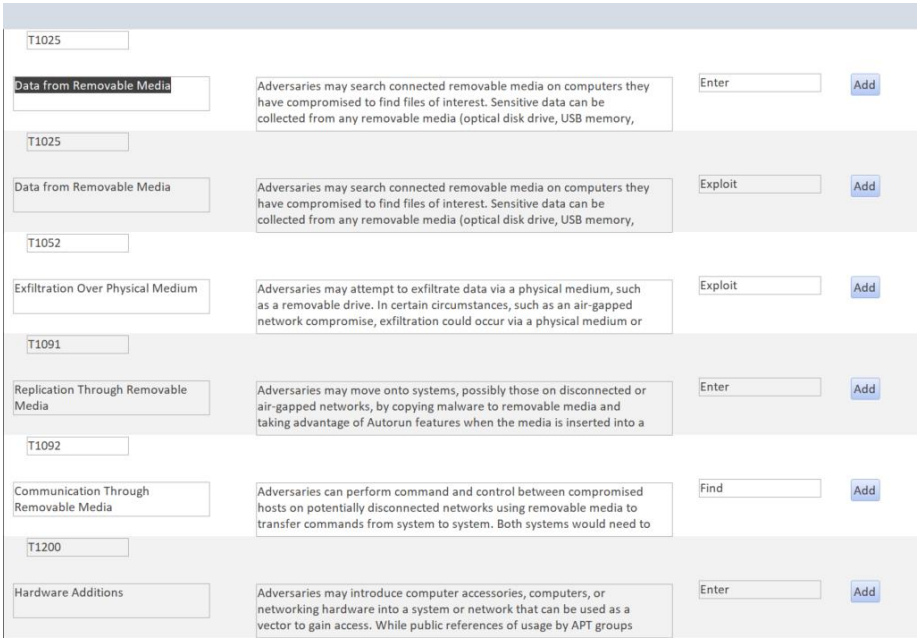

Figure 14: Example Proposition of list of techniques

Identify the functional attribute

For the PT16 vulnerability, a query is conducted in the CMDB for asset/Configuration Item from the CMDB PC1-HR. The DB query return a set of technical services to retain.

- "Office network"
- "SGTIN network"

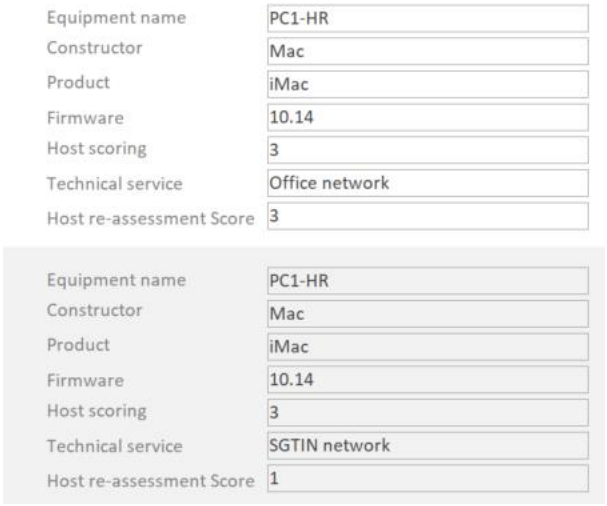

Figure 15: Example Technical services

Identifying the steps of the Operational Scenario.

Once we have identified the Technique attribute and the technical service/functional attribute of a vulnerability a query can be built in order to retrieve the steps of Operational scenarios.

Vulnerability.name	Vulnerability.Description	ID_tech	ID_Path	get steppath realisable.Description	TechnicalService.name
PT-16	Port lockdown missing on Mac equipment, the attacker may use this non lockdown to insert a non authorised removal media as USB key, CD…	T1025	2.2	Trapped removal media inserted on a computers of the office network	Office network

Figure 16: Example match between vulnerability and Operational Scenario

6.2. STEP 2: Re-assessment scoring of the Operational Scenario

The step 2.2 of the attack path is impacted by the vulnerability PT16. This scenario with the all identified vulnerabilities are then presented to security experts who will re-evaluate the likelihood of the scenario. In our case, has the vulnerability taken as example is impacting a enter tactic the likelihood could increase.

7. Conclusion

This paper proposes an interface for both processes of risk management and vulnerability management. It presents information flows that can be exchanged between operational scenarios and vulnerabilities and a proposition of format for operational scenarios description allowing automation

In order to interface those processes, two challenges have been identified (top-down approach challenge §2.1 and bottom up challenge §2.2) in order to exchange information.

The described approach has been set up and is used operationally. It is partially automated and areas of improvement have been identified. The main problem faced is the lake of consistency in description of Operational Scenarios and the description of vulnerabilities. That is why an emphasis on using referential (CMDB) and MITRE ATT&CK are important. The other challenge is to improve the accuracy of the CMDB (have all elements of the network architecture) and a description at technical service level.

8. References

[1] I. 27005, “ISO 27005 - Information technology - Security techniques - Information Security Risk management,” International Standard Organization, 2018.

[2] M.U.Aksu, M.H.Dilek, E.I.Tatli, K.Bicakci, H.I.Dirik, M.U.Demirezen, T.Aykır, “A Quantitative CVSS-Based Cyber Security Risk,” in *2017 International Carnahan Conference on Security Technology (ICCST)*, Madrid, Spain, 23-26 Oct. 2017.

[3] Wenrui Wang; Fan Shi; Min Zhang; Chenxi Xu; Jinghua Zhend, “A Vulnerability Risk Assessment Method Based in Heterogeneous Information Network,” IEEE, Hefei, China, 10/08/2020.

[4] FIRST, “Common Vulnerability Scoring System Version 3.1,” FIRST, [Online]. Available: https://www.first.org/cvss/v3-1/. [Accessed 5 May 2021].

[5] L. Martin, “The Cyber Kill Chain,” 31th May 2021. [Online]. Available: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

[6] ENISA, “State of Vulnerabilities 2018/2019,” ENISA, December 2019.

[7] BSI, “IT-Grundschutz-Kompendium,” Federal Office for Information Security (BSI), Bonn, Germany, Feb. 2021.

[8] BSI Standard 100-2, IT-Grundschutz Methodology, 2.0 ed., Bonn: Bundesamt für Sicherheit in der Informationstechnik (BSI), 2008, p. 93.

[9] ANSSI, “EBIOS Risk Manager, version 1.1,” Paris, Agence Nationale de la Sécurité des Systèmes d'Information, 2018, p. 49.

[10] A. Kuppa, L. Aouad and N.-A. Le-Khac, “Linking CVE’s to MITRE ATT&CK Techniques,” in ARES, Vienna, 2021.

[11] MITRE, “CVE MITRE,” [Online]. Available: https://cve.mitre.org/. [Accessed 5 May 2021].

[12] ISO 30111, «Information technology - Security techniques - Vulnerability handling,» International Standard Organization, 2020.

[13] ISO 29147, “Information technology - Security techniques - Vulnerability disclosure,” International Standard Organization, 2020.

[14] NIST, “Official Common Platform Enumeration (CPE) Dictionary,” NVD, [Online]. Available: https://nvd.nist.gov/products/cpe. [Accessed 5 May 2021].

[15] I. 27001, “Information Technology - Security techniques - Information Security Management Systems - Requirements,” International Standard Organization, 2013.

[16] Microsoft, “Disrupting the kill chain,” 28 11 2016. [Online]. Available: https://www.microsoft.com/security/blog/2016/11/28/disrupting-the-kill-chain/.

[17] MITRE, “ATT&CK Enterprise Matrix,” 29 04 2021. [Online]. Available: https://attack.mitre.org/matrices/enterprise/.

[18] ANSSI, FORMATION EBIOS RISK MANAGER, Paris, 2021.

[19] O. o. G. Commerce, ITIL v3 Service Transition Book, TSO (The Stationery Office), 2007.

[20] NIST, “Glossary - Vulnerability Management,” 31th May 2021. [Online]. Available: https://csrc.nist.gov/glossary/term/Vulnerability_Management#:~:text=Definition(s)%3A,extend%20compromise%20to%20the%20network..

[21] FIRST, “List of Potential Improvements for CVSS v4.0,” [Online]. Available: https://docs.google.com/document/d/1qmmk9TQulW9d1cuipu_ziXDX0pUswbZ1WSQyynHbvKU/edit#heading=h.ynfuvu3y72hy. [Accessed 11 September 2021].