Tomi Poutanen

Automation of Telecom Network Vulnerability Management

Risk Driven Approach

Metropolia University of Applied Sciences

Master of Engineering

Information Technology

Master's Thesis

5 December 2021

PREFACE

Taking on the school lessons and writing out this thesis while working full time ended up being quite a challenge. Managing time between all the interesting work activities, while leaving some time to learn new things, was a struggle.

The COVID-19 pandemic, working from home, highlighted the importance of secure global communications networks. Traffic is sometimes considered to be priority one in networks. Each new generation of mobile networks starts with the news on broken speed records. Luckily more and more the attention is turning to the invisible side of the networks. The advanced and automated functionalities, which are not visible to the normal consumers. I am excited to see security being one of them and it has been exciting to see the growth of our product and at the same time work with the future of it.

Especially valuable, for the progress of my thesis, has been working in the customer interface, hearing the pain points of our customers. This has ensured me in that the research will be valuable to our organization and then the world of telecommunications security.

I wish to express my gratitude to Anu Puhakainen, my supervisor, and Harri Hakala for sharing their expertise in the subject. I also want to express my appreciation to Kaisa Korhonen and Tapio Vuorinen for the information shared on the Vulnerability Management Service.

Special, warm thank you, to my friends and colleagues working in Product Security.

Remember, security first, then cake.

Espoo December 5, 2021
Tomi Poutanen

Abstract

Author:	Tomi Poutanen
Title:	Automation of Telecom Network Vulnerability Management, Risk Driven Approach
Number of Pages:	40 pages + 1 appendix
Date:	5 December 2021
Degree:	Master of Engineering
Degree Programme:	Information Technology
Professional Major:	Information Technology
Supervisors:	Anu Puhakainen, Strategic Product Manager Harri Hakala, Security Specialist Ville Jääskeläinen, Principal Lecturer

---

Many network assets use some free and open-source software (FOSS) or commercial off-the-shelf software (COTS) to provide industry standard services or functionality. This makes vulnerability management a crucial part of network security, same applies also to telecommunication networks.

Modern, highly complex, telecommunications networks are constantly evolving and use of old methods in managing vulnerabilities, risks, in the networks will not work much longer. At the same time the number of possible vulnerabilities is increasing year by year.

This thesis helps commissioner company to map the information in the pre-existing systems and services in a way that brings most value to the operators. Limiting the visibility to the risks, vulnerabilities, that really matter. This will allow efficient use of resources.

The thesis is limited to the Security Manager and Vulnerability Management Service database integration, this was also the first to be implemented in the study. Integration of external vulnerability feeds and scanner reports were excluded. Excluded were also the connectivity from operator networks towards the vulnerability management database and the UX/UI layer. Most of these will require further studies.

Key finding was that the integration is possible. Data structures in both systems are compatible and the only limitation currently left out is the connectivity.

Keywords: Vulnerability management, security automation, vulnerability management service, risk management

Contents

List of Abbreviations

3GPP	3rd Generation Partnership Program.
3PP	3rd Party Product
5G	5th Generation (mobile network).
5GC	5th Generation Core (mobile network).
CIS	Center for Internet Security.
CSP	Cellular Service Provides.
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System.
ENISA	European Union Agency for Cybersecurity.
ESM	Ericsson Security Manager.
EVMS	Ericsson Vulnerability Management Service
FIRST	Forum of Incident Response and Security Teams.
IS/IT	Information Systems/Information Technology.
ISO	International Organization for Standardization.
NIST	National Institute of Standards and Technology.
NSCS	National Cyber Security Centre.
PSIRT	Product Security Incident Response Team.

RM	Risk Management.
RBVM	Risk Based Vulnerability Management.
SOC	Security Operations Center.
VA	Vulnerability Assessment.
VM	Vulnerability Management.
VMS	Vulnerability Management System.

1 Introduction

According to European Union Agency for Cybersecurity (ENISA) “Mobile telecommunications networks remain under daily attack” [1]. While the attacks to the traditional Information Systems/Information Technology (IS/IT) networks and services might hit the news more often, the telecommunication networks are also constantly targeted by different kind of attempts to gain unsolicited access. Target of these malicious users varies from gaining reputation, getting financial benefit to considerable data extraction.

Telecommunications networks have traditionally been closed. Modern mobile networks however are opening and using more and more open interfaces and commonly available software components.

Mobile networks are secure by default. But since all software is designed, developed, delivered and operated by humans, mistakes happen, risks are introduced. To manage these risks Ericsson, the commissioner of this research, has developed a tool that addresses the pain points of Cellular Service Providers (CSPs).

> Ericsson Security Manager (ESM) provides industry standards-based security policy driven security automation, compliance monitoring and security analytics functions. ESM helps to automate security controls, maintains them in desired level even in changing threat landscape and shortens the average reaction time to respond to possible breaches. [2]

Network protection includes many different aspects, still there is no single method to mitigate all potential risks. Today, one of the hottest trends in network security appears to be active or periodic scanning for vulnerabilities. This, setting a Common Vulnerability Scoring System (CVSS) score threshold and attempting to blindly mitigate, patch, all vulnerabilities above that score, is not the way to best results. This approach wastes resources, more on that in section 3.

Vulnerability management process that provides coverage for all assets can and should have many external vulnerability intelligence sources, such as different National Cyber Security Centre (NSCS) feeds. The focus of this thesis is on processing of the valid vulnerabilities, vulnerabilities that are both observed and exploited and reported through the Ericsson Vulnerability Management Service (EVMS). EVMS is maintained by Ericsson Product Security Incident Response Team (PSIRT) organisation. Next challenge is in visualising the assets at most risk and in need of attention. This, again, depends on the asset, the exposure and criticality and the risk generated by the vulnerability. The purpose of this research is to act both as a pre-study for the development of new functionality for ESM and basis for training material for the same value pack.

1.1 Telecom Operators and Security

Telecommunication Operators, CSPs, commonly operate in multiple different domains. They have the visibility to the open internet and the trends, best practices and must haves therein. This is causing increased demand on better, telecommunication specific, visibility to the security posture, risks, across all the telecommunication network domains.

Networks are constantly changing and evolving. Yearly or monthly security scans performed in the network are no longer sufficient. CSPs expect to get frequent updates on active vulnerabilities, risks, in order to be able to plan the mitigation of them. All this must happen in a timely manner, before those vulnerabilities can be exploited.

1.2 Research Question

The research question of this study is as follows.

How to best ensure telecom operator visibility to the valid vulnerabilities in the network assets?

The objective of this thesis is to find out how Ericsson Security Manager can best be integrated to EVMS. How the data structures in both systems can be matched and be utilized in providing accurate and timely information on vulnerabilities that pose a real risk.

1.2.1 Out of Scope

Research area has a lot of subareas that could potentially be researched indefinitely, but to keep the scope manageable some limits have been set. Not in scope of this research

- Vendor specific vulnerabilities.
- External vulnerability feed integration.
- Vulnerability scanner report integration.
- Integration with other ESM functionalities
- Data structures inside commissioners' products
- Protocol recommendation between ESM and EVMS

In addition to these, implementation specific information has been excluded from the external version.

1.2.2 Scoped In

Main interest for the research is in ESM and the value that the new functionality brings to the customers. How vulnerability management can be bound together with the other functionalities and how to limit the number of reported vulnerabilities only to the valid vulnerabilities when known and commonly used software and software components are used.

1.3 Research Approach

Research assisted development was selected as the method since the aim of the commissioner organisation was the development a new functionality for an existing security product. The beginning of the research was spent on collecting information and external references. Commissioner company's internal material has been excluded from this, public version of the research. Since the aim of the research was development of new value package, the development teams were kept in the loop and development backlog development items were generated and updated as needed.

Most critical step in the research was scope setting. What is essential for the research to be able to develop a prototype product and what can be excluded at this point. Research would easily have been expandable to cover the additional content, but the research would not have been successful in the time given by the organisation. All excluded parts will need separate studies to conducted on them.

Research process was linear in nature, starting situation was clear. Both ESM and EVMS are extremely well documented products, including all the interfaces and data structures they provide.

Automating the vulnerability data visibility to CSPs must bring value. Sending too many alerts, events and notifications on possible vulnerabilities that do not pose a real risk, will only decrease the value of the tool. Concentrating on the vulnerabilities that are critical and valid, decreases event fatigue and brings in the best results.

Figure 1 below illustrates the research process overview.

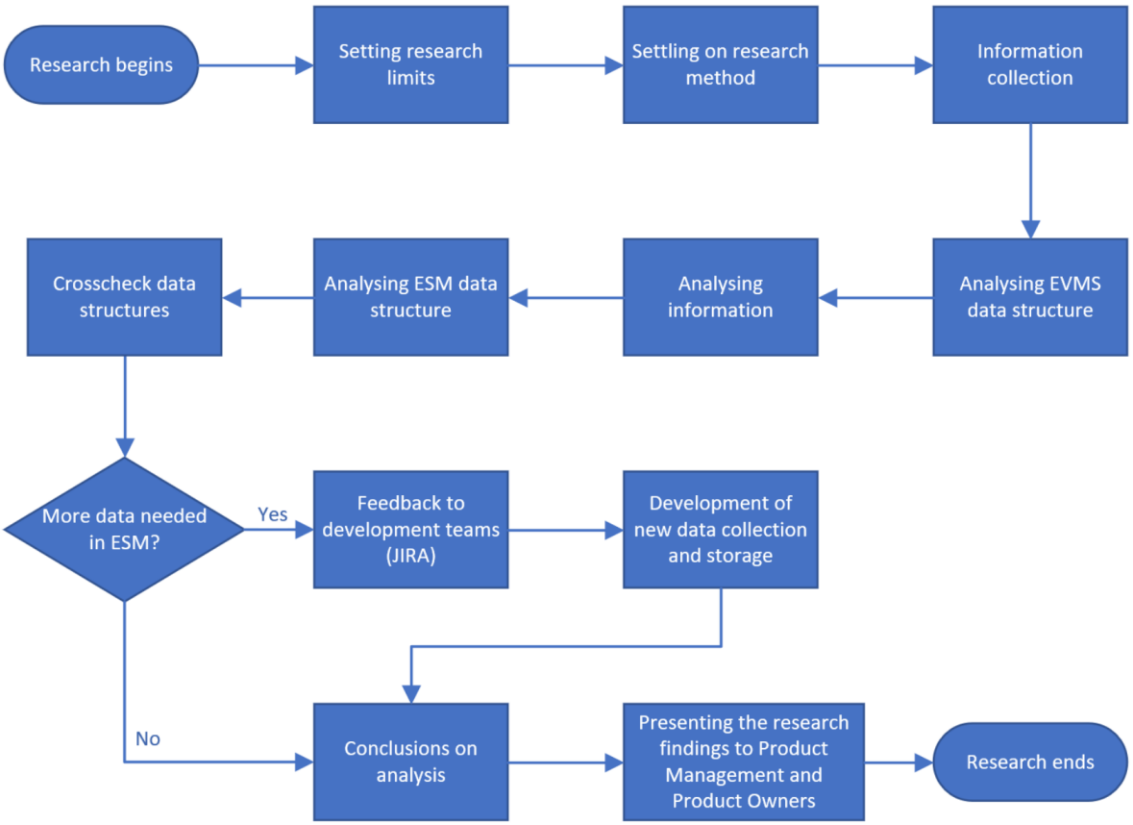

Figure 1. Research process

In order to keep the amount of research reasonable, limiting the study is crucial activity. Research is limited only to the integration of ESM and the vulnerability data available in EVMS. Additional interfaces and integrations were identified but scoped out from this research.

1.4 Research Commissioner

Research was assigned by Ericsson Finland. Security Solutions organisation in Ericsson Finland is responsible of developing, delivering and supporting CSPs around the world with the security automation tools.

Due to the nature of the commissioner's role in the global telecommunications field, some parts of the research are only for internal use and excluded from the public version.

1.5 Structure of Research

The thesis has been divided into 7 sections. The first section gives a short introduction to the problem. The second section describes the research method and sources of material for it. In the third section the thesis introduces the needed basics for vulnerability management, from vulnerability to impact of them and what to prioritize. The fourth section explains the Ericsson Vulnerability Management Service (EVMS), what is it for and how does it work. In the fifth section one gets an introduction on Ericsson Security Manager, what is it and how the integration with EVMS should work. Next section, sixth section, combines the information learnt in the previous 2 sections and explains the Ericsson Security Manager – Automated Vulnerability Management functionality in, as much as possible, detail. Last section, the seventh section, explains the outcome of this research in compact form, what should be implemented and how.

2 Research Material

This section first introduces how the different input material was collected and analysed. Then the inputs from industry frameworks, standards and reports were collected.

2.1 Data Collection and Analysis Methods

Most important source of relevant information for this research was commissioner company's internal documentation. The documentation describing the different data structures, databases, interfaces and information therein. Both Ericsson Security Manager and Ericsson Vulnerability Management Service contain sensitive information and Ericsson Intellectual Property (IP), this means that the research will not be able to illustrate or describe many things in detail. Some things are described in general terms, on a level that many other vendors, commercial or not, describe their products.

2.1.1 Industry Frameworks and Reports

NIST, CIS, ISO, ENISA, 3GPP, FIRST and various CERT organizations have all published standards, frameworks, scoring systems, recommendations and research material on the area of Vulnerability Management, Vulnerability Assessment (VA) or Risk Management (RM). These common frameworks and ways of working ensure that all players on the field talk about the same things.

For the commissioner company the overarching internal framework called Security Reliability Model (SRM). Please see [3] for more details on the SRM. Figure 2 below shows how the SRM applies throughout the lifecycle of all network elements, assets, provided and developed by the commissioner company.

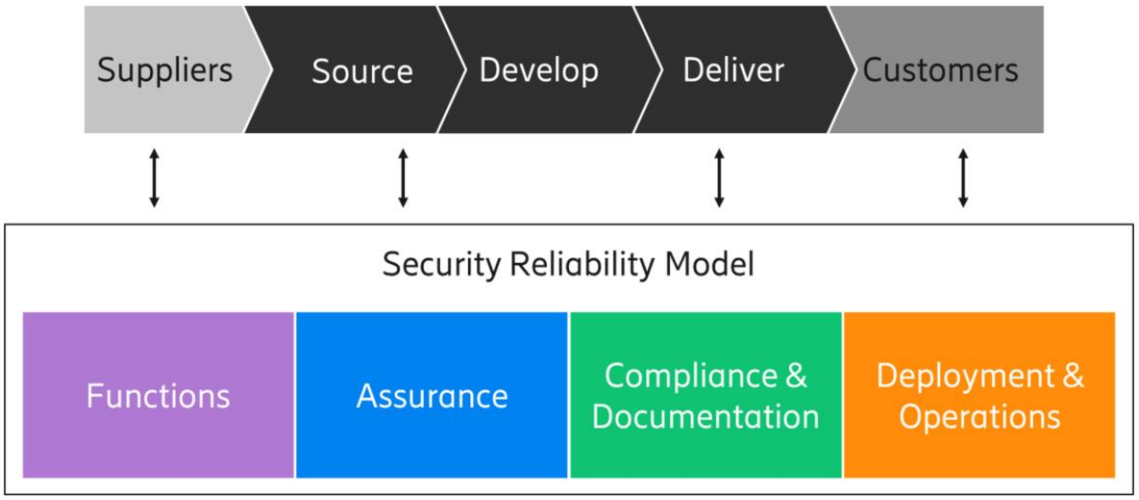

Figure 2. SRM interacts with all stages of the commissioner company's value flow. [3]

All mentioned frameworks mention and highlight the importance of continuous vulnerability management. It is not sufficient that vulnerabilities in any network are mitigated at the time of software release, but it is important to continue the process daily after the deployment, during operational time all the way until decommissioning. This is, if possible, even more important in telecommunications networks.

The practical part is completely left out of the frameworks. The question "how do you do it?" is left unanswered. It is up to the organisation to decide how to best implement vulnerability management process during the time that the assets are deployed and operational in the network.

2.1.2 Other Data

Cyber security is a field which has evolved throughout its approximately 30 years of existence and continues to do so. There is plenty of studies, research and other source material available for any segment of the field. No matter how specific or peculiar the subject is.

One could also notice that there are a lot of bachelor's and master's thesis written, in Finland, on cyber security and network security.

2.2 Reliability and Validity

All information in this research is founded on cyber security frameworks, standards and commissioner company's processes. New functionality will support customers in automating the existing procedures and processes. This, removing some of the human factor in the risk management process, ensures that risks management, mitigation and treatment, can be executed in a repeatable and reliable way. Information processed by EVMS and the customers has been and remains to be extremely important from business continuity perspective.

Research results are valid and implementable. Information, on which the research is based, rely on industry standards, recommendations and best practices.

3 Principles of Vulnerability Management

This section describes the basics for Vulnerability Management that are needed to understand this research.

3.1 Vulnerability – What is it?

There are several different types of vulnerabilities. Asset can be vulnerable due to a bug in the software or service running on it. It can also be vulnerable if the secure program or service is not configured according to up-to-date security hardening guidelines. According to NIST a vulnerability is a “Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source”. [4]

Vulnerability Management is often combined with term Risk Management. Each unprocessed vulnerability is a potential risk for the network operator. All unacceptable risks, based on the risk rating, should be treated. But for that to be even possible one will first have to know what risks one might have.

All vulnerabilities published as part of the CVE program are given two things. The first one is a Common Vulnerabilities and Exposures (CVE) vulnerability ID. This ID is used to identify and distinguish different vulnerabilities from each other. The second thing every CVE gets is a Common Vulnerability Scoring System (CVSS) score. Valid range for this score is from 0,1 to 10. To put it simply: bigger the score, easier it is to exploit and more severe the impact is. This is dramatically oversimplified, there are exceptions to this, but will act as a principle for our use. This is a fact, but not the whole story. More on the vulnerability prioritization or risk in the section 3.6 below. Additional information on the CVSS scoring also available on the FIRST.org CVSS user guide. [5]

3.2 Why to Have Vulnerability Management

Vulnerability management is important throughout the lifetime of the asset. It starts when asset is being developed and continues until the asset is decommissioned. One reason for an CSP to have a vulnerability management process is usually requirements from regulators and possible legislation. Alternatively, on many occasions the organisation would also encounter the same requirements when aiming for compliance for any of the Information Security Management Systems (ISMS).

> One of the most widely used standards in the extensive ISO family, ISO 27001 provides guidance on cybersecurity management, including vulnerability management as well as information security risk assessment and risk management. [6]

Without Vulnerability Management network asset owner do not have proper visibility to the potential risks that are exposed at any given point in time. Vulnerability Management, combined with up-to-date asset inventory information, is mandatory in modern, complex, telecommunications networks.

> Vulnerability management is not a single tool or resource. It’s an ongoing program with people, policies and processes that work together toward common goals to ensure your attack surface and cyber risk are as small as possible. [7]

Commissioner company has a process also for vulnerability management. It is one, essential, part of the Security Reliability Model (SRM). Please find an overview of the SRM process in Figure 3 below. Even though managing vulnerabilities is essential throughout the life of a network asset, greatest significance for it is during the Deployment & Operations time. This is also exactly the time when ESM is monitoring the assets in the customer networks.

Figure 3. Ericsson SRM, risk management process [3]

Continuous process - that is common for all the risk management processes. For one example of generic risk management process, please see Appendix 1 - General Risk Management Process.

3.3 Vulnerabilities in Telecommunications Networks

Modern 5th generation mobile networks are built mainly with containerized network functions. As mentioned already earlier these networks are secure by default, but where there is network, there is also risk. Software running in these containers might still partially be 3rd party developed. The infrastructure, hardware, on which the networks are running is generic IS/IT servers. The software and services deployed on the hardware, even though not exposed to external networks, contain vulnerabilities.

When considering the older mobile network technologies and network assets, which might not even be maintained anymore, risks increase dramatically. Unmanaged risks and software, when exposed to malicious actors, be just what is needed to gain access to the network. After gaining access, it might be easier to move laterally inside the network.

3.4 Impact of a Vulnerability

Explaining the impact of a vulnerability is not easy. It varies a lot depending on many of the same points that are used to determine the CVSS score for a vulnerability.

Basic principles can be explained by two different examples. First, if the vulnerability can be easily exploited remotely and it provides a way for the malicious user to easily shutdown an asset or part of the network, the impact of it might be dramatic. Potential loss of mobile network service or for example lowered quality of service is not acceptable in any scenario. Then if the vulnerability requires that the exploit is triggered while tampering the server hardware, in customers server room, risk and potential impact is considerably smaller.

Above, extreme examples, combined with the fact that the telecommunication network assets are not the same as IS/IT network assets. This also means that the same rules and principles of vulnerability management can not be directly applied. Telecommunication networks use special software, interfaces and protocols. In addition telecommunication assets often use normal, known and commonly used, software and software components to implement functions.

Using known and commonly used software components is justified. Commonly used software is thoroughly tested and usually also well maintained. But the use cases in telecommunications networks are special and software configurations do not match the configurations in normal IS/IT systems and services. These, different use cases, limited configurations, special operating systems and different deployment environment, create a scenario that is prone for false positive results in the IS/IT vulnerability scanning reports.

False positive means that a vulnerability has been discovered when it in reality has not. It is a common occurrence in vulnerability scans.

> A False Positive is when you think you have a specific vulnerability in your program but in fact you don't. Many security scanners such as Nessus scan an application (or service/daemon) and attempt to find a vulnerability in it. Sometimes the signatures (the 'check logic') make mistakes and report a vulnerability that may not exist. [8]

Getting a vulnerability report for an telecommunications asset must not be taken with the face value, all the information in it has to be analysed and in the context that it was found in. So, having a vulnerability of 9.x CVSSv3.1 score might not be that critical in the telecommunication network context where many things are either disabled, made useless or the implementation differs from normal. Naturally there is a chance for the opposite too.

3.5 Telecom Operators Perception on Vulnerabilities

All telecommunication service providers acknowledge the risks introduced by the possibility of vulnerabilities. Still, depending on the maturity of the organization, the approaches to vulnerability management vary considerably.

There are CSPs, which only concentrate on the CVSS score of each CVE. More mature CSPs usually take more risk-based approach. More about this approach in the section 3.6.

Differences on the approach on cyber security do not limit on the vulnerability management. Transparency on security practices and requirements appears to be good indication on how seriously security is taken in the CSP.

Some operators have their security policies visible for all to see. KPN, a Dutch telecommunications company, has their KPN Security Policy (KSP) [9] visible for all to see on their web pages. KSP has several requirements relating to vulnerabilities, including but not limited to vulnerability management, vulnerability scanning and vulnerability mitigation.

Another example of an operator that has public security policies is Deutsche Telekom (DT). DT security requirements can be downloaded from ‘Privacy and

Security Assessment process' -web page [10]. Similarly, to KSP, the DT security policy has references to vulnerability management and mitigation.

Above two CSPs are good examples of operators who take security seriously. This approach has come from the world of IS/IT systems and now it is time for the telecommunication vendors to respond to the same call.

3.6 Vulnerability Prioritisation

Every year thousands and thousands of vulnerabilities are reported and analysed. It is a mission impossible for any organisation, enterprise or CSP to try and mitigate all of them. In reality they should not even need to attempt that.

Why should CSPs put any effort in vulnerability mitigation if the vulnerability is impossible to exploit? Another question often asked is: has this vulnerability, with CVSSv3 of 8.6 been patched from asset A? Answer to the first one is simple: they should not. Second one is more complicated.

CVSS score is not an indication of actual risk. Latest FIRST.org CVSSv3.1 user guide also acknowledges this by stating "CVSS Measures Severity, not Risk" [6]. Same guide goes on:

> CVSS Base Score should be supplemented with a contextual analysis of the environment, and with attributes that may change over time by leveraging CVSS Temporal and Environmental Metrics. More appropriately, a comprehensive risk assessment system should be employed that considers more factors than simply the CVSS Base Score. Such systems typically also consider factors outside the scope of CVSS such as exposure and threat [6].

So, prioritization of vulnerabilities blindly based only on CVSS score is not the way to go. Instead of the score the environment, exposure, threat and asset criticality, to mention few additional factors, should be weigh in and be calculated in to the actual risk score of the vulnerability. Then by beginning the vulnerability management journey from the vulnerabilities posing the most risk, CSPs can get best value for the work done.

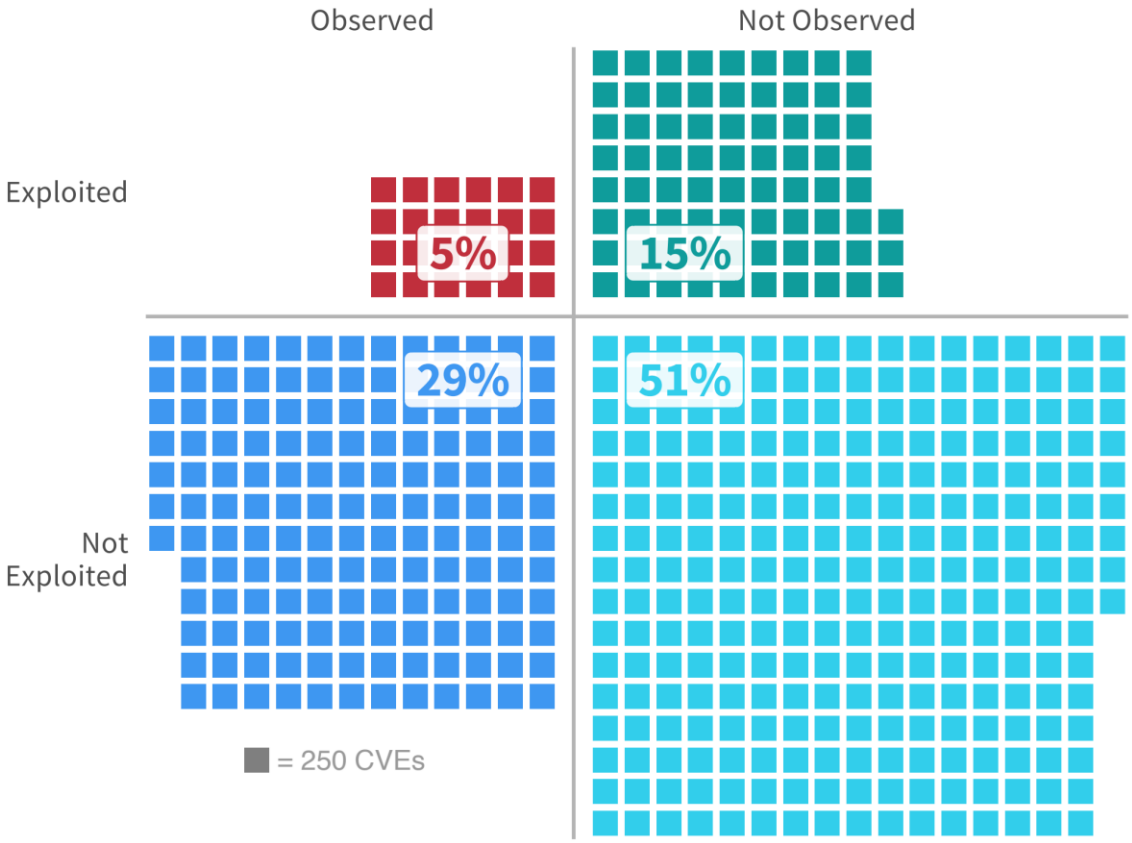

Figure 4. Ratio of observed/not observed and exploited/not exploited vulnerabilities [11, p. 5].

Above Figure 4 shows the current split between the four main groups of vulnerabilities. If the vulnerability management and mitigation activities can successfully be focused on the observed and exploited quadrant, then the organisation is spending least resources to get the maximal benefit. In the end the mitigation effort still needs resources, mostly time and money. All resources spent on mitigating a vulnerability that is never exploited or observed is wasted. This, focusing the mitigation effort, is especially important since all the cyber security budgets, before any security incidents, are slim at best.

4 Ericsson Vulnerability Management Service

Ericsson Vulnerability Management Service (EVMS) is operated by Ericsson Product Security Incident Response Team (PSIRT) organization. Following sections will describe both abbreviations more.

4.1 Ericsson PSIRT

As other PSIRT organisations, Ericsson PSIRT, among other responsibilities, owns and is responsible of the vulnerability management process (see Figure 5 below).

Figure 5. PSIRT Vulnerability Management Process [12, p. 5]

The purpose of the Ericsson Vulnerability Management Service (EVMS) is to minimize the risks of impacts from product vulnerabilities on customer assets. All Ericsson developed and maintained products are managed and controlled by a common Ericsson Vulnerability Management. The ambition is to be the most reliable, communicating accurately and acting quickly on vulnerability analyses and delivering solutions according to plans.

The Ericsson Vulnerability Management Service (EVMS) is a service provided by Ericsson PSIRT for monitoring product vulnerability status of all Ericsson developed products. PSIRT continuously monitors for new vulnerabilities and security updates published in various feeds and stores the information into the EVMS database, see Figure 6 below. More details on Ericsson PSIRT and EVMS in the FIRSTCon21 talk: Product Security Vulnerability Management Metrics are Hard [14, 11min 10sec]. Each individual release of a product, network asset, is created in EVMS with the internal software components.

Due to the sensitivity of the information in the system, pictures below have been cropped and detailed information on the data structures and interfaces have been left out of this research.

Figure 6. Example of EVMS data for one asset.

Vulnerabilities (see Figure 7 below) are then mapped to Ericsson products, and notifications are sent to registered users. All related organizations (PSIRT, Product Development (PDU), 3rd Party Products (3PP) Technology, Customer Support etc.) are working as a trusted intermediary between the vulnerability discovered, affected operators, 3PP vendors and the public. At this stage the vulnerability does not yet have any vendor specific information. Same information can be found in external, public, sources. As an example, the SUSE Linux Enterprise vulnerability info mail list post [13], same vulnerability shown in the Figure 7 below.

Date Created	2020-10-14 07:50:12
Date Published	2020-10-14 09:13:22
Revision	A
Priority	Medium
Slogan	SUSE 15, 15-SP1, 15-SP2: Security update for bind (SUSE-SU-2020:2914-1)
Vendor Solution	Install vendor's patches.
Vendor Reference	SUSE-SU-2020:2914-1
Reference Links	http://lists.suse.com/pipermail/sle-security-updates/2020-October/007552.html
Description	SUSE has released an update that fixes 12 vulnerabilities in bind. Affected products: SUSE Linux Enterprise Server for SAP 15 SUSE Linux Enterprise Server 15-LTSS SUSE Linux Enterprise Module for Server Applications 15-SP2 SUSE Linux Enterprise Module for Server Applications 15-SP1 SUSE Linux Enterprise Module for Development Tools 15-SP2 SUSE Linux Enterprise Module for Basesystem 15-SP2 SUSE Linux Enterprise Module for Basesystem 15-SP1 SUSE Linux Enterprise High Performance Computing 15-LTSS SUSE Linux Enterprise High Performance Computing 15-ESPOS

JLNERABILITIES

CVE ID	Description	Base Score	Temp Score	Actions
CVE-2020-8623	In BIND 9.10.0 -> 9.11.21, 9.12.0 -> 9.16.5, 9.17.0 -> 9.17.3, also affects 9.10.5-S1 -> 9.11.21-S1 of the BIND 9 Supported Preview Edition, An attacker that can reach a vulnerable system with a specially crafted query packet can trigger a crash. To be vulnerable, the system must: * be running BIND that was built with "--enable-native-pkcs11" * be signing one or more zones with an RSA key * be able to receive queries from a possible attacker	7.5	6.9	

Figure 7. Vulnerability details from EVMS.

Data in EVMS is always up to date. And since it has been validated by Ericsson PSIRT and PDUs it contains more valuable information to the operators. The answered vulnerability entry in EVMS includes the information on the possible mitigation of the vulnerability and if patch is needed. Please see an example of an EVMS view below in Figure 8.

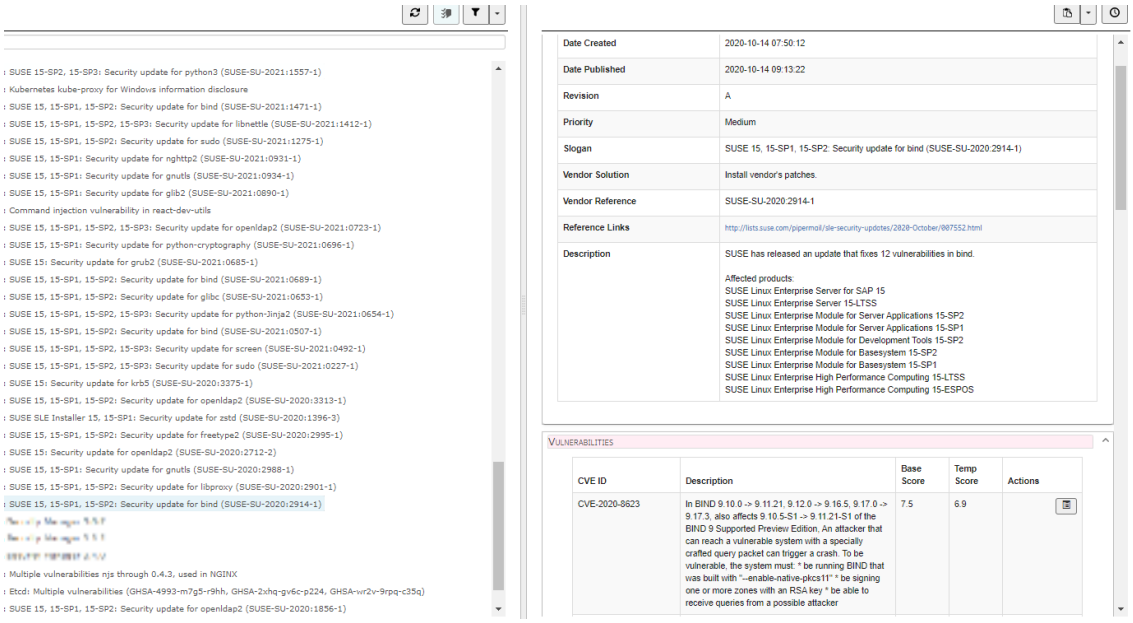

Figure 8. EVMS overview - vulnerability alert.

It is worth noting that ESM is not, nor will it ever be, the only way that the information regarding vulnerabilities have and always will be communicated to customers. The vulnerability information is already being communicated to the customers in various ways. These include, but are not limited to, release notes, security bulletins and Security Test Reports (STR). These are not considered in the scope of this research.

4.2 Integration to ESM

Currently EVMS is fully internal tool for Ericsson, it does not allow any external interfaces or outbound integrations. Additional development on EVMS side is required to ensure real-time information transfer to ESM deployments on customer premises. This requires additional study, how to best implement this and the connectivity around the globe.

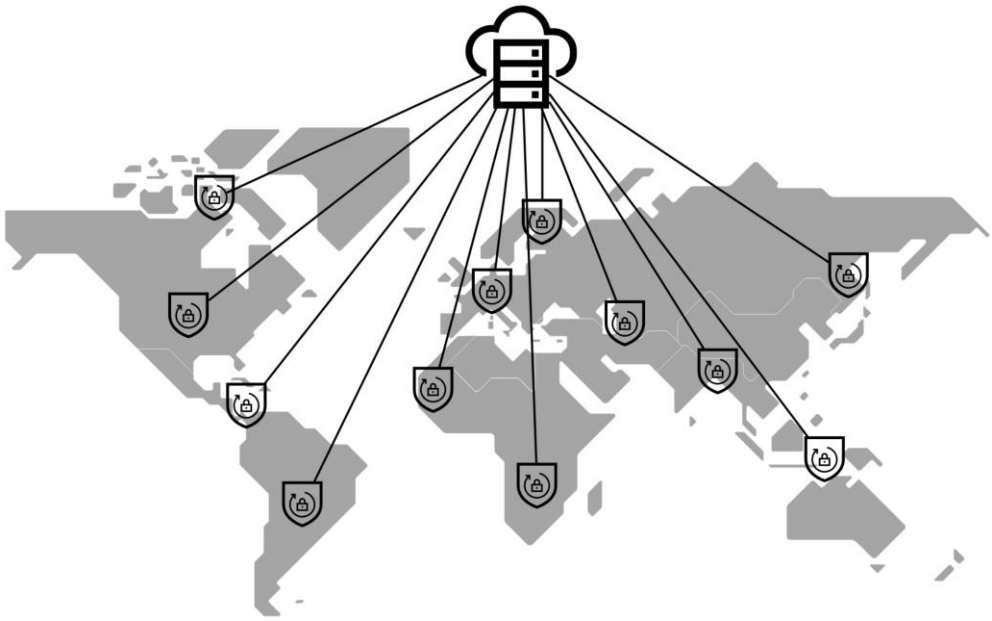

Figure 9. World of Security Managers connecting to EVMS

Ericsson Security Manager instances have been deployed in the customer networks which have no external access. Policies on opening external connectivity to critical network segments, which ESM is part of, varies from customer to customer. To ensure that the service can be delivered to these isolated ESM instances, alternative information transfer methods must be provided. These alternatives could involve for example an EVMS data export file transfer alternative.

4.3 Inventory Management

As all Ericsson products have a version specific entry in the EVMS, all information needed is there. This information can easily be mapped to the information structure on ESM side.

Asset type naming convention varies slightly between systems, this is easy enough to remediate in the ESM side input parser. Evolution of the functionality will involve additional information collection on the ESM side. This is to ensure that all vulnerabilities can be assigned to the correct components of the network assets. This is applicable especially on the Containerised Network Functions

(CNFs), where the component execution location can vary on the cloud infrastructure.

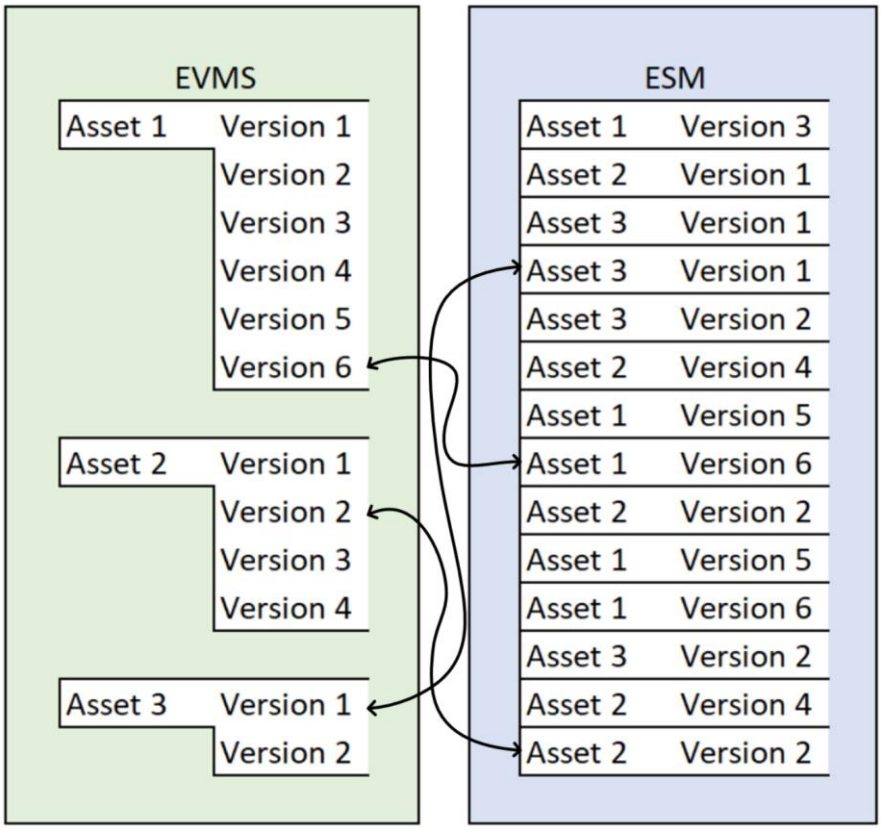

Figure 10. Simplified overview of asset inventory structures.

Figure 10 above shows a simplified overview on the asset inventory structures in both products. EVMS contains all commissioner company assets, with dedicated entries for each release. On the ESM side the inventory contains the customers network assets. Each asset has a version and possibly some substructures. These substructures have been omitted from the figure.

5 Ericsson Security Manager

ESM, see example UI below in Figure 11, aims to be the system to provide visibility to all the security related things. Currently, among other things, it has the information on customer network assets though automatic asset discovery procedures.

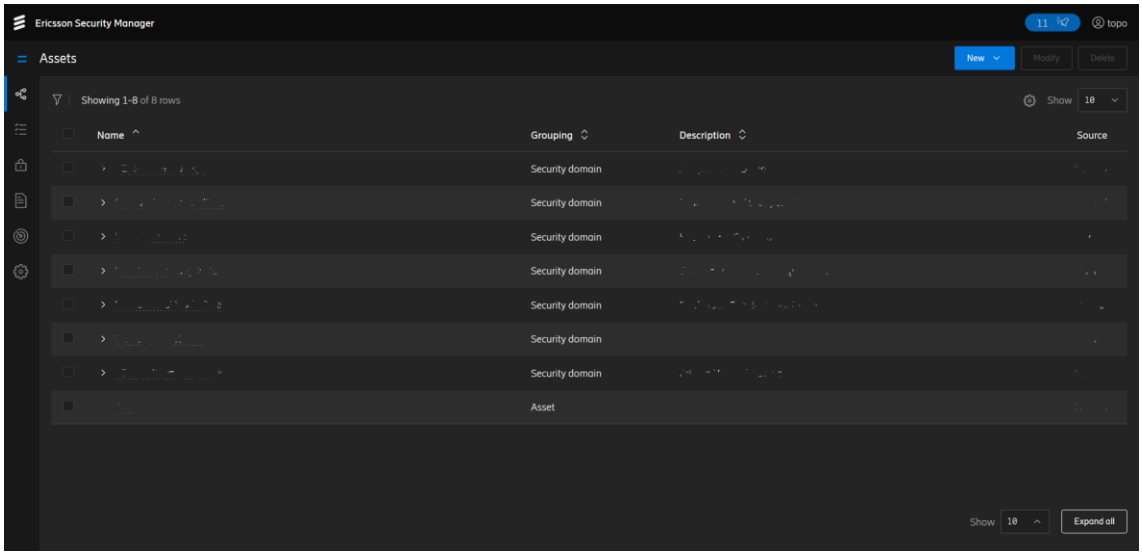

Figure 11. Ericsson Security Manager asset inventory example

Through the same automatic asset discovery ESM knows all the assets in the network, the deployment variants they have been deployed with and the exact software version they have been deployed with.

ESM aim to be the answer to many of the operator questions “how do you do it?” when it comes to alignment to different frameworks. This research concentrates on one of the components of those frameworks, vulnerability management.

5.1 Complementary Value Packages

As described, on the Ericsson internet webpages [2], Security Manager already has other functionalities. These functions will be complementary to the new vulnerability management value package. Following subsections will describe these functions on a high level. Certificate Automation is omitted.

5.1.1 Protect Functionality

Purpose of the protect is both to implement and maintain the security policies according to the customer security baseline requirements across different network vendors, domains and individual assets.

> Baseline Automation functionality provides repeatable process for systematic selection of technical security and privacy policies and controls, their automatic enforcement towards the network context and continuous compliance monitoring after initialization. [2]

This functionality can be used in conjunction with vulnerability management. More specifically the risk treatment or mitigation part could potentially include an additional security policies or controls for it.

5.1.2 Detect Functionality

Security Manager includes a powerful detection engine, that enables execution of different threat detection logics on top of it. One of these logics is monitoring syslog events.

> Security manager will collect data to enable threat visualization in order to identify incident chains, visualize statistics and create threat heat maps. Data collection is made from the network at hand. [2]

This functionality can also be used in the risk treatment of discovered vulnerabilities. If you can monitor the risk generating activity on the network assets that are at risk, you can bring down the risk to an acceptable level.

5.2 New Functionality

Vulnerability management automation value package will be a natural expansion of Security Manager capabilities. Vulnerability management related to the NIST Cybersecurity Framework [15] the subcategories would mainly fall in the Identify and Respond functions of the framework.

Vulnerability management components can integrate with other components in the ESM deployment. Depending on the other value packages, that the customer has chosen and are deployed, vulnerability management function brings varying levels of automation to support customer activities. Information from protect and detect can be utilised as input, help in identification of potential risks in the network. This also works the other way around. Risks identified by the vulnerability management can potentially be treated with functionality provided by protect and detect functionality.

5.3 Vulnerability Information Sources

For Security Manager it is essential that one does not lock in on one source for vulnerability information. This section goes through different sources and interface recommendations.

5.3.1 EVMS

For Ericsson products EVMS will be the most important information source. This is because of all the additional, asset specific, information added by both the PDU and PSIRT organisations in to the individual vulnerability entries in the EVMS database. Information contains detailed listing of all 3rd and 2nd party software components used in the products. More information on EVMS was provided in the section 4 previously.

This integration is illustrated with a solid arrow in the Figure 12 below. This, encrypted, subscription-based integration between the two systems, provides real-time updates on the verified vulnerabilities in the customer network. Interface could offer different alternatives for vulnerability data synchronisation. Starting, for example, from entry level once per quarter and ending up to the top-of-the-line alternative of daily updates from EVMS.

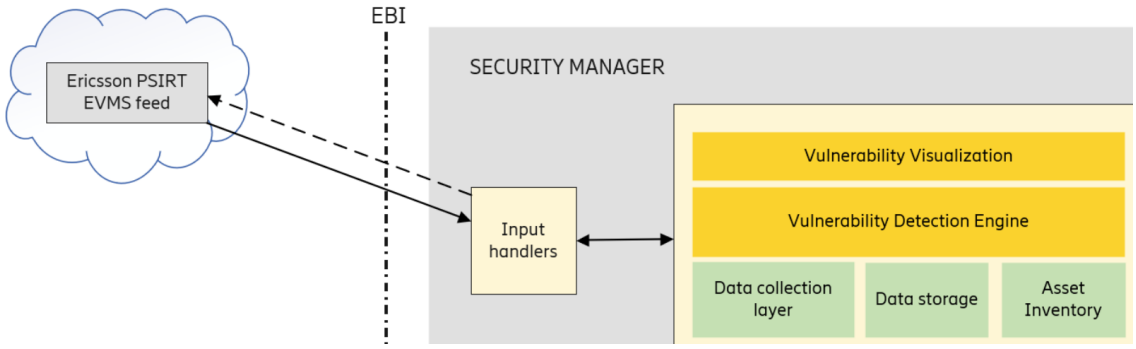

Figure 12. EVMS integration to ESM.

Dashed line, shown in the above Figure 12, could potentially be used as a customer feedback channel, communication regarding the vulnerabilities reported or observations of active exploits. This return channel would also provide additional subscription models also towards PSIRT and asset PDUs.

Protocol used in this interface is not included in the scope of this research, best alternative should be studied together with PSIRT organisation.

5.3.2 External Vulnerability Feeds

For practical reasons all external feeds are bundled here in one. Input handlers should be developed in a way that allows easy addition of additional data sources. Sources might be in variety of formats, some even proprietary for some providers.

CSPs might have their own national NSCS or commercial vulnerability feeds that they would like to follow. Adding additional parsers or input handlers would enable ESM to process these too.

Having more than one feed has many benefits. Firstly, comparing the external feed data to the data received from EVMS, will validate the real vulnerabilities leaving out the false positives and vulnerabilities that do not expose risk. Secondly, it enables CSPs to act on the vulnerabilities that they have not seen before and that they think are valid vulnerabilities. Both use cases limit the amount of effort needed at the CSP Security Operations Center (SOC) or similar

organisation. Figure 13 below shows the integration of external vulnerability feeds to ESM. This link is unidirectional, no feedback is to be sent to the external party.

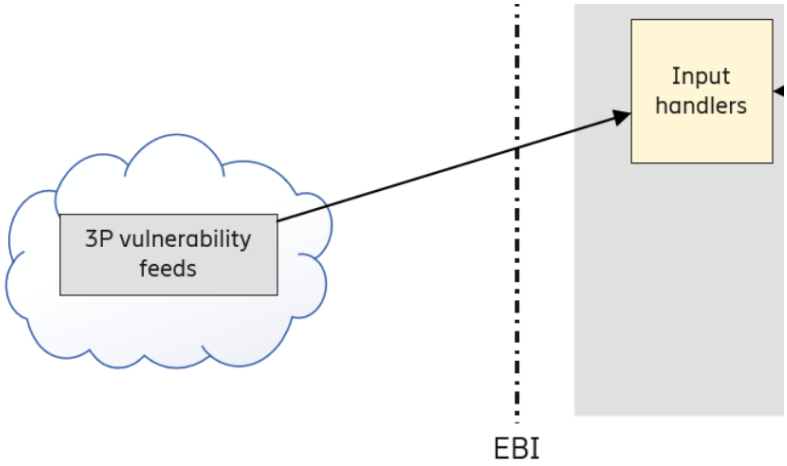

Figure 13. Integrating external vulnerability feeds to ESM.

External vulnerability feed can also come from in-house. This can be especially useful in case the company has a dedicated threat hunting team or for example active bug bounty program.

5.3.3 Vulnerability Scanner Reports

So that things would not be too easy, CSPs execute their own security scans on assets deployed in their networks and premises. This is an essential part of the RM process and must not be omitted. After the network assets have been deployed, and post deployment security hardening has been completed, all the findings done by CSP scanners should be in line with the EVMS data.

As was the case with the external vulnerability feed data, in section 5.3.2 above, mapping the scanner output data with the data from EVMS will limit the effort needed in CSP SOC and also interaction needed with asset PDU post-deployment.

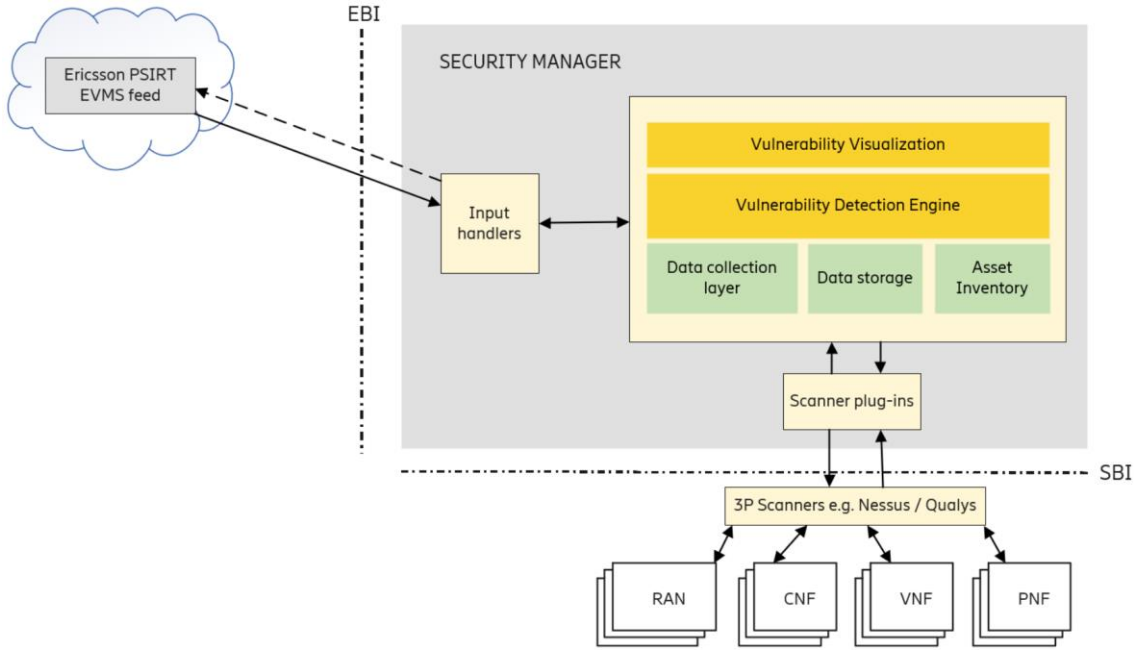

Figure 14. Vulnerability scanner integration to ESM.

Different scanners should be treated the same as other threat detection data. Integration point should be on the southbound interface of ESM. It must also be possible to deploy additional scanner plug-ins to ESM to support additional scanners.

Also, here the feedback channel, back towards EVMS, could be utilized for scenarios which CSP wants to flag something for PSIRT verification or validation. At the same time some statistics on the scans could be collected and uploaded.

6 Automated Vulnerability Management

This section of the research is dedicated for the conclusions or the result of the research, how RBVM should be implemented with ESM. In addition to conclusions, it also includes some additional research recommendations.

6.1 Risk-based Vulnerability Management

The research question has two key points or clues already included. The first point being the word pair ‘valid vulnerabilities’ and the second ‘best ensure’. Combining these to statements could alternatively be replaced with risk-based and usability.

Valid vulnerabilities implies that the vulnerabilities, which do not generate risk are excluded. Only a vulnerability that can potentially harm the organisation or the asset can be risky, valid.

Ensure best visibility or make sure that the valid vulnerabilities are visualised in a way that is intuitive and highlights the order of criticality. The vulnerabilities that generate the highest risk for the operator or asset should be prioritised in all layers

6.2 ESM Architecture

Further research is needed on how different risks are portrayed in ESM. Other value packages should also be tied in to the risk-based visualisation. This integration should not be unidirectional. As an example, some of the vulnerabilities found, could potentially be treated, mitigated, with other ESM value packages.

This should work in all directions. Detection of non-compliance risk could be treated by activating a threat monitoring logic on the asset. Or in case of

discovered, risk generating, vulnerability it could be treated or mitigated by updating an operational time security configuration on the asset.

Below Figure 15 shows a way how the different value packages could be logically on the lower level than the risk orchestration layers. With the help of asset criticality and risk history information, would enable asset risks to be front and centre of all ESM activities.

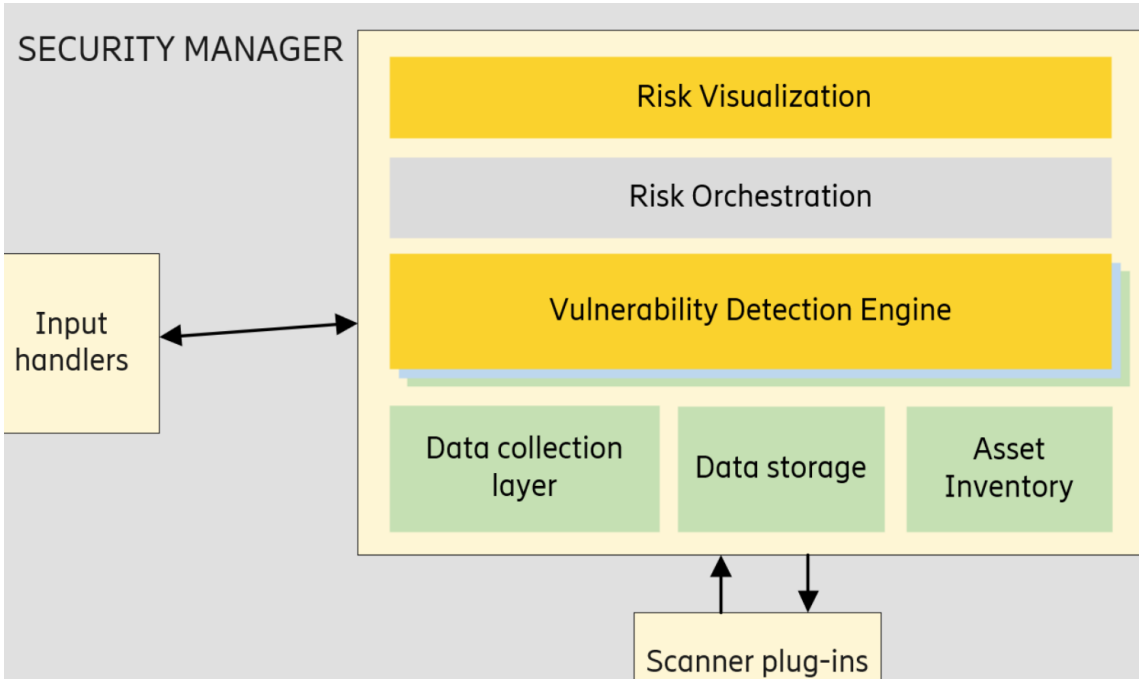

Figure 15. ESM Architecture overview – proposal

Risk orchestration illustrated above in Figure 15, will help in partially replacing or enhancing the manual process of risk treatment. Helping with additional information such as risk validity, is the risk observed and exploited, and removing some of the effects of human ‘gut feeling’-like effects on prioritisation. More about this in the following section 6.2.1.

Appendix 1 describes the generic risk management process. Numerous adaptations of this exist. Main point to acknowledge from this is that the process is iterative, never-ending.

6.2.1 Link to Risk Orchestration

As mentioned, the additional value point, of the combined data of ESM and EVMS, can be the automation of risk discovery, treatment options and the treatment. This will ease the iterative process and help in concentrating, again, to unknown new threats and other processes.

Figure 16 below shows how there is two factors affecting the Risk Orchestration. The first one being the likelihood, for which input can be received from external threat logs, ESM detect functionality or from weaknesses in software or configuration. Likelihood can also be decreased by applying mitigating actions such as enforcing additional security configurations or adding new threat detection logics. The second factor is the potential impact. How serious the impact for the risk is in case the risk becomes reality.

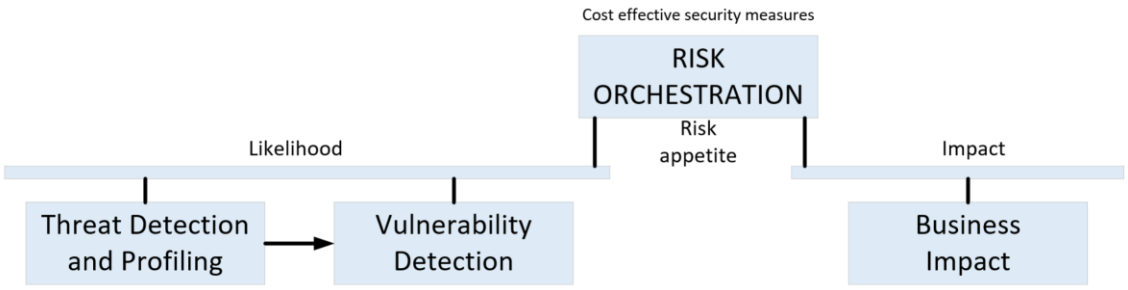

Figure 16. Likelihood and the potential are inputs to risk orchestration.

On the business side of the equation, one has the impact to one's business, cost of protecting the value of the assets. Here the actions include but are not limited to

- Determine the asset criticality.
- Cost of asset recovery or re-deployment.
- Position of the asset in the network in case of a breach or attack.

Compiling this information will result in knowing what one has to lose, what is worth protecting and in what order.

On the opposing side of the process the threat detection and profiling could include actions such as

- Mapping assets that are potentially under threat.
- Scoping and mapping possible threat events.
- Analyse active threat indicators.
- Identify one's online threat landscape.
- Maintain complete network inventory.
- Match threat indicators to assets likely to be impacted.

Vulnerability detection includes actions

- Identify and rank incoming weaknesses.
- Assess the effectiveness of existing, already enforced, technical controls against the threat indicator profiles.

On this side one has information on the active threats, where these threats will hit and where the possible weaknesses are. Also, one has the knowledge which threats are hitting the existing weaknesses, vulnerabilities, that one has in their assets.

By bringing in the vulnerability management functionality customers will be able to automate considerable amount of the largely manual risk management process by risk orchestration in ESM.

6.2.2 Vulnerability Treatment

When one knows the risks, one can plan the protection against them. This called risk mitigation. One can also treat the risks in a way that will bring the risk down to an acceptable level, plan and prepare the detection of certain threat events in the network. These events can then be used to trigger countermeasures such as network isolation.

Treatment and mitigation alternatives could come directly from the asset PDU. Mitigation alternatives, by using ESM, are dramatically increased. As an example, the PDU can suggest patching the vulnerable software component, mitigation

with update of an operational time security configuration attribute or treatment by adding a threat detection logic to monitor possible exploits.

Telecommunication networks have the burden of legacy, as do all networks. Fifth generation cellular networks are being deployed around the world. This does not mean that the older networks would suddenly disappear. This fact must also be acknowledged on the security automation. Continued support for older physical assets alongside the more recent virtualised and containerised assets is essential.

Risk mitigation on older products might not always be feasible by patching, but certainly other ways to treat risks are on the table. This is assuming that all the valid risks are known to the network owner.

7 Proposed Implementation

This, the final section, summarises the findings and then proposes an implementation approach.

Similar approach, as has been used with other functionalities, is strongly recommended. First version should be a barebone kind of minimal viable product. Testing this, especially the user experience (UX), within customer environment gives more insight on the direction that the development should go.

Starting with Ericsson assets will give the most value to customer risk management processes. Including the 3rd party asset types later will boost the value even further.

7.1 Summary

Role of ESM is critical in modern telecommunications networks. Depending on the maturity of the CSP, different aspects of it provide value. Taking the next step on the security automation journey, with the help of information that no one else has, will emphasise Ericsson’s role as a trusted security partner.

Developing yet another Vulnerability Management tool will not suffice. Automating vulnerability management activities and linking it together with the other value packages in Security Manager will act as market differentiator. When a new vulnerability is discovered, giving the operator alternatives how to best treat the risk is nothing new. But if one can give automated options, enabling the operator to, with a click of a button, select a risk treatment alternative for the vulnerability and execute it, that brings immediate value. Additionally, concentrating on the vulnerabilities that are generating real risk, meaning that they are potentially both observed and exploited in the customer networks, will be the right approach. This way the operators limited resources are targeted where it matters the most.

Optimal vulnerability management scenario could also be explained with coverage and efficiency. Risk-based vulnerability management is union of:

- Coverage: treat every vulnerability that matters.
- Efficiency: deprioritise vulnerabilities that do not matter.

With given resources fix all that matters and down prioritise what does not matter. Please see Figure 17 below for visualisation.

Figure 17. Perfect vulnerability management is the combination of best possible coverage as efficiently as possible.

First step and priority one, when thinking about the data sources, should be EVMS integration. Later one could add in parsers for external vulnerability feeds and scanners. These are out of scope of this research; separate studies must be conducted for them.

Logically the integration to external vulnerability feeds should happen through eastbound interface (EBI), please see Figure 18 below for an illustration. This is to allow proper traffic separation in the customer environments. Dedicated VLAN and IP addressing is recommended for this interface, which is going to communicate outside customer network. Data availability could be subscription based, catering also different subscription models. For offline updates of vulnerability data, file-based interface should be supported. This is, in case the customer does not allow any external connections to or from the ESM.

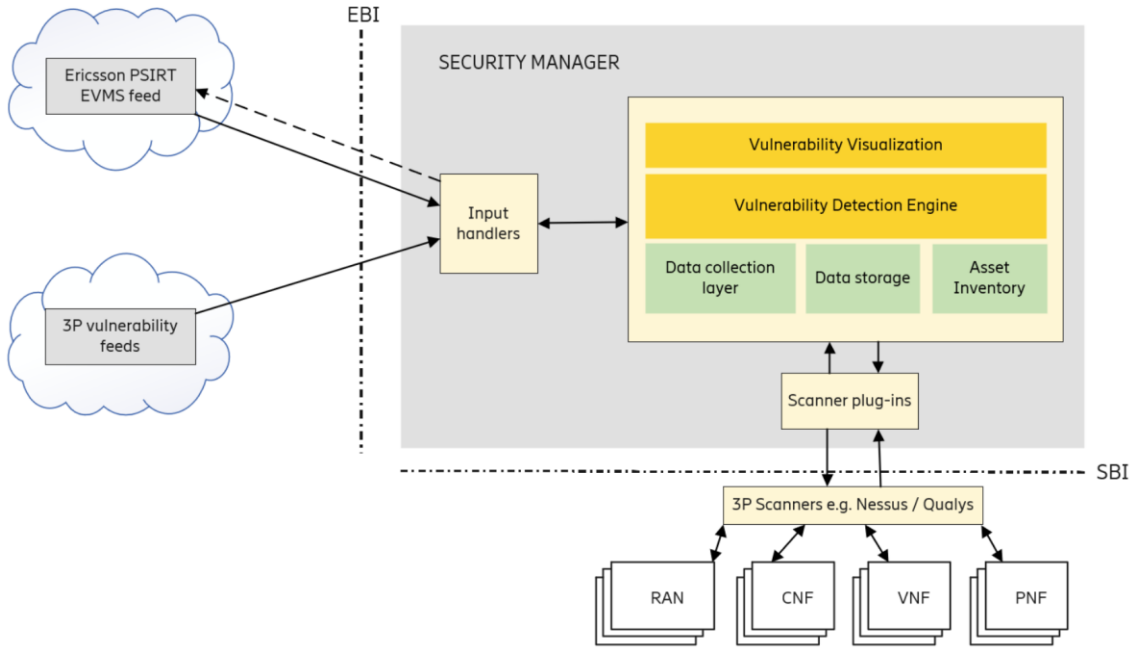

Figure 18. High-level ESM-EVMS architecture

For the future use case of integrating on-premises vulnerability scanners and processing the reports from them, CVE and asset component mapping is easy to implement in ESM. In case additional use cases are needed for the return channel towards EVMS, summaries of these reports could be shared.

Further benefits can be achieved by customising reports from ESM. These reports could be used as evidence in ISMS audits and regulatory requirements.

Several additional use cases were also identified. There is a lot of potential in utilising the link between ESM and EVMS, if it can be used for bi-directional communication.

7.2 Evaluation of This Study

Every security framework and standard highlights the importance of managing vulnerabilities in your assets. More recent evolution of the vulnerability management part is the risk-based vulnerability management. Over 16 thousand published vulnerabilities, yearly, makes it impossible for any organisation to treat all the vulnerabilities. That is why putting weight on the vulnerabilities that

generate risk is a must in modern networks. See Appendix 1 for an overview of a General Risk Management Process.

Integration of EVMS and ESM, and the added information on top of the customers asset inventory, will bring the information on valid risks in to the reach of the customers. This will make customers even more efficient in risk treatment, which then will make customer better able meet the ever more demanding requirements and regulations put on them. Most importantly it will enable operators to protect our data and privacy as efficiently as possible.

There does not seem to be any negative aspects on this. While it might be true from the functionality and customer value points of view there is some development, new functionality is required on both systems involved. One should not understand development need as negative, but as some additional effort is needed, one can interpret the consumption of commissioner company's resources as negative thing. As an example of development needs on ESM side one can mention the storage of asset specific vulnerability data and visualisation the full security posture of individual assets and the whole network. This information is also valuable information when deciding different, risk based, security configuration compliance monitoring policies and threat detection logics.

On the EVMS side all the needed information is already available. Only remaining development requirement is the interface or interfaces towards customers. How can one cater for different subscription levels and methods of information delivery to customer ESM deployments? Answer to this question was scoped out from this research.

Customers need the vulnerability information to be timely, accurate and with as much additional information as possible. Additional information must include reasoning, mitigation procedure or plan, monitoring procedure, explanation on risk exposed or why risk is not valid (false positive). Ericsson Product Development Units (PDUs) and Product Security Incident Response Team

(PSIRT) help to enrich normal CVSS vulnerability information to be more valuable.

Correlating this information with the information customers can obtain from on premise vulnerability scanners will dramatically cut down the resources spent on vulnerability validation. This will ensure that the customers are always aware of all the real risks in their networks and how to treat the ones that matter.

References

1 Mobile Telecommunications Security Landscape, GSMA, March 2021. <https://www.gsma.com/security/wp-content/uploads/2021/03/id_security_landscape_02_21.pdf>. Accessed 5 Dec 2021.

2 Security Manager – Ericsson, Web page. <https://www.ericsson.com/en/portfolio/iot-and-new-business/new-business/security-and-risk-management/security-manager>. Accessed 5 Dec 2021.

3 The Ericsson Security Reliability Model | Ericsson. <https://www.ericsson.com/495435/assets/local/security/the-ericsson-security-reliability-model.pdf>. Accessed 5 Dec 2021.

4 Vulnerability – Glossary | CSRC. <https://csrc.nist.gov/glossary/term/vulnerability>. Accessed 5 Dec 2021.

5 CVSSv3.1 User Guide | FIRST.org. <https://www.first.org/cvss/v3.1/user-guide>. Accessed 5 Dec 2021.

6 Why Vulnerability Management is Important | Reciprocity. <https://reciprocity.com/why-vulnerability-management-is-important/>. Accessed 5 Dec 2021.

7 Vulnerability Management Principles | Tenable®. <https://www.tenable.com/principles/vulnerability-management-principles>. Accessed 5 Dec 2021.

8 What is a False Positive? | cgisecurity.com <https://www.cgisecurity.com/questions/falsepositive.shtml>. Accessed 5 Dec 2021.

9 KPN Security Policy. <https://ciso-ksp.kpnnet.org/>. Accessed 5 Dec 2021.

10 Privacy and Security Assessment process | Deutsche Telekom. <https://www.telekom.com/en/corporate-responsibility/data-protection-data-security/security/details/privacy-and-security-assessment-process-358312>. Accessed 5 Dec 2021.

11 Prioritization to Prediction Volume 5: In Search of Asset at Risk | Kenna Security. <https://website.kennasecurity.com/wp-content/uploads/2020/09/Kenna_Prioritization_to_Prediction_Vol_5.pdf>. Accessed 5 Dec 2021.

12 PSIRT Product Security Incident Response Team | Ericsson. <https://www.ericsson.com/49611c/assets/local/security/psirt-product-security-incident-response-team_rev-a.pdf>. Accessed 5 Dec 2021.

13 SUSE-SU-2020:2914-1: moderate: Security update for bind | lists.suse.com. <https://lists.suse.com/pipermail/sle-security-updates/2020-October/007552.html>. Accessed 5 Dec 2021.

14 FIRSTCon21 talk – Ericsson PSIRT: Product Security Vulnerability Management Metrics are Hard | YouTube. <https://www.youtube.com/watch?v=UgxCkYd5Oko>. Accessed 5 Dec 2021.

15 Framework for Improving Critical Infrastructure Cybersecurity, version 1.1 | NIST. <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>. Accessed 5 Dec 2021.

16 DRAFT INTERNATIONAL STANDARD - ISO/IEC DIS 27005: Information security, cybersecurity and privacy protection — Guidance on managing information security risks. <https://www.iso.org/standard/80585.html>. Available for purchase. Accessed 5 Dec 2021.

General Risk Management Process

This appendix contains the illustration of the generic risk management process. It is the same process as documented in the ISO standards ISO 31000:2018 and the draft of ISO/IEC DIS 27005:2021

> The information security risk management process can be iterative for risk assessment and/or risk treatment activities. An iterative approach to conducting risk assessment can increase depth and detail of the assessment at each iteration. The iterative approach provides a good balance between minimizing the time and effort spent in identifying controls, while still ensuring that high risks are appropriately assessed. [16]

All risk management processes can be mapped to this same structure, see Figure 1 below for illustration of the process.

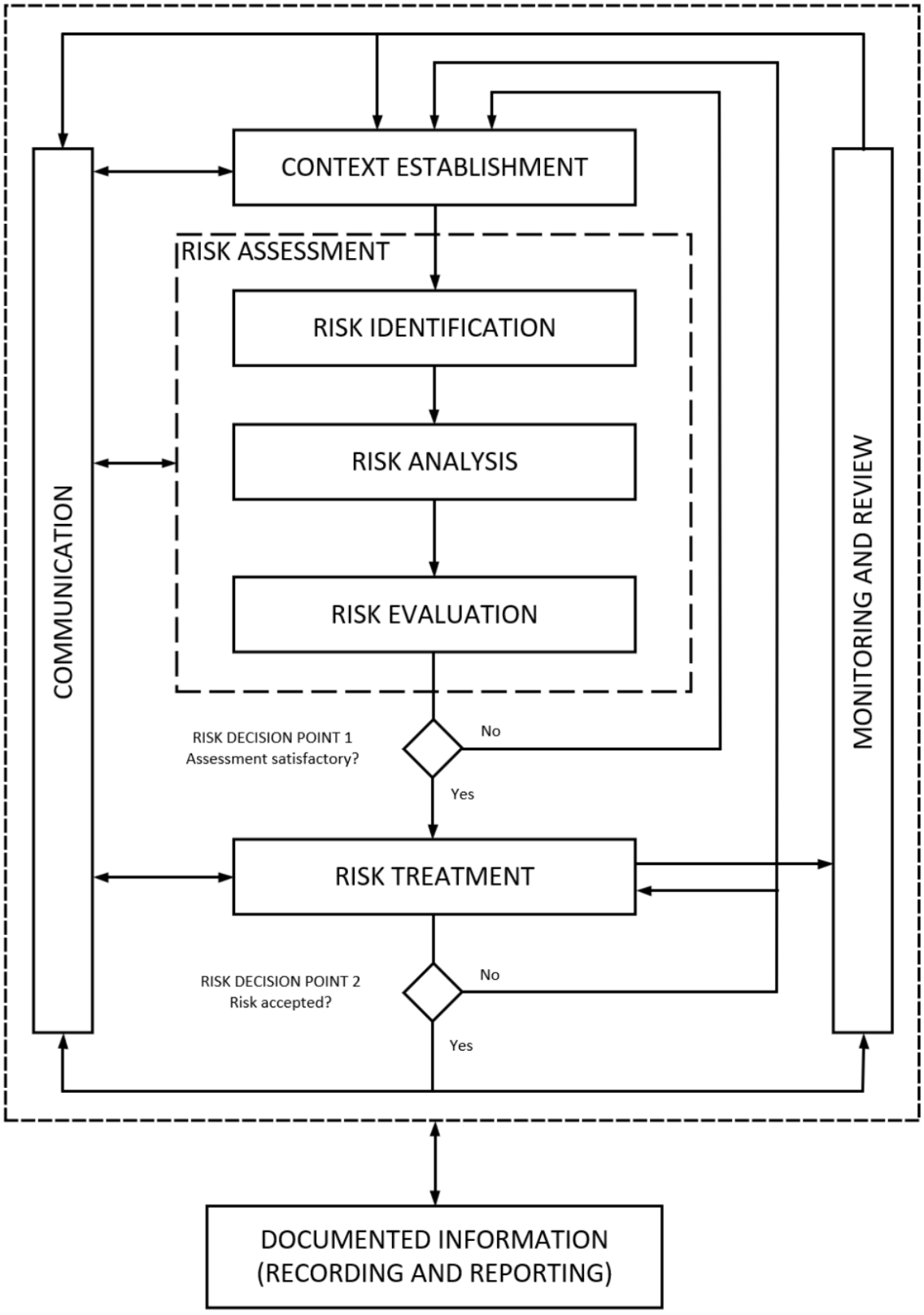

Figure 1. Generic risk management process. [16]