jamk.fi

Automated ISMS control auditability

Mikko Suomu

Master's Thesis
May 2015

Master's Degree Programme in Information Technology

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖN
KUVAILULEHTI

Tekijä(t) Suomu, Mikko	Julkaisun laji Opinnäytetyö	Päivämäärä 17.05.2015
	Sivumäärä 107	Julkaisun kieli Englanti
	Luottamuksellisuus ( ) saakka	Verkkojulkaisulupa myönnetty X
Työn nimi Automated ISMS control auditability		
Koulutusohjelma Master's Degree Programme in Information Technology		
Työn ohjaaja(t) Hautamäki, Jari		
Toimeksiantaja(t) Oy LM Ericsson Ab		

Tässä opinnäytetyössä tutkitaan mahdollista viitekehysmallia tietoturvan hallintajärjestelmän (ISMS) teknisten kontrollien automaattisesta auditoitavuudesta. Päätavoitteena oli kehittää viitekehysmalli ISO27001:2013 standardin säännönmukaisuuden automaattisesta arvioinnista jota voitaisiin uudelleenkäyttää missä tahansa ISMS-järjestelmässä. Viitekehysmalli testattiin empiirisellä tutkimuksella jossa ratkaisu pyrittiin todentamaan (Proof of concept). Tavoitteen saavuttamiseksi analysoitiin mitkä ISO27001:2013 kontrollit voitaisiin toteuttaa teknisesti ja olisiko niiden säännönmukaisuuden todennus tehtävissä automaattisesti. Useita eri lähteitä käytettiin hyväksi määriteltäessä miten kontrollit tulisi toteuttaa, todentaa ja miten niitten säännönmukaisuus voitaisiin mitata.

Kehitetty viitekehys koostuu kolmesta osasta, viitekehykseen valituista kontrolleista, viitekehyksen arkkitehtuurista sekä käyttöohjeistuksesta ja se sisältää ISO27001:2013 kontrollit jotka voitaisiin automaattisesti auditoida, menetelmä tämän tekemiseen ja varsinaisen viitekehyksen automaattisen auditoitavuuden saavuttamiseen.

Testauksessa käytettiin kolmea eri tyyppistä kaupallista työkalua jotta ymmärrettäisiin voisivatko ne toteuttaa osan kehitetystä viitekehyksestä. Mikään työkaluista ei pystynyt tähän suoraan. Empiirinen tutkimus on osoittanut eheyden varmistamisen tärkeyden tavoiteltaessa automaattista säännönmukaisuuden varmistamista. Tämä on olennainen osa joka näyttää puuttuvan testatuista työkaluista.

Avainsanat (asiasanat)
Auditointi, Tietoturvan hallintajärjestelmä, standardi, viitekehys, kontrolli, määräystenmukaisuus

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

DESCRIPTION

Author(s)	Type of publication	Date
Suomu, Mikko	Master's Thesis	17.05.2015
	Pages 107	Language English
	Confidential ( ) Until	Permission for web publication X

Title
Automated ISMS control auditability

Degree Programme
Master's Degree Programme in Information Technology

Tutor(s)
Hautamäki, Jari

Assigned by
Oy LM Ericsson Ab

This thesis focuses on researching a possible reference model for automated ISMS's (Information Security Management System) technical control auditability. The main objective was to develop a generic framework for automated compliance status monitoring of the ISO27001:2013 standard which could be re-used in any ISMS system. The framework was tested with Proof of Concept (PoC) empirical research in a test infrastructure which simulates the framework target deployment environment. To fulfil the objective the thesis analysed first which ISO27001:2013 controls could be implemented using technical means and whether it would be possible to automate the measurement of the control compliance for these controls. After that different sources were used as input material to actually define how to fulfil, verify and measure the selected controls.

The developed framework consists of three parts, Framework Selected Controls, Framework Architecture and guidance how to use the framework. It includes ISO27001:2013 controls which could be automatically audited, a methodology to do this and a framework how this could be fulfilled.

The testing was performed using three different types of commercial tools to understand if they could fulfil a part of the developed framework. None of the tested tools was able to fulfil the framework as it is. Empirical research has showed the importance of the integrity assurance when reaching for automated security control compliance. This is the essential part and is somewhat lacking on the tested tools.

Keywords
Audit, Information Security Management System, standard, framework, control, compliance

Acknowledgements

I would like to express my gratitude to my colleagues and managers at Ericsson Network Security for providing support and feedback for the thesis and for the possibility to carry out the studies. I'd like to also thank my tutor and fellow classmates at JAMK University of Applied Sciences.

Special thanks to my wife and two sons; I would not have been able to make this without your love, patience, support and understanding.

Acronyms

Term	Explanation
AIK	Attestation Identity Key
BSM	Basic Security Mode
CCE	Common Configuration Enumeration
CPE	Common Platform Enumeration
CSC	Critical Security Controls
CVE	Common Vulnerability Enumeration
CVSS	Common Vulnerability Scoring System
DMZ	Demilitarized zone
DNS	Domain Name System
EMET	Enhanced Mitigation Experience Toolkit
FISMA	Federal Information Security Management Act
GID	Group Identifier
GUI	Graphical User Interface
HIPAA	Health Information Portability and Accountability Act
ICMP	Internet Control Message Protocol
IdAM	Identity and Access Management
IDS	Intrusion Detection System
ISMS	Information Security Management System
LDAP	Lightweight Directory Access Protocol
NAC	Network Access Control
NCP	National Checklist Program
NIST	National Institute of Standards and Technology
NMAP	Network Mapper
NSA	National Security Agency
NVD	National Vulnerability Database
OCIL	Open Checklist Interactive Language

OS	Operating System
OSSEC	Open Source Security
OVAL	Open Vulnerability and Assessment Language
PCR	Platform Configuration Register
PKI	Public Key Infrastructure
PoC	Proof of Concept
PRADS	Passive Real-time Asset Detection System
SCAP	Security Content Automation Protocol
SIEM	Security Incident and Event Management
SMTP	Simple Mail Transfer Protocol
SoA	Statement of Applicability
SOX	Sarbanes-Oxley Act
SPF	Sender Policy Framework
SSLA	Security Service Level Agreement
SUT	System Under Test
TCG	Trusted Computing Group
TCP	Transmission Control Protocol
TPM	Trusted Platform Module
TXT	Trusted Execution Technology
UDP	User Datagram Protocol
UID	User Identifier
URL	Uniform resource locator
VM	Virtual Machine
VPN	Virtual Private Network
XCCDF	Extensible Configuration Checklist Description Format

Contents

FIGURES

TABLES

1. INTRODUCTION

This thesis focuses on researching a possible reference model for automated ISMS (Information Security Management System) technical control auditability. The main objective was to develop a generic reference model for ISO27001:2013 standard automated compliance status monitoring which could be re-used in any ISMS system. To elaborate on this, it means that technical security controls used within the ISMS are measured in an automated and continuous way so that the provided result gives assurance to information owners and stakeholders.

The United States' National Institute of Standards and Technology, NIST, has included a "Compelling Argument for Assurance" to its new Special Publication draft related to Information Security. It says that in order to be able to provide information security assurance, security controls and activities need to be specified to gain credible evidence of their functionality and overall behavior of the information systems. This evidence then provides the necessary degree of confidence of information security assurance; in other words, systems comply with security requirements and at the same time effectively support the organization's mission and business. (NIST Special Publication 800-53 revision 4, 2013, 23).

There are two main reasons which have motivated development of the framework: An organization which has given the assignment for the thesis hosts certain information security environments which require very high information security and continuous compliance monitoring. As said on the above NIST publication, one crucial part of any security system is to have appropriate security controls which provide credible evidence of their functionality. This evidence provides confidence of information assurance for system owner and stakeholders. It is intended that the framework would ease the gathering of this evidence when deployed to one of these environments (called "framework target deployment environment"). The other reason is that the framework could act as design guidance in possible products in this area (for example security operations tools). Therefore the framework should be generic enough and not focus only on a single environment; instead, it should be a reference

model which could be re-used to manage any ISMS system. One area where automated auditing would be of high value is cloud based computing. This due to the deployment models where various parties need to agree on who is responsible for which controls, and be able to prove they have done their share.

1.1. Research Objective

The main research objective is to develop a generic reference model for ISO27001:2013 compliance status monitoring which could be re-used in any ISMS system. The reference model is tested with an empirical Proof of Concept (PoC) research using a test infrastructure which simulates the framework target deployment environment. The research questions are:

- What ISO 27001:2013 controls can be implemented by technical means?
- Is it possible to automate the measurement of control compliance for technically implemented controls?
- What mechanisms are required to provide integrity assurance for the audit data?
- Can the framework provide compliance status in automated way for the selected controls?

1.2. Scope

The following areas are included in the framework and PoC study scope:

- Control selection, verification and measurement methods
- Selection of tools to analyse fulfilment of the developed framework
- PoC for selected number of applicable controls

The following areas are excluded from the scope:

- Full implementation of framework
- Full deployment of the developed framework to the framework target deployment environment

1.3. Structure of the Thesis

The research is conducted using the following process:

Chapter 2 - Analysis of the theoretical base.

Chapter 3 - Analysis of the currently existing research, tools and methods.

Chapter 4 - Proposing the framework based on analysis.

Chapter 5 - Empirical research of the framework using a proof of concept.

Chapters 6 and 7 - Analysis of the results and conclusions.

Chapter two focuses on building the theoretical base; it aims to highlight the importance of data integrity and the auditor's view. The theory is continued in Chapter three by further analysing the current research tools and methods.

The framework and controls which can be automated are introduced in chapter four based on the theoretical base and literature review.

Chapter five presents the PoC. For it, a test environment was built which simulates the actual framework deployment target environment. From the refined list of controls (that are part of the framework) a number of controls were selected based on the potential risk level for this type of environment. The measurement part of the selected controls was then used as evaluation criteria for the framework. The framework was tested using three different types of tools.

The results are summarized in Chapter six continued by conclusions in Chapter seven.

2. THEORETICAL BASE

2.1. Compliance

Merriam-Webster online encyclopaedia defines the word *compliance* as the act or process of complying to a desire, demand, proposal, or regimen or to coercion and as the conformity in fulfilling official requirements (Merriam-Webster 2014). As such

this definition is quite straight-forward and concrete, one either fulfils the requirements or not. On the other hand, according to NIST, compliance is more than adhering to static checklists or generating unnecessary paperwork. NIST refers to due diligence with regard to information security and risk management and use of all appropriate information as part of risk management program, so that selected security controls meet the mission and business requirements that organization has (NIST Special Publication 800-53 2013, page *x*).

In the chapter where compliance with regulatory, quasi regulatory, contract requirements and industry standards is discussed in Information Security Management Handbook, the importance of understanding applicable requirements to an organization and authorities placing them is highlighted. (Harold F. Tipton, Micki Krause, 2010, 281). Officially mandated policy generally means that compliance is mandatory, depending also on the authority of the policy maker, for example an executive management or regulatory authority. Still, organizations may see external compliance requirements as a burden and additional cost; however, being compliant could be the only way to stay in the business. Regardless if the requirements are internal or external to an organization, a global or holistic compliance requires also proper governance and risk management. (R. Bonazzi, L. Hussami, Y. Pigneur, 2010, 2).

What is the issue with compliance then? One identified problem (which was also discovered during the writing of this thesis and in the author's opinion is also applicable to ISO27001) is that mandates or requirements are not necessarily defined precisely. The issue is described by Creech and Alderman in IT Policy Compliance for Dummies: For example the SOX (Sarbanes-Oxley) mandate which concerns data security (Section 404) is just one paragraph. Ambiguity comes from the fact that laws are meant to be universally applicable and to any technological solution. They argue that creation of policies based on these types of mandates and applying them to complex systems is one of the major challenges in policy compliance. Also, it is a fact that the IT infrastructure, hardware and software that organization uses has direct impact on the design of the controls and measurement of the effectiveness of a poli-

cy compliance program. How is it then determined that high level mandate is translated properly into clean audit result? This is done by an independent auditor who tests an organization's controls. (Creech, Alderman, 2010).

The overall policy compliance, according to Creech and Alderman, is a complete ecosystem which includes also strategic objectives, user awareness and training, procedures and standards, configuration settings, technical controls, continuous monitoring, business risk assessment and internal and external audits. (Creech, Alderman, 2010)

In order to be fully in control, it is not enough to show that one is compliant to technical requirements, it requires having a proper governance structure and risk management program as well. Although this thesis aims to focus on just the compliance part of technical security controls, it should not be interpreted so that having objective evidence of their conformity would be sufficient.

2.2. Integrity Assurance

According to Information Security Management Handbook compliance programs require several information security attributes such as confidentiality, integrity and non-repudiation. In this context cryptographic mechanisms are often used to implement these attributes (Harold F. Tipton, Micki Krause, 2010, 281). Considering the topic of this thesis, integrity assurance could be considered as one of the attributes with the most importance. This applies to overall integrity of the system under audit on all layers. On Ericsson Review article "Trusted computing for infrastructure", these layers are called "Trusted compute initialization: boot integrity", "Data integrity: at rest and in motion" and "Run-time integrity: protection and privacy" as shown in Figure 1. (Eriksson, Pourzandi, Smeets, 2014).

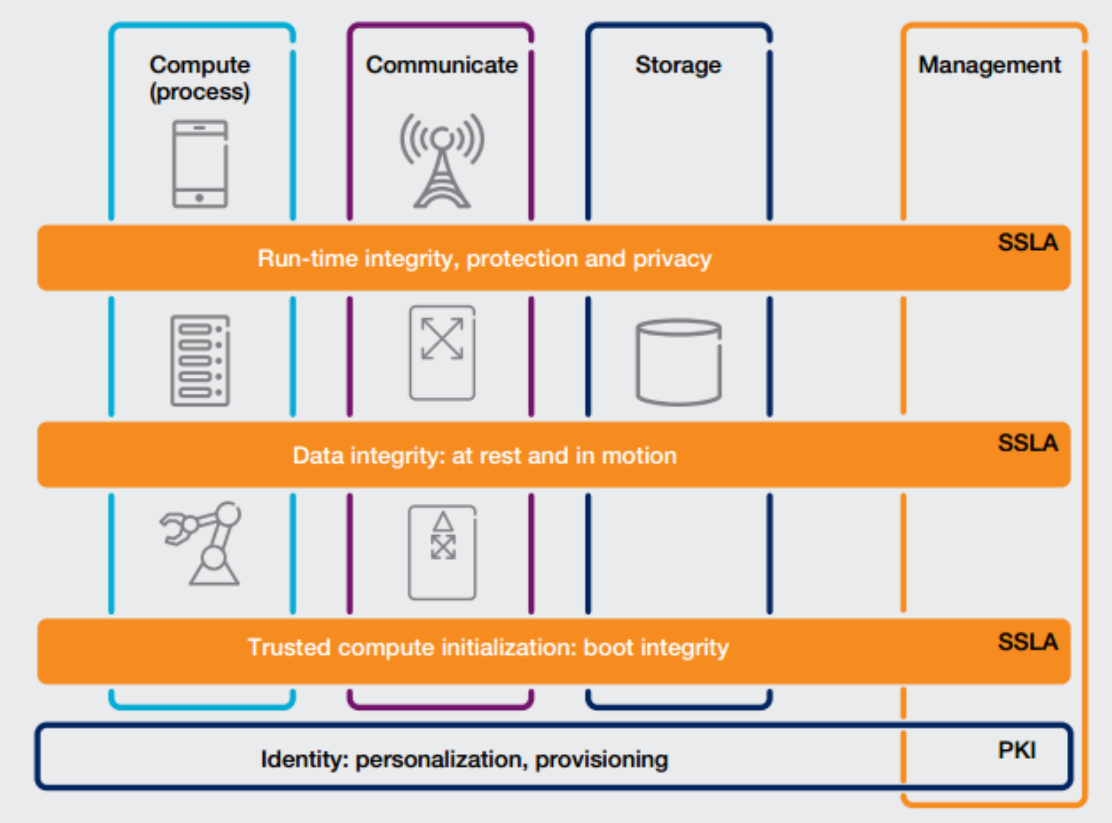

Figure 1. Integrity layers (Eriksson, Pourzandi, Smeets, 2014)

Boot integrity means that a system behaves as expected and runs in a known and trustworthy platform and basic Operating System (OS) or hypervisor configuration. Data integrity refers to data storage and transaction integrity, meaning that data integrity is protected while at rest and in motion and any modification is being noticed. Finally run-time integrity means that any software which is executed behaves according to design and certain predefined properties, so that it would not be possible to exploit software vulnerabilities caused by programming errors. This would also ensure that the audit evidence, which a system under audit provides, is trustworthy and not fake.

Attacks to data integrity are known to happen. At 2010 it was found out that an industrial control system used to operate Iran's nuclear centrifuges was infected with a malware which altered the process so that uranium enrichment failed. This was not

noticed by the operators of the process or the control system as malware reported that process and equipment was working normally (Symantec Security Response, 2010). An article from 2011 lists several attack types which break the data integrity, such as fraud, web site defacements, logic bombs, unauthorized modification of OS, application software, databases, production data or infrastructure configuration, undocumented backdoors, etc. In the article it is stated that these are in many cases due to weaknesses in key processes such as change management, separation of duties, log monitoring and management of privileged access. In order to improve the assurance of data integrity the article mainly suggests implementation of best practices in terms of governance and risk management and use of separation of duties (Gelbstein, 2011).

Considering the technical, rather than administrative or procedural, controls for integrity assurance which would apply to at least boot and data integrity layers (on above figure) there are still few good mechanisms.

Trusted Computing Group (TCG) is an industry standard group which was established in 2003. Its goal is to develop specifications and publish them for use and implementation by the industry (About TCG, 2014). TCG has published a specification for Trusted Platform Module, TPM, which has been standardized as ISO/IEC 11889 standard. Boot integrity protection is one of the tasks which TPM aims to fulfil, meaning that it can be verified that platform behaves as expected what comes to I/O functions and memory and storage operations. In a TPM-protected system, it is possible for a remote actor (so called remote attester) to verify if there have been any unauthorized changes in platform configuration. This is achieved by storing platform configuration values to a secure storage, Platform Configuration Register (PCR). The PCR is stored in non-volatile memory and in order to modify the PCR data, trusted authorization is required. The data is populated during the initial set up of the platform as hash values. During the boot sequence similar data is created from the current platform configuration and compared to the initial values. In case the values match the platform boot process proceeds and system starts up. The hash values created from the cur-

rent configuration during the platform boot are signed with Attestation Identity Key (AIK), which is an alias key for a platform unique endorsement key, i.e. digital identity. This cannot happen if the hash value has changed from the original value. In that case the trusted state of the platform could be considered to be compromised (Trusted Computing Group, 2005). The technology is currently feasible to use for anyone, for example Intel had adopted TPMs into their server processor hardware and call their implementation of the solution Trusted Execution Technology (TXT). Today, it is mainly used for cloud and virtualized environment where a tenant having a virtual machine may not have any control about the hardware. Hypervisor integrity in this context is part of the platform configuration register and will be validated during the boot sequence (See Figure 2). And in this way the tenant also has a possibility to verify the integrity of the hardware using remote attestation. (James Greene, 2012).

There are a number of commercial server products, operating systems and virtualization solutions which take advantage of Intel's TXT technology, such as Dell, Hitachi, Lenovo, SuSe, Red Hat, Ubuntu, VMware, Crowbar, Hytrust, Virtustream, etc. (Solutions and Products with Intel® Trusted Execution Technology (Intel® TXT), 2014). Many of them also use OpenAttestation, which is an open source implementation of remote attestation procedure as described by TCG (OpenAttestation, 2014).

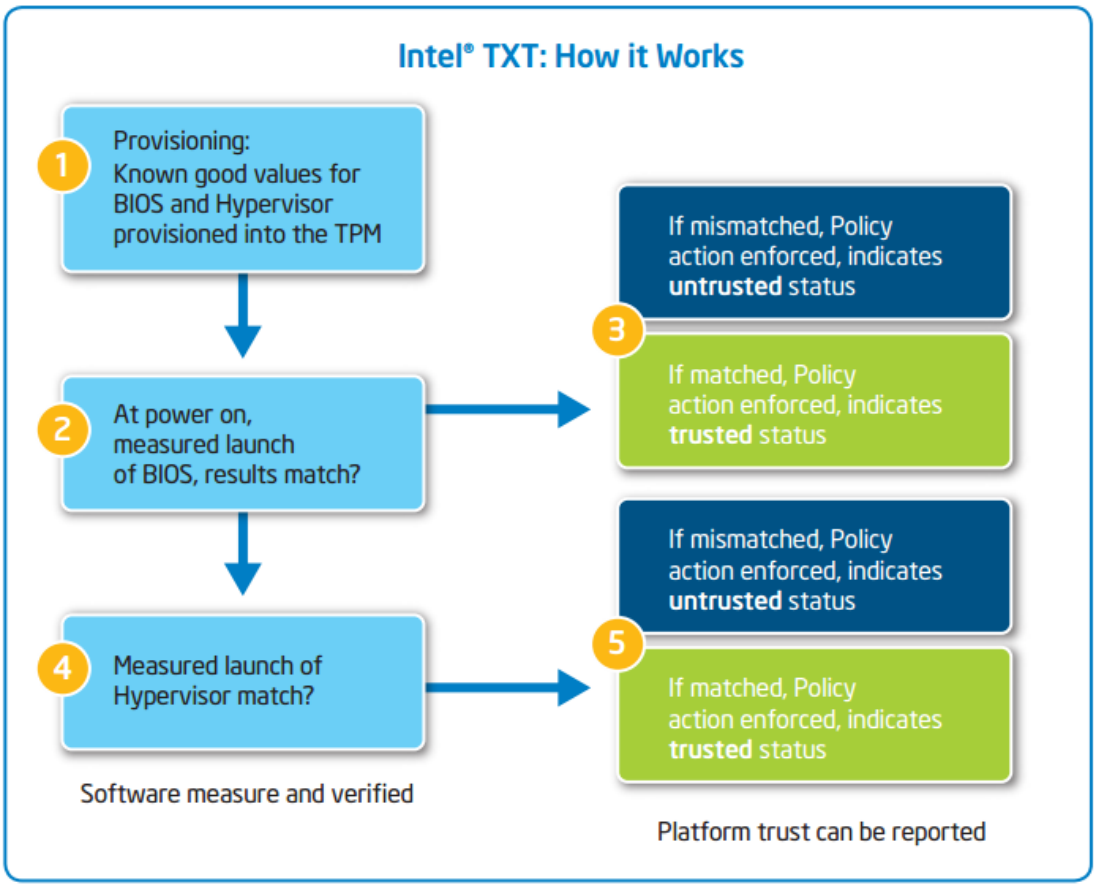

Figure 2. Intel TXT. (James Greene, 2012).

There are certain challenges which relate to this: It could be possible (at least in theory) that the key which is the basis for remote attestation (endorsement private key) is leaked; one could attest anything without actually running it (Dan Boneh, 2006). Considering this and the cloud and virtualized service scenario, there needs to be a linkage from the observation of the platform that the tenant has to the remote attestation, at least what comes to the administrative security domain (meaning that the response is coming from this particular platform, not a replica hosted by a malicious party.) In Ericsson Review article, two ways of attesting a secure VM (Virtual Machine) launch to clients are presented: the cloud provider can deploy the trusted cloud and prove its trustworthiness to the client; or trustworthiness measurements can be conveyed to the client – either by the cloud provider or by an independent trusted third party. (Eriksson, Pourzandi, Smeets, 2014).

Remote attestation only attests the code that was loaded, but if vulnerabilities in the code were exploited after it was loaded this is not seen. Validation of the integrity of the tenant's running virtual machine would be required, not only the boot integrity. A research made by AT&T Labs, Microsoft and Georgia Institute of technology suggests as a possible way a snapshot application which creates the hash (or hash tree) of the running virtual machine and signs it using the keys in TPM. The integrity of the snapshot program itself is protected with a platform configuration register (Srivastava, Raj, Giffin, England, 2012).

TPMs can also be used to support post-boot processes: A SANS document which talks about implementing a hardware root of trust, it is mentioned that Price Waterhouse Coopers (PwC) uses TPMs to protect their X.509 VPN certificates.
(Gal Shpantzer, 2013). Ericsson Review article mentions that a coming release of Ericsson SGSN-MME node will use TPM to store secure PKI credentials which are used for data encryption and TLS connections. (Eriksson, Pourzandi, Smeets, 2014).

Sometimes there is no TPM to be used in the target environment where code is executed. A research paper called "Extending Tamper-Proof Hardware Security to Untrusted Execution Environments" proposes a solution where integrity (and confidentiality) of the execution is supported by encrypting or obfuscating the functions which are executed on untrusted environment so that the input parameters and output of the function are only meaningful for the party which orders the execution of such a function. Although it is mentioned that this could be possible, authors have a certain level of doubts regarding its actual feasibility what comes to real life implementation. (Loureiro, Bussard, Roudier, 2001). An Ericsson Review article mentions homomorphic encryption as an alternative and says that research on this and similar techniques are promising and could provide reasonably fast processing of encrypted data without exposing it in clear text during processing. It is mentioned that it is still rather undeveloped technology and does not necessarily solve all trusted computing aspects, but may still become a complementary technology.

The use of TPMs provides a way for platform integrity validation. It also enhances and supports security audit processes and can further be used to meet compliance requirements. TPMs also support post-boot applications. One possible use could be for example validation of the software signatures for any software during load time. This could also help achieve integrity assurance on the data, not only the platform. On the other hand, it comes with a certain cost: It increases the system complexity, especially what comes to handling of upgrades (and downgrades), high-availability set-ups and hardware failures.

There are a number of options available, both open source and free to use and commercial solutions to build a virtualized environment where remote attestation, as described by TCG, can be deployed. A limitation on building such environment is that it always requires hardware support (i.e. TPMs), processes and mechanisms to handle personalization and provisioning of secret keys and a number of physical nodes. For example Ubuntu Openstack reference environment requires at least 6 physical servers. (Ubuntu Cloud Infrastructure, Community Help Wiki, 2014).

2.3. Assessment versus Audit

According to the Certified Information Systems Auditor Study Guide, an audit is a review of past history applying various techniques for collecting objective evidence and comparing this evidence against the auditing criteria. It is expected that the results of the audit are accurately reported, whether indicating conformity or nonconformity. The audit results shall be also verifiable. Generally, audits can be classified into three categories (Cannon, 2011, 15):

- Internal audits or assessments: Auditors within the organization are performing the audit inside the organization. The audit target depends on the defined scope and it could be for example a certain IT system. These types of audits can provide insight for executive governance or risk management but are generally considered to have lower assurance.

- External audits: A customer audits a supplier or vendor to verify the integrity of internal controls, transactions or compliance to requirements. The purpose can be for example to ensure that defined performance and service levels are met.
- Independent audits: An independent third party performs and audit and compares the evidence against the defined auditing criteria. The type of audits can be applied on licensing, certification or product approval purposes.

When comparing an assessment and independent audit, the main difference is that an audit must be performed by an independent third party who is both objective and impartial. An audit is a systematic inspection of records involving analysis, evidence testing and confirmation and it generates a report considered to represent a high assurance of truth. Audits performed by an independent third party are considered to provide the highest assurance (Cannon, 2011, 17). Assessments are by nature less formal and mainly used as a mechanism to collect insight on functionality of internal controls.

In the context of this thesis, the aim is to develop a framework which could be usable for an independent third party to provide constant compliance data. This does not exclude the fact that same framework could be used for internal audits or assessments.

2.4. ISO2700x Information Security Management Systems

ISO/IEC 2700x standard is a series of international standards for Information Security Management Systems (ISMS). Each of the standards in the series has its own purpose; ISO 27001 provides requirements and controls for establishing, implementing, maintaining and continually improving an information security management system and ISO 27002 provides the further reference and implementation guidance for these security controls (International Standard ISO/IEC 27001:2013)(International Standard ISO/IEC 27002:2013).

Generally speaking, an ISO2700x ISMS implementation can be described as a straightforward process, which starts from policy establishment and asset identification and ends in a situation where the organization has adopted a standardized process for managing their assets and risks related to their business and information security. When established correctly, the ISMS always has management commitment and focuses on continuous improvement through internal audits and management reviews.

On a high level the ISMS is implemented as follows: After the management has decided to implement an ISMS, and defined the ISMS policy and scope, the next step is to identify the assets, their owner and make classification and valuation for these assets. After that threats related to assets should be identified as well as vulnerabilities which can be exploited by those threats. Also, risk owners shall be identified. The risks should be evaluated based on their impact and probability, where impact relates to the asset value and probability to existence of vulnerabilities. The metrics used during the risk assessment shall be selected so that the process, when repeated, produces consistent, valid and comparable results. Once this has been done, mitigations for at least the highest priority risks should be proposed to the management or risk owners. Estimated residual risks should be also highlighted and owners need to either approve or act on them. Controls from ISO27001 standard shall be evaluated and a Statement of Applicability (SoA) of these controls shall be made. Once management has reviewed the plans and provided their authorization of ISMS implementation and operation, only then the actual implementation can begin. Once all the controls are implemented, the processes for continuous improvement need to be established. Like any organization process establishment, proper implementation requires good corporate governance and it is always done from top-down.

As ISO2700x is Information Security Management System, there are many controls which are procedural or administrative. On the other hand, some controls which sound administrative could be implemented with a tool which enforces certain pro-

cess to be followed; this could apply to for example user access management controls. One part of the complexity is that one may be compliant to the standard either way, using technical means and automated processes or doing everything manually. In any case, this means that only part of ISO27001 controls could be executed using technical methods, therefore providing automatic compliance for all controls in the standard could be considered to be impossible.

As neither ISO27001 nor ISO27002 are clearly pointing to any technical method or mechanism it may be difficult to achieve automated compliance of ISO27001 requirements. The same applies to the majority of the requirements. As mentioned, ISO27002 contains implementation guidance for requirements described in ISO27001; however, research on this standard reveals that the implementation guidance is not self-evident. As an example, for the control A.8.1.1, Inventory of assets states:

> *Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained. (International Standard ISO/IEC 27001:2013).*

ISO27002 gives following text as implementation guidance:

> *An organization should identify assets relevant in the lifecycle of information and document their importance. The lifecycle of information should include creation, processing, storage, transmission, deletion and destruction. Documentation should be maintained in dedicated or existing inventories as appropriate.*
>
> *The asset inventory should be accurate, up to date, consistent and aligned with other inventories.*
>
> *For each of the identified assets, ownership of the asset should be assigned (see 8.1.2) and the classification should be identified (see 8.2). (International Standard ISO/IEC 27002:2013).*

The wording "*should"* used on the implementation guidance may be interpreted so that this is not mandatory to follow and being used so widely, it may reduce the effectiveness of the message. Also the implementation guidance lists a number of

things that should be included in the asset inventory without pointing to actual mechanism or method to manage this.

The requirements may also be on a very high level without self-evident implementation guidance. Possibly this is due to fact that the standard is meant to be universal without any connection to certain technical solution.

2.5. SANS top 20 Critical Security Controls

The danger of implementing a security standard or requirements framework within an enterprise is that the effort turns just into an exercise of reporting on compliance. This consumes security resources and the possibility to keep track, detect and prevent constantly evolving attacks will diminish. This was identified as serious problem by U.S. National Security Agency (NSA), which began an effort with “offense must inform defense” approach, prioritizing controls that work against real-word threats. This eventually led to list called Critical Security Controls which was published and coordinated through the SANS Institute. Critical Security Controls (CSC) prioritize security controls which have been shown to work effectively. There is also notable focus on standardization and automation of these controls to gain operational efficiency and to improve effectiveness. Some controls within the Critical Security Controls are considered to create the most significant improvement and should be implemented first; they are so-called “quick wins”. (SANS Institute. Critical Security Controls - Version 5.)

For Critical Security Controls there are two guiding principles: “Prevention is ideal, but detection is a must” and “Offense informs defense”. “Offense informs defense” effectively means that one needs to have knowledge of actual attacks to be able to build effective and practical defenses and to use the controls which can be shown to stop known real-world attacks. (SANS Institute. Critical Security Controls - Guidelines.)

Critical Security Controls cover 20 different domains which are as follows:

1: Inventory of Authorized and Unauthorized Devices

2: Inventory of Authorized and Unauthorized Software

3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

4: Continuous Vulnerability Assessment and Remediation

5: Malware Defenses

6: Application Software Security

7: Wireless Access Control

8: Data Recovery Capability

9: Security Skills Assessment and Appropriate Training to Fill Gaps

10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

11: Limitation and Control of Network Ports, Protocols, and Services

12: Controlled Use of Administrative Privileges

13: Boundary Defense

14: Maintenance, Monitoring, and Analysis of Audit Logs

15: Controlled Access Based on the Need to Know

16: Account Monitoring and Control

17: Data Protection

18: Incident Response and Management

19: Secure Network Engineering

20: Penetration Tests and Red Team Exercises

(SANS Institute. Critical Security Controls - Version 5.)

Each of these domains contains a control and guidance to implement the control. For example, the control text for control "1: Inventory of Authorized and Unauthorized Devices" is:

> *Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and un-*

authorized and unmanaged devices are found and prevented from gaining access.

This control contains seven different items 1-1— 1-7 which describe in detail how the control should be implemented. (SANS Institute. Critical Security Control: 1.) The number of implementation items varies for each control.

The SANS top 20 critical security controls were developed to overcome the generic ambiguity of security standards and requirements frameworks which attempt to address risks to enterprise systems and critical data but end up failing on this task. It has a practical approach what comes to implementation of controls and detection of attacks and quite detailed instructions how each control can be actually implemented.

In this thesis, a mapping between ISO27001 controls and SANS Top 20 Critical Security Controls was done and it was interesting to observe how different approach SANS has for certain controls compared to the ISO27002 implementation guidance. For example, for the ISO27001 control 12.5.1: Installation of software on operational systems, ISO27002 suggests mainly administrative controls whereas SANS for control CSC2, Inventory of Authorized and Unauthorized Software suggests mainly technical controls.

3. Current research, tools and methods

3.1. Control Automation possibilities

There has been quite extensive research done by Montesino and Fenz regarding control automation possibilities in information security management. Their research papers from 2011 "Information security automation: how far can we go?" and "Automation possibilities in information security management" analyse how many controls from the older ISMS standard, ISO 27001:2005 could be automated. It does not only focus on technical controls, but aims to automate also procedural and adminis-

trative controls to a certain extent. They have also considered security controls from NIST SP 800-53 (Security and Privacy Controls for Federal Information Systems and Organizations) and from Consensus Audit Guidelines, which is what Critical Security Controls used to be called earlier. On the research, possible use of SCAP, Security Content Automation Protocol, is also mentioned briefly. According to Montesino and Fenz (2011, 260), a control can be automated if the operation is done without human intervention in the process; some controls can be fully automated and some partially. As criteria of whether the control can be automated or not they use following: the operation needs to be only machine-readable and processable, and that it can be implemented using a security application that they have previously selected, which are mainly commercial and open source applications and tools. According to their research using the above mentioned criteria, they argue that 27.8 percent of ISO 27001:2005 security controls could be automated. Table 1 is an excerpt of the table describing their analysis for each domain. (Montesino, Fenz, 2011 a, 2011 b).

Table 1. ISO27001:2005 controls that can be automated (Montesino, Fenz, 2011 b).

Domain	Information Security Controls			
	Controls that can be automated	*Total controls*	*Percent*	*Examples of controls*
Security policy	0	2	0	-
Organization of information security	0	11	0	-
Asset management	1	5	20%	Inventory of assets
Human resources security	1	9	11.1%	Removal of access rights
Physical and environmental security	2	13	15.4%	Physical entry controls
Communications and operations management	15	32	46.9%	Controls against malicious code
				Information back-up
				Audit logging
Access control	13	25	52%	Unattended user equipment
				Network connection control
Information systems acquisition, development and maintenance	4	16	25%	Key management
				Control of technical vulnerabilities
Information security incident management	0	5	0	-
Business continuity management	0	5	0	-
Compliance	1	10	10%	Technical compliance checking

The research does not mention, however, what are the actual controls on each of the domains that can be automated based on their criteria. (Montesino, Fenz, 2011 b).

The later research done by Montesino, Fenz and Baluja proposes a SIEM (Security Incident and Event Management) tool based framework for automation of security control. As automation criteria they have used similar criteria than on their previous research, with an addition that security operations and management of tools used for automated monitoring is handled centrally. According to their analysis, they argue that existing research focuses only on automation of some specific controls, such as vulnerability and configuration management, however it does not focus on automation of all information security controls that standards like ISO 27001 define. According to their analysis, this leads to a dispersion of tools and methods for security control automation. (Montesino, Fenz, Baluja, 2012).

The authors have selected 38 controls (out of 133 in ISO 27001:2005) that could be automated using the SIEM based framework that they propose. Comparing to their previous research, the number has increased (from 37), as it seems that they have now included the control which relates to incident handling (ISO 27001:2005 control 13.1.1.). They have furthermore grouped these controls to ten domains, visible in the table 2 below. Also, a mapping to NIST 800-53 and Consensus Audit Guidelines (i.e. SANS top 20 Critical Security Controls) has been performed in the research. (Montesino, Fenz, Baluja, 2012).

Table 2. ISO 27001:2005 controls that could be automated using SIEM based framework (Montesino, Fenz, Baluja, 2012).

No.	Control	Controls mapping		
		ISO/IEC 27001	NIST SP 800-53	CAG
1	Asset inventory (hardware and software)	7.1.1, 10.1.2, 11.4.3	CM-8, SA-7	1, 2, 14
2	Account management	8.3.3, 11.2.2, 11.2.3, 11.3.2, 11.4.2, 11.4.6, 11.5.1, 11.5.2, 11.5.3, 11.5.5, 11.5.6, 12.3.2, 12.4.3	AC-2, AC-7, AC-8, AC-9, AC-10, AC-11, AC-17, AU-14, IA-2, IA-3, IA-5, SC-17, SC-23	8, 9, 11
3	Log management	10.10.1, 10.10.3, 10.10.4, 10.10.5, 10.10.6	AU-6, AU-8, AU-11, AU-12, PE-8	6
4	System monitoring	10.3.1, 10.6.1, 10.7.1, 10.7.4, 10.9.3, 10.10.2, 11.4.6, 11.4.7, 12.4.3, 12.5.3	AC-8, AU-6, AU-7, AU-14, CA-7, CM-3, IR-5, MP-2, PE-6, SA-10, SC-5, SC-14, SI-4, SI-5, SI-7, SI-13	6, 8, 13, 15
5	Malware protection	10.4.1, 10.8.4	SI-3, SI-8	12
6	Vulnerability scanning and patch management	11.4.4, 12.6.1	RA-5, SC-14	7, 10
7	Security assessment and compliance checking	10.1.2, 10.6.1, 11.4.4, 11.4.6, 11.4.7, 15.2.2	CA-2, CM-2, CM-3, CM-6, SC-7, SC-14	3, 4
8	Information backup	10.5.1	CP-6, CP-7, CP-9	19
9	Physical security	9.1.2, 9.2.2	PE-3, PE-11, PE-12, PE-13, PE-14	–
10	Incident management	13.1.1	IR-4, IR-5, IR-6	18

Note: Mapped to ISO/IEC 27001, NIST SP 800-23 and CAG

Based on this, Montesino et al. have proposed a SIEM based framework for automation of security controls, visible in the following Figure 3. In the research, each domain is elaborated in more detail and it has been described how SIEM can support automation of controls on this specific domain. (Montesino, Fenz, Baluja, 2012).

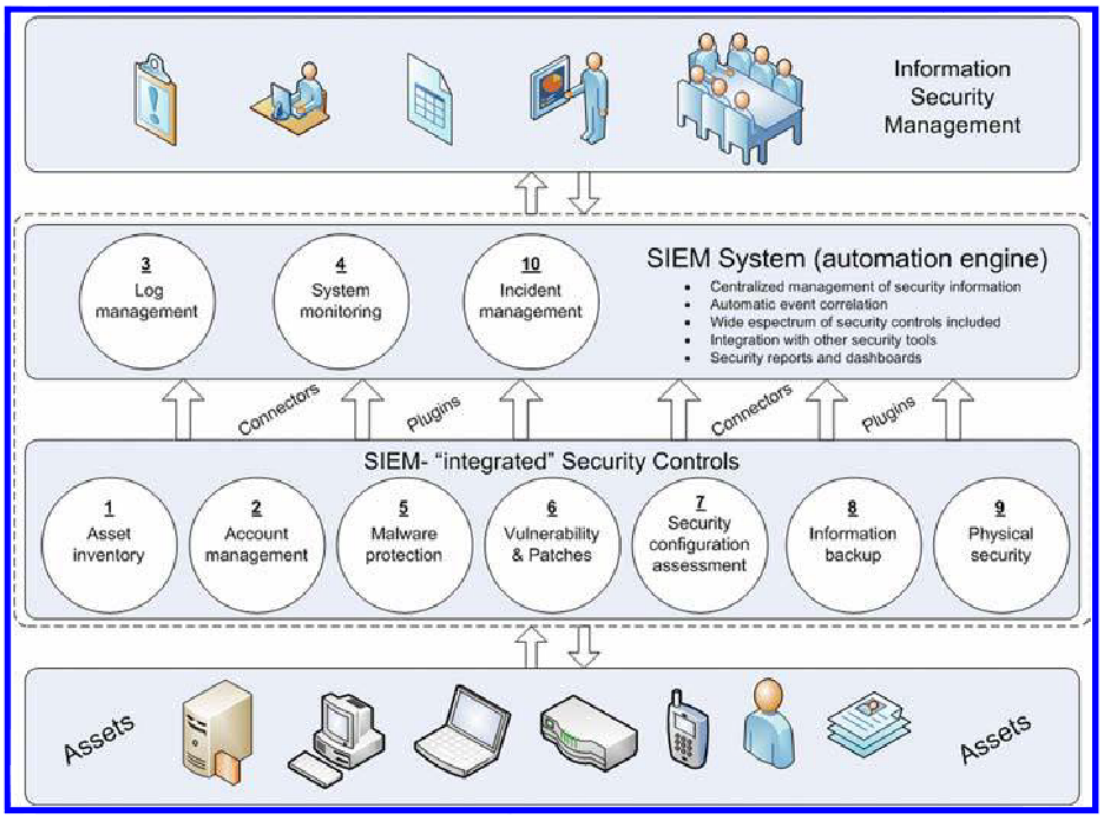

Figure 3. SIEM-based framework for security controls automation (Montesino, Fenz, Baluja, 2012).

Although this thesis focuses on compliance automation of technical ISMS controls, rather than automation of the information security controls, research from Montesino et al. has shown to be a valuable source of information. It shows that based on the automation criteria they have chosen it could be argued that ISMS security controls could be automated up to a certain level. This could be considered to be a prerequisite for compliance automation as well. From the compliance perspective, maybe one missing component from the framework they have proposed is the integrity protection of platforms, security configuration data and audit evidence.

3.2. Security Content Automation Protocol

The number and variety of systems in organizations may be extensive; however, it still needs to be possible to respond quickly to new threats. This equation may become quite challenging due to lack of interoperability in tools for system security.

Organizations may also need to demonstrate compliance against standards and regulations, such as Federal Information Security Management Act (FISMA), Health Information Portability and Accountability Act (HIPAA), Sarbanes-Oxley (SOX), etc. The Security Content Automation Protocol, SCAP, was developed by NIST (National Institute of Standards and Technology) to address these issues: to provide an automated and standardized way to maintain security of enterprise systems, especially considering implementation and assessment of security configuration baselines, vulnerability assessment and verification of the present patches. (Quinn, Scarfone, Waltermire, 2012, page 6).

SCAP is a series of specifications to standardize the format and naming format used to describe security configuration and vulnerability information. (The word “protocol” in SCAP refers to series of specifications, it should not be interpreted as set of rules governing the exchange or transmission of data between devices as defined in computing generally.) Particular specifications in SCAP are known as the SCAP component specifications. The security information used by the protocol is known as SCAP content, which includes standards for presenting vulnerabilities, security configuration and platform identification data. The following table 3 presents SCAP version 1.2 component specifications. (Quinn, Scarfone, Waltermire, 2012, page 7).

Table 3. SCAP Version 1.2 Component Specifications (Quinn, Scarfone, Waltermire, 2012, page 8).

SCAP Component	Description
Languages	
Extensible Configuration Checklist Description Format (XCCDF) 1.2	A language for authoring security checklists/benchmarks and for reporting results of evaluating them
Open Vulnerability and Assessment Language (OVAL) 5.10	A language for representing system configuration information, assessing machine state, and reporting assessment results
Open Checklist Interactive Language (OCIL) 2.0	A language for representing assessment content that collects information from people or from existing data stores made by other data collection efforts
Reporting Formats	
Asset Reporting Format (ARF) 1.1	A format for expressing the exchange of information about assets and the relationships between assets and reports
Asset Identification 1.1	A format for uniquely identifying assets based on known identifiers and/or known information about the assets
Enumerations	
Common Platform Enumeration (CPE) 2.3	A nomenclature and dictionary of hardware, operating systems, and applications, plus an applicability language for constructing complex logical groupings of CPE names
Common Configuration Enumeration (CCE) 5	A nomenclature and dictionary of software security configurations
Common Vulnerabilities and Exposures (CVE)	A nomenclature and dictionary of security-related software flaws
Measurement and Scoring Systems	
Common Vulnerability Scoring System (CVSS) 2.0	A system for measuring the relative severity of software flaw vulnerabilities
Common Configuration Scoring System (CCSS) 1.0	A system for measuring the relative severity of system security configuration issues
Integrity Protection	
Trust Model for Security Automation Data (TMSAD) 1.0	A specification for using digital signatures in a common trust model applied to other security automation specifications

To simplify how SCAP could be used: A tool that supports SCAP specifications may do automated scans based on a SCAP checklist (expressed with XCCDF, Extensible Configuration Checklist Description Format) that are defined in OVAL (Open Vulnerability and Assessment Language) format. In addition, the tool may be capable of fetching data from users or other data sources using OCIL (Open Checklist Interactive Language) formatted queries. In SCAP checklist platforms are defined using CPE (Common Platform Enumeration) format, security settings with CCE (Common Configuration Enumeration) and software vulnerabilities with CVE (Common Vulnerability Enumeration). Each of the SCAP components may be used also independently, nevertheless, one of the main purposes of the standard is to provide benefits by using them together. SCAP content is available from multiple sources, such as NVD (National Vulnerability Database, http://nvd.nist.gov/), through The National Checklist

Program (NCP) Repository, (http://checklists.nist.gov/) and from vendors (for example, SUSE Linux Enterprise OVAL Information Definition Repository: http://ftp.suse.com/pub/projects/security/oval/). (Quinn, Scarfone, Waltermire, 2012, pages 8 - 9).

Koschorreck examines in the research paper, "Automated Audit of Compliance and Security Controls", possibility to use SCAP-based solution for automated audit compliance. SCAP components (especially XCCDF and OVAL) are implemented in a tool called UPW Compliance Guard and examples are given, how automated audit compliance could be achieved for particular security controls. One conclusion that can be drawn from this work is that if data collection and compliance decision making is done automatically (i.e. without human intervention) for a specific control, it could be possible to have automated audit compliance (for particular control.) (Koschorreck, 2011).

NIST maintains a validation program for SCAP products via accredited SCAP laboratories to make sure that validated products conform to SCAP requirements. At the time of writing this thesis, there are five products conforming to SCAP 1.2; four commercial and one open source software called OpenSCAP. (Security Content Automation Protocol Validated Products, 2014.) The open source project is sponsored by RedHat, but as open source software it is applicable to number of platforms. For example, how to use it for SUSE Linux Enterprise Server and openSUSE is described in following articles: "OpenSCAP in SUSE Manager" (SUSE, 2014) and "Detecting Vulnerable Software Using SCAP/OVAL" (Adams, 2011).

For automated security compliance, using a SCAP capable product might be an interesting and feasible option. It is not possible to cover all the technical controls with just SCAP, nevertheless, it offers a good basis to build on. There are not that many certified SCAP capable products yet, but the fact that there is an open source certified product makes the implementation threshold smaller, especially for small and medium sized environments. MITRE, a US non-profit organization specializing in high

technology systems engineering, lists currently 45 organizations (for 63 products) which are participating in the OVAL Adoption Program. The program aims to educate vendors on best practices for OVAL implementation and give declaration regarding a product's OVAL capabilities. Capabilities and their relationships are described in the following Figure 4. (MITRE, 2013). Based on this it can be concluded that there are quite many products which have or aim to have at least some OVAL capabilities so it is not only handful of products which have adopted it. It should be noted still, that adopting OVAL does not mean that a product fully conforms to SCAP; it could be just XCCDF and OVAL for example in a case of OVAL based Definition Evaluator (from figure below).

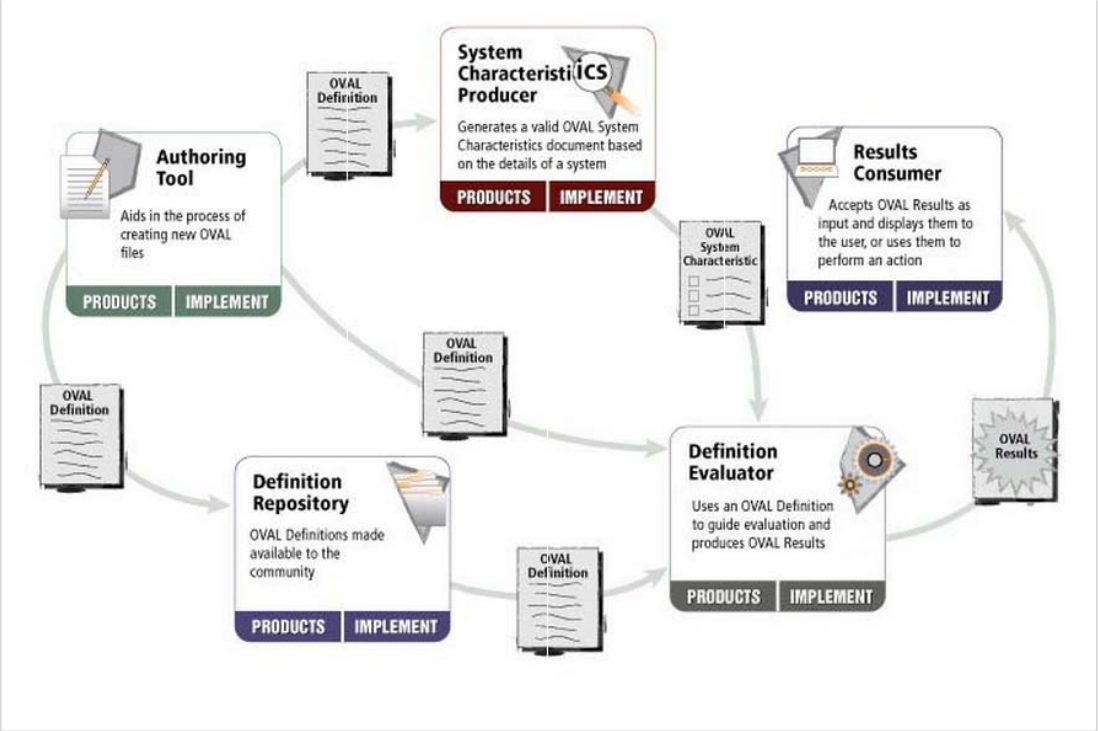

Figure 4. Defined OVAL capabilities in MITRE OVAL Adoption Program (MITRE, 2013).

3.3. ISO27001 Compliance Tools

When searching for compliance tools for ISO27001, it is quickly noticed that there seems to be a massive amount of different kinds of tools promising to support an ISO27001 Compliance Program. The main observation was that in general the tools could be grouped into three different categories.

Administrative tools, which are mainly used to manage an ISMS and processes related to it. They may contain different features for policy management, risk management, manual asset management, gap analysis, etc. The common nominator in all administrative tools is that they require human interaction, i.e. a user needs to operate the tool and feed in the details. The reason for this is mainly that they relate to controls which cannot be automated. Ahmet Erkan has analysed in his Master's Thesis "An Automated Tool for Information Security Management System" 16 different ISMS automation tools which are all mainly administrative. (Erkan, 2006). Some of the administrative tools are checklists or questionnaires where controls are assessed manually by asking certain questions related to them. The tool eventually provides a report stating how well each of the ISO27001 requirements is implemented providing a gap assessment towards the standard controls. An example of such a tool is provided in the research paper from Heru Susanto, Mohammad Nabil Almunawar and Yong Chee Tuan "A Novel Method on ISO 27001 Reviews: ISMS Compliance Readiness Level Measurement". (Susanto, Almunawar, Tuan, 2012). Another similar type of tool is provided by a company called "verinice." (verinice,2014).

Technical tools that provide certain security controls such as asset management and discovery, vulnerability assessment/management, configuration management, file integrity monitoring, centralized audit logging and analysis, threat detection, security incident and event management (SIEM) capabilities, etc. These are not compliance tools as such, although they provide compliance data and some may even provide compliance reports against different mandates. Examples of such tools are Alienvault Unified Security Manager, Tripwire Enterprise File Integrity Manager, Tripwire IP360, ManageEngine Eventlog Analyzer and Tenable SecurityCenter Continuous View.

These kinds of tools may be used as standalone products; however, they can also be part of a policy compliance tool. (Alienvault USM, 2014. Tripwire Enterprise File Integrity Manager datasheet, 2014. Tripwire IP360 v7.4 datasheet, 2014. ManageEngine Eventlog Analyzer, 2014. SecurityCenter CV Features, 2014.)

Policy compliance tools are especially designed to provide compliance data and reports for different mandates. These tools may have multiple different components (which may also be used as standalone products) providing similar functionalities as those mentioned previously, but with the difference that a policy compliance tool integrates these modules into single tool which aims to provide mandate-based reporting. Policy compliance tools may also be able to automate the assignment and management of roles and responsibilities. In many cases the reports are highly customizable, allowing an organization to measure risk and track the performance of its security and compliance programs in better way. These types of tools may also provide reports which help prioritize the remediation efforts based on the criticality of the findings and the risk posture the organization has. Examples of such tools are Qualys Policy Compliance, Tripwire Enterprise 8.3 and Symantec Control Compliance Suite (Qualys Policy Compliance, 2014. Tripwire Enterprise 8.3 product brief, 2014. Symantec Control Compliance Suite, 2014. Creech, Alderman, 2010.)

4. Framework proposal

The framework is proposed based on the analysis of theoretical base, current research, tools and methods. It includes ISO27001:2013 controls which could be automatically audited, a methodology to do this and guidance on how this could be fulfilled. The framework consists of three parts; framework selected controls, architecture and guidance how to use it.

4.1. Framework Selected Controls

As stated earlier in this thesis, describing compliance for a certain mandate may be difficult if the requirements are not precisely specified. For the framework proposal it

must be determined, what the technical controls in ISO27001 are which could be considered for automation, and whether compliance to this control could be automatically measured. The chosen approach to answer this question was to go through each of the ISO27001 controls and to answer following questions:

1. Can this control be implemented by technical means (i.e. it is not administrative control, policy or process)?
2. When measuring control compliance, could this operation be machine readable and processable? (I.e. would not require human intervention. This selected criteria is similar than the one used by Montesino et al. in their research.)

During the process it was also considered what could be then actually implemented for the proof of concept part which is feasible and measurable, how to do the verification and how the verification of compliance could be automatically measured. When going through the controls it was seen that it is possible to answer "yes" to the first question above in many cases; however, the answer to the second question in many cases could be "partially yes" and not definitely yes or no. Even so, controls where the answer was "partially yes" were selected as well. If the answer was clearly no to either of the questions, related control was disregarded.

Due to the fact that SANS top 20 Critical Security Controls have a practical approach compared to the somewhat indefinable approach that ISO27002 has in its implementation, SANS top 20 CSC was chosen as one of the main inputs when defining what to actually implement for each selected ISO27001 control. In order to decide what to actually implement, the following sources were used: SANS top 20 Critical Security Controls (SANS Institute. Critical Security Controls - Version 5, 2014), mapping of the ISO27001 controls to the SANS critical security controls (SANS Critical Security Controls Poster, 2014.), ISO27002 Code of practice for information security controls (International Standard ISO/IEC 27002:2013) and a presentation regarding how to protect against computerized corporate espionage (Jarno Niemelä, 2013). Based on this, a worksheet was created which includes the selected control number (according to ISO27001), a domain name (assigned for the control used in this framework proposal), heading of the control and control text (according to ISO27001), what to ac-

tually implement, a verification method and what to measure in order to determine control compliance. The worksheet also includes a mapping to SANS top 20 Critical Security Controls.

Then, the previous research from Montesino et al. (Montesino, Fenz, Baluja, 2012.) was used as a further input. The controls which they claimed that can be automated for ISO27001:2005 using the automation criteria they have specified, were mapped to latest ISMS standard, ISO27001:2013 using a mapping guideline from British Standards Institution (BSI), (Mapping between the requirements of ISO/IEC 27001:2005 and ISO/IEC 27001:2013, 2013). It was then analysed which domain (in the framework proposal) these controls would belong to and if there were any controls which could be added to the worksheet. Also, based on the input material it was analysed if there was anything else that would be needed to be implemented for the already selected controls. The observation was that SANS Critical Security Controls cover all technical security controls that Montesino et al. suggest in their research. The control selection workflow is described in Figure 5 below.

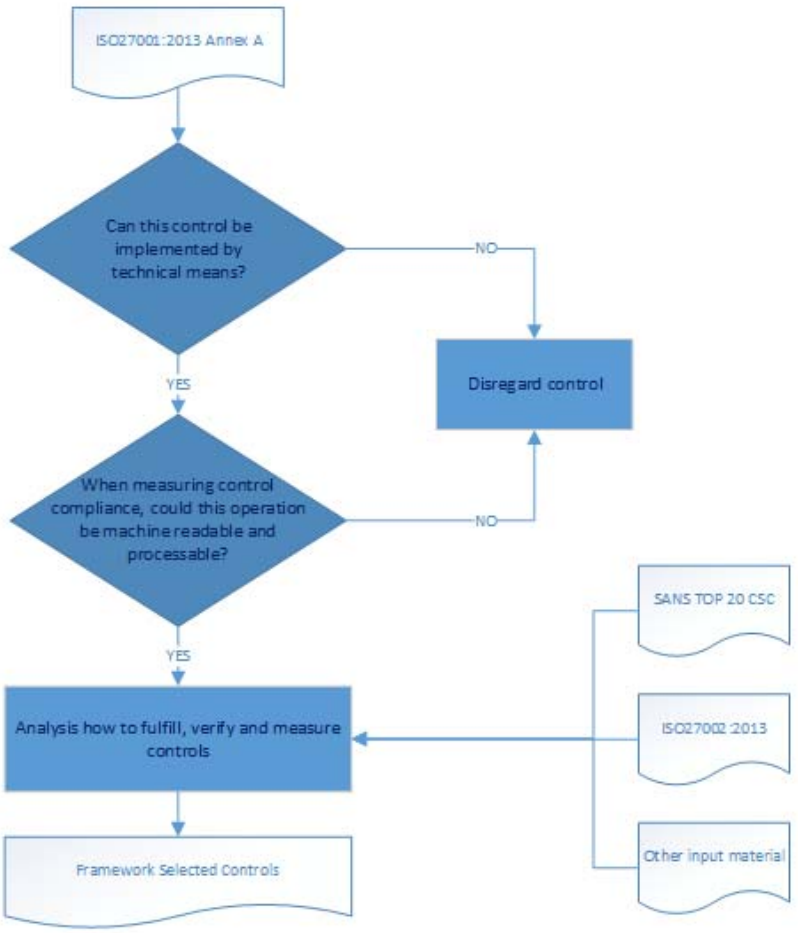

Figure 5. Control selection workflow

Based on this, the worksheet were refined as well as the controls which can be implemented using technical means and audited automatically. As this thesis focuses on automatic compliance rather than controls automation (as the research done by Montesino et al.) the list of selected controls is quite much shorter than presented in previous research. Also, previous research has been using ISO27001:2005 and the number and nature of controls has changed quite much on ISO27001:2013.

On the framework selected controls worksheet (at Appendix A.) the measurement column is divided into two different columns called “Measurement (Monitoring System)” and “Measurement (Domain Component)”. The term “Monitoring System” could be interpreted as a synonym for a SIEM or compliance tool, in other words it is

expected that it is a tool capable of providing this type of measurement data so that it can be said that compliance is achieved. However, it is not possible to implement all the controls only in the Monitoring System, part of that needs to take place in the monitored asset or in a system which provides certain functionality, such as user management. Therefore, a part of the measurement needs to occur outside of the Monitoring System in a component which provides dedicated functionality and that is called “Domain Component”. For example, to detect if there are any disabled user accounts, one could do a query to the user management system (such as Active Directory, LDAP, etc.). If the Monitoring System were tightly integrated to the Domain Component, it could also query this information and provide more detailed evidence for control compliance.

The worksheet is presented in Appendix A. Framework Selected Controls.

4.2. Framework Architecture

The proposed framework is presented in the Figure 6 below.

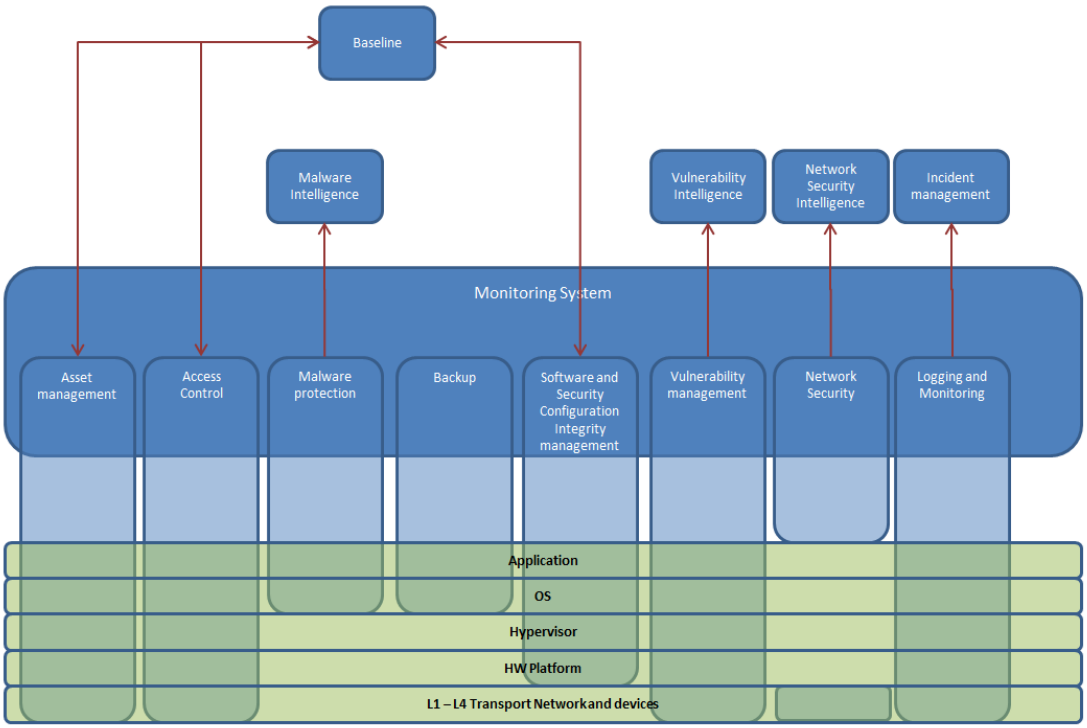

Figure 6. ISMS Compliance framework

In the middle of the above figure there is the Monitoring System; a tool that is expected to provide essential security capabilities and to provide compliance data and status information. Closely integrated to the Monitoring System reside the Domain Components (overlapping with Monitoring System on above figure, described in more detail below). Domain Component functionality may be achieved with the Monitoring System. However, this could also be achieved using an external tool which provides the functionality. For example, asset management could be carried out using dedicated software which could be then integrated to the Monitoring System. Nevertheless, many SIEM and information security compliance tools may already include asset management capabilities.

On the bottom part of Figure 6 there are six layers to represent the assets. Following is a short description of each layer:

- "Application" represents any applications that the guest machine is running.
- "OS" is the operating system of the guest machine, i.e. running on top of a hypervisor
- "Hypervisor" is a layer that runs virtual machines, i.e. host machine
- "HW platform" is a physical HW such as server, workstation, etc.
- The lowest layer is called "L1 – L4 Transport Network and devices", meaning network medium and devices, such as switches, routers, firewalls, IDS/IPS devices etc. mainly working on OSI layers 1 to 4.

Following is a short description of each of the Domain Components:

- Asset Management – The component which handles automatic asset discovery and inventory for hardware and software. The inventory shall include all hosts from the network which have an IP address. Once the component is authenticated to a host, it shall analyse installed software. The inventory shall include at least the operating system and application versions. The component shall be able to detect any new hosts added to the network and unauthorized changes in software (i.e. a deviation compared to the expected inventory or baseline) and alert security personnel in these cases.

- Access Control – The component which takes care of user registration, de-registration and access provisioning, including secure log-on procedures and password management. The component shall be able to monitor the use of accounts and disable in-active accounts. Changes on user privileges shall be detected as well as failed and successful authentication events.
- Malware Protection – The component which takes care of controls against malicious software. It includes several detection, prevention and recovery controls against malware, such as application whitelisting, file integrity monitoring, file reputation queries, centrally management anti-virus software, application access restrictions, etc. The component uses external sources (for example anti-virus vendor malware signatures) as intelligence to fulfil the controls. An alarm or event shall be triggered to inform security personnel when a malicious activity is detected.
- Backup – The component which manages backups. Failures to take the back-up or to verify the backup image's integrity shall be detected and security personnel shall be alerted.
- Software and Security Configuration Integrity management – The component which includes several controls to manage installation of software and to maintain integrity of the system. For example: platform, runtime and transaction integrity could be verified by using trusted execution technology and remote attestation. The security configuration could be checked against standard, best practice or policy using for example SCAP compliant tool. Changes shall be detected and security personnel shall be alerted.
- Vulnerability management – The component which includes controls to perform vulnerability management. It scans the network periodically for vulnerabilities. When vulnerabilities are found security personnel shall be alerted.
- Network Security – The component that includes network level security controls, for example monitoring of network traffic, IDS functionality, honeypots, segregation of networks, etc. Security personnel shall be alerted of violations of the network policy.

- Logging and Monitoring – The component which manages audit logging and monitoring. It includes controls which aim to detect suspicious user activity as well as controls related to log management in general.

Figure also presents which asset layer each of the Domain Component is affecting.

4.3. Using of the framework - Risk based approach

When using the framework, it is suggested that a risk based approach is used to select the controls. Based on the risk assessment results, controls from the framework selected controls list shall be chosen to mitigate the vulnerabilities related to the risks. Once the controls are implemented, the *framework selected controls* list can be further used to perform control verification and measurement. As a result for each control that is implemented, a measurable event can be provided.

The steps in order are:

1. Risk assessment
2. Selection of controls from the framework to mitigate the vulnerabilities related to the risks
3. Control implementation
4. Control verification
5. Control measurement

As subsequent risk management activities are taken, the Framework Selected Controls list may be used again to implement, verify and measure new controls to the environment.

5. Proof of Concept

5.1. Overview

A proof of concept provides empirical evaluation of the feasibility of the proposed framework. The scope of the PoC is to focus on the controls for the Monitoring System to understand if tools selected for the PoC could fulfil the framework. The research is done according to following steps:

1. Building of the test environment which corresponds to the actual environment to which it is intended to implement the framework.
2. Selection and implementation of the controls from the Framework Selected Controls worksheet was based on a potential risk level for this type of environment. The measurement part of the selected controls is used as evaluation criteria.
3. Deployment of the selected tools to the PoC environment one-by-one.
4. Performing the evaluation using evaluation criteria, scoring and analysis of the fulfilment of controls.
5. Conclusions.

5.2. Environment

The PoC environment is a test environment which simulates the actual environment to where it is intended to implement the framework. Due to the sensitivity of the framework target deployment environment, the test environment was only built using some of the same principles as the actual environment, however, many of the components used here differ from those actually used. The environment is described in Figures 7 and 8.

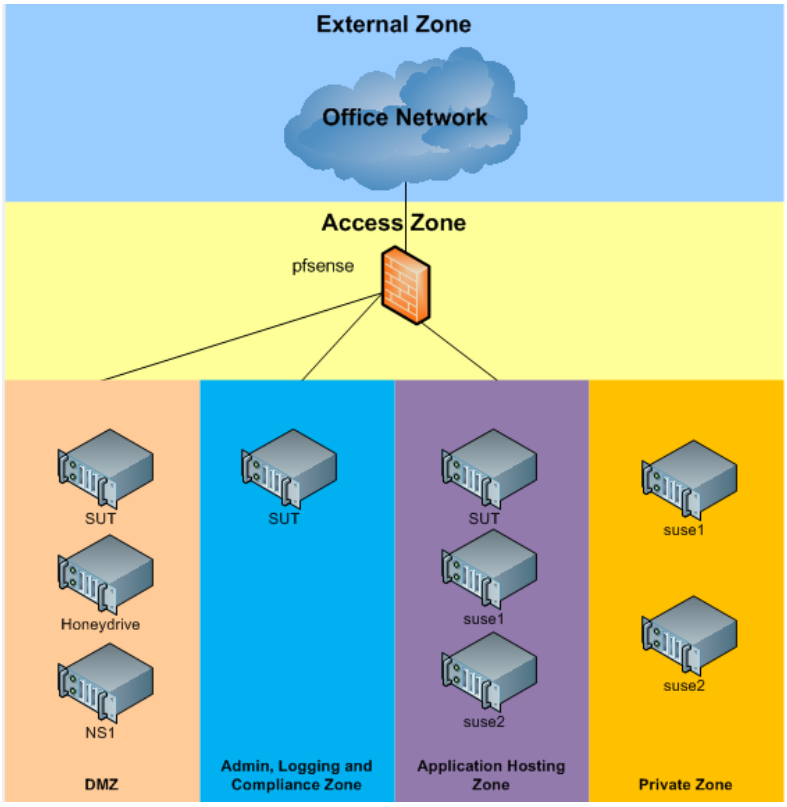

Figure 7. Functional specification

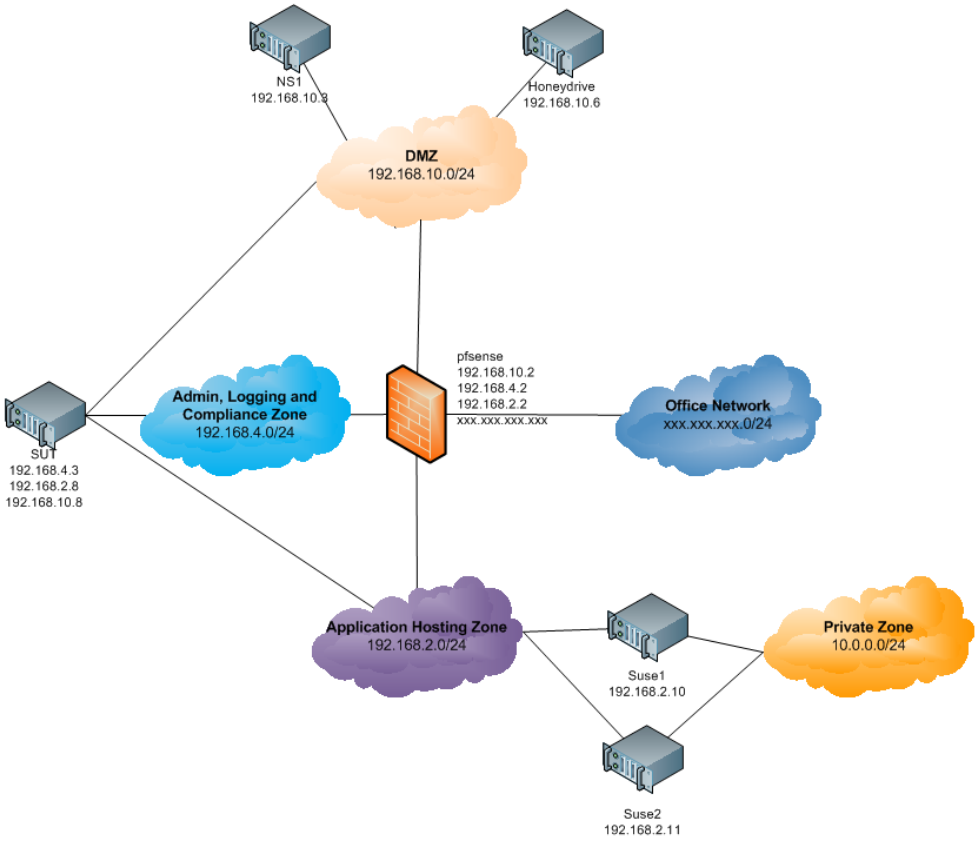

Figure 8. Addressing scheme

The environment consists of different segregated networks with different dedicated functionalities as described on Figure 7, where the communication is restricted using pfsense firewall. Pfsense was configured to push the firewall logs and netflow data to the tool which was under testing.

On Figures 7 and 8, SUT is System Under Test, a tool which is being tested against evaluation criteria to understand if the framework could be fulfilled. NS1 is a server on DMZ which runs internal www-proxy, SMTP server and DNS server. The proxy server requires authentication to be able to provide an access to external proxy (reachable via Office Network). Whitelisting functionality is added to DNS, SMTP and Proxy servers so that domain name queries and mail sending is allowed only to pre-defined domains. The logs from all services running at NS1 are pushed to the SUT. BSM (Basic Security Mode) audit logging was configured on the servers NS1, suse1 and suse2 for the "/etc/" folder. It can provide detailed audit logging for any file access related events such as reading and modification of the file.

Servers on Application Hosting Zone are providing different type of web based services. In addition, there was a Kali Linux which could be deployed to any network that was used for control verification.

Honeydrive server is running different honeypot servers; during the PoC honeypot services called honeyd and kippo were used. It is based on a ready-made honeypot bundle linux distro (http://bruteforce.gr/honeydrive). The logs are pushed again to the SUT to analyse if it is possible to use this information as threat intelligence.

All the systems in the test environment are running on VMware Workstation using virtual host networks. The HW platform was HP DL 380 G7 with 8GB of RAM and quad core Intel Xeon processor.

5.3. Tool Selection

Three different tools were selected for the PoC:

- Vulnerability Management Solution (SecurityCenter Continuous View by Tenable Network Security)
- SIEM Solution (Alienvault's Unified Security Management)
- Policy management solution (Qualys Policy Compliance from Qualys)

Administrative tools were not tried on this thesis as the focus was on technical controls.

These particular vendors were chosen because their products have been highly ranked by SCMagazine (a magazine which focuses on IT security news and security product reviews) in 2014 yearly awards and also since they are mentioned on SANS Critical Security Solutions Poster to fulfill certain controls. According to SCMagazine, Alienvault Unified Security Management (USM) was a finalist in "Best SIEM Solution" category and highly recommended as "Best SME Security Solution." Qualys Policy Compliance was a winner of Best Risk/Policy Management Solution category and Tenable Network Security SecurityCenter Continuous View was a Winner of the "Best Vulnerability Management Solution" category. (SCMagazine Awards Europe 2014 Results, 2014. SANS Critical Security Controls Poster, 2014).

During the selection of the tools it was also analysed if it is possible to deploy a certain tool to the test environment. The intention was to test Tripwire Enterprise 8.3 initially. However, it was seen that it would be too difficult to deploy it and because of that this was not done.

5.4. Evaluation Criteria

A number of controls from the framework were used as evaluation criteria. The controls were selected based on a potential risk level of this type of environment also considering the applicability of controls to the environment to which this framework is intended to be implemented. The business motive is to mitigate vulnerabilities

related to certain specific risks. On the PoC it was tested if the chosen tool could fulfil the framework's Monitoring System part and that was being measured using the evaluation criteria questions. The evaluation criteria are presented on Table 4.

Table 4. Evaluation criteria

EC-x	Domain	Evaluation criteria
EC-1	Asset mgmt	Is the monitoring system capable of detecting new hosts? (If so, how long does it take that this could be noticed?)
		Is the monitoring system capable of detecting new software modules on hosts? (If so, how long does it take that this could be noticed?)
		Is it possible to define rules for expected and unexpected changes in asset management database and create alarms based on those rules?
EC-2	Vulnerability mgmt	Is the monitoring system capable of generating an alarm in case new software vulnerabilities are found?
		Is the monitoring system capable of generating an alarm if a scan fails?
		Is the monitoring system capable of providing criticality scoring based on risk level? (for example CVSS-based)
		Is the monitoring system capable of detecting and creating an alarm if new listening ports are detected?
		Is the monitoring system capable of detecting new hosts in the network that are serving non-documented ports?
EC-3	Software and Security Configuration Integrity management	Is the monitoring system capable of detecting and creating an alarm in case files in the scanned system have been changed? Does this alarm contain information who made the change and when?
		Is the monitoring system capable of performing security configuration checks against pre-defined baseline/standard/best practice?
		Is the monitoring system capable of detecting and creating an alarm in case there have been changes in the software asset inventory?
EC-4	Access Control	Is it seen from the monitoring system when new users are added or removed?

		Is it seen from the monitoring system what type of privileges a user has for each system (for example under certain group?)
		Are access attempts with deactivated account visible in the monitoring system?
		Is it possible to see from a monitoring system that user is about to expire?
		Does the monitoring system offer a possibility to perform baseline checks and compare the results to the system's current user account list periodically?
		Is it possible to see from the monitoring system if user authentication fails?
		Is it possible to see from the monitoring system if user authentication succeeds?
		Is security event in the monitoring system raised after number of failed authentication attempts?
		Are there any accounts which are: - not authorized - only in one system - generic (not bound to user account) - not having expiry date? - locked-out - disabled - with passwords that exceed the maximum password age - with passwords that never expire - are there any system accounts which are not supposed to be there (i.e. no business owner). And can the monitoring system provide a list of these accounts?
EC-5	Logging and Monitoring	Is the monitoring system able to receive, correlate and create events for the log events (defined in test sequence)?
		Does the monitoring system preserve the integrity of the logs?
		Is the integrity of audit logs checked periodically?
		Is it possible to observe and analyse afterwards what has been done during the administrative session?
		Is the monitoring system capable of raising alarms to certain type of administrative actions (for example use of commands sudo or su)?
		Is an alarm raised if system time or time sources

		are re-configured?
EC-6	Network Security	Is it possible to define the current network policy to the monitoring system?
		Is the traffic monitoring system able to capture and create an alarm on traffic which violates the current policy?
		Does the log event contain enough details about the traffic information (for example time, date, system id, source IP, destination IP, packet details)?
		Is the monitoring system able to detect network scans for DMZ (using for example an IDS as intelligence)?
		Is modification of configuration on router, switch or firewall being detected?
		Is the monitoring system able to use logs from honeypots, DNS, proxy, mail server and firewall as threat intelligence?

5.5. Framework PoC Testing

The tools which were used to evaluate the feasibility of the proposed framework are presented on subsequent chapters. Also the observations made during the testing and the overview of the results is presented for each tool. Comparison, summary and analysis of the results is performed on the chapter 6.

5.5.1. Tenable SecurityCenter Continuous View

According to SC Magazine, Tenable SecurityCenter Continuous View (CV) could be described to be one of the industry's best vulnerability management tools. It combines Nessus vulnerability scanner with Tenable's Passive Vulnerability Scanner (PVS) and Log Correlation Engine (LCE) components. (Stephenson, 2014.) SecurityCenter CV has an extensive set of features such as discovery of assets, vulnerability scanning (using Nessus and PVS), configuration audits, network behaviour analysis and event log collection, normalization and categorization. (Tenable SecurityCenter CV, 2015.)

Nessus is an active vulnerability scanner capable of doing multiple different types of security checks and it can be used to scan targets with or without user credentials.

When scanning with credentials, it can perform much deeper checks on installed software and security configuration. PVS is a component which is listening to network traffic passively and is monitoring it on the packet level. It is capable of discovering new hosts and vulnerabilities on the data passed over in the network. It can also identify if application behaviour has changed, for example in a case where it has been compromised. (Tenable Passive Vulnerability Scanner Features, 2015.)

LCE provides centralized logging capabilities and performs analysis for any type of log data. Using the log analysis it can effectively detect anomalies, use of privileges, file integrity changes, etc. To collect audit trails from Linux servers, an LCE client needs to be installed to the monitored host. The LCE client can also provide file integrity monitoring. (Tenable Log Correlation Engine Features, 2015.)

Each of the components that SecurityCenter CV provides has also its own user interface and can be used separately. However, SecurityCenter CV could be considered as a centralized interface to access and analyse the security analytics data gathered by these components. It can use data gathered from the different components and combine this intelligence to create a variety of different types of reports.

Installation and Observations

For the evaluation, Tenable provided SecurityCenter CV as an appliance in virtual image which included Nessus and PVS. Basic installation and configuration to the test environment was easy to execute without any major issues. The documentation is comprehensive and provides sufficient details so that the task can be completed successfully. The LCE server was installed as a separate component, also provided by Tenable in a virtual image. This added one additional server to the Admin, Logging and Compliance zone, visible in Figure 9.

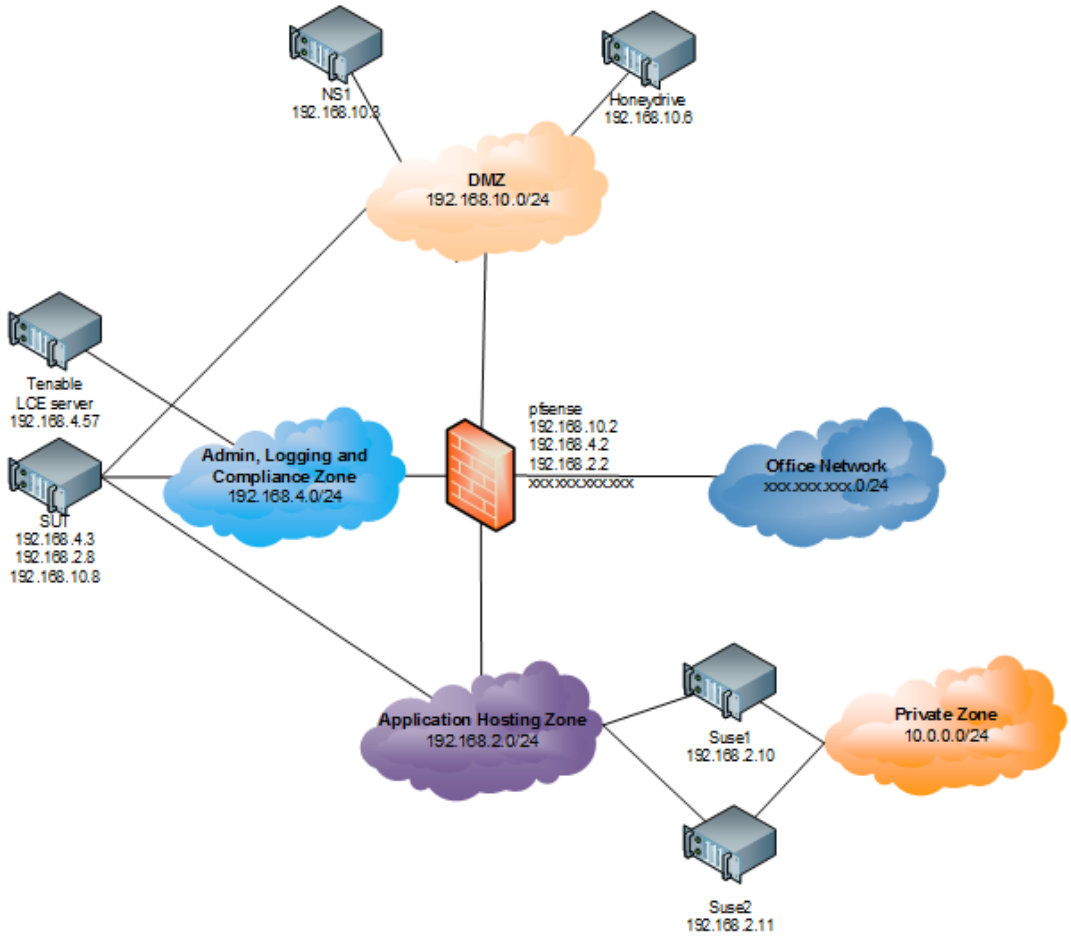

Figure 9. PoC environment with Tenable SecurityCenter Continuous View and LCE

PVS events were being forwarded to LCE server, and this needed to be configured via PVS's own management console.

LCE clients were installed to the monitored servers; (NS1, suse1 and suse2 in Figure 9). LCE clients were configured to send the audit log events to the LCE server. Also application (DNS, SMTP and proxy -server) audit log events were being sent to LCE server. The firewall was configured to send its audit log events to the LCE server via syslog.

As SecurityCenter CV is also capable of receiving Netflow traffic, the firewall was configured to provide Netflow data as well. More detailed correlation and analysis of Netflow data was performed by the LCE server.

After the installation and basic configuration the task which required the most effort was control configuration, verification and measurement of each of the items in the evaluation criteria.

Results

The results are analysed here for Tenable SecurityCenter Continuous View for each evaluated domain, detailed results are visible in Appendix B.

EC-1 Asset Management: Tenable SecurityCenter Continuous View is capable of detecting new hosts in the network immediately when it sends or receives traffic. It is possible to create dynamic asset lists which are being updated based on this information. It is also possible to classify the hosts which have appeared but have never been scanned for vulnerabilities. The tool is also capable of doing software enumeration when it is being scanned using credentials and detect if new software has been installed.

EC-2 Vulnerability Management: The main purpose of Tenable SecurityCenter Continuous View is to do vulnerability management and it is clear that this is the area which it handles best. Using Nessus, PVS and LCE it is capable of finding server- and client based vulnerabilities. (For a server based vulnerability, a service which is hosted is exploitable and for a client based vulnerability, it is the client software. In the latter, exploitation in many cases requires that a user performs an action by going to a malicious web-site for example, which then executes the exploit.) It can also detect new ports and services as they appear in the network and create alarms for them.

EC-3 Software and Security Configuration Integrity Management: File integrity monitoring is mainly managed by the LCE client. When the file integrity changes, in order to detect who made the change, additional auditing capabilities need to be configured, for example BSM (Basic Security Mode) audit logging. It is possible to validate the security configuration also against pre-defined baseline. Tenable provides pre-formatted CIS (Center for Internet Security) audit files for various operating systems. CIS is an organization which provides best-practice secure configuration benchmarks and security automation content. SCAP compliant checks are possible to do against operating systems for which there is a possibility to get an audit file, usually provided by NIST. When using SCAP baseline xml files, it is required to re-format them so that they can be interpreted as audit files in SecurityCenter. Tenable provides a tool for this purpose (called xTool). In case there have been changes in the software asset inventory, those can be detected using customized reports.

EC-4 Access Control: Addition and removal of users is being detected if the LCE client is installed on the host. The LCE client can also provide the information about user privileges. Otherwise it is quite dependant on the logging that host provides. For the Windows OS, SecurityCenter CV offers a User Management plugin and that could do a number of queries (for example regarding users that are about to expire or perform baseline checks), however, this type of plugin does not exist for the Linux OS.

EC-5 Logging and Monitoring: The test sequence as defined for control A.12.4.1 (See Appendix A, verification method column for control A.12.4.1) consists of actions that are attempted as unauthorized and authorized users and then it is checked whether the monitoring tool is able to receive and correlate those events and create alarms for them. Tenable SecurityCenter CV was configured to receive the events (sent as BSM audit logs) which appeared as unnormalized LCE events. (Unnormalized event in this context is a term used by Tenable to classify events that are received but not parsed by any special type of plug-in). For this type of event, it is possible to create a query and then a workflow based on that if it is known what types of events to expect. The integrity of the logs received by the tool is not being preserved or checked

i.e. to fulfil requirements to preserve log integrity another log storage which does that would be required.

EC-6 Network Security: It is not possible to make Tenable SecurityCenter CV aware about the network policy, but on the other hand it is capable of seeing all the traffic on the network if configured correctly. Also, if firewall logs are forwarded to LCE, alarms can be created for any types of events that appear on the firewall log. This applies to any type of log coming from any device. The tool is also able to detect network and service reconnaissance activity.

5.5.2. AlienVault USM

Alienvault Unified Security Management (USM) is a tool that integrates several open source security tools to a single platform and management console. The most important tools to mention are PRADS (Passive Real-time Asset Detection System), OpenVAS (Open Vulnerability Assessment System), NMAP (Network Mapper) used for active asset detection, network IDS'es Suricata and Snort, and OSSEC (Open Source Security). There are several other components as well, as visible in Figure 10 below.

Alienvault USM provides asset discovery (using active scanning and passive monitoring), behavioural monitoring, vulnerability assessment, SIEM event correlation and threat detection using a network Intrusion Detection System (IDS), a host based IDS and file integrity monitoring (Alienvault USM, 2014). Host based intrusion detection and file integrity monitoring is achieved using OSSEC, Open Source Security. OSSEC includes also capabilities for rootkit detection and active response. Protected assets can be monitored using either agentless mode (where a centralized server performs login to the monitored system and scans it periodically) or using OSSEC agents which are installed to the monitored system. USM provides OSSEC agent management functionality and centralized log collection for OSSEC agents. It stores the file integrity checking databases and log events. All the rules, log decoders and major configu-

ration options are stored centrally in the management interface, which simplifies administration. The OSSEC agent is a small program installed on the monitored system. It will collect information in real time and forward it to the OSSEC manager for analysis and correlation. The agent runs with a low privilege user (created during the installation) and inside a chroot jail isolated from the system. Most of the agent configuration is pushed from the manager, while just some of them are stored locally on each agent. In case these local options are changed, the manager will receive the information and will generate an alert. The OSSEC agent will push the logs to the server where they will be analysed based on pre-defined rules. Logs are pushed using a OSSEC proprietary protocol, which uses UDP (User Datagram Protocol) port 1514 (OSSEC, How it works, 2015).

Figure 10. Alienvault USM open source components (Leveraging Open Source Security Tools: The Essential Guide, 2014)

Installation and Observations

Alienvault provides the USM as an virtual image (i.e. virtual appliance) which has all features enabled (called Alienvault USM-All-in-one). The installation procedure was

straightforward using a text based menu and by following the installation instructions. Figures 7 and 8 in chapter 5.2 present the environment. Alienvault USM has 6 network interfaces on the virtual appliance and these were configured so that it has capability to do scanning and has visibility to all the networks in the test environment. During the initial set-up, networks were scanned to detect the assets. OSSEC-agent was installed to the servers that are the main assets (NS1 and SUSE1) and logs were pushed to USM using OSSEC-agent. DNS and proxy server logs were sent using syslog. File integrity monitoring was configured to run every 2 hours for the main configuration directory (/etc). In addition, a detection mechanism to see new opened ports (using netstat -tan |grep LISTEN |grep -v 127.0.0.1 | sort) was taken into use. This will detect if a new port is opened on the server and create an event for this which can be used as a basis to create an alarm. The firewall was configured to send the Netflow data to USM.

Results

The results are analysed here for Alienvault Unified Security Management for each evaluated domain. Detailed results are visible in Appendix B.

EC-1 Asset Management: Alienvault USM is able to detect hosts that are added into the environment and it is possible to create an alarm for this if wanted. By default, Alienvault USM does not maintain a software asset lists and therefore does not provide mechanisms to see any new software modules on the hosts nor compare the current installed software base to the baseline. Still it may be possible to do this using an external script or software. It would require that an event related to installation of new software is first received (triggered for example by OSSEC file integrity monitoring which can also detect addition of new files) and that event triggers an external tool to do software scanning, enumeration and comparison to a pre-defined baseline. External software may then trigger another event for USM which could be used to create an alarm.

EC-2 Vulnerability Management: Alienvault USM uses OpenVAS as a vulnerability assessment tool which is capable of providing a criticality scoring for found vulnerabilities based on CVSS. Figure 11 shows the overview page of vulnerability management. When new vulnerabilities are found, a system also opens up a ticket in the ticketing section of the Alienvault USM. If a scan fails, for a reason or another, the system will not be able to notify on that, however it is possible to make the system to send an email when the scan is completed. If new listening ports are opened on a host, it is possible to detect this using either OSSEC-agent or with a passive monitoring tool. It is possible to configure the system so that this will also trigger an alarm as presented in Figure 12. In case it is known what ports are generally used in the network, it is possible to make a baseline comparison using an external tool or script in a similar way as above for EC-1. File integrity monitoring can effectively detect changes on security configuration files, but in order to see what was changed and by whom, additional logging (for example BSM audit logging) would be required. At the time of writing this thesis there were not plugins for BSM audit logs so that they could be correlated yet.

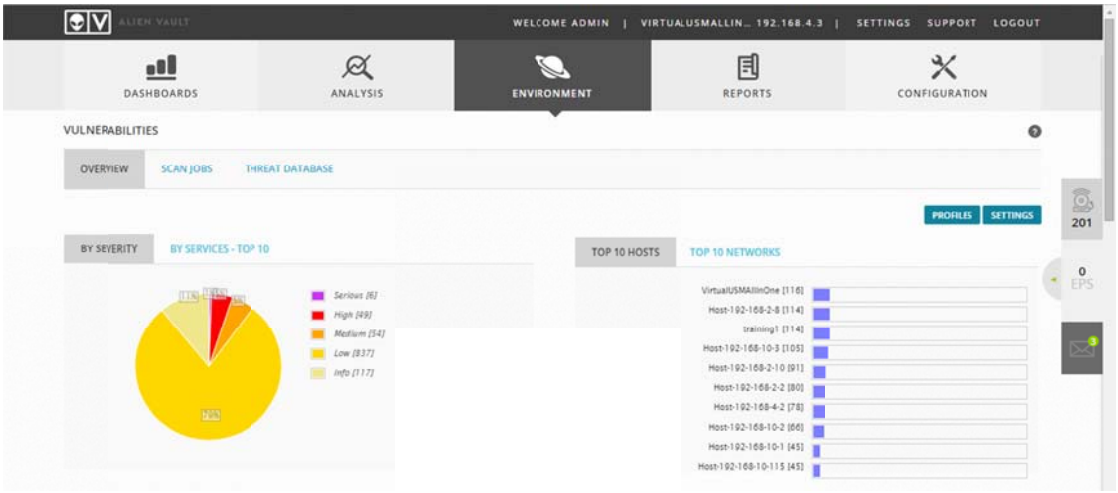

Figure 11. Alienvault USM vulnerability overview

Figure 12. Alarm created on opened port

EC-3 Software and Security Configuration Integrity management: For software and security configuration integrity, Alienvault USM provides just basically file integrity monitoring via OSSEC. It is not possible to perform configuration check scanning against known baselines. SCAP and CIS audit baselines are not supported either. It is possible to run the scans using Nessus and import results to Alienvault, which may bring some additional value considering reporting and ticket handling.

EC-4 Access Control: Creation or deletion of users can be detected with Alienvault USM as well as failed and successful authentication events and access attempts using deactivated user accounts. The logs can be sent either via syslog or using OSSEC-agent. It is possible to configure threshold limits for failed authentication attempts using a correlation directive, where it can be described that if a certain event occurs number of times within certain time period, an alarm is raised as presented on Figures 13 and 14. There is no user management features on USM; it is not possible to do scanning against baseline (unless using external tools) or to detect what type of users and privileges there are on each system.

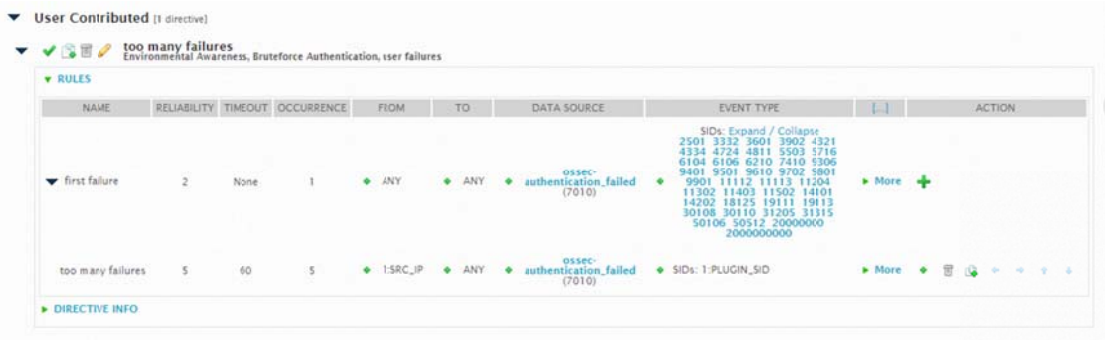

Figure 13. Correlation directive for five consecutive OSSEC authentication failures within 1 minute

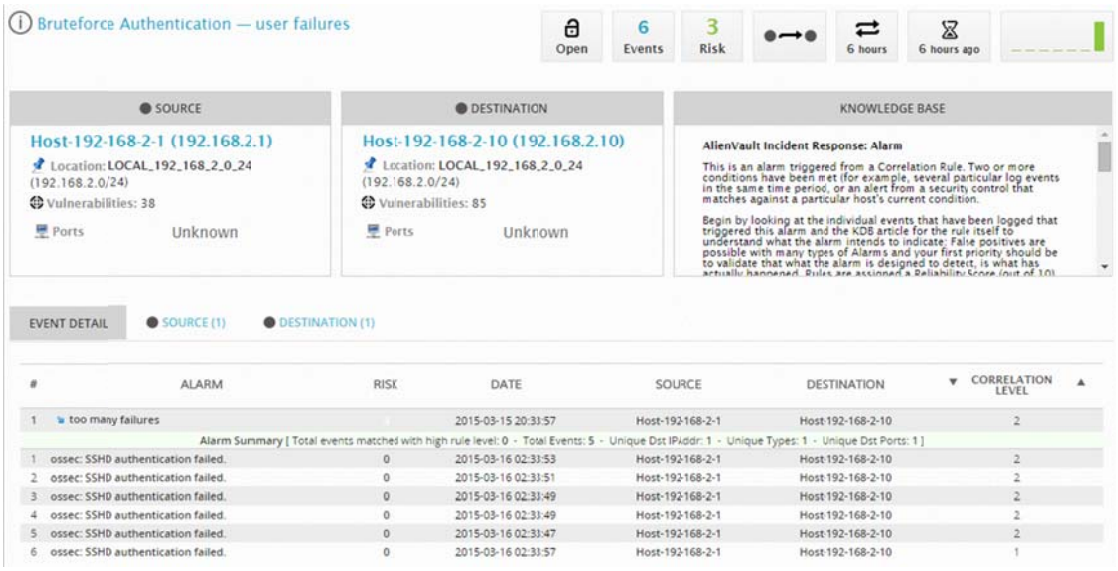

Figure 14. Alarm created based on directive correlation rule

EC-5 Logging and Monitoring: When BSM Audit logging is configured and the test sequence where unauthorized and authorized users (try to) access and modify files, Alienvault USM does not have capabilities to receive and correlate the events related to those actions by default. This is mainly due to a missing BSM audit log plugin. There is a mechanism to preserve log integrity within Alienvault USM using signing of the log file hashes. The integrity can be checked using the management GUI, as presented in Figures 15 and 16. However, there is no built-in mechanism to check log integrity. Alarm for use of sudo or su and for the change of system time or time sources can be raised when events for that are received, either using OSSEC-agent or syslog.

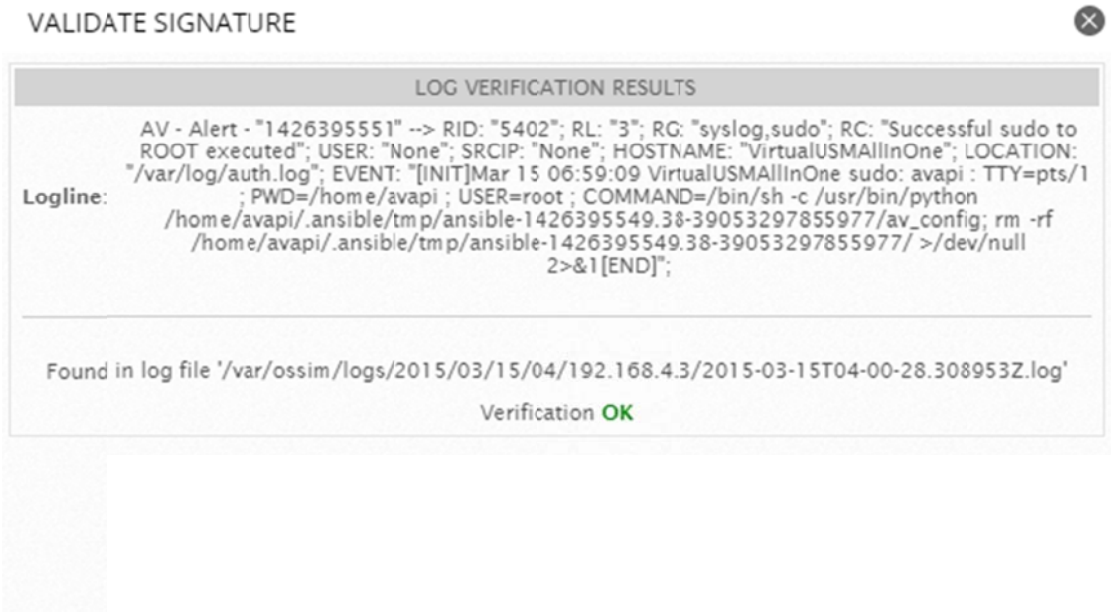

Figure 15. Log validation successful.

Figure 16. Log validation failed.

EC-6 Network Security: It is not possible to configure network policy to Alienvault USM, but it could be possible to do Netflow analysis using external tools if triggered by event. For example firewall log events could be used as a trigger. Firewall logs can be used to detect possible violations of network policy considering that a plugin exists to correlate the events. System is capable of detecting and making alarm for un-

authorized hosts that are not known by the tool beforehand. Netflow data is collected and can be used to do more detailed analysis of the traffic. Using in-built network IDS (which is Suricata on default set-up but also Snort is available) it is possible to detect network scans. The threat intelligence may also be based on honeypots, DNS, proxy, mail server or firewall logs. There are available USM plugins for a number of different types of honeypots, also BIND (DNS-server) and Squid (Proxy-server) log plugins exist.

5.5.3. Qualys Policy Compliance

From the policy compliance tool category, tool to evaluate the feasibility of the proposed framework was “Qualys Policy Compliance”. Qualys features are delivered in separate modules. During the testing the focus was mainly on Policy Compliance module. Qualys is most known for its vulnerability management product (Qualys Vulnerability Management, VM) and for the general interest also Qualys VM was trialled, however, the results are not included in this thesis as this part was outscoped. The modules that were included in the testing scope are all based on active scanning, meaning that there is no passive traffic monitoring capabilities.

There is an Asset Management module which is common for all different modules and was part of the test license. Other Qualys modules can be acquired separately and there are also different modules for example for PCI Compliance, Web Application Scanning (WAS) and Continuous Monitoring (CM), which enables monitoring of the external perimeter from the Qualys cloud. These were not tested. Figure 17 below includes the modules that were part of the test license.

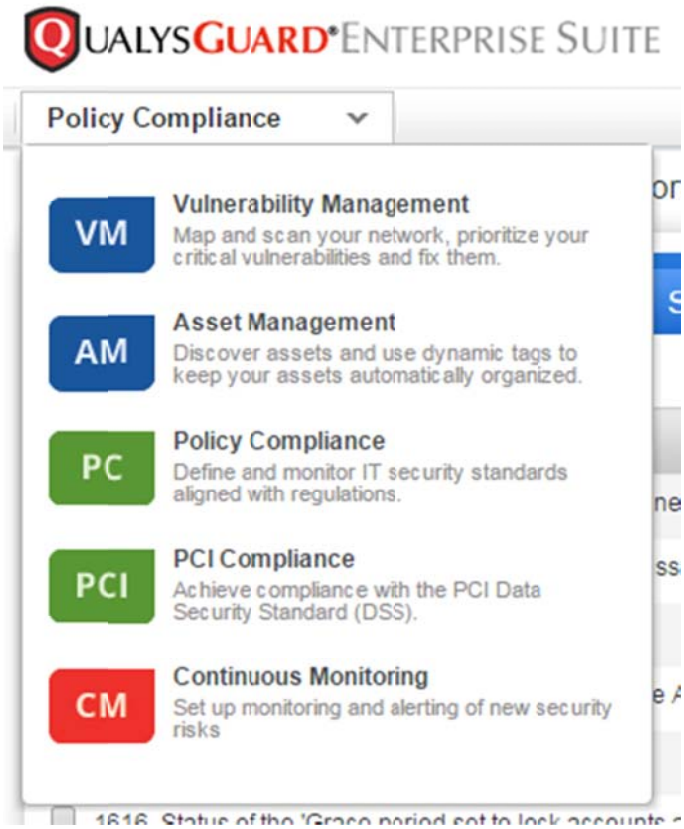

Figure 17. Qualys modules part of the test license.

Qualys has quite different deployment model than the other tools that were tested; it utilizes cloud based architecture where the control and management is centralized to the cloud provided by Qualys. The scanner sensors are installed as virtual appliances to the network and managed centrally. According to Qualys, the benefits of this deployment are that it is easy to deploy and set up, has a small footprint and total cost of ownership as there is no need to maintain it (the appliance updates itself) and all the data that is gathered by sensors is available from Qualys cloud for making reports and detailed analysis. (Qualys Cloud Platform, 2015). This type of deployment model enables reporting based on existing scan results without a need to rerun the scans for every new report.

Qualys Policy Compliance has been awarded as best risk and policy management tool for year 2014 selected by the readers of TechTarget Security (Security Readers'

Choice Awards: Risk and policy management, 2015.) and as best regulatory compliance solution for year 2015 by SC Magazine (SC Magazine Awards 2015, 2015.)

Installation and Observations

The scanner appliance is deployed to the network as a virtual image (i.e virtual appliance) having a footprint of couple of gigabytes and after configuration of IP address and making sure it is able to communicate with external network, there is no additional configuration required for it. After this, appliances can be added and managed from the user interface provided by Qualys visible on Figure 18.

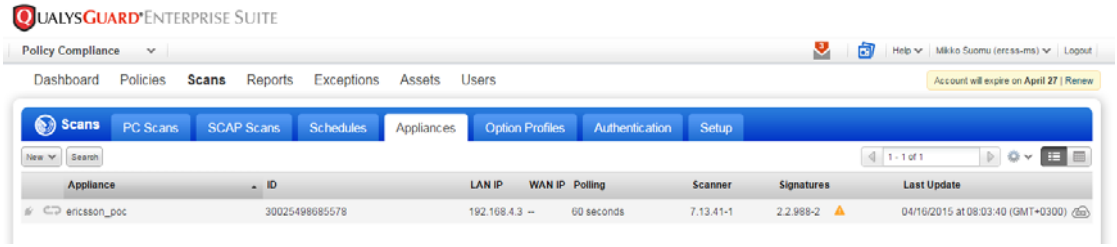

Figure 18. Qualys appliance management

The first steps after the scanner has been deployed are to detect the network assets using mapping scan, create the asset groups and configure the scans in more details. Figure 19 below presents the first mapping scans made with Vulnerability Management module.

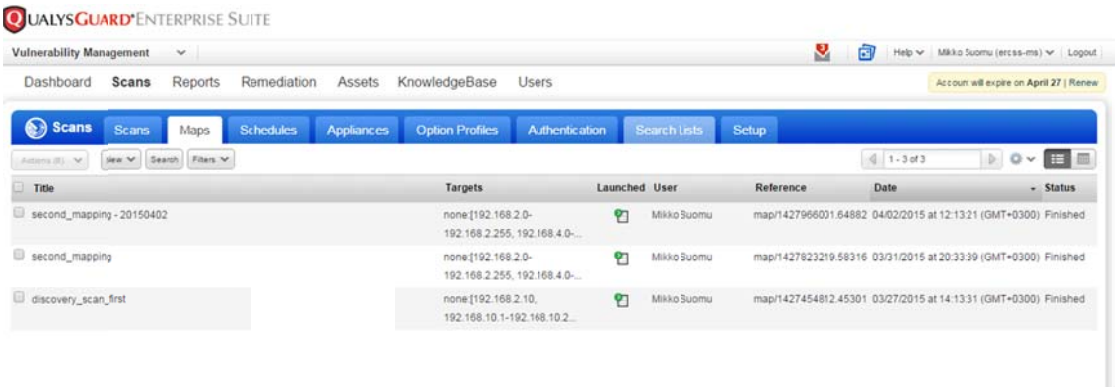

Figure 19. First mapping scans

After getting to know the tool own ISO27001 policy was built using Qualys Policy Compliance so that each of the actual controls at the evaluation criteria is mapped to the controls that Qualys Policy Compliance is able to provide.

Results

The results are analysed here for Qualys Policy Compliance for each evaluated domain, detailed results are visible in Appendix B.

EC-1 Asset Management:

Qualys Policy Compliance is capable of detecting new hosts at the network using network mapping scan. The tool has a capability to perform scanning against a predefined good image (i.e. golden image) which supports detection of any types of changes towards that image.

EC-2 Vulnerability Management: Qualys Policy Compliance is capable of creating tickets for new software vulnerabilities and the findings are rated based on the criticality of the vulnerability. If a known host opens new network ports, this can be detected.

EC-3 Software and Security Configuration Integrity management: There is a possibility to perform file integrity scans, scans using a golden image as a base and CIS and SCAP based scans. This provides a possibility to assess the security configuration of

the target as well as detect any possible changes. In order to detect who has performed the change, additional logging would be required. There are several audit baselines in Qualys Policy Compliance to choose from. There are also policy files which are CIS certified. These policy files are provided by CIS to security software vendors and allow their customers to comply with unchangeable CIS policies. There are also CIS based policy files which can be changed, Figure 20 below presents an overview of that type of file on Qualys Policy Compliance.

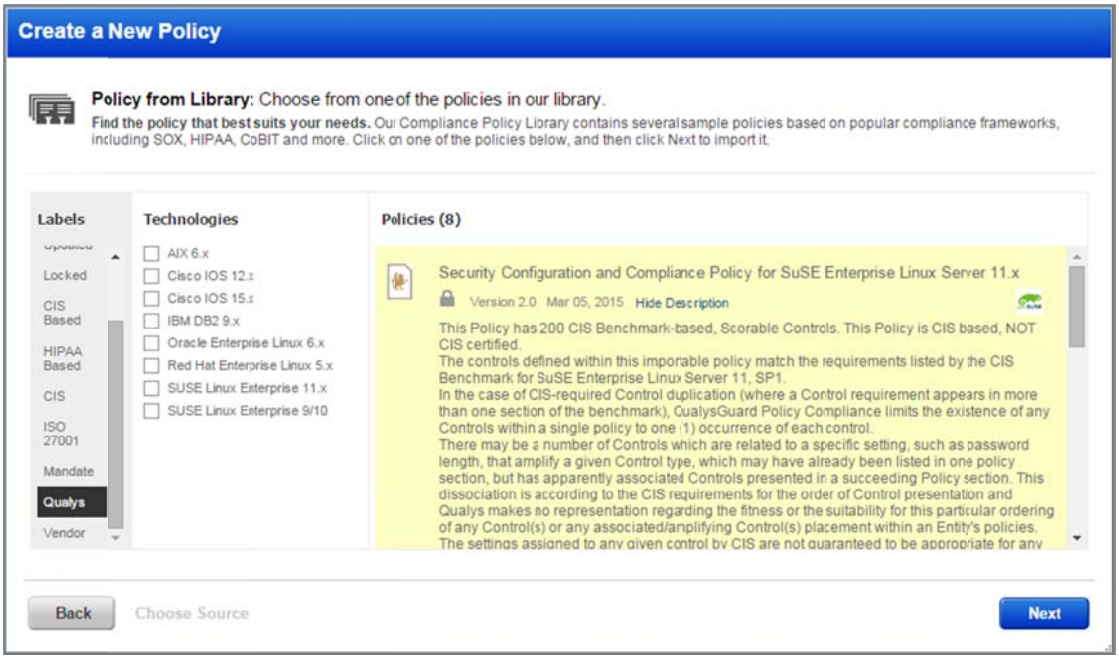

Figure 20. CIS-based benchmark audit policy for SLES 11.x

EC-4 Access Control: For a Linux system Qualys Policy Compliance is able to monitor files containing user information, which allows detection of new and changed user accounts and comparison to a known baseline using a golden image. There are also controls to detect certain type of user privileges (for example if UID (User Identifier) or GID (Group Identifier) equals zero) or if accounts are about to expire, presented in Figure 21. However, it is not possible to detect any active attempts to misuse the user accounts as the tool is mainly based on active scanning.

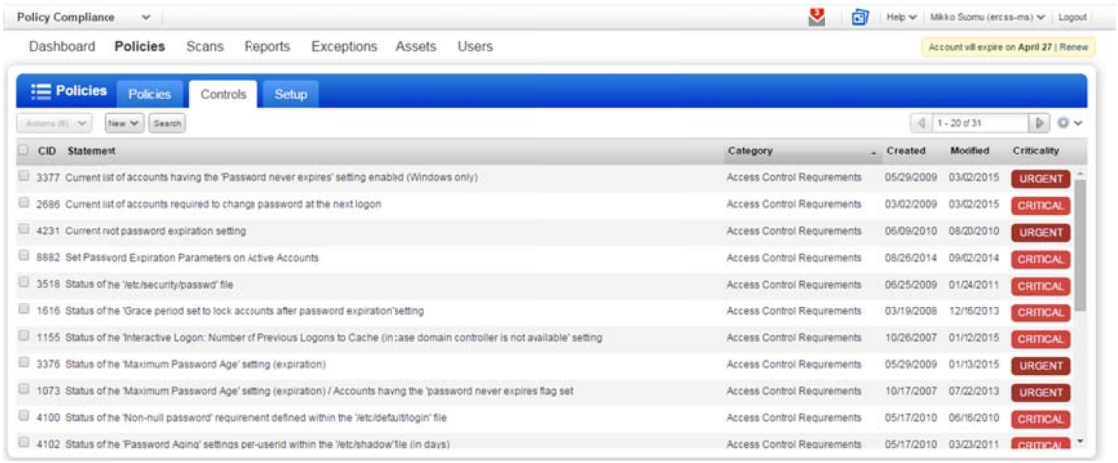

Figure 21. Controls to detect expirying user accounts.

EC-5 Logging and Monitoring: Due to designed functionality, Qualys Policy Compliance does not perform very well on this area. The tool does not collect any audit logs as it is not meant for that purpose. Instead, integration with a SIEM system would be required.

EC-6 Network Security: Due to designed functionality, Qualys Policy Compliance does not perform very well on this area. The tool is not meant to provide any real-time threat detection information.

6. Summary and Analysis of the Results

Three different types of tools were selected to analyse whether the “Monitoring System”-part of the developed framework could be fulfilled. Based on the potential risk level for this type of environment, controls were selected from the list of Framework Selected Controls (Appendix A.) and implemented to the PoC environment. Tested tools were deployed one-by-one to the PoC environment and verification and measurement was done. Detailed results of the evaluation are presented in Appendix B, table 7.

Table 5 summarizes how well each of the tools was able to fulfil the “Monitoring System”-part per domain area. Fulfilment percentage is calculated based on the yes/no answers received during the measurement. Asset detection is possible with all tools, whereas there are different types of capabilities when it comes to the detection of new software modules on the hosts. The tools are almost equally strong on the vulnerability management area, difference being that only Tenable SecurityCenter Continuous View is capable of creating an alarm if a scan has failed for a reason or another. However, this is still visible on the other tools as well and can be detected as well. On the software and security configuration integrity management area, Tenable and Qualys are equally strong, having capabilities to do scans against different types of baselines (CIS, SCAP). On Alienvault, the controls can be fulfilled only by using file integrity monitoring. Qualys is capable of doing scans based on the golden image as well, which is not possible to do with other evaluated tools.

On the access control area there was quite much dispersion while comparing Tenable and Alienvault towards Qualys although the fulfilment percentage is rather equal for all evaluated tools. This is mainly due to fact that Qualys is used in a different way and has different types of capabilities. Due to being a tool which is based on active scanning and reporting it lacks a possibility to receive logs and do the threat analysis based on that, but it in turn has other features what other tools do not have, like possibility to perform scans against a golden image.

Due to its different deployment model Qualys is lacking on areas which require active response whereas Tenable SecurityCenter Continuous View and Alienvault USM perform more or less equally. Alienvault USM is the only tool which has capabilities to monitor the integrity of the log files within the tool itself. On Network Security area, Alienvault USM performs better than other tools by having in-built IDS capabilities and existing plugins for parsing log events from various sources producing network level threat intelligence.

Table 5. Summary of the results

EC-x	Domain	Tenable Security Center Continuous View Fulfilment Percentage	Alienvault USM Fulfilment Percentage	Qualys Policy Compliance Fulfilment Percentage
EC-1	Asset mgmt	100	33	100
EC-2	Vulnerability mgmt	100	80	80
EC-3	Software and Security Configuration Integrity management	67	33	67
EC-4	Access Control	67	56	56
EC-5	Logging and Monitoring	50	50	0
EC-6	Network Security	50	67	0
Total		69	56	44

On higher level, it can be said that none of the tools was able to fulfil the framework as is; however, many of them are capable of providing certain essential security features, such as asset detection, vulnerability management and file integrity monitoring. Empirical research has showed the importance of the integrity assurance when reaching for automated security control compliance. This is the essential part and is somewhat lacking on the tested tools. In order to be able to do automated ISMS control auditability even for the controls that were used as evaluation criteria, it is required to have capabilities for active scanning of the targets, passive listening of network traffic and correlation of the log events so that the system would have up-to-date information of possible emerging threats but also capabilities to compare the current configuration and system state to “known-good” state and capabilities to trigger alarms or notifications in case current policy is breached.

Ease of deployment and use was not part of the evaluation, however on this area there is quite much dispersion. Tenable states that their tool is able to receive any type of logs, but in order to use these events as actual threat intelligence to detect threats significant configuration effort might be required. Some of the tested tools are clearly targeted for operating environment including possibly thousands of hosts, and would not be the best fit for a small and concise environment, mainly due to large implementation and configuration effort that is required.

Alienvault USM and Qualys Policy Compliance have capabilities to create their own policy sets which can include a number of controls to monitor. A user can in this way define what would be the ways to fulfil a particular policy. When using ISO27001 this is really beneficial feature as the standard itself has a certain level of ambiguity and it is the responsibility of those who implement the standard in use to actually define the controls based on the individual risk posture.

7. Conclusions

7.1. Summary of the thesis

The objective of this thesis was to develop a generic reference model for ISO27001:2013 standard compliance status monitoring which could be re-used in any ISMS and to test this framework using Proof of Concept. To fulfil the objective it was first analysed which ISO27001:2013 controls could be implemented using technical means and whether it would be possible to automate the measurement of the control compliance for these controls. During this analysis an imminent issue noticed was the ambiguity of standards: Generally laws and standards are meant to be universally applicable and to any technological solution and this leads to the situation that requirements may not necessarily be defined precisely. To overcome the ambiguity issue, different sources were used as input material to actually define how to fulfil, verify and measure the selected controls.

The developed framework consists of three parts, Framework Selected Controls, Framework Architecture and guidance how to use the framework. It includes ISO27001:2013 controls which could be automatically audited, a methodology to do this and a framework how this could be fulfilled.

The framework was tested with a Proof of Concept and the scope of the testing was limited to Monitoring System part of the framework to understand if tools selected for the PoC could fulfil the framework. The PoC environment was designed to correspond to an actual environment to which it is intended to implement the framework. Selection and implementation of the controls from the Framework Selected Controls table was based on a potential risk level of this type of environment. The measurement part of the selected controls was used as evaluation criteria. Three different types of tools were selected for the PoC and they were deployed to the PoC environment. An evaluation criteria table was filled for each tool. Conclusions presented on the subsequent chapters were drawn based on the empirical research and experience gained during the research of the theoretical base and background material.

7.2. Conclusions on the research questions

What ISO 27001:2013 controls can be implemented by technical means?

At first ISO 27001:2013 Annex A was used as an input to select controls which could be implemented using technical means by disregarding controls which are administrative controls, policies or processes. This provided a list that was then further refined on the next phase.

Is it possible to automate the measurement of control compliance for technically implemented controls?

It was then analysed if measuring of control compliance, could be achieved using machine readable and processable operation without human intervention. As a conclusion a list of controls that could be implemented technically and audited automatically was refined. The list is visible on table 6. Process to select the controls was pre-

sented on chapter 4.1. Also a methodology to measure their compliance was developed.

What mechanisms are required to provide integrity assurance for the audit data?
The PoC showed the importance of the integrity assurance when aiming for automated security control compliance. Instead of defining the exact mechanisms to provide integrity assurance for audit data on all levels, the main finding during the thesis was to identify where integrity assurance is required. Figure 22 presents the modified framework architecture which includes the areas where integrity assurance is most required. Orange boxes are additions to the Framework Architecture compared to the chapter 4.2. (Framework Architecture was presented there) considering to which levels the domain component is affecting. On the Network Security domain, the controls have been expanded to the hypervisor layer, which is relevant when virtualized networks are being used.

On the Software and Security Configuration Integrity Management domain, the Framework Selected Controls control list includes controls to achieve integrity assurance by using secure boot and signed images and software. In addition it is suggested to use file integrity monitoring for active device configuration (the control was expanded to that area as well) and critical security configuration files on hypervisor, OS and application layers. Security configuration scanning could be also performed using either a golden image or existing security configuration baseline (for example CIS or SCAP based.) It was realized during the making of the thesis that these mechanisms alone could provide rather comprehensive understanding if the integrity of the target system has been compromised. SCAP based scanning seems to have high potential but the observation was that it is yet not that widely deployed, the targets that are mainly supported there are Windows Servers and workstations and Red Hat Linux servers. There seems to be still increasing need to expand this beyond US government use cases and in some of the conversations with vendors of the tools (which were being tested) the impression was that there is quite much interest in Europe as

well for SCAP based scanning, especially in the financial industry. When using golden images, it is required that the image is really “golden” and that in turn requires certain level of maturity on preparing and handling pre-hardened OS images.

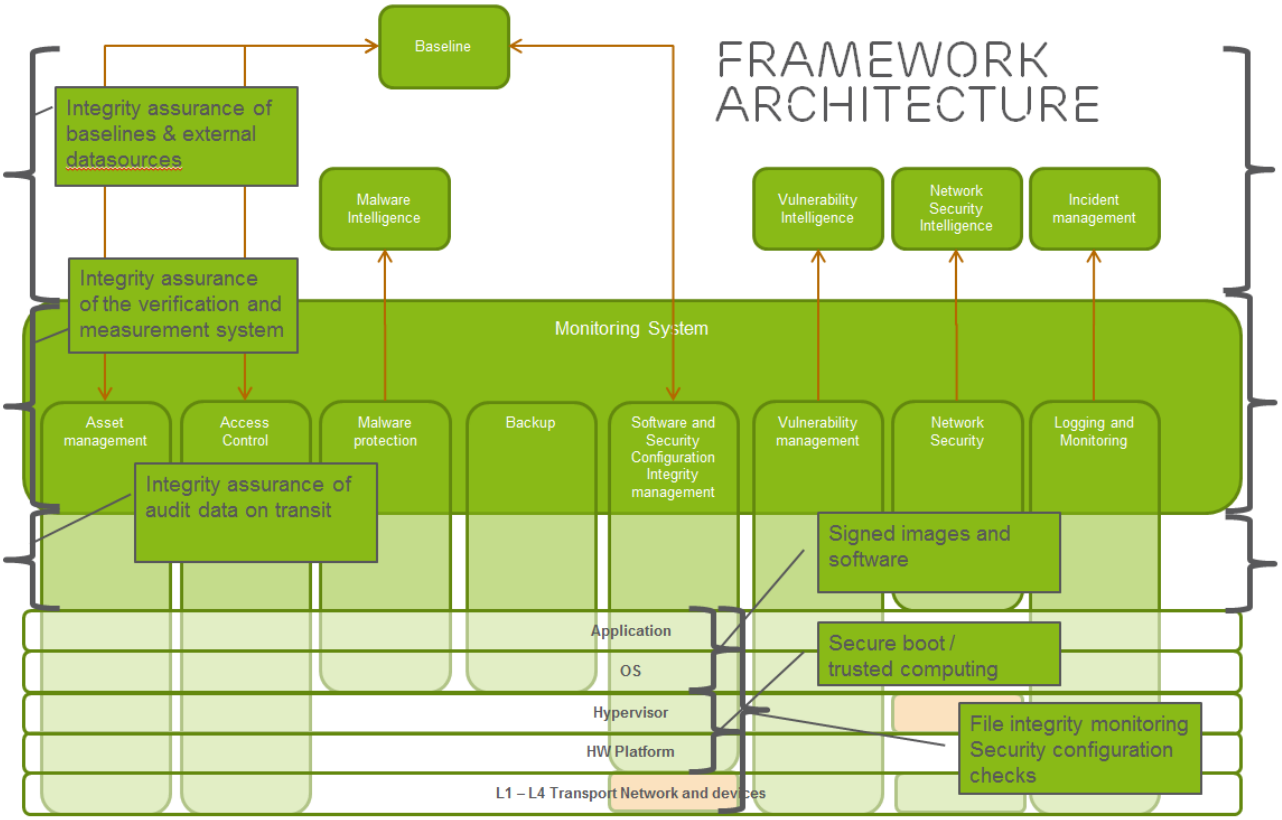

Figure 22. Modified ISMS compliance framework architecture highlighting the requirements for integrity assurance

Integrity assurance is also required when audit data is transferred, meaning use of secure protocols which provide integrity protection, such as IPsec. Integrity of the baselines and external data sources should be protected as well, to avoid potential risk that someone modifies the content to something which is undesirable.

The main components in the developed framework which provide the compliance data are Monitoring System and the domain components; therefore it is crucial to have integrity assurance for them as well. As an analogy this could be considered as a measurement tool which needs to be correctly calibrated to have the correct results.

Integrity assurance would in any case require trusted computing base i.e. use of cryptographic verification of boot loader, hypervisor, operating system and installed software. This applies not only for the target systems which are being audited but also the Monitoring System.

Can framework provide compliance status in automated way for the selected controls?

For this question it is difficult to provide an exact answer. On a high level one could argue that this is possible given that the integrity is assured and the used tools are correctly configured and they do what they actually promise. On the other hand, as stated in the NIST Special Publication 800-55 regarding Performance Measurement Guide for Information Security:

The measures corresponding to security control families or individual security controls should be mapped directly to the individual security control(s). (NIST Special Publication 800-55 Revision 1, 2008, 29).

This is understood that every control (or group of controls) shall be measured individually and in the best case, the framework would be just able to provide mechanisms to measure the effectiveness of the implemented controls. From the perspective of an independent 3rd party auditor it may be difficult to just rely on a security framework and tools that provides compliance data as it requires that the implemented controls and all the related components are anyway being audited and verified to work as expected. Also mitigation activities (removal of nonconformities) should be audited to measure the effectiveness of implementation and maintenance of ISMS which would provide the visibility of the overall maturity of ISMS deployment. An auditee needs to be able to prioritize, plan and execute the mitigation activities in a manner that is logical, repeatable, and defendable to auditors. This in turn raises a question what can be the level of compliance automation if the process includes steps that are impossible to automate.

Considering nonconformities, they could be controls which are not working but are left undetected and therefore are not fixed. Therefore it would be required to have a mechanism to automatically verify that the implemented controls are actually working, for example by triggering the controls periodically or on demand and results would be compared against the currently defined policy (or a set of security controls fulfilling that policy.)

Alternatively, they may be controls which are clearly missing but should exist to mitigate certain risks in the current risk posture. These types of areas may also be very difficult to identify using automated mechanisms and would require a thorough auditing process. If that is not done, then there is a risk that having this type of framework would just create a false sense of security; however, it would not be able to actually target those risks which are to be mitigated. The ISMS is anyway information security *management* system which is meant for organizations to manage their information security in a holistic way, not only to manage the technical systems and controls related to them. Depending on the size of the organization it may still create added value to have an automated mechanism to monitor and measure the effectiveness of the technical controls as well.

7.3. Areas for Further Research

The areas of interest for further research would be to analyse the effort of the full implementation of the controls, their verification and measurement and to have concise measurement reports of the effectiveness of implemented controls. This would probably require adding several tools into the actual implementation which would be integrated under one Monitoring System. It would be also interesting to analyse if new attack vectors would rise due to automation of auditing.

From testing perspective it would be interesting to use hardware and hypervisor that support trusted computing and to build a fully virtualized environment using for example Ubuntu open-stack to actually verify the remote attestation and its benefits.

During the making of this thesis this was not possible due to the lack of appropriate test environment. (The current resources used for the testing were shown to be insufficient overall, there were difficulties to run all the virtual images at same time due to lack of space, memory and processing capabilities.)

From the framework point of view it would be interesting to add in more standards and mandates and to analyse how that would impact the framework: would it add in more domain areas and if so what would those be? In the current form, the thesis may provide a concrete approach to implement technical controls to meet the requirements of ISO27001 standard and it is to be questioned if technical controls on ISO27000-series are sufficient. Nevertheless, ISO27001:2013 does not mandate that the actual controls to be implemented would be selected from the standard, instead these should always be selected according to the actual risk posture that an organization has. Framework Selected Controls list could be used to identify those controls that are actually needed to be implemented and a mechanism to verify and measure their effectiveness.

REFERENCES

Bonazzi R., Hussami L., Pigneur Y. 2010. Compliance management is becoming a major issue in IS design. Accessed on 02.09.2014. Retrieved from http://www2.hec.unil.ch/wpmu/ypigneur/wp-content/uploads/sites/15/2010/01/complianceManagement.pdf

Tipton Harold F., Krause Micki. 2010. Information Security Management Handbook, Volume 4, Sixth Edition. 22.06.2010. AUERBACH PUBLICATIONS. ISBN-13: 978-1439819029, ISBN-10: 1439819025.

Merriam-Webster Online dictionary. Accessed on 02.09.2014. Retrieved from http://www.merriam-webster.com/dictionary/compliance

NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations. April 2013. Revision 4. Accessed on 01.09.2014. Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Symantec Security Response, Exploring Stuxnet's PLC Infection Process. 22.09.2010. Accessed on 04.09.2014. Retrieved from http://www.symantec.com/connect/blogs/exploring-stuxnet-s-plc-infection-process

Gelbstein Ed. ISACA Journal. Data Integrity—Information Security's Poor Relation. 2011. Accessed on 04.09.2014. Retrieved from http://www.isaca.org/Journal/Past-Issues/2011/Volume-6/Pages/Data-Integrity-Information-Securitys-Poor-Relation.aspx

About TCG. 2014. Accessed on 07.09.2014. Retrieved from http://www.trustedcomputinggroup.org/about_tcg

Trusted Computting Group. Trusted Platform Modules Strengthen User and Platform Authenticity. January 2005. Accessed on 07.09.2014. Retrieved from http://www.trustedcomputinggroup.org/files/resource_files/8D46621F-1D09-3519-ADB205692DBBE135/Whitepaper_TPMs_Strengthen_User_and_Platform_Authenticity_Final_1_0.pdf

Greene James. Intel Trusted Execution Technology White Paper. Intel. 2012. Accessed on 07.09.2014. Retrieved from http://www.intel.com/content/dam/www/public/us/en/documents/white-papers/trusted-execution-technology-security-paper.pdf

Shpantzer Gal. Implementing Hardware Roots of Trust: The Trusted Platform Module Comes of Age. SANS. June 2013. Accessed on 07.09.2014. Retrieved from http://www.trustedcomputinggroup.org/files/temp/76882F9C-1A4B-B294-D09D38B918AD23D0/SANS%20Implementing%20Hardware%20Roots%20of%20Trust.pdf

Boneh Dan. TPMs in real world. Spring 2006. Accessed on 08.09.2014. Retrieved from http://crypto.stanford.edu/cs155old/cs155-spring06/08-TCG.pdf

Srivastava Abhinav, Raj Himanshu, Giffin Jonathon, England Paul. Trusted VM Snapshots in Untrusted Cloud Infrastructures. 2012. Accessed on 08.09.2014. Retrieved from http://www2.research.att.com/~abhinav/papers/raid12-hypershot.pdf

Loureiro Sergio, Bussard Laurent and Roudier Yves. Extending Tamper-Proof Hardware Security to Untrusted Execution Environments. 2001. Accessed on 09.09.2014. Retrieved from http://www.eurecom.fr/~nsteam/Papers/cardis02.pdf

Solutions and Products with Intel® Trusted Execution Technology (Intel® TXT). 2014. Accessed on 10.09.2014. Retrieved from

http://www.intel.com/content/www/us/en/architecture-and-technology/trusted-execution-technology/where-to-buy-isv-txt.html

OpenAttestation. 16.04.2014. Accessed on 10.09.2014. Retrieved from https://01.org/openattestation

Ubuntu Cloud Infrastructure, Community Help Wiki. 16.04.2014. Accessed on 10.09.2014 Retrieved from https://help.ubuntu.com/community/UbuntuCloudInfrastructure

Cannon David. 2011. CISA Certified Information Systems Auditor Study Guide, Third Edition. 22.03.2011. Wiley Publishing, Inc. ISBN: 978-0-470-61010-7

International Standard ISO/IEC 27001:2013, Information Technology - Security Techniques - Information Security Management Systems - Requirements, Second edition: 2013-10-01

International Standard ISO/IEC 27002:2013, Information technology — Security techniques — Code of practice for information security controls, Second edition: 2013-10-01

SANS Institute. Critical Security Controls - Version 5. Accessed on 08.10.2014. Retrieved from http://www.sans.org/critical-security-controls/

SANS Institute. Critical Security Controls - Guidelines. Accessed on 08.10.2014. Retrieved from http://www.sans.org/critical-security-controls/guidelines

SANS Institute. Critical Security Control : 1. Accessed on 08.10.2014. Retrieved from http://www.sans.org/critical-security-controls/control/1

Montesino Raydel, Fenz Stefan. 2011. Information security automation: how far can we go? 2011 IEEE Sixth International Conference on Availability, Reliability and Security. Vienna, Austria. 22-26 Aug, 2011 a

Montesino Raydel, Fenz Stefan. 2011. Automation possibilities in information security management. 2011 IEEE European Intelligence and Security Informatics Conference. Athens Greece. 12-14 Sept. 2011 b

Montesino Raydel, Fenz Stefan, Baluja Walter. 2012. SIEM-based framework for security controls automation, Information Management & Computer Security, Vol. 20 Iss 4 pp. 248 - 263

Koschorreck Gerhard, 2011. Automated Audit of Compliance and Security Controls. 2011 Sixth International Conference on IT Security Incident Management and IT Forensics. Stuttgart, Germany. 10 - 12 May 2011.

Radack Shirley, Kuhn Rick. 04.02.2011. Managing Security: The Security Content Automation Protocol. IT Professional (Volume:13 , Issue: 1). Pages 9 - 11.

Quinn Stephen, Scarfone Karen, Waltermire David. January 2012. National Institute of Standards and Technology, NIST Special Publication 800-117 Revision 1 (Draft), Guide to Adopting and Using the Security Content Automation Protocol (SCAP) Version 1.2 (Draft). Accessed on 27.10.2014. Retrieved from http://csrc.nist.gov/publications/drafts/800-117-R1/Draft-SP800-117-r1.pdf

Security Content Automation Protocol Validated Products. 2014. Accessed on 29.10.2014. Retrieved from http://nvd.nist.gov/scapproducts.cfm

SUSE. OpenSCAP in SUSE Manager. 2014. Accessed on 29.10.2014. Retrieved from https://www.suse.com/documentation/suse_manager/book_susemanager_ref/data/s1-openscap-suma.html

Adams Jamie. Detecting Vulnerable Software Using SCAP/OVAL. 7.4.2011. Accessed on 29.10.2014. Retrieved from http://www.infosecisland.com/blogview/12804-Detecting-Vulnerable-Software-Using-SCAPOVAL.html

MITRE. OVAL Adoption Program. 7.5.2013. Accessed on 29.10.2014. Retrieved from http://oval.mitre.org/adoption/

Erkan Ahmet. An Automated Tool for Information Security Management System. September 2006. Accessed on 3.11.2014. Retrieved from http://etd.lib.metu.edu.tr/upload/12607783/index.pdf

Susanto Heru, Almunawar Mohammad Nabil, Tuan Yong Chee. A Novel Method on ISO 27001 Reviews: ISMS Compliance Readiness Level Measurement. Computer Science Journal, Volume 2, Issue 1, April 2012. Accessed on 3.11.2014. Retrieved from http://arxiv.org/ftp/arxiv/papers/1203/1203.6622.pdf

Verinice. 2014. Refererred at 3.11.2014. Retrieved from http://www.verinice.org/en/products/screencasts/

Alienvault USM. 2014. Accessed on 5.11.2014. Retrieved from https://www.alienvault.com/products

ManageEngine Eventlog Analyzer. ISO27001 Compliance Reporting. 2014. Accessed on 5.11.2014. Retrieved from http://www.manageengine.com/products/eventlog/iso-27001-compliance-audit.html

Tripwire IP360 v7.4 datasheet. 2014. Accessed on 5.11.2014. Retrieved from http://www.tripwire.com/register/tripwire-ip360-datasheet/

Tripwire Enterprise File Integrity Manager datasheet. 2014. Accessed on 5.11.2014. Retrieved from http://www.tripwire.com/register/tripwire-enterprise-file-integrity-manager/

SecurityCenter CV Features. Tenable, 2014. Accessed on 9.11.2014. Retrieved from http://www.tenable.com/products/securitycenter-continuous-view/features

Qualys Policy Compliance. 2014. Accessed on 9.11.2014. Retrieved from https://www.qualys.com/enterprises/qualysguard/policy-compliance/

Tripwire Enterprise 8.3 product brief. 2014. Accessed on 9.11.2014. Retrieved from http://www.tripwire.com/register/tripwire-enterprise-product-brief/

Symantec Control Compliance Suite. 2014. Accessed on 9.11.2014. Retrieved from http://www.symantec.com/control-compliance-suite

Creech Jason, Alderman Matthew. IT Policy Compliance for Dummies. 2010. A John Wiley and Sons, Ltd, Publication. ISBN: 978-0-470-66535-0

Mapping between the requirements of ISO/IEC 27001:2005 and ISO/IEC 27001:2013. 2013. Accessed on 6.1.2015. Retrieved from http://www.bsigroup.com/Documents/iso-27001/resources/BSI-ISO27001-mapping-guide-UK-EN.pdf

SANS Critical Security Controls Poster. FALL 2014 31st edition. 2014. Accessed on 08.01.2015. Retrieved from https://www.sans.org/media/critical-security-controls/fall-2014-poster.pdf

Niemelä Jarno. Protecting against computerized corporate espionage. 2013. Accessed on 08.01.2015. Retrieved from http://www.cse.tkk.fi/fi/opinnot/T-

110.6220/2013_Reverse_Engineering_Malware/luennot-files/Protecting%20against%20computerized%20corporate%20espionage.pdf

SCMagazine Awards Europe 2014 Results. 2014. Accessed on 08.01.2015. Retrieved from http://www.scawardseurope.com/results-2014

Eriksson Mikael, Pourzandi Makan, Smeets Ben. 24.10.2014. Trusted computing for infrastructure, Ericsson Review. Accessed on 09.02.2015. Retrieved from http://www.ericsson.com/eg/res/thecompany/docs/publications/ericsson_review/2014/er-trusted-computing.pdf

Tenable SecurityCenter CV. 2015. Accessed on 24.02.2015. Retrieved from http://www.tenable.com/products/securitycenter-continuous-view

Stephenson Peter. 03.02.2014. SC Magazine Reviews Tenable SecurityCenter Continuous View. Accessed on 24.02.2015. Retrieved from http://www.scmagazine.com/tenable-securitycenter-continuous-view/review/4101/

Tenable Passive Vulnerability Scanner Features. 2015. Accessed on 25.02.2015. Retrieved from http://www.tenable.com/products/passive-vulnerability-scanner/features

Tenable Log Correlation Engine Features. 2015. Accessed on 25.02.2015. Retrieved from http://www.tenable.com/products/log-correlation-engine/features

Leveraging Open Source Security Tools: The Essential Guide. 11.03.2014. Accessed 18.03.2015. Retrieved from http://www.slideshare.net/alienvault/leveraging-open-source-security-tools-thetheessentialguide

OSSEC, How it works. 2015. Accessed 19.03.2015. Retrieved from http://www.ossec.net/?page_id=169

Qualys Cloud Platform. 2015. Accessed 20.04.2015. Retrieved from https://www.qualys.com/enterprises/security-compliance-cloud-platform/

Security Readers' Choice Awards: Risk and policy management. 2015. Accessed 27.04.2015. Retrieved from http://searchsecurity.techtarget.com/feature/Security-Readers-Choice-Awards-Risk-and-policy-management

SC Magazine Awards 2015. 21.04.2015. Accessed 27.04.2015. Retrieved from: http://media.scmagazine.com/documents/118/botn2015sm_29485.pdf

Chew Elisabeth, Swanson Marianne, Stine Kevin, Bartol Nadya, Brown Anthony, Robinson Will. July 2008. Performance Measurement Guide for Information Security. NIST Special Publication 800-55 Revision 1. Accessed 30.04.2015. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf

APPENDICES

APPENDIX A. Framework Selected Controls

Selected controls are presented in the table below.

Table 6. Framework Selected Controls

Control number	Domain (used in my framework proposal)	Heading	Control Text	What to implement actually	Verification method	Measurement		mapping to sans top 20 CSC
						Measurement (monitoring system)	Measurement (domain component)	
A.8.1.1	Asset Management	Inventory of assets	Control Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.	Automatic asset management tool / Monitoring system which consist of automatic asset inventory and management.	Add new host into different parts of the network which is not in asset management tool. Install new software module to the host which is on the asset inventory.	Is the monitoring system capable of detecting new hosts? (If so, how long does it take that this could be noticed?) Is the monitoring system capable of detecting new software modules on hosts? (If so, how long does it take that this could be noticed?) Is it possible to define rules for expected and unexpected changes in asset management database and create alarms based on those rules?	Same measurements apply even if asset management is fulfilled using component which is not part monitoring system.	1 - Inventory of Authorized and unauthorized devices

A.9.1.2	Network Security	Access to networks and network services	Control Users shall only be provided with access to the network and network services that they have been specifically authorized to use.	<u>Packet Capture:</u> - Monitoring of the use of network devices and services on and between different subnets to observe what type of traffic is sent within the network including source and destination using tool with packet capture capabilities (e.g. Netflow). <u>Web-traffic (http, https, ftp, ssh) specific:</u> - Create and deploy company specific user-agent to the browser. Alarm for traffic which uses anything else. (MS example for creating user agent: http://technet.microsoft.com/en-us/library/cc770379.aspx) - Deploy own proxy server and allow web traffic only through company proxy. Proxy should support logging individual TCP sessions; blocking specific URLs, domain names, and IP addresses to implement a black list; and applying whitelists of allowed sites that can be accessed through the proxy while blocking all other sites <u>Email specific:</u> - Deploy own email servers and allow emails only through company mail servers. - Scan mails before they are placed in user's mailbox and block known malicious code or other file types not relevant to business (e.g. exe, msi, zip) - Perform custom stripping for documents (for example conversions from docx to txt).	<u>Packet Capture:</u> Create traffic which is allowed and non-allowed according to the current usage policy. <u>Web-traffic:</u> Send traffic using non-company specific user agent. Send traffic to predefined blacklisted URLs, domains or IPs. Send traffic to predefined non-whitelisted URLs, domains, IPs. <u>Email specific:</u> Send email to an address within a company consisting blocked filetypes, eicar antivirus test file and filetypes configured to use custom stripping. Send mail with wrong domain (e.g. from open SMTP relay). <u>System hardening:</u> Verify firewall rules (with for example nmap, hping). Confirm that there are no unintended ports listening the connections (even if blocked by firewall). Confirm that outbound firewall is configured. Modify firewall rules to verify if this is logged or visible.	<u>Packet Capture:</u> Is the traffic seen and categorized correctly? Is it possible to define the current network policy to the monitoring system? <u>Web-traffic:</u> Is the monitoring system capable of logging individual TCP sessions and blocking URLs, domains and IPs using blacklist and whitelist? Are alarms generated for these events? <u>System hardening:</u> Is monitoring system capable of creating alarm or event if new listening ports are opened or if firewall rules are being modified?	<u>Packet Capture:</u> Is the traffic seen and categorized correctly? Is it possible to define the current usage policy to the system? <u>Web-traffic:</u> Is the system capable of logging individual TCP sessions and blocking URLs, domains and IPs using blacklist and whitelist? Are alarms generated for these events? <u>Email specific:</u> Are the files blocked or stripped appropriately? Is each of the events logged? Is the mail sent with wrong domain-name blocked and is the event logged? <u>System hardening:</u> Are firewall rules implemented correctly? Is there firewall event logged in case of blocked traffic? Is it visible in logs if new ports are opened for listening or if firewall rules are being modified?	1 - Inventory of Authorized and unauthorized devices 10 - Secure Configuration for Network Devices 11 - Limitation and Control of Network Ports 13 - Boundary defence

				- Deploy SPF (sender policy framework) with SPF records in DNS and receiving side verification. System hardening: - host based firewalls with default deny - uninstall and remove any unnecessary components				

A.9.2.1	Access Control	User registration and de-registration	Control A formal user registration and de-registration process shall be implemented to enable assignment of access rights.	Controlled way of assigning and enabling, or revoking, a user ID and providing, or revoking, access rights to such user ID via centralized point of authentication. Centralized user repository and/or IdAM system.	Create normal user Create user with administrative privileges Deactivate an account. Try to access deactivated account. Remove normal user Remove user who had administrative privileges Try to login with incorrect passphrase multiple times.	Is it seen from the monitoring system when new users are added or removed? Is it seen from the monitoring system what type of privileges a user has for each system (for example under certain group?) Are access attempts with deactivated account visible in the monitoring system? Is it possible to observe from the monitoring system if user(s) are created to local system and not via centralized management? Is it possible to see from a monitoring system that user is about to expire? Does the monitoring system offer a possibility to perform baseline checks and compare the results to the system's current user account list periodically?	Is it possible to use deactivated account?	16 - Account Monitoring and Control

A.9.2.2	Access Control	User access provi-sioning	Control A formal user access provision-ing process shall be implemented to assign or revoke access rights for all user types to all systems and services.	Authorization log. Central record of access privileges and rights granted. IdAM system, maybe openIAM. Deploy a tool which can perform queries/scans to detect different types of user accounts in the system.	Scan system accounts on different systems.	Are there any accounts which are: - not authorized - only in one system - generic (not bound to user account) - not having expiry date? - locked-out - disabled - with passwords that exceed the maximum password age - with passwords that never expire - are there any system accounts which are not supposed to be there (i.e. no business owner). And can the monitoring system provide a list of these accounts?	Is there are workflow (or similar which can pro-vide authorization log?) Are there any accounts which are: - not authorized - only in one system - generic (not bound to user account) - not having expiry date? - locked-out - disabled - with passwords that exceed the maximum password age - with passwords that never expire - are there any system accounts which are not supposed to be there (i.e. no business owner).	12 - Controlled User of Ad-ministrative privileges 16 - Account Monitoring and Control

A.9.4.2	Access Control	Secure log-on procedures	Control Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.	a) not display system or application identifiers until the log-on process has been successfully completed; b) display a general notice warning that the computer should only be accessed by authorized users; c) not provide help messages during the log-on procedure that would aid an unauthorized user; d) validate the log-on information only on completion of all input data. If an error condition arises, the system should not indicate which part of the data is correct or incorrect; e) protect against brute force log-on attempts; f) log unsuccessful and successful attempts; g) raise a security event if a potential attempted or successful breach of log-on controls is detected; h) display the following information on completion of a successful log-on: 1) date and time of the previous successful log-on; 2) details of any unsuccessful log-on attempts since the last successful log-on; i) not display a password being entered; j) not transmit passwords in clear text over a network; k) terminate inactive sessions after a defined period of inactivity, especially in high risk locations such as public or external areas outside the organization's security management or on mobile devices;	For systems which provide log-on interface, do following tests. Capture traffic and: a,b) login normally. c) try to login with incorrect username and/or password d) enter only username and let the session expire e) try to login with a wrong password multiple times f,g) try login with incorrect username and / or password/credential h, i, j) login normally k) login normally and leave the session idle?	f) Is it possible to see from the monitoring system if user authentication fails? Is it possible to see from the monitoring system if user authentication succeeds? g) Is security event in the monitoring system raised after number of failed authentication attempts?	a) Are application identifiers sent before the log-on is completed successfully? b) Is there a general notice regarding computer usage policy? c,d) Is there any help messages providing information what data was incorrect? e) Is user account locked after number of invalid logon attempts? h) Is there information about date and time of previous successful login? Is there information about details of any unsuccessful login attempts since the last successful login? i) Are password / credentials presented? j) Are password / credentials sent in clear text? k) Is the session terminated automatically after certain time?	12 - Controlled User of Administrative privileges 16 - Account Monitoring and Control

				l) restrict connection times to provide additional security for high-risk applications and reduce the window of opportunity for unauthorized access.				

A.9.4.3	Access Control	Password management system	Control Password management systems shall be interactive and shall ensure quality passwords.	Change default administrative passwords Implement a password policy which enforces quality passwords, maintains a record of previously used passwords and prevents re-use and storing of password files separately from application system data. Set-up specific user accounts to administrators (with different username). Disable remote login with root. Enforce use of sudo. Rename built-in administrative accounts (i.e. windows administrator).	1) Attempt to gain access to a cross section of devices within the system, using default administrative passwords. 2) Attempt to log-in remotely to machines using administrative accounts directly. 3) Attempt to log-in directly to a workstation or server with root or administrator accounts. 4) Attempt to gain access to password files within the system using unauthorized accounts. 5) Attempt to elevate to a privileged account on the system. 6) Attempt to configure weak user account passwords that are non-compliant with established policy. Query the password policy from server that it meets the requirements (contain letters, numbers, and special characters, be changed at least every 90 days, have a minimal age of one day, and not be allowed to use the previous 15 passwords as a new password) 7) Attempt to re-use a user account password that was previously used for the account.		1,2,3) Is the access granted? 4) Is the access disallowed and are attempts logged and reported? 5) Is the administrator password is required to perform the elevation? Is the elevation is logged and reported by the system? Is the traceability within the audit logs provided to detail the user account that performed the elevation? 6) Does the system allow weak passwords to be used? Is password policy set correctly? 7) Does the system require unique new passwords during each update?	12 - Controlled User of Administrative privileges 16 - Account Monitoring and Control

A.12.2.1	Malware Protection	Controls against malware	Control Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.	Deploy application whitelisting Deploy file integrity monitoring Deploy centrally managed and logged antivirus software including a number of features like anti-virus, anti-spyware, firewall, host-based IDS/IPS. Keep anti-virus software up-to-date and real-time protection and behaviour based anomaly detection on. Employ file reputation queries Prevent auto-running of removable media. Prevent using unknown input devices and monitor use of input devices. Perform automatic scanning of removable media when inserted. Use tools which harden application memory handling (i.e. EMET, Enhanced Mitigation Experience Toolkit). Block creation and execution of files from locations which are normally not used and are preferred by malware (e.g. C:\) Monitor for unusual process activity (e.g. docx accessed by some other program than winword.exe) Restrict actions that installed software can take (e.g. SELinux, AppArmor)	1) using removable media, - deploy eicar file on random servers - try to install a "hacker tool" which is not whitelisted software 2) using email, repeat the previous test 3) as a user, either download, upload or create the files used in previous tests 4) try to create and execute a file from blocked location 5) Run commands that are considered to be part of unusual process activity. 6) Try to access data with a process which should be restricted (e.g. try to access web content with text editor, e.g. start WinWord, file -> open -> http://www.google.com).	Is the monitoring system capable of providing an alert or a notification in case malicious software is installed, attempted to be installed, executed, or attempted to be executed? Does monitoring system detect in case anti-virus software is malfunctioning or is not up-to-date? Does monitoring system detect in case there are any changes noted by file integrity monitoring? Does monitoring system detect in case application access restrictions are not working?	Is the system capable of providing an alert or a notification in case malicious software is installed, attempted to be installed, executed, or attempted to be executed? Does the system have the ability to block installation, prevent execution or quarantine malicious software? Does the system have automatic remediation mechanisms? Is the system capable of providing an alert or a notification in case anti-virus software is malfunctioning or is not up-to-date? Is application whitelisting working as expected? Is the system capable of providing an alert or a notification in case there are any changes noted by file integrity monitoring? Is the system capable of providing an alert or a notification in case external media is taken into use? Is the system capable of preventing creation and	5 - Malware Defences

							running files in the blocked locations? Monitor for unusual process activity and service creation events. Is the system capable of providing an alert or a notification in case there is process activity which is unusual? Are the access re-strictions for application working and is the system capable of providing an alert or a notification in case there is an attempt to brake these restrictions?	

A.12.3.1	Backup	Information backup	Control Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.	Deploy mechanisms for automated backup, backup verification and testing of the backup images. System shall store the backup to a location which is not continuously addressable from the backed up system.	check that there is a log event that system has been backed up verify the backup image integrity test the backup images by performing a restore to the test system	Does monitoring system detect if backup has failed? Does monitoring system create an event or alarm if backup has not been taken according to the policy? Does monitoring system detect if backup image integrity tests have failed?	Is the system capable of creating an alarm if there's an event indicating that the backup has failed? Is the system capable of creating an alarm if verification of the backup image integrity fails? Is the system capable of performing restore automatically to a test system? (If yes, will system generate an alarm if the restore test fails?)	8 - Data Recovery Capability

A.12.4.1	Logging and Monitoring	Event logging	Control Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.	Implement automatic monitoring and analysis of the event logs to servers, network devices and hosts.	As a user, try to read file which is not allowed (e.g. cat /etc/shadow). As a user (which is not defined in “sudoers” file) try to run command "sudo su -" As a user (which is defined in sudoers file) try to read a file which is allowed when using sudo (e.g. "sudo cat /etc/shadow") Change system's firewall configuration. Change any other random configuration file at the system. Disable antivirus. Disable IDS. Print details about the logging system capacity and perform estimation whether the capacity is sufficient during peak hours.	Is monitoring system able to receive, correlate and create events for the log events (defined in test sequence)?	Does all log events for this test include user ID, date, time and device identity? Does the log event indicate successful and rejected data and other resource access attempts? Does the log event indicate that firewall configuration was changed? Does the log event indicate that system configuration was changed? Does the log indicate when privileges have been escalated? Does the logs from network devices include date, timestamp, source address, destination address and other details about the packet? Is alarm raised in case anti-virus is disabled? Is alarm raised in case IDS is disabled? According to the calculated estimated, does the logging system have enough capacity during peak hours? Do the applications create logs of transac-	13 - Boundary Defence 14 - Maintenance, Monitoring and Analysis of Audit Logs

							tions and are these logs automatically analysed and stored to central logging system?	

A.12.4.2	Logging and Monitoring	Protection of log information	Control Logging facilities and log information shall be protected against tampering and unauthorized access.	Deploy centralized audit logging. Separation of duties shall be enforced when planning log administration practices. Archive and digitally sign log files periodically.		Does the monitoring system preserve the integrity of the logs? Is the integrity of audit logs checked periodically?	Does each system log appropriately to a central log management system? Does the system create an alarm if logging has been stopped? Does the logging machine have user credentials for any other user than those dedicated to the administration of this machine?	14 - Maintenance, Monitoring and Analysis of Audit Logs
A.12.4.3	Logging and Monitoring	Administrator and operator logs	Control System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.	Monitoring for the system admin and operator activities (for example SSH Cryptoauditor). Filters for certain type of events indicating administrative privileges being used (e.g. commands sudo, su).	Initiate administrative access to the number of servers in the network.	Is it possible to observe and analyse afterwards what has been done during the administrative session? Is monitoring system capable of raising alarms to certain type of administrative actions (for example use of commands sudo or su)?	Is it possible to observe and analyse afterwards what has been done during the administrative session? Is system capable of raising alarms to certain type of administrative actions (for example use of commands sudo or su)?	14 - Maintenance, Monitoring and Analysis of Audit Logs
A.12.4.4	Logging and Monitoring	Clock synchronisation	Control The clocks of all relevant information processing systems within an organization or security domain shall be synchronised to a single reference time source.	Impement at least two synchronized time sources, i.e. NTP servers, from where all servers and network equipment fetch the time information.	Log in to servers and observe that time is set correctly.	Is alarm raised if system time or time sources are re-configured?	Is the time correctly configured? Is alarm raised if system time or time sources are re-configured? Is the system capable of restoring the time automatically?	14 - Maintenance, Monitoring and Analysis of Audit Logs

A.12.5.1	Software and Security Configuration Integrity management	Installation of software on operational systems	Control Procedures shall be implemented to control the installation of software on operational systems.	Use software signed with proprietary CA only. Use application whitelisting technology (e.g. Applocker for Windows) Use system integrity monitoring which alarms on new and changed files. Deploy software asset inventory tools. Implement possibility to perform regular scanning for unauthorized software. Implement mechanisms to verify the integrity of the platform (for example using trusted execution technology and remote attestation). Perform scanning with a tool which can do a technical compliance checking for security configuration against standard/best practice document or guideline, for example a SCAP compliant tool.	Try to install unsigned software. Download compressed software package which contains libraries and binaries and is not on white-list. Try to install software which is not on the white-list and/or software asset inventory. Scan servers for unauthorized software. Scan the security configuration on regular basis and compare the results against known baseline.	Is the monitoring system capable of detecting and creating an alarm in case files in the scanned system have been changed? Does this alarm contain information who made the change and when? Is the monitoring system capable of performing security configuration checks against pre-defined baseline/standard/best practice? Is monitoring system capable of detecting and creating an alarm in case there has been changes in the software asset inventory?	Does the application whitelisting functionality work? Is system capable of detecting and creating an alarm in case there's an attempt to install unsigned software? Is system capable of detecting and creating an alarm in case there's a compressed file which contains unauthorized software? Is system capable of detecting and creating an alarm in case files in the scanned system have been changed? Does this alarm contain information who made the change and when? Is the system capable of performing security configuration checks against pre-defined baseline/standard/best practice? Is system capable of detecting and creating an alarm in case there have been changes in the software asset inventory?	2 -Inventory of authorized and unauthorized software

A.12.6.1	Vulnerability management	Management of technical vulnerabilities	Control Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	Software asset inventory combined with continuous vulnerability scans. Configure only required ports, protocols, and services to each system. Keep the vulnerability scanning tools updated. Perform scans for configuration based vulnerabilities. Correlate the event logs with information from vulnerability scans. Perform scans using administrative account which is dedicated for this purpose and is tied to scanners IP address. Deploy automated patch management and software update tools. Install software patches regularly.	Verify that scanning tools have successfully completed the scans. Install software module known to be vulnerable (or downgrade software module to previous, vulnerable version.) Make the scan fail (i.e. by off lining scan target) Open new listening port. Deploy new system in the network which is not based on the standard system image and contains additional services or ports. Perform configuration changes in standardized system which are against the policy. Left them for 30-60 minutes and revert back.	Is the monitoring system capable of generating an alarm in case new software vulnerabilities are found? Is the monitoring system capable of generating an alarm if a scan fails? Is the monitoring system capable of providing criticality scoring based on risk level? (for example CVSS based) Is the monitoring system capable of detecting and creating an alarm if new listening ports are detected? Is the monitoring system capable of detecting new hosts in the network that are serving non-documented ports? Is the monitoring system capable of detecting security configuration changes in the system and if yes, is it capable of determining what was done (for example addition, removal, alteration, owner, permissions, contents) and who did it?	Does event logs indicated that vulnerability scan has been made and does the system create event / alarm when the scan is performed?	3 - Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers 4 - Continuous Vulnerability management and Remediation 11 - Limitation and Control of Network Ports

A.13.1.1	Network Security	Network controls	Control Networks shall be managed and controlled to protect information in systems and applications.	Deploy network traffic collection and analysis (using Netflow or similar.) Configure current network traffic policy to the monitoring tool. Deploy Intrusion Detection System (for example snort based), to DMZ, which are connected to SIEM and complemented with IPS. Deploy firewalls to protect each network segment/zone and configure traffic restrictions on IP level and port level (whitelist / blacklist) with default deny rule. Restrict ICMP traffic to intranet only. Create an alarm and capture traffic if there's an attempt to send ICMP traffic to external networks. Deploy honeypots to detect network reconnaissance and hacking attempts: (for example www-proxy.domainname, smtp-proxy.domainname, dns.domainname, www-site.domainname). Set-up proxy servers to DMZ with less obvious domain names (make sure all connections are being logged and sent to centralized logging.) Make sure that network devices (switches, firewalls, routers) send their logs to centralized logging and that log contains sufficient information about the traffic. Deploy host-based firewalls to servers (and workstations). Monitor network device configuration and issue alarms in case the configuration has been changed.	Try to send generate which brakes the firewall policy (e.g. to IP address which is not allowed). Perform a network scanning for DMZ. Try to generate ICMP traffic towards external networks. Perform network scan towards honeypot(s). Try to abuse or exploit the services offered by honeypot(s). Try to abuse or exploit services offered by actual proxy servers. Perform network scan towards servers (not on DMZ). Change router, switch and firewall configuration. Try to establish remote administrative connection (e.g. psexec, RDP, SSH from one host within a network zone to another). Add new system to the network which is not registered in asset management system and does not have sufficient client credentials (for example certificates used for 802.1x authentication.) Try to transfer or send out sensitive information or documents containing the keywords that are configured in perimeter monitoring tool. Deploy a test service on exter-	Is traffic monitoring system able to capture and create an alarm on traffic which violates the current policy? Is system capable of detecting and creating an alarm if unauthorized hosts, not in asset management system, are being added into the network? Does the log event contain enough details about the traffic information (for example time, date, system id, source IP, destination IP, packet details)? Is IDS able to detect network scans for DMZ? Is modification of configuration on router, switch or firewall being detected? Is the monitoring system able to use logs from honeypots, DNS, proxy, mail server and firewall as threat intelligence?	Is firewall effectively blocking the traffic and is it capable of creating an alarm for the blocked traffic? Does the log event consist enough details about the traffic information (for example time, date, system id, source ip, destination ip, packet details)? Is monitoring system able to detect network scans for DMZ (using for example an IDS as intelligence)? Is IPS able to block network scans for DMZ? Is outbound ICMP traffic detected, blocked and captured? Are honeypots creating system events that can be used to create alarms when honeypot services are being abused or exploited? Are actual proxy servers able to create system events that can be used to create alarms when there's an attempt to exploit or abuse these services? Does host based firewall effectively block the scanning attempts and	1 - Inventory of Authorized and unauthorized devices 10 - Secure Configuration for Network Devices 11 - Limitation and Control of Network Ports 13 - Boundary Defence

				Prevent lateral movement within a network zone and between the zones (generally, there should be no need for inbound access to clients or outbound from servers, or client-to-client connections.) Block remote administration from any other than admin network zone. Deploy DHCP logging (and correlate the information from DHCP logs with asset management to detect unauthorized systems). Deploy 802.1x network level authentication Deploy Network Access Control (NAC) Deploy an automated tool on network perimeters that monitors for certain sensitive information (for example personally identifiable information), keywords, and document characteristics to discover unauthorized attempts to exfiltrate data across network boundaries. Block the transfer and alert administrative personnel. Deploy automated tool to perform scanning on external perimeter (from outside of an organization's network) to detect possible exposure of unwanted services. Make use of anti-abuse feeds (such as Shadowserver, Spamhaus, etc to effectively monitor the abuse of the resources under your domain.	nal perimeter Deploy a host under your domain and register that to anti-abuse service.		create system events that can be used to create alarms? Is modification of configuration on router, switch or firewall being detected? Are remote administration attempt within a network zone blocked and detected? Is an unauthorized system able to get IP address? Is unauthorized host being quarantined to certain restricted network zone? Is unauthorized host able to have visibility to servers providing actual business services? Is exfiltration of data containing sensitive information or predefined keywords being blocked and detected? Is the exposure of new services on external perimeter detected? Is information regarding the host that is registered to the anti-abuse service received, handled and properly processed?	

A.13.1.3	Network Security	Segregation in networks	Control Groups of information services, users and information systems shall be segregated on networks.	Deploy segregated network zones (at least three-tier architecture, DMZ, middleware and private network). Configuration communication policies so that it goes always through proxy servers located in DMZ. Set-up internal DNS servers and deploy DNS logging. Deploy DNS whitelisting. Block and capture DNS traffic which is not going via internal DNS server.	Verify that traffic policies are correctly defined using scanning tools and tools which generate traffic that violate the policy (for example using nmap, hping). At host on each network segment, verify that inbound and outbound communications which is not going via proxy is blocked. (Perform tests also from external networks). Make domain name query to internal DNS server. Make domain name query to external DNS server. Make domain name query to internal DNS server using domain not in whitelist.	Is the monitoring system able to detect DNS queries which are destined to external DNS servers? Is the monitoring system able to detect DNS queries to domains which are not in the whitelist?	Is it possible to send traffic which violates the current network policy? Is it possible to establish inbound or outbound connections which are not going via proxy? Are DNS queries logged? Are DNS queries to external DNS servers blocked and detected? Are DNS queries to domains which are not on whitelist being blocked and detected?	10 - Secure Configuration for Network Devices 13 - Boundary Defence 19 - Secure Network Engineering

APPENDIX B. Detailed results from evaluation

Detailed results from evaluation are presented on the table below.

Table 7. Detailed results from evaluation

			Tenable SecurityCenter Continuous View		Alienvault USM		Qualys Policy Compliance	
EC-x	Domain	Evaluation criteria	**Observation**	**Additional info (when applicable)**	**Observation**	**Additional info (when applicable)**	**Observation**	**Additional info (when applicable)**
EC-1	Asset mgmt	Is the monitoring system capable of detecting new hosts? (If so, how long does it take that this could be noticed?)	Yes	PVS can notice this immediately when traffic is passed on new host. The detection time on the monitoring console depends on configured alarms/events.	Yes	Alienvault has active detection via scheduled nmap scans as well passive method to detect new hosts (PRADS, Passive Real-time Asset Detection System) which can detect the hosts almost in real-time. The alarm can be triggered using for example Inventory Anomalies Data Source.	Yes	Mapping scan can detect new hosts added to the network. This is done using active scan.

		Is the monitoring system capable of detecting new software modules on hosts? (If so, how long does it take that this could be noticed?)	Yes	System can do software enumeration for Windows and Linux targets. It is also possible to detect changes on installed software modules but this requires customized alarm/event. The detection time on the monitoring console depends on configured alarms/events. Not all OSes may be supported (at the time of writing software enumeration did not work for the Ubuntu 14.)	No	USM does not create a software asset list, for that purpose e.g. OCS INVENTORY could be used.	Yes	This is possible if scan is performed against golden image. Full software enumeration is only possible for Windows hosts.
		Is it possible to define rules for expected and unexpected changes in asset management database and create alarms based on those rules?	Yes	It is possible to configure dynamic assets that can be used to generate an alarm/event.	No	By default this is not possible, this would require using additional scripts or external software.	Yes	It is possible to create a baseline (or golden image) using any target. Deviations from this baseline can be pointed out. It is to be noted that full software enumeration is possible only for Windows hosts using authenticated scan.
		Is the monitoring system capable of generating an alarm in case new software vulnerabilities are found?	Yes	Vulnerability management is the main functionality of the tool	Yes	By default the vulnerability scan is creating tickets of the found vulnerabilities.	Yes	It is possible to create tickets based on vulnerabilities.
EC-2	Vulnerability mgmt	Is the monitoring system capable of generating an alarm if a scan fails?	Yes	There are plugins which indicate a scan failure. Scan failure will also be logged in SecurityCenter logs.	No	It is not possible to create an alarm, however it is possible to send a notification when the scan has ended.	No	It can be configured that status mail is being sent when scans start and finish. It is also possible to receive mails when scanners have not had any contact for x number of heartbeats.

		Is the monitoring system capable of providing criticality scoring based on risk level? (for example CVSS based)	Yes		Yes		Yes	
		Is the monitoring system capable of detecting and creating an alarm if new listening ports are detected?	Yes		Yes	This can be detected either via passive monitoring and also if host which has ossec-client installed has a monitoring for this (using for example netstat command).	Yes	New ports can be detected using scans which can be used as a basis to create tickets. Qualys has a feature (separate license) for VM on external perimeter: CM (Continuous Monitoring) which can continuously scan the external perimteer and can alert on changes. E.g. Ports, hosts, certificates, software, vulnerabilities.
		Is the monitoring system capable of detecting new hosts in the network that are serving non-documented ports?	Yes	The rulesets for approved and non-approved ports need to be defined.	Yes	It could be possible to configure this type of alarm but it would require use of external program (for example a script). The way to configure this is to trigger the external program via certain event and then do a white-list comparison using external program, and trigger another event that makes alarm / ticket if comparison notices forbidden ports.	Yes	If there are deviations to the golden image, these are pointed out in the reports.

		Is the monitoring system capable of detecting and creating an alarm in case files in the scanned system have been changed? Does this alarm contain information who made the change and when?	Yes	LCE client can monitor file integrity on the target. However, in order to determine what was done, additional logging (for example BSM audit logs) is required.	Yes	File integrity monitoring feature from ossec can be used for this, it is also possible to use ossec in agentless mode, meaning that system is scanned for file integrity changes regularly. It cannot be seen who made the change and when, to have this information additional logging (for example BSM audit logs) is required. Alienvault USM does not include a plugin for BSM audit log events.	Yes	It is possible to use file integrity monitoring and create a ticket in case changes are detected. It is not visible who has made the changes and when for that additional logging (for example BSM audit logs) is required.
EC-3	Software and Security Configuration Integrity management	Is the monitoring system capable of performing security configuration checks against pre-defined baseline/standard/best practice?	Yes	It is possible to run vulnerability scans against audit files, provided for example by CIS (Center for Internet Security) or NIST. Used audit file depends on the target OS. For example SCAP compliant scans can only be done for those to which there is a possibility to get audit file from NIST. Tenable provides a tool (xTool) for re-formatting NIST SCAP baseline files so that they can be interpreted by SecurityCenter. Tenable provides pre-formatted CIS-audit files.	No	Alienvault does not provide baselines for security configuration and the tool does not include these types of checks.	Yes	Either comparing to the policy based on the golden image or optionally using existing security configuration policy templates. There are several different policy templates to assess security configuration, for example CIS based policies (for many different Operating Systems) and SCAP policies (mainly for Windows.) SCAP files can also be imported to the tool.

		Is the monitoring system capable of detecting and creating an alarm in case there have been changes in the software asset inventory?	No	There is currently no standard report that could provide this information. However this could be achieved using customized report.	No	Other tools would be required to do this, for example OCS inventory. However, ossec inventory monitoring can detect addition of new files and change of integrity of the monitored files.	No	This is possible if software enumeration can be performed (which is mainly targeted for Windows). For Linux there is limited capability.
		Is it seen from the monitoring system when new users are added or removed?	Yes	Requires that LCE client is installed. Might work also if server is sending logs to LCE server via syslog.	Yes	If OSSEC agent is installed. It is possible to receive the logs also via syslog to Alienvault USM.	Yes	Files containing user info can be monitored.
		Is it seen from the monitoring system what type of privileges a user has for each system (for example under certain group?)	Yes	Requires that LCE client is installed. Might work also if server is sending logs to LCE server via syslog.	No		Yes	It is possible to detect users with certain privileges (for example if UID or GID equals 0).
		Are access attempts with deactivated account visible in the monitoring system?	Yes	It is seen as login failure.	Yes	If OSSEC agent is installed. It is possible to receive the logs also via syslog to Alienvault USM.	No	The tool is mainly based on scanning the targets and is not able to actively monitor the logs. It could be possible to use cron based scripts to analyse the logs and then the results of these scripts could be further made available for Qualys for reporting.
		Is it possible to see from a monitoring system that user is about to expire?	No	There is no such plugin in Nessus for Linux. For Windows there is (User Management)	No		Yes	There are controls which can see if user accounts are about to expire.
EC-4	Access Control	Does the monitoring system offer a possibility to perform baseline checks and compare the results to the system's current user account list periodically?	No	There is no such plugin in Nessus for Linux. For Windows there is (User Management)	No	There is no such feature, additional tools would be required.	Yes	By using for example Golden Image policy.

		Is it possible to see from the monitoring system if user authentication fails?	Yes		Yes	If OSSEC agent is installed. It is possible to receive the logs also via syslog to Alienvault USM.	No	The tool is mainly based on scanning the targets and is not able to actively monitor the logs. It could be possible to use cron based scripts to analyse the logs and then the results of these scripts could be further made available for Qualys for reporting.
		Is it possible to see from the monitoring system if user authentication succeeds?	Yes		Yes	If OSSEC agent is installed. It is possible to receive the logs also via syslog to Alienvault USM.	No	The tool is mainly based on scanning the targets and is not able to actively monitor the logs. It could be possible to use cron based scripts to analyse the logs and then the results of these scripts could be further made available for Qualys for reporting.
		Is security event in the monitoring system raised after number of failed authentication attempts?	Yes	This depends on the configured alarms/events.	Yes	If OSSEC agent is installed. It is possible to receive the logs also via syslog to Alienvault USM. The threshold used to create an alarm can be configured using correlation directive, i.e. if certain event occurs n times within certain time period alarm can be raised.	No	The tool is mainly based on scanning the targets and is not able to actively monitor the logs. It could be possible to use cron based scripts to analyse the logs and then the results of these scripts could be further made available for Qualys for reporting.

		Are there any accounts which are: - not authorized - only in one system - generic (not bound to user account) - not having expiry date? - locked-out - disabled - with passwords that exceed the maximum password age - with passwords that never expire - are there any system accounts which are not supposed to be there (i.e. no business owner). And can the monitoring system provide a list of these accounts?	No	There is no such plugin in Nessus for Linux. For Windows there is (User Management)	No	Monitoring system cannot provide a summary or list of user accounts.	Yes	Generally speaking user information can be compared to the Golden Image. Some of the other settings for user account can be detected also using in-built policies (such as users not having account expiry date, maximum password age, etc.)
EC-5	Logging and Monitoring	Is the monitoring system able to receive, correlate and create events for the log events (defined in test sequence)? The test sequence consist of actions where unauthorized and authorized users (try) to access and modify files and then it is checked whether the monitoring tool is able to receive and correlate those events and create an alarms for them.	Yes	When BSM audit is configured on target, logs regarding file access are sent to LCE. These appear as unnormalized LCE events. It is possible to create an alarm out of LCE query. (LCE alarms (save as query, create workflow)	No	Not by default. Only if additional audit logging is configured on the monitored system and Alienvault can interpret the event. There is currently no BSM audit log plugin.	No	Integration with SIEM (for example Arcsite, Logpoint Splunk etc.) via the Qualys API would be required to fulfil this. The tool is only able to see modification of the files if it has occurred.

		Does the monitoring system pre-serve the integrity of the logs?	No		Yes	Processed log events are stored in the system and SHA1 hash of the logs is taken which is signed. This could be used later on to validate the log integrity.	No	The tool does not collect any audit logs, it is not meant for that purpose. (This refers to integrity of the logs that it collects from the systems.)
		Is the integrity of audit logs checked periodically?	No		No	The log integrity is not validated or checked. This can be only done manually.	No	The tool does not collect any audit logs, it is not meant for that purpose.
		Is it possible to observe and analyse afterwards what has been done during the administrative session?	No	This is only possible if additional controls and logging is provided by the target. Any type of log can be sent to LCE server.	No	There is no log correlation for BSM audit logs.	No	The tool is mainly based on scanning the targets and is not able to actively monitor the logs.
		Is the monitoring system capable of raising alarms to certain type of administrative actions (for example use of commands sudo or su)?	Yes	Requires that LCE client is installed.	Yes	If OSSEC agent is installed. It is possible to receive the logs also via syslog to Alienvault USM.	No	The tool is mainly based on scanning the targets and is not able to actively monitor the logs.
		Is an alarm raised if system time or time sources are re-configured?	Yes	Requires that LCE client is installed.	Yes	If the is modified and an event is raised this can be collected and used to create an alarm.	No	The tool is mainly based on scanning the targets and is not able to actively monitor the logs.
		Is it possible to define the current network policy to the monitoring system?	No		No	It could be possible to do for exam-ple netflow data analysis using external program if triggered by certain event.	No	The tool is mainly based on scanning the targets and is not able to actively monitor the network traffic.
EC-6	Network Security	Is traffic monitoring system able to capture and create an alarm on traffic which violates the current policy?	Yes	In case firewall logs are sent to LCE and assumption being that firewall is configured according to the network policy and works as expected.	Yes	Firewall logs can be received for example via syslog. It is required to have a plugin to do a log correlation. Assumption being that firewall is configured according to the network policy and works as expected.	No	The tool is mainly based on scanning the targets and is not able to actively monitor the network traffic.

		Does the log event contain enough details about the traffic information (for example time, date, system id, source IP, destination IP, packet details)?	No	System does not contain traffic dumps.	Yes	Netflow data is collected and can provide some of this information.	No	The tool is mainly based on scanning the targets and is not able to actively monitor the network traffic.
		Is the monitoring system able to detect network scans for DMZ (using for example an IDS as intelligence)?	Yes	PVS is able to detect this.	Yes	Using the in-built IDS (suricata) it can detect network scans.	No	The tool is mainly based on scanning the targets and is not able to actively monitor the network traffic.
		Is modification of configuration on router, switch or firewall being detected?	No	Only in case this info is visible on device log events and if they are sent to LCE. There is no integrity checking of configuration.	No	Only if a log event is generated on the change and this information is sent to Alienvault USM and there is a plugin which can interpret the event. For a limited set of vendors (for example Cisco) Alienvault USM can do configuration integrity checking.	No	It is possible only for Cisco and Juniper, others are not supported.
		Is the monitoring system able to use logs from honeypots, DNS, proxy, mail server and firewall as threat intelligence?	Yes	Any type of logs can be sent to LCE but by default these logs will not trigger any alarms. All alarms need to be configured separately.	Yes	Log correlation plugins exist for bind and squid and for number of honeypots. Events can be sent either via syslog or sometimes using ossec if it has a decoder already in-built for that type of log. When ossec is used there is no need to use USM plugin.	No	The tool is mainly based on scanning the targets and is not able to use logs as threat intelligence.