jamk.fi

Practical implementation of Windows end-point security controls

Facing the KATAKRI requirements

Tuomo Leppänen

Master’s thesis
October 2017
Cyber Security
Master’s Degree Programme in Information Technology

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Description

Author(s) Leppänen, Tuomo	Type of publication Master's thesis	Date October 2017
		Language of publication: English
	Number of pages 65	Permission for web publication: x

Title of publication
Practical implementation of Windows end-point security controls
Facing the KATAKRI requirements

Degree programme
Master's degree programme in Information Technology

Supervisor(s)
Kotikoski, Sampo

Assigned by
Mustikkamaa, Tommi

Abstract

National Security Auditing Criteria (KATAKRI) is used as a tool for assessing the ability of different organizations to protect classified information. The criteria themselves can be interpretative and as such difficult to understand in practice. The aim of this thesis was to build a proof-of-concept solution that could give an answer to certain of the KATAKARI auditing criteria's I-series questions in practice. This series focuses on the technical information security requirements. In the thesis the subject was approached from the point of view of workstations.

The assigner required that the Microsoft Windows 10 operating system is to be used in the assignment. The suitability of improving the overall security with the operating system's new security features was also studied during the assignment. When the hardware manufacturers stop supporting Microsoft's previous operating systems, moving to the company's latest operating system is inevitable.

The top four mitigation strategies defined by the Australian Signals Directorate were used to assist in the implementation of the project. This list is based on statistical research of attack techniques and therefore provides good grounds for implementing such security controls. The strategies consist of minimizing the administrative privileges, application and operating system patching and using application whitelisting.

The proof-of-concept solution implemented in the assignment can be used to meet the requirements of certain KATAKRI auditing criteria. As a result of this study, it can be said that all additional security features provided by the used version of Microsoft Windows 10 operating system are not yet mature enough for a comprehensive deployment.

Keywords/tags (subjects)

KATAKRI, Windows 10, Mitigation, Security Controls

Miscellaneous

jamk.fi

Kuvailulehti

Tekijä(t) Leppänen, Tuomo	Julkaisun laji Opinnäytetyö, ylempi AMK	Date Lokakuu 2017
		Julkaisun kieli: Englanti
	Sivumäärä 65	Verkkojulkaisulupa myönnetty: x

Työn nimi

Practical implementation of Windows end-point security controls

Facing the KATAKRI requirements

Tutkinto-ohjelma

Master's degree programme in Information Technology

Työn ohjaaja(t)

Kotikoski, Sampo

Toimeksiantaja(t)

Mustikkamaa, Tommi

Tiivistelmä

Kansallisen turvallisuuden auditointikriteeristöä (KATAKRI) käytetään työkaluna arvioitaessa eri organisaatioiden kykyä suojata viranomaisen salassa pidettävää tietoa. Kriteeristön asettamat vaatimukset voivat olla tulkinnanvaraisia ja sellaisenaan hankalasti ymmärrettäviä toteuttaa käytännössä. Opinnäytetyön tarkoituksena oli rakentaa proof-of-concept-ratkaisu, jolla voitaisiin vastata osaan KATAKARI-auditointikriteeristön I-sarjan kysymyksistä käytännössä. Kyseinen sarja keskittyy teknisen tietoturvallisuuden vaatimuksiin. Opinnäytetyössä aihetta lähestyttiin työasemien näkökulmasta.

Työn toimeksiantaja halusi, että työssä käytetään Microsoft Windows 10-käyttöjärjestelmää. Käyttöjärjestelmä esittelee uusia tietoturvaominaisuuksia joiden toimivuutta kokonaisturvallisuuden parantamiseksi myös tutkittiin. Laitevalmistajien lopettaessa tuen Microsoftin edellisille käyttöjärjestelmille siirtyminen yrityksen viimeisimpään käyttöjärjestelmään on väistämätöntä.

Australian Signals Directoraten määrittelemää top 4-mitigointistrategialistaa käytettiin avuksi työn toteutuksessa. Kyseinen lista perustuu hyökkäystekniikoiden tilastolliseen tutkimukseen ja antaa näin ollen hyvät perusteet kyseisten tietoturvakontrollien implementoinnille. Strategiat koostuvat järjestelmänvalvojien käyttöoikeuksien rajaamisesta, sovellusten ja käyttöjärjestelmän päivittämisestä sekä whitelisting-tekniikoiden käyttämisestä.

Lopputuloksena rakennettu proof-of-conceptilla voidaan vastata KATAKRI auditointikriteeristön asettamiin vaatimuksiin. Voidaan myös todeta, että kaikki työssä käytetyn Microsoft Windows 10-käyttöjärjestelmä version tarjoamat lisäturvallisuusominaisuudet eivät ole vielä kypsiä kokonaisvaltaiseen käyttöönottoon.

Avainsanat (asiasanat)

KATAKRI, Windows 10, Mitigointi, Tietoturvakontrollit

Muut tiedot

ACKNOWLEDGMENTS

I would like to thank my employer for the opportunity and support for doing this thesis. Special thanks for Mr. Sami Laiho for giving technical advice during the course of writing.

Contents

Acronyms

AD	Active Directory
ASD	Australian Signals Directorate
APT	Advanced Persistent Threat
ATP	Advanced Threat Protection
BIOS	Basic Input Output System
BYOD	Bring Your Own Device
CB	Current Branch
CBB	Current Branch for Business
CIA	Confidentiality, Integrity and Availability
DLL	Dynamic Link Library
DMA	Direct Memory Access
EMET	Enhanced Mitigation Experience Toolkit
FSCS	F-Secure Client Security
FSPM	F-Secure Policy Manager
FSSS	F-Secure Server Security
GPO	Group Policy Object
KATAKRI	National security auditing criteria
KMCI	Kernel-Mode Code Integrity
LAPS	Local Administrator Password Solution
LTSB	Long-term Servicing Branch
MD5	Message Digest 5
MSI	Microsoft Installer
POC	Proof of concept

RTM	Released To Manufacturing
SCCM	System Center Configuration Manager
SCM	Security Compliance Manager
SHA1	Secure Hash Algorithm 1
SLAT	Second Level Address Translation
SYSMON	System Monitor
TPM	Trusted Platform Module
UAC	User Account Control
UEFI	Unified Extensible Firmware Interface
UMCI	User-Mode Code Integrity
VBS	Virtualization-based security
WHQL	Windows Hardware Quality Labs
WIP	Windows Information Protection
WSUS	Windows Server Update Services

Figures

Tables

1 Introduction

1.1 Motivation and background

The purpose of this assignment was to develop a proof of concept based on certain limitations and regulations that the assigner is obligated to comply with. These requirements and regulations are based on the Finnish National Security Auditing Criteria (KATAKRI). Fulfilling these requirements creates a challenge on how to deal with certain administrative processes and how to implement the security controls in practice, while keeping the organization's business needs as effective as possible. Earlier research on this kind of practical implementation against Windows workstations did not exist.

Microsoft has stated that new PC chipsets produced by major manufacturers will only be supported on Windows 10 and not the earlier Windows versions (Myerson, 2016). As the organizations using older Windows versions have to renew their PC equipment at some point, this leaves no other choice than to move to the Windows 10 platform as well. This lead the assignment to focus on using Windows 10 and its new security features to address modern world security threats.

One of the requirements set by the assigner was that the implementation shall be done in an environment that does not have an Internet connection available at all, thus, using an operating system heavily dependent on Internet facing cloud services could be a challenge. Offline environments without a real-time cloud protection do not have the same protection level as the with a working Internet connection. On the other hand, offline environment does not have the same attack surface compared to the ones connected to the Internet.

1.2 Scope and objectives

The scope of thesis consisted of creating practical implementations on how Windows 10 operating system enhanced with additional technologies could fulfill end-user workstation related requirements defined in KATAKRI auditing criteria in practice. Besides fulfilling the requirements, another objective was to create working administrative processes for ways to maintain the implemented security controls.

As the assigner had already made some technology choices for anti-malware and Windows configuration management, the F-Secure and Microsoft management products were used in the thesis.

1.3 Research methods

Choosing the research method for this study proved to be quite difficult. As the assigner wanted to have a practical implementation on KATAKRI requirements against Windows 10 workstations, a decision was made to carry out a case-study in the form of proof-of-concept. The main research questions were:

- Can statistically proven mitigation strategies (The Australian Signals Directive, 2012) be used to answer the criteria defined in KATAKRI 2015, targeting end-point workstations?
- Can the new security features of Windows 10 operating system give any additional value for the mitigation strategies?
- How implement the above two in practice?

2 Basis for the study

2.1 About information security in general

Information security can be illustrated as a confidentiality, integrity and availability (CIA) triangle (Figure 1). According to Easttom (2012), CIA stands for confidentiality, integrity and availability. Confidentiality is used to make sure that only authorized users have access to the information, integrity is for ensuring that only authorized users can modify the information and availability is for ensuring that the information is accessible to the authorized users when it is requested (Kim & Solomon, 2014, 414).

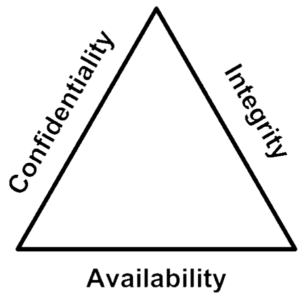


Figure 1. CIA triangle

2.2 Security controls and auditing

As noted by Kim & Solomon (2014, 232-233), security controls address a risk that might be targeted to the organization in case. These controls should be maintained so that they are effective and current. Reviewing the effectiveness and continuous improvement can be illustrated in a security cycle (Figure 2).

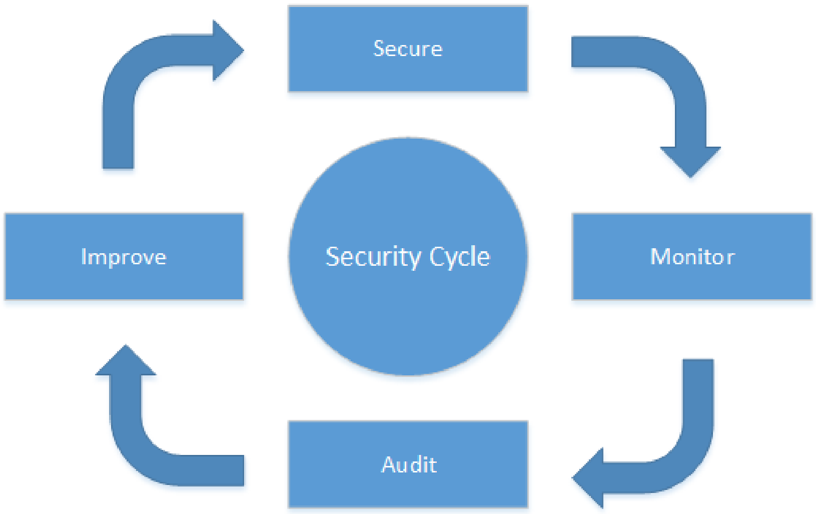


Figure 2. Security cycle

To protect business assets and mission from the risks they face is the main purpose of information security. Maintaining information systems and making sure that security controls work as expected, security audits can be conducted for verifying them. The implementation of security controls should be done so that they address the actual risks and not just because of security itself (Kim & Solomon, 2014, 231-232).

2.3 National Security Auditing Criteria – KATAKRI

KATAKRI is a Finnish auditing tool used to determine an organization's capabilities to secure government officials classified information. KATAKRI auditing criteria do not give implicit requirements, instead they are based on existing Finnish legislation and international regulations for information security obligated to the Finnish government. The principal source for KATAKRI's requirements is the Finnish government's regulation of information security in national government authorities. It also refers to other commonly known standards such as ISO 27000. The requirements in the criteria are divided into three different areas: security management (T), physical security (F) and information assurance (I). The requirements of the information assurance section can be fulfilled according to the three Finnish national protection levels IV, III and II which are equal to the international levels of classification: RESTRICTED, CONFIDENTAL and SECRET. (Ministry of Defence, 2015, 3-4).

The current publication of KATAKRI is the 3rd version, also known as KATAKRI 2015. The most significant change in the criteria between earlier releases is the focus on risk-based evaluation, which can be reflected to the ones in ISO 27001 (Nixu, N.d.). KATAKRI 2015 is used in this thesis.

2.4 Top four strategies to protect ICT systems

The Australian Signals Directorate (ASD) (2012) has created top four strategies to mitigate against threats targeted at ICT systems. The strategies are based on the analysis of known intrusions techniques. These top four mitigations are: application whitelisting, allowing only the needed applications to be run on the target machine; patching applications, running the latest versions of the software; patching operating systems, using the latest versions and minimizing administrative privileges.

2.4.1 Application whitelisting

According to Sedgewick, Souppaya & Scarfone (2015, 2), a whitelist is a discrete list of entities such as applications that are authorized to be present or active on a host according to a defined baseline. Whitelisting of applications is intended to stop the execution of unauthorized software, for example malware. The concept of application whitelisting is the opposite of blocking malicious files, instead whitelisting only permits to run known good executables on the target system. This can be achieved by creating a list of known file hashes and allowing the running of those files only on the target system (Beechey 2010, 3). Limiting what to run on gives administrators more control on what is happening in the environment.

2.4.2 Application and operating system patching

Flexera Software's Vulnerability Review (2016) research based on more than 50 000 applications, operating systems and appliances reveals that in the year 2015, 79% of software vulnerabilities affected non-Microsoft applications. The same report also shows the increase in vulnerabilities in all Microsoft Windows operating systems. Notable here is that Flash player is bundled with Windows 8 and Windows 10, thus it is added to the overall vulnerability count, which causes the increase in vulnerabilities against Windows 7 (Figure 3). As can be seen, the overall trend of vulnerabilities in Windows operating systems is rising.

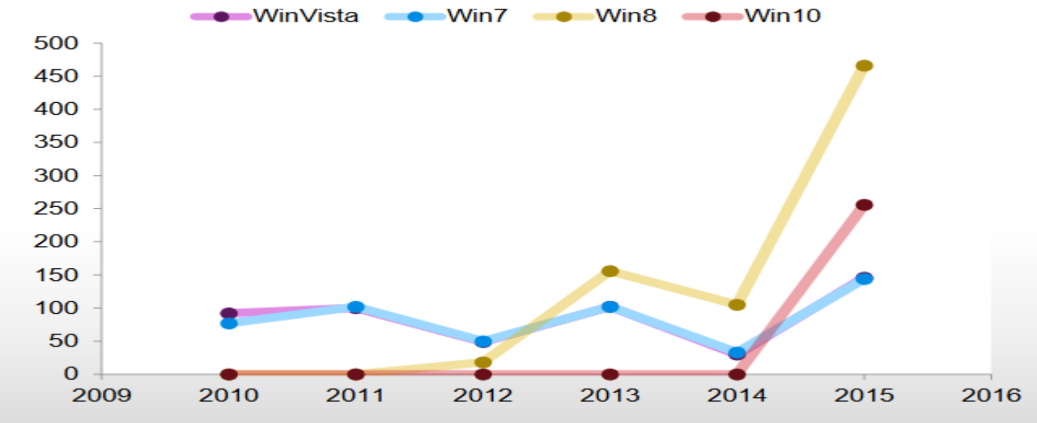


Figure 3. Vulnerabilities in Windows operating systems (Flexera Software, 2016)

According to Kim & Solomon (2014, 214), an organization must have a working process for handling patch-management so that all known vulnerabilities are addressed without causing any system outages. The patches should be reviewed and tested before the actual roll-out to make sure that they will not disable the functionality of working systems.

2.4.3 Minimizing administrative privileges

As noted by the Australian Defence Signals Directorate (2012), a usual target for an attacker is a user account with administrative privileges. Because administrators have high level access to the organization's systems, if these accounts are compromised, the attacker can have access to any data that the administrator can.

Restricting administrative privileges makes the doings of malicious code more difficult. An environment where privileges of the administrators are restricted becomes more stable, predictable, easier to administer and support because of the fact that only few trusted users can make changes to the operating environment (Australian Cyber Security Centre, 2016). A research made by Avecto (2017) reveals that 93% of critical Windows 10 vulnerabilities could be mitigated by removing administrative rights. Avecto's research was based on an analysis of security bulletins released by Microsoft in 2016.

3 Technology background

Windows 10 was the main target on the technology choices. As some of the technologies used by the assigner were already selected based on Microsoft Windows, a decision was made to make use of the existing and add something that has been proven to add value for the overall security. Metcalf (2016) describes that for the creation of a secure Windows end-point, the deployment of free Microsoft provided tools like Enhanced Mitigation Experience Toolkit (EMET) and Local Administrator Password Solution (LAPS) are required to increase the overall security of the system.

3.1 Windows 10 operating system and its security features

Windows 10 offers built-in security features such as the Windows Defender and most notably it is an advanced threat protection component (only offered to enterprise business customers). This chapter focuses mainly on the features that are not cloud-based since the limitation of proof-of-concept was the isolation of the Internet. As the technology choices for some parts of the implementation were driven by the assigner, the usage of antimalware solutions built into Windows 10 are not properly addressed here.

3.1.1 About different Windows 10 editions

Windows 10 operating system has four different versions or editions; Home, Pro, Enterprise and Education. From these the Pro and the Enterprise versions are targeted at business users. The Pro version lacks the security functionalities e.g. Device Guard, Credential Guard and AppLocker (Howse 2015) as well as disabling of Microsoft's data collection features. A more specific comparison of the features between each version can be found in Appendix 1.

3.1.2 Privacy concerns

Microsoft has publically admitted that its newest operating system, Windows 10, collects information about the user activity of the operating system. Exactly what is collected and sent back to Microsoft remains unknown. What is known, or at least most people suspect is that the data collected is used for profiling users for targeted advertisements. Microsoft says that the information is used to improve the user experience for the operating system (Sebastian 2015).

Most people do not even bother to read end-user license agreements and can therefore accept to act without even thinking what it actually means. Configuring what data is allowed to send is scattered in different places in the operating system, which also makes it much more difficult for the users to control. According to blog post by Kelly (2015), Microsoft’s corporate vice president Joe Belfiore has admitted that the end-users cannot control every data collecting feature of the operating system.

3.1.3 Changes in operating system updates – Windows as service

With Windows 10, Microsoft changed its approach dramatically on how the operating system is kept up to date. In earlier Windows operating systems there would be multiple individual patches that address certain security issues or bugs. As described by Mercer (2016a), some Microsoft customers would selectively choose what updates to install and that lead into problems such as complexity of testing those updates and different combinations of updates causing errors. The overall situation of selectively patching is illustrated in Figure 4.

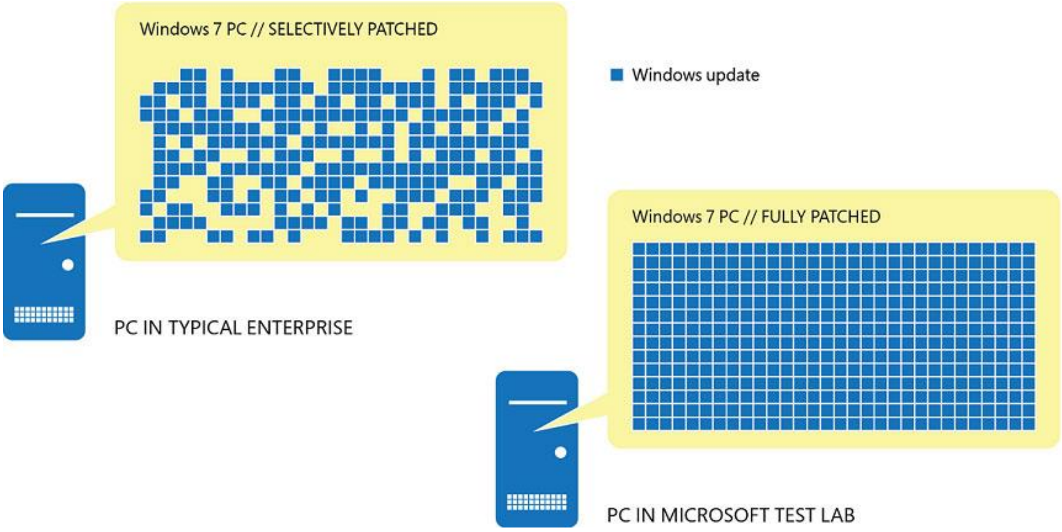

Windows 7 PC // SELECTIVELY PATCHED
Windows update
Windows 7 PC // FULLY PATCHED
PC IN TYPICAL ENTERPRISE
PC IN MICROSOFT TEST LAB

Figure 4. Illustration of selective patching in Windows OS.

When Windows 10 was launched, it introduced the new way of monthly patching, a cumulative approach. Each month there is only one software update to be delivered, including all the security updates and other fixes for that month, which are called *quality updates*. This way the operating system is always kept at certain level, even if the administrator forgot to deploy patches in some month. As of October 2016, Microsoft introduced this same approach for lower-level operating systems starting with Windows 7 (Niehaus 2016).

Another big change Microsoft introduced with Windows 10 is the way the new operating system features are delivered to the end-users. Traditionally, a new version of Windows operating system was released every 3 to 5 years. Although Microsoft is marketing Windows 10 as the last version of Windows, these *feature updates* are actually new build versions of the operating system. At the time of the writing, there have been three major version releases (or *feature updates*) of the operating system. The versions are labeled as the year and month they were released, which can be seen in Table 1.

Table 1. Windows 10 release information. (Microsoft Technet, 2016).

Servicing option	**Version**	**OS build**	**Availability date**
Current Branch (CB)	1703	15063.296	11.4.2017
Current Branch (CB)	1607	14393.1198	2.8.2016
Current Branch (CB)	1511	10586.916	12.11.2015
Current Branch (CB)	1507 (RTM)	10240.17394	29.7.2015
Current Branch for Business (CBB)	1607	14393.1198	29.11.2016
Current Branch for Business (CBB)	1511	10586.916	8.4.2016
Current Branch for Business (CBB)	1507 (RTM)	10240.17394	29.7.2015
Long-Term Servicing Branch (LTSB)	1607	14393.1198	8.2.2016
Long-Term Servicing Branch (LTSB)	1507 (RTM)	10240.17394	29.7.2015

As described by Halfin (2016) these new versions of Windows 10 are called *feature updates*. The delivery time (Figure 5) of each version is divided into different branches, which are basically a release cycle of builds for Windows 10 targeted for different audiences of the operating system:

- *Insider or preview branch* feature updates are the ones that are targeted at only those who want to test out the new features of the operating system before they are released for a broader audience. Basically this is a pre-version of the operating system.

- *Current Branch* (CB) feature updates are delivered as soon as Microsoft releases them, these would be the ones that normal home users get. Only one CB version is supported by Microsoft at a time. The new current branch version is delivered every 4 to 6 months.

- *Current Branch for Business* (CBB), is targeted for business users. Basically these are the same versions that were released as CB. CBBs are released about four months after CB and are supported by Microsoft for business users. Two CBB builds, plus 60-day grace period are supported by Microsoft at a time. To stay supported by Microsoft, administrators need to upgrade these versions of Windows 10 builds to new ones in about every 1 and half to 2 years.

- *Long-term Servicing Branch* (LTSB), is targeted for specialized systems and only receive quality updates. New LTSB versions are released every 2-3 years and are supported by Microsoft for a 10-year life cycle.

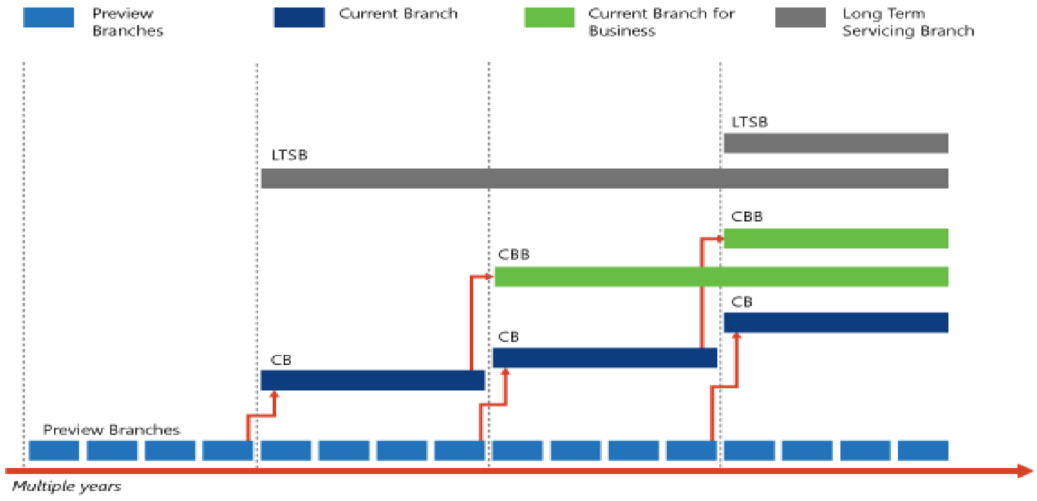


Figure 5. Time vs. Windows 10 servicing branches.

Microsoft markets the LTSB branch as only designed for mission-critical devices where it is more important to keep devices as stable and secure possible. The usual marketing punch-line is that, if there's a Microsoft Office installation on the computer, it should not run the LTSB version. LTSB comes only with the Enterprise edition features, so it has all the same security features as the standard Enterprise version of Windows 10. What really differs LTSB from other branches is the fact that it actually lacks some of the major features of Windows 10 that might not suit businesses. These features include Store, Cortana and Microsoft Edge browser as well as the built-in modern apps (Camera, Calendar, Calculator, Weather, News…) however it can run still these modern apps just like any other Windows 10 version (Hoffman 2016).

3.1.4 Malware resistence - Windows Defender ATP

Windows Defender Advanced Threat Protection (ATP) is a major feature of Windows 10, as described by Savill (2016), it is “a post-breach solution that aims to be the black box flight recorder to enable forensic analysis of exactly what happened”. This includes an answer to questions when, where and what exactly happened. Technically Windows Defender ATP sends data from the Windows operating system to the cloud where it is analyzed and enables the administrators to track the entire security breach timeline, nicely visualized through dashboards. As Kaelin (2016) explains, this kind of technology sounds good; however, the businesses need to give Microsoft access to the data in their environments, which might not be acceptable for everyone.

3.1.5 Biometric user authentication – Windows Hello

As described by Decker (2017), Windows Hello is a built-in biometric authentication feature of Windows 10. It lets the end-users to use their face or fingerprint for authentication instead of traditional username / password –pair. The biometric data is always stored locally on the device so there is no built-in centralized management solution, such as for example Active Directory, available at the time of this writing. Both facial and fingerprint recognition require Windows Hello certified hardware. The fingerprint sensor requires anti-spoofing measures implemented by the manufacturer and facial recognition cameras must use IR light, so that they can tell the difference between a living person and a photo while used. Facial recognition sensors must also have anti-spoofing measures implemented.

3.1.6 Information protection – BitLocker and WIP

BitLocker is a built-in disk volume encryption solution Microsoft has shipped since Windows Vista. It uses a Trusted Platform Chip (TPM) to detect unauthorized changes in the PC hardware and if changes are detected, read access to the secrets stored in the chip are denied. (Paul 2016). BitLocker also supports two-factor or even three-factor authentication when used with TPM + PIN or TPM + PIN + USB-key for unlocking the encrypted hard drive.

Microsoft (2005) describes TPM chip as "a microcontroller that stores keys, passwords and digital certificates." Access to this confidential information can be denied if the boot sequence of the computer is not as expected. Windows 8 introduced another technology called Secure Boot, which basically allows only authorized boot loaders to run when the PC starts. Secure Boot requires Unified Extensible Firmware Interface (UEFI) which replaces or works in conjunction with the legacy Basic Input Output System (BIOS). UEFI works as an interface between the operating system and the PC (Microsoft N.d.). BitLocker Using Secure Boot with BitLocker adds additional security to the overall configuration as no other but digitally signed bootloaders are allowed to be used in the system. Windows 10 introduced a few new features to the BitLocker platform compared to the older Windows versions; most notably the XTS-AES encryption algorithm support and DMA protection which can be used when the device is locked or starting up (Hakala 2017). BitLocker has been proven to be vulnerable to certain types of attacks: coldboot, also known as the Princeton attack being one of them (Appelbaum 2008). In a coldboot attack, the memory chips of the target machine are frozen, removed from the target and attached to another computer or specialized hardware to get the crypto keys out of them and use then that information to unlock the BitLocker encrypted hard drive. This kind of attack against the technology is plausible; however very unlikely, especially if the target machine resides in physically safe perimeter. A more likely attack method against BitLocker is to use direct memory access (DMA), where the crypto keys are stolen from the target machine through accessible high-speed extension port, such as FireWire (Panholzer 2008).

Windows information protection (WIP) is a new feature introduced in Windows 10 version 1607. This feature is designed to prevent accidental data leakage and to provide a seamless user experience for dividing personal and company data. Mercer (2016b) describes that the technology enables the administrators to configure a set of policies for company devices and the applications running on them, so that the end-users, or the company, can control which data is saved as personal. Smith (2016) explains that this feature also includes the restrictions for copy-paste actions, where users cannot paste company data to another application which is not configured as managed. A good example of this could be pasting data from company confidential document to a web browser. The use scenario for this feature is more likely on bring your own device (BYOD) type of scenarios where end-users are using their own equipment for doing their work.

3.1.7 Identity and access control - Credential Guard

Credential Guard is a new technology in Windows 10, and it isolates the user credentials from the local memory to a stored virtual container that the operating system cannot directly access. As described by Khanse (2016), the credential guard of Windows 10 increases the overall security of the domain credentials and hashes.

This technology can only be used to protect domain credentials from common tools such as Mimikatz to prevent the stealing of them from the computer's memory; it does not provide additional security for local accounts on a Windows machine. The credential guard requires a 64-bit processor, processor virtualization extensions and extended page tables (VT-x for Intel, AMD-V and Second Level Address Translation a.k.a. SLAT), TPM and UEFI with Secure Boot feature enabled (Lich 2017). Modern PCs have the technology required for this technology to work out of the box.

3.1.8 Malware resistance – AppLocker and Device Guard

Windows AppLocker introduced in Windows 7 is a successor of Software Restriction Policies feature. AppLocker can be used by administrators to control how and what standard users can run on the Windows operating system. AppLocker covers executable files, scripts, DLLs and Windows installer files. Rules can be defined based on attributes of the files, e.g. path, file name, version or digital signature. Targeting of the rules can be done with the help of security groups in either local computer or Microsoft Active Directory. Exceptions for different users or groups for the rules can also be made. (Microsoft TechNet Library, N.d.a).

Graeber (2016) describes Windows Device Guard as "a powerful set of hardware and software security features available in Windows 10 Enterprise and Server 2016 that aim to block the loading of drivers, user-mode binaries, Microsoft Installer (MSI) and scripts that are not explicitly authorized per policy. In other words it is a whitelisting solution. The idea, in theory, being a means to prevent arbitrary unsigned code execution."

Windows 10 devices configured with Device Guard do not allow running anything else than what is allowed, so it provides better security against zero day exploits and malware. Device Guard requires a 64-bit CPU, hardware virtualization extensions, UEFI with Secure Boot enabled and Hypervisor Code Integrity (HVCI) compatible drivers to work correctly (Microsoft, 2017). HVCI is used to determine whether the executed code in Windows kernel mode is securely designed and trusted. In general, virtualization-based security (VBS) is an overall solution for Windows 10 to isolate core operating system services (Hakala 2016). The same requirements apply to the earlier described Credential Guard feature.

The main difference between AppLocker and Device Guard is that AppLocker can be used to further adjust based on the file path, running user or group, i.e. what exactly is allowed to run. Device Guard works system-wide and doesn't care about the file location or the user running the code; this way Device Guard prevents malicious code from running by administrators or the system account itself.

3.2 Active Directory Domain Services and group policies

As described by Dubey (2016), Active Directory (AD) “provides a centralized solution for managing users, verifies the identity of users and authorizes resources on each access”. Active Directory is a widely-used technology in Windows based computer system environments.

Computers in an Active Directory domain can be managed through Group Policy Objects (GPO). Hoffman (2012) explains the Group Policy as a Windows feature that can be used to adjust settings for computers and users in an Active Directory Domain environment. Policies can be used to control what is allowed and what is not allowed for an end-user on a Windows operating system. Group Policies can also be used to automate administrative tasks in the environment.

3.3 Local Admin Password Solution

The Microsoft Local Administrator Password Solution is a group policy client-side extension enabling organizations to securely rotate the local administrators’ passwords on Windows operating systems. Technically, the passwords are stored in the Active Directory object of the computer account, this enables more granular control on who are allowed to read the password for each device (Beckman 2015). According to Penshorn (N.d.) LAPS significantly lowers the risk of pass-the-hash attacks in Active Directory environment, since the solution configures a different password for the administrator account on each device. This way if one device is compromised, the attacker doesn't gain access to other devices using the stolen password. Penshorn (N.d.) also points out that since the solution stores passwords as a clear text into Active Directory, misconfiguration may cause a critical security issue, thus the solution should be configured carefully.

3.4 System Monitor

System Monitor (Sysmon) is a freeware tool part of Sysinternals Suite, offered by Microsoft that extends the standard Windows event log with logging activity of process creations, network connections with involved processes, changes in the file system and generates events from early stages of the boot process to capture malicious activity (Perez, 2014). As mentioned by Russinovich (2016), built-in

Windows operating system logging functionality lacks the information captured for Dynamic Link Library (DLL) loading and process creation, as well as network connection information.

Events generated by Sysmon can be used to track which process initiated which network connection to what destination as well as tracking down which child process was started by another process. This information is useful while gathering evidence of malicious activity in the environment.

3.5 Enhanced Mitigation Experience Toolkit

Enhanced Mitigation Experience Toolkit (EMET) is a freeware tool offered by Microsoft to address 0-day vulnerabilities by using the built-in Windows security defenses such as address space layout randomization (ASLR) and data execution prevention (DEP). As described by Krebs (2013), “DEP is designed to make it harder to exploit security vulnerabilities on Windows and ASLR makes it more difficult for exploits and malware to find the specific places in a system’s memory that they need to do their dirty work.”

As statistically proven by Niemelä (2013) system hardening by itself is not effective mitigation against advanced persistent threat (APT) –based attacks. Instead, adding additional controls that can handle application memory, such as EMET, is effective. Furthermore, according to Dormann (2016), Windows 10 capabilities to mitigate against threats without EMET are not as effective as they are marketed to be.

3.6 Microsoft Security Compliance Manager

Microsoft offers a free tool called Security Compliance Manager (SCM). The tool is used to configure and manage Group Policy objects against Microsoft operating systems and other products, based on the recommended Microsoft security baselines (Andrabi 2016). Security baselines are collections of different settings that impact the overall security of the product in case. According to Lich (2016), baselines ensure that the device in case is configured accordingly. Microsoft recommends implementing industry-standard configurations that are commonly known and tested, instead of creating a baselines by oneself. Microsoft collaborates with the Center for Internet Security (CIS) to develop the baselines used with Security Compliance Manager (Center for Internet Security, 2013). Security Compliance Manager reduces the administrative effort of re-inventing the wheel by the administrators figuring out what controls to implement against their environment, as it gives clear startup points.

3.7 Microsoft System Center Configuration Manager

Microsoft System Center Configuration Manager, also known as SCCM or ConfigMgr, is a computer management system that is widely used in Windows environments. SCCM has capabilities to install applications, software updates and operating systems to computers as well as collect information out of them. Administrators can run any given command, executable or a script on SCCM managed endpoint, which gives major flexibility to do the tasks centralized. The endpoints targeted at different types of administrative tasks are gathered into collections, which can be made based on different set of rules, for example all the machines with Windows 10 as their operating system. These collections are dynamic which would mean that when the device in case meets the definition configured (in the managed environment), it would be automatically added to its dedicated collection and ready for accepting tasks defined by the administrator (Holt 2012).

3.8 F-Secure Policy Manager and Client Security

Finnish information security company F-Secure offers an overall solution for on-premises malware protection. The solution consists of management server and client agents for both server and workstation end-points. F-Secure Policy Manager (FSPM) offers the malware definition updates as well as policies for managed clients, F-Secure Client Security (FSCS) for workstations and F-Secure Server Security (FSSS) for servers. To update the anti-virus definitions in offline environments, the company offers a separately downloadable executable which includes the latest updates for their products (F-Secure, N.d). The product suite also includes a device control functionality which can be used in Windows environments to block devices attached to the clients from functioning based on device classes or hardware identifiers.

4 Proof of concept

The main focus of the proof of concept (POC) was to create an environment focusing on the end-point workstation that had the following elements:

- Requirements and limitations defined by the assigner
- Addressed the top 4 mitigation strategies defined by ASD
- Used additional technologies and built-in Windows 10 security features to face the mitigation strategies defined by ASD

4.1 Requirements for the assignment

The assigner's requirements for the POC were as follows:

- Environment shall be disconnected from the Internet, purely offline
- Try to find practical solutions for the requirements defined in KATAKRI, with the focus on the workstation requirements
- Windows 10 as the operating system running on a hardware provided by the assigner, acting as the targeted workstation
- Usage of technologies already in use
    - F-Secure products as an antimalware solution
    - SCCM as the centralized end-point management solution
- Usage of new technologies to better protect against modern threats potentially facing workstations in disconnected environments
- Design the usage of administrative processes for maintaining the overall security these new controls produce, trying to automate as much as possible to lower administrative effort

The focus was strictly on the operating system and its features and for the POC, the physical security was not taken into account. The targeted workstation would be used purely for creating documents, spreadsheets and presentations, thus Microsoft Office was the only additional end-user software installed.

4.2 Description of the POC environment

The POC environment consisted of three servers:

- Active Directory Domain Controller, DC
- System Center Configuration Manager, SCCM
- F-Secure Policy Manager, FSPM

All the servers in the environment were running Windows Server 2012 R2 operating system. The whole server environment was virtualized using Microsoft Hyper-V using a laptop as the hypervisor. This approach was suitable for demoing as the whole POC environment was portable. As some security features of Windows 10 require physical hardware to work, the client PC for the POC was also running on a laptop. Illustration of the environment can be seen in Figure 6.

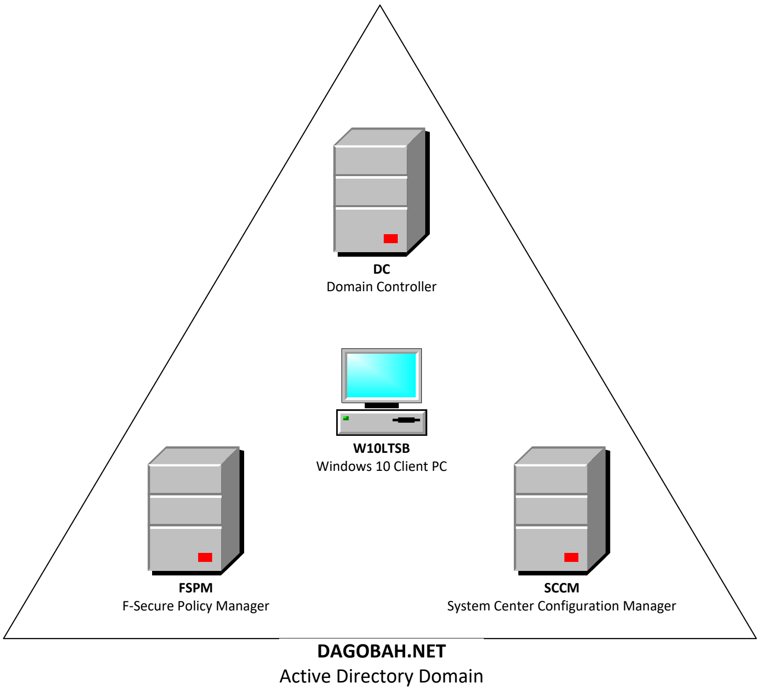


Figure 6. Illustration of the POC environment.

Since the focus was only on the client PC, the servers were not configured with best practices. For example, no additional administrative accounts were configured for the AD or the whole environment. All the configuration focused on the targeted workstation only.

The targeted client PC was installed using the LTSB version 2016 of Windows 10 operating system. LTSB 2016 is based on the 1607 version of Windows 10, so the same configurations and features apply to that as well. The reason for choosing the LTSB version was quite simple:

- It has all the same security features as the Current Branch version of Windows 10 1607 Enterprise has.
- It lacks the Windows Universal Apps that update themselves from the cloud-based Windows Store. These would not work in a disconnected environment.
- It offered a 10 year support-period, keeping the administrative costs at minimum as required by the assigner

Since the POC workstation was going to be used for working on documents, Microsoft Office 2016 was also installed to the machine.

4.3 Approach on configuration of the environment

The decision was made to test technologies behind the security controls one by one and explain the basics of how they worked in practice. The controls implemented in the POC were divided into varies of entities, beginning with configuring the client computer hardware to support the features described earlier.

As the implementation had certain parts that affect each other, the controls were implemented in order that everything would work as expected, thus the additional applications were configured first, before implementing the whitelisting solutions.

Australian Signals Directorate’s top four mitigation strategies were divided into different phases and are addressed in the following chapters.

4.4 Minimizing administrative privileges

One of the ASD's top four mitigation strategies was the minimizing of administrative privileges. As the POC environment consists of Active Directory and workstations for the standard users a decision to follow Microsoft's best practice on a so-called tier-model for administrating the environment was implemented. The tier-model consists of many considerations; however as the purpose for the POC was to protect the end-points, logon restrictions (Figure 7) of the model were implemented. In short, the administrators administer only the things they are allowed to administer with dedicated accounts and dedicated workstations. Since the assigned environment was a small case implementation, the dedicated workstations were left out of the scope on the assignment.

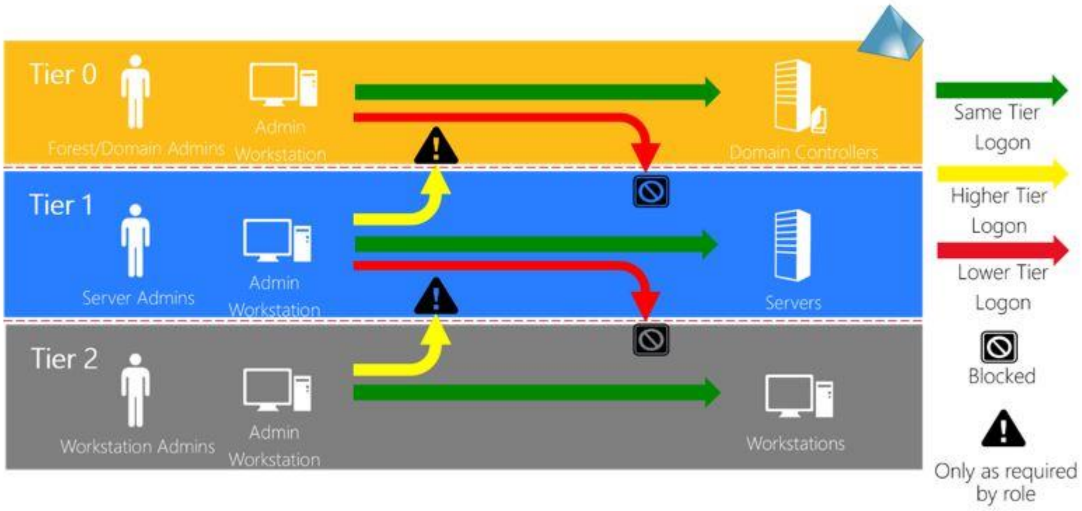
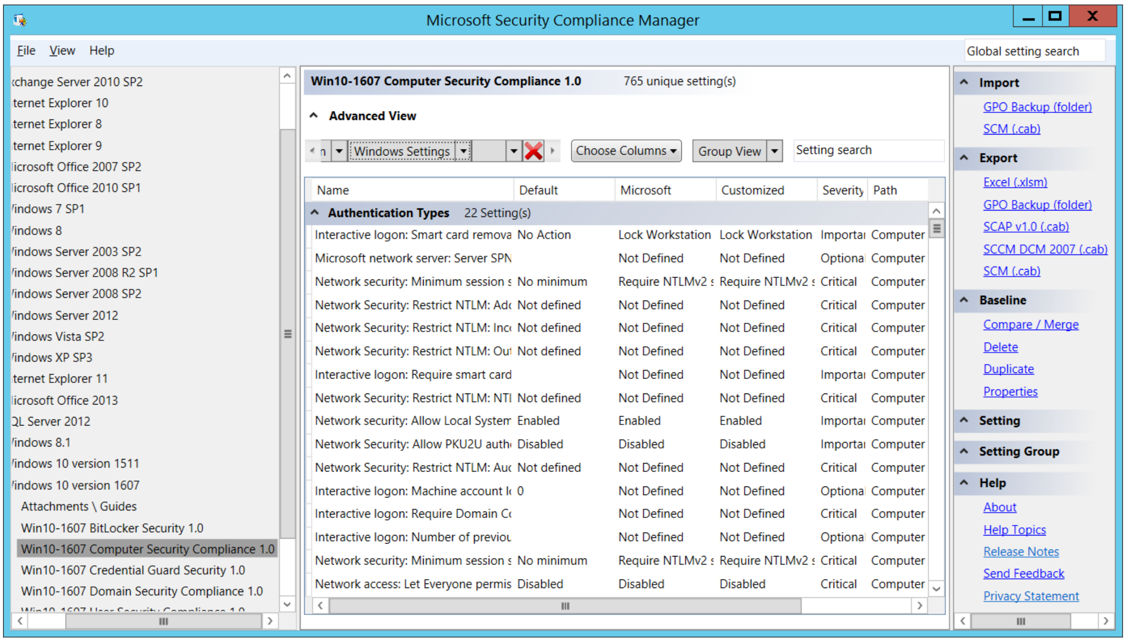


Figure 7. Logon restrictions in 3-tier model. (Plett 2016).

By default, when Windows operating system is joined to an Active Directory domain, Domain Admins group is added to the local Administrators group which then breaks the idea of limiting Domain Admins access on the workstations.

4.4.1 Implementing SCM’s baseline policies

Since group policies can be used to configure Windows operating systems and limit the account’s privileges, a decision was made to configure it accordingly. As Microsoft has their own best-practice security guides, so the decision was made to just follow the company’s guides and configure these well-known policies to the environment. Microsoft Security Compliance Manager provides tested baselines and it also provides functionality to export them to the environment in case (Figure 8).



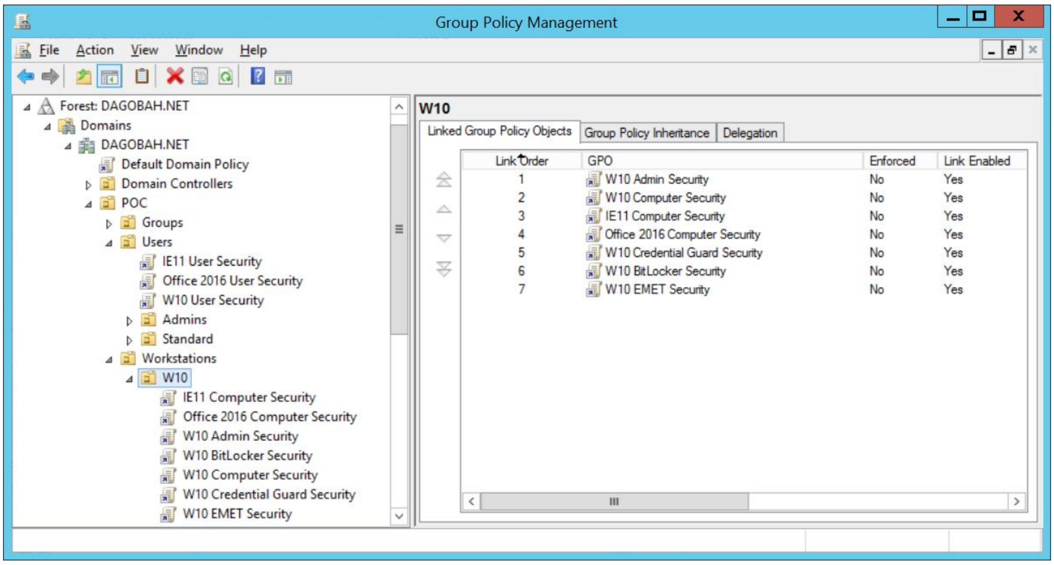
Win10-1607 Computer Security Compliance 1.0 765 unique setting(s)

Name	Default	Microsoft	Customized	Severity	Path
Authentication Types 22 Setting(s)					
Interactive logon: Smart card remova	No Action	Lock Workstation	Lock Workstation	Importa	Computer
Microsoft network server: Server SPN		Not Defined	Not Defined	Optiona	Computer
Network security: Minimum session s	No minimum	Require NTLMv2 s	Require NTLMv2 s	Critical	Computer
Network Security: Restrict NTLM: Ad	Not defined	Not Defined	Not Defined	Critical	Computer
Network Security: Restrict NTLM: Inc	Not defined	Not Defined	Not Defined	Critical	Computer
Network Security: Restrict NTLM: Ou	Not defined	Not Defined	Not Defined	Critical	Computer
Interactive logon: Require smart card		Not Defined	Not Defined	Importa	Computer
Network Security: Restrict NTLM: NTI	Not defined	Not Defined	Not Defined	Critical	Computer
Network security: Allow Local System	Enabled	Enabled	Enabled	Importa	Computer
Network Security: Allow PKU2U auth	Disabled	Disabled	Disabled	Importa	Computer
Network Security: Restrict NTLM: Au	Not defined	Not Defined	Not Defined	Critical	Computer
Interactive logon: Machine account l	0	Not Defined	Not Defined	Optiona	Computer
Interactive logon: Require Domain C		Not Defined	Not Defined	Critical	Computer
Interactive logon: Number of previou		Not Defined	Not Defined	Optiona	Computer
Network security: Minimum session s	No minimum	Require NTLMv2 s	Require NTLMv2 s	Critical	Computer
Network access: Let Everyone permis	Disabled	Disabled	Disabled	Critical	Computer

Figure 8. Microsoft Security Compliance Manager user interface.

The policies offered by SCM are divided into different purposes. Some of these policies are targeted at the operating system and its specific features or components (for example BitLocker and Internet Explorer) as well as to Microsoft Office. At the time of writing, Microsoft did not offer a baseline policy for Office 2016 used in the POC, therefore the policy of 2013 version was used as a baseline for creating a new policy for 2016 version. The policies were exported from the SCM and then imported to the POC environment’s corresponding empty GPOs with Group Policy Management Console.

Since the policies were delivered to the workstation through group policy mechanism of the Windows operating system, designing the organizational unit (OU) structure needed to be made. Workstations and the end-users were placed in dedicated organizational units so that the targeting of the policies would be simplified. As can be seen in Figure 9, policies that are effective on users and computers are targeted at their respective OUs. As there would also be administrator accounts in the environment, the policies targeted at standard users would affect the administrators also.



- Forest: DAGOBAH.NET
  - Domains
    - DAGOBAH.NET
      - Default Domain Policy
      - Domain Controllers
      - POC
        - Groups
        - Users
          - IE11 User Security
          - Office 2016 User Security
          - W10 User Security
          - Admins
          - Standard
        - Workstations
          - W10
            - IE11 Computer Security
            - Office 2016 Computer Security
            - W10 Admin Security
            - W10 BitLocker Security
            - W10 Computer Security
            - W10 Credential Guard Security
            - W10 EMET Security

W10

Link Order	GPO	Enforced	Link Enabled
1	W10 Admin Security	No	Yes
2	W10 Computer Security	No	Yes
3	IE11 Computer Security	No	Yes
4	Office 2016 Computer Security	No	Yes
5	W10 Credential Guard Security	No	Yes
6	W10 BitLocker Security	No	Yes
7	W10 EMET Security	No	Yes

Figure 9. OU structure and baseline policy implementation.

Microsoft’s baselines do not configure logon restrictions that Plett’s (2016) 3-tier model suggests. To overcome this problem in the POC environment, a new Active Directory group called WS Admins was created. This group includes the domain user accounts that would have local Administrator –rights on the target workstations of the environment. Also, another customized computer settings GPO was created (W10 Admin Security) which would add this newly created group to be a member of local Administrators group, as well as deny local access of Domain Admins to the workstations through user rights assignment policies as described by Mathers (2017a).

As SCM’s baseline policies do not interfere with the local administrator privileges, a decision was made to include Microsoft’s recommended limited configuration for local administrators as well (Mathers 2017b). Since User Right Assignment –settings are not cumulative, the customized GPO had to maintain the settings defined in the SCM’s baseline policy as well as the ones affecting the administrative privileges that were to be changed (Appendix 2).

One major usability setting of the SCM's Windows 10 Computer Security policy was the configuration of the built-in User Account Control (UAC) feature. As described by Russinovich & Margosis (2016, 16-17), UAC is a feature introduced in Windows Vista that forces the members of the administrators group to run applications in standard user context and require elevation of privileges to an administrative level when needed. SCM's policy configures the UAC so that standard users cannot elevate their privileges to an administrative level, instead the administrators are forced to log in to a full user session for administrative tasks on the workstation. Because of this, the administration of the POC workstation becomes slightly more complex from the standard Windows configuration where elevation of privileges is allowed.

The process for changing the applied policies should be made so that the changes in the environment were not to be made by a single person but instead all the parties involved in the administration of the workstations. The changes would also have to be tested prior implementing them in to the production environment. This would ensure that all the administrators know what change has occurred and why. One way of accomplishing the administration of the policies targeted at the workstations in the environment would be to delegate permissions for the workstation administrators group.

4.4.2 Mitigation against pass-the-hash attacks using LAPS

LAPS installation consists of two parts: the installation of the LAPS client to the target workstation or server and configuration of the Active Directory. The AD was configured first. LAPS provides PowerShell module that can be used for configuration; this was done on the domain controller with a user account that had schema admin rights on the Active Directory:

```
Import-Module AdmPwd.PS

Update-AdmPwdADSchema
```

This process creates two new attributes for the Active Directory schema:

- *ms-Mcs-AdmPwd* which stores the administrator's password
- *ms-Mcs-AdmPwdExpiratioTime* which stores the time for resetting the password

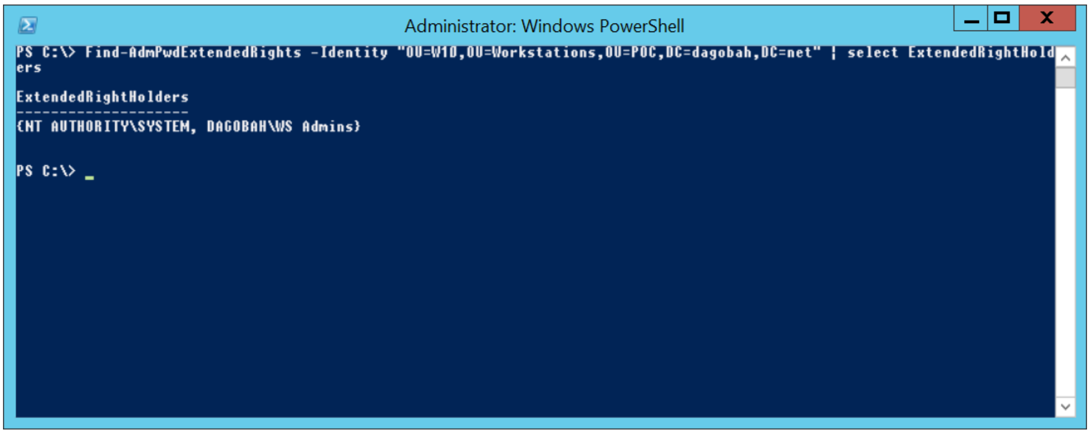
After the schema has been extended, the LAPS configured computer accounts need permissions to write on these two new attributes, so that they can update the information on them. Again, this configuration was done with PowerShell:

Set-AdmPwdComputerSelfPermission –OrgUnit "OU=W10,OU=Workstations,OU=POC,DC=dagobah,DC=net"

For limiting the reading of the newly created attributes to the WS Admins group, another PowerShell command was used:

Set-AdmPwdReadPasswordPermission -OrgUnit "OU=W10,OU=Workstations,OU=POC,DC=dagobah,DC=net"-AllowedPrincipals "WS Admins"

Since the next step was to separate the administrative tasks in the environment so that the people responsible of the workstations (WS Admins) are the only ones who can access the local administrator account's passwords, a decision was made to remove the Domain Admins right for reading the attribute containing it. This was done by removing 'All Extended Rights', permissions for Domain Admins group from the W10 organizational unit with ADSIEdit. To confirm the user rights for reading the password attribute were correctly configured, *Find-AdmPwdExtendedRights* PowerShell command was used (Figure 10).



```
PS C:\> Find-AdmPwdExtendedRights -Identity "OU=W10,OU=Workstations,OU=POC,DC=dagobah,DC=net" | select ExtendedRightHold
ers

ExtendedRightHolders
--------------------
{NT AUTHORITY\SYSTEM, DAGOBAH\WS Admins}

PS C:\> _
```

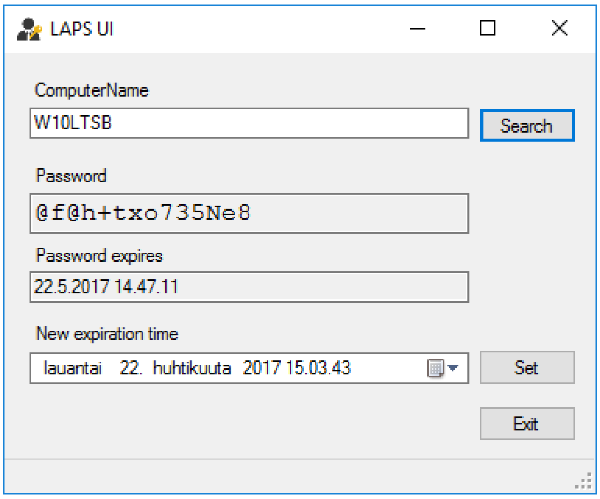
Figure 10. Determine who has rights to read the LAPS attributes.

GPO extensions were used to configure the LAPS. These extensions are added to the client during the installation. Baseline policy for Windows 10 Computer Security provided by Microsoft SCM had LAPS only enabled by default, however the name of the administrator account, password complexity and age requirements needed to be configured additionally.

The complexity and age requirements were configured to be the same as for the standard domain users in the SCM's Windows 10 Default Domain Policy; 14 characters, must meet the complexity requirements and be effective for 60 days.

SCM's baseline policy also disables the built-in Administrator account of the targeted workstation, so a new local administrator account for the workstation needed to be created and that same account was also configured to be the one LAPS is managing. This created a sort-of chicken-egg situation where one needs to have the account to be managed already present in the target workstations as LAPS does not create it automatically on the target computer.

For retrieving the local administrator password, LAPS provides a separate application that can be used to retrieve the password for the targeted machine. When running the application with the user account that is member of the WS Admins group, local administrator password can be retrieved (Figure 12).



ComputerName: W10LTSB

Password: @f@h+txo735Ne8

Password expires: 22.5.2017 14.47.11

New expiration time: lauantai 22. huhtikuuta 2017 15.03.43

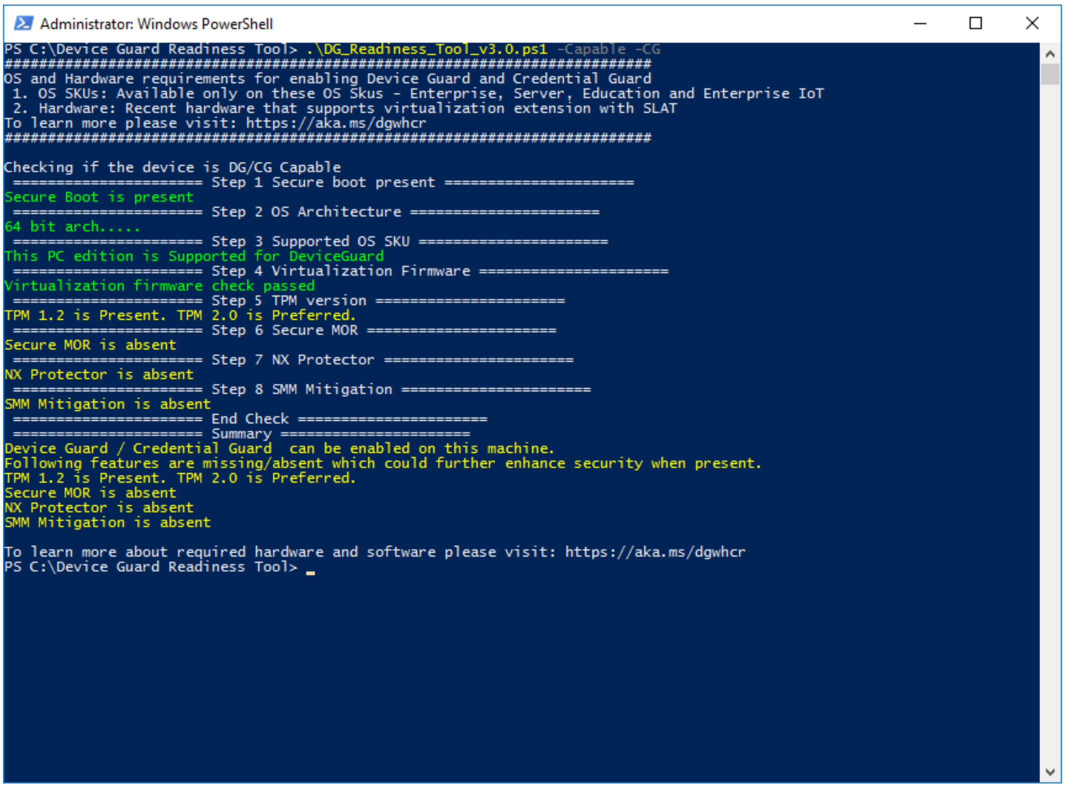
Figure 11. Retrieving the local administrator password with LAPS UI.

Decision on who can have these local administrative rights should be considered very carefully. Users with these privileges pose a significant risk for the overall security of the environment, therefore they should be trustworthy and well trained professionals who know what they are doing.

4.4.3 Securing credentials with Credential Guard

As one of the objectives for the POC was to use new security features introduced in Windows 10, Credential Guard was implemented. Credential Guard protects the Active Directory Domain credentials on Windows 10 end-points, therefore it deals with a different target than the previously introduced LAPS implementation. The POC environment assumes that all users are Active Directory Domain users, therefore implementing additional controls to protect those credentials seemed to be justified.

Credential Guard implementation started with system readiness tool provided by Microsoft Download Center (2017). This tool can be used to determine if the hardware in case is compatible with Windows 10’s Credential or Device Guard features. It can also be used to enable the functionality on a device that is hardware ready. The tool is relatively simple PowerShell script that carries out certain checks against the hardware by running the tool with *–Capable –CG* parameter. The output showed warnings of features that are not supported but it also showed that the hardware in case is indeed capable of running Credential Guard (Figure 13).



```
PS C:\Device Guard Readiness Tool> .\DG_Readiness_Tool_v3.0.ps1 -Capable -CG
###########################################################################
OS and Hardware requirements for enabling Device Guard and Credential Guard
 1. OS SKUs: Available only on these OS Skus - Enterprise, Server, Education and Enterprise IoT
 2. Hardware: Recent hardware that supports virtualization extension with SLAT
To learn more please visit: https://aka.ms/dgwhcr
###########################################################################

Checking if the device is DG/CG Capable
 ====================== Step 1 Secure boot present ======================
Secure Boot is present
 ====================== Step 2 OS Architecture ======================
64 bit arch.....
 ====================== Step 3 Supported OS SKU ======================
This PC edition is Supported for DeviceGuard
 ====================== Step 4 Virtualization Firmware ======================
Virtualization firmware check passed
 ====================== Step 5 TPM version ======================
TPM 1.2 is Present. TPM 2.0 is Preferred.
 ====================== Step 6 Secure MOR ======================
Secure MOR is absent
 ====================== Step 7 NX Protector ======================
NX Protector is absent
 ====================== Step 8 SMM Mitigation ======================
SMM Mitigation is absent
 ====================== End Check ======================
 ====================== Summary ======================
Device Guard / Credential Guard  can be enabled on this machine.
Following features are missing/absent which could further enhance security when present.
TPM 1.2 is Present. TPM 2.0 is Preferred.
Secure MOR is absent
NX Protector is absent
SMM Mitigation is absent

To learn more about required hardware and software please visit: https://aka.ms/dgwhcr
PS C:\Device Guard Readiness Tool> _
```

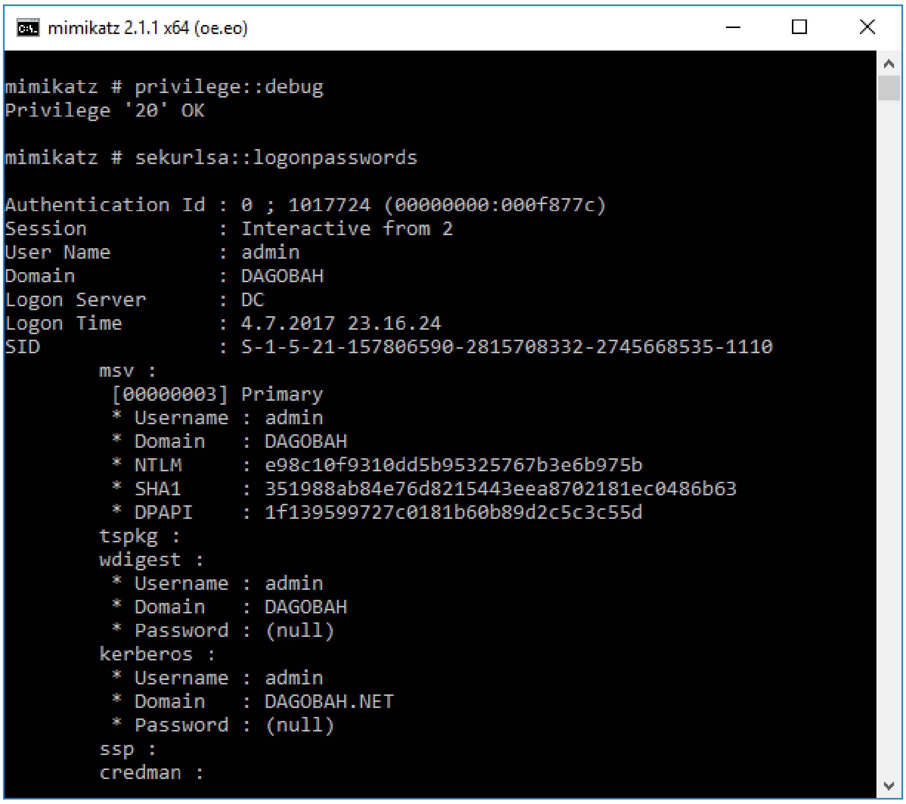
Figure 12. Checking Credential Guard readiness.

For passing the test some modifications had to be made in the BIOS:

- Virtualization technologies had to be enabled
- TPM chip had to be enabled
- Secure Boot had to be enabled
- Full UEFI mode had to be enabled

At this point of the implementation, the settings were configured manually. For actually enabling the Credential Guard, the same tool was used with parameter –*Enable –CG* which would also need a reboot of the machine. The tool adds registry keys that are used to configure Credential Guard and enables Hyper-V virtualization feature of Windows operating system. These same registry keys would be configured in the POC environment with the Credential Guard group policy provided by the SCM.

To see if the Credential Guard was actually working, a check was made with Mimikatz before the implementation of Credential Guard (Figure 13).



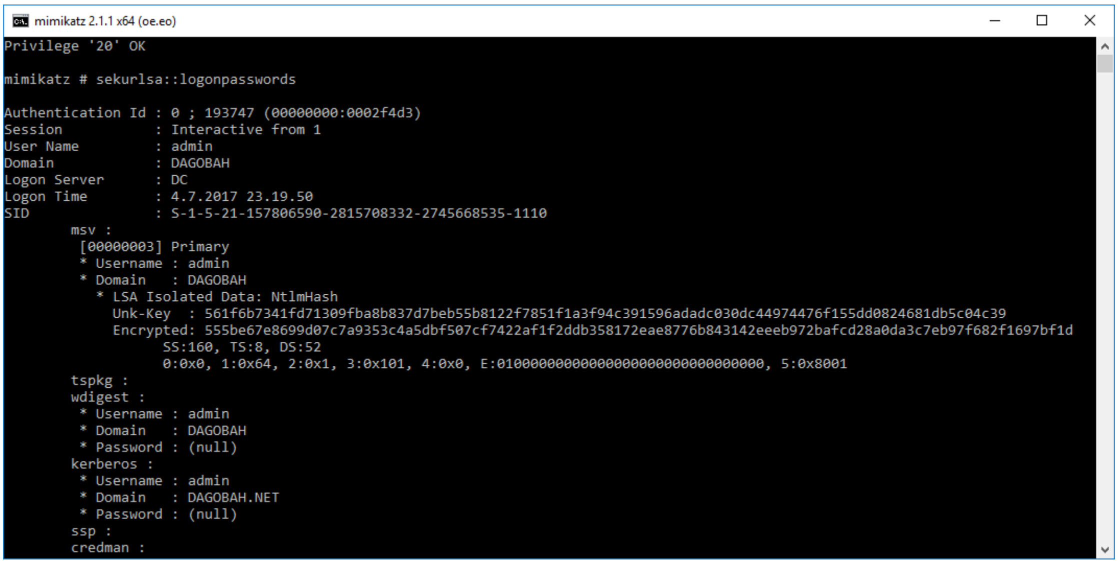
```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 1017724 (00000000:000f877c)
Session           : Interactive from 2
User Name         : admin
Domain            : DAGOBAH
Logon Server      : DC
Logon Time        : 4.7.2017 23.16.24
SID               : S-1-5-21-157806590-2815708332-2745668535-1110
        msv :
         [00000003] Primary
         * Username : admin
         * Domain   : DAGOBAH
         * NTLM     : e98c10f9310dd5b95325767b3e6b975b
         * SHA1     : 351988ab84e76d8215443eea8702181ec0486b63
         * DPAPI    : 1f139599727c0181b60b89d2c5c3c55d
        tspkg :
        wdigest :
         * Username : admin
         * Domain   : DAGOBAH
         * Password : (null)
        kerberos :
         * Username : admin
         * Domain   : DAGOBAH.NET
         * Password : (null)
        ssp :
        credman :
```

Figure 13. Using Mimikatz to retrieve password hash.

As Figure 13 shows, the tool can be used to provide password hash for a domain user account. After the Credential Guard implementation, Mimikatz was used again to see if the hashes were still accessible. Figure 14 shows how Credential Guard works as expected and the hash is not accessible, instead the tool shows that the hash is isolated and cannot be accessed straightly.



```
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 193747 (00000000:0002f4d3)
Session           : Interactive from 1
User Name         : admin
Domain            : DAGOBAH
Logon Server      : DC
Logon Time        : 4.7.2017 23.19.50
SID               : S-1-5-21-157806590-2815708332-2745668535-1110
        msv :
         [00000003] Primary
         * Username : admin
         * Domain   : DAGOBAH
           * LSA Isolated Data: NtlmHash
             Unk-Key  : 561f6b7341fd71309fba8b837d7beb55b8122f7851f1a3f94c391596adadc030dc44974476f155dd0824681db5c04c39
             Encrypted: 555be67e8699d07c7a9353c4a5dbf507cf7422af1f2ddb358172eae8776b843142eeeb972bafcd28a0da3c7eb97f682f1697bf1d
                   SS:160, TS:8, DS:52
                   0:0x0, 1:0x64, 2:0x1, 3:0x101, 4:0x0, E:01000000000000000000000000000000, 5:0x8001
        tspkg :
        wdigest :
         * Username : admin
         * Domain   : DAGOBAH
         * Password : (null)
        kerberos :
         * Username : admin
         * Domain   : DAGOBAH.NET
         * Password : (null)
        ssp :
        credman :
```

Figure 14. Using Mimikatz after Credential Guard implementation.

4.5 Application and operating system patching

ASD’s mitigation strategies included the application and operating system patching. In the POC environment, System Center Configuration Manager would be responsible for delivering both application and operating system updates. SCCM uses Windows Server Update Service (WSUS) feature of the Windows Server operating system to fetch the information about which updates are available and which computers needing them. WSUS also has a mechanism of exporting and importing the update metadata manually from environment to another (Microsoft TechNet Library, N.d.b).

SCCM can also be used to patch the 3rd party applications by crafting an installation package and a command to be executed on the managed clients. This solution provides a centralized management for the application and operating system patching. Reporting capabilities of the product can be used to determine the overall compliance of the managed clients.

4.5.1 Process of delivering Windows updates through air-gap

As a starting point for delivering the updates, a way was needed to first get those updates from the Microsoft servers. This was done by installing a Windows Server machine that was connected to the Internet and had WSUS configured for synchronizing updates of the Microsoft products used in the POC environment. When the updates were downloaded to the WSUS server connected to the Internet, they would be delivered via offline media to the POC environment's SCCM server (Figure 15).

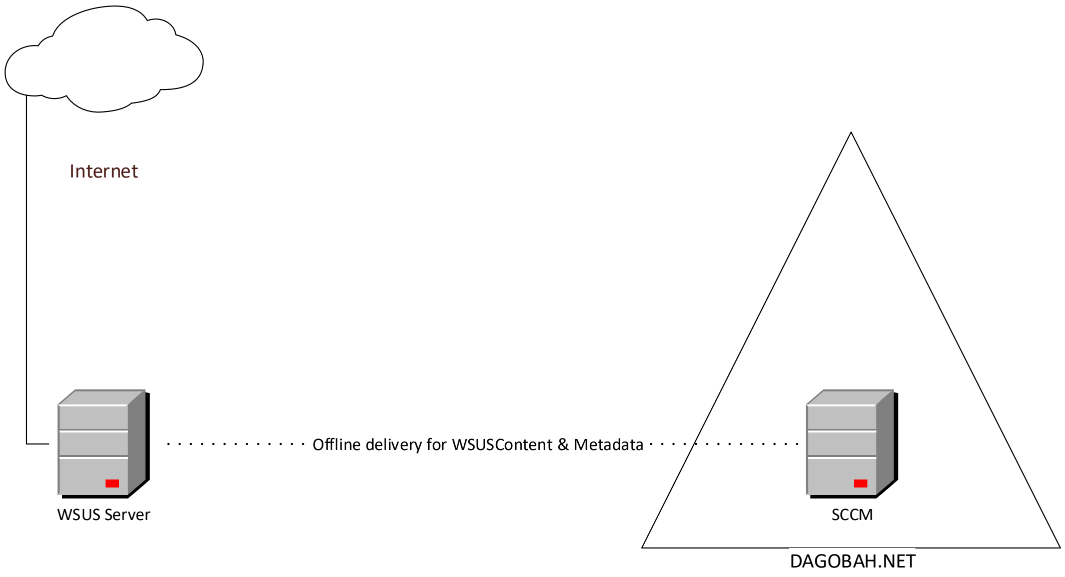


Figure 15. Delivering Microsoft updates to POC environment.

To make sure that the WSUS server connected to the Internet, Windows built-in firewall configuration of the server was modified according to the documentation provided by Microsoft's TechNet documentation (2014). This would ensure that the server was only allowed to access Microsoft's update servers and nothing more. F-Secure's anti-malware solution was also installed on the server and an access to F-Secure servers for virus definition downloads allowed as well.

Microsoft updates delivered through WSUS server feature consist of two components:

- Metadata, the information of the updates

- Content, the actual update files

To accomplish this kind of delivery scenario, the following commands were used on the Internet connected WSUS server to export the metadata:

```
%ProgramFiles%\Windows Update Services\Tools\wsusutil.exe export D:\WSUSContent\export.xml.gz
```

This command will create a dump of the metadata offered by the WSUS server to a file called export.xml.gz. After the metadata export, the exported file and the actual update files were copied to an external USB-media:

```
robocopy D:\WSUSContent E:\WSUSContent /E /B
```

At this point metadata and the update files were on an external media. This media would then be connected to the POC environment and copied to the SCCM server, in its respective *WSUSContent* –folder. For performing the importing and synchronization of the updates to the POC environment, two steps needed to be made:

- Run wsusutil.exe to import the update metadata to WSUS on the SCCM server
- Synchronize the WSUS server component with SCCM

For lowering the administrative effort, these steps could easily be automated with for example using scripts and scheduled tasks in both servers, the Internet connected WSUS and the disconnected SCCM server.

4.5.2 Deploying software updates

Microsoft has traditionally been releasing security updates for its products on the 2nd Tuesday of every month, although after the release of Windows 10, this cycle has not always been as accurate as it has been. As the Windows 10 updates include both security and feature updates, there also have been some problems of the patches breaking functionalities of the operating system.

The testing of the operating system updates can be a tricky thing to do, therefore a decision was made to build a solution where:

- Update delivery to the environment is delayed. This approach gives Microsoft some time to fix or pull back the problematic updates.
- Updates are firstly deployed to administrative computers. This would ensure they are working correctly before deploying them to the end-user workstations.

A timeline was created to visualize how the update delivery and deployment process would work in the environment on monthly basis (Figure 16).

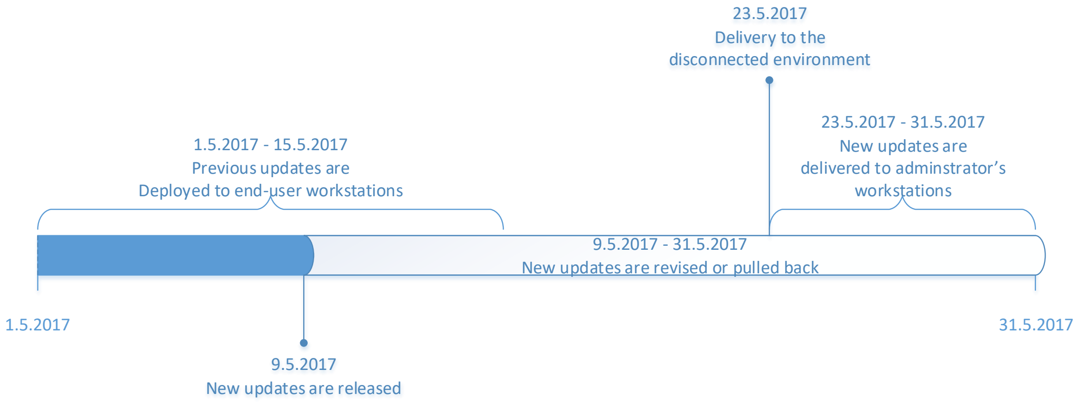


Figure 16. Update delivery timeline.

After the new update release date administrators responsible for the software update process would have to review the updates carefully before delivering them to the environment. The deadline for the delivery would be one week before the end of the month, so that the updates could be tested in the environment for one full week before deploying them to the end users. For reviewing the updates, official Microsoft documentation would be a starting point for checking any known issues.

Additionally, other channels such as Twitter should be followed for any inconsistences with the monthly updates.

To automate this kind of scenario, configuration of the update synchronization and automatic deployment rule (ADR) targeted at the administrative workstations would be created. SCCM's synchronization of the updates was configured to take place on the 23rd of every month. The configuration assumed that the updates were already synchronized with the WSUS service and that the actual update files were already copied to the environment, so a scheduled task for WSUS offline import for the metadata was made to occur before this. All the workstations (end-user and administrative) would have a maintenance window configured to them through SCCM. This window would be on every 15th of every month between 00:00 – 06:00, which would give the workstations 6 hours of time to install the updates they are required to install.

The updates would be configured to be required for the administrative workstations on every 24th day with a deadline that would be on the 15th day of the next month at 00:00. This configuration would give the administrators roughly three weeks of time to install the updates for their workstations before they would be installed forcefully. During the first week, administrators install the updates for themselves, test them and remove problematic updates from the configuration if needed. On the 1st day of each month, additional deployment would be made targeted at the end-user workstations with the same deadline of 15th at 00:00; the same time as the maintenance window would occur. Communication with the end-users should be done properly, so that they would understand the whole process of automatic software update delivery and how they can control the installation of the updates by themselves without interrupting their work.

If there were a case of delivering an update outside of the automated configuration, the administrator could always download the update in case and use the package / program functionality of SCCM to deliver this update to the end-points as soon as possible. An example for this kind of scenario would be the case of a 0-day vulnerability. This process would include the downloading of the update from the

Internet, delivering it to the POC environment, crafting an installation command and creating the actual deployment package. The same technique would also work the other way around. If there were a problematic update, it would be first removed from the automatic deployment rule and then a crafted uninstallation command of the update would be deployed against the affected clients.

4.5.3 Monitoring the update compliance

SCCM offers built-in reports to monitor the compliance state of the software updates in the managed environment. Monitoring the compliance state gives administrators a good view on which of the environment's workstations are still requiring updates to be installed. Monitoring the state should be a monthly process for the organization so that actions could be taken if the state was to change from the targeted result.

4.6 Additional controls

The top four mitigation strategies of the ASD do not include data protection, system logging and multi-factor authentication that Windows 10 operating system provides as built-in features, however, the POC environment was configured to use these as well.

4.6.1 Facing the privacy concerns of Windows 10

As noted before, Windows 10 has the built-in features that are used for data collecting by Microsoft. Additional configuration of the operating system was made to restrict this kind of behavior. This was accomplished by implementing the *Windows Restricted Traffic Limited Functionality Baseline* (Lich 2017c), which is a set of group policy and additional configurations such as removing the built-in modern applications of the operating system. Group policy settings offered by Microsoft were adjusted to the baseline security policy that was already implemented. As the LTSB version of the Windows 10 does not include the same built-in applications as other versions, there was no need for removing those. Restricted traffic baseline configures the operating system to minimize the unwanted traffic made by the operating system.

4.6.2 Data protection, BitLocker and Windows Information Protection

BitLocker was implemented with the simplest configuration on the POC workstation: use only TPM protection. This was because of the different bypass mechanisms as described by Laiho (Appendix 4) were implemented. To protect against DMA – attacks, hardware device classes were blocked with F-Secure Client security as will be described later. Also, a registry setting Laiho (2017) provides in his blog post was used to protect Windows 10 (version 1607 which the LTSB 2016 is based on) against these attacks when the computer is in logon screen:

- *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\PnP\Pci*
    - *DisableExternalDMAUnderLock (DWORD) = 1*

Besides these configurations, the SCM's default BitLocker policy was changed from the default that it uses the newest XTS-AES 256 algorithm for encrypting the removable drives also. This would mean that the encrypted removable device is usable only on Windows 10 operating systems because the encryption algorithm is not supported in the earlier versions of Windows. Secure Boot was also enabled on the POC workstation, as it already was the case while implementing Credential Guard earlier. SCM's default configuration for BitLocker (Win10-1607 BitLocker Security) enables Secure Boot integrity validation, which means that the operating system only loads firmware that is trusted. Policy also configures removable devices so, that it disables write-access to them, if they are not encrypted. This would ensure that the data going out of the POC environment is always encrypted.

Windows Information Protection feature was tested briefly, however quickly turned out that the technology is not really usable in a small-sized disconnected environment. Another point was that if it was truly meant to be used, a public key infrastructure (PKI) would had to be in place, which was not the case within the targeted environment. The feature can be deployed through SCCM, however, at the time of the writing, support for Microsoft Office 2016 products was missing.

4.6.3 Implementation of biometric authentication

Windows 10’s built-in feature of Windows Hello offers the opportunity to use biometric authentication as a part of POC. The only drawback comes from the centralized management point of view. Technically the biometric data is stored on each individual device and thus it is not replicated between Active Directory servers. This leads to manual process of the administrators to handle while they give away the computer to end-users:

- Administrator delivers a computer to the end-user
- User’s fingerprint is scanned and attached to the Active Directory account on the delivered computer

Bio-key’s (N.n.) EcoID fingerprint reader was used in the POC environment to test this kind of scenario as the device offers full support for Windows Hello. The first problem was that the policy (Win10-1607 Computer Security) offered by SCM breaks the functionality of Windows Hello. To fix this problem, the *Turn on convenience PIN sign-in* setting had to be enabled and the following registry entry had to be made

- *HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System*
    - *AllowDomainPINLogon (DWORD) = 1*

This allowed the PIN logons in Active Directory domain environment and therefore would allow the usage of fingerprint authentication on the POC workstation.

As the PIN authentication had to be enabled for the device before biometrics could be used, this would pose a risk of end-users having simple PINs for authentication purposes on their devices. On the other-hand, the PIN is specific only for the device in case. Knowing this, a decision was made that the end-users shall not know the PIN they are using, instead, administrators would use a randomized number every time they enroll a new user with fingerprint authentication. This would ensure that PIN is not used in the environment as no one knows what it is. If the biometric authentication does not work, users can always fallback to traditional username / password pair which would have additional complexity and age controls as defined in the SCM’s policy.

The fingerprint reader was tested with one finger acting as the administrative user and another finger as a standard user.

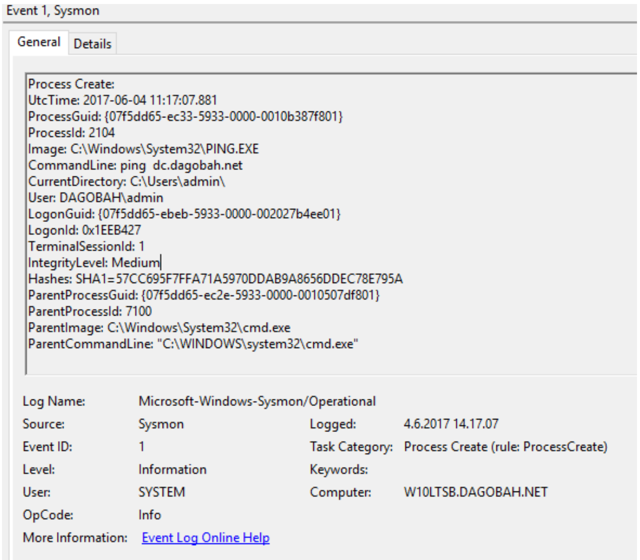
4.6.4 Logging and Sysmon implementation

As described by Kim & Solomon (2014, 246), log files are useful for providing evidence about abnormal and normal activities on systems. The Australian Cyber Security Centre (2017) offers a hardening guide for Windows 10 version 1703 which was used as a basis for creating the audit policies implemented against the workstation. Security Compliance Manager's baseline policy for 1607 version of Windows 10 had some of the same settings already configured so only fine-tuning of the settings was made to the baseline policy according to the guide.

Besides implementing the built-in auditing features of the operating system, Sysmon configuration was done as well. The implementation began with simply installing the Sysmon service to the target workstation with a simple installation command:

sysmon64.exe -i -h SHA1 -n

This would install (-*i*) the Sysmon service configured to log SHA1 *(-h*) hash of created processes and log network (-*n*) activity as well. To confirm that the Sysmon logging was working as expected, a check in *Microsoft-Windows-Sysmon/Operational* log was made (Figure 17).



```
Process Create:
UtcTime: 2017-06-04 11:17:07.881
ProcessGuid: {07f5dd65-ec33-5933-0000-0010b387f801}
ProcessId: 2104
Image: C:\Windows\System32\PING.EXE
CommandLine: ping  dc.dagobah.net
CurrentDirectory: C:\Users\admin\
User: DAGOBAH\admin
LogonGuid: {07f5dd65-ebeb-5933-0000-002027b4ee01}
LogonId: 0x1EEB427
TerminalSessionId: 1
IntegrityLevel: Medium
Hashes: SHA1=57CC695F7FFA71A5970DDAB9A8656DDEC78E795A
ParentProcessGuid: {07f5dd65-ec2e-5933-0000-0010507df801}
ParentProcessId: 7100
ParentImage: C:\Windows\System32\cmd.exe
ParentCommandLine: "C:\WINDOWS\system32\cmd.exe"

Log Name:          Microsoft-Windows-Sysmon/Operational
Source:            Sysmon                      Logged:         4.6.2017 14.17.07
Event ID:          1                           Task Category:  Process Create (rule: ProcessCreate)
Level:             Information                 Keywords:
User:              SYSTEM                      Computer:       W10LTSB.DAGOBAH.NET
OpCode:            Info
More Information:  Event Log Online Help
```

Figure 17. Eventlog entry by Sysmon.

4.7 Application whitelisting and malware defense

Last of the mitigation strategies introduced by the ASD was the application whitelisting. As this environment is disconnected from the Internet, it does not have the modern cloud-based detection functionalities provided by the either Microsoft or the 3rd party anti-malware software company’s products do use straightly from the cloud. From this perspective, additional controls are indeed needed to ensure that the environment is safe. As noted by Niemelä (2013), preventing execution of applications in certain paths of Windows operating system is an effective method to disable malware from functioning; this was taken in to the consideration while implementing the controls to the POC environment.

4.7.1 F-Secure Client Security and Policy Manager

One of the requirements set by the assigner was to use F-Secure products for malware protection in the POC. The F-Secure Policy Manager server was installed in the environment as well as the Client Security (version 12.31) for the Windows 10 end-point. The main concern was how and when the antimalware definitions would be delivered into the environment. Since there is no Internet connection available, updating virus definitions produces an administrative task that had to be dealt with. As antimalware definitions are changed on a daily basis, the process for delivering the updates to the environment would have to be a daily process for administrators.

F-Secure offers offline update (F-Secure, N.d.) to be used with Policy Manager which then again distributes the definitions for all the managed client systems (Figure 18).

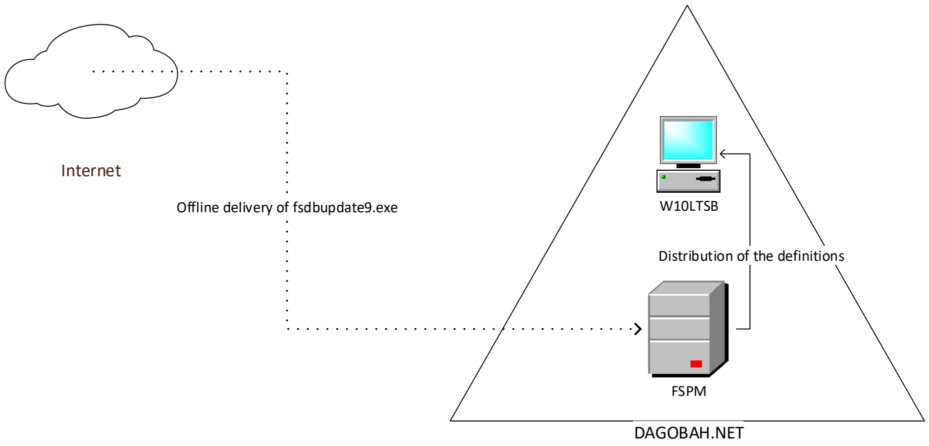

Internet
Offline delivery of fsdbupdate9.exe
W10LTSB
Distribution of the definitions
FSPM
DAGOBAH.NET

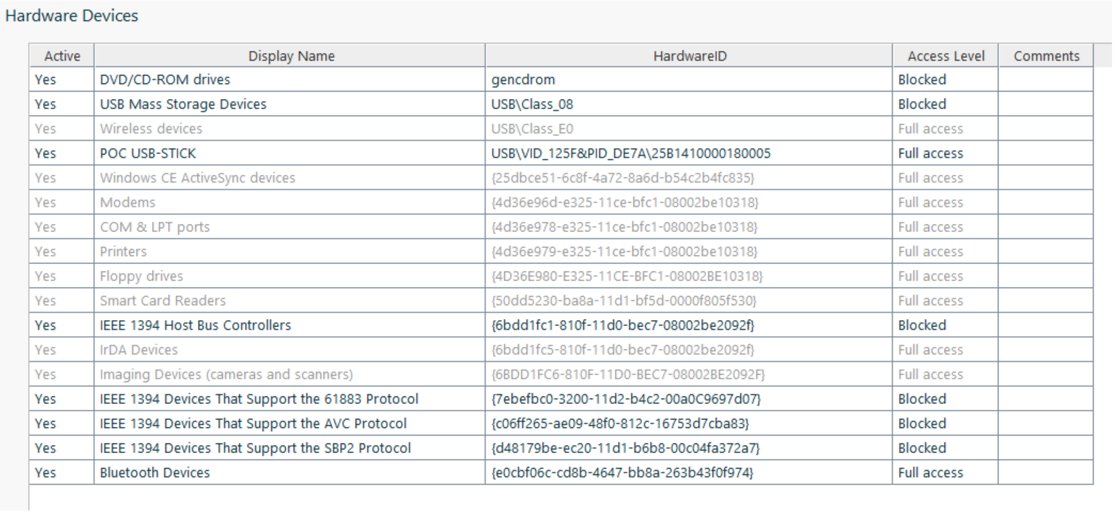
Figure 18. F-Secure definition delivery for the end-point.

F-Secure also provides a separate *.txt* file which includes the Message Digest 5 (MD5) and Secure Hash Algorithm 1 (SHA1) hashes for the current fsdbupdate9.exe file as well as information about the definitions themselves. For additional security measures a decision was made to craft a PowerShell script which would deal with the downloading of the update definition file and check that it is not tampered with by comparing the file hash to the one F-Secure provides (Appendix 4). This script could also be used for automating the process of downloading the antimalware definitions when configured as a scheduled task on the WSUS server that also handles the Microsoft update downloads for the POC environment.

After the definition file is delivered to the FSPM server in the POC environment, it needs to be run. This configuration was made with a simple Windows Scheduled Task that would run the fsdbupdate9.exe from a specific folder on the server. An administrator's daily tasks would include the delivery of the definition file to this location. The Client Security settings were configured by locking the settings so that end-users could not for example change any of the settings made by the administrator.

Another feature that F-Secure Client Security offered for the environment would be the usage of Device Control feature. With the feature, administrators can define which devices are allowed on the client. Using this technology, a decision was made to block devices that are known to be used in DMA attacks against BitLocker as Laiho (2017a) describes. Laiho's blog post (2017a) has a list of device classes related to IEEE 1394.

As one of the requirements by the assigner was to figure out how to restrict the data transfers from and to the POC environment, a decision was made to configure Device Control for this purpose. For the POC, one USB stick was allowed to work on the workstation. To further configure on how data might go in or out of the environment, a decision was made to block CD/DVD devices also (Figure 19).



Hardware Devices

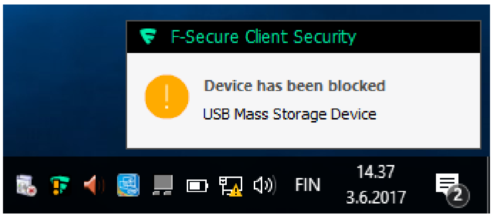
Active	Display Name	HardwareID	Access Level	Comments
Yes	DVD/CD-ROM drives	gencdrom	Blocked	
Yes	USB Mass Storage Devices	USB\Class_08	Blocked	
Yes	Wireless devices	USB\Class_E0	Full access	
Yes	POC USB-STICK	USB\VID_125F&PID_DE7A\25B1410000180005	Full access	
Yes	Windows CE ActiveSync devices	{25dbce51-6c8f-4a72-8a6d-b54c2b4fc835}	Full access	
Yes	Modems	{4d36e96d-e325-11ce-bfc1-08002be10318}	Full access	
Yes	COM & LPT ports	{4d36e978-e325-11ce-bfc1-08002be10318}	Full access	
Yes	Printers	{4d36e979-e325-11ce-bfc1-08002be10318}	Full access	
Yes	Floppy drives	{4D36E980-E325-11CE-BFC1-08002BE10318}	Full access	
Yes	Smart Card Readers	{50dd5230-ba8a-11d1-bf5d-0000f805f530}	Full access	
Yes	IEEE 1394 Host Bus Controllers	{6bdd1fc1-810f-11d0-bec7-08002be2092f}	Blocked	
Yes	IrDA Devices	{6bdd1fc5-810f-11d0-bec7-08002be2092f}	Full access	
Yes	Imaging Devices (cameras and scanners)	{6BDD1FC6-810F-11D0-BEC7-08002BE2092F}	Full access	
Yes	IEEE 1394 Devices That Support the 61883 Protocol	{7ebefbc0-3200-11d2-b4c2-00a0C9697d07}	Blocked	
Yes	IEEE 1394 Devices That Support the AVC Protocol	{c06ff265-ae09-48f0-812c-16753d7cba83}	Blocked	
Yes	IEEE 1394 Devices That Support the SBP2 Protocol	{d48179be-ec20-11d1-b6b8-00c04fa372a7}	Blocked	
Yes	Bluetooth Devices	{e0cbf06c-cd8b-4647-bb8a-263b43f0f974}	Full access	

Figure 19. Configuration of FSCS Device Control.

As the SCM's default BitLocker configuration requires the external media devices to be encrypted before any data can be written to them, this would also affect on how the data is transferred out of the environment. The end result of data delivery out of the POC workstation requires as follows:

- A predefined USB mass storage device
- That the written data to external media is encrypted with BitLocker

The Device Control policy was tested by inserting a not defined USB stick to the POC workstation which FSCS blocked as can be seen in Figure 20.



F-Secure Client Security

Device has been blocked

USB Mass Storage Device

Figure 20. F-Secure Client Security's Device Control functionality.

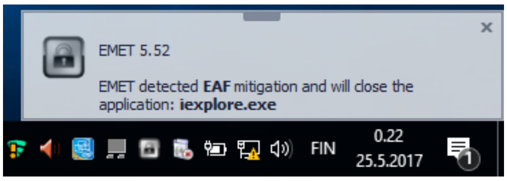
Since only predefined external mass storage devices are allowed, the organization can control to whom these devices are given. Prior to giving the USB sticks to end-users, they should be properly trained on how to use the devices and how to report if they're lost or otherwise compromised.

4.7.2 Implementation of Enhanced Mitigation Experience Toolkit

For lowering the risk that something can bypass the mitigations described earlier, EMET (version 5.52) was implemented on the POC workstation. The configuration was performed with a recommended policy that comes with the product itself; this configuration was loaded to the operating system during the testing phase.

The recommended configuration applies protection to a defined list of commonly used applications, including Microsoft Office and Internet Explorer, which were a part of standard configuration of the POC workstation.

For testing EMET's mitigations, SurfRight's (2015) HitmanPro.Alert Exploit Test Tool was used. The tool is capable of demonstrating different exploit techniques. Although it was developed for testing SurfRight's another product, it can be used for testing other products as well. EMET was tested so that the SurfRight's tool was used to inject malicious code into *iexplore.exe* which was part of the EMET configuration. As can be seen in Figure 21, EMET worked as expected and crashed the Internet Explorer process.



EMET 5.52

EMET detected **EAF** mitigation and will close the application: **iexplore.exe**

Figure 21. EMET blocking malicious activity.

4.7.3 Configuring Device Guard

Since AppLocker policies are only enforced in the user-mode of the Windows operating system, Device Guard was used to enforce the overall mindset of trusting only the things known to be trusted, thus even the administrator of the system cannot bypass those settings. The process of deploying a working Device Guard policy is illustrated in Figure 22.

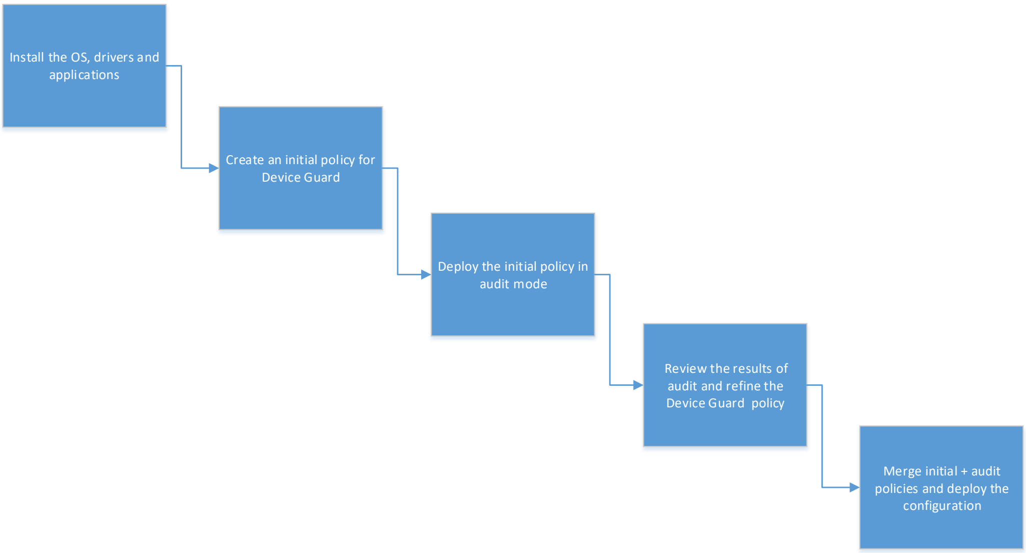

Install the OS, drivers and applications
Create an initial policy for Device Guard
Deploy the initial policy in audit mode
Review the results of audit and refine the Device Guard policy
Merge initial + audit policies and deploy the configuration

Figure 22. Process of creating Device Guard policy.

To prepare the POC workstation for Device Guard, the same tool that was used earlier for Credential Guard was also used here. Both technologies also require the same virtualization technologies to be enabled on the hardware prior to the implementation.

For the initial configuration a decision was made to use *PCACertificate* file rule level and to include user mode executables in the policy. Lich (2017b) defines the PCACertificate level: “*Adds the highest available certificate in the provided certificate chain to signers. This is typically one certificate below the root certificate, because the scan does not validate anything beyond the certificates included in the provided signature (it does not go online or check local root stores)*”. This would ensure that the trusted code signers on the machine at the time of the initial scan would be trusted and therefore allowed to run it.

This initial policy was created the following PowerShell command:

```
New-CIPolicy –Level PcaCertificate –Filepath C:\DG\InitialPolicy.xml –UserPEs –Fallback Hash
```

The command would create a policy based on PCACertificates and if they were not available, filehashes would have been used as a fallback. After about an hour of scanning, the *InitialPolicy.xml* –file which was gained which would then be refined with the following PowerShell commands:

```
Set-RuleOption –Filepath C:\DG\InitialPolicy.xml –Option 0
```

The option forces to include the User-Mode Code Integrity (UMCI) to the Device Guard policy, as the default option would only be Kernel-Mode Code Integrity (KMCI). The .xml –file needed to be converted to a binary format and copied to CodeIntegrity directory, again with PowerShell:

```
ConvertFrom-CIPolicy –XmlFilePath C:\DG\InitialPolicy.xml –BinaryFilePath C:\DG\InitialPolicy.bin
```

```
Copy-Item –Path C:\DG\InitialPolicy.bin –Destination C:\Windows\System32\CodeIntegrity\SIPolicy.p7b
```

Prior to this, a separate GPO for configuring Device Guard was created that configures the path to the policy file. Virtualization Based Security (VBS) was already configured through Credential Guard's group policy object which would also affect Device Guard implementation.

After a reboot, the POC workstation would start logging to *Microsoft-Windows-CodeIntegrity/Operational* –eventlog about how Device Guard would have acted, if the initial policy had been in enforced mode. At this point several tests were made to see, how Device Guard would act:

- Install software updates through SCCM according to the process described earlier
- Open and use applications such as Office, FSCS, EMET etc. to include the Dynamic Link Libraries (DLL) that they might require to function properly

The first issue spotted in the CodeIntegrity –log was the information about how the policy would have blocked couple of drivers loaded by F-Secure Client Security during the startup of the operating system, if the policy was configured to require Windows Hardware Quality Labs (WHQL) approved kernel mode drivers. According to the Device Guard documentation, the WHQL approved drivers are going to be mandatory in the future versions of Windows 10. F-Secure Corporation was informed about these findings.

Another notice made was that some processes were also loading unsigned .DLL –files residing in *%windir%\assembly* –folder. Those files were most certainly a native part of the operating system itself.

During the test of installing software updates through SCCM, it turned out that, the standard cumulative updates for Windows 10 operating system would've got installed just fine, however, Office 2016 updates were not. A further inspection of this indicated that the Office updates are delivered in Microsoft Installer Patch (MSP) –format and they are unsigned. Windows Installer creates temporary files during the installation of these patches and these are removed after the installation, thus they were not present when the policy file of the audit was created.

After the audit phase, the policy was created based on it:

```
New-CIPolicy –Audit –Level PCACertificate –FallBack Hash –FilePath C:\DG\AuditPolicy.xml
```

For merging the initial policy with the audit policy, another PowerShell command was used:

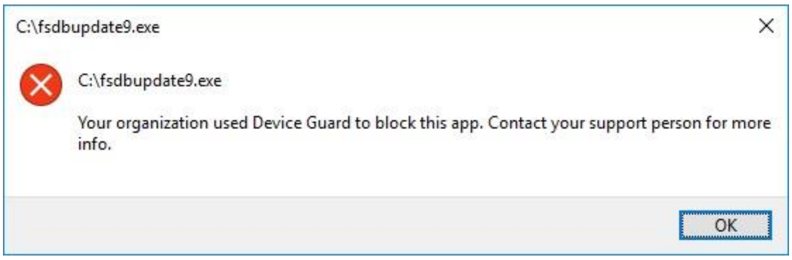
```
Merge-CIPolicy –PolicyPaths C:\DG\InitialPolicy.xml,C:\DG\AuditPolicy.xml –OutputFilePath C:\DG\Merged.xml
```

To get the policy into enforced mode after merging, the audit rule was removed from the merged xml-file:

```
Set-RuleOption –FilePath C:\DG\Merged.xml –Option 3 –Delete
```

After this the final policy for Device Guard was ready to be converted to the binary format and copied to the configured path as described earlier. Before copying the file in place, the computer was re-installed to the state where there were no updates installed at all, only the operating system and the applications that were also installed during the initial policy scan.

To test the enforced policy, a test was made to manually update F-Secure Client Security’s anti-malware definitions by running fsdbupdate9.exe. Because this executable was not part of the policies, it was blocked as can be seen in Figure 23. Since the offline definition file is not signed at all and its hash changes daily, it would not be allowed to run with Device Guard at all. F-Secure was informed about this finding as well.



C:\fsdbupdate9.exe

C:\fsdbupdate9.exe

Your organization used Device Guard to block this app. Contact your support person for more info.

Figure 23. Device Guard blocking fsdbupdate9.exe

As already noticed in the audit phase of the implementation, Office updates would have problems with our Device Guard policy. When the policy was enforced, Microsoft Office updates would not get installed, since the installation files it was using were not part of the policy; neither signed nor they were available during the calculation of the hash that could have been added to the policy. Device Guard documentation does provide a guide on how to sign unsigned binaries so that they would work with the technology, however, this could not be used with the Office updates as they are delivered through SCCM's built-in functionalities. The guide could be used against other 3rd party software, however, an additional infrastructure (PKI) would be needed.

Device Guard implementation was dropped at this point of the POC as it introduced a breakage of software updates that was considered more important, knowing that another whitelisting solution would be implemented anyway. Another reason for dropping was that the implementation of Device Guard would have a massive impact on administering the environment. If there were several new application installations, different hardware used etc., every change in either software or hardware would add additional administrative work to get it all working without breaking anything.

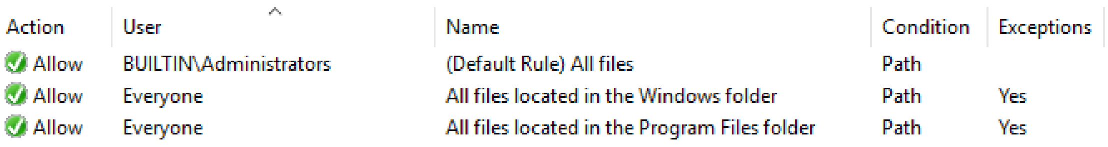
4.7.4 Using AppLocker as a perimiter

If the Device Guard code-integrity policy had been enforced, still there would be a need for further filtering of what and from which paths are the end-users allowed to run executables on the workstation. Device Guard permits the usage of digitally signed trusted executables, but what if they are not wanted to be run by end-users? Device Guard does not address the location of the file running, thus everything signed and trusted is allowed to run everywhere and by anyone.

Since the Device Guard implementation was based on 'run-only-what-you-know-you-trust' basis, the approach on the AppLocker was slightly different from the administrative point of view. The aim was to lower the administrative effort when there are changes in the client computer. Instead of doing a full whitelisting solution as with Device Guard, a more flexible configuration was implemented instead.

For limiting running of not trusted executables on Windows operating system, the first point is to figure out where the standard users have write access on the system. Microsoft's freeware tool which is part of Sysinternals Suite, AccessChk (Microsoft TechNet, Windows SysInternals, 2017) can be used to list what permissions Windows groups have in different places of the operating system, for example the file system. Simply running *accesschk.exe –w –d –s Users C:\* provides a list for directories to which the operating systems built-in Users group have write access (Appendix 5) on the C: drive of the targeted computer. The command was run after all the applications, and other components were installed into the system, because some applications might alter the default access rights defined in the operating system. This was also the case in the POC as F-Secure Client Security modifies certain access control lists (ACL) to grant write-access for standard users group under paths that are by default denied, for example, *%ProgramFiles(x86)%*. This behavior would break the default AppLocker rules which explicitly allow standard users to run everything from *%WinDir%* and *%ProgramFiles%* / *%ProgramFiles(x86)%* paths. This flaw was reported to F-Secure Corporation in May 2017 and it was fixed in the later versions of the product.

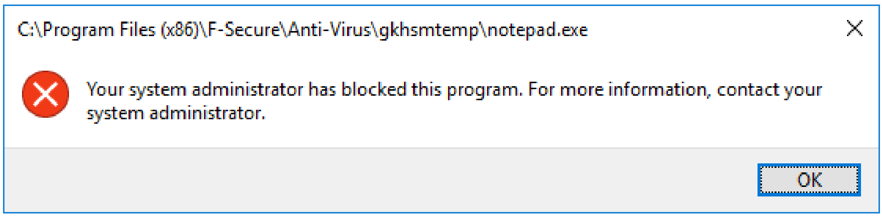
For configuring the AppLocker, the default rules were generated for executables, windows installers and scripts. Although AppLocker does provide the ability to configure rules for DLL –files as well, Microsoft does not recommend using those so they were left out of the implementation. After the default rules were generated, the file list generated by the AccessChk utility was used to configure exceptions for all the default rules that allow Windows local group *Everyone* group to execute anything from either *%ProgramFiles%* or *%WinDir%* paths. (Figure 24). This configuration would ensure that standard Users are not allowed to run any executables, MSI packages or scripts from the locations they have write access to.



Action	User	Name	Condition	Exceptions
✓ Allow	BUILTIN\Administrators	(Default Rule) All files	Path	
✓ Allow	Everyone	All files located in the Windows folder	Path	Yes
✓ Allow	Everyone	All files located in the Program Files folder	Path	Yes

Figure 24. Default rules for AppLocker with exceptions.

For testing the configuration, notepad.exe from the *%WinDir%* -directory was copied to the location F-Secure Client Security's installation folder under *%ProgramFiles%* which had the user write access granted. Trying to run the executable from there was blocked with the following policy as can be seen in Figure 25.



C:\Program Files (x86)\F-Secure\Anti-Virus\gkhsmtemp\notepad.exe

Your system administrator has blocked this program. For more information, contact your system administrator.

Figure 25. AppLocker blocking excluded path.

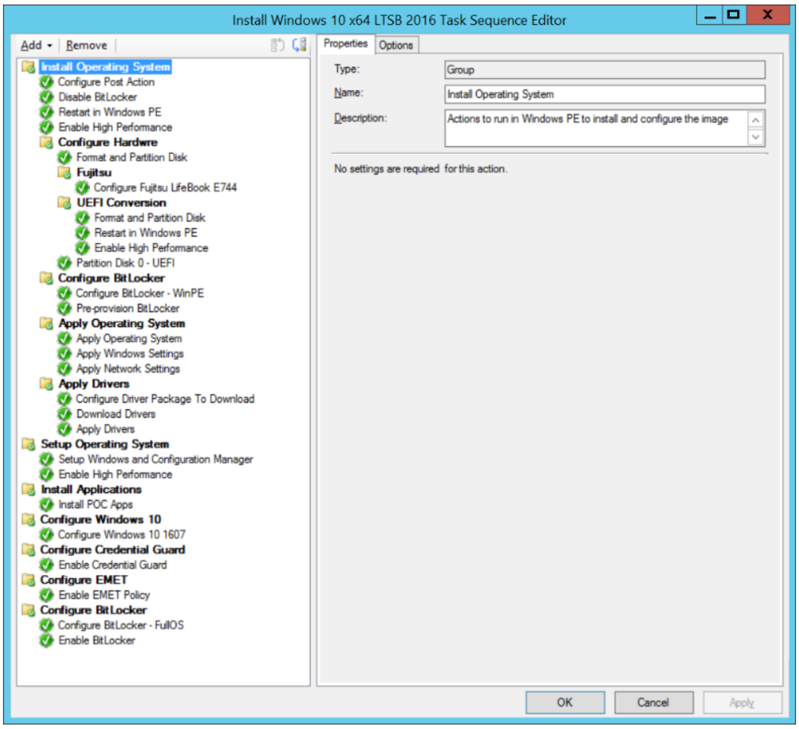
Configuration without packaged app rules broke the Windows 10 built-in functionality for opening Start Menu, Settings app, etc. so an addition was made to the configuration by allowing the running of only Microsoft signed .appx –formatted applications (Packaged app Rules).

AppLocker configuration implemented gives administrative flexibility, for example when new applications are installed, they are allowed to run by default. However, every application installation should be reviewed thoroughly, if they alter the default ACLs of the file path rules defined in the policy.

4.8 Automating the implementation with SCCM

The assigner had been using SCCM as their centralized management solution for the Windows environment and therefore it was also chosen as the management product in this assignment. SCCM provides ways to deliver operating systems, applications and patches to Windows end-points.

The whole process of building the Windows 10 workstation began with implementing an operating system deployment solution with SCCM's task sequence functionality. The task sequence automates the process of creating the POC workstation with the operating system installed with all controls that were introduced earlier implemented (Figure 26). During the course of the implementation, the sequence was modified to include every step needed for automating the installation of the POC workstation.



- **Install Operating System**
  - Configure Post Action
  - Disable BitLocker
  - Restart in Windows PE
  - Enable High Performance
  - **Configure Hardwre**
    - Format and Partition Disk
    - **Fujitsu**
      - Configure Fujitsu LifeBook E744
    - **UEFI Conversion**
      - Format and Partition Disk
      - Restart in Windows PE
      - Enable High Performance
    - Partition Disk 0 - UEFI
  - **Configure BitLocker**
    - Configure BitLocker - WinPE
    - Pre-provision BitLocker
  - **Apply Operating System**
    - Apply Operating System
    - Apply Windows Settings
    - Apply Network Settings
  - **Apply Drivers**
    - Configure Driver Package To Download
    - Download Drivers
    - Apply Drivers
- **Setup Operating System**
  - Setup Windows and Configuration Manager
  - Enable High Performance
- **Install Applications**
  - Install POC Apps
- **Configure Windows 10**
  - Configure Windows 10 1607
- **Configure Credential Guard**
  - Enable Credential Guard
- **Configure EMET**
  - Enable EMET Policy
- **Configure BitLocker**
  - Configure BitLocker - FullOS
  - Enable BitLocker

Type: Group

Name: Install Operating System

Description: Actions to run in Windows PE to install and configure the image

No settings are required for this action.

Figure 26. Task sequence for the POC workstation.

Automating the building process for the POC workstations proved to be quite useful, especially while testing the Device Guard functionality. The sequence also makes sure that the implemented controls are in place and repeatable for multiple computers. Although some of the configuration was made through Active Directory's Group Policy mechanism, the balance between these two approaches complements each other; SCCM is used to configure the hardware of the workstation, install the operating system and applications as well as configure the settings ready to be managed through Active Directory’s GPOs.

5 Reflecting the KATAKRI requirements

5.1 Choosing the KATAKRI requirements

Since the assignment was to delimit the requirements explained in KATAKRI to only concern the end-user workstations, a decision was made to use only the following requirements of the criteria:

- I06 – The principle of least privilege – *Management of access rights*
- I07 – Defence-in-depth – *Identification of actors of the information processing environment within a physically protected area*
- I08 – Principle of minimality and of least privilege rights – *Configuration with dedicated system parameters*
- I09 – Defence-in-depth – *Protection against malware*
- I10 – Defence-in-depth – *Traceability of security events*
- I12 – Evaluation and approval of cryptographic products – *Crypto solutions*
- I23 – Security throughout the information processing environment lifecycle – *Management of software vulnerabilities*

The reason for choosing the requirements of the criteria was that, those can be reflected against standard user environment’s end-point workstations and the operating system laying on top of it. These requirements can also be met from the technical point of view. The chosen requirements also reflect the top four mitigation strategies introduced by the Australian Signals Directive.

5.2 Approach on addressing the KATAKRI requirements

This chapter focuses on how to address the requirements using the tools described in Chapter 3. Some of these requirements cross paths between the previously explained ASD's top four mitigation strategies, so those would be dealt here also.

The approach on addressing how to handle certain requirements does not give a straight answer to the requirement defined in KATAKRI, instead real-life risks are used as key factors on how to lower them with real-life implementations using the technologies implemented in the POC environment. This assignment focuses more on the technical implementations, although some of the requirements are addressed from process of act point-of-view.

5.3 Management of access rights – I06

Requirement I06 of KATAKRI states:

1. *CIS users and automated processes shall be given only the access, privileges or authorisations they require to perform their tasks.*
2. *Unauthorised modifications or other unauthorised or inappropriate handling of classified information is prevented through access control management and the appropriate use of security controls within the IT system.*

This requirement (and its implementation example) has the qualifications that concern more how organizations handle the whole process of user rights management. As the POC environment focuses more on the technical aspects of security, this requirement is approached from that point of view.

- Standard users are able to do what they are supposed to be doing on the POC workstation, create documents, presentations and spreadsheets with different applications.
- Standard users cannot make any modifications to the system configuration because of the GPO configuration implemented.
- Standard user accounts are separated from administrative user accounts
- The POC workstation is configured so that the information can only be transferred in or out with dedicated USB mass storage devices

5.4 Identification of actors of the information processing environment within a physically protected area - I07

Requirement I07 of KATAKRI states:

Reliable methods to identify the actors of the information processing environment have been taken into use.

Users in the environment are identified either by username and password, or with biometric identifier (fingerprint). Two-factor authentication is usually the standard for reliability, to make sure the person is who he/she claims to be with something they have and something they know. The implemented biometric authentication can be seen as a two-factor authentication: the computer the user's fingerprint is stored into and the actual fingerprint itself, thus making it a reliable method for identifying the user. From the administrative point-of-view, the lack of centralized management of the users' fingerprints will increase the IT administrator's workload and thus might not be the most efficient way to handle authentication in a centralized Active Directory environment.

The implementation example of the requirement further explains that the users in the environment shall be using individual user accounts and that all accounts are identified. POC environment did not define on how the individual accounts should be configured, one example could be the usage of an employee number or ID which should be individual for every user. The example also defines that the accounts shall be locked out after too many failed login attempts. This requirement is handled through the baseline policy offered by Microsoft through SCM. For protection level III or II, additional identification of the device should be done technically also, which was not the case in the POC implementation.

5.5 Configuration with dedicated system parameters – I08

Requirement I08 of KATAKRI states:

1. *Only the essential functionalities, devices and services to meet operational requirements shall be implemented in order to avoid unnecessary risks.*

2. *Organisation uses a procedure through which systems are installed and configured systematically, resulting in a hardened installation, following the configuration rules set by the organisation itself.*

3. *Configuration contains only such components, services, user and process rights which are mandatory in order to fulfil the operational as well as the security requirements*

To meet these three requirements:

1. The environment has the essential functions for the end-users to do their work. Although there are many security controls in-place, they are there because of the fact that they are proven to be affective against modern day threats. Those controls might pose a risk if they are not administered correctly.

2. Automated process of installing workstations is implemented in the POC environment. Configuration rules are based on the good-known configuration, with minor modifications that can be justified.

3. This requirement can be met in many different ways. As the operating system itself has plenty of components and these components talk to each other, turning off every single ‘not-needed’ service for example would be just overkilling. Instead, following the industry best practices presented a more appropriate way to handle the overall configuration.

The whole requirement is slightly controversial. The requirement states that one needs to ‘meet operational requirements in order to avoid unnecessary risks’ and then it orders the configuration to contain only ‘components, services etc.’ that are mandatory to fulfil the operational and security requirements. As an IT administrator, the writer sees that that alone poses a risk for the overall operational functionality if too much of the operating system’s services, for example, are stopped.

The implementation example of the requirement has further details about these configurations dealt with the usage of baseline policy offered by Microsoft. Some of these include the disabling of the autorun/autoplay functionality and the usage of password protected screensavers. The example also mentions that additional security features such as DEP/ASLR/AppLocker should be used, which is in line with the POC implementation as they are used through both, the usage of EMET and AppLocker. The implementation example also defines that the procedure of system installation should be carried out so that the end-result is hardened and configured accordingly. In the POC environment this is achieved by the automated installation process configured through SCCM in conjunction with the baseline policies defined through Active Directory.

On protection levels II and III, the example goes further by telling that the systems should be configured so that the network traffic is minimized and the updates for the target systems in the environment are fetched from trusted locations. For the POC Microsoft's own recommendations were used on how to restrict the traffic from the Windows 10 operating system and the software updates are delivered only through the SCCM server. The update source shall be considered as trusted, since the environment itself is not connected to any other networks and the update delivery is done through air-gap. The example also details on how BIOS should be configured for the targets. This was also done for the POC environment, although it was not the main focus during the implementation phase.

5.6 Protection against malware – I09

Requirement I09 of KATAKRI states:

Reliable methods for deterrence, prevention, detection, resilience and recovery measures of malware are used in the information processing environment in order to prevent unauthorized changes and other unauthorized use of the information.

As the POC environment is disconnected from the Internet, it does not have the same kind of cloud-based protection available as the connected environments would have. For this reason, more controls focusing on malware protection were implemented:

- antimalware solution using F-Secure Client Security
- whitelisting solution using Microsoft AppLocker
- additional solution against 0-day exploits using Enhanced Mitigation Toolkit

POC environment is only thought from the technical point-of-view, thus the focus is more on the technical aspect of prevention, detection and resilience. The implemented controls worked as expected while they were tested during the building of the POC environment.

The implementation example of the requirement details on how the antimalware solution should work in practice, which is basically just stating that the solution should be active and working. On protection levels II and III the example introduces the consideration for the usage of USB-ports or other interfaces at all. Since the POC environment uses Device Control feature of FSCS, this requirement shall be dealt with accordingly. Only known external devices (USB sticks in this case) are usable on the target workstations and the administrators can control which they are and to who they are given to.

5.7 Defence-in-depth – Traceability of security events – I10

Requirement I10 of KATAKRI states:

In order to detect unauthorised changes or other unauthorised or inappropriate information handling within the information processing environment, reliable methods have been taken into use for tracing the security events.

POC workstation uses the ASD’s auditing configuration for Windows 10, which can be identified as reliable since based on best practices. Additional logging is implemented through Sysmon. The implemented configuration can be used to trace which processes are responsible for network connections, who initiated them etc. as well as auditing of user logons and group management actions made locally on the workstation.

The implementation example of the requirement focuses on the whole process of how the logged data should be handled, nevertheless, it also defines that the gathered log information should be sufficient enough to detect security breaches or attempts of such afterwards. Auditing configuration provided by Microsoft’s baseline policy should be considered efficient enough on the operating system side to accomplish this. As the POC environment did not have a centralized log management system implemented, this requirement can only be met from a technical point of view for the target workstation.

5.8 Crypto solutions – I12

Requirement I12 of KATAKRI states:

Competent authority has approved crypto solutions or products in current environment to the respective protection levels in order to safeguard and protect the information against unauthorised disclosure or loss of integrity.

Ficora’s National Communications Security Authority (NCSA) offers a list of ‘Encryption solutions approved by NCSA-FI for classified information’ (Ficora, 2016), however, in the list itself there is no mention of BitLocker. This was quite surprising, as BitLocker is a very commonly used technology in Windows operating systems, yet it still does not have a clearance of any level according to the Finnish authority. The requirement also refers to a list of accepted crypto solutions approved by NATO. The Netherlands accepts the usage of BitLocker on Windows 7 with the security level of NATO restricted (NATO Information assurance product catalogue, N.d.).

The strategies implemented in the POC do met the most notable flaws of the technology (DMA) and try to mitigate them. As Laiho’s (2017b, Appendix 4) flowchart shows, the difference between the operating systems used with BitLocker is significantly different, thus the configuration used can be assumed to be safer than the one which for example the Netherlands has approved for NATO restricted level.

The details of the requirement define that the overall threat level should be taken into consideration in the evaluation of the crypto products. The requirement itself cannot be fulfilled with the current configuration as it would need Ficora’s auditing for the configured disk encryption implementation.

5.9 Management of software vulnerabilities - I23

Requirement I23 of KATAKRI states:

Reliable arrangements are established for the entire lifecycle of the information processing environment to manage programme vulnerabilities.

Software update process for the POC environment was technically implemented so that the products used in the environment would be updated at monthly basis. Although the delivery of 0-day patches can be a difficult task, the POC has the technology to achieve these goals.

The whole vulnerability management is more about the process on how the administrators follow what is happening in the world at the time being and how to implement these changes in the environment they are responsible for. Details of the requirement define that on the protection levels II and III additional vulnerability scanning would be need to be performed in the environment on a regular basis. To fulfill this, additional processes and products should be implemented in the POC environment.

6 Conclusions and further improvements

The approach on the assignment was to focus on technical and more practical side of implementing security controls proved to be quite good from the learning point of view. The reflection of Australian Signals Directorate top four mitigation strategies (2012) on the practical side of things was a good starting point for building a proof of concept that would also answer the requirements that were given by the assigner as well as what was defined in KATAKRI. The top four mitigation strategies were relatively easy to digest for technical implementation compared to the requirements KATAKRI introduced. As the top four mitigation strategies are based on statistical results, they are proven to be effective.

The scope of the implementation was wide, as one point was to study the new features offered by Windows 10 that could be used in the work. As Windows 10 was a quite new operating system at the start of the writing this assignment, not much information was available on the subject. Microsoft’s own documentation lacked on some of the subjects; therefore, a decision was made to use other sources as well for the technology background of the work. The LTSB version of the operating system and its features is not very well covered by Microsoft itself. The used version of Windows 10 (LTSB 2016, based on the CBB 1607) does offer good features in the terms of security, however, as was quickly seen in the implementation, all of these new features are not mature enough to be used in environments such as the one this assignment produced. Most notably, the Device Guard feature of Windows 10 is fascinating from the security perspective, however, as long as the administrative effort is as challenging as it is during the time of the writing, I do not see it to be used in larger environments. Restricting the unneeded traffic made by the operating system was a big question mark at the beginning of writing this assignment, however, during the implementation phase, Microsoft started offering a solution that was later used in the environment.

The overall configuration of the operating system and the environment in this case was challenging as several matters needed to be taken into consideration. The controls had to be implemented simultaneously so that they would not interfere with each other and could be used hand-in-hand. One example of this was the configuration of hardware to be used with the BitLocker feature in the most secure way possible by utilizing UEFI and Secure Boot functionalities. This involved the configuration of the group policies, the hardware itself as well as putting it all together to be fully automatized for the operating system deployment. Besides the technical configuration, additional consideration was given to the processes involving the administrative tasks the POC environment would introduce. Processes and technology have to support each other so that they work hand-in-hand correctly. One good example of this kind of work is the handling of the software update delivery in the assignment.

Facing the requirements defined in the KATAKRI auditing criteria proved to be quite challenging as well. Choosing only few requirements was a good decision, since the work had to be narrowed down to only concern the end-user workstations. Defining the requirement itself and researching its implementation examples, the crafted environment answers the questions introduced. The biggest surprise from the technological point of view was the BitLocker absence from the NCSA-FI’s list of approved crypto solutions, remembering the fact that Windows operating system has a really big market share in the PC world. As KATAKRI noted, cryptographic product evaluations should be conducted in a way that the overall security is measured. Knowing this, the whole POC environment and its other security controls should be evaluated by approved officials to be or not to be accepted on the usage of BitLocker. Some of the requirements defined in KATAKRI crossed each other a slightly and they could be narrowed and simplified to the way the ASD’s top four mitigation strategies are structured.

The assigner’s requirements concentrated on the practical implementation as well as the usage of the new technologies. Besides the practical implementation, administrative processes were considered as was assigned. Overall, the environment built in the assignment can be used as an example of dealing with the requirements defined in KATAKRI as well as the usage of Windows 10 operating system. As the environment does not fully comply with the requirements, further improvements would need to be made. The most notable of these would be a centralized log management solution as well as the implementation of a vulnerability scanning mechanism and a process to help to evaluate the overall health of the environment on a regular basis. Other KATAKRI requirements should also be taken into consideration for an overall review of the environment like the one introduced in the POC.

The implementation of the same kind of controls against other possible operating systems, such as Linux could be researched further. The assignment clearly focuses more on the technical side, so further improving the processes behind the technologies used should be the most important item to research.

References

Andrabi, S. Microsoft Technet, Security Guidance Blog. 2016. *Security Compliance Manager 4.0 now available for download!* Accessed on 6th March 2017. Retrieved from https://blogs.technet.microsoft.com/secguide/2016/07/28/security-compliance-manager-4-0-now-available-for-download/

Appelbaum, J., Callandrino, J., Clarkson, W., Feldman, A., Felten, E., Halderman, J., Heninger, N., Paul, W. & Schoen, D. Princeton University. 2008. *Lest We Remember: Cold Boot Attacks on Encryption Keys*. Accessed on 5th February 2017. Retrieved from http://citpsite.s3-website-us-east-1.amazonaws.com/oldsite-htdocs/pub/coldboot.pdf

Australian Cyber Security Centre. 2016. *Restricting Administrative Privileges.* Accessed on September 29th 2016. Retrieved from http://www.asd.gov.au/publications/protect/Restricting_Admin_Privileges.pdf

Australian Cyber Security Centre. 2017. *Hardening Microsoft Windows 10, version 1703 Workstations*. Accessed on 4th June 2017. Retrieved from https://www.asd.gov.au/publications/protect/Hardening_Win10.pdf

Australian Signals Directorate. 2012. *Top four mitigation strategies to protect your ICT system.* Accessed on September 29th 2016. Retrieved from http://www.asd.gov.au/publications/protect/Top_4_Mitigations.pdf

Avecto. 2017. *94% of critical Microsoft vulnerabilities mitigated by removing admin rights.* Accessed on 27th February 2017. Retrieved from https://www.avecto.com/news-and-events/news/94-of-critical-microsoft-vulnerabilities-mitigated-by-removing-admin-rights/

Beckman, K. 2015. 4sysops. *FAQs for Microsoft Local Administrator Password Solution (LAPS) - Part 1*. Accessed on 6th March 2017. Retrieved from https://4sysops.com/archives/faqs-for-microsoft-local-administrator-password-solution-laps/

Beechey, J. 2010. *Application Whitelisting: Panacea or Propaganda?* SANS Institute. Accessed on September 29th 2016. Retrieved from https://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599

Bio-Key. N.n *EcoID product page*. Accessed on 18th May 2017. Retrieved from http://www.bio-key.com/products/ecoid/

Center for Internet Security. 2013. *Press Release*. Accessed on 6th March 2017. Retrieved from https://www.cisecurity.org/about/news-room/press-releases/2013-02-04.cfm

Decker, J. Microsoft TechNet. 2017. *Windows Hello biometric in the enterprise*. Accessed on February 5th 2017. Retrieved from https://technet.microsoft.com/en-us/itpro/windows/keep-secure/hello-biometrics-in-enterprise

Dormann, W. 2016. Carnegie Mellon University Software Engineering Institute CERT/CC blog. *Windows 10 Cannot Protect Insecure Applications Like EMET Can.* Accessed on 15th March 2017. Retrieved from https://insights.sei.cmu.edu/cert/2016/11/windows-10-cannot-protect-insecure-applications-like-emet-can.html

Dubey, U. 2016. *How to install Active Directory in Windows Server 2012?.* Accessed on 19th February. Retrieved from https://www.znetlive.com/blog/install-active-directory-windows-server-2012/

Easttom, C. 2012. *Computer Security Fundamentals 2nd Edition.* Indianapolis: Pearson.

Finnish Communications Regulatory Authorigy. 27th April 2016. *Viestintäviraston NCSA-toiminnon hyväksymät salausratkaisut*. Accessed on 30th May 2017. Retrieved from https://www.viestintavirasto.fi/attachments/tietoturva/NCSA_salausratkaisut.pdf

Finnish Ministry of Defence. 2015. *Katakri – Information security tool for authorities – 2015, Finland.* Accessed on October 29th 2016. Retrieved from http://www.defmin.fi/files/3417/Katakri_2015_Information_security_audit_tool_for_authorities_Finland.pdf

Flexera Software. 2016. *Vulnerability Review 2016.* Accessed on September 29th 2016. Retrieved from http://resources.flexerasoftware.com/web/pdf/Research-SVM-Vulnerability-Review-2016.pdf

F-Secure. N.n. *Database Updates*. Accessed on 1st May 2017. Retrieved from https://www.f-secure.com/en/web/labs_global/database-updates

Graeber, M. Exploit Monday Blog. *Introduction to Windows Device Guard: Introduction and Configuration strategy*. Accessed on 3rd March, 2017. Retrieved from http://www.exploit-monday.com/2016/09/introduction-to-windows-device-guard.html

Hakala, T. Microsoft TechNet. 2016. *What's new in Windows 10 security*. Accessed on 7th March 2017. Retrieved from https://technet.microsoft.com/en-us/itpro/windows/whats-new/security

Hakala, T. Microsoft TechNet. 2017. *What's new in Windows 10, versions 1507 and 1511*. Accessed on February 5th 2017. Retrieved from https://technet.microsoft.com/itpro/windows/whats-new/whats-new-windows-10-version-1507-and-1511

Halfin, D., Microsoft TechNet Blog. 2016. *Overview of Windows as a service*. Accessed on February 5th 2017. Retrieved from https://technet.microsoft.com/en-us/itpro/windows/manage/waas-overview

Hallum, C. Microsoft Windows Blog. 2015. *Windows 10 Security Innovations at RSA: Device Guard, Windows Hello and Microsoft Passport*. Accessed on 5th February. Retrieved from https://blogs.windows.com/business/2015/04/21/windows-10-security-innovations-at-rsa-device-guard-windows-hello-and-microsoft-passport/

Hoffman, C. How-To Geek. 2016. *Windows 10 Without the Cruft: Windows 10 LTSB (Long Term Servicing Branch), Explained.* Accessed on 5th February 2017. Retrieved from http://www.howtogeek.com/273824/windows-10-without-the-cruft-windows-10-ltsb-explained/

Hoffman, C. How-To Geek.2012. *What is "Group Policy" in Windows?*. Accessed on 6th March 2017. Retrieved from https://www.howtogeek.com/125171/htg-explains-what-group-policy-is-and-how-you-can-use-it/

Holt, B., Meyler, K., Oh, M., Ramsey, G., Sandys, J. 2012. *System Center 2012 Configuration Manager Unleashed*. Indianapolis: Pearson.

Howse, B. 2015. Anandtech. *Windows 10 Editions compared*. Accessed on 6th March 2017. Retrieved from http://www.anandtech.com/show/9413/windows-10-editions-compared

Kaelin, M. TechRepublic. 2016. *Microsoft announces new Windows Defender Advanced Threat Protection (but there's a catch).* Accessed on 5th February 2017. Retrieved from http://www.techrepublic.com/article/microsoft-announces-new-windows-defender-advanced-threat-protection-but-theres-a-catch/

Kelly, G. 2015. *Microsoft admits Windows 10 automatic spying cannot be stopped.* Accessed on 27th February 2017. Retrieved from http://www.forbes.com/sites/gordonkelly/2015/11/02/microsoft-confirms-unstoppable-windows-10-tracking/

Khanse, A. The Windows Club. 2016. *What is Credential Guard In Windows 10*. Accessed on 3rd March, 2017. Retrieved from http://www.thewindowsclub.com/credential-guard-windows-10

Kim, D., Solomon, M. 2014. *Fundamentals of Information Systems Security 2nd Edition.* Burlington: Jones & Bartlett Learning.

Krebs, B. Krebs on security. 2013. *Windows Security 101: EMET 4.0*. Accessed on 5th February 2017. Retrieved from https://krebsonsecurity.com/2013/06/windows-security-101-emet-4-0/

Laiho, S. 2017. Win-Fu Official Blog. *The True Story of Windows 10 and the DMA-protection*. Accessed on 17th May 2017. Retrieved from http://blog.win-fu.com/2017/02/the-true-story-of-windows-10-and-dma.html

Lich, B. Microsoft Technet. 2016. *Windows security baselines.* Accessed on 6th March 2017. Retrieved from https://technet.microsoft.com/en-us/itpro/windows/keep-secure/windows-security-baselines

Lich, B. Microsoft Technet. 2017a. *Protect derived domain credentials with Credential Guard*. Accessed on 3rd March, 2017. Retrieved from https://technet.microsoft.com/en-us/itpro/windows/keep-secure/credential-guard

Lich, B. Microsoft TechNet. 2017b. *Deploy code integrity policies: policy rules and file rules*. Accessed on 14 th May, 2017. Retrieved from https://docs.microsoft.com/en-us/windows/device-security/device-guard/deploy-code-integrity-policies-policy-rules-and-file-rules

Lich, B. Microsoft TechNet. 2017c. Manage connections from Windows operating system components to Microsoft services. Accessed on 3rd September, 2017.

Retrieved from https://docs.microsoft.com/en-us/windows/configuration/manage-connections-from-windows-operating-system-components-to-microsoft-services

Mathers, B. Microsoft Technet. 2017. *Appendix F: Securing Domain Admins Groups in Active Directory*. Accessed on 23rd April, 2017. Retrieved from https://technet.microsoft.com/en-us/windows-server-docs/identity/ad-ds/plan/security-best-practices/appendix-f--securing-domain-admins-groups-in-active-directory?f=255&MSPPError=-2147217396

Mathers, B. Microsoft Technet. 2017. *Appendix H: Securing Local Administrator Accounts and Groups.* Accessed on 23rd April, 2017. Retrieved from https://technet.microsoft.com/en-us/windows-server-docs/identity/ad-ds/plan/security-best-practices/appendix-h--securing-local-administrator-accounts-and-groups

Mell, P. Bergeron, T., Henning, D. 2005. *Creating a Patch and Vulnerability Management Program.* Gaithersburg: National Institute of Standards and Technology. Accessed on September 29th 2016. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf

Mercer, N., Microsoft TechNet Blog. 2016a. *Further simplifying servicing models for Windows 7 and Windows 8.1*. Accessed on February 5th 2017. Retrieved from https://blogs.technet.microsoft.com/windowsitpro/2016/08/15/further-simplifying-servicing-model-for-windows-7-and-windows-8-1/

Mercer, N., Microsoft Technet, Windows for IT Pros. 2016b. *Introducing Windows Information Protection*. Accessed on 3rd March, 2017. Retrieved from https://blogs.technet.microsoft.com/windowsitpro/2016/06/29/introducing-windows-information-protection/

Metcalf, S. 2016. Active Directory Security. *Securing Windows Workstations: Developing a Secure Baseline*. Accessed on 7th March 2017. Retrieved from https://adsecurity.org/?p=3299

Microsoft Download Center. 2017. *Device Guard and Credential Guard hardware readiness tool.* Accessed on 4t May 2017. Retrieved from https://www.microsoft.com/en-us/download/details.aspx?id=53337

Microsoft TechNet Library. N.d.a *Overview of Windows AppLocker*. Accessed on 5th February 2017. Retrieved from https://technet.microsoft.com/en-us/library/dd759113.aspx

Microsoft TechNet Library. N.d.b. *Set Up a Disconnected Network (Import and Export Updates)* Accessed on 22nd October 2017. Retrieved from https://technet.microsoft.com/en-us/library/cc720512(v=ws.10).aspx

Microsoft TechNet, Windows Sysinternals. 2017. *AccessChk v6.1*. Accesed on 20th February 2017. Retrieved from https://technet.microsoft.com/en-us/sysinternals/bb664922.aspx

Microsoft TechNet. 2014. *Step 3: Configure WSUS.* Accessed on 26th April 2017. Retrieved from: https://technet.microsoft.com/en-us/library/hh852346.aspx

Microsoft TechNet. 2017. *Windows 10 release information*. Accessed on February 5th 2017. Retrieved from https://technet.microsoft.com/en-us/windows/release-info.aspx

Microsoft Technet. N.d. *Windows 8.1 boot security FAQ*. Accessed on 7th March 2017. Retrieved from https://technet.microsoft.com/en-us/windows/dn168169.aspx

Microsoft. 2005. *Secure Startup-Full Volume Encryption: Technical overview*. Accessed on 7th March 2017. Retrieved from http://download.microsoft.com/download/5/D/6/5D6EAF2B-7DDF-476B-93DC-7CF0072878E6/secure-start_tech.doc

Microsoft. Hardware Dev Center. 2017. *PC OEM requirements for Device Guard and Credential Guard*. Accessed on 3rd March 2017. Retrieved from https://msdn.microsoft.com/en-us/windows/hardware/commercialize/design/minimum/device-guard-and-credential-guard

Microsoft. N.d. *Find out which Windows 10 edition is right for you.* Accessed on 19th February 2017. Retrieved from http://wincom.blob.core.windows.net/documents/Win10CompareTable_FY17.pdf

Myerson, T., Microsoft Windows Blog. 2016. *Windows 10 Embracing Silicon Innovation*. Accesed on January 28th 2017. Retrieved from https://blogs.windows.com/windowsexperience/2016/01/15/windows-10-embracing-silicon-innovation

NATO Information assurance product catalogue. N.n. *Bitlocker - Windows 7, Windows Server 2008 (R2)*. Accessed on 24th July 2017. Retrieved from http://www.ia.nato.int/niapc/Product/Bitlocker---Windows-7--Windows-Server-2008--R2-_567

Niehaus, M., Microsoft TechNet Blog. 2016. *More on Windows 7 and Windows 8.1 servicing changes*. Accessed on February 5th 2017. Retrieved from https://blogs.technet.microsoft.com/windowsitpro/2016/10/07/more-on-windows-7-and-windows-8-1-servicing-changes/

Niemelä, J. Virus Bulletin. 2013. *Statistically effective protection against ATP attacks.* Accessed on February 6th 2017. Retrieved from https://www.virusbulletin.com/uploads/pdf/conference_slides/2013/Niemela-VB2013.pdf

Nixu. N.d. *Katakri*. Accessed on 20th March 2017. Retrieved from https://www.nixu.com/en/service/katakri

Panholzer, P. SEC Consultant Vulnerability Lab. 2008. *Physical security attacks on Windows Vista*. Accessed on February 7th 2017. Retrieved from https://dl.packetstormsecurity.net/papers/win/Vista_Physical_Attacks.pdf

Paul, I. PCWorld. 2016. *A beginner's guide to BitLocker, Windows' built-in encryption tool*. Accessed on 7th March 2017. Retrieved from http://www.pcworld.com/article/2308725/encryption/a-beginners-guide-to-bitlocker-windows-built-in-encryption-tool.html

Penshorn, R. N.d. Praetorian Security Blog. *Microsoft's Local Administrator Password Solution (LAPS)*. Accessed on 6th March 2017. Retrieved from https://www.praetorian.com/blog/microsofts-local-administrator-password-solution-laps

Perez, C. Shell is only the beginning. 2014. *Sysinternals New Tool Sysmon (System Monitor)*. Accessed on 5th February 2017. Retrieved from http://www.darkoperator.com/blog/2014/8/8/sysinternals-sysmon

Plett, C. Microsoft Technet. 2016. *Securing Privileged Access Reference Material.* Accessed on 2nd April, 2017. Retrieved from https://technet.microsoft.com/en-us/windows-server-docs/security/securing-privileged-access/securing-privileged-access-reference-material

Russinovich, M. 2016. *Tracking Hackers on Your Network with Sysinternals Sysmon*. Accessed on 7th March 2017, retrieved from https://www.rsaconference.com/writable/presentations/file_upload/hta-w05-tracking_hackers_on_your_network_with_sysinternals_sysmon.pdf

Russinovich, M., Margosis, A. 2016. *Troubleshooting with the Windows Sysinternals Tools.* Washington: Microsoft Press.

Savill, J. Windows IT Pro. 2016. *Learn what Windows Defender Advanced Threat Protection is*. Accessed on 5th February 2017. Retrieved from http://windowsitpro.com/windows-10/learn-what-windows-defender-advanced-threat-protection

Sebastian, A. 2015. *Windows 10 doesn't offer much privacy by default: Here's how to fix it*. Accessed on 27th February 2017. Retrieved from http://arstechnica.com/information-technology/2015/08/windows-10-doesnt-offer-much-privacy-by-default-heres-how-to-fix-it/

Sedgewick, A., Souppaya, M., Scarfone, K. 2015. *Guide to Application Whitelisting.* Gaithersburg: National Institute of Standards and Technology. Accessed on September 29th 2016. Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf

Shultz, G. TechRepublic. 2016. *The Windows 10 roadmap provides in-depth details on Device Guard and Credential Guard.* Accessed on 5th February 2017. Retrieved from http://www.techrepublic.com/article/the-windows-10-roadmap-provides-in-depth-details-on-device-guard-and-credential-guard/

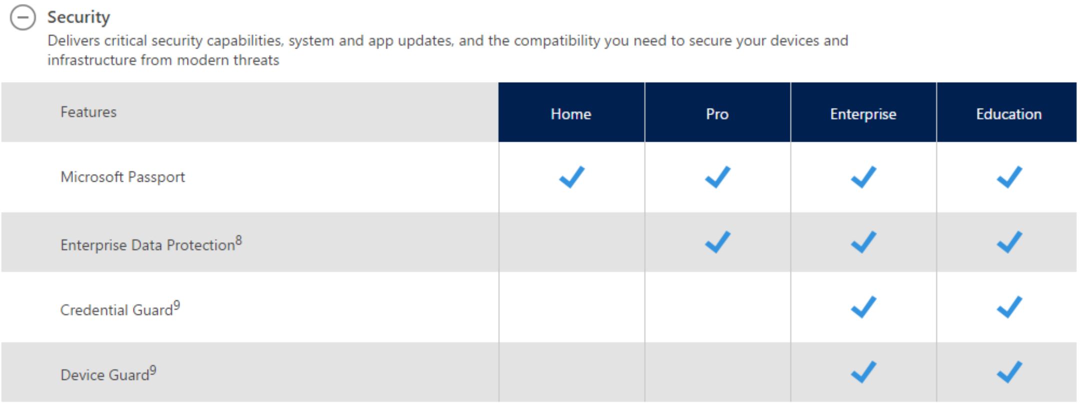
Smith, R. Netwrix Blog. 2016. *Windows Information Protection: Your Private Security Helper*. Accessed on 3rd March, 2017. Retrieved from https://blog.netwrix.com/2016/11/17/windows-information-protection-your-private-security-helper/

SurfRight. 2015. *HitmanPro.Alert Exploit Test Tool Manual 1.6.* Accessed on 18th May 2017. Retrieved from http://dl.surfright.nl/Exploit%20Test%20Tool%20Manual.pdf

Zeltser, Lenny. 2015. *What is cloud anti-virus and how does it work?.* Accessed on 19th February 2017. Retrieved from https://zeltser.com/what-is-cloud-anti-virus/

Appendix

Appendix 1. Windows 10 version security feature comparison.

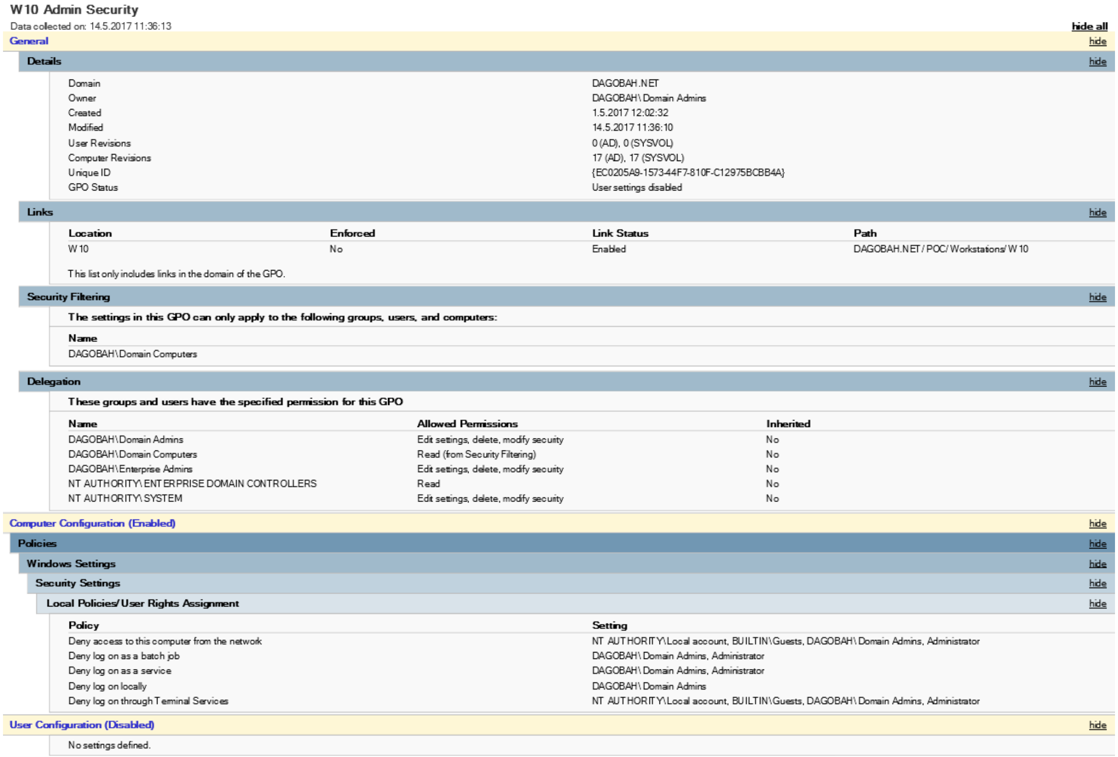


Security

Delivers critical security capabilities, system and app updates, and the compatibility you need to secure your devices and infrastructure from modern threats

Features	Home	Pro	Enterprise	Education
Microsoft Passport	✓	✓	✓	✓
Enterprise Data Protection[8]		✓	✓	✓
Credential Guard[9]			✓	✓
Device Guard[9]			✓	✓

Appendix 2. Admin security group policy object.



W10 Admin Security

Data collected on: 14.5.2017 11:36:13

General

Details

Domain	DAGOBAH.NET
Owner	DAGOBAH\ Domain Admins
Created	1.5.2017 12:02:32
Modified	14.5.2017 11:36:10
User Revisions	0 (AD), 0 (SYSVOL)
Computer Revisions	17 (AD), 17 (SYSVOL)
Unique ID	{EC0205A9-1573-44F7-810F-C12975BCBB4A}
GPO Status	User settings disabled

Links

Location	Enforced	Link Status	Path
W 10	No	Enabled	DAGOBAH.NET / POC/ Workstations/ W 10

This list only includes links in the domain of the GPO.

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name
DAGOBAH\Domain Computers

Delegation

These groups and users have the specified permission for this GPO

Name	Allowed Permissions	Inherited
DAGOBAH\Domain Admins	Edit settings, delete, modify security	No
DAGOBAH\Domain Computers	Read (from Security Filtering)	No
DAGOBAH\Enterprise Admins	Edit settings, delete, modify security	No
NT AUTHORITY\ ENTERPRISE DOMAIN CONTROLLERS	Read	No
NT AUTHORITY\ SYSTEM	Edit settings, delete, modify security	No

Computer Configuration (Enabled)

Policies

Windows Settings

Security Settings

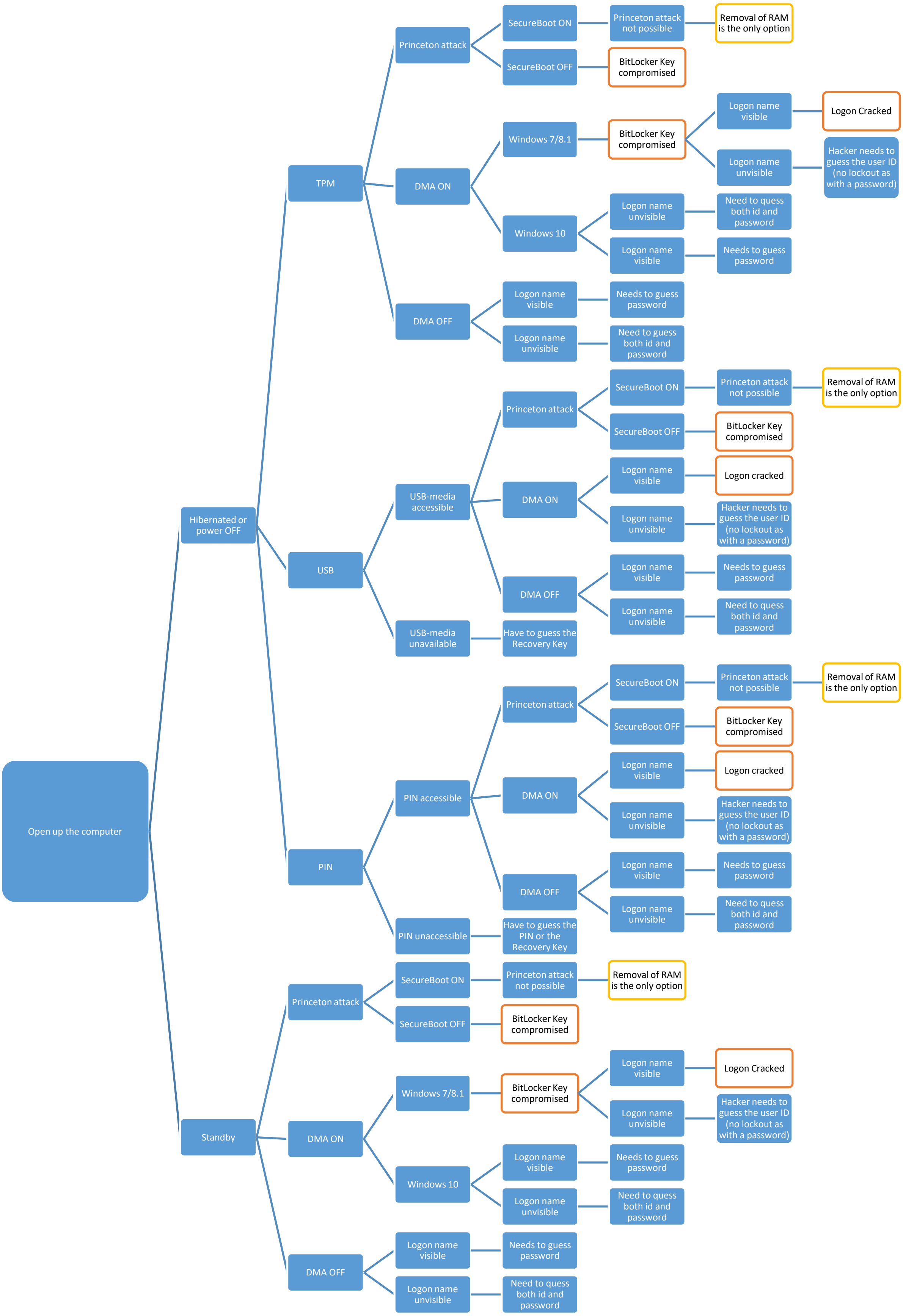
Local Policies/ User Rights Assignment

Policy	Setting
Deny access to this computer from the network	NT AUTHORITY\Local account, BUILTIN\Guests, DAGOBAH\ Domain Admins, Administrator
Deny log on as a batch job	DAGOBAH\ Domain Admins, Administrator
Deny log on as a service	DAGOBAH\ Domain Admins, Administrator
Deny log on locally	DAGOBAH\ Domain Admins
Deny log on through Terminal Services	NT AUTHORITY\Local account, BUILTIN\Guests, DAGOBAH\ Domain Admins, Administrator

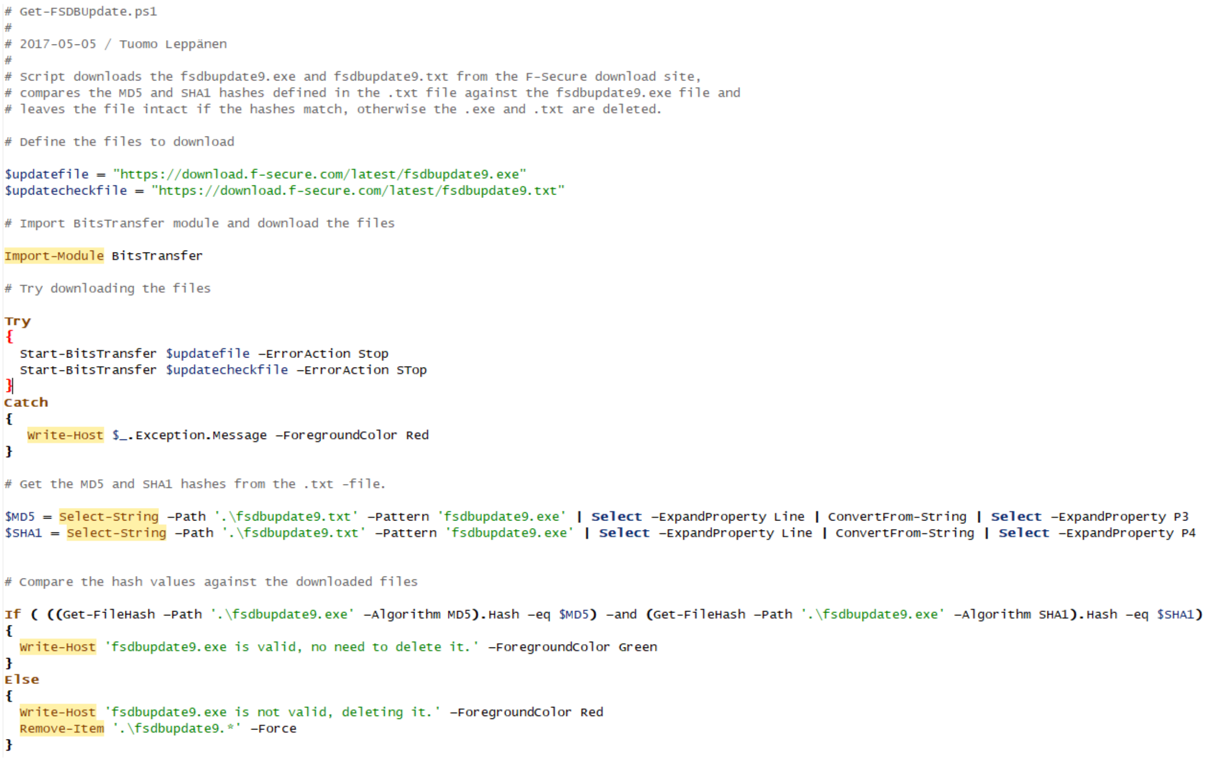
User Configuration (Disabled)

No settings defined.

Appendix 3. BitLocker compromise flowchart. Sami Laiho. 2017.



Appendix 4. Script for downloading F-Secure antivirus definitions



```
# Get-FSDBUpdate.ps1
#
# 2017-05-05 / Tuomo Leppänen
#
# Script downloads the fsdbupdate9.exe and fsdbupdate9.txt from the F-Secure download site,
# compares the MD5 and SHA1 hashes defined in the .txt file against the fsdbupdate9.exe file and
# leaves the file intact if the hashes match, otherwise the .exe and .txt are deleted.

# Define the files to download

$updatefile = "https://download.f-secure.com/latest/fsdbupdate9.exe"
$updatecheckfile = "https://download.f-secure.com/latest/fsdbupdate9.txt"

# Import BitsTransfer module and download the files

Import-Module BitsTransfer

# Try downloading the files

Try
{
  Start-BitsTransfer $updatefile -ErrorAction Stop
  Start-BitsTransfer $updatecheckfile -ErrorAction STop
}
Catch
{
   Write-Host $_.Exception.Message -ForegroundColor Red
}

# Get the MD5 and SHA1 hashes from the .txt -file.

$MD5 = Select-String -Path '.\fsdbupdate9.txt' -Pattern 'fsdbupdate9.exe' | Select -ExpandProperty Line | ConvertFrom-String | Select -ExpandProperty P3
$SHA1 = Select-String -Path '.\fsdbupdate9.txt' -Pattern 'fsdbupdate9.exe' | Select -ExpandProperty Line | ConvertFrom-String | Select -ExpandProperty P4


# Compare the hash values against the downloaded files

If ( ((Get-FileHash -Path '.\fsdbupdate9.exe' -Algorithm MD5).Hash -eq $MD5) -and (Get-FileHash -Path '.\fsdbupdate9.exe' -Algorithm SHA1).Hash -eq $SHA1)
{
  Write-Host 'fsdbupdate9.exe is valid, no need to delete it.' -ForegroundColor Green
}
Else
{
  Write-Host 'fsdbupdate9.exe is not valid, deleting it.' -ForegroundColor Red
  Remove-Item '.\fsdbupdate9.*' -Force
}
```

Appendix 5. List of folders users have write access to

```
RW C:\Program Files (x86)\F-Secure\Anti-Virus\gkhsmtemp
RW C:\ProgramData\Comms
RW C:\ProgramData\F-Secure
RW C:\ProgramData\Microsoft OneDrive
RW C:\ProgramData\USOShared
RW C:\ProgramData\F-Secure\FSAUA
RW C:\ProgramData\F-Secure\FSMSI
RW C:\ProgramData\F-Secure\Logs
RW C:\ProgramData\F-Secure\Quarantine
RW C:\ProgramData\F-Secure\sidegrade
RW C:\ProgramData\F-Secure\FSAUA\content
RW C:\ProgramData\F-Secure\FSAUA\header
RW C:\ProgramData\F-Secure\FSAUA\installation_status
RW C:\ProgramData\F-Secure\FSAUA\segmentation_rules
RW C:\ProgramData\F-Secure\FSAUA\subscriptions
RW C:\ProgramData\F-Secure\FSAUA\temp
RW C:\ProgramData\F-Secure\FSAUA\content\aquawin32
RW C:\ProgramData\F-Secure\FSAUA\content\avmisc
RW C:\ProgramData\F-Secure\FSAUA\content\fsav_1100_bin
RW C:\ProgramData\F-Secure\FSAUA\content\gemdb
RW C:\ProgramData\F-Secure\FSAUA\content\hipsn
RW C:\ProgramData\F-Secure\FSAUA\content\hydrawin
RW C:\ProgramData\F-Secure\FSAUA\content\mlcwin
RW C:\ProgramData\F-Secure\FSAUA\content\nifbin
RW C:\ProgramData\F-Secure\FSAUA\content\orsp-win-v2
RW C:\ProgramData\F-Secure\FSAUA\content\aquawin32\1488140398
RW C:\ProgramData\F-Secure\FSAUA\content\avmisc\1457957074
RW C:\ProgramData\F-Secure\FSAUA\content\fsav_1100_bin\1485959324
RW C:\ProgramData\F-Secure\FSAUA\content\gemdb\1487940417
RW C:\ProgramData\F-Secure\FSAUA\content\hipsn\1487932806
RW C:\ProgramData\F-Secure\FSAUA\content\hydrawin\1487936965
RW C:\ProgramData\F-Secure\FSAUA\content\mlcwin\1467788443
RW C:\ProgramData\F-Secure\FSAUA\content\nifbin\1486548835
RW C:\ProgramData\F-Secure\FSAUA\content\nifbin\1486548835\browser
RW C:\ProgramData\F-Secure\FSAUA\content\nifbin\1486548835\latebound
RW C:\ProgramData\F-Secure\FSAUA\content\nifbin\1486548835\resources
RW C:\ProgramData\F-Secure\FSAUA\content\nifbin\1486548835\resources_14
RW C:\ProgramData\F-Secure\FSAUA\content\nifbin\1486548835\resources_cs

RW C:\ProgramData\F-Secure\FSAUA\content\nifbin\1486548835\static

RW C:\ProgramData\F-Secure\FSAUA\content\nifbin\1486548835\browser\install

RW C:\ProgramData\F-Secure\FSAUA\content\nifbin\1486548835\browser\install\fs_firefox_https

RW C:\ProgramData\F-Secure\FSAUA\content\nifbin\1486548835\browser\install\fs_ie_https

RW C:\ProgramData\F-Secure\FSAUA\content\nifbin\1486548835\latebound\BPP

RW C:\ProgramData\F-Secure\FSAUA\content\nifbin\1486548835\latebound\BPP\localization

RW C:\ProgramData\F-Secure\FSAUA\content\nifbin\1486548835\resources\image

RW C:\ProgramData\F-Secure\FSAUA\content\nifbin\1486548835\resources_14\image

RW C:\ProgramData\F-Secure\FSAUA\content\nifbin\1486548835\resources_cs\image

RW C:\ProgramData\F-Secure\FSAUA\content\nifbin\1486548835\static\css

RW C:\ProgramData\F-Secure\FSAUA\content\nifbin\1486548835\static\images

RW C:\ProgramData\F-Secure\FSAUA\content\nifbin\1486548835\static\scripts

RW C:\ProgramData\F-Secure\FSAUA\content\orsp-win-v2\1432729310

RW C:\ProgramData\F-Secure\FSAUA\segmentation_rules\FSPM.DAGOBAH.NET

RW C:\ProgramData\F-Secure\Logs\ComputerSecurity

RW C:\ProgramData\F-Secure\Logs\custom

RW C:\ProgramData\F-Secure\Logs\DAAS2

RW C:\ProgramData\F-Secure\Logs\FSAUA

RW C:\ProgramData\F-Secure\Logs\FSAV

RW C:\ProgramData\F-Secure\Logs\fsdevcon

RW C:\ProgramData\F-Secure\Logs\FSFW

RW C:\ProgramData\F-Secure\Logs\FSMA

RW C:\ProgramData\F-Secure\Logs\fspmsupport

RW C:\ProgramData\F-Secure\Logs\removal

RW C:\ProgramData\F-Secure\Logs\Safe Banking

RW C:\ProgramData\F-Secure\Logs\Setup

RW C:\ProgramData\F-Secure\Logs\sidegrade

RW C:\ProgramData\F-Secure\Logs\WMI Provider

RW C:\ProgramData\F-Secure\Logs\ComputerSecurity\WSC

RW C:\ProgramData\F-Secure\Logs\FSAV\Users

RW C:\ProgramData\Microsoft\DeviceSync

RW C:\ProgramData\Microsoft\PlayReady
RW C:\ProgramData\Microsoft\User Account Pictures
RW C:\ProgramData\Microsoft\Crypto\DSS\MachineKeys
RW C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys
RW C:\ProgramData\Microsoft\DataMart\PaidWiFi
RW C:\ProgramData\Microsoft\DRM\Server
RW C:\ProgramData\Microsoft\NetFramework\BreadcrumbStore
RW C:\ProgramData\Microsoft\OFFICE\Heartbeat
RW C:\ProgramData\Microsoft\Windows\DeviceMetadataCache\dmrccache
RW
C:\ProgramData\Microsoft\Windows\DeviceMetadataCache\dmrccache\downlo
ads
RW C:\ProgramData\Microsoft\WinMSIPC\Server
RW C:\ProgramData\Microsoft\WwanSvc\DMProfiles
RW C:\ProgramData\Microsoft\WwanSvc\Profiles
RW C:\ProgramData\Microsoft OneDrive\setup
RW C:\ProgramData\USOShared\Logs
RW C:\Users\Default
RW C:\Users\Default\AppData
RW C:\Users\Default\Application Data
RW C:\Users\Default\Cookies
RW C:\Users\Default\Desktop
RW C:\Users\Default\Documents
RW C:\Users\Default\Downloads
RW C:\Users\Default\Favorites
RW C:\Users\Default\Links
RW C:\Users\Default\Local Settings
RW C:\Users\Default\Music
RW C:\Users\Default\My Documents
RW C:\Users\Default\NetHood
RW C:\Users\Default\Pictures
RW C:\Users\Default\PrintHood
RW C:\Users\Default\Recent
RW C:\Users\Default\Saved Games
RW C:\Users\Default\SendTo
RW C:\Users\Default\Start Menu
RW C:\Users\Default\Templates
RW C:\Users\Default\Videos
RW C:\Users\Default\AppData\Local
RW C:\Users\Default\AppData\Roaming
RW C:\Users\Default\AppData\Local\Application Data
RW C:\Users\Default\AppData\Local\History
RW C:\Users\Default\AppData\Local\Microsoft
RW C:\Users\Default\AppData\Local\Temp
RW C:\Users\Default\AppData\Local\Temporary Internet Files
RW C:\Users\Default\AppData\Local\Microsoft\InputPersonalization
RW C:\Users\Default\AppData\Local\Microsoft\Windows
RW C:\Users\Default\AppData\Local\Microsoft\Windows Sidebar
RW C:\Users\Default\AppData\Local\Microsoft\InputPersonalization\TrainedDataStore
RW C:\Users\Default\AppData\Local\Microsoft\Windows\GameExplorer
RW C:\Users\Default\AppData\Local\Microsoft\Windows\History
RW C:\Users\Default\AppData\Local\Microsoft\Windows\INetCache
RW C:\Users\Default\AppData\Local\Microsoft\Windows\INetCookies
RW C:\Users\Default\AppData\Local\Microsoft\Windows\Shell
RW C:\Users\Default\AppData\Local\Microsoft\Windows\Temporary Internet Files
RW C:\Users\Default\AppData\Local\Microsoft\Windows\WinX
RW C:\Users\Default\AppData\Local\Microsoft\Windows\History\History.IE5
RW C:\Users\Default\AppData\Local\Microsoft\Windows\INetCache\Content.IE5
RW C:\Users\Default\AppData\Local\Microsoft\Windows\INetCache\IE
RW C:\Users\Default\AppData\Local\Microsoft\Windows\WinX\Group1
RW C:\Users\Default\AppData\Local\Microsoft\Windows\WinX\Group2
RW C:\Users\Default\AppData\Local\Microsoft\Windows\WinX\Group3
RW C:\Users\Default\AppData\Local\Microsoft\Windows Sidebar\Gadgets
RW C:\Users\Default\AppData\Roaming\Microsoft
RW C:\Users\Default\AppData\Roaming\Microsoft\Internet Explorer
RW C:\Users\Default\AppData\Roaming\Microsoft\Windows
RW C:\Users\Default\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch
RW C:\Users\Default\AppData\Roaming\Microsoft\Windows\CloudStore
RW C:\Users\Default\AppData\Roaming\Microsoft\Windows\Network Shortcuts
RW C:\Users\Default\AppData\Roaming\Microsoft\Windows\Printer Shortcuts
RW C:\Users\Default\AppData\Roaming\Microsoft\Windows\Recent
RW C:\Users\Default\AppData\Roaming\Microsoft\Windows\SendTo
RW C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu
RW C:\Users\Default\AppData\Roaming\Microsoft\Windows\Templates
RW C:\Users\Default\AppData\Roaming\Microsoft\Windows\CloudStore\Store
RW C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs
RW C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Accessibility

RW C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Accessories

RW C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Maintenance

RW C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\System Tools

RW C:\Users\Default\Documents\My Music

RW C:\Users\Default\Documents\My Pictures

RW C:\Users\Default\Documents\My Videos

RW C:\Windows\Temp

RW C:\Windows\tracing

RW C:\Windows\CCM\Inventory\idmifs

RW C:\Windows\CCM\Inventory\noidmifs

RW C:\Windows\CCM\Inventory\noidmifs\badmifs

RW C:\Windows\PCHEALTH\ERRORREP\QHEADLES

RW C:\Windows\PCHEALTH\ERRORREP\QSIGNOFF

RW C:\Windows\Registration\CRMLog

RW C:\Windows\servicing\Packages

RW C:\Windows\servicing\Sessions

RW C:\Windows\System32\FxsTmp

 W C:\Windows\System32\Com\dmp

RW C:\Windows\System32\Microsoft\Crypto\RSA\MachineKeys

 W C:\Windows\System32\spool\PRINTERS

 W C:\Windows\System32\spool\SERVERS

RW C:\Windows\System32\spool\drivers\color

RW C:\Windows\System32\Tasks\Microsoft\Windows\SyncCenter

RW C:\Windows\System32\Tasks\Microsoft\Windows\WCM

RW C:\Windows\System32\Tasks\Microsoft\Windows\PLA\System

RW C:\Windows\SysWOW64\FxsTmp

 W C:\Windows\SysWOW64\Com\dmp

RW C:\Windows\SysWOW64\Tasks\Microsoft\Windows\SyncCenter

RW C:\Windows\SysWOW64\Tasks\Microsoft\Windows\WCM

RW C:\Windows\SysWOW64\Tasks\Microsoft\Windows\PLA\System

RW C:\Windows\Temp\DisplayAudio

RW C:\Windows\Temp\DisplayAudio\6.16

RW C:\Windows\Temp\DisplayAudio\8.20
```