Expertise
and insight
for the future

Heikki Jauhiainen

Designing End User Area Cybersecurity for Cloud-based Organization

Metropolia University of Applied Sciences

Master of Engineering

Information Technology

Master's Thesis

15 February 2021

Author	Heikki Jauhiainen
Title	Designing End User Area Cybersecurity for Cloud-based Organization
Number of Pages	52 pages + 2 appendices
Date	15 Feb 2021
Degree	Master of Engineering
Degree Programme	Information Technology
Instructor	Sami Sainio, Principal Lecturer

This work was conducted for a Nordic company as a part of a larger cloud transformation initiative. The company started to fully utilize public cloud services. The company's security postures needed to be aligned with the new cloud operating model. The outcome of this thesis will form the baseline for a forthcoming Cybersecurity project.

The cyber defense model for public cloud computing differs from the traditional on-premises model. Due to those differences it's important to renew cybersecurity postures when moving to public cloud. This thesis analyzes these differences and tries to provide a holistic view of required cybersecurity functions for public cloud use.

The scope of this thesis is to identify the best practices of Cybersecurity protection for end users on a public cloud-based environment. In creating a cybersecurity strategy and choosing the right tooling for the defenses, the Sherwood Applied Business Security Architecture (SABSA) model as well as the ISF Standard of Good Practice for Information Security (ISF SOGP) were used as guidelines throughout this thesis.

The key results of this study are from a top-down description of how cybersecurity defense postures can be created with industry best practices by starting from business requirements and ending in evaluating the security measures. The study makes good use of National Institute of Standards and Technology (NIST) recommendations and the MITRE ATT&CK knowledge base. This thesis also attempts to provide an overall description of the automation and tooling needed for cloud-based end user cybersecurity.

The key finding is that even when a company relies on public cloud and the responsibility of managing the infrastructure is passed to the cloud vendor, the implementation challenges that enable secure and modern end user experience remain.

The other key finding is that current level of security automation is not sufficient to replace trained cybersecurity professionals, but rather these new tools bring forth additional competence requirements. The availability of trained professionals for certain types of technology needs to be considered when planning for new cloud security tools or acknowledging that the company needs to rely on a consulting company (partner).

Keywords	Cybersecurity, Microsoft 365, EM+S, SIEM, SOAR, SABSA

Tekijä Otsikko Sivumäärä Aika	Heikki Jauhiainen Designing the End User Area Cybersecurity for Cloud-based Organization 52 sivua + 2 liitettä 15. Helmikuuta 2021
Tutkinto	Insinööri (ylempi AMK)
Tutkinto-ohjelma	Information Technology
Ohjaajat	Sami Sainio, Yliopettaja

Opinnäytetyö tehtiin pohjoismaiselle yritykselle osana yrityksen laajempaa pilvi-transformaatiohanketta. Yrityksen tavoitteena oli alkaa hyödyntämään julkisia pilvipalveluja täysimääräisesti. Yrityksen tietoturvatoiminnot suuniteltiin vastaamaan uutta toimintamallia julkisessa pilvessä. Opinnäytetyö toimii perustana tulevalle tietoturvaprojektille.

Julkisessa pilvessä toimiessa tietoturvamalli on erilainen kuin perinteisessä ympäristössä. Tästä johtuen tietoturvatoiminnot pitää uudistaa vastaamaan julkisen pilven tuomia erilaisia tietoturvahaasteita. Opinnäytetyössä analysoidaan näitä eroja ja yritetään antaa kokonaisvaltainen kuva tarvittavista tietoturvatoiminnoista, joita julkisessa pilvessä tarvitaan.

Opinnäytetyön tarkoituksena oli selvittää parhaat käytännöt loppukäyttäjän kyberturvallisuustoimintojen rakentamiseksi pilvipohjaisessa ympäristössä. Kyberturvallisuusstrategian luomisessa ja oikeiden tietoturvatyökalujen valinnassa käytettiin Sherwood Applied Business Security Architecture (SABSA) -mallia ja ISF Standard of Good Practice for Information Security (ISF SOGP) -Mallia.

Tutkimuksen keskeisin tulos on kokonaisvaltainenkuvaus siitä, miten kyberturvalliisuus puolustusstrategia voidaan luoda alan parhaiden käytäntöjen avulla aloittamalla liiketoiminnan vaatimuksista ja lopulta päättymällä käyttötapausten arviointiin National Institute of Standards and Technology NIST:n suositusten ja MITER ATT & CK -tietokannan avulla. Opinnäytetyössä yritetään myös antaa yleiskuvaus pilvipohjaisen loppukäyttäjän kyberturvallisuuden edellyttämästä automaatiosta ja työkaluista.

Keskeinen havainto on, että vaikka yritys luottaa julkiseen pilvipalveluun ja vastuullinen infrastruktuurin hallinta on pilvipalvelujen toimittajan puolella, tarvittavien kyberturvallisuustyökalujen monimutkaisuus turvallisen ja modernin loppukäyttökokemuksen mahdollistamiseksi on vielä ratkaisematta.

Toinen keskeinen havainto on, että turvallisuuden automaatio ei poista koulutettujen kyberturvallisuuden ammattilaisten tarvetta. Uusilla työkaluilla tarvitaan uusia taitoja. Koulutettujen ammattilaisten saatavuus tietyntyyppiselle tekniikalle on otettava huomioon

suunniteltaessa uusien työkalujen käytön aloittamista tai tukeutumalla konsulttiyritykseen (kumppaniin).	
Avainsanat	Cybersecurity, Microsoft 365, EM+S, SIEM, SOAR, SABSA

Contents

Abstract

List of Abbreviations

1 Introduction 1

2 Method and Material 3

2.1 Reliability and Validity 3

3 Project Specifications 5

3.1 Current State Analysis 5

4 Theoretical Background 7

4.1 Designing Cloud-based Organization Cybersecurity Postures 7
4.1.1 Defining Business Requirements 8
4.1.2 Creating Security Strategy 9
4.1.3 Logical Security Architecture 19
4.1.4 Physical Security Architecture 19
4.1.5 Component Level Security Architecture 20
4.2 Concepts and Tooling for Cloud-based End User Cybersecurity 21
4.2.1 Detection capabilities 23
4.2.2 Protecting Administrative Access to Cloud Resources 24
4.2.3 Protecting Cloud Identity 25
4.2.4 Protecting End Point 27
4.2.5 Protecting Cloud-based Data 28
4.2.6 Protecting Applications in Cloud 29
4.2.7 Extended Detection and Response (XDR) 29
4.2.8 Security Incident and Event Management (SIEM) Tools from Cloud 30
4.2.9 Verifying State of Security 32

5 Results and Analysis 33

5.1 Defining requirements for H-Corp End user cybersecurity 33
5.2 Analysing the security automation 34
5.3 Analysing the detection capabilities 35
5.4 Decisions after the analysis 37

6 Discussions and Conclusions 40

References

Appendices

Appendix 1. Requirements mapping

Appendix 2. Testing Azure Sentinel automation

List of Abbreviations

AIP	Azure Information Protection, Microsoft product naming
ATP	Advanced Threat Protection, Microsoft product naming
SABSA	Sherwood Applied Business Security Architecture
Azure AD P2	Azure Active Directory Premium 2, Microsoft product naming
Office 365 ATP P2	Office 365 Advanced Threat Protection Plan 2
AV-scan	Antivirus Scan / End Point Protection
API	Application Programming Interface
PIM	Privileged Identity Management
PAW	Privileged Access workstation
RBACK	Role Base Access control
AWS	Amazon Web Services
MITRE ATT&CK	Cybersecurity kill chain framework from MITRE
ISF SOGP	ISF The Standard of Good Practice for Information Security
COBIT	Control Objectives for Information and Related Technologies
IRAM2	Information Risk Assessment Methodology 2
DLP	Data Loss Prevention
GDPR	General Data Protection Regulation
IaaS	Infrastructure as a Service
PaaS	Platform as a Service
SaaS	Software as a Service
HTTPS	Hypertext Transfer Protocol Secure
TLS	Transport Layer Security
SDN	Software Defined Networking
WAF	Web Application Firewall
PKI	Public Key Infrastructure
IT/OT	Information Technology / Operational Technology
CSA	Cloud Security Alliance
NIST	National Institute of Standards and Technology
PCI DS	Payment Card Industry Data Security Standard
OS	Operating System
XDR	Extended Detection and Response
AI	Artificial Intelligence
NTA	Network Traffic Analysis

IPA	Identity management framework
DLP	Data Loss Prevention
EDR	End Point Detection and Response
CASB	Cloud App Security Broker
IAM	Identity and Access Management
SIEM	Security Incident and Event Management
SOAR	Security Orchestration, Automation and Response
IBM	International Business Machines (Company)
KQL	Kusto Query Language
ISO (27001)	The International Organization for Standardization

1 Introduction

This thesis will provide an overview of the best practices of end user area cybersecurity design for a company relying solely on public cloud. The thesis aims to identify the differences between cybersecurity approaches in traditional on-premise and cloud-based environments.

In particular the thesis tries to answer the following research question: what are the best practises and tooling needed to build up cybersecurity for a public cloud-based end user environment?

The H-Corp (name masked) is a Nordic manufacturing company. The company headquarters and engineering department are in Nordics and the manufacturing plant is in China. The total amount of employees is approximately 2100. Half of them are in Nordics and half in China. The challenges include the low maturity level of cybersecurity postures as well as the upcoming transformation to solely utilize public cloud services.

Enhancing the level of cybersecurity is essential in order to make the organization a less likely target for cyberattacks and to protect the business from security threats. Raising the level of cyber defence automation helps to remediate threats faster and to mitigate the risk of larger cybersecurity breaches. In the long term, automating feasible parts of cyber defence might lead to cost savings, but the need for trained personnel should not be forgotten when considering these investments.

The thesis follows the Sherwood Applied Business Security Architecture (SABSA) model as a guiding framework for building cyber defence. The thesis outcome will be solutions needed for valid cyber defence postures. The actual project documents, processes and project work for test, user acceptance or production environment are not included in the scope of this thesis.

The thesis has been divided into three sections. The first section follows the SABSA model to create organizational cyber defence starting from Business requirements (Chapter 4.1). The second section (Chapter 4.2) introduces cloud-based cybersecurity tools. The third section (Chapter 5) is the analysis for H-Corp and security automation

and the fourth section (Chapter 6) is for conclusions. The analysis is done for protecting End User computing area.

2 Method and Material

The thesis follows the SABSA model. The SABSA model was chosen because it is free to use modular method focused to create overall security architectures with practical action steps. According to SABSA, thousands of professionals have qualified as SABSA Chartered Architects in nearly 50 countries [1].

Alongside SABSA the thesis relies on the ISF Standard of Good Practice for Information Security (SOGP) 2020. SOGP 2020 is a commercial subscription used by ISF Members. The latest version (2020) includes Cloud Security Controls used in this thesis.

Microsoft 365 E5 licenses and Azure subscription were used for evaluating Microsoft Security features. From the cloud service provider side Microsoft is compliant with most of the security standards, including the Payment Card Industry Data Security Standard (PCI DSS) [2]. Microsoft also offers customer instructions and checklists on how to build up compliance from customer side of responsibility. Generally, the public cloud and cloud services referred to in this thesis mean computing services offered by third-party providers over the public Internet.

For information security reasons, company details including the company name have been “firewalled” from the author of this thesis to avoid any accidental exposure of company secrets. The client interviews conducted are also refined to a generic form for the same reason without changing the contents.

2.1 Reliability and Validity

This thesis aims to provide guidance for selecting the right toolsets and for choosing the most appropriate vendor for cloud security. This thesis provides recommendations for tools and needed licenses but additional iteration rounds (assessment project) are needed with the customer before planning the implementation project itself.

Part of the thesis scope was to try identifying whether the readymade automation baseline for Azure Sentinel exists or not. The automation test conducted with Azure Sentinel was for evaluating the basic concept. There was a problem that live test data was missing from the analysis.

The study conducted tries to rely as much as possible on vendor and industry best practices. The weak point of analysis is investigating the Microsoft cybersecurity products detection capabilities. For analyzing the detection capabilities, the study is relying on SE labs and sect AV TEST Institute's reports on 5.3. The level of objectivity of these reports is unknown.

3 Project Specifications

The thesis project is an assessment on building up H-Corp end user cybersecurity postures relying on public cloud and identifying the automation baseline. The outcome consists of recommendations for building and enhancing the H-Corp cybersecurity maturity level when starting to rely fully on public cloud. The assessment was conducted in autumn 2020. The cybersecurity project will be executed in spring 2021.

3.1 Current State Analysis

This section introduces the current high-level ICT connectivity architecture and security architecture of H-Corp.

H-Corp makes use of Microsoft's public cloud and some functions are delivered from H-Corp's own datacenter in Norway. H-Corp users connect directly to the Microsoft cloud with Azure Active Directory (Azure AD) as identity provider. Figure 1 illustrates how end users connect to IT resources relying on Microsoft cloud. The cybersecurity of manufacturing plant Information Technology / Operational Technology (IT/OT) and Edge devices are not discussed in this study.

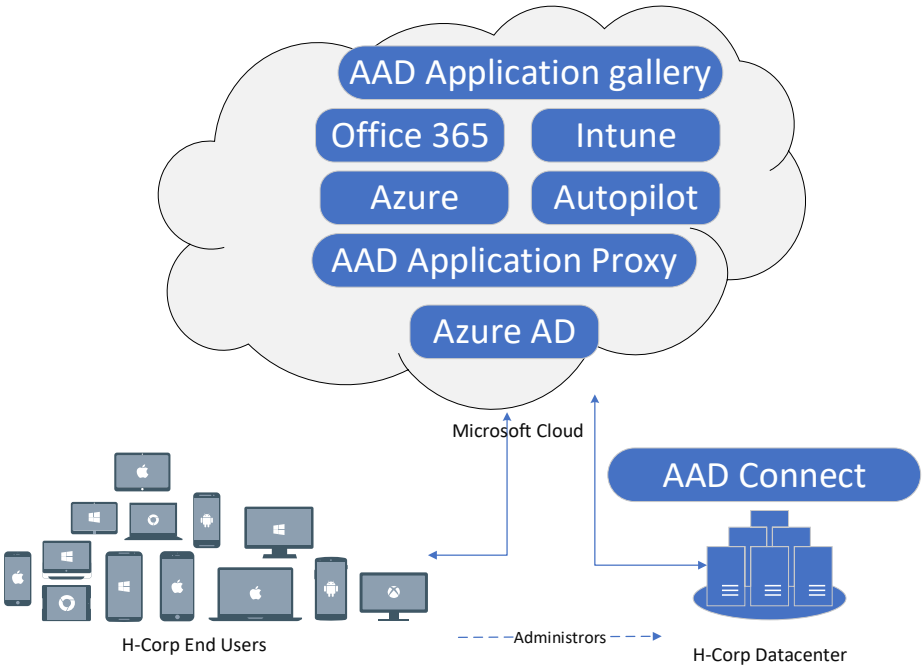


Figure 1. Current H-Corp ICT connectivity architecture.

The H-Corp has made a strategic decision to start fully consuming public cloud and to get rid of their own datacenter. In accordance with the move to cloud, H-Corp has a strategic initiative to enhance the cybersecurity postures of the company. Currently the datacenter is protected with firewalls and Azure services are protected with cloud Azure Firewalls and Azure Application Portal (includes Web Application Firewall) (WAF) features). Administrators use Virtual Private Network (VPN) connections to connect directly to the H-Corp datacenter. The end user devices are protected with End Point protection software. (*For customer privacy reasons the current security architecture is only described in general terms).*

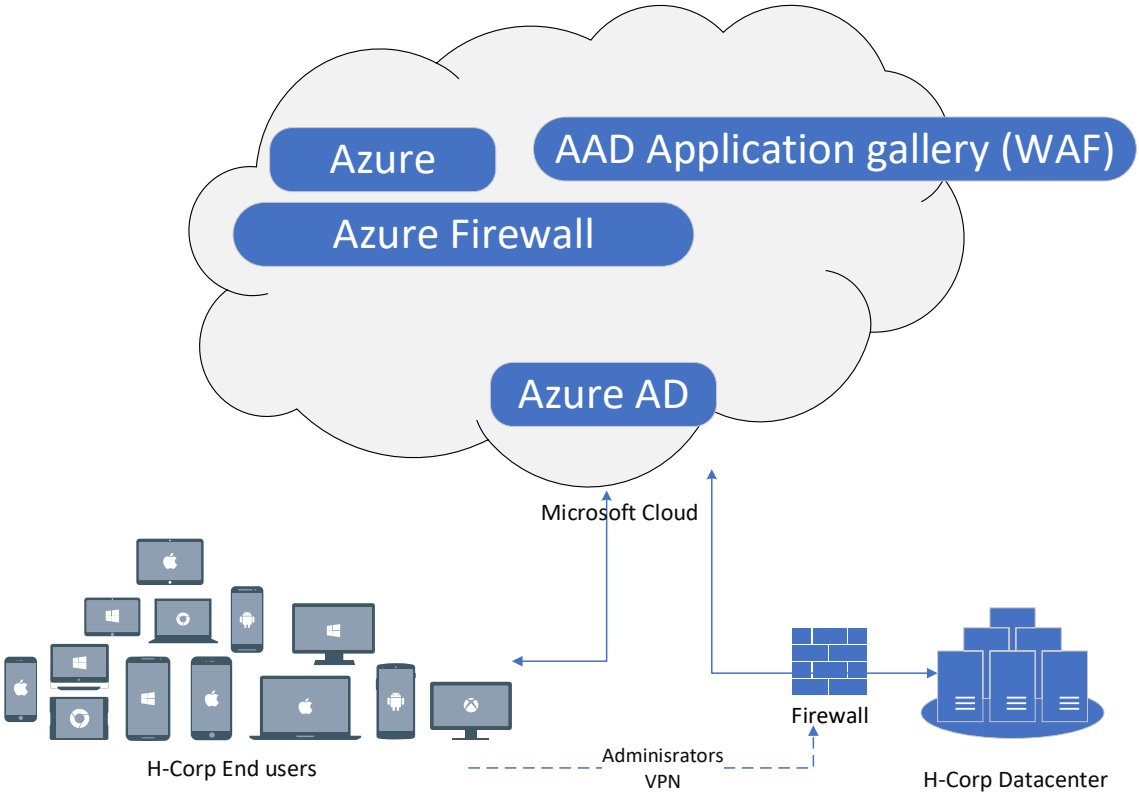


Figure 2. Current H-Corp ICT security architecture.

4 Theoretical Background

This chapter introduces theoretical background on how organizations can plan cyber defence and how protecting cloud-based assets differs from defending traditional on-premises assets. The chapter also describes the concepts and tooling for end user area cloud based cyber defence.

Chapter 4.1 with subchapters describes how to design with SABSA -model cybersecurity strategy based on business requirements and it describes the methods for choosing the right tooling for cloud-based cybersecurity. In the subchapter 4.1.2 the SOGP 2020 categories will be reflected against cloud-based cybersecurity.

Chapter 4.2 with subchapters describes the actual cybersecurity tooling for cloud-based end user environment. The chapter starts with describing the general concepts and ends with subchapter 4.2.9 describing how to verify the state of cybersecurity,

4.1 Designing Cloud-based Organization Cybersecurity Postures

For designing the overall cyber defence, the big picture contains more than just technology and detailed features. The processes, policies, and security culture matter in properly mitigating cyberthreats and risks. The SABSA and ISF SOGP models make it easier to consider all the aspects of cyber defence.

The SABSA model consists of six different phases for building up the organization cybersecurity postures described in Figure 3. Defining of operations security is out of this work's scope, but it means continuous support services in the SABSA model.

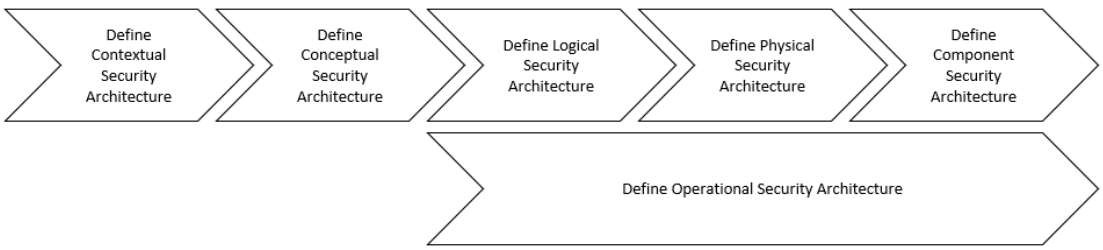


Figure 3. The SABSA model for security architecture development [3].

The SABSA model contains more templates and practices than are detailed in the scope of this thesis. The overall philosophy for SABSA is to use the right set of models to help organizations define security to the level of detail needed.

4.1.1 Defining Business Requirements

The first layer in the SABSA model is named **Contextual Security Architecture**. It defines how to map out the cybersecurity requirements and drivers from the business point of view. There are many different architectural approaches that can be taken. The most suitable approach will be drawn from a clear understanding of the business requirements [3].

Security architecture planning needs to be a comprehensive process comprising all viewpoints. Without the comprehensive approach and understanding of the requirements, there is a risk for a fragmented and poorly protected system.
The security architect needs to fully grasp business attributes such as business strategy and goals without forgetting any existing constrains. Constraints can include, for example, legal compliance obligations or requirements for data to be located in a certain area.

Methods for capturing the business requirements can be workshops, surveys, interviews and existing technical documentation. Security architect can help and guide the business owners with industry best practices and case studies to understand what is required from them. This concept of gathering the business requirements does not vary whether the organization is fully cloud-based or relies on on-premises components.

The SABSA model helps to elaborate understanding of the business requirements with these questions:

What type of system needs to be protected?
Why the system needs to be protected?
How the system will be used?
Who is using the system?
Where and when the system will be used?

It is not possible to mitigate all risks and create foolproof cybersecurity defense. That is why it is important to know what risks are the most valid and to prioritize defense measures accordingly.

The SABSA model classifies four domains of risks that are described in Table 1. Based on these domains, risks can be quantified and prioritized in line with the business requirements.

Table 1. SABSA risk domains.

Risk Domain	**Example of risk**
People	Policy violation
Processes	Failure to follow defined process
Systems	Breakdown of technical system
External	Malicious actions from third parties

4.1.2 Creating Security Strategy

The second step towards security strategy is the **Conceptual** phase within the SABSA model. When designing the security strategy, it is important to think of the big picture, instead of focusing on specific technical details. The move from business drivers to more specific security requirements is done via business attributes. At this stage, a business attribute profile is created and mapped in reference to the business requirements. Attributes are selected to best describe business requirements.

This phase is also for policy architecture. The organization may be moving into the cloud for the first time, and there is need to define new and to refine existing policies mitigating cloud risks.

The focus of the thesis is on cloud-based end user cybersecurity. The traditional approach (on-premises based) to cybersecurity relies upon barriers like firewalls to control traffic coming in and out of a network. Table 2 below describes in general terms the difference between cloud and on-premises end user cybersecurity aspects affecting the security architecture.

Table 2. Differences between Cloud and on-premises end user cybersecurity.

Cloud	**On-Premises**
Access from everywhere	Access through firewall device
Data located on any device (managed and unmanaged devices), multiple cloud solutions	Data located in company datacentre
Always up to date	Updates according to company timeline
Shared responsibility model between customer and cloud vendor	Company fully responsible for the environment
Multitenant environment. Supporting infrastructure serves multiple customers but each customer tenant is isolated	Company dedicated infrastructure

For the cloud-based organization, the overall security concept can be described as a zero-trust security model. The zero-trust architecture is based on the principle that nothing can be trusted. Devices, users or applications attempting to interact with the environment cannot be considered secure. Within the zero-trust security model, the critical components are identity and access management.

There are two main principles for identity and access management. Granular access rights with Role Based access control (RBACK) and the principle of least privilege. This means that the users and process identities should only access the resources they need to fulfil their tasks and the level of access should follow the same thinking.

Another key concept for cybersecurity is called defence in depth. The concept acknowledges that almost every security control can fail, because the attacker is determined and has resources or because of a problem how security controls are implemented. The defence in depth concept creates multiple layers of overlapping security controls; if one fails the next one can intercept [4].

The one difference between on-premises and cloud-based environments is the responsibility model. Cloud providers like Microsoft, Google and Amazon assume some responsibilities from the client organization. Generally, cloud providers are responsible for the security of the cloud, organizations utilizing the cloud are responsible for security of their data in the cloud. For example, the cloud vendor is responsible for the server infrastructure and the client organization is responsible for the configuration of the infrastructure.

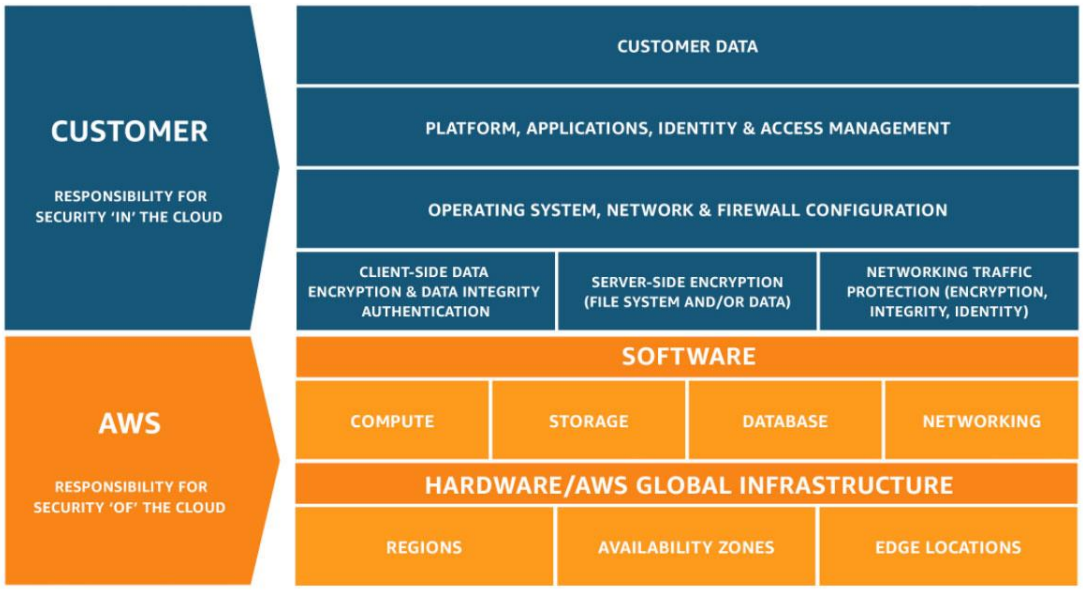


Figure 4. Shared responsibility between Amazon Web services (AWS) and the customer [5].

For creating business attributes, getting the overall picture, and verifying that there will be no conceptual caps in the cybersecurity strategy can be reflected against the ISF SOGP 2020 standard. The standard provides coverage of information security topics including those associated with security strategy, security governance, business continuity and cyber resilience. SOGP consists of 17 different categories described in Table 3.

For the reader, SOGP standard is a comprehensive list of security postures, this thesis is not listing all of those, but only the valid for evaluating differences of cloud and on-premises postures are described.

Table 3. SOGP 2020 categories [6].

Category
1. Security Governance 2. Information Risk Assessment 3. Security Management 4. People Management 5. Information Management 6. Physical Asset Management

7. System Development
8. Business Application Management
9. System Access
10. System Management
11. Networks and Communications
12. Supply Chain Management
13. Technical Security Management
14. Threat and Incident Management
15. Local Environment Management
16. Business Continuity
17. Security Assurance

The SOGP category of **security governance** guides the establishment of a security governance framework and sets clear directions for cloud security. For cloud-based environments, the overall governance practise is an important function. Without planned governance with clearly defined responsibilities and ownership, the entire environment will be difficult to maintain and secure. The general cloud governance goes tightly hand in hand with security governance. Control Objectives for Information and Related Technology (COBIT) 2019 structures the governance model as seven different components described in Figure 5 below. The components interact with each other, resulting in a holistic governance system for I&T [7]. These components can be tailored against needed specific purposes e.g. security governance.

Figure 5. COBIT 2019 Framework: Basic Concepts: Governance Systems and Components [7].

All cloud providers have their own best practises for cloud governance. Figure 6 depicts Microsoft Azure cloud governance aspects. These aspects could be used as a baseline in a cloud security governance model.

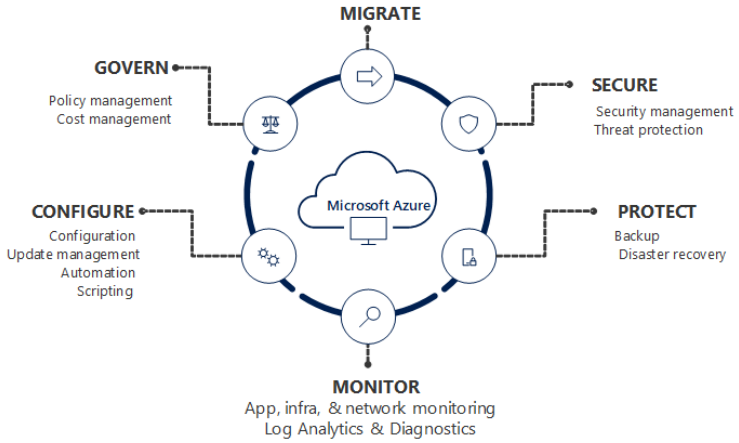


Figure 6. Azure management areas [8]

The Microsoft Azure is one part of Microsoft cloud services. The other general part is Microsoft 365 productivity suite. The suite relies on Microsoft Azure AD identity database, providing single identity across Microsoft 365 resources. The areas presented in Figure six should be taken into consideration when defining Microsoft 365 security governance. Microsoft 365 suite also includes the data compliance application for helping to govern and protect data itself.

The SOGP category **Information Risk Assessment** guides how information risks should be taken into consideration. Information risk assessments should be performed on a regular basis for target environments (business environments, processes and applications). Defining risk assessment processes should be done. Key information risks should be identified, and mitigation planned to acceptable level. The ISF SOGP provides IRAM2 methodology for assessing information risk. The six-phase process consist of Threat Profiling, Business Impact Assessment, Vulnerability Assessment, Risk Evaluation, and Risk Treatment [6]. For cloud-based organizations, the information can be accessible with any device and from all over the world so assessing information risk is important.

The SOGP category **Security Management** consists of security policy management and information security management. There are no major differences between traditional on-premises and cloud-based environments in this category. Tools and technologies vary but the basic concepts remain the same. In SOGP, information security management also includes legal and regulatory compliance. Cloud service providers like Microsoft, Google and Amazon are fulfilling almost all regulatory compliancy requirements

from their side. This kind of regulatory compliance requirement can be for example finance industry standard PCI DC or ISO 27001 security standard. It is possible to check from cloud provider web sites the evidence of compliancy for certain standard to fulfil the audit requirements. This reflects the shared responsibility model introduced in Figure 4. Cloud service provider is compliant but the organization utilizing the cloud must also be compliant on their part in accordance with the shared responsibility model.

The SOGP category **People Management** is about embedding information security into each stage of the employment and about promoting security awareness for employees. There is no major conceptual difference in this category between traditional on-premises and cloud environments.

The SOGP category **Information Management** describes information classification and protection methods. This category is especially important in cloud-based environments. Organization data can be stored in all kinds of devices and data is accessible over the Internet. Data Loss Prevention (DLP) policies also fall to this category. Cloud vendors have tools and methods for data labelling, encryption and for DLP functions. Third party tools can also be used to those functions. As an example, the Microsoft 365 tool stack includes Azure Information protection for classification and encrypting the documents.
The General Data Protection (GDPR) EU law on data protection and privacy states the following:

> In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption [9].

The SOGP category **Physical Asset Management** describes hardware and workstation, device management and industrial control systems. There is no major conceptual difference in this category between traditional on-premises and cloud environments.

The SOGP category **System Development** is guiding the build of business applications and incorporating information security during each stage of the application lifecycle staring from software development.

For cloud-based software development there are two basic concepts for secure and well-built applications. Those methods are the twelve-factor app and cloud native [29 p.253].

The SOGP category **Business Application Management** is for protecting business applications against unapproved access and misuse. For securing those applications, it is critical to protect the API connections. The API gateway concept can be used for protection and control [10]. The logging of usage of applications and data should be enabled, and logs aggregated to security information and event management (SIEM) / security orchestration, automation and response (SOAR) tools. The authentication to applications should be done with modern authentication and secure authentication protocols.

Among others the category contains guidance for end-user developed applications. The cloud-based tools enable end users to develop and run their own created features and functions. It is important to document, set administrative policies and governance for those. An example of end-user-developed functionalities are set of possibilities with Microsoft Teams, power apps and power automate [11].

The SOGP category **System Access** is for identity and access management (key part of cloud-based organization cybersecurity). The basic process flow for cloud identity and access management is as follows:

- AUTHENTICATION – The user/process will be authenticated (signed into cloud) using the credentials.
- AUTHORIZATION – Cloud entity checks for policies that apply to the request. It then uses the policies to determine whether to allow or deny the request.
- ACTIONS - After request has been authenticated and authorized, operations are defined by a service viewing, creating, editing, and deleting the resource; role-based access control (RBACK). Principle of least privilege should be applied.

Logging and aggregating logged data to SIEM/SOAR tool should be considered.

In the cloud context, the SOGP category **System management** refers to the design and building of systems, i.e. virtual servers, storage, serverless functions, micro services, and containers. All cloud vendors have their own best practises and readymade infrastructure templates. These best practises and configuration baselines should be used as a starting point for design in the cloud environment. Same basic concepts apply on cloud-based environment than on on-premises; network segmentation, server hardening, encryption, monitoring etc. The main differentiator is the shared responsibility model. Cloud provider does their part and the organization consuming the cloud does their part.

The SOGP category **Networks and communications** describes controls for physical, wireless and voice networks. For cloud-based environment, the network perimeter is not easy to define compared to on-premises components relying on network topology. Dotson [4] describes the complexity of trying to define the cloud network perimeter delivery models with following description:

> IaaS environments, such as bare-metal and virtual machines. These are the closest to traditional environments, but can often benefit from per-application segmentation, which is not feasible in most on-premises environments.
>
> Orchestrated container-based environments such as docker and Kubernetes. If applications are decomposed into microservices, more granular network controls are possible inside the individual applications.
>
> Applications PaaS environments such as cloud Foundry, Elastic Beanstalk and Heroku. These differ in the number network controls available. some may allow per component isolation, some may not provide configurable firewall functions at all, and some may allow the use of firewall functions from the IaaS down.
>
> Serverless or Function-as-a-Service environments, such as AWS Lambda, Open Whisk, Azure Functions and Google Cloud Foundations. These operate in a shared environment that may not offer network controls or that may offer network controls only on the Frontend.
>
> SaaS environments. While some SaaS offerings provide simple network controls (such as access only VPN or from whitelisted IP addresses), many do not.

In abstraction, the user of cloud-based networking connects to cloud services (Cloud providers network edge) through the Internet. Data communication is commonly secured with the Hypertext Transfer Protocol Secure (HTTPS) protocol and the communication protocol is encrypted using the Transport Layer Security (TLS) protocol. Other cloud security methods include segmenting networks by implementing Virtual Local Area Networks (VLANs), utilizing Software defined Networking (SDN) technology, cloud provider inbuild firewalls and WAF functions. Utilizing company existing on-premises firewalls with cloud is also possible.

The SOGP category **Supply Chain Management** contains a chapter of its own for cloud security controls. Whether acting in a cloud or on-premises environment is not so relevant. The cloud security part highlights the importance of effective cloud security governance and defined policies for mitigating the security risks created by users' freedom to consume versatile cloud services in many ways. The chapter lists core cloud security services including securing network connectivity, securing user access, protecting sensitive data, configuring and administering security and monitoring security-related events

and logs [6]. The importance of protecting and monitoring administrative access is listed in cloud security controls. Microsoft's security best practices require utilizing Privileged Access Workstation (PAW), a dedicated operating system for administrative tasks. The security hardened PAW can be virtual jump server or physical dedicated workstation [12]. The Privileged Access Workstation to securely administer cloud-based resources is described in Chapter 4.2.2.

The SOGP category **Technical Security Management** is for developing security architecture. The security architecture should support the security by design thinking [29 p.15]. The category includes malware protection. In cloud environment, Malware protection is handled with end point protection software where at least the control plane is cloud. This SOGP category also includes identity and access management, intrusion detection and data leakage prevention. Cloud vendors have native solutions for these listed.
A significant technology in Technical Security Management is cryptography. Data encryption means that contents are stored in a non-readable format and a key is required for decryption.

The data travelling between the cloud and the destination should be encrypted. The general term for that kind of moving data is *"at transit".* Data stored and residing in some media is called *"at rest"* and is by default encrypted by cloud providers. For companies utilising cloud services, there are vast possibilities for defining layered data encryption solutions. The following passage from Microsoft Azure training describes some of Azure's encryption possibilities [13].

> Azure Storage Service Encryption, which is used for encrypting the data stored in the managed disks, blobs, queues, files, etc. So this is considered as the low-level protection. Then we have the Virtual Machine Hard Disks Encryption, where the VHDs are encrypted. This is known as the Azure Disk Encryption. This will help in cases where a malicious user got access to subscription and wishes to steal your complete VM along with it's data.
>
> Next is the Database encryption, where we have the Transparent Data Encryption, abbreviated as TDE, which helps in the real-time encryption and decryption of databases, its associated backups and also the transaction logs. By default, TDE is enabled for all the newly deployed Azure SQL Database instances.
>
> Finally we have the Azure Key Vault, which is a centralized cloud service for storing the secrets and the keys to be used for your applications. It provides secure access, permission control, and access logging capabilities. It can be used for certificate management, key management, secrets management, and also store secrets backed by hardware security modules. So the bottom line is that they provide

huge benefits like – centralized management, easy integration with azure services, easy and simplified management.

For internal certificates the Public Key Infrastructure (PKI) can be built on cloud services like Azure, AWS and Google Cloud Platform. For example, Google Cloud Platform delivers cloud-based service for delivering internal digital certificates. [14].

The SOGP category **Threat and Incident Management** contains vulnerability management, security event logging, threat intelligence, cyber-attack protection, security, incident management and forensic investigation. This category is for creating active cyber defence. Vulnerability management is for patching devices and applications to reduce cyber-attack surface area. Based on the shared responsibility model where cloud provider is responsible for parts of infrastructure, the amount of vulnerabilities managed in a cloud environment is lower than in on-premises environments. There are external tools for vulnerability management relying on cloud.

Logging security events and protecting logs from tampering are highly important issues. Firstly, a decision should be taken on what kinds of logging information needs to be gathered from what sources. Without proper logging organizations are unavailable to recognise attacks. Regular monitoring should aggregate logs to the SIEM tool. The cost of storing log data is low, for example 10TB data stored to Amazon Glacier is less than 100 dollars per month. The cost of retrieving data from Glacier is much higher but in case of a security event the cost is justified [28 p.202]

Cloud-based security solutions utilize their own threat intelligence feeds for mitigating cybersecurity risks. For example, Microsoft Threat Intelligence has analysed trillions of signals and the security automation actions are based on those learnings [15]. For Cyber-attack protection, the big picture matters from employee training to Security Operations Centre (SOC) team, SOAR automation and everything in between.

The SOGP category **Local Environment Management** provides guidelines for local security including physical office and datacentre security.

The last SOGP category is **Business Continuity.** It lists the importance of disaster recovery and business continuity planning. On a conceptual level the cloud-based environment is more persistent on disasters than the on-premises environment. A cloud provider

with economy of scale can build up fault tolerant infrastructure and if cloud consuming company manages to build up fault resiliency on their side through e.g. geo-replication, a fault tolerant environment can be built. The cloud-based environment also better enables disaster recovery testing to apply with certain compliancy requirements. A cloud-based environment is more easily scaled up for temporary disaster recovery tests.

After the SABSA conceptual phase is ready, needed business attributes and policies should exist. The SABSA model highlights the importance of validating the architectural plans with business stakeholders with clear sign off documentation before moving forward.

4.1.3 Logical Security Architecture

The third step in the SABSA model is to move from business security strategy and business attributes to **Logical Security Architecture.** This means translating the security strategy into a functional view of security services, defining a comprehensive set of functional requirements. The logical phase provides the ability to identify which security services need to be implemented.

The outcomes of the process include logical architecture diagrams, lists, policies, governance documents, and disaster recovery procedures. It is a means for mapping out needed features and functions from the conceptual phase.

4.1.4 Physical Security Architecture

The fourth step in the SABSA model is the creation of **Physical Security Architecture** based on the Logical Security Architecture. This calls for defining more detailed security mechanisms and mapping requirements with industry best practises for effective defence.

The following figure is an example of physical security architecture from Cloud Security Alliance (CSA) reference architecture.

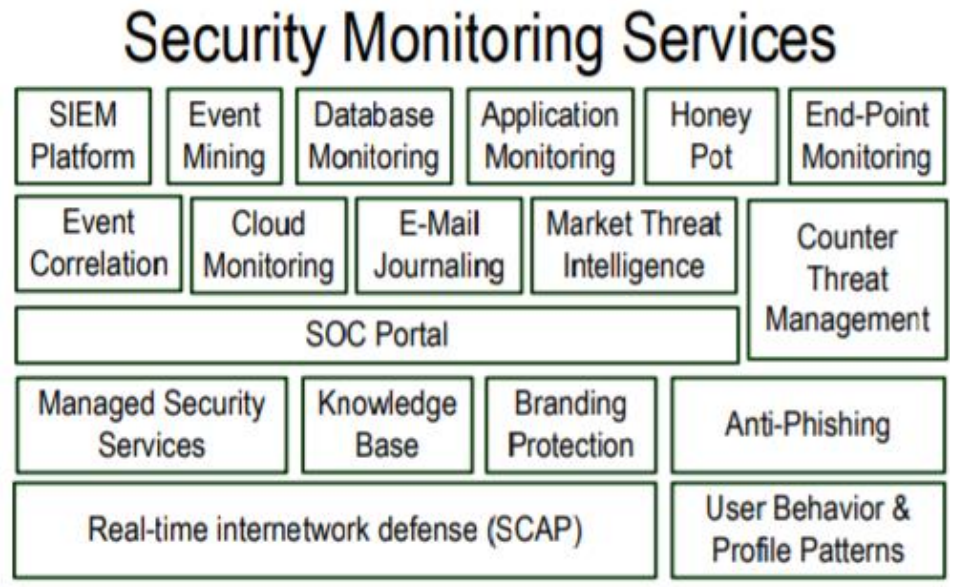


Figure 7. Example of logical security architecture, monitoring [16].

In this phase understanding specific target cloud platform capabilities is essential. In the end-user context the most significant cloud environments are Microsoft Office 365 and Google Workspace.

4.1.5 Component Level Security Architecture

The fifth and final step in the SABSA model means transferring from physical security architecture to **Component Level Security Architecture**. Needed security tools and products will be mapped at this stage. Figure 8 is an example of component level security architecture diagram from Microsoft reference architecture (high level).

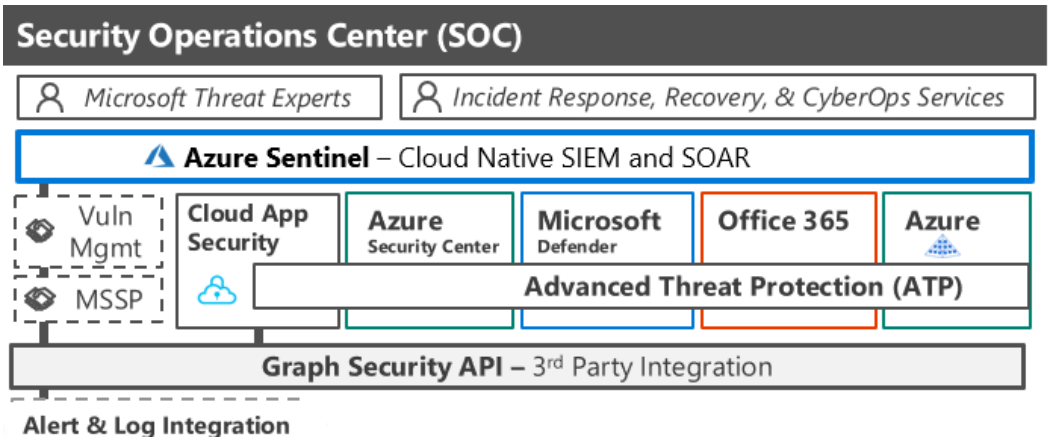


Figure 8. SOC Part of Microsoft Cybersecurity Architecture [17].

At this final stage all detailed information is ready for starting the security project. The detailed information should include:

- Security governance documents and process
- Disaster recovery documents and policies
- Business continuity documents
- Risk management process
- Backup and data retention documents and policies
- Data classification and protection (e.g. encryption) documents
- Software development process aligned with cybersecurity
- Overall cybersecurity architecture

Company's existing cybersecurity functions and license investments should also take in account. At this stage the clearly defined roles and responsibilities and communication flows supported by suitable collaboration tools should be defined as well.

4.2 Concepts and Tooling for Cloud-based End User Cybersecurity

This section introduces how organizations can enhance the level of end user cybersecurity protection. The focus is on Microsoft tooling because the study's subject company has chosen the Microsoft cloud as their preferred cloud.

The unified thinking around the cloud cybersecurity protection is the previously mentioned zero-trust model. Instead of believing that the company data and assets are safe, the zero-trust model assumes breaches and verifies each request as though it originated from an uncontrolled network regardless of where the request originates or what resource it accesses. Key guiding principles of the zero-trust model according to Microsoft are [18]:

> **Verify explicitly** - Always authenticate and authorize based on all available data points.
>
> **Use least privileged access** - Limit user access with Just-In-Time and Just-Enough-Access (JIT/JEA), risk-based adaptive policies, and data protection.
>
> **Assume breach** - Minimize blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses.

A zero-trust approach should extend throughout the entire organization, it serves as an end-to-end cybersecurity strategy. The idea of cybersecurity tooling is to get visibility into threats across all resources and to be able respond swiftly across the organization.

The other key cybersecurity concept is defence in depth. Figure 9 visualises how Microsoft tooling interrupts and blocks intrusion with multiple techniques in multiple touchpoints.

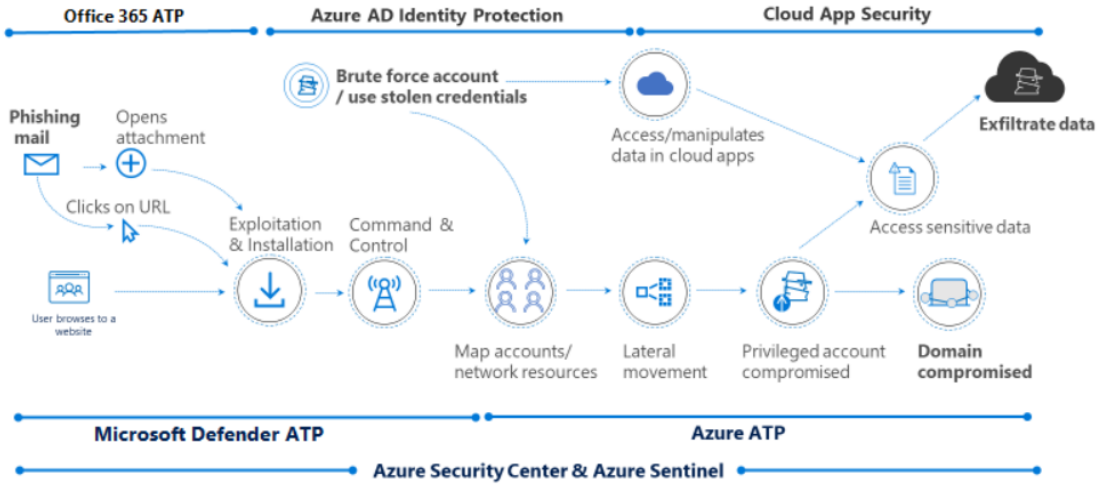


Figure 9. Example protection flow, defence in depth with Microsoft tooling [33].

The National Institute of Standards and Technology (NIST) framework visualises the organizational security needed with following core categories depicted in Figure 9 below. The description of security tooling loosely follows the NIST Core framework parts highlighted as red line.

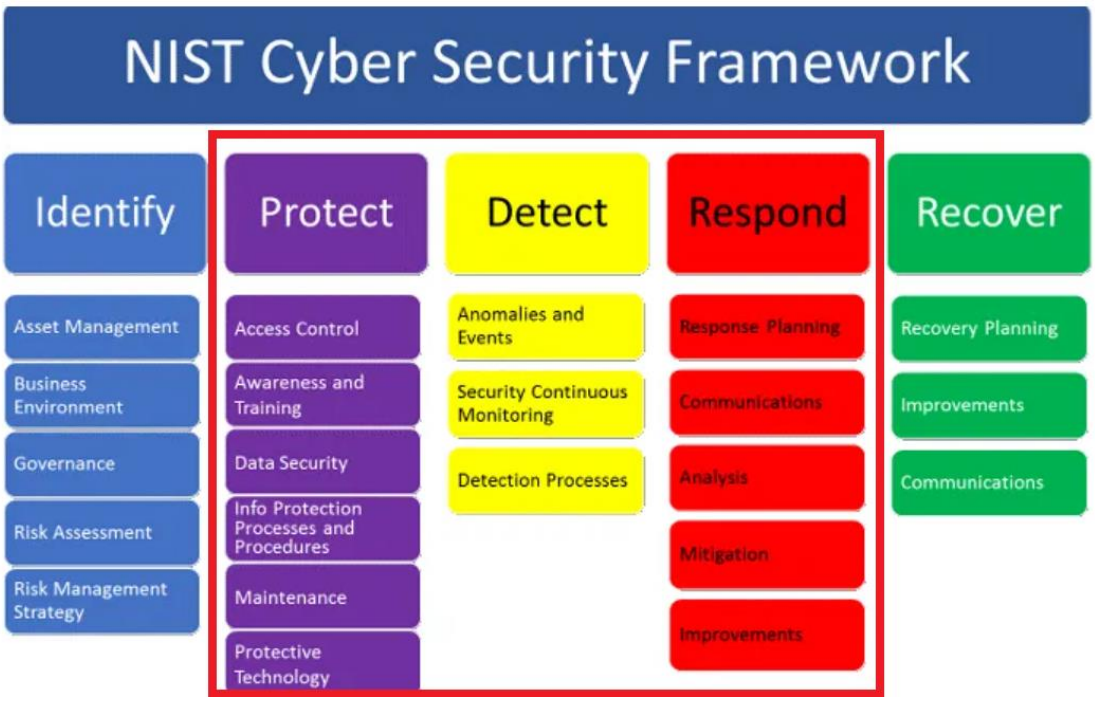


Figure 10. NIST Cybersecurity framework Core categories [19].

4.2.1 Detection capabilities

If all cybersecurity defences are showing the green light and everything seems to be working well but the detection capabilities are not up to date, the results will remain insufficient. In other words, if organization is unable to detect the security breach, it is not possible to respond to the threat. There is a need to develop a strategy for testing and improving the new and existing detection capabilities.

Firstly, the scope of the monitoring should be evaluated in organised way. Monitoring just the audit and security logs might not be enough. The monitoring needs should be reflected with overall architecture to be able identify that right kind of data is logged to achieve the desired visibility. Linkage between asset management and monitoring should also exists to be able to protect the new assets as well. The MITRE ATT&CK framework described in chapter 4.2.9 can be used for identifying most probable threats and monitoring needs should be also evaluated against those.

Secondly when the right kind monitoring and visibility is in place for analytics to investigate the lifecycle of detection capabilities should be created with continuous testing and

improvements for the future. This testing could include penetration testing and end user training.

4.2.2 Protecting Administrative Access to Cloud Resources

There should always be emergency/break-glass access for administrative purposes. With conditional access policies or other controls, it is easy to completely reject administrative access.

Monitoring and controlling the use of accounts with administrator authority is important. These accounts provide elevated access to the underlying IT resources and technology, which is why malicious actors seek to gain access to them. Workstations used for administrative tasks can also become access points to the enterprise. Microsoft best practice for protecting administrator devices is to provide each such administrator a dedicated operating system that is exclusively used for the administrative tasks. The concept is known as privileged access workstations (PAW) [20].
PAWs can be hardened physical workstations, virtual workstations or jump servers. The PAW workstation should not be used for non-administrative user activities like emailing, web browsing or other activities.

Following actions should also be taken in consideration for protecting the administrative accounts.

- Utilizing FIDO2 security keys for authentication of all administrators with Windows 10 workstation. FIDO2 Security key enables passwordless authentication with Windows 10.

- Activating Azure AD Privileged Identity Management (PIM) to reduce the attack surface by enabling temporally admin access to resources. Azure AD PIM enables just in time access for administrator, reducing attack surface

- Enabling conditional access controls and strongest level of authorization policies when accessing to administrative consoles.

- Enabling logging and monitoring connected to SIEM tool for administrative accounts with tested SOAR functions to prevent malicious access. Utilizing principle of least privilege with administrative accounts. Conducting the governance for administrative accounts including HR flow procedures when account owner has left the organization.

NIST [21] has created guidelines for privileged account management for financial services. They describe reference architectures and 3rd party tools for hardening the administrative access (Figure 11).

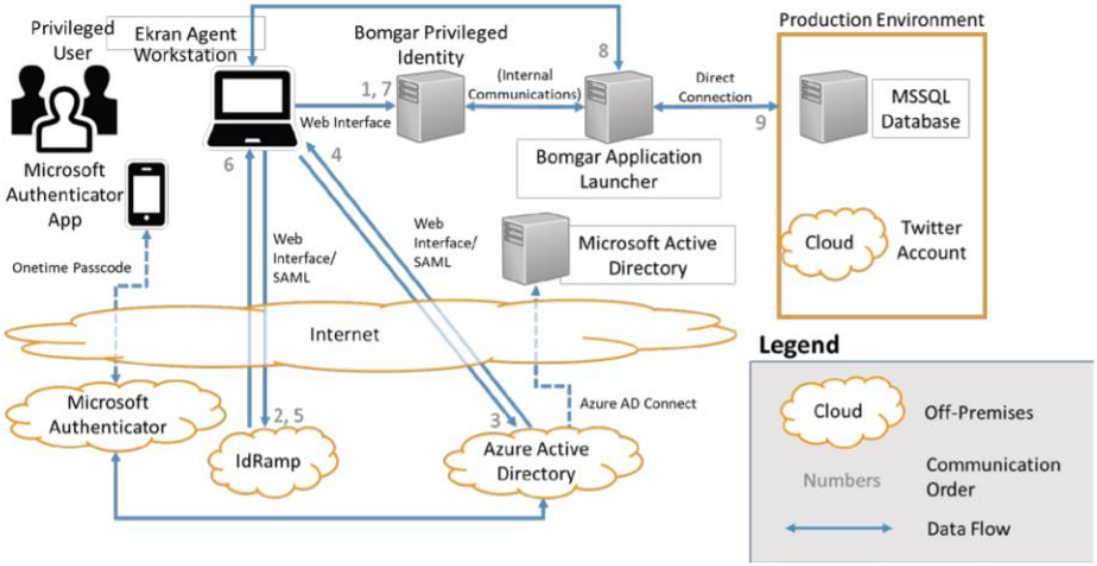


Figure 11. Example of reference architecture, protecting the administrative user account [21].

4.2.3 Protecting Cloud Identity

Identity is the primary perimeter for cloud security. One step for protecting the identity is to take care of the identity lifecycle, i.e. what happens before and after the identity is needed. Automated process flow with approvals and clear responsibilities should be activated. It is common knowledge that when an auditor starts to audit a company, the first request is for a list of users that have left the company. This list will be reflected against company identity database to find old users still existing there. There are several cloud-based identity services, some of those are listed in Table 4.

Table 4. Cloud-based identity services (not all listed here).

Provider	Cloud Identity Service
Amazon Web Services	Amazon IAM
Microsoft	Azure AD
Google	Cloud Identity
Alibaba	Resource Access Management (RAM)
Octa	Octa Identity Cloud
Ping Identity	PingCloud

Azure AD is Microsoft's cloud-based identity service and it is the most widely used. Azure AD Premium 2 (P2) has a vast amount of security features, including a connection to Microsoft Security Graph. According to Microsoft they analyse 18 billion login attempts each day and a certain part of those are done by adversaries (i.e., criminal actors, hackers) [22]. With this database of information, they can provide automated services running behind the Azure AD (Table 5).

Table 5. Azure AD P2 automated threat protection services [23]

Risk detection type	Description
Atypical travel	Sign in from an atypical location based on the user's recent sign-ins.
Anonymous IP address	Sign in from an anonymous IP address (for example: Tor browser, anonymizer VPNs).
Unfamiliar sign-in properties	Sign in with properties we've not seen recently for the given user.
Malware linked IP address	Sign in from a malware linked IP address.
Leaked Credentials	Indicates that the user's valid credentials have been leaked.
Password spray	Indicates that multiple usernames are being attacked using common passwords in a unified, brute-force manner.
Azure AD threat intelligence	Microsoft's internal and external threat intelligence sources have identified a known attack pattern.

The Azure AD P2 comes with features like multifactor authentication, conditional access and privileged identity management (PIM). PIM is for administrators' just in time access (temporary access for certain amount of time). Both Microsoft 365 and Azure cloud services rely on Azure AD.

Azure AD gathers a wide number of logs from activities, but client organizations still need to verify that logging is enabled, and that the right kind of data is gathered. By default, Azure AD P2 audit and sign logs are stored for 30 days. The logs can be stored to other medias for longer backup retention times. The logs should be aggregated to the SIEM tool (e.g. Azure Sentinel).

4.2.4 Protecting End Point

The diversity of different devices connecting to cloud resources (PC's, tablets, mobile phones, etc.) creates a large attack surface area. For this end point protection tooling is needed.

Microsoft Defender for Endpoint is an end point protection service. It is made up of a combination of Windows 10 features and services running within the Microsoft cloud. Windows 10 contains sensor applications that collect and process signals from the operating system and sends this data to cloud instance of Microsoft Defender for Endpoint. The installation and baseline policies can be done with Microsoft End Point manager cloud service (Intune). The Intune licensing is part of the Office 365 license.
The protection is real time – there is no periodical AV-scan process. Defender for Endpoints also includes a vulnerability management feature, taking care of vulnerabilities found in end point devices.

Trend Micro Apex One Endpoint protection tool has similar features than Microsoft End Point tool. Apex One has been chosen here as another example of end point protection tool. Figure 10 illustrates the touchpoint where Apex One can break a malware attack on a device [24].

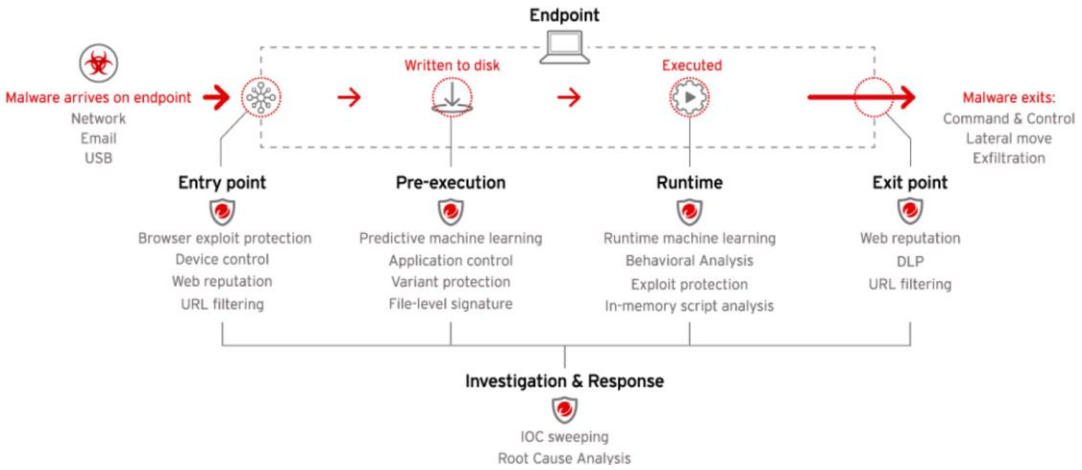


Figure 12. Trend Micro Apex One, protecting the device.

Apex One is integrated with thread intelligence feed and can be connected to a SIEM tool. Apex One does not have natively installed agent on Windows 10 Operating system (OS) so a separate agent needs to be installed.

Windows Defender for Endpoint and Trend Micro Apex One both offer protection also for iOS/Android devices, Linux/Windows servers and macOS.

4.2.5 Protecting Cloud-based Data

To protect the cloud-based assets, a company must know what kind of data resides there. Automated tools for the classification and labelling of data exist as commercial products. Data can be classified with meta-data tags depending on the organizational policies. For data protecting purposes, the documents can be automatically encrypted according to the document classification.

Besides encrypting the documents, DLP polices can be activated for identifying and governing data. Simplest form of DLP policy could be credit card number. If user sends out email or shares a document with credit card number, the DLP function can warn the user or block sending the document.

Azure Information Protection (AIP) from the Microsoft product stack is a tool for labelling and encrypting data and Microsoft Office 356 includes basic DLP functions.

The volume of information and multiple collaboration systems creates complexity for data management. Data can be moved between systems. For these reasons and compliancy, active data governance plans are also important for securing data.

4.2.6 Protecting Applications in Cloud

The Cloud Access Security Broker (CASB) is a general industry term for a tool protecting cloud applications. It acts as a mediator to examine cloud traffic and to extend the reach of their security policies. CASB solutions can also investigate data inside the cloud, by connecting on the cloud provider's own API connectors.

4.2.7 Extended Detection and Response (XDR)

Extended Detection and Response (XDR) is an approach to simplify the security technologies from the administrative and security operator viewpoints. The technologies and tooling used to be scattered and not working as unified single engine. XDR solutions are powered with machine learning and Artificial Intelligence (AI). XDR is built on security platforms like End Point Protection tools and cloud security tools by adding telemetry streams from multiple control points to unify the incident detection and response platform. XDR solutions vary by vendor, mostly covering endpoint, network, and cloud workload protections.

Figure 13 below showcases the conceptual Architecture abstraction of an XDR solution. The upper layer of the figure describes some data sources in which the XDR solution connects with and gets the data feed for analytics. In this case data comes from End Point Detection and Response (EDR), Cloud App Security Broker (CASB), Identity and Access Management (IAM), Data Loss Prevention (DLP), Network Traffic Analysis (NTA) and Identity management framework (IPA) solutions.

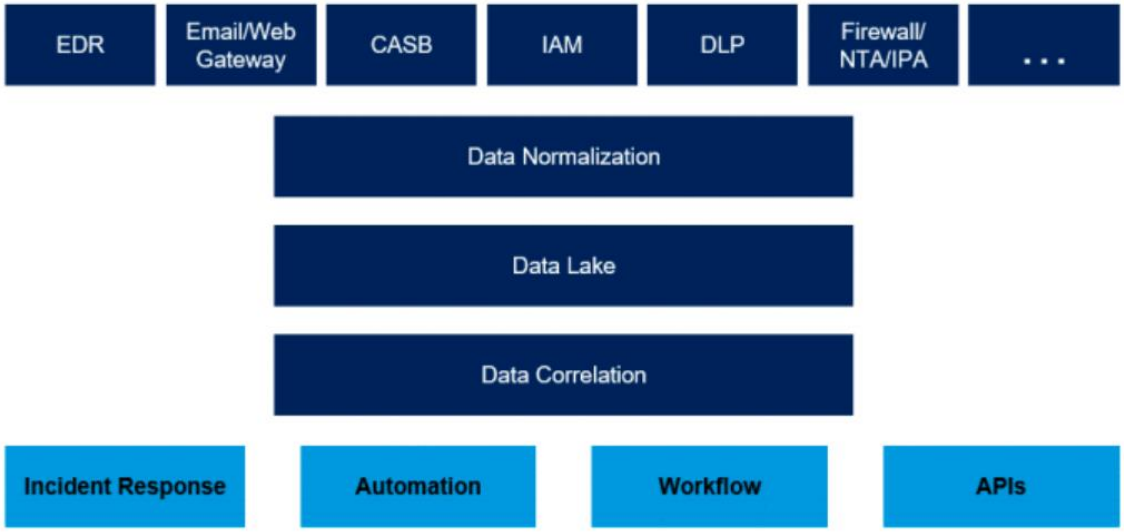


Figure 13. High level Abstraction of XDR solution.

Figure 14 is an abstraction of how Microsoft XDR provides an integrated platform that automatically collects data from multiple security components and simplifies the security operators work.

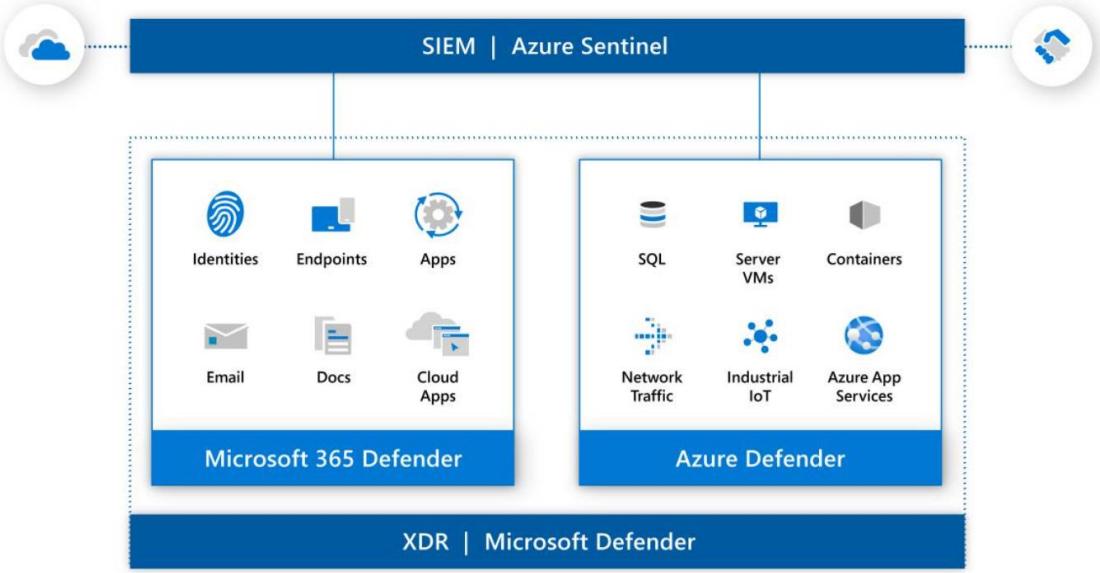


Figure 14. XDR -Microsoft Defender [25].

4.2.8 Security Incident and Event Management (SIEM) Tools from Cloud

A SIEM tool collects and combines data from event sources across an organization's IT landscape, including devices, firewalls, networks, and clouds assets. It performs analysis of the collected data against security rules and analytics to identify potential security

issues within the enterprise. When a security event is identified, analysed and categorized, the organization security team will be alerted and prompted to investigate with the help of the SIEM tool and logged data.

SIEM tools can also function Security Orchestration, Automation and Response (SOAR) functions. SOAR enables the automation incident response procedure. Automated responses could include blocking IP addresses on a firewall or IDS system, suspending user accounts or quarantining infected endpoints from a network. Figure 13 from IBM (International Business Machines) illustrates the investigation funnel needed from SIEM point of view to respond to the threat.

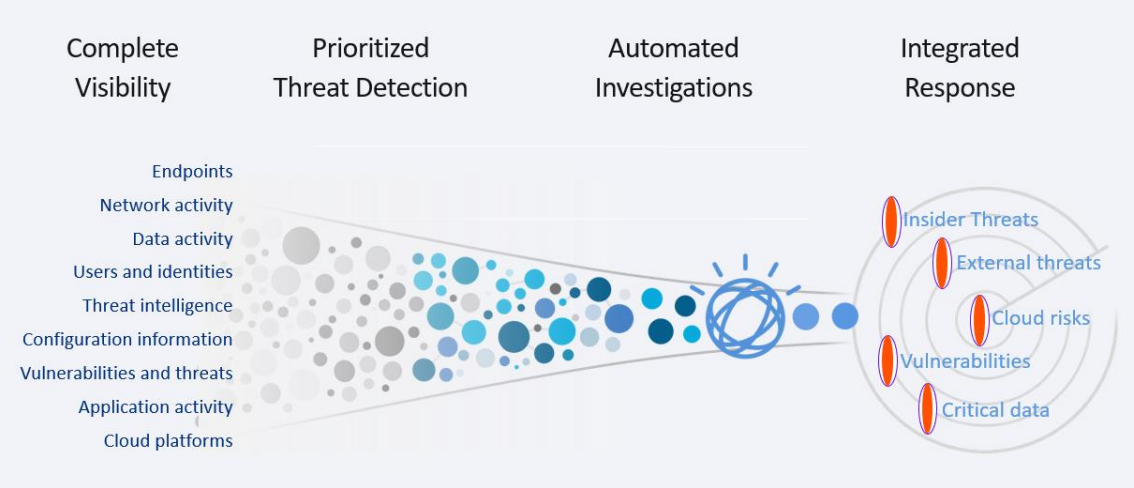


Figure 15. Four pillars of effective SIEM (And SOAR) [26].

To achieve visibility to cyber threats it is important that the organization defines and documents in advance what kinds of data they are logging. This is needed in order to understand whether logged data is sufficient or if there are additional data sources required for logging.

Azure Sentinel is a cloud based SIEM and SOAR tool from Microsoft running on the Azure platform. Azure Sentinel connects with various data sources and performs data correlation across these sources. Azure Sentinel identifies suspicious activities and threats. With Azure Sentinel automating routine responses to recurring types of alerts which is done with Azure Logic app playbooks and Python code. The query language used for investigation is KQL.

4.2.9 Verifying State of Security

The organization defence postures, and the depth of defence can be mapped against frameworks like Cyber Kill Chain (Lockheed Martin) or MITRE ATT&CK framework. The ATT&CK framework represents real-world cyberattack scenarios. Most cloud providers are mapping their product with that and refer to the ATT&CK terminology. The frameworks methods are commonly used by an attacker to gain access, to move further into the environment and to execute on end goals. The Cyber Kill Chain assumes a traditional perimeter-focused defence where a firewall is the main line of defence and so fails to cover other attack vectors and internal attack paths [27]. Figure 16 describes MITRE ATT&CK techniques identified for Microsoft Office 365

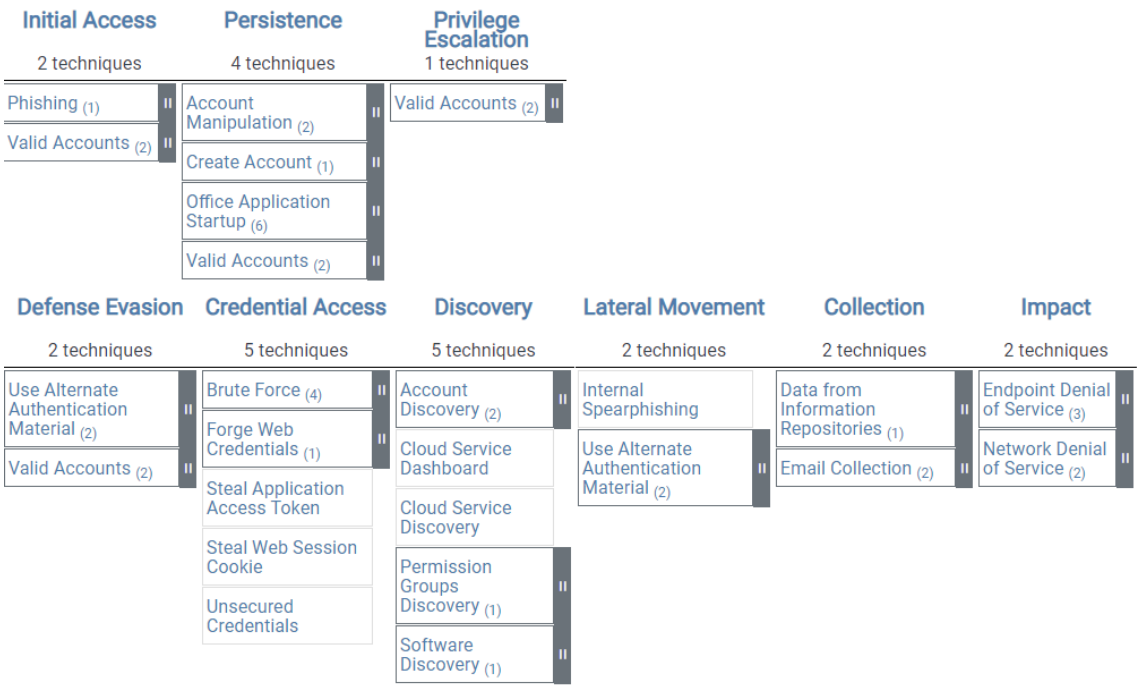


Figure 16. MITRE ATT&CK knowledgebase attack techniques for Office 365 [35].

Microsoft Office 356 includes Secure score application. Secure score allows the organization administrator to see the analysis of Microsoft Office 365 security state and receive recommendations on how to improve it.

5 Results and Analysis

In the analysis phase the requirements mapping conducted for customer is described in section 5.1 and Appendix one. Section 5.2 and appendix two is for testing Azure Sentinel and finding automation baseline for it. Sections 5.3 is for analysing the Detection capabilities of Microsoft security tooling and the section 5.4 is the security tools proposed for customer

5.1 Defining requirements for H-Corp End user cybersecurity

Definition work of the cybersecurity requirements are following for SABSA model. The definition process is started from Business requirements mapping and will go from layer to layer to component level architecture (product mapping).

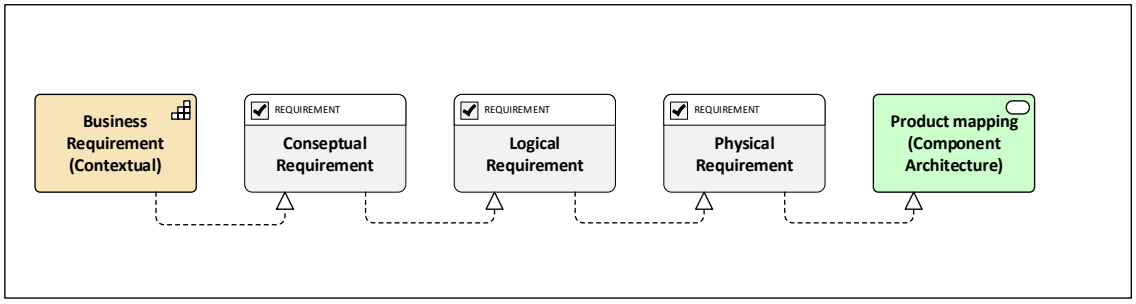


Figure 17. Requirement process flow.

Figure below illustrates how the business strategy statement will be refined as product mapping. The code inside textbox is for mapping requirements together described in Appendix 1.

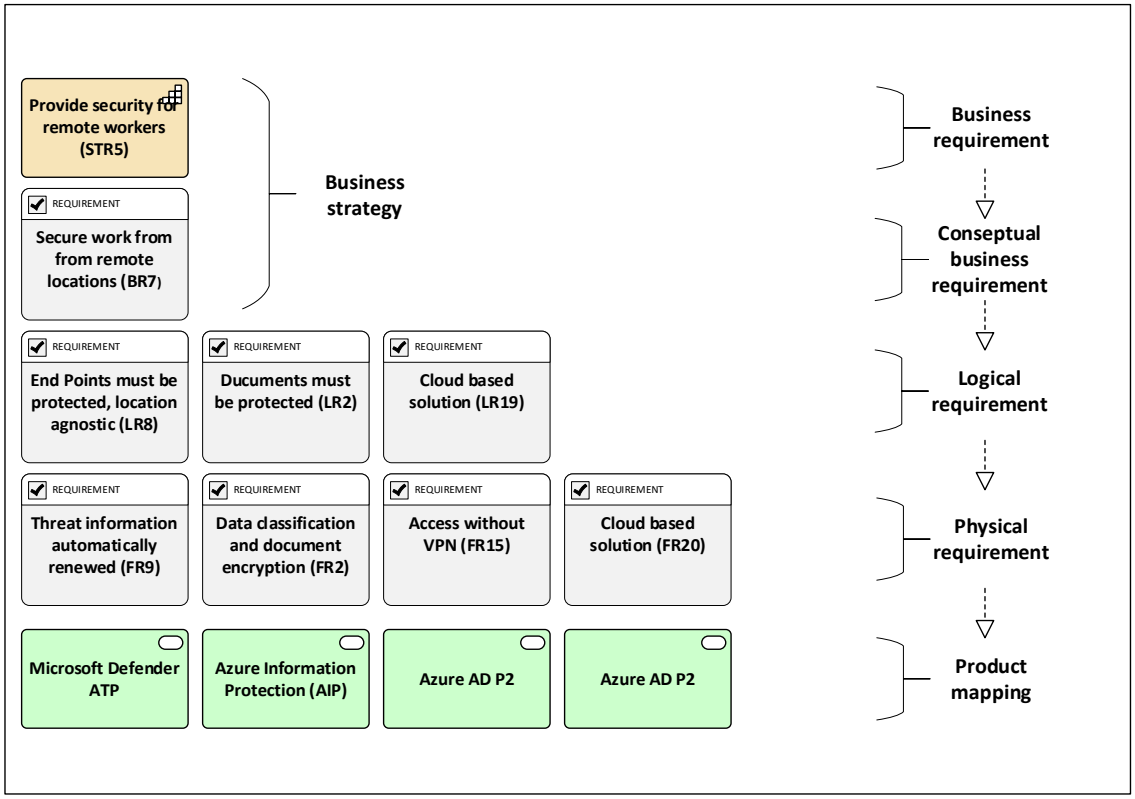


Figure 18. Example of individual requirement process flow.

Appendix 1. contains full requirement mapping for the customer.

5.2 Analysing the security automation

For Azure AD P2 and other EM+S licenced security applications Microsoft offers best practises and security baseline described in Appendix two. After the Microsoft security applications are activated and the first line automation baseline created the alerting and logging should be connected to Azure Sentinel and the SOAR automation baseline should be created with automation playbooks.

Analysis for the Azure Sentinel automation was conducted with small proof of concept test environment. It included Office Microsoft 365 E5 licensed environment connected with Azure Sentinel. The main goal of analysis was to find if there is ready-made security and automation baseline for Office 365 and Azure Sentinel.

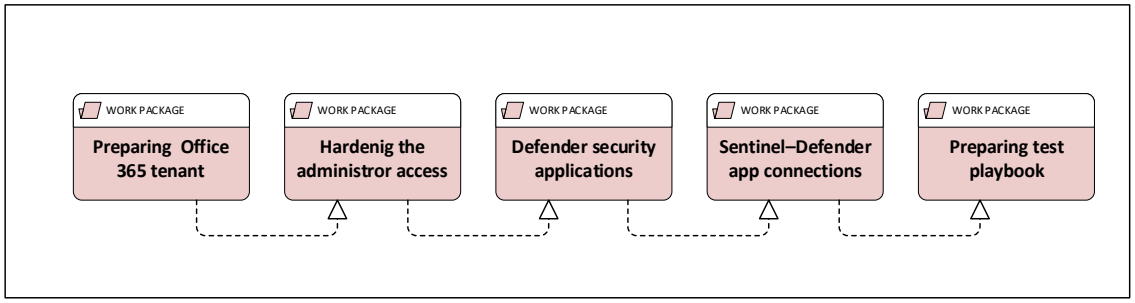


Figure 19. Azure Sentinel test process.

There are ready made connectors (August/2020) for connecting Office 365 data sources:

- Azure AD
  - Directory Sign-In logs
  - Directory Audit logs
- Azure AD Directory Identity Protection
- Azure Activity alerts to Azure Sentinel (for protecting the Sentinel)
- Office 365 alerts
  - SharePoint
  - Exchange
  - Teams (Preview)
- Cloud App Security alerts
  - Alerts
  - cloud discovery logs
- Office 365 ATP alerts (Defender for Office 365)

During the time this thesis was conducted, Microsoft added more connectors including Microsoft Defender for Endpoint and Azure Information Protection. The Azure automation baseline for Microsoft End User applications and Azure Sentinel could not be found from GitHub. It needs to be created from scratch. The GitHub Sentinel playbooks could be the starting point.

5.3 Analysing the detection capabilities

Identifying the detection capabilities of Microsoft security tool stack relays on reports from SE labs and AV TEST Institute.

Microsoft Defender for Endpoint got a good result from SE labs analysis Q4/2020 [32]. Old defender naming was used in the report. The tested software version can be found from the report. Figure 19 indicates the analysis.

TOTAL ACCURACY RATINGS			
Product	Total Accuracy Rating	Total Accuracy (%)	Award
Broadcom Endpoint Security Enterprise Edition	1,150	100%	AAA
Kaspersky Endpoint Security	1,149	100%	AAA
Microsoft Defender Antivirus (enterprise)	1,146	100%	AAA
McAfee Endpoint Security	1,139	99%	AAA
FireEye Endpoint Security	1,106	96%	AAA
Sophos Intercept X	1,080	94%	AA
Crowdstrike Falcon	1,072	93%	AA

Figure 20. SE Labs Detection capabilities analysis, End Point Detection software [32].

Tests conducted by SE Labs was done with threats created using publicly available free hacking tools, can mean that it was easy to get good results by vendors.

AV TEST Institute protection part was composed of two stages [34].

> Stage 1 – Test of the protection function: protection against 0-day malware attacks from the Internet, inclusive of web and e-mail threats (real-world testing)
>
> Stage 2 – Test of the detection function: detection of widespread and prevalent malware discovered in the last 4 weeks (the AV-TEST reference set).

Microsoft Defender ATP scored good results on test conducted 10/2020. Test results described figure below.

	Industry average	September	October
Protection against 0-day malware attacks, inclusive of web and e-mail threats (Real-World Testing) 334 samples used	97.9%	100%	100%
Detection of widespread and prevalent malware discovered in the last 4 weeks (the AV-TEST reference set) 12,316 samples used	100%	100%	100%
Protection Score	6.0/6.0		

Figure 21. AV TEST Institute test results for Microsoft Defender ATP.

For getting organised view of protection the MITRE ATT@CK framework was used as reference. The Microsoft End User security tool stack was compared against ATT@CK office 365 Matrix [35]. Figure 22 below illustrates the comparison in high level for Initial access threat. The Matrix contains information for the Office 365 platform with mitigation options.

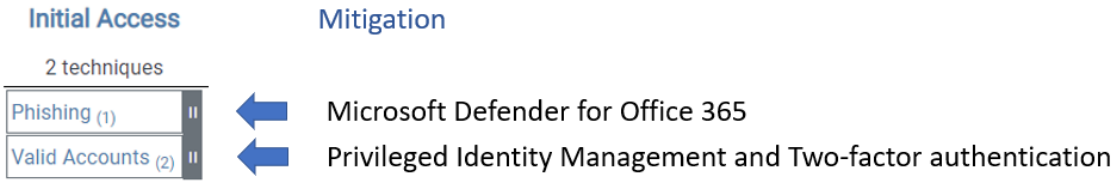


Figure 22, MITRE ATT@CK Initial access

5.4 Decisions after the analysis

The Microsoft E5 security license bundle will be proposed as the security solution. The reasoning behind the decision is:

- H-Corp is already using Microsoft ecosystem (Office 365 and Microsoft Azure). This means that Microsoft security is a natural fit.
- Microsoft E5 security complies to the requirement mapping.
- Microsoft E5 security solutions function together as unified engine, supporting the threat hunting and automation.

- Gartner named Microsoft a Leader in 2019 Endpoint Protection Platforms Magic Quadrant [31].

  Microsoft E5 security license bundle contains following security SaaS applications.

  - Microsoft Defender for Endpoint (End point protection).
  - Azure AD P2 (Cloud-based identity database with security functions).
  - Microsoft Defender for Office 365 (Cloud-based security solution).
  - Cloud app security (cloud base security solution).
  - Microsoft Defender for Identity (Security solution for protecting the on-premises AD/Domain identities (out of this thesis scope).

By unifying incident response process by integrating key capabilities across Microsoft Defender for Endpoint, Microsoft Cloud App Security, Microsoft Defender for Office 365, Microsoft Defender for Identity, Azure AD P2 and Azure Sentinel (SIEM/SOAR) creates the complete security solution with automation and SOAR options.

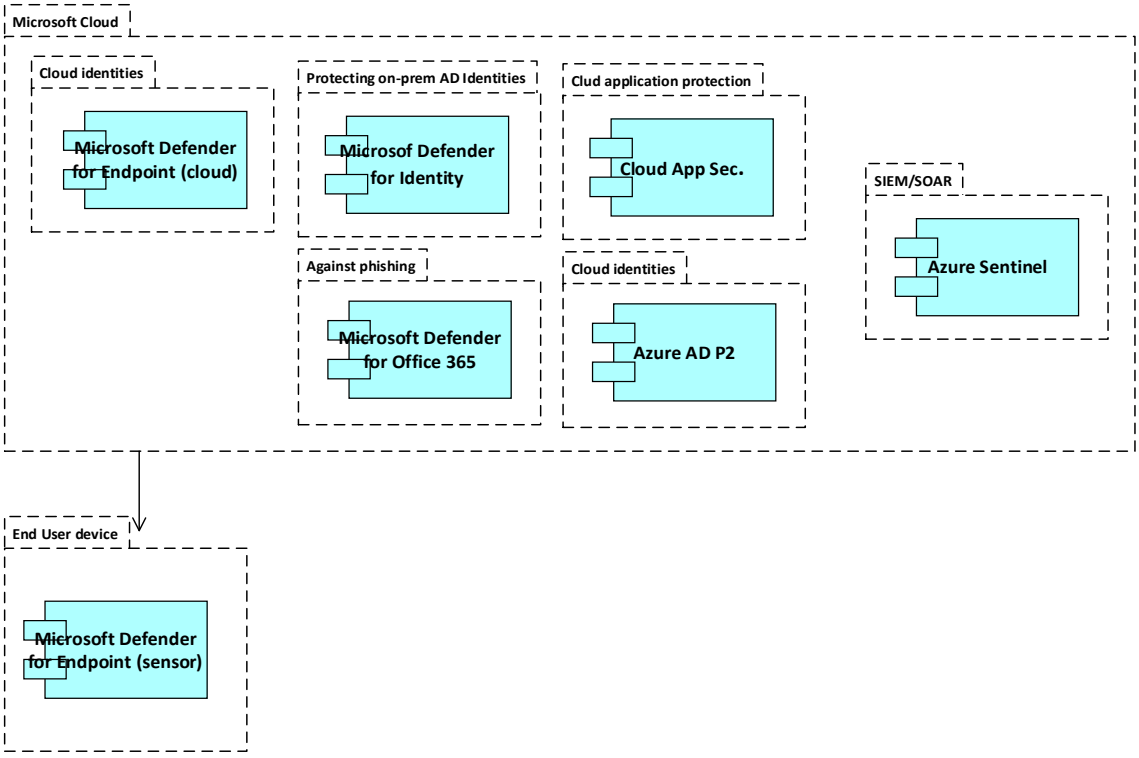


Figure 23. Microsoft security services in scope (Excluding Microsoft Defender for Identity).

Azure Sentinel will be proposed as a one option for SIEM and SOAR product. The reasoning behind the decision.

- Azure Sentinel complies with the requirement mapping
- Azure Sentinel fits to Microsoft ecosystem (Microsoft product)

Reminding customer that Azure Sentinel is not a silver bullet, investment and employees needed for creating security baseline and taking care of it for the future. Azure Sentinel is a SIEM/SOAR platform and the building work on platforms needs to be done.

6 Discussions and Conclusions

When using SABSA there seems to be a risk of losing focus and get overwhelmed with the functions. Using the SABSA should be tailored for choosing just the needed functions. The big picture should be kept in mind when defining the cybersecurity for organization.

For defining the organization cybersecurity, the following top to down approach can be taken. The security postures can be defined with SABSA model and ISF SOGP model could be used in that same process. After that the NIST framework can be utilized as a baseline and Mitre ATT&CK framework could be used for evaluating the state of security and use cases.

Securing the end user cloud environment differs significantly from securing the traditional firewall protected on-premises environment. Access to traditional on-premises environment will be done via VPN connection from one access point and the protection is mainly based on protecting that access. The cloud environment gives a lot of benefits what comes to devices, user access and collaboration but the freedom of choice raises the complexity of needed security model (zero-trust model).

Cloud based environment is more standardised and the responsibility for infrastructure is on the cloud vendor side. This helps mitigate the risks with infrastructure and IT-architecture. On-premises environment can be built by company itself and the infrastructure and IT-architecture depend on the skillsets of builder.

The pre-defined policies and governance is highly important with the cloud for getting control of whole entity. For those activities there is no mind to “invent the wheel” again. The starting point should be specific cloud vendor’s own best practises and baselines.

All cloud vendors have their own tooling for protecting their cloud entities. After the decision which cloud platform will be implemented the most reasonable way is to first investigate the cloud vendors own tooling. The cloud vendor has best insights and best methods to provide the basic security tooling for their own cloud. The missing gaps and extra security can be added with third party products. Example of such a third-party tool could be vulnerability management.

Relying on cloud vendor's own tooling could be more cost effective, the vendor pricing for tooling is done usually more desirable that external dedicated tool vendor by vendor. This is depending highly on what kind of assets need to be protected and where.

Azure Sentinel is reasonable new technology from Microsoft. It is more a security platform than product, where company can start to build up the automation routines. When testing and trying to define the security baseline with (Azure Sentinel and Microsoft End User Area tooling) the experience was fragmented from Azure Sentinel side. Company should not underestimate the investment and new skilling needed for that.

Observations from Azure Sentinel tests

- New features and functions almost weekly based
    - Negative side for this is that there needs to be allocated recourses to follow the new features and functions
    - Positive side for this is that Microsoft does constant development and the platform is evolving against new threats and automation.
- No clear security baseline from Microsoft side (August 2020). There are ready made plans in GitHub for certain tasks but no silver bullet for whole baseline. If utilizing community-based code, it needs to be reviewed carefully to understand what the code does.
- The Sentinel user interface is difficult to understand with all different consoles and different naming. The "feeling" of full control is missing at out of the box stage. This can be achieved with creating that security baseline with automation and playbooks, it takes time and money from company. It is also possible to set real-time automation as to fully automate a defined response to particular security alerts.
- The staffing and finding skilled subject matter experts for Azure Sentinel is an aspect that should be taken in consideration.

References

1 SABSA < https://sabsa.org/sabsa-executive-summary/#:~:text=SABSA%20ensures%20that%20the%20needs,methodology%2C%20not%20a%20commercial%20product.// >. Accessed 08 Dec 2020

2 Microsoft < https://docs.microsoft.com/en-us/azure/compliance// >. Accessed 08 Dec 2020

3 Sherwood J. Clark A. Lynas D., Enterprise Security Architecture, CMP Books. 2005.

4 Dotson C., Practical Cloud Security: A Guide for Secure Design and Deployment. O'Reilly Media. 2019

5 Amazon Web Services, compliance < https://aws.amazon.com/compliance/shared-responsibility-model/ >. Accessed 20 Nov 2020.

6 ISF, Standard of Good Practice for Information Security. Information Security Forum Limited. 2020

7 ICASA < https://www.isaca.org/resources/cobit>. Accessed 20 Nov 2020.

8 Microsoft < https://docs.microsoft.com/en-us/azure/governance/azure-management / >. Accessed 23 Nov 2020.

9 European Union / GDPR, Regulation (EU) 2016/ 679 of the European Parliament and of the council. 2016

10 Amazon Web Services, developer guide < https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-control-access-to-api.html/ >. Accessed 20 Nov 2020

11 Microsoft, < https://docs.microsoft.com/en-us/power-platform/admin/governance-considerations/ >. Accessed 05 Dec 2020.

12 Microsoft < https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/privileged-access-workstations/ >. Accessed 05 Dec 2020.

13 Azure Training Series, Kumar N. < https://azure-training.com/2020/06/02/manage-identity-and-access-in-azure-ad-part-1/5/ >. Accessed 05 Dec 2020

14 Google < https://cloud.google.com/blog/products/identity-security/introducing-cas-a-cloud-based-managed-ca-for-the-devops-and-iot-world>. Accessed 05 Dec 2020.

15 Microsoft Digital Defence Report 2020 September. Microsoft. 2020.

16 CSA Reference Architecture. < https://cloudsecurityalliance.org/artifacts/tci-reference-architecture-v2-0/ >. Accessed 05 Dec 2020.

17 Microsoft, Microsoft Cybersecurity Reference Architecture 2018. < https://www.microsoft.com/security/blog/2018/06/06/cybersecurity-reference-architecture-security-for-a-hybrid-enterprise/ >. Accessed 20 Nov 2020

18 Microsoft, < https://docs.microsoft.com/fi-fi/security/zero-trust/ >. Accessed 20 Nov 2020.

19 NIST, < https://www.nist.gov/cyberframework/online-learning/components-framework >. Accessed 08 Dec 2020

20 Microsoft, < https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/privileged-access-workstations > Accessed 20 Nov 2020.

21 NIST, National Institute of Standards and Technology. Special Publication 1800-18B. 2018.

22 Simmons Alex < https://techcommunity.microsoft.com/t5/azure-active-directory-identity/eight-essentials-for-hybrid-identity-3-securing-your-identity/ba-p/275843// >. Accessed 08 Dec 2020

23 Microsoft < https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection// >. Accessed 08 Dec 2020

24 Trend Micro < https://www.trendmicro.com/en_fi/business/products/user-protection/sps/endpoint.html>. Accessed 08 Dec 2020

25 Microsoft < https://www.microsoft.com/en-ww/security/business/threat-protection >. Accessed 08 Dec 20220

26 IBM. 4 pillars of effective SIEM (And SOAR). Conference Proceeding. 2020.

27 Cycraft < https://medium.com/cycraft/cycraft-classroom-mitre-att-ck-vs-cyber-kill-chain-vs-diamond-model-1cc8fa49a20f/ >. Accessed 20 Nov 2020.

28 Vehent J., Securing DevOps, Manning Publications Bo. 2018.

29 Bergh D., Deogun D., Sawano D., Secure by Design. Manning Publications Co. 2019

30 Weldon M., The future X netwfork a Bell Labs perspective. CRC press. 2015.

31 Microsoft < https://www.microsoft.com/security/blog/2019/08/23/gartner-names-microsoft-a-leader-in-2019-endpoint-protection-platforms-magic-quadrant// >. Accessed 17 Jan 2021.

32 Se Labs < https://selabs.uk/reports/enterprise-endpoint-protection-2020-q4/ >. Accessed 19 Jan 2021.

33 Microsoft < https://www.microsoft.com/security/blog/2019/11/14/security-incident-response-utilizing-cloud-dart-tools-techniques-procedures-part-1/ >. Accessed 19 Jan 2021.

34 AV TEST institute < https://www.av-test.org/en/antivirus/business-windows-client/windows-10/october-2020/microsoft-defender-antivirus-4.18-204116/ > Accessed 24.11.2020.

35 MITRE ATT&CK < https://attack.mitre.org/matrices/enterprise/cloud/office365/ > Accessed 06.01.2021.

Requirements mapping

Business requirements

Requirement code	Strategic objective	Rationale
STR1	Enable the shift to cloud	From Capex to Opex. Get rid of on-premises servers and stop protecting just the front gate. Flexibility and scale.
STR2	Secure the company data and assets	Company data should be protected and monitored.
STR3	Secure the customer data	Customer data should be protected and monitored
STR4	Secure the business globally	Secure all business locations.
STR5	Provide security for remote workers	Should be able secure the company data wherever the End-User is located.
STR6	Cost of security should not be too high.	Security level should be reasonable, but security functions should not be too expensive.
STR7	Security should be flexible and should support rapidly the business initiatives.	Business is the driving force and security should be able to support the Business.
STR8	Measurability	Provide evidence of the security state.
STR9	Cybersecurity is aligned with all ICT functions.	Cybersecurity is taken in consideration in all phases; architecture, operations, including the decommission of services.

Conceptual requirements

Requirement code	Requirement	Rationale	Mapping with Business requirement
BR1	The solution must meet the industry standard cybersecurity best practices and industry regulations.	The security must be high enough level to make the business unwanted target. Data and assets should be protected by following industry standard best practices at minimum.	STR2, STR8
BR2	The solution must ensure the business continuity in event of Cyber threat.	AV signatures should be up to date. SOAR automation should be in place.	STR2
BR3	Automation	SOAR automation and threat hunting should be possible.	STR2, STR6, STR7
BR4	Disaster recovery	Disaster recovery plan documents should be in place and have clear ownership	STR2, STR9
BR5	Risk management	Information security risks must be identified, quantified, and managed	STR8
BR6	End-User satisfaction	The solution should not disturb End-Users work. The solution should give confidence to End-Users that they are protected.	STR7, STR9
BR7	End-User working habits	End-Users should be able to work securely from remote locations and also with mobile devices.	STR5, STR9
BR8	Company, customer data and company devices must be protected	Company-, customer data and company devices must be protected	STR2, STR3, STR8

BR9	Security monitoring	Options to monitor the security and remediate the violations should be in place	STR2, SRT4
BR10	The Identity and access management (IAM) toolset must be agile enough to support the business	Avoiding the bottlenecks when business orders new IAM services - Business to Business, IoT etc.	STR7
BR11	The security project cost should not be too high	The transformation project price should not be too high. (The project enabling the new features). Rough Order of Magnitude (ROM) estimation of needed resources and -manhours should be done.	STR6
BR12	Running cost of the solution should be reasonable	The cost of the solution should not be too high.	STR6
BR13	Cloud-based solution	Cloud-based solution for avoiding on-premises servers and datacentres	STR1
BR14	Solution should be provided from one or two vendors	To avoid the complexity. Preferred that solution would work together as unified engine.	STR6
BR15	Solution should be cloud-based and support for multi cloud environment.	To avoid unnecessary on-premises servers and for supporting the shift to cloud. Operating with IaaS if servers are needed (public cloud).	STR4, STR6
BR16	Apply zero-trust model.	Protecting the data wherever it is located.	STR2
BR17	Partner identities	Partner identities should be protected	STR3
BR18	Complete Cybersecurity protection	Prevent, detect, respond and recover	STR9

Logical business requirements

Requirement code	Requirement	Rationale	Mapping with conceptual business requirements
LR1	Confidentiality	Data must be protected at transit and at rest.	BR1, BR8
LR2	Data protection	Documents must be protected.	BR16
LR3	Authentication	Authentication must be secure.	BR16,
LR4	Authentication must be risk based	Authentication options must be risk based.	BR6, BR7
LR5	Audit trail	Audit trail must exist	BR9, BR18
LR6	Base level security policies	Baseline security policies documented.	BR5
LR7	Automation for remediating threats	SOAR options, SIEM options	BR2, BR3, BR11
LR8	End Points must be protected, location agnostic	Workstations and devices must be protected at all time and all locations	BR8
LR9	Applications must be protected	Applications, cloud and on-premises must be protected	BR1
LR10	Visibility to Cyber threats	Overall visibility to company Cyber threads	BR5
LR11	Easy to use	Cybersecurity needs to be invisible to end-Users. Easy to use operations from End-User perspective.	BR6, BR7
LR12	Administrative access	Administrative access needs to be high secure.	BR1
LR13	Partner users' needs access	Partner user access	BR17

LR14	Processes for new and leaving users/Administrators needs to be in place	Processes will be aligned with HR system. Clear ownership wil be defined	BR10, BR17
LR15	Vendor lock	Risk of vendor lock needs to take in consideration	BR12
LR16	Baseline policies needs to be created and documented	Living documents needs to be created with clear ownership.	BR1
LR17	Disaster recovery process needs to be defined.	Disaster recovery will be aligned the policies and retention times.	BR4
LR18	State of security needs to be benchmarked	Reflecting security with some industry framework	BR1
LR19	Cloud-based solution	The solution will rely on public cloud.	BR13, BR14, BR15
LR20	Prevention of security incidents	Security based on threat intelligence	BR17
LR21	Zero-trust model	Protecting the data wherever it is located. Principle of least privilege. AI and Risk based access control.	BR16
LR22	Agile Identity and Access Management (IAM) options	IAM must support business	BR10
LR23	Security following the industry best practices	SOGP framework	BR1

Physical business requirements

Requirement code	Requirement	Rationale	Mapping with Logical requirement (TAB Logical requirements)
FR1	Encryption	Data must be encrypted at transit and at rest.	LR1
FR2	Data Classification and document encryption	Data Classification and document encryption	LR11
FR3	Authentication	Two factor authentications.	LR3
FR4	Conditional access	Possibility provide conditional access and force authentication based on risk level	LR4, LR11
FR5	Audit trail	Logs and named accounts	LR5
FR6	Access control	Role based access control (RBACK).	LR21
FR7	Base level security policies	Baseline security policies documented, and document ownership defined.	LR16
FR8	Automation for remediating threats	Security Orchestration, Automation and Response (SOAR) for protecting the baseline and lowering the long-term cost.	LR7
FR9	End Point protection	End Point protection with threat information automatically renewed or up to date Realtime	LR8
FR10	Protection against phishing Emails	Automatically identifying phishing attacks	LR9, LR11
FR11	Protection against malicious links	Automatically identifying malicious links	LR9, LR11
FR12	Identifying shadow IT	Whitelisted and blacklisted applications	LR9
FR13	Possibility to protect cloud applications	Applications from endpoint and cloud must be protected	LR9

FR14	Possibility for aggregating the alerts From SIEM to SOC must exists	SIEM (Security Incident and Event Management). SOC Security Operation Centre (team for monitoring the security).	LR7
FR15	End-User access to company data and assets without VPN	Identity and Access management, cloud-based. No need to access recourses via. Company firewall.	LR19, LR21, LR22
FR16	Password reset	Self-service password reset must exist and be secure	LR11
FR17	Just in time access and granular access for administrators	Administrative access just for the needed usage for needed time period. The principle of least authority	LR22, LR23
FR18	Partner accounts	Possibility to create accounts to partners.	LR22
FR19	Administrative access only from defined/protected workstation	The workstations where administrative actions will be done, should be highly protected	LR23
FR20	Cloud-based solution	The solution will rely on public cloud.	LR19
FR21	Preventive security	Security protection is based on threat intelligence	LR10
FR22	Break a class account	Break a class administrative accounts for emergency use.	LR23
FR23	Process for evaluating the administrator rights	Process with ownership for evaluating administrative rights	LR6
FR24	HR process for creating new users	Automated process for creating new users - depending HR system.	BR10
FR25	HR process for denying access for left users	Denying access for left users and partner account. Automated process	LR14
FR26	Study for avoiding security vendor lock and exit strategy	To be created	LR15
FR27	Disaster recovery plan	To be created	LR17

FR28	Company internal Security Audit plan	To be created	LR23
FR29	Security solution evaluated by external auditor. Evidence from solution provider	Needs to be evaluated	LR23
FR30	Vulnerability management	Is there some Gaps that solution provider does not cover, needs to take in consideration	LR23
FR31	Documenting the security baseline	documenting and ownership for security baseline and policies	LR6
FR32	Security and solution evaluated against MITRE ATT&CK framework	MITRE ATT&CK is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. The Security solution must be reflected against MITRE ATT&CK	LR23
FR33	Security solution vendor compliance		LR23

Product mapping

Requirement code	Rationale	Mapping the functional requirement with products	information
PR1	Data must be encrypted at transit and at rest.	FR1	Office 365 data is encrypted as REST and TRANSIT. Email can go as plain text to other Email servers (outside Microsoft ecosystem).
PR2	Data Classification and document encryption	FR2	Azure Information Protection (AIP) enables data classification and Document encryption.
PR3	Two factor authentication (MFA).	FR3, FR15	Azure AD P2 enables MFA
PR4	Possibility provide conditional access and force authentication based on risk level	FR4	Azure AD P2 enables the risk based conditional access (Azure AD Identity protection)
PR5	Logs and named accounts	FR5	Named accounts is through corporate IT policy. Azure AD P2 and Azure Ad Identity protection can be connected to Azure Sentinel
PR6	Access Control lists (ACL) , Role based access control (RBACK).	FR6	Azure AD P2 acts as Identity Database. Azure AD P2 enables granular role-based access control (RBACK).

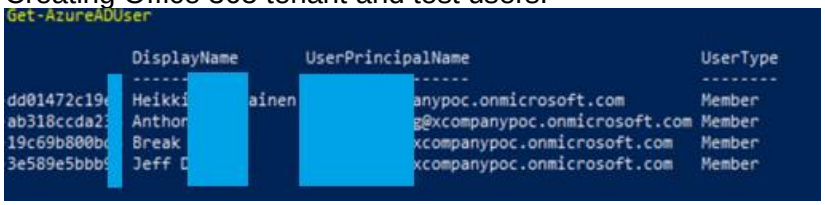
PR7	Baseline security policies documented, and document has owner.	FR7	Baseline policies. Document owner needs to be agreed.
PR8	Security Orchestration, Automation and Response (SOAR) for protecting the baseline and lowering the long-term cost.	FR8	Azure Sentinel is the Security Orchestration Automated Response (SOAR) solution,
PR9	End Point protection with threat information signatures automatically renewed	FR9	Microsoft Defender ATP is the End Point Protection solution. Microsoft Defender ATP can be connected to Azure Sentinel
PR10	Automatically identifying phishing attacks	FR10	Office 365 ATP P2 is for identifying phishing attacks
PR11	Automatically identifying malicious links	FR11	Office 365 ATP P2 is for identifying malicious links
PR12	Whitelisted and blacklisted applications	FR12	Blacklisting applications with Cloud App Security
PR13	Applications from endpoint and cloud must be protected	FR13	Cloud App Security protects the SaaS apps from cloud
PR14	SIEM (Security Incident and Event Management). SOC Security Operation Centre (team for monitoring the security).	FR14	Azure Sentinel is the Security Orchestration Automated Response (SOAR) solution,
PR15	Identity and Access management, cloud-based. No need to first access via. Company firewall.	FR15	Azure AD P2 as a identity database. Azure AD P2 application portal.
PR16	Self-service password reset must exist and be secure	FR16	Self-service password reset is Azure Ad P2 feature
PR17	Administrative access just for the needed usage for needed time period. The principle of least authority	FR17	Privileged Identity management (PIM) is Azure AD P2 feature

PR18	Possibility to create accounts to partners.	FR18	Partner accounts needs Azure AD P2 licensing in ratio of 1/5. Azure Ad B to B
PR19	The workstations where administrative actions will be done, should be highly protected	FR19	Privileged Access Workstation (PAW) is the preferred method.
PR20	The solution will rely on public cloud.	RF20	Relying on Microsoft Cloud
PR21	Break a class administrative accounts for emergency use.	FR22	Break a class Global administrator account will be created
PR22	Process with ownership for evaluating administrative rights	FR23	Process need to be created. Azure AD P2 enables Access review feature.
PR23	Automated process for creating new users - depending HR system.	FR24	HR process needs to be created
PR24	Denying access for left users and partner account. Automated process	FR25	Process need to be created. Azure AD P2 enables Access review feature.
PR25	Study for avoiding security vendor lock	FR26	Exit strategy options needs to be investigated
PR26	Disaster recovery plan with clear ownership	FR27	To be created
PR27	documenting and ownership for security baseline ans policies	FR31	Relying on Microsoft security features and recommendations
PR28	MITRE ATT&CK is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. The Security solution must be reflected against MITRE ATT&CK	FR32	To be created
PR28	Threat intelligence	FR21	Azure AD P2 identity protection uses the Microsoft

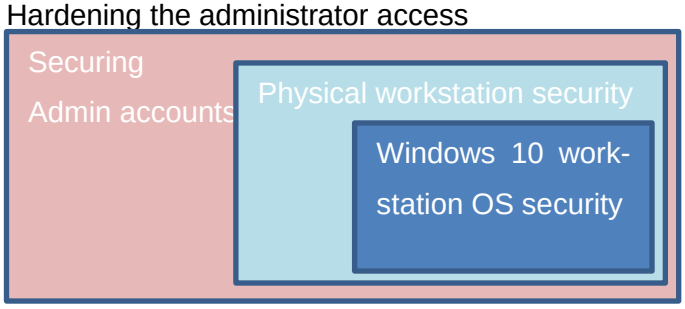
			threat intelligence to identify risk.
PR29	Security solution vendor compliance	FR33	Microsoft compliance centre
PR30	Company internal audit plan	FR28	To be created
PR31	Security solution provider audits	FR29	Needs to be verified
PR32	Is there some Gaps that solution provider do not cover, needs to take in consideration	FR30	Needs to be planned

Testing Azure Sentinel automation

Creating Office 365 tenant and test users.



Hardening the administrator access



Securing Administrator Accounts

- Creating the emergency access administrator account
- Utilizing FIDO2 security keys on authentication
- Activating Azure AD Privileged Identity Management
- Adding Conditional Access controls to require strongest authentication level for admins
- Applying Intune security baseline
- Removing the Local administrator rights with Intune
- Monitor the administrative access with Azure Sentinel
- Limit the amount of Administrator roles using least privilege roles

Physical Workstation Security

- Setting password for intel AMT
- Setting very short suspend mode to enable the hibernation mode
- Disallowing the hybrid sleep
- Applying encryption, Bit locker
- Disabling un-needed services
- Disabling DMA interfaces

Windows 10 Enterprise Workstation OS Security

- Checking Windows 10 Security baseline - Specialized Compliance is a script
- Activating Windows Defender Credential Guard.
- Activating Windows Defender device guard. Whitelisting trusted applications
- Activating Microsoft defender for Endpoint
- Protected Users, Authentication Policies, and Authentication Silos
- Setting Windows firewall rules

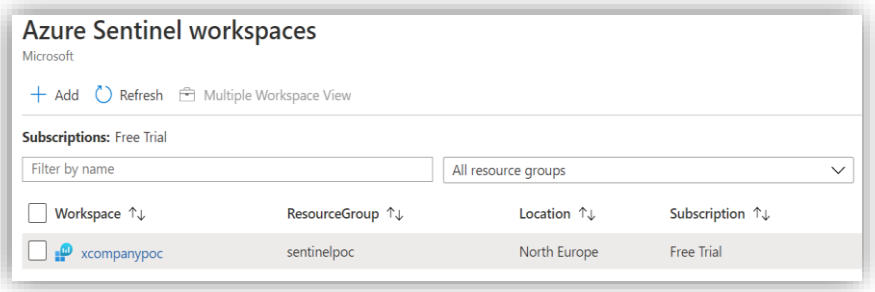
Activating Microsoft E5 Security Applications

-Cloud App Security
-Office 365 ATP
-Checking Azure AD P2

Setting up Azure Sentinel

Creating Log Analytics workspace

Subscription	free trial
resource group	sentinelPOC
Instance name	xcompanypoc
Region	North Europe
Adding Azure Sentinel to Log Analytics workspace	xcompanypoc
Connecting Azure AD with Azure Sentinel	
Integrate Azure AD Logs with Azure Monitor (Log Analytics)	



Connecting Azure Sentinel connectors

Connecting Azure AD alerts to Azure Sentinel (connector)

-Azure Active Directory Sign-in logs
-Azure Active Directory Audit logs

Connecting Azure Active Directory Identity Protection alerts to Azure Sentinel (connector)

-Azure Active Directory Identity Protection

Connecting Azure Activity alerts to Azure Sentinel (connector) (for protecting the Sentinel)

-Azure Activity

Connecting Office 365 alerts to Azure Sentinel (connector)

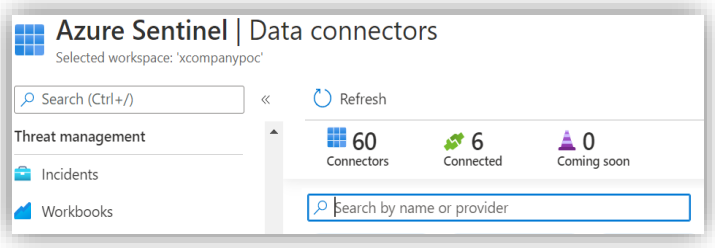
-Exchange -SharePoint -Teams (Preview)

Connecting Cloud App Sec alerts to Azure Sentinel (connector)

-Alerts -Cloud Discovery Logs (Preview) -Create incidents automatically from all alerts generated in this connected service -Enabled

Connecting Office 365 ATP alerts to Azure Sentinel (connector)

-Data that is collected by Office 365 Advanced Threat Protection service

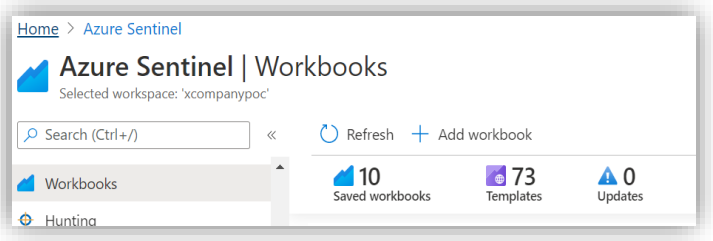


Adding Workbooks

Adding Microsoft recommended workbooks	Provider	Related to Connector
Azure AD Audit logs	Microsoft	Azure AD
Azure AD Audit, Activity and Sign-in logs	Sentinel Community	Azure AD
Azure AD Sign-in logs	Microsoft	Azure AD
Insecure Protocols	Microsoft	Azure AD
Azure activity	Microsoft	Azure
Microsoft Cloud App Security - discovery logs	Microsoft	Cloud app security
Exchange Online	Microsoft	Office 365
Office 365	Microsoft	Office 365
SharePoint & OneDrive	Microsoft	Office 365
Security alerts	Microsoft	Office 365

Entity behavior - activation

Data source, Audit Logs Data source, signing logs



Adding connector for Logic apps

Azure Sentinel Logic Apps connector	Using Administrative Identity (August 2020) note; new feature managed Identity in the Logic Apps resource (January 2021)

Table below from Microsoft describes the different types Azure Sentinel automation tools.

Contribution	Enables...
Playbook	setting up automated procedures while responding to threats
Workbook	data insights and monitoring with visualizations
Hunting	quick start security threat hunting capabilities with queries
Notebook	advanced hunting capabilities using Jupyter / Azure Notebooks
Analytic Rule Template	customized alert generation and automated incident creation with queries
Investigation Graph	full investigation scope discoverability with queries
Data Connectors	collect data at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds

Azure Sentinel includes built in workbooks for visualizing the Office 365 data and from GitHub more workbooks can be found.
Azure Sentinel don’t include readymade automation playbooks for Office 365.
There are some automation playbooks for Office 365 and Azure Sentinel at GitHub, general baseline and starting point for automation could not be found.