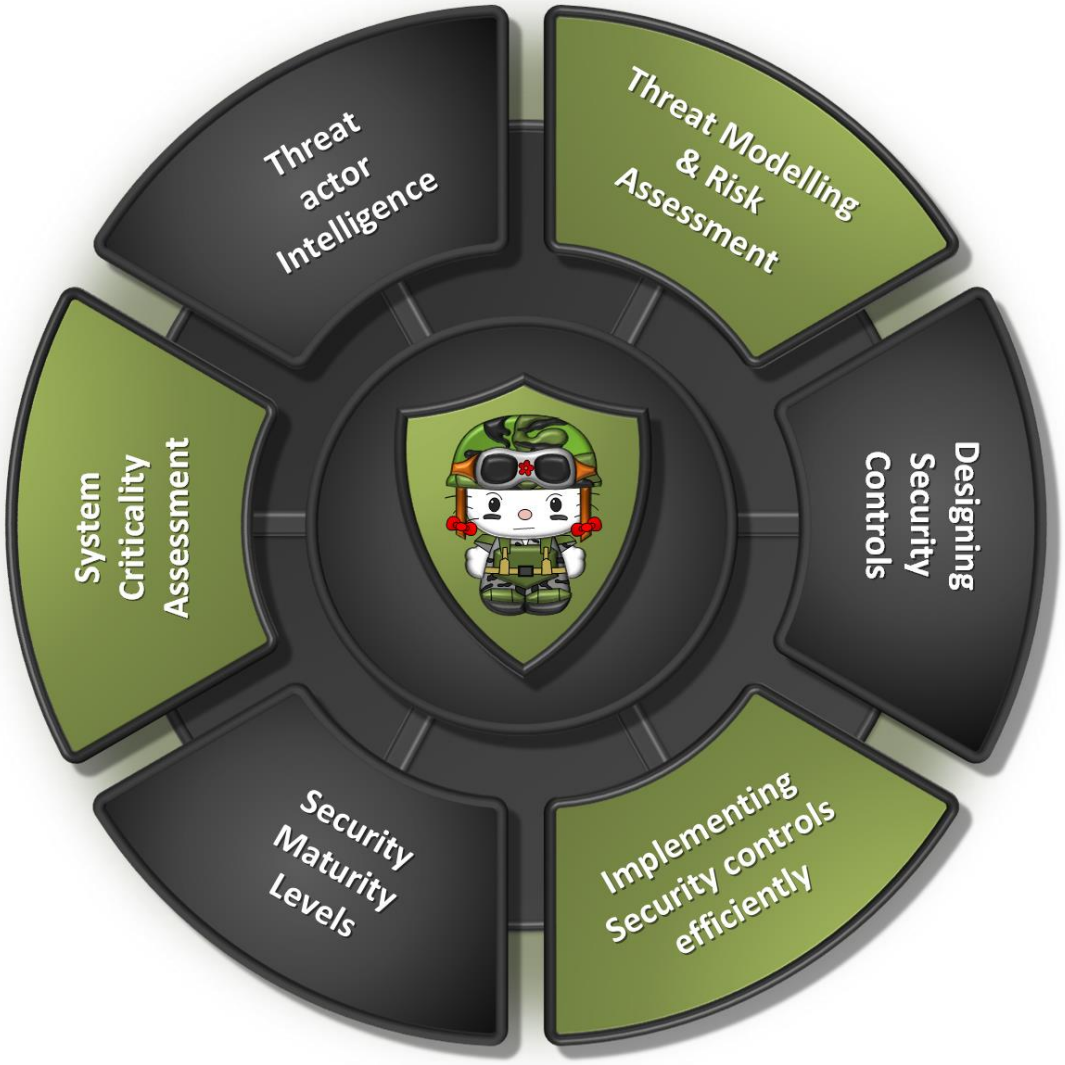
Defendable Architecture Guideline



Designing, Implementing & Defending a threat intelligence driven architecture

DAG-2020-002

Document Author: Erik Kvarvåg

Published 26.10.2023

Version 1.74

About the Author

As an IT professional devoted to technology Erik[1] provide more than 25 years of experience with the majority of time in key roles ranging from IT system administrator to network operations engineer and chief infrastructure & security architect in a tier one service provider operating in markets in both Europe and Asia.

Having spent most of his career within the telecom industry, Erik have seen technology evolve from dial-up modems into fiber access and 5G mobile networks. Always ready to dive into new technology or infrastructure areas to learn more about them but have in later years focused more on security related topics, both within the technology space as well as information security.

As Chief Security Architect with Telenor Group, a mobile operator focusing on Scandinavia and Asia with approx. 180 million customers[2] Erik regularly interacts with most major established and upcoming vendors in the Telecomm industry. The development on the virtualization of telecom operator networks makes IT infrastructure, virtualization and security skills extremely also relevant in the telco space and key development and focus have in later years been on NFV and cloud native technologies for 5G usage.

Among his many accomplishments you can find:

- Author of target architectures for cloud infrastructure and infrastructure security
- Design and delivery of NFVi platforms in Thailand, Malaysia, Pakistan, Bangladesh and Myanmar
- Design and delivery of IT datacenter networks in Norway, Pakistan and Malaysia
- Countless solution designs for various infrastructure projects in Telenor's business units
- Several technical whitepapers on cloud, infrastructure, security architecture and networking

Originally from Oslo, Norway, Erik decided that after spending several years on assignments in different places in Asia that friendly warm Thailand was a better place to stay than a country where half of the landmass is above the arctic circle and large parts of the year the temperature is in the range between -20C and 5C. Currently a Bangkok citizen with no intention of leaving soon greatly enjoying Thai food and developing a growing Hello Kitty obsession.

When not being glued in front of his work computer, Erik is a big fan of books and computer games, and enjoys movies to the extent that he built a complete home cinema in the basement of his house back in Norway to properly enjoy his sci-fi movie collection. Occasionally seen jogging in Benjakiti Park near Asoke.

[1] https://www.linkedin.com/in/erikkvarvag/
[2] https://www.telenor.com/about-us/telenor-at-a-glance/

Executive Summary

In recent years, the trend of cyber-attacks is continuing to point upwards. According to IBM X-Force 2020 report, over 8.5 billion records were compromised in 2019, a number that's more than 200 percent greater than the number of records lost in 2018. Ransomware was up 67% in Q4 of 2019 in a year-on-year assessment. This happens across a multitude of industries ranging from government to healthcare, manufacturing and telecom. As attacks grow in scale and sophistication a more intelligent and efficient approach is required to stay both secure and competitive at the same time.

Combining two well-known threat model methodologies, Process for Attack Simulation and Threat Analysis (PASTA) from Versprite with that of the threat driven Defendable Architecture (DA) model from Lockheed Martin gives birth to the concept of a "threat intelligence based, business driven defendable architecture".

This concept aims to apply security controls in a more targeted and efficient manner through the lifecycle of the infrastructure's design, build, operate and defend phases while at the same time utilizing threat modelling and analysis as a continuous process.

The combined methodology applies a multi-step process to align business objectives with technical requirements taking into account regulatory requirements, compliance and business impact. Security and technology experts can then use recommendations from industry frameworks such as ISO/NIST-CSF/CIS as a baseline, apply the principle of zero trust architecture "never trust, always verify" and then combined with a thorough analysis of identified threats, design a set of security controls specifically tailored to mitigate threats targeting the organization.

The process begins by trying to understand what assets are important to the organization through their business value to the organization and then breaking them down into their individual software and technology components. This will map out the assets attack surfaces and the possible attack vectors and threats specific to them. It is also important to analyze and categorize the threat actors themselves, to understand what their motivation and their goals are, what are their techniques and tools and what level of resources are they capable of committing against their targets to succeed in their goals.

Threat modelling around the different levels of threat actors and understanding the potential business impact on a successful breach of an asset is key to apply the "right" level of defensive security controls according to regulatory requirements, business requirements and then measure this up against the organizations level of risk appetite.

Using methodology as described, a set of 14 key defensive security controls with incremental levels implementation have been defined and are described on a high level in this document. These controls helps to increase the level of security posture for an organization using the controls in their infrastructure. Similarly the different defensive controls along with their definitions can also be used to make a simplified measurement and KPI tracker of the organizations currently implemented technology based controls and then assess the effectiveness of the security posture without using a full threat model analysis.

By combining threat analysis and assessing the current set of implemented controls and defining what threats should be properly mitigated, a gap analysis can be conducted to identify what controls are missing and then a roadmap on how to gradually reach the desired level of controls can be created. The defined security controls and the associated price tag of the implementation levels then can be used for budget planning.

A subset of the defined key capabilities, mainly those of detective nature, corresponds directly with the tools and capabilities that are required for the various functions of the security operations teams to provide efficient incident response. The defined security controls not only require technology

capabilities but also need sufficiently mature processes and people competencies to make them efficient. The Security Operations function is an integral as part of the defend phase of defendable architecture and applying multiple defensive capabilities thus helps increasing the ability to perform incident response in a timely fashion. The threat intelligence data gathered through the detection tools are then re-applied to measure and, if required, improve the effectiveness of the defined security controls to increase the overall security posture of the organization.

Table of contents

Table of figures

1 Introduction

1.1 Objective

The purpose of this document is to provide insight into the methodology for defining the level of threat mitigation and define the required security controls required for an organization to efficiently resist cyber-attacks.

The methodology introduces a risk driven assessment methodology supported by threat intelligence. It further describes a generic and non-tailored set of defensive capabilities based on the methodology and elements that can be implemented for different organizations. Also in scope is measurement for the threat actor mitigation efficiency of the different capabilities when implemented in regard to technology quality, process support and competencies required. Further details and how technology, process maturity and competencies will influence the organization's overall security maturity in security operations and incident response is given. The overall objective is to help organizations to be aware of their faced threats, their state of sensitivity and the maturity of their security controls to reduce the frequency and impact of cyber security incidents resulting in lowered business risk.

1.2 Scope

The target scope for this document is to provide as set of effective security controls for information and communications technology (ICT) platforms hosting workloads in either private or public cloud environments. While some common security controls such as network tapping and endpoint detection and response have use cases both for the datacenter domain as well as enterprise domain, aspects of security controls specifically addressing enterprise/business users and their devices such as end user compute (EUC), mobile devices etc. is not in scope of this document.

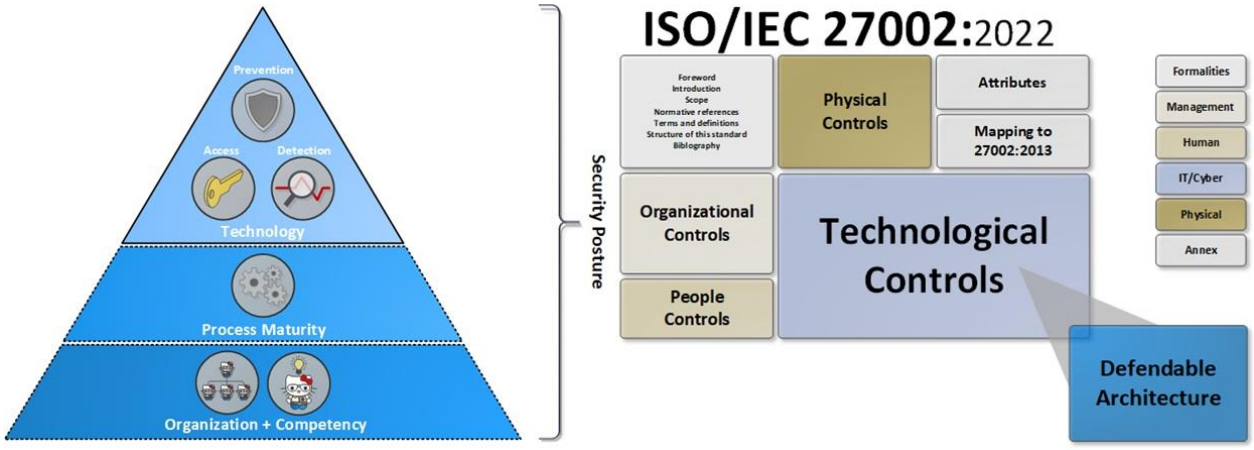


Figure 1. Defendable Architecture domains and areas

A complete security posture for an organization needs to be end-to-end and cover all aspects of technology, processes and people in the security domain to be truly effective. Defendable architecture focuses on the technical security controls and is the core content in this document. The ambition is to provide guidance of deploying the security controls and capabilities relevant for a range of organizations ranging from medium to large across multiple industry sectors with the purpose of mitigating potential threats while at the same time following a risk based and modular approach.

The concepts of a threat driven security architecture is provided in DA-2020-002. This document describes the foundation principles of defendable architecture, detailing the entire process on threat assessment, identifying relevant threat actors along with their techniques, tools and procedures (TTP), outlining principles of analyzing threat actors most commonly used vectors of attack and how to apply suggested and differentiated security controls per organizations' regulatory constraints, industry sector requirements, budgets and risk appetite.

A set of key technical security controls have been defined in DA-2020-002 and with these controls being divided into three main categories.

The following functional defendable architecture categories have been defined under the technology domain:

- Preventive capabilities and controls
  - Hardening of infrastructure components and surrounding them with security boundaries to prevent initial breach
  - Compartmentalizing of infrastructure to limit lateral movement in case of breach
  - Continuously updating software components to reduce attack surface cataloging inventory
- Detection capabilities and controls
  - Establishing visibility across the organization's assets
  - Provide telemetry from multiple sources by combining active and passive sources for correlation and analysis for security operations
  - Enable effective incident response
- Access capabilities and controls
  - Provide a secure/controlled environment for operators to perform their administrative duties
  - Role-based and least-privilege credentials for operators' required tasks throughout their entire lifecycle
  - Tools and processes to authorize and audit any type of access granted at any given time

Within each of the areas are described detailed descriptions and requirements for different security controls and capabilities. Subsequent additional documents will highlight each of the defensive capabilities individually with example implementations and solution designs and blueprints.

A stepwise approach to build up the maturity of the security operations center is also provided to highlight the importance of processes and people and how to utilize the described defensive capabilities in the right way to support incident response.

The final section addresses the methods for measuring the effectiveness of the controls through implementation quality, process maturity and competency required to support each individual capability and show how it will impact the overall organizations security posture.

Detailed descriptions of process and competency requirements of the capabilities are currently not part of the current scope of this document.

1.3 Target Audience

This guiding is intended to be read, understood, and used by:

- Infrastructure architects and other architects (enterprise, system, network, security…)
- Solution designers
- Project managers
- Security managers
- Lead architects

To get full benefit and understanding of this document the reader needs to have a good technical knowledge and understand the basics of infrastructure and information security terminology,

1.4 Definitions

Asset: Any form of object, physical or logical that either stores, processes, transports or in the wider context, access information related to the organizations business operations. Something that a person (or a software component) can get access to, such as a system, system component, application, or information, and so on. See system,

Availability: Availability means that a system, service function or data is accessible to users that are authorized to access it.

Confidentiality: System and data confidentiality refers to the protection of information from unauthorized, unanticipated, or unintentional disclosure.

Critical Information Infrastructure: Facilities, systems or functions whose incapacity or destruction would cause a debilitating impact on national security, governance, economy and social well-being of a nation.

Defendable Architecture: A conceptualized security architecture framework that is utilizing a risk and threat intelligence-based design process to describe a set of defined security controls based on CIS[3] controls.

Integrity: System and data integrity refers to the requirement that information be protected from improper modification. Integrity is lost if unauthorized changes are made to the data or a system or service by either intentional or accidental acts.

Managed services provider: External entities that access the organization's resources and does work on those resources on behalf of the organization like internal employees.

Monitoring: Capability or tool deployed within or in close proximity to a system to collect telemetry

Most: Quantitative measurement, implies greater than 90% of a measured scope

Operator: Any person having administrative rights to change the configuration on an application, system, infrastructure component or other resource.

Platform or **Infrastructure** in the context of this document is referred to as infrastructure for either IT or Telecom usage, deployed in a public or private cloud environment.

Risk: the possibility, or the potential occurrence of events or incidents that might materially harm the organization's interests.

Some: Quantitative measurement, implies less than 20% of a measured scope

System: A collection of components in the form of virtual or physical assets such as infrastructure components, or applications that together become something that performs one or more service functions which are being used by the organization for either internal or external purposes.

Threat: Relevant hostile entities (insiders and outsiders) or natural events that might cause incidents. If triggered on vulnerabilities threats cause business impacts.

Vendor: Also known as supplier. supplier of HW or SW components in the organization's infrastructure that usually requires access to different systems or assets for 2nd or 3rd line of support.

[3] https://www.cisecurity.org/controls

Suppliers are always external of nature but may also be treated differently for geo-political reasons, or for the level of criticality of the assets they deliver and requires access to.

Zero-Trust: A concept model of "never trust, always verify," which means that no devices or users should by default be trusted, even when originating from a "trusted" network such as the organization's enterprise network, even if they were previously verified. Requires multiple security controls at both network and identity/user layers and assurance through continuous monitoring. Zero-trust architecture is a fundamental input factor in the defendable architecture control design process.

2 Background

If there is a case to be made, it is that the steadily increasing horde of threat actors appears to be winning the battle in the ongoing cyber-war. According to the IBM X-Force 2020 report, over 8.5 billion records were compromised in 2019, more than a doubling compared to 2018. Ransomware was up 67% in Q4 of 2019 in a year-on-year assessment. This happens across a multitude of industries, ranging from government to healthcare, manufacturing and telecom.

Major incidents are happening with alarming frequency, and the incidents keep getting bigger in regards of impact. Various vendors are bringing out new products that are trying to close the gaps and catch up to keep the growing amount of threat actors out, but this will never happen unless the right people are engaged with security. If there is not a change in the approach to security and a business-driven strategy is not implemented, then this is a trend that will continue to grow.

The conventional approaches to security architecture is to focus on hardening the infrastructure against attack. The implicit expectation is that, once it is deployed, responsibility to block all attacks against it falls on the infrastructure's operations team. A more effective approach is for security architecture to address security from a business risk perspective and protect what matters the most to the organization. Key steps in business-driven security include understanding risks and speeding the response to breaches through effective incident handling and orchestration.

Defendable Architectures[4] was first introduced by Scott C. Fitch and Michael Muckin at the Lockheed Martin Corporation and describes an alternative approach to infrastructure security architecture by designing, implementing, and maintaining systems by applying a threat intelligence and risk-driven driven practice[5] using a similar approach on the principles from PASTA threat modelling. By following this methodology an organizations most important assets will have a set of security controls tailored to mitigate the defined attack vectors with a mapped-out level of risk that originates from the most likely threat actor tiers to carry out attacks against the organization.

In the realm of business-driven security, mapping risks and performing not only threat management but instead applying a higher degree of risk management and threat intelligence is required. This results in a more targeted and balanced focus between preventive capabilities that enable containment of threat actors using security zoning models applying resource isolation and the detection capabilities such as network monitoring, endpoint security and vulnerability management to support an effective incident handling and response process.

To create a business-driven security strategy, it is required that the organization does the following:

1) Identify where the main assets or so-called "crown jewels" are, what systems they are connected to and where they are most vulnerable to attack. With this in place it will be possible to assess the risk to the business if those assets are compromised by a threat actor and allocate resources appropriately.
2) A defense strategy should be built tailored to those particular assets and vulnerabilities. This should include having clear cost/benefit relationships outlined. The strategy should be holistic; it should include people and processes, as well as the required investment in adequate mechanisms in the form technology and tools.
3) Determine the gaps between the current security situation and where it ideally should be and start immediately on closing those gaps. During this phase the worst and/or critical areas

[4] See Lockheed Martin, Defendable Architectures
[5] See Lockheed Martin, Threat driven Architectures

should be the ones addressed first, having been ranked in accordance with the risk they pose to the business.

4) Take into account the aspect of the value chain of connected systems and who are operating them. How difficult is it to get something done? The more of the systems operations that are outsourced, the further away the competence is to remediate. This needs also need to be accounted for in any incident response strategy to defend the platform once its designed and built.

This entire process needs to be constantly repeated throughout the organization. It is also critical that response plans are in place should an incident happen. Response plans may vary depending on the asset in question.

3 Designing a threat driven, defendable architecture

While security design conventionally focuses on selecting controls, security architects must start with an understanding of what assets that reside within the infrastructure, what threats are likely to face them, and the impact of those potential threats to customers and overall business requirements. The main goal of an organization's security infrastructure architecture is to protect its assets.

The process of identifying threats and mitigating them is a continuous process that needs to be repeated throughout the lifecycle management of the infrastructure. Threats and vulnerabilities are identified, controls are implemented, and as both attackers and technology evolve the controls lose their effectiveness and needs to be updated or replaced to ensure that the intended behaviors is reflected and security posture is maintained. This process needs to cover the phases for the design, build and the run phases when the infrastructure is being setup and turned operational and then being defended through effective security operations.

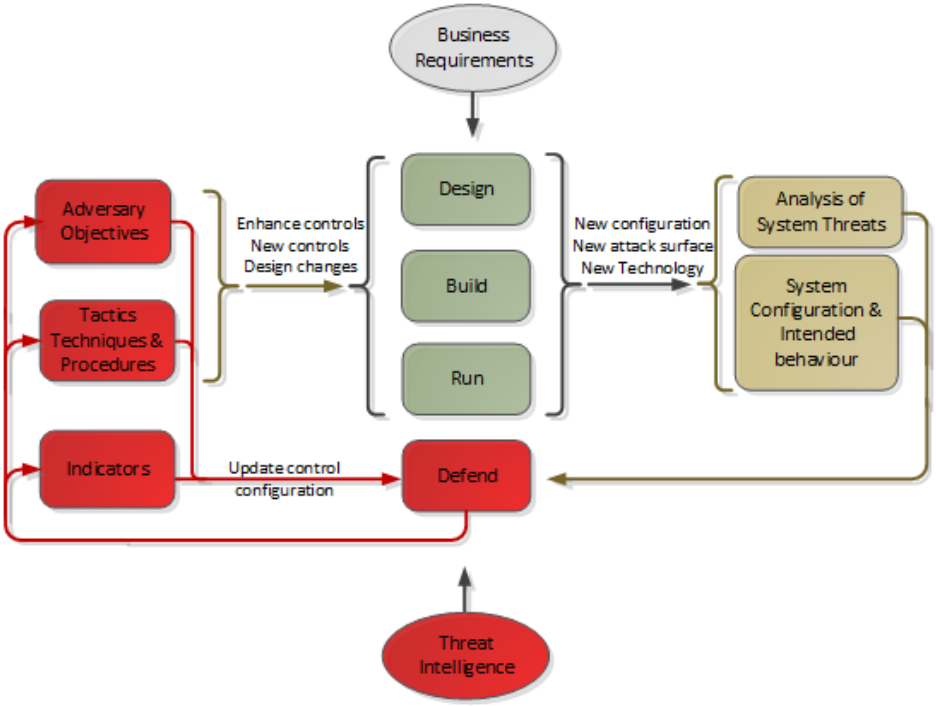


Figure 2. The defendable architecture process from LHM

Following the structured threat analysis methodology as described in the defendable architecture from Lockheed Martin helps to identify the potential threats against the infrastructure and its assets. It also provides a methodology to assess which controls and design alternatives will be most effective to mitigate identified threats and attack vectors. As an example, a preventive control can be deployed to mitigate an identified attack vector or risk, but the specific implementation of the control and the type of threat actor that is likely to make use of it determines the effectiveness of the control.

The approach is based on to that of PASTA[6] (Process for Attack Simulation & Threat Analysis) which is a 7-step threat modelling methodology invented in 2015 by Tony Uceda Vélez & Marco M Morana but with some differences. The first is the use of threat intelligence throughout the threat modelling

[6] https://en.wikipedia.org/wiki/Threat_model#P.A.S.T.A.

process and also the fact that Defendable Architecture looks at assets through their entire lifecycle of design build, run and defend.

The figure below shows the methodology that have been applied and shows how to use the principles in performing an identification of the company critical assets, applying regulatory and industry framework requirements, doing an analysis of likely threat vectors, attack methods and likely threat actors and selecting mitigating security controls based on those inputs while applying threat intelligence along the way in every single step.

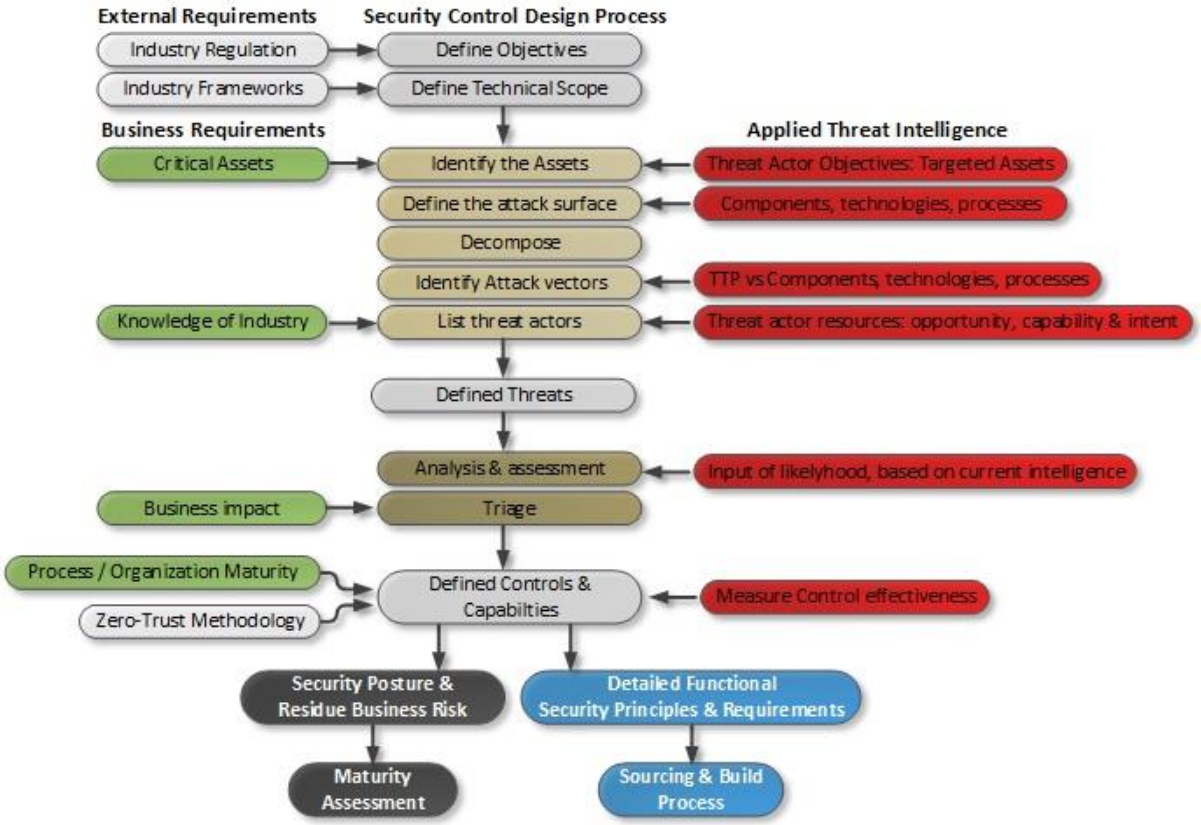


Figure 3. Systematic Threat assessment methodology combining different elements

The process on a high level looks like described below and will be further detailed and will be explained throughout the document.

- Defined objectives and scope based on business as well as regulatory or industry requirements
- Identify major assets (f.ex CRM,UDR) and classes of assets (such as internet exposed web servers, databases etc)
- Define attack surface by identifying infrastructure boundaries like internet gateways, mail servers or management systems
- Decompose the assets of the organization to identify risk and complexity
- Utilize threat intelligence to identify current and emerging attack vectors. Consider unexploited or undiscovered attack vectors.
- Utilize threat intelligence to identify different tiers of threat actors and their objectives.
- Perform analysis and assess potential business and technical impacts based on the identified threats and using relevant industry frameworks such as NIST-CSF, CIS, PCI-DSS or other

relevant input methodology

- Use triage to prioritize threats and mitigations based on impacts, threat intelligence, available mitigations and recommendations from industry frameworks
- Based on the outcome of the process define new and/or update existing security controls in the infrastructure and apply the principles of zero-trust end-to-end to control design
- Measure and track effectiveness of defined controls to determine residue risk and overall security posture
- Based on the defined controls, create detailed functional security requirements to support a sourcing process

Observation 002-1: *Protecting the most critical assets by selecting the right security controls and providing guidance to implementing them in the correct way to mitigate unacceptable or unavoidable levels of risk is the core principle of a business-driven security architecture.*

3.1 The big why, defining the overall objectives

First the main business goal of Defendable Architecture and what is the objective of the threat modelling process, and the actual benefits of the subsequent security controls needs to be defined. It is captured in the following mission statement:

"Building trust with the customers of the organization's offered services by preventing unauthorized access to critical systems and strengthen the ability to detect and mitigate potential incidents and data theft"

The main business objective is supported by several other specific goals as part of the threat modelling process:

1. Build an infrastructure and application centric threat model to identify potential risks to either confidentiality, integrity or availability of national critical services.
2. Analyze attack vectors and identify targets that include sensitive data and/or high-risk assets
3. Identify security controls and processes to be put in place to mitigate threats
4. Create a risk mitigation strategy that includes defining preventive, detection and access controls along with a target setting and roadmap on how to implement them
5. Use the gathered information about threats, risk assessment and business impact to comply with defined regulatory requirements such as national cyber security laws on critical information infrastructure , GDPR and other relevant privacy frameworks that's applicable for the industry sector which the organization operates.
6. Implement defined security controls to close any gaps in security posture and keep any residue risk within the organization's defined risk profile to a level where it's possible maintain a responsible business and license to operate.

Delivering on the main business goal as well as the defined specific goals shall be the outcome of the guidance provided in this document. Going through the risk assessment process, the awareness of actual concrete threats and risks should also be increased by bringing insights into the organizations' assets and the threats facing them.

Security Principle 002-1: *Security control design shall address relevant regulatory requirements and mandatory industry frameworks that apply for the industry that the organization operates in*

Security Principle 002-2: *Security control design shall use threat modelling as part of the design process*

3.2 Locking down the technical scope

To help designing the necessary controls to properly defend the infrastructure it is required to define a specific scope of what parts of the infrastructure shall be subject to the threat modelling and risk assessment. Low level design details need to be collected and then utilized to defining the scope:

- Relevant infrastructure components including management and service domain applications along with their zoning that forms the system(s)
- Network topology to clarify segmentation and to identify security boundaries
- Application flow diagrams showing protocols and/or services used in the different components and the relationship between them
- Use cases for the relevant services and value chains of systems, showing who is using them and how
- Privileged and non-privileged access rights required to both operate and use the systems
- Classification of data either processed, stored or transported through the components

From the information collected design details then needs to be extracted to define the scope of the different security controls. This would include identified critical assets along with their application-level security controls such as authentication, encryption, session management, auditing, logging etc.

Security Principle 002-3: *Threat modelling shall be precisely scoped to the asset(s) it is meant to protect*

3.3 Applying principles of Industry frameworks

It should be mentioned on where defendable architecture stands vs defendable architecture. Industry level frameworks such as NIST-CSF are complimentary and foundational when being applied to a security control design the process. They are very useful to identifying key functionality or controls that should be present in any organization's infrastructure, but as a *baseline* or a *shell* around what minimum level of controls that need to be implemented. Other industry frameworks such as PCI-DSS may also apply and influence the scope by defining controls that *must* be present.

While these frameworks describe what needs to be done, they will not in any detail describe how it is done or provide any reference designs or valid design artifacts while doing so. Defendable architecture has as key objectives to describe both the process to use for designing these controls, measuring their effectiveness and also provide a set of pre-defined security controls including valid reference designs and design artifacts that can be applied in a modular and risk-based fashion.

3.4 Deciding what assets to protect

The first step of the process of defining efficient security controls is to determine what to protect. Asset management of the organization's infrastructure and systems is a foundational requirement for information security in general. This is normally used to establish a baseline for what components are actually is authorized to be running in the organizations infrastructure and what is not but is key in this process to separate what is important from that which is not.

Identification, applying business value and categorization of those assets out of the total amount and to determine which of them that are considered to be critical is the essential part to properly develop and deploy the required security controls as part of defendable architecture. Its more effective to concentrate efforts and investments to protect what is important in a very good way, than trying to half-heartedly protect everything (and most likely fail miserably).

For the organization to able to implement effective security controls for the critical assets by using the defendable architecture model, all the assets must first be identified and categorized through the following process:

- Identify and list all the assets internally or externally which are being used by the organization (cloud services and the like also apply)
- Identify the system owner of each asset.
- Map out all interfacing applications for the asset and who have access to it
- Identify what kind of data and information the asset is either processing, storing, transporting or otherwise is in contact with
- Identify the asset's business criticality and its estimated value
- Identify what technologies, both SW and HW, that are used by the asset
- Identify any external requirements applying to the asset

If a proper asset management process is in place, this job will be significantly easier than for an organization who does not have proper inventory or change management processes in place and thus needs to start from scratch in mapping out their entire infrastructure.

With the organizations assets documented and mapped out the business criticality dimension for each of them should be applied since all similar assets are not equally important to the organization. The business value of the data is usually determined by its sensitivity when either stored, processed or transported by the asset. Business impact is assessed later when applying the risk dimension

The process of identifying the value of an asset is not necessarily so complex, the three main evaluation criteria for the value of assets can be used:

- Initial and maintenance costs
    - A specific price tag that includes the initial purchase, licensing, development, maintenance, and support costs estimated during its lifetime.
- Organizational value
    - The cost of creating, acquiring, and re-creating the information, associated with the asset and the business impact or calculated loss if the information is lost or compromised.
- Public value
    - Public value may include loss of intellectual property in the form of information or processes and loss of business reputation
- Regulatory value
    - Regulatory value may include fines or penalties the organization may incur in case of loss of data containing personal information or a service outage exceeding SLA's defined in operator license

Using the principles above the total value of the organization's effort placed into the asset is considered, including the information stored, processed or transported by it. In addition comes the amount of effort required to develop the asset, how much it costs to maintain, and what damage would incur to the organization if it were lost or destroyed.

To exemplify the above looking at Bob's online sock shop, the e-commerce application PCI-DSS compliance and availability may be of the highest importance. For a Silicon Valley startup, the most valued asset may be its developed source code for some new revolutionary gadget. A mobile service provider's most valuable assets may on the other hand be the availability of connectivity services

that are considered basic national functions, critical to society or for a healthcare provider the data of its customers falling under GDPR jurisdiction.

Security Principle 002-4: *All the assets internally or externally which are being used by the organization shall be identified and added to the asset inventory database (cloud services and the like also apply here)*

Security Principle 002-5: *All technologies, both SW and HW, that are used by each individual asset shall be identified, documented and added to the asset inventory database*

Security Principle 002-6: *Each asset shall have a dedicated system owner that can be identified*

Security Principle 002-7: *Documentation shall be created and maintained for all assets mapping out interfacing applications and protocols*

Security Principle 002-8: *All access to individual asset shall be documented and be traceable*

Security Principle 002-9: *information the asset is either processing, storing, transporting or otherwise is in contact with shall be identified and documented*

Security Principle 002-10: *Each asset's business criticality and its estimated value shall be documented*

A detailed methodology for classifying of assets following attributes for confidentiality, integrity and availability to provide risk analysis can be found at ISACA website here

After mapping out the assets, determining the overall attack surface comes next and for that the applications running on the needs to be decomposed to determine the technologies used and what data is store, processed or transported in each of them. Let's use an online banking application as an simplified example. In **Figure 4** below all the production assets (internal assets such as management systems, laptops, mobile devices etc is not taken into account in this example for simplicity) that are mapped out and the application stack that's the core of the online business is decomposed so all the technologies used are visible.

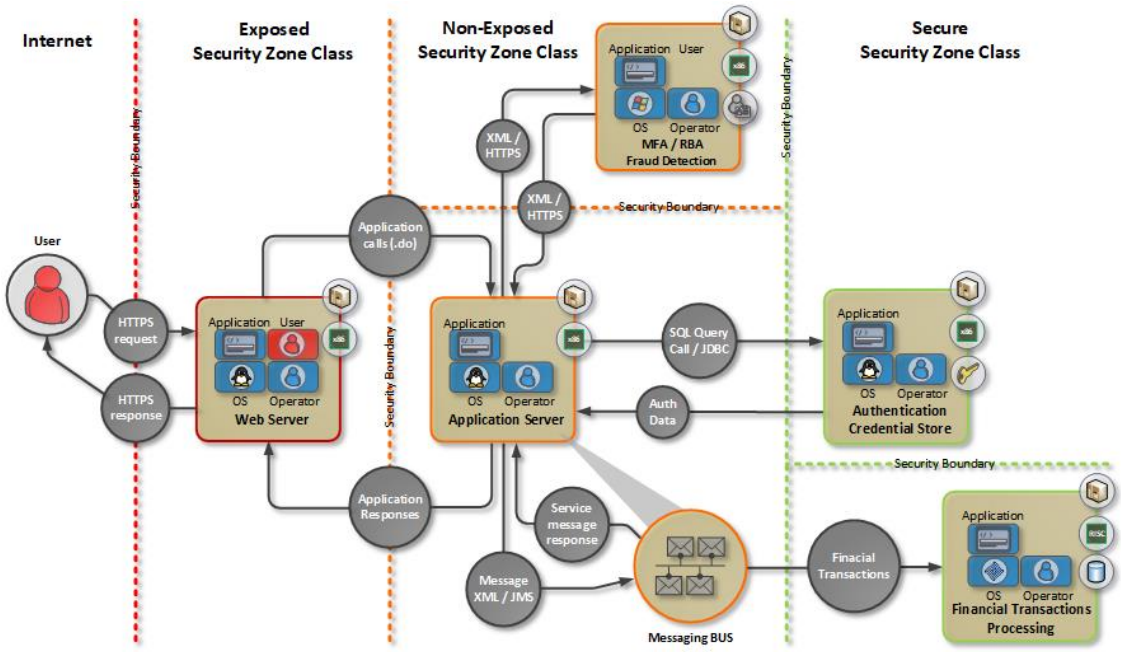


Figure 4. Sample e-commerce application

Decomposing the application shows a combination of operating systems such as Linux, Windows and SunOS and all the functions and protocols used between them. In this example, all the functions have

also documented network segmentation and resource isolation as applied by a security zoning model (one of the defined controls that are explained later). Each of the assets would have their software components documented such as OS, application versions and the protocols used.

The primary attack surface as shown in the figure above would typically be the web server in the exposed zone class that is open to the internet. Other more complex deployments would have multiple other services exposed to external networks.

3.5 Identifying possible attack vectors

Studying the history of warfare and conflicts none of them are exactly the same but still, there are some similarities between them in the forms of strategies and tactics because they are proven over time to be effective. In the world of cyber warfare (which threat actors for all practical purposes are conducting) the principles are the same. A threat actor will not put lots of energy into developing how to exploit a new vulnerability unless they have to and will often use common techniques that are proven to be effective, whether it is malware, phishing or exploiting a widely known vulnerability.

In particular, the more advanced threat actors usually will save their most powerful shiny tools and techniques if a much simpler way can be found into an organizations network. Identifying the methods being used throughout the multistage process of a break-in is key to define the different actor vectors available for a threat actor.

Mitre Attack[7] is a global knowledge base of threat actor tactics and techniques based on real-world observations and provides an excellent methodology by mapping out attack vectors at different stages. It shows how initial access, persistence, defensive evasion, lateral movement exfiltration etc., is conducted and what techniques that are commonly being used at each individual stage. Combined with the information about the critical assets themselves in the form of surrounding network configuration, running software etc. a pretty precise picture can be drawn of potential weak spots and thus possible attack in the infrastructure.

Using the sample application as shown in **Figure 4** above, securing the network perimeter with a firewall having threat detection capabilities and the web server itself with a web application firewall would come a long way. The firewall would make access to anything in the exposed network segment limited to the services of the web server and the web application firewall would mitigate classic methods of attacking web servers. A web server's dynamic code may be insecure and susceptible to SQL injections, cross site scripting and other classic exploits and establishing a secure hardened perimeter would reduce the attack surface for the initial access from a threat actor.

This is just a single example as documented in the Mitre attack framework there are a myriad of ways to either gain access, avoid defense, escalate privileges, lateral movement and the like that needs to be evaluated for the different assets.

Security Principle 002-11: *Possible attack vectors and known vulnerabilities for each assets shall be documented*

3.6 Sprinkling with Threat intelligence

Apart from understanding the threat actors, analyzing attack vectors and conduction risk assessment, threat intelligence can also be applied. Threat intelligence is information that is used by an organization uses to better understand the threats that are currently targeting the organization. The

[7] https://attack.mitre.org/

information is used to prepare, prevent, and identify threat actors looking to take advantage of critical assets, by looking for known so-called indicators of compromise[8] (IOC) and indicators of attack (IOA) through-out the different phases of an attack as shown in the Mitre Atta&k matrix earlier. Threat intelligence can be from multiple sources both internal and external. Monitoring capabilities installed in the infrastructure can reveal the techniques, tools and procedures that a threat actor that is already inside the infrastructure is using. Threat intelligence feeds

Knowledge about attackers and their techniques are often shared between different companies through collaborative organizations such as FIRST[9], through national intelligence services or via more informal security communities. Any information gathered that can help identify and narrow down potential threats should be considered and applied when doing the analysis of the different defensive controls during the different stages of their life cycle.

Security Principle 002-12: *Threat intelligence shall be gathered both internally and externally at regular intervals to assess threat landscape and design effective security controls*

[8] https://www.crowdstrike.com/blog/indicators-attack-vs-indicators-compromise/
[9] https://www.first.org/

3.7 Getting to know the opposition

As part of determining the exposure of the organization it is important to understand both the external security threats to the organization as well as any internal security threats posed by inappropriate use and lack of awareness of its employees.

From perspective of analysis the definition of threat assumes the existence of a threat "source," which is an actor posing the threat, referred to as threat actor or TA for short. Threat is defined as being composed of Capability, Intent and Opportunity.

The commonly accepted components of threat which includes the concept of opportunity and hostile intent. It also shows the overlapping fields of the different threat elements can be used to display the different levels of threat states posed by threat actors:

- Impending threat is the combination of capability and hostile intent, however, without the opportunity to act, the threat remains in the impending stage and is considered to be dormant
- Potential threat is the combination of capability and opportunity. Without hostile intent, this threat remains in the potential stage. This is the main category of the insider threats. Insiders have both the opportunity and capability but in general does not display any hostile intent until something triggers a change in motivation.
- Insubstantial threat is the combination of hostile intent and opportunity. Without the capability, many attempts to act will fail or turn out to be insubstantial

To continue the threat driven assessment, let's look at the different types of adversaries that organizations are facing. The different types of threat actors have, based on the index of capabilities as mentioned above, been classified into tiers based on their capabilities, potential for damage and their available resources. Keep in mind that this is a generalized view, there may be threat actors that have significantly better (or lower) capabilities than their generic "label" would say, but the tiers described below gives an assumption of what to expect on an average from the various types of threat actors out there.

What defensive capabilities to deploy against each threat actor type is essential for a security strategy to be business driven, as there is no upper limit on how many controls that can actually be implemented, and money spent on them. The key is to deploy the right capabilities for the right purpose to mitigate the relevant risks. If the crown jewels and the data that is to be protected is not likely to be the target of a nation state, there is no grounds for deploying capabilities to such an extent to defeat them either.

Correspondingly, if there is unwillingness in the organization to properly invest into security capabilities beyond a certain level you cannot expect to stop more than a tier 4 attacker from breaching your perimeter and compromise systems. On a similar note, the deployed monitoring capabilities might not be able to detect anything more than a tier 3 attacker once they have managed to breach a system and enter the infrastructure if they are of not a sufficient level. This might lead to a substantial data loss and damages over time.

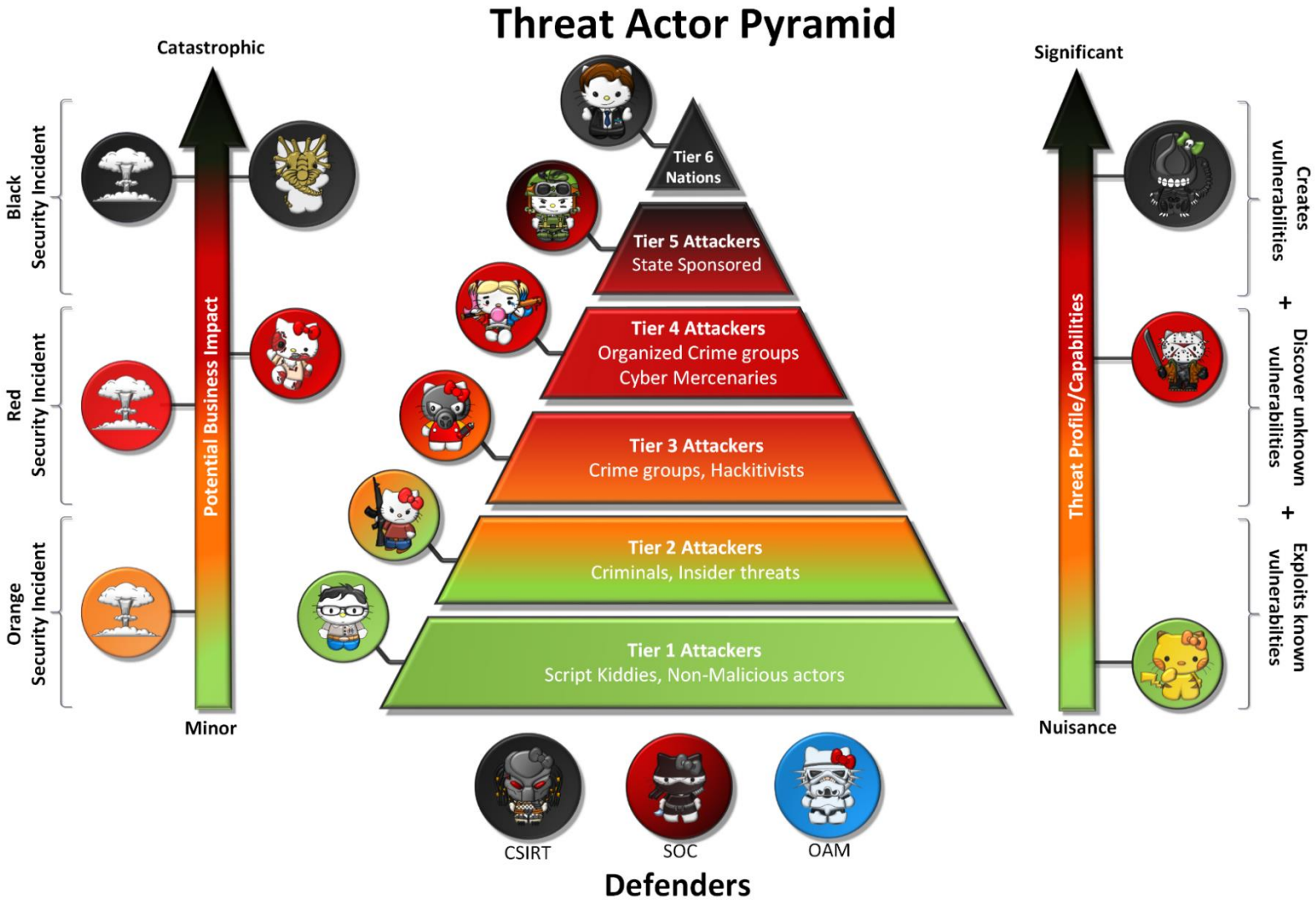


Figure 5. Threat Actor Pyramid

The threat actors are as shown in **Figure 5** are listed in 6 tiers ranging from fairly harmless lone wolves with a limited set of resources at their disposal, to government agencies with a much larger amount resources and manpower available. The state sponsored or state agencies pose a significant threat to any organization or individual who comes into their crosshairs and becomes a target. Similarly, incident response has been classified into orange, red or black incidents depending on the seriousness of the incident and the threat actor behind it. The classification of incidents and threat actors is important as it give a clear indication on what an implemented security capability is meant to address.

It should be noted that the representation in the figure above is generalized and not all threat actors are the same or can be mapped directly into a tier based on their motivations, there can be criminals normally being mapped to tier 2 but who are highly skilled, and which would instead be putting them on the level of a tier 4 threat actor. Similarly, there may be government agencies (ordinarily put at level 5 or 6) that behave like elephants in a porcelain shop and due to lack of experience and/or sophistication lands in the tier 2 category when it comes to skills and techniques. The threat actor pyramid shown in Figure 5 above shows a representation of the average threat actor of each individual tier.

While the approach being shown here is based on generic tiering, an organization if it have developed a high maturity in situational awareness and security intelligence capabilities be create a much more tailored response by customizing specific security controls in response to specific threat actors.

As shown in this article from Mitre, an organization can look at specific threat actors known to either attack their sector, or if threat intelligence is more accurate which APT groups are known to target them directly and then tailor a defense strategy and deploy security controls that specifically mitigates the TTP's of these specific threat actors.

Information can then be aggregated to determine which techniques are commonly used, which can help the organization to know what to prioritize. This allows the prioritization of techniques and when shared with the SOC provides them with the ability to focus on specific threat. If APT3[10] and APT29[11] were two groups an organization considered to be a specific threat, the specific techniques of these groups as documented in Mitre Atta&k may be the highest priority to determine how to mitigate and detect.

3.7.1 Tier 1 Threat Actor

"Script kiddies & technology enabled vandals"

On the internet there are the always the dangers of various individuals with that try to break into available systems with no more specific motives than "because they can". These actors are often referred to as script kiddies meaning individuals who one way or another have managed to get access to powerful tools written by someone else and use them against targets for entertainment or just to test if something can be done successfully. A script kiddie is however not always entirely correct as a label and reduce the perceived risk and potential of the threat from these threat actors. Script kiddies were earlier assumed to be mostly teenagers motivated by peer competition or simple mischief, but they are in reality threat actors who lack skills to write malicious code on their own, so

[10] https://attack.mitre.org/groups/G0022/
[11] https://attack.mitre.org/groups/G0016/

they rely on scripts and tools they can get from various sources. These actors are usually external but may also be internal as employees or contractors.

The attacks they carry out are usually not very sophisticated, but despite that and even if they are only out for some simple mischief, script kiddies can still cause serious damage to an IT system if they get their hands on powerful tools. Ranging from defaced websites to DOS attacks, actions can result in more than simple loss of face for the entities that are on the receiving end of their activities.

Like hacktivists (another category of threat actors), script kiddies have at their disposal a wide variety of acquired tools as well as social engineering techniques and can actually be quite persistent in carrying out their activities. With knowledge of exploits and attack techniques just a google search away, and tools continuously being developed and released. This level of threat actors can be compared to a kid bringing a live hand grenade to school and script kiddies have the potential to cause significant damage and be as dangerous as any other malicious actor given the right opportunity.

A good example is the case of a developer that for seemingly no reason, or at least not a reason that fits into the categories discussed above broke into a major financial institution [12] as well as several other companies causing data breaches that could potentially result in millions of dollars in penalties from regulatory authorities.

Threat Actor Attributes:

- Commitment
  - Intensity: Low
  - Timing sensitivity: Days
  - Stealthiness : Noisy
- Capability
  - Personnel: Ones
  - Knowledge: Limited
  - Exploit Access: None

Typical attacks: phishing, viruses, DNS attacks

Key mitigating defensive capabilities[13]:

- Basic (CL2) Resource isolation and zone model
- Basic (CL2) Stateful internet-facing security boundaries
- Basic (CL2) Stateless platform security boundaries for all assets
- Basic (CL2) Internet-facing Signature-based IDS for exposed systems
- Basic (CL2) Integrated signature-based endpoint protection (AV)

This threat actor type can be internal as well as external of nature. A good endpoint detection and response solution would defeat most non-targeted attacks from a tier 1 attacker. Strong security in the endpoint detection and response domain with anti-phishing strategies should also be in place since phishing software kits are common among script kiddies that checking for what they can come across of useful information, much like the other threat actor types. Equally basic resource isolation separating exposed, internal and management services with security boundaries using standard firewalls at the perimeter and between the services would keep most tier 1 attackers out. Detection capabilities such as intrusion detection systems (IDS) or endpoint protection & response may use

[12] https://www.wired.com/story/capital-one-paige-thompson-case-hacking-spree/
[13] Defined security controls highlighted later in this document, controls listed are the most central and not an exhaustive list

signature-based detection since it is considered to be sufficient to mitigate the mostly *known* tools and exploits used by a lower tier threat actor.

3.7.2 Tier 2 Threat Actor

"Criminals and insider threats, hostile intent"

When key personnel go postal, the impact of their actions can be quite severe and potentially devastating, and possibly significantly more disastrous than any half-hearted attempts of an attack from any external threat actors. It is common to perceive insider threats as being a risk due to open hostile intent, but it can be just as much of a factor due to negligence and unintentional errors. Financial enterprises such as HSBC[14], and Ascension[15] have suffered significant embarrassing and costly data breaches due to unintentional errors.

Intentional insider threats are however increasing according to recent industry reports. An insider threat may be difficult to detect because the personnel performing the actions may have valid login credentials as well as insight into the operational security procedures. On top of this there is an increasing number of applications being moved along with their data to public cloud where monitoring of user behavior and file access is less comprehensive or not yet implemented at the same level as in an on-prem environment. Operators being able to use BYOD devices on the corporate network is also an area where that need to be closely monitored if such usage is permitted.

Threat actor Attributes:

- Commitment
  - Intensity: Low
  - Timing sensitivity: Days
  - Stealthiness : Noisy
- Capability
  - Personnel: Ones
  - Knowledge: Limited
  - Exploit Access: Limited

Typical attacks: Bots, DoS and other advanced tier 1 attacks

Key mitigating defensive capabilities:

- Basic (CL2) Internet-facing Signature-based IDS for exposed systems
- Basic (CL2) Centralized Logging for all assets
- Basic (CL2) Integrated signature-based endpoint protection
- Standard (CL3) Process driven IAM with integrated user-provisioning

For internal threats, apart from the mitigation of tier 1 attackers, it is also important that user behavior that is considered abnormal is detected and triggers and incident response, for this to work properly visibility is required in the network. Centralized logging goes a long way into collecting all the system and application logs in a single secured location for analysis of either operational or security related incidents. Keeping all the logs in a location out of reach from the individual components that produce the events also ensures the log information is less likely to be tampered with.

[14] https://www.telegraph.co.uk/technology/2018/11/06/hsbc-suffers-data-breach-us-bank/
[15] https://www.komando.com/security-privacy/millions-of-loan-and-mortgage-records

Access to internal data and files should be limited according to “least privilege” and “need to know” principles, and all endpoints used by operators, and which is connected to the infrastructure should have proper endpoint security functions installed.

3.7.3 Tier 3 Threat Actors

“Hacktivists, digital rebels, or maybe just random griefers”

More advanced attackers such as hacktivists like to pool their resources and operate coordinated. Being stealthy however is usually not on their agenda, rather the opposite. The main target of hacktivist groups is to bring attention to a specific issue, person or organization that they want single out for either positive or negative purposes sharing information in the form of promotion or information disclosure of illicit activities or IPR of their targets. Groups such as LulzSec and Anonymous have caused major problems for businesses and organizations across the world. Enterprises such as Sony Pictures [16], CIA [17] and government agencies of countries such as the Philippines [18] and Thailand [19] have all been targeted in the past and suffered embarrassing breaches as a result of these types of groups.

Hacktivists methods of attack include DDoS attacks on externally exposed services using botnets, defacing websites, and taking over social media accounts of high-profile individuals and enterprises.

Threat actor attributes:

- Commitment
  - Intensity: Medium
  - Timing sensitivity: weeks
  - Stealthiness: Noisy
- Capability
  - Personnel: Tens
  - Knowledge: General
  - Exploit Access: Through others

Typical attacks: DDoS, root kits, 0-day exploits, C2 architectures

Key mitigating defensive capabilities:

- Standard (CL3) Stateful platform security boundaries with DPI
- Standard (CL3) Stateful perimeter security boundaries with DPI and airgap
- Standard (CL3) Integrated event-based endpoint protection & response (EDR)
- Standard (CL3) Centralized Logging with security analytics (SIEM)
- Basic (CL2) Limited network tapping with NPB
- Basic (CL2) Internet-facing Signature-based IDS for exposed systems
- Standard (CL3) Data protection

Hacktivist campaigns usually target internet exposed web services or other applications, so in addition to implementing earlier mentioned security capabilities, deploying L7 inspection capabilities

[16] https://en.wikipedia.org/wiki/Sony_Pictures_hack
[17] https://en.wikipedia.org/wiki/Vault_7
[18] https://www.computerweekly.com/news/450297996/Philippines-government-data-breach
[19] https://www.bangkokpost.com/thailand/general/913068/data-breach

to the security boundaries in the form of web application firewalls and deploying DDoS mitigation capabilities that analyses network traffic and identify anomalous requests gives the best results against these types of threat actors.

Deploying a SIEM[20] solution that starts to perform real-time analysis of collected logs to automate processing and raising alerts on detected anomalies in the centralized log platform is a natural next step to detect a tier 3 threat actor that relies more on unknown vulnerabilities than known ones.

More sophisticated endpoint agents that are more meant for passive analysis and detection will alert on suspicious behavior within an OS instance and passive tapping of endpoint network traffic that are suspected of a compromise will greatly help in the detection and supporting a proper incident response to evict a slightly more advanced threat actor.

While added L7 inspection capabilities add greatly to the capabilities of keeping a tier 3 threat actor away from potentially vulnerable and exposed applications, mature incident response processes are becoming a must to mitigate this type of threat actor should they manage to breach the perimeter defenses and gain a foothold. Incident response plans need to include mitigation strategies for any reputational damage that could be caused since unauthorized information disclosure and defacing of the organization's public facing websites are two typical outcomes of a breach from a hacktivist threat actor group.

3.7.4 Tier 4 Threat Actors

"Organized crime groups/cyber mercenaries, making money from cyber-crime"

The most widespread, serious threat currently comes from organized groups of criminals seeking to make money. Criminals all over the world have been quick to adapt themselves to the opportunities for various illegal methods for making money via internet connected societies. Activities range from stealing information or other IPR and selling the data for profit, planting ransomware within an unsuspecting organization or stealthy inserting bitcoin miners into a target's infrastructure. There is an digital equivalent of pretty much any real-world type of financial crime, ranging from fraud to kidnapping and bank robbery. To further stimulate to this behavior, there is a 2-1 reward model since cyber-crime can offer much higher rewards with much lower risks in a classic win-win scenario.

The lower factor of risk is due to the ability of criminals to hide their activity online and the easiness of money laundering using digital currencies such as Bitcoin or Ethereum.

In 2019, ransomware attacks have increased significantly [21] and the number compromises are up from 2018 numbers. It is not only large corporations[22] or fortune 500 companies that are targeted. All kinds of organizations ranging from local governments [23] to SME sized companies all are potentially soft and squishy targets for an increasingly experienced and well-equipped cybercrime underworld.

Threat actor attributes:

- Commitment

[20] https://en.wikipedia.org/wiki/Security_information_and_event_management
[21] https://www.cnet.com/news/ransomware-devastated-cities-in-2019
[22] https://krebsonsecurity.com/wp-content/uploads/2014/01/Inside-a-Targeted-Point-of-Sale
[23] https://gizmodo.com/report-ransomware-goons-had-a-great-2019-with-at-leas-1840542724

    - Intensity: high
    - Timing sensitivity: months
    - Stealthiness: good
- Capability
    - Personnel: tens of tens
    - Knowledge: specialized
    - Exploit Access: indirect

Typical attacks: Backdoors, Crypto jacking, advanced malware

Key mitigating defensive capabilities:

- Standard (CL3) Resource isolation
- Standard (CL3) Stateful platform security boundaries with DPI
- Standard (CL3) Stateful perimeter security boundaries with DPI and airgap
- Standard (CL3) Flow-based network monitoring
- Standard (CL3) Continuous network tapping
- Standard (CL3) External-facing event-based IDS sensors
- Standard (CL3) Operator access with PAW
- Advanced (CL4) Data protection

To protect from external threats like organized groups of cyber-criminals, it is important that both the network infrastructure and the endpoints carrying the organization's workloads are protected by event-based IDS, EDR and network tapping giving a multi-layered detection capability focusing more on previously more *unknown* TTPS's and to be able to trigger an immediate incident response. Proven by the number of successful attacks shown in media on a regular basis, the traditional protective software agents using signature-based detection is a thing of the past. Signature-based detection capabilities focuses on what are mostly *known* TTPs and are simply obsolete and inadequate in stopping organized cyber criminals in the form of tier 4 threat actors as these are equipped with more advanced attack tools and techniques which are increasingly more *unknown.*

Since cyber criminals are frequently targeting data, a more increased posture in the containment area is required, justifying another layer in the zoning model dedicated to databases and critical systems storing data of interest, the secure services class in addition to the exposed and non-exposed service classes. This provides an increased predictability into where sensitive data, and in particular customer data if applicable is stored in the infrastructure

A proper containment security posture and subsequently deployed monitoring capabilities should be able to detect anomalous behavior both before and during the execution of exploits and the infrastructure should have change capabilities in place to deal with threats such as ransomware. Detection tools should therefore come with machine learning and analytics capabilities as these are critical in detecting and subsequently evicting tier 4 threat actors.

In addition to that, it is very important that a more active vulnerability management program is launched and that systems, in particular exposed or those containing sensitive data, are patched within a sensible timeframe. Cyber-Criminals will always jump on newly discovered exploits although security monitoring solutions can easily detect exploitation of known vulnerabilities, patching and updating all software components is an additional layer of defense that may cause an attacker to look for another and easier target.

Access capabilities also needs to be better equipped to avoid the abuse of legitimate credentials as the path of least resistance. Closely monitored PAWs provide a secured environment for operators which are accessed via vpn and supported by MFA and other security controls shall be the basis for all remote access. Secured remote access will avoid that regular operator credentials are not

compromised via HUMINT[24] methods and used for unauthorized access of the organization's infrastructure.

Having a proper incident response process is also of key importance to detect cyber-criminals and to improve the overall posture. Be sure that all personnel know the defined communication processes in the event of a breach.

By default, all infrastructure components should be hardened, Consequence and risk management process applied to all assets to determine criticality and result of an eventual compromise.

3.7.5 Tier 5 Threat Actors

"State sponsored actors, technology theft, sabotage, cyber heists"

Tier 5 and 6 threat actors are by itself the definition of so-called advanced persistent threats [25] (APT). APT's have become increasingly active as an increasing number of developed nations conduct cyber warfare operations on political, economic, military and commercial infrastructure of their political rivals' respective countries.

Tier 5 threat actors are the first level of the more sophisticated APT groups and are mostly acting as the proxies of nation states to avoid a direct connection with the conducted activities, have increased significantly in recent years. While techniques, tools and processes to a large degree may be similar, the main distinction between a state sponsored APT (T5) and that of an APT run directly by a government (T6) is typically that of their available resources. A state sponsored APT group does not have the same level of personnel available and is therefore more limited in the number of operations they can run simultaneously or a sustained level of focus. When a nation state government itself is an APT, they may have personnel available in the hundreds as salaried employees working in shifts and can run focused operations against multiple targets over a very long period of time as required.

A key difference for an APT as opposed to the other lower tiers of threat actors is that they are not opportunistic and usually attack a target with a specific objective in mind. Such an objective may be as destroying a city's power grid, stealing trade secrets from a company to bolster the nations own enterprises or gaining communication data about political dissidents abroad in other countries.

Although APTs are mainly performing activities that benefit the interests of one country or some countries over another, it is easy to get caught in the crossfire. It may be a nation-state that wants technology that is being developed for their own use or cyber weapons to escape into the wild or weaponized zero-day vulnerabilities like the Eternalblue[26] being made available to the general public by accident and then being used in active cyber warfare.

Activities by an APT can have a catastrophic impact to an organization if being targeted. A well-documented example of how devastating attack can be from a from a state sponsored threat actor is when a Russian apt group called Sandworm[27], over several years terrorized Ukrainian national power infrastructure[28] and in 2017 let loose the NotPetya[29] worm which decimated thousands of networks all over Ukraine before spreading across the world. The worm caused global widespread havoc world resulting in damage estimated to more than 10 billion USD in total.

[24] https://en.wikipedia.org/wiki/Human_intelligence_(intelligence_gathering)
[25] https://en.wikipedia.org/wiki/Advanced_persistent_threat
[26] https://en.wikipedia.org/wiki/EternalBlue
[27] https://www.csoonline.com/article/3455172/russias-sandworm-hacking-group
[28] https://www.wired.com/story/russia-ukraine-cyberattack-power-grid-blackout-destruction/
[29] https://www.wired.com/story/notpetya-cyberattack

State sponsored APTs are not unknown to perform direct financial theft similarly to ordinary cyber-criminals. APT groups such as North Korea's Lazarus[30] group have been engaged in various cyber heists[31] such as SWIFT-related attacks against financial institutions across the world or attacks targeting bitcoin exchanges to bolster either their own or their nation's economy. These attacks have resulted in losses ranging from tens to 100+ million USD for the targeted organizations.

Threat actor attributes:

- Commitment
  - Intensity: very high
  - Timing sensitivity: year(s)
  - Stealthiness: sneaky
- Capability
  - Personnel: tens of tens
  - Knowledge: multi-scope
  - Exploit Access: direct

Typical attacks: Full range of high caliber and long-term attacks, unique multi -stage exploits available.

Given the more sophisticated TTP's used by this tier of threat actors and their ability to use previously unknown exploits, the deployed security controls need to be more dynamic and focus on event-based detection of anomalies and usage of threat intelligence to find more relevant IOC's. Security intelligence and situational awareness start to become more important to mitigate tier 5 threat actors as controls may require to be specifically tuned to TTP's that are unique to the specific threat actor that is found to be likely to attack the organization.

Key mitigating Defensive Capabilities:

- Advanced (CL4) Resource Isolation
- Advanced (CL4) Stateful platform application-aware security boundaries with SSL intercept
- Advanced (CL4) Stateful perimeter application-aware security boundaries with SSL intercept
- Advanced (CL4) Threat-intel driven Integrated vulnerability management
- Advanced (CL4) Threat-intel driven centralized logging with security analytics
- Advanced (CL4 Threat-intel driven event-based IDS covering all external facing interfaces
- Advanced (CL4 Threat-intel driven Flow-based network monitoring with SSL intercept
- Advanced (CL4) Continuous network tapping with SSL intercept

3.7.6 Tier 6 threat actors

"Nation states' offensive cyber warfare units, industrial espionage, communication tapping, political manipulation & more"

[30] https://en.wikipedia.org/wiki/Lazarus_Group
[31] https://www.zdnet.com/article/north-korea-s-apt38-hacking-group-behind-bank-heists

Tier 6 threat actors, the topmost category of threat actors is that of the nation states themselves with directly controlled functions capable of highly sophisticated attacks and are often organized as an offensive capability unit under the military command of respective country. These actors have large resources at their disposal when it comes to developing exploits themselves along with the tools to use them as well as personnel running cyber warfare operations similarly to the in-real-life version of commando raids.

This group of threat actors usually have a specific target in mind such as extracting a specific piece of information and well pursue their target relentlessly until it is achieved, or it becomes too costly and time-consuming to continue the operations. Often a tier 6 attacker have been inside the infrastructure for years being undetected setting up multiple attack infrastructures for quick re-entry into the network in case they are discovered and initially evicted.

Nation state threat actors focus on several attack vectors simultaneously and exploit a number of vulnerabilities. In recent years, many high-profile attacks have been attributed to nation state actors. With the most known is when British Intelligence agency launched its “operation socialist” against Belgian telecom operator Belgacom[32] and resulting in a total compromise of the company’s both internal and customer serving infrastructure.

Defending against targeted attacks from APT groups requires both resources in the form of a significant deployment of advanced security controls and the organizational capabilities and staff to operate. A different approach to security in general but in particular detection is also required. Machine learning, big data analytics and community threat intelligence feeds need to be applied to the different capabilities where applicable to make them more dynamic in nature to discover previously unknown methods of compromise based on deviating behavior. The more dynamic capabilities added to security controls make them more up-to-date and efficient also to detect *known* threats .in addition automated response functions on anomaly detection become important in ensuring that APT’s does not get an initial foothold or if they manage to get one are detected and evicted as soon as possible.

In addition to deploying relevant security capabilities, it is also required to apply a security risk assessment includes evaluation of what assets that might be an attractive target to nation states, the earlier named crown jewels. The threat profiles of known actors need to be continuously evaluated through security intelligence and develop proper strategies around those.

Threat actor attributes:

- Commitment
  - Intensity: fanatical
  - Timing sensitivity: years
  - Stealthiness: nearly undetectable
- Capability
  - Personnel: hundreds
  - Knowledge: multi-scope
  - Exploit Access: direct

Typical attacks: Full spectrum, high caliber and long-term attacks, unique multi -stage exploits.

[32] https://theintercept.com/2014/12/13/belgacom-hack-gchq-inside-story/

Key mitigating Defensive Capabilities:

- Intelligent (CL5) Resource Isolation
- Intelligent (CL5) Threat-intel driven stateful platform boundaries with dynamic filtering and SSL intercept
- Intelligent (CL5) Threat-intel driven stateful perimeter boundaries with dynamic filtering, SSL intercept and airgap
- Intelligent (CL5) External-facing Threat-intel driven event-based IDS with packet capture playback
- Intelligent (CL5) Threat-intel driven integrated flow-based network monitoring
- Intelligent (CL5) Threat-intel driven centralized logging with security analytics & automated response
- Intelligent (CL5) Integrated & automated continuous network tapping with SSL intercept
- Intelligent (CL5) Threat-intel driven, Integrated, vulnerability management with automation
- Advanced (CL4) Operator Access with privileged access management (PAM)
- Mature response processes by applying threat, risk and business impact with analysis & triage

With critical assets being identified, their applications decomposed, and likely threat actors assessed the next steps if for the organization to understand the likelihood of threats and the business impact of the breach of each individual asset and estimate the likelihood and frequency for one to happen. There are two phases to this step. The first is by assessing threats through attack trees to determine a set of specific threats to an asset, measure the complexity of the attacks and then apply the likelihood of it to happen based on exposure and susceptibility. This will assign a threat profile to the specific asset. The second phase is a risk analysis to measure the business impact if an attack is successful. For this purpose, either qualitative or quantitative risk assessment can be used to identify a risk rating. The approach used here uses the baseline of the qualitative risk analysis but have quantified values attached to them to calculate the business impact of a risk.

3.8 Using attack trees to determine threat levels

To more accurately determine the threat value of a specific asset's different attack vectors, a methodology as described by information security guru Bruce Schneier[33] called "attack trees" can be used. An attack tree looks at the identified attack surface of the decomposed components of the critical assets as described in section **3.4** from an attacker's point of view. The attacks are represented against a system in a tree structure, with the target goal as the root node and different ways of achieving that goal as leaf nodes.

[33] https://www.schneier.com/academic/archives/1999/12/attack_trees.html

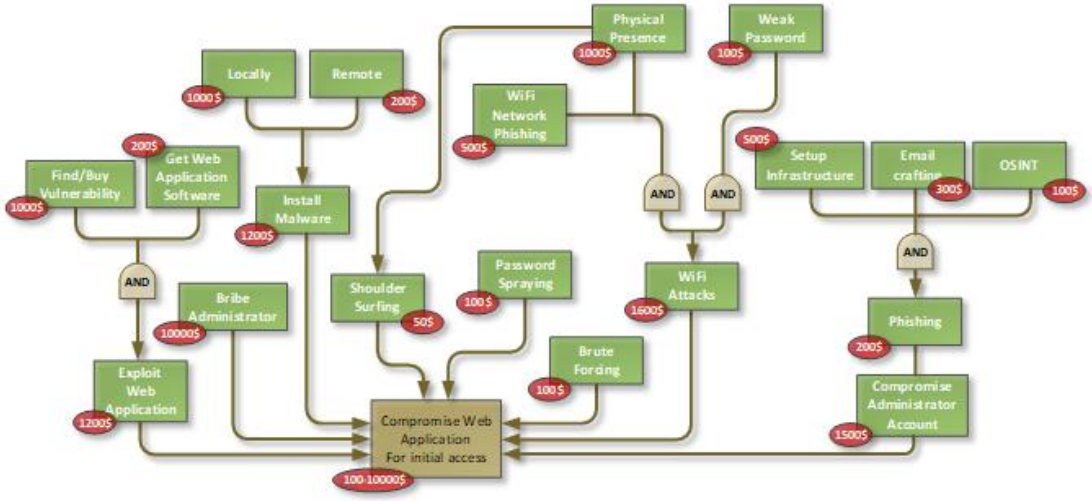


Figure 6. Sample attack tree for initial breach

An attack tree is composed by two (2) main elements: leaf nodes and root node(s).

- A root node is the goal of the overall attack
- A leaf node is a specific attack (or sub goal)
- AND / OR node represent different way to achieve the attack:
  - AND node means all sub-attacks must be achieved.
  - OR node means at least one attack must be achieved

An estimated value is placed on each of the leaf nodes to represent the resource requirement for that specific attack. The total amount is places on the root node and represents a range from the cheapest single attack to the most expensive chain of staged attacks

The use of attack trees allows investigating possible attack scenarios, and to understand which attacks can be performed, how risky they are, what benefits that can be achieved from a successful attack and how much resources that are required, in terms of time and money, to execute it.

The price tag that is applied to each of the attacks to come up with an estimate of how much resources that would be required to complete the attack chain. The more advanced tiers of threat actors (typically tier 5 and 6) are doing this from a resource planning perspective since they also don't have a infinite amount of resources that can be pooled against each target and operate on budgets like any other delivery project.

Security Principle 002-13: *Attack trees should be created for assets as part of the security control design process*

Once an attack tree of a particular asset has been completed it can be linked with other attack trees for an interconnected set of asserts. In the figure above, only the initial access of the stages documented in the Mitre attack matrix is shown, but for more complex scenarios there are multiple goals, and/or assets, to protect. It is fully possible (and recommended) to create an attack tree for several assets a chain them together to represent the different phases of a multistage attack to create a complete "battle plan".

Observation 002-2: *From a defensive point of view, the objective of an attack tree is to identify possible attacks and implement defensive controls to increase the costs/risk to make them either unsustainable to achieve or to reduce the probability of them occurring.*

The combination of different goals based on assets attack surface and the attack vectors from Mitre Attack should be combined with intelligence about the different tiers of threat actors as described earlier when creating the attack tree. The different tiers of threat actors have different levels of skill, resources, access and risk aversion. If tier 4 or above is on the top of the concern list, “expensive” attacks is what should be considered just as likely as the cheaper ones. The advanced threat actors often have multiple teams with a varying degree of skill. If the concern is about non-malicious users, or insider threats, the more expensive and directly illegal attacks such as bribery is not very realistic. A threat actor’s profile and mode of operations will imply which parts of the attack tree that is most likely to be used.

3.9 Risk analysis

Risk is the possibility, the potential occurrence of events or incidents that might materially harm the organization’s interests. And applying a risk analysis methodology on how to mitigate identified threats and vulnerabilities stands at the core of Defendable Architecture and the security control design process as indicated in **Figure 3**.

The organization must plan how to address the risks, threats, and opportunities. This is also greatly emphasized in ISO 27001 which focus on:

- How the risks integrate into the wider information security management system
- How actions are taken, and evaluating the effectiveness of the implemented controls and policies taken

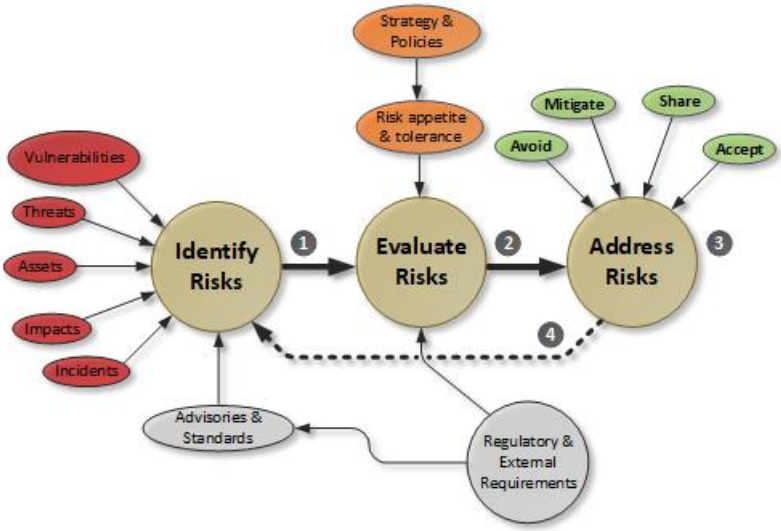


Figure 7. Defined Risk Analysis Process

The objective of the risk analysis process is to identify the relevant risks. Several input sources go into identifying the relevant risks as described earlier in the form of:

- Vulnerabilities
  - The inherent weaknesses within technologies, people and relationships
- Threats
  - Relevant internal or external hostile entities that might cause incidents
  - If triggered on vulnerabilities threats cause business impacts
- Assets
  - Primarily information Assets that either, store, process or transport information under either regulatory scope or which is considered business sensitive. May include

infrastructure HW/SW objects, end user equipment or other components relevant to access

- Impacts
  - Negative effects or consequences as a result of incidents or disaster that affects assets and cause a degree of damaging to the organization and its business. See **Table 1** for reference
- Incidents
  - Events that scale from minor (very low), or events of limited consequence (low to medium) up disasters (high) and catastrophes (very high). See **Table 2** for reference
- Advisories, standards
  - Refers to relevant documentation from either official standards organization such as ISO/IEC, technology vendor recommendations, national cyber security defense warnings or CERT flash memo lists

The next step, which is to evaluate the risks involves processing and analyzing the information collected to determine the importance of the identified risks, the importance directly dictates the priorities for the next step in the chain. The organization's tolerance for risks needs to be clearly defined and applied at this stage. The risk tolerance levels need to come all the way from the top and reflect the relevant business strategies

Treating risks means how to deal with them and there are several outcomes of how to address each individual risk. They can be avoided, mitigated, shared and/or accepted them. For the sake of designing security controls the assumption is that the risk is to be mitigated, but it may also be avoided, shared or accepted depending on what may be most effective from a business strategy point of view.

The 4th step as illustrated in the figure above means to represent that the risk management process is continuous. As the threats, vulnerabilities and assets change, so does the risks associated with them which may change in either frequency or impact. It is thus required to continuously repeat the process at regular intervals.

Regulatory requirements are external to the organization, but is important input, since relevant authorities may demand that certain risks are kept at a certain tolerance level, thus impacting both prioritization and the resolution of the risk, as it may not be permissible to tolerate certain regulatory risks for instance.

The risk analysis can be used to apply and approximate values of impacts for the loss of confidentiality, integrity or availability if an asset with an approximate calculation. Impact and likelihood is applied to the identified critical assets and its threats based on identified attack vectors, vulnerabilities and threats. Each organization needs to define what is considered as high or low impact, but the table below gives an example of the impact of a security breach affecting confidentiality, integrity or availability of an asset.

Based on the total value of the asset potential business impact can range from very low (nuisance/fairly minimal) up to very high (potentially catastrophic). The table below attach a monetary value to quantify the business impact.

Business Impact of incident

	Very high (5)	High (4)	Medium (3)	Low (2)	Very Low (1)
Revenue	>30 % decrease	> 10 % decrease	5 - 10 % decrease	2 - 5 % decrease	< 2 % decrease
Cost	>30 % increase	> 10 % increase	5 - 10 % increase	2 - 5 % increase	< 2 % increase
Regulatory	Catastrophic regulatory constraint. Loss of license to operate or government shutdown, etc	Major regulatory constraints to business (loss of competitive advantage, longer time to market, loss of opportunity, etc)	Considerable regulatory constraints to business (loss of competitive advantage, longer time to market, loss of opportunity, etc)	Noticeable regulatory constraints to business (loss of competitive advantage, longer time to market, loss of opportunity, etc)	Minor regulatory constraints to business (loss of competitive advantage, longer time to market, loss of opportunity, etc)
Brand Reputation	International concern. Government inquiry or sustained adverse international media.	Negative national coverage over a long period and/or major social media storm	Negative national coverage over a short period and/or considerable social media storm	Negative national headline news and/or minor social media storm	Local headline news and/or sporadic social media discussion

Table 1. Incident Business Impact

The second dimension is that of likelihood, or more precise what's the chance of an identified incident to happen and how often will it occur. The table below puts definitions to the range from very low to very high along with a percentage chance for the likelihood of it occurring within a given year.

Likelihood of occurrence

	Very Low (1)	Low (2)	Medium (3)	High (4)	Very High (5)
Frequency	< once every 5th year	Every 5th year to 1 year	Every 12 months to 6 months	> once every 6 months	> once every month
% per year	< 20 % (YoY)	20 - 50 % (YoY)	50 - 85 % (YoY)	> 85 % (YoY)	100 % (YoY)

Table 2. Incident Likelihood

With the rating scales for both impact and likely having definitions attached to them, a Risk Assessment Matrix can be prepared to help categorize the assumed risk of each individual threat.

Security Principle 002-14: *All security controls shall through the design process, apply risk analysis to measure the business impact it is meant to mitigate*

Security Principle 002-15: *For the security architecture to remain business driven, the cost of implementing a security control should not significantly exceed the estimated business impact of the risk it is meant to mitigate*

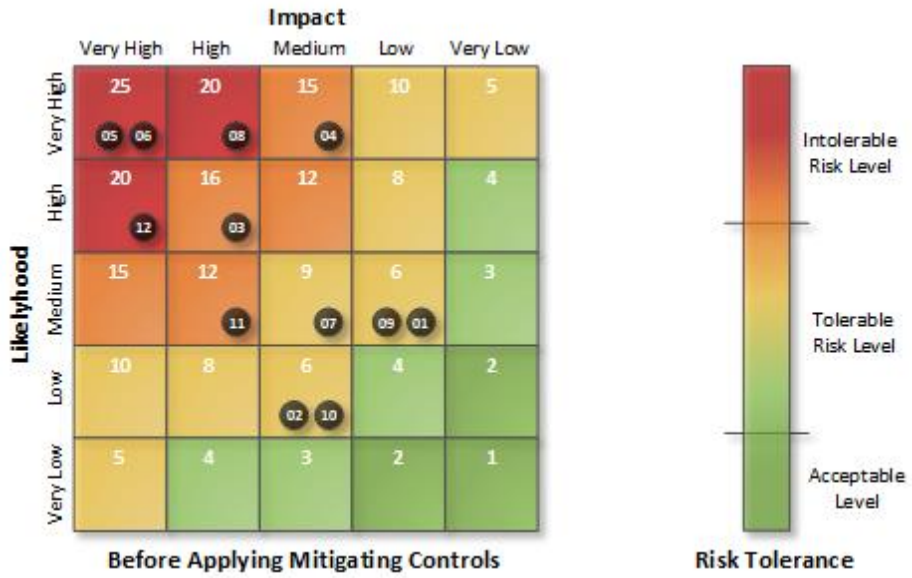


Figure 8. Risk Assessment Matrix and tolerance levels

Using the matrix and rating scales, the likelihood of each individual threat occurring, and its impact can be analyzed to determine what risk level the threat can be classified as. Plotting in all the identified threats as shown in the figure above will give the information needed to prioritize the list of threats that needs to be mitigated.

The combination gives the following levels of risk applied to each threat.

- Acceptable
  - 1-2 Negligible
- Tolerable
  - 3-4 Minor
  - 5-10 Moderate
- Intolerable
  - 12-16 Major
  - 20-25 Critical

Acceptable are minimal risks that can be properly managed to be kept remaining at an insignificant level. The tolerable range is risks which are considered where mitigating measures cannot be applied or where the cost of mitigating the risk would outweigh the potential business impact. Intolerable risks are those which are to be considered unacceptable under any circumstances and cost levels and which require immediate attention to resolve. The thresholds which are defined above are based on an average organizations organization's risk appetite and may change based on the willingness to accept risk.

Security Principle 002-16: *Clear tolerance levels for acceptable risk should be defined*

Security Principle 002-17: *Risk tolerance levels should be anchored with senior management and/or the board of the organization*

A risk assessment can help determine if there are any specific types or categories of threats that would require special attention or any threats that need to be handled in the immediate future.

Minor or moderate threat risks can be managed for continuous improvement and may not necessarily require immediate remediation in the form of implemented security controls. For a major threat risk, risk reducing measures must be implemented in the form of security controls and for critical ones, immediate action needs to be performed. In the example above, 7 out of 12 identified threats are in the area of intolerable risks and thus requires an action plan to implement controls to bring down the threat risk to acceptable levels.

The identified action plan will give a priority to what threats are identified as potential risks and the potential business impact may be. This input is important in the work of defining the controls since the price tag of implementing a control should not exceed the risks it aims to mitigate by a tenfold. Once the controls are defined, the efficiency of them can be measured and an updated risk matrix after applying the controls can be made to see the remaining, or so-called residue risk for the organization. Residue risk and capability development tracking is described in section **5** together with the method for measuring security control effectiveness.

3.10 Measuring control effectiveness

Through the discovery process and the earlier steps of the threat, risk and business impact assessment and evaluated in section a set of security controls are implemented to mitigate the risk factor to the various threats and bring them down to tolerable or manageable levels. To see how good these controls are at reducing risk, their effectiveness needs to be assessed.

Measuring the effectiveness of a defined control is difficult for many organizations and is often subjectively applied. Actual and concrete evidence is required to prove the controls in place are right for the resources, budget and assumed risk mitigation, and this section tries to apply a mathematical and objective way of doing measurement and apply them to the designed controls

Each security control is something that is currently in place to reduce risk within the organization as shown in the figure below, but special focus should be looked at for those security controls that are being implemented to mitigate the major or critical risks. These are identified risks that if they were to materialize as a security incident, would have serious impact for the sustainability and survivability of the organization.

From a security posture perspective, that applies in particular to controls that are required in the dimension of visibility and incident response capabilities to detect and deal with identified threats. Although focus should first be placed on the critical controls, the broader spectrum of capabilities also needs to be addressed since it makes no sense to go threat hunting if perimeter boundaries are not properly managed and the red carpet is rolled out for threat actors of all tiers.

The first thing to measure effectiveness of a control to define its level of criticality to the risk it is meant to mitigate. This can be done on a scale from 1-5 as shown in the table below.

Control Criticality	**Description**
5	The control is absolutely critical to the management and reduction of the risk. If this control is ineffective or partially effective, the likelihood and/or impact of the risk will increase significantly (3+ levels)
4	The control is very important to the management and reduction of the risk. If this control is ineffective or partially effective, the likelihood and/or impact of the risk will increase (2+ levels)
3	The control is important to the management and reduction of the risk. If this control is ineffective or partially effective, the likelihood and/or impact of the risk will increase (1+ levels)
2	The control has some impact on the management and reduction of the risk. Depending on the criticality of the other controls, an analysis should be undertaken to determine the necessity of this control.
1	The control has little to no impact on the management and reduction of the risk. It is unlikely this control is required.

Table 3. Control Criticality

This method can be used to identify a control, map it against the risks with the highest level of consequence and then assess them for their criticality. Using this approach, a list of controls associated with that risk that they mitigate can be produced. The next step is to measure them for their effectiveness since they not only need to be effective, but require also require proof of their effectiveness, which needs to be obtained in an objective manner. The table below gives a mathematical approach into defining what is defined as effective.

Effectiveness	**Performance**
Effective	100% of the incidents the control is meant to mitigate is prevented 100% of incidents identified by the control are mitigated within specified timeframes
Mostly Effective	80-99% of the incidents the control is meant to mitigate is prevented 80-99% of incidents identified by the control are mitigated within specified timeframes
Partially Effective	50-79% of the incidents the control is meant to mitigate is prevented 50-79% of incidents identified by the control are mitigated within specified timeframes
Not Effective	<50% of the incidents the control is meant to mitigate is prevented <50% of incidents identified by the control are mitigated within specified timeframes

Table 4. Control Effectiveness

Based on the assessment above a series of security controls can be defined, have criticality levels attached to them and then measured for their ability to mitigate risks originating from different levels of threat actors based the measurement of mitigation as described in **Table 4**. Threat actor mitigation level (TAML) efficiency ratings are based on the ability to suppress and mitigate the

different threat actors' ability to exploit attack vectors and vulnerabilities as identified in attack trees or through other security intelligence. The efficiency of the defined control to mitigate those threats at its different implementation levels.

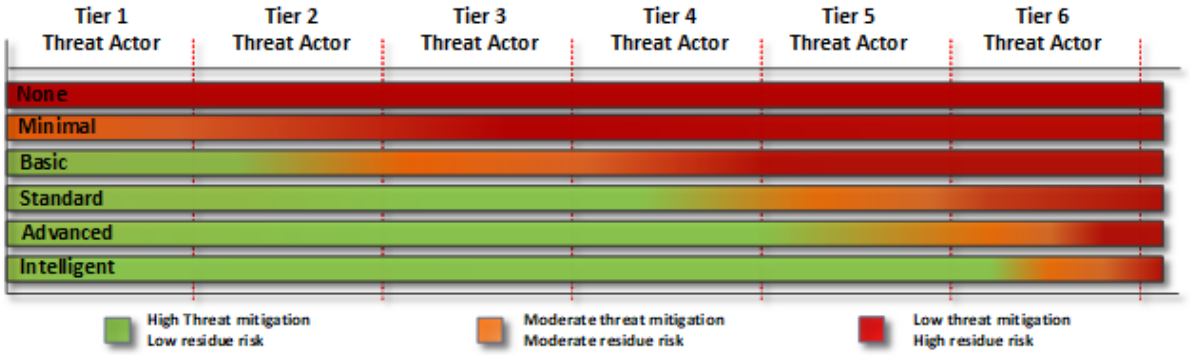


Figure 9. Sample security control threat mitigation efficiency

In the figure above a sample capability is green when assumed to be effective or mostly in mitigating a threat, orange when of partially effectiveness, and red when it is considered to not be effective to mitigate a threat. This is based on the assumption that more advanced threat actors are able to circumvent to more basic controls and additional and more advanced features are required for those. To see the residue risk after finalizing and applying the controls see section **5**.

Security Principle 002-18: *Security control effectiveness shall be measured at regular intervals and no less than on a yearly basis*

Security Principle 002-19: *Security control effectiveness shall always be measured after a successful breach is conducted*

3.11 Applying principles of zero-trust

Defendable architecture applies the principles of the zero-trust security model, also known as zero trust architecture (ZTA) as part of the security control design process.

The main concept behind the zero-trust security model is "never trust, always verify," which means that no devices or users should by default be trusted, even when originating from a "trusted" network such as the organization's enterprise network, even if they were previously verified.

ZTA is implemented by through

- Establishing strong identity verification
- Validating device compliance prior to granting access,
- Ensuring least privilege access to only explicitly authorized resources.

Most modern organizations infrastructure consist of many interconnected network zones various cloud services, connections to remote and mobile environments, and connections to non-conventional environments, such as IoT devices or OT and the reasoning for zero trust is that the traditional approach of trusting devices within a defined perimeter or connected remotely via a VPN is not sufficient to properly secure these complex environments.

Defendable architecture applies the abovementioned principles of zero- through its three pillars of preventive, detection and access related security controls:

- Verify explicitly, all network access
    - Use security boundaries to inspect and analyze all network traffic to and from all endpoints and devices

- Limit blast radius
  - Use security boundaries to apply micro segmentation to compartmentalize the infrastructure limiting lateral movement
- Use least privileged access
  - Restrict all resource access through privileged access management using identity-based role assignment and life cycle management of users
- Assume Breach
  - Continuous monitoring of all network infrastructure and endpoints while applying analytics for detection of both known and unknown threats at multiple levels of the infrastructure

A zero-trust model approach will, using the capabilities above, require mutual authentication, including verifying the identity and integrity of all connecting devices without regards to their geographical location, and provides access to the organization's resources such as applications and services based on a risk-score combining device identity, device health and role/attribute-based user authentication.

3.12 Finalizing the controls

The controls as shown in this document and implemented as part of a defendable architecture centers around three key areas.

Within each of the 3 defined main areas of defendable architecture there are specific security controls in the form functional capabilities, 14 in total, which aims to mitigate one or more of a threat actors attack method. Within in each of these capabilities there are 5 implementation "sub" levels meaning that additional functionality can be supplemented to the initial installed capability to address more sophisticated attack techniques.

A higher level of implementation includes the functionality in the level below in addition to new and more sophisticated features. Using a tiered approach makes it easy to measure the overall security posture of an organization as well implementing security capabilities in a staged approach as well as clearly identify what level of threat actors the enterprise is capable of resisting and detecting. These implementation levels are represented using the following labels:

- None
- Minimal
- Basic
- Standard
- Advanced
- intelligent

The none and minimal level is added for reference only and should for a security conscious organization only be a stepping stone towards the higher levels of implementation.

The first main area is that of **prevention,** which is to limit a threat actors' possibility to break into the infrastructure in the first place by building a strong perimeter and putting sensitive data in the internal parts of the infrastructure. The second purpose of an infrastructure focusing on prevention is to have proper mechanisms for resource isolation to make lateral movement in the infrastructure as difficult as possible.

Basic capabilities in this area aim to provide the separating external and internal applications from each other using security boundaries with port and protocol capable filtering. The standard capabilities aim to protect data to a larger degree, putting critical data in more well protected parts of the infrastructure and using security boundaries that are capable of recognizing specific

applications traversing the network. The more advanced capabilities are targeting sophisticated threat actors and also takes into account the companies operating model and any threat actors targeting any third parties to use their credentials for unauthorized access. Security boundaries can correspondingly be more intelligent using community-based analysis and malware detonation services and threat intelligence feeds to be able to provide a dynamic and automated enforcement of policies.

Equally important to preventive capabilities if not more is the second area of defendable architecture which is **detection**. If a threat actor manages to breach the network perimeter and gain a foothold, it is paramount that it is detected so that a proper incident response can be conducted with the aim of evicting the threat actor. Since all components used are software with billions of lines of code collectively in them, all with the possibility of a flaw, having a threat actor being able to eventually breach a system if not an eventuality, it's a certainty. While the preventive capabilities will keep out the lower levels of threat actors in the pyramid shown in **Figure 5** the more advanced threat actors will sooner or later find their way in and when they do they need to be detected and evicted.

Basic detection capabilities is mostly signature based and manually triggered, thus targeting known exploits and attack methods used by threat actors. Intermediate detection takes into account that the threat actors are using 0-day exploits that are not known and thus will not be captured by signature-based tools and response mechanisms. The advanced detection capabilities assumes that threat actors are capable of creating their own vulnerabilities as required and applies AI and machine learning capabilities to deployed tools to perform behavioral analysis of network traffic and log data. Making detection more Integrating detection capabilities with each other using automated triggers on anomaly detection is also a key to the advanced detection capabilities giving a response time significantly faster against the higher tiers of threat actors.

If the aim is to primarily mitigate tier 5 and tier 6 threat actors, monitoring should be higher on the priority list than preventive capabilities as there is no such thing as an impenetrable defensive fortress [34] since new techniques and attack methods are continuously being developed. That being said, keeping perimeter defenses and resource isolation up to a proper level is still important to maintain security posture and ensure that the job for a threat actor to get into the infrastructure in the first place and to make lateral movement as difficult as possible while at the same time avoiding detection.

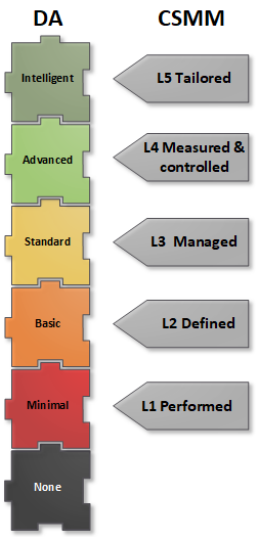
The third key area is **access** to the infrastructure, both on allowing operators legal access in a secure way to perform their daily tasks and ensure that what they access is based on least privilege and need to know basis. With infrastructure operations in a larger degree than before becomes outsourced, the requirement for well-developed capabilities for access is also increasing.

Basic capabilities include a centralized directory for user access and authorization so that access to a given system can be managed in a single point along with using PAWs during installation and vpn and multi factor authentication to access the infrastructure remotely. The intermediate capabilities add on a more sophisticated remote access platform to verify the integrity of the endpoints connecting and mandatory use of PAWs for all access. The more advanced access capabilities introduce a full-fledged use of VDI for remote operators using dynamic desktops as well as identity management to support the full lifecycle of user access of all internal and external users. Intelligent level of access management includes dynamic desktops and policy driven and automated identity management and access provisioning

[34] https://en.wikipedia.org/wiki/Maginot_Line

Security Principle 002-20: *Clearly define the threat actor levels that are required to be mitigated to build the most efficient security controls to reach the targeted security posture*

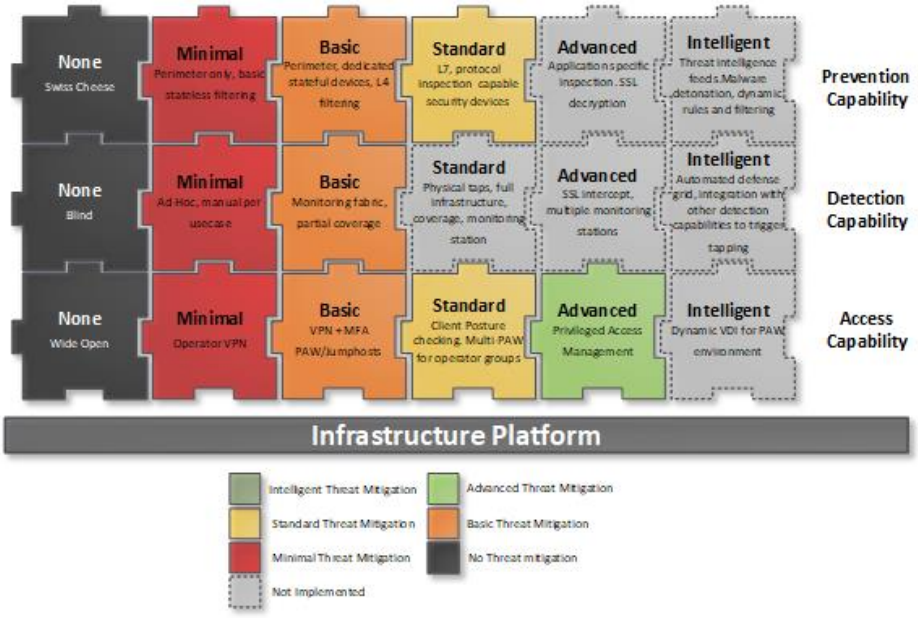
4 Defined defensive security controls and capabilities



In the previous section about designing the defendable architecture, the process of defining a set of defensive controls through threat modelling and risk analysis was described. Now let's assume that this process has been conducted and a set of defined capabilities along with their presumed effectiveness can be presented.

To mitigate the various types of threat actor types, both a multi-function and multi-tiered approach to security and implementing multiple types of control needs to be taken since their approach and methods of attack differ greatly, a control that mitigates one type of attack vector may be useless against another. Mind that the controls mentioned here is focusing on the technology aspects of control and that processes and people/competency also is fundamental for an end-to-end security posture. Maturity in security operations is essential to respond to threats and incidents but that is covered in section **7** which handle the final aspect of defendable architecture, about how to properly defend it.

A set of 14 security controls which are both interlinked and overlapping, have been defined along with different levels of implementation. This will provide direct guidance for what needs to be in place for this control to be effective and what level of threat actor mitigation it gives to measure its effectiveness. These capabilities have many things in common with the basic and foundational controls of CIS but are specifically defined and concretely scoped in regard to technology implementation and deliveries. The different types of capabilities range from minimal to intelligent, at 5 levels to also be compatible with the NIST CSMM model and drive expectations on what tools and technologies that need to be present. This can be considered a more specific guidance in the infrastructure domain in addition to the overall security maturity in the organization as measured by CSMM. Each of the defensive capabilities are detailed in separate documents in the DA framework. In the sections below, **Table 5**, **Table 6** and **Table 7** below lists the defined controls with their corresponding implementation levels while a table showing the estimated mitigation effectiveness of all capabilities can be found in **Appendix 1**.



On a high level, the capability levels can be described as follows:

Minimal is considered the least possible effort that should be taken in a capability area to have some mitigation provided. This is considered to only address low hanging fruits risk at a minimal investment level and will leave a considerable amount of unmitigated risk.

Coverage of the implemented capability is considered to be limited.

Basic applies additional effort and investments addressing more advanced threats and reduce risk more than a minimal level but should still be considered as a steppingstone to further developing the capability to a higher level. It is assumed that from basic level and beyond that the capability is operationalized and integrated into OSS systems and the OAM teams existing processes. Coverage of the implemented capability may be partial or focusing only on certain key assets.

Standard implementation level is assumed to mitigate the bulk of perceived threats, typically tier 1-4 of threat actors. For an organization that is serious about its security posture and wants to conduct a responsible level of business, this is the recommended baseline minimum in a capability area and provides a balanced approach for cost vs mitigation results. If the organization is the operator of national critical infrastructure or are regularly targeted by the higher levels of threat actors, so-called advanced persistent threats, an increased security posture and in the form higher implementation levels are required, which in turn implies additional time and effort, and not least, more money. Depending on the sector the organization operates in, this may also be subject to regulatory controls. Coverage of implementation at this level and beyond is expected to cover all of the organizations critical assets and the majority of the remaining systems

Advanced implementation levels are meant to address the higher tiers of threat actors or for organizations where a high security posture is required by default, eithers as business requirements or driven by regulations. Security capabilities are more sophisticated, and dynamic of nature involving threat intelligence feeds or the ability to do detection of previously unknown threats and identifying and classifying them through external intelligence or the ability to analyze them directly using machine learning or other behavioral based detection. The more dynamic nature of advanced capabilities is meant to address so-called zero-day threats which may be previously unknown and thus not easily detected by less advanced and often signature based capabilities that are more geared towards *known* threats.

Intelligent levels of implementation would cater for capabilities to be automated. Automation would give more efficiency into the implemented capabilities, in particularly the detection space so that more routine cases will be automatically mitigated freeing up response capabilities for the higher tiers of threat actors. An intelligent implementation level also implies that capabilities are integrated with each other to provide additional context and thus strengthen each other.

In general, the DA implementation levels defines technical capabilities which in in turn support the cyber security maturity model which measures the organization as a whole.

The different implementation levels allow the organization to pursue a stepwise implementation strategy and operationalize the usage of the capabilities to the greatest extent possible before moving on and implementing new features. Budget wise, a stepwise approach can be favorable, more on this in section **6.4.1**.

Observation 002-3: *The defendable architecture implementation levels can be used to create an overview of the implemented capabilities in the organization, so if investment doesn't allow for more than basic or minimal levels in certain capability areas, then the definitions can be used to document this so that relevant risks can be documented and addressed as per the organizations risk strategy.*

Capability	Level	Description
Resource Isolation	Minimal	Exposed services separated from other systems
	Basic	Management and service domains established. Test/dev environments are isolated from production
	Standard	Service domain segregated into exposed, non-exposed and secure zone classes. Management is shared. 4 zone classes in total
	Advanced	Management domain segregated into service management, platform management, device management, access management. 7 classes in total
	Intelligent	Dynamic resource allocation with automatic sanitation and reprovisioning.
Platform Security Boundaries	Minimal	Internal security boundaries are established only around critical assets only
	Basic	All assets have established boundaries. Security devices are stateless with L4 filtering capabilities
	Standard	Security devices are stateful have both L4 and L7 filtering capabilities. Dual technology for inter-class inspection
	Advanced	Security devices have application filtering capabilities and capabilities for SSL inspection
	Intelligent	Security devices utilize threat Intelligence feeds and malware detonation capabilities to classify unknown patterns. Dynamic filtering
Perimeter Security Boundaries	Minimal	Perimeter security boundaries are established at internet border
	Basic	Security devices have L4 filtering capabilities. Internal and external entry points covered
	Standard	Security devices are stateful have both L4 and L7 filtering capabilities. DDOS protection at internet border
	Advanced	Security devices have application filtering capabilities and capabilities for SSL inspection
	Intelligent	Security devices utilize threat Intelligence feeds and malware detonation capabilities to classify unknown patterns. Dynamic filtering
System Security	Minimum	Hardening of exposed systems, ad-hoc software updates on critical assets
	Basic	Asset management on HW assets, hardening and configuration management of all critical systems. Ad-hoc software updates on all assets
	Standard	Asset management on all SW and HW assets, hardening and configuration management of all systems. TPM supported for all critical assets. Regular process-controlled software updates on all systems.
	Advanced	Application whitelisting. TPM supported configuration management on all system.
	Intelligent	Asset management, patch management, and configuration management systems integrated and automated and policy driven. Asset discovery automatic using integration with infrastructure automation and ITSM/CMDB. Asset discovery integrated with vulnerability management.

Capability	Level	Description
Data Protection	Minimal	Data classification process, service classification process. TLS in transit on relevant exposed systems
	Basic	KMS established, at rest encryption for critical assets,
	Standard	private certificate authority & management systems, TLS in transit for all relevant systems,
	Advanced	Privacy capabilities including tokenization and data masking. Secrets management for all development processes and CI/CD pipeline. Partial confidential compute for critical assets
	Intelligent	Automated and policy driven application of controls for confidentiality and integrity, and backup for availability classes of data. confidential compute for all critical assets

Table 5. Preventive Capabilities

Capability	Level	Description
Vulnerability Management	Minimal	External scans on exposed systems. Vulnerability management process established
	Basic	Regular external scans on exposed systems, regularly. External and internal scanning performed regularly.
	Standard	VMS integrated with asset management. Prioritized patching. Output used in risk analysis process
	Advanced	Threat intelligence feed applied.
	Intelligent	Automated scans + integration with SIEM and/or EDR to trigger scans on anomaly detection
Endpoint Detection & Response	Minimal	Standard AV, critical assets only
	Basic	Standard AV, all assets,
	Standard	EDR on all assets, classes and domains. Application whitelisting on critical assets. Forensics capabilities in EDR
	Advanced	EDR with threat intelligence feeds and malware detonation for dynamic mitigation. Application whitelisting on all assets. Dedicated forensics suite for CSIRT
	Intelligent	Multi-domain XDR
Flow based network monitoring	Minimal	Partial coverage, critical assets only
	Basic	Partial coverage, management domain only
	Standard	Full coverage, service and management domains
	Advanced	Threat intelligence feed applied for anomaly detection. Encryption analysis
	Intelligent	Integration to SIEM and other detection capabilities enabling automated response

Capability	Level	Description

Logging and auditing	Minimal	Centralized logging established, critical assets log source data collected
	Basic	Centralized log platform, all systems log source data collected
	Standard	SIEM and analysis capabilities applied to centralized collected log data.
	Advanced	Threat intelligence feeds applied. Security analytics expanded to cover user behavior.
	Intelligent	Automated response capabilities applied to SIEM, SOAR systems implemented.
IDS/IPS	Minimal	signature based IDS at internet border
	Basic	signature based IDS at internet border and exposed systems
	Standard	Event based IDS, all internal and external entry points and critical assets covered
	Advanced	Threat intelligence feeds and malware detonation
	Intelligent	Traffic playback capabilities
Network Tapping	Minimal	Ad-hoc, built-in functionality of network switches
	Basic	Monitoring network established, partial coverage of assets using taps and/or mirror ports, can support 1-2 continuous use cases on selected parts of network
	Standard	All assets covered by network tapping, can support 5+ continuous use cases, ad-hoc tapping at any point in the network. Security monitoring station for analysis of captured traffic in IR.
	Advanced	SSL decryption capabilities built into the monitoring network. Multiple security monitoring stations to support different use cases-
	Intelligent	Automated tapping, integrated with SIEM and triggered on anomaly detection

Table 6. Detection Capabilities

Capability	Level	Description
Privileged Access Workstation	Minimal	Shared PAW group for all categories of business users, operators, partners and vendors
	Basic	PAW's divided between business users and operators. Directory services and attributes to assign policies to different operator groups on shared operator PAW's
	Standard	Shared operator PAW's divided into dedicated pools based on operator groups.
	Advanced	PAW uses VDI infrastructure supporting hosted desktops for key operator groups
	Intelligent	PAW uses VDI infrastructure with dynamic and/or hosted desktops
Secure remote and Operator Access	Minimal	VPN for all remote access. Direct access to resources via vpn
	Basic	VPN and MFA for operator access. All resources accessed via PAWs.
	Standard	Posture checking of remote clients connecting to VPN
	Advanced	privileged access management solution with session recording of all operators and password rotation
	Intelligent	Context based access control. ABAC
Identity and Access Management	Minimal	IGA Process established, manual approval, audit and reporting
	Basic	IAM system established. Lifecycle of identities managed. Approval, audit and reporting streamlined. Centralized directories, GPO controls everything. Role based access control model.
	Standard	IAM system integrated with target systems for user (de)provisioning. Critical assets and most of management domain IAM integrated. All accesses role based. Centralized AD with multi-tiered privilege separation. SSO available for applications.
	Advanced	Periodic reconciliation of provisioned accesses. Full IAM solution for identity lifecycle management and asset authorization. Identity Analytics for user behavior. Authentication services are context based and attribute driven (ABAC).
	Intelligent	Automated provisioned auditing, reporting and reconciliation of provisioned accesses. Majority of target systems in management and service domains integrated. Policy driven access rights.

Table 7. Access Capabilities

*An organization who is responsible for **critical information infrastructure** (CII) for delivering basic national functions (BNF) in different industry sectors are **required** to be able to mitigate **minimum tier 4 threat actors.** CII organizations are also **strongly advised** to build the required capabilities able mitigate up to **tier 6 threat** actors if this is not already mandated in relevant national security or industry sector specific regulations.*

*For CII organizations, the **advanced** capability levels of the defined security controls are then used as the **baseline**, thus forming the requirements of the security principles covering this capability for these organizations.*

*Other **non-CII organizations** are **advised** to implement security controls capable of mitigating up to **tier 4 threat** actors, thus using the **standard** implementation levels as a default recommendation. This tier of threat actors is considered the currently largest risk likely to target organizations, either opportunistically or on purpose with the potential for major business impact.*

***Minimal** and **basic** levels are provided for **reference** and as defined steppingstones to reach the higher capability levels or as accepted risk through a defined risk management process.*

4.1 Preventive Capabilities

To address the protective capabilities to ensure containment, one of the key attributes of a defendable architecture, the technical implementation of the infrastructure itself plays an important role as attacks become increasingly targeted and more technically advanced as documented in the earlier mentioned Mitre attack chart. Critical infrastructure will be subject to further attacks in the years to come by multiple threat actors including criminals, foreign government agencies, and their contracted proxies.

Newer threats are launched faster than ever. Threat sophistication uses ever-evolving attack methods, which are increasingly targeting application-layer vulnerabilities as shown the figure below. Targeted attacks are another major concern.

Threat actors often develop customized attack mechanisms to take advantage of an organization's specific equipment, systems, applications, configurations, cloud environments, and even personnel employed at specific locations,

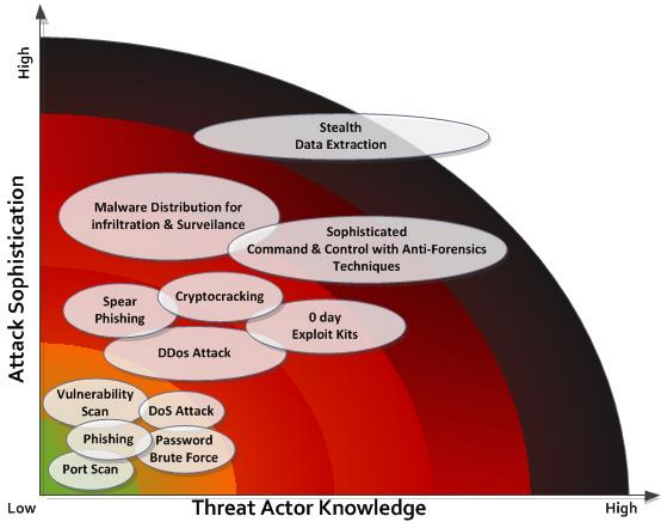


Figure 10**. Threat actor tactics techniques and procedures**

A secure operating environment provides the foundation for operational stability, enables secure outsourcing and offshoring, and creates the necessary prerequisites for meeting legal/regulatory

requirements and building trust with the customer. Creating such an environment requires a holistic security approach across multiple and overlapping security controls.

Preventive capabilities set out to define the requirements for achieving this goal and to describe the different aspects of the infrastructure security architecture as well as explain its concepts and terminology. Specifically, sections of defendable architecture document detail:

- How a zoning model can created differentiated policy domains within the infrastrucutre
- How Security Classes will be used to classify system elements according to their exposure requirements and trust level.
- How Security Zones will be used within each Security Class to group and separate system elements according to their nature and communication requirements.
- How assets are classified according to their importance to the business as a foundation to prioritization in other processes and that an inventory is built for these assets, so the organization have the knowledge about its running resources
- How data is classified and in which security classes it is stored, processed or transported and which required security controls are required to meet defined acceptable risk levels and regulatory requirements.
- How the assets are maintained in regard to configuration hardening and software updates
- How can different capabilities integrate to strengthen each other, and the combined data output provide a near real-time threat picture feeding the organization's enterprise risk management process

The goal is to conduct a responsible business by achieving a high level of control of the organization's infrastructure. To attain this control, the principles highlighted in the defendable architecture framework need to be adhered to and deviations from it be kept to a minimum.

4.1.1 Resource isolation

The different workloads of the organization usually run on an infrastructure platform that is usually shared and operated and maintained by different groups of operators and users accessing it. Since the components are shared and interlocked to remain effective there is always the risk that a security breach within one component can then spread to other components and result in several undesirable scenarios ranging from devastating data loss through exfiltration and subsequent sale of confidential data on the dark web, to having the organizations systems and data encrypted by ransomware or stolen by foreign intelligence services.

To properly address the risk of using shared components in a multi-tenant platform and avoid a threat actor to spread uncontrollable though the infrastructure it is required to sufficiently isolate the resources from each other according to the threat level that is required to be mitigated. To assist in a systematic approach to provide sufficient resource isolation and containment, a concept called “security zoning model” or zone model for short have been developed into a security capability.

The defined zone model regulates how an infrastructure platform should be built with resources isolated from each other in different layers and enables the creation of different policy domains where rules for exposure, data processing/storage and access can be defined independently from each other. Resource isolation and zone model is also fundamental into achieving zero trust networking by creating isolated segments for different services that is enforced by security boundaries and thus provides an effective segmentation is of the entire infrastructure. Resource isolation is one of the cornerstones of the defendable architecture as the zone model influences the practical implementation of many of the other security capabilities.

The zoning model partitions the infrastructure into watertight compartments that are isolated from each other, and the different zones are labelled and graded depending on the data stored in them, their exposure to high-risk environments, and the trust worthiness of the people accessing and operating the components inside the zones. Principles and examples of how to apply zoning for the different types of HW and SW components is at the core of this document.

Depending on requirements of what tiers of threat actors to mitigate, risks and chosen operating model of the infrastructure, different zone models for resource isolation can be used as defined by the different capability levels described. The model chosen will reflect the requirements of the respective enterprise, but the policies attached to the chosen zone model needs to be clearly defined, documented and communicated to be anchored through the entire organization.

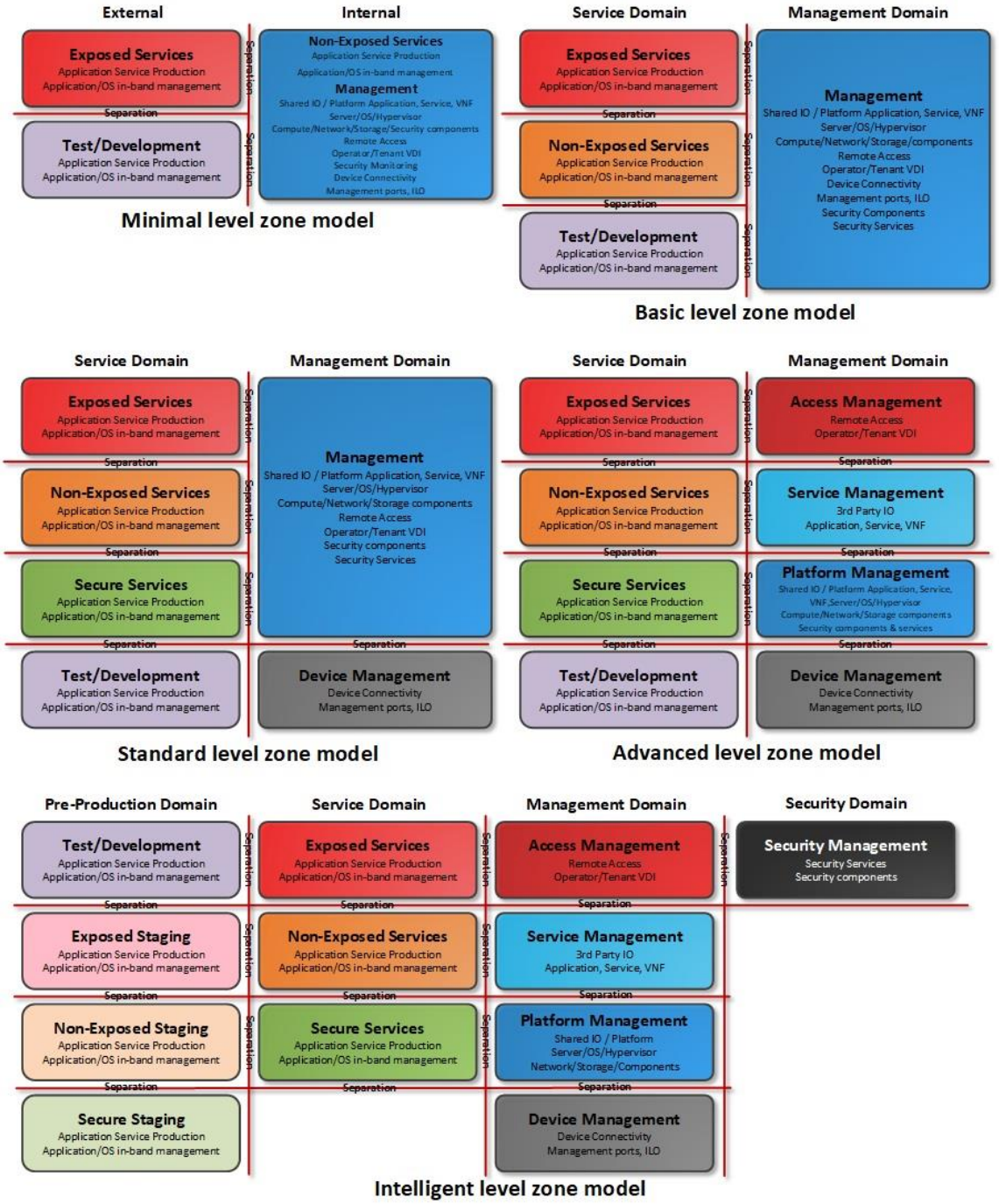


Figure 11**. Differentiated zone model deployments**

There is possible to optimize cost vs risk levels and mitigation efficiency by looking into what technology choices are made in building the different security boundaries between the security zone classes. This is described in detail in the security boundaries section as the resource isolation defines the level of separation required for inter zone and intra zone class traffic, but technology choices and suggested optimization is a topic when discussing the security boundary itself.

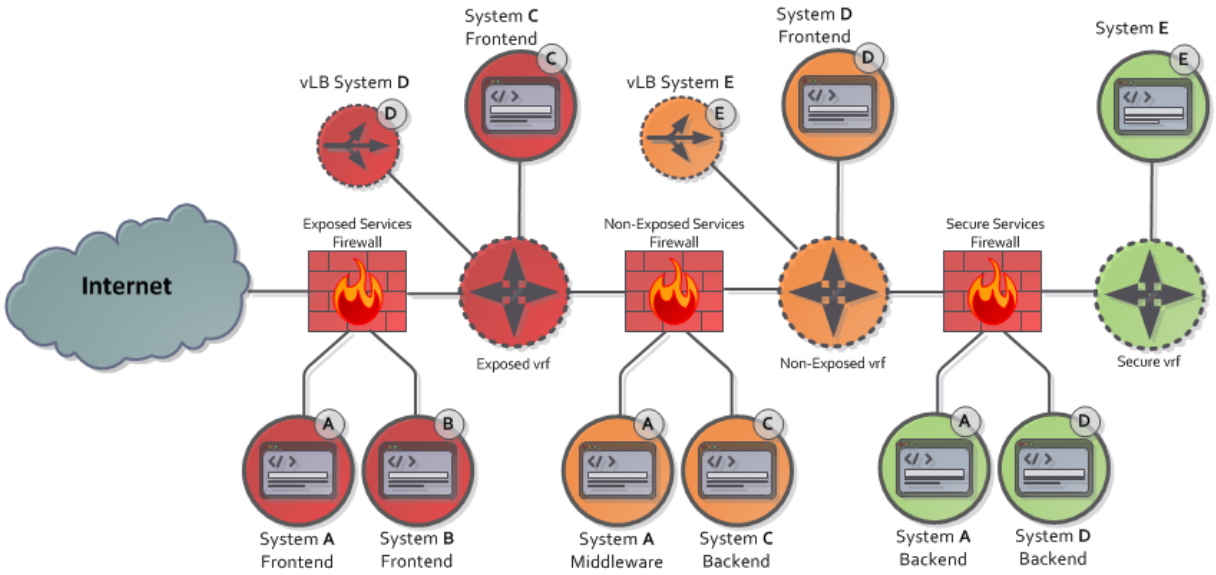


Figure 12. Resource isolation using application zoning

The infrastructure support services are those that all the applications in the infrastructure are dependent on such as active directory domain controllers, dns, ntp, media servers for application backup, session recording proxies for the PAM solution etc. When every single component in the infrastructure needs to communicate with a small subset of shared components, these components can become excellent pivot points if compromised. When breached they can be utilized by a threat actor to move around laterally after an initial breach since the security boundaries are configured for them to freely communicate with all the components. It is therefore important that these services are deployed in a federated way that reduces the exposure of a single support service system to the overall production systems so that the possibility to leverage them for lateral movement is as small as possible.

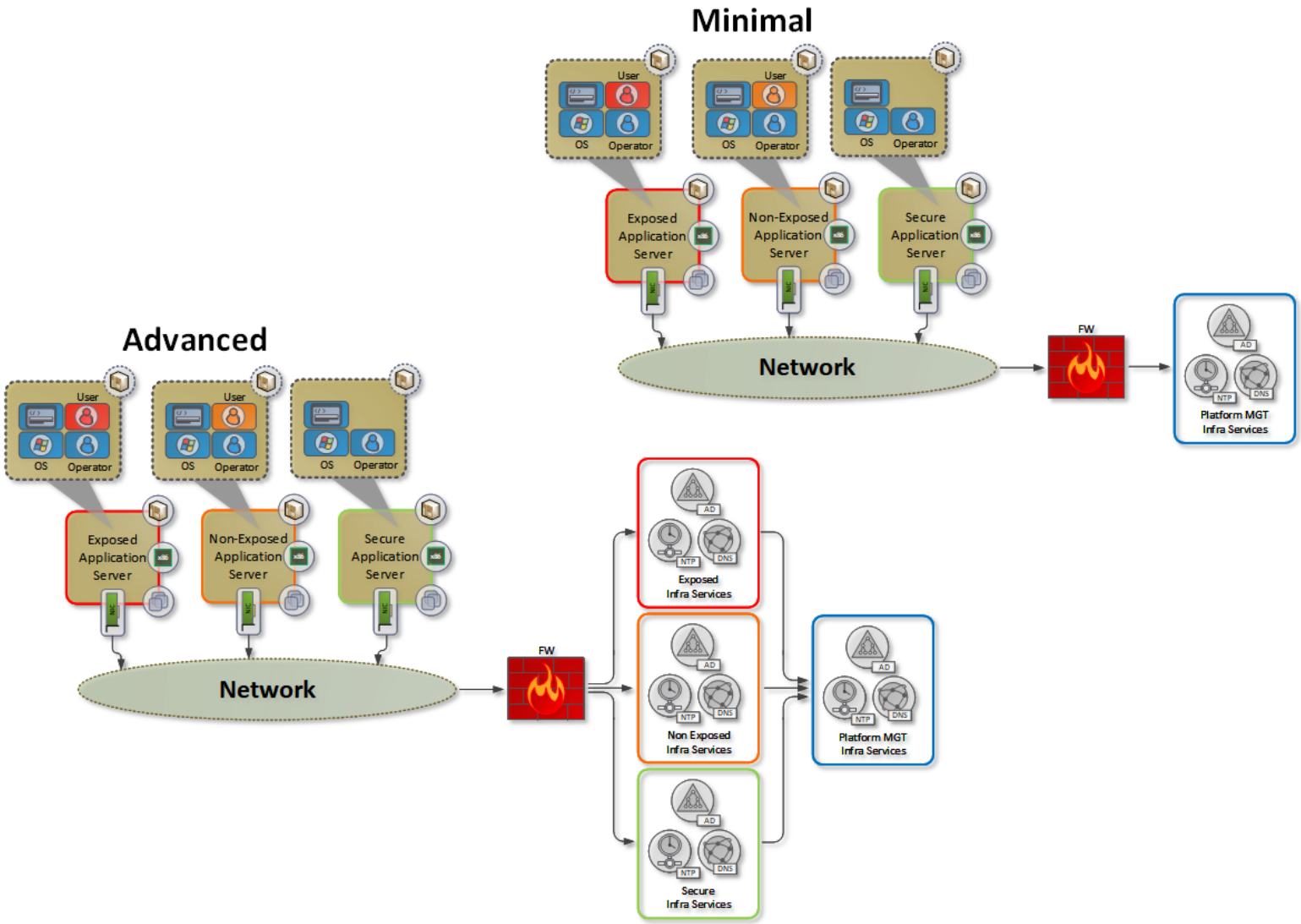


Figure 13. Infrastructure support services

The table below shows an example policy as applied to a CL5 zone mode:

Classification		*Network Communication*			*Data*		*Access*
Security Domain	**Security Class**	**Controlled Zone**	**Uncontrolled Zone**	**EUC Zone**	**Processed**	**Stored**	**Typical User group**
Service	Exposed Services	Yes	Yes	Yes	D1-D4	D1	End customer Accessible Services
	Non-Exposed Services	Yes	N	Yes	D1-D4	D1-D2	Employee Accessible Services
	Secure services	Limited[35]	No	No	D1-D5	D1-D5	N/A
Pre-Production	Test/Dev	Yes	Yes	Yes	D1-D4*	D1-D4*	Developers Testers
	Exposed Staging	Yes	Yes	Yes	D1-D4	D1-D4	Testers
	Non-Exposed Staging	Yes	N	Yes	D1-D4	D1-D2	Employee Accessible Services
	Secure Staging	Limited[36]	No	No	D1-D5	D1-D5	N/A
Management	Platform Management	Yes	No	No**	D1-D4	D1-D4	Platform Operators IO Vendor
	Service Management	Yes	No	No**	D1-D4	D1-D4	App/Service Operators
	Access Management	Yes	Yes	Yes	D1-D2	D1-D2	All operators
	Device Management	Limited[37]	No	No	N/A	N/A	Platform Operators IO Vendor
Security	Security Management	Limited[38]	No	No	D1-D5	D1-D5	SOC CSIRT

Table 8. Zone class requirement reference

The policies applied clearly regulating what traffic is allowed to other networks, and what data is allowed to be stored and processed in the different parts of the infrastructure. Other attributes can be applied regulating any specific behavior of workloads or access models but having the definitions

[35] From non-exposed security class in staging domain and management domain
[36] From non-exposed security class in service domain and management domain
[37] From access management and platform management only
[38] Only for select authorized user groups

of the zone model as a baseline, this behavior becomes predictable and the infrastructure can be come more manageable, a key condition to properly support automation. Resource isolation and policy enforcement is strongly connected to asset classification (highlighted under DA capability system protection) and data classification (highlighted under DA capability data protection) processes.

The **minimal** level of resource isolation separates only the external facing service that exposed to untrusted domains such as the internet, all other service production is in one policy domain/security zone class. Non-exposed production applications and management services reside together in the same zone class with no hard separation boundaries. Test and development are kept separate from the production. Isolating the exposed services from internal data and management functions and test/dev from production is to be considered a bare minimum and would require significant effort in the other capability areas for the overall risk profile to be kept at reasonable levels.

Infrastructure support services are typically deployed as a single tier, this applies no additional mitigation measures or isolation apart from what is already implemented in the security boundaries and the resource isolation model.

The **basic zone model** segregates the platform infrastructure components one step further into additional security classes. External services facing uncontrolled network domains such as the internet remain in a separate zone class similar to the minimal model but internal services for various backend services such as file and data base storage and management for all administrative functions is separated into an additional policy domain/zone class. All management functions are mixed together, and application and database layers are also sharing resources.

It is however possible to build a strong network perimeter for the external services and thus being able to mitigate efficiently threat actors up to a certain level of sophistication depending on what additional defensive capabilities that are deployed.

The **standard zone model** deployment acknowledges that the main important assets to protect, is the organization's data from either theft or hijacking with ransomware from more sophisticated threat actors. All critical data is moved further into the infrastructure in the secure services zone class where stricter policies can be enforced such as denying corporate end user devices access directly. Adding the device management zone class for direct access to physical devices and separating this from the general management acknowledges that physical access to devices is key to defending whatever is running on top of them and that separate out of band access will provide an additional benefit for operational staff to handled operational incidents.

All other management functions such as tools, remote access and operator jumphosts are sharing components though. This zone model is meant to mitigate up to tier 4 threat actors who are mainly cyber criminals whose objective is to seek out the organizations data or other information that can be sold.

The **advanced zone model** further separates the management domain into 4 classes. Access management which involves anything related to remote access such as vpn, jumphosts etc. have its own security class not sharing resources with the other management classes. This concept is key to make sure that the VDIs and terminal servers used as jumphosts cannot be used as a pivot point to attack other services in the management domain by isolating them physically. In addition, the service management class is created to serve operators and application administrators and developer who largely may be external entities such as managed services providers.

Isolating the resources and tools for this group of users from those operators who are responsible for the operations of the entire platform mitigates the threat of a service provider being compromised and their resources being used to attack other management functions and services via shared components. The advanced zone model is meant to mitigate up to tier 6 threat actors. The advanced

zone model is also very costly to deploy for small or medium infrastructure installations. For this to be effective it makes sense to deploy this model where APT groups are being faced and data that needs to be protected falls under regulatory legislation where large fines are applicable for data loss. Alternatively, if the size of the infrastructure is very large, the scale may naturally mitigate the cost of the advanced and more complex resource isolation deployments, since it will be just another way of structuring the components together.

At **intelligent** level, the zone class model introduces two additional domains, the pre-production domain which isolates the test/dev as well as staging environments from the production domains and the security domain.

The pre-production domain isolates staging in addition to test/dev environments further, whereas in the earlier models staging was part of the service domain. This promotes stability when developing services and provides the ability to isolate the test/dev and staging from the production domain by policy.

Establishing the security domain physically isolates all security related services such as logging, security analytics capabilities of flow-based networking, IDS management etc. The rationale for this class is to it completely isolate it from the rest of the production domain, so in case of a compromise of the entire platform, the security management class can be the secure bastion from which the CSIRT team performs incident response to regain control of the rest of the infrastructure.

All infrastructure support services are at this level deployed in a federated fashion using two tiers. The first tier is zone class specific and all the endpoints in their respective zone class communicates with these services. The second tier is the “master” of the zone class specific services and will be deployed in will be in the platform management zone class., and the management systems in the two tiers will communicate in a master-slave setup, where the platform management instance will act as the master.

The intelligent level zone model, similar to the advanced option, also comes with significant cost implications and should be deployed by those organizations that need to resist tier 5 and 6 threat actors on a regular basis or is considering using their infrastructure to offer managed security services and and/or needs to have a very strict cadence on their infrastructure.

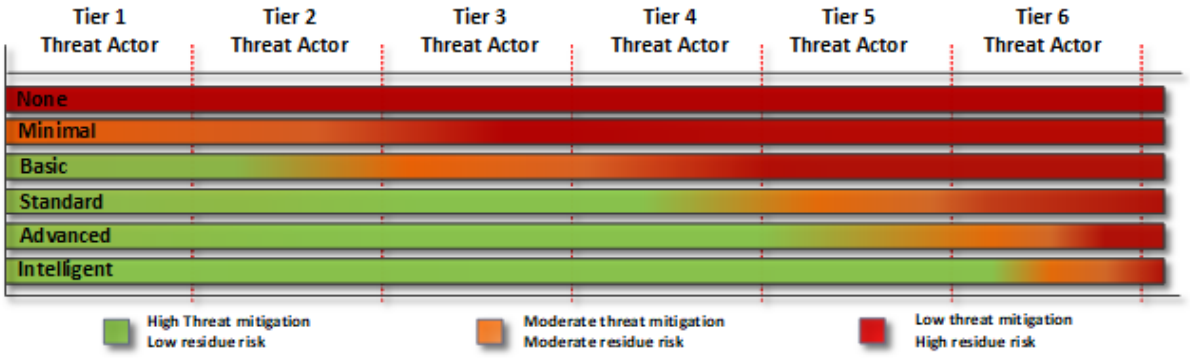


Figure 14. Resource isolation mitigation efficiency

The mitigation efficiency for each of the types of deployment is measured in the figure above.

4.1.2 Platform security boundaries

The security boundaries are the gatekeepers that verify traffic between the different network zones and zone classes of the platform to ensure that the traffic is according to defined policy and to validate that the traffic types are what they are claiming to be. Depending on how advanced the feature set is on the different devices being deployed as security boundaries are, they can be more

effective to detect more sophisticated threat actors performing lateral movement between the different network segments or turn unknown patterns into known ones through analysis and decryption.

At a **minimal** level of implementation, platform security boundaries are established only around critical assets and using stateless filtering in the form of network access lists or embedded functionality in the underlying network infrastructure. These stateless boundaries are capable of layer 4 inspection only, such as source/destination ip address and port/protocol.

At **basic** implementation level the devices used as security boundaries have filtering capabilities on port and protocol level, they may be either stateful or stateless, but does not have to have deep packet inspection capabilities to verify the actual content of the packet stream. Router Access List, Open vSwitch filters, host iptables or firewalls with basic filtering capabilities fall within this category. At basic level, all services have established internal security boundaries between in a zero-trust model and can be considered micro segmented. Security devices are limited in functionality to stateless filtering devices for both interclass as well as intra class boundaries.

At **standard** level, security devices used to form the platform security boundaries are supplemented with more advanced capabilities in the form of do deep packet inspection of the network traffic and is able to recognize what applications that are being used, giving the ability to do much more detailed filtering. Deep packet inspection gives intelligence to the protocol level inspection and can determine that the protocol being used is the one that was actually permitted so unauthorized traffic can not leverage authorized network openings. Intra-class traffic may still use stateless filtering devices, but interclass traffic always pass through a device capable of stateful, deep packet inspection. Critical assets are expected to have stateful security devices as their security boundaries also for intra-class traffic where possible.

At the **advanced** level, the stateful security boundary devices should also have the ability to do full layer 7 inspection of application specific controls and be capable of decrypting SSL traffic so that protocols such as https and ssh can be properly inspected.

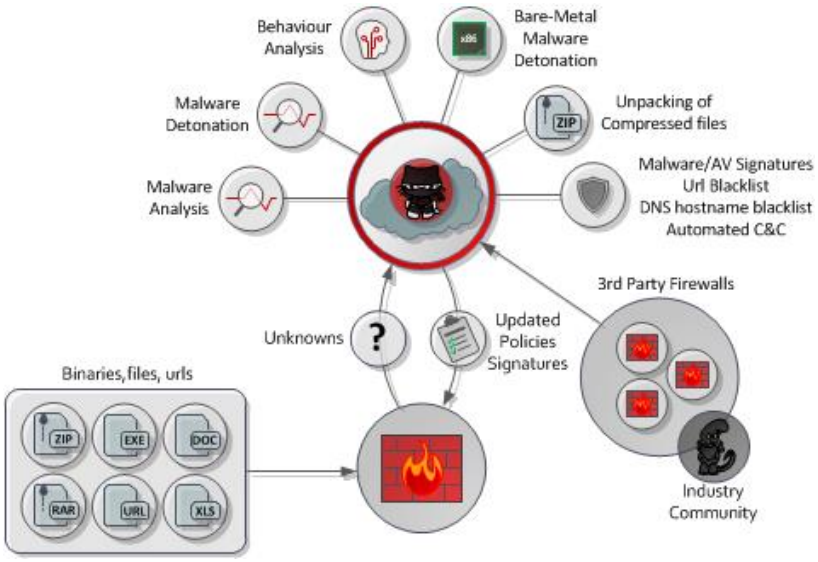


Figure 15. Intelligent security boundary device using unknown file analysis

The main differentiator between the **intelligent** level of capability implementation of security boundaries and the others, is the ability to ingest external threat intelligence feeds. In combination with community-based threat intelligence where unknown files or patterns are sent for external analysis to look for indicators of compromise, which is then shared among all the subscribers to that

threat feed. The enables the security boundary devices to be able to apply dynamic policies for threat prevention to enable automated prevention of detected threats when using deep packet inspection.

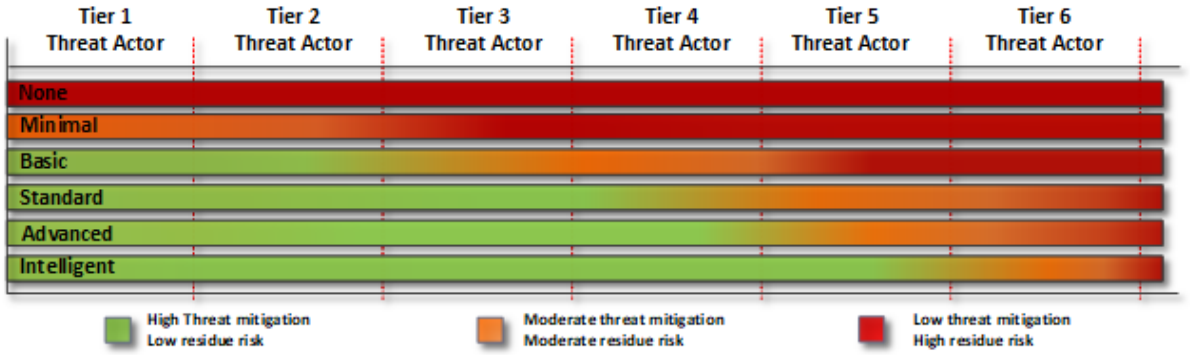


Figure 16. Platform Security boundaries mitigation efficiency

The mitigation efficiency for each of the types of deployment is measured in the figure above.

4.1.3 Perimeter security boundaries

The perimeter security boundaries are the external boundaries that are deployed between the infrastructure platform and uncontrolled or untrusted networks. Some of the components would be using the same technology as for platform security boundaries, but since they are guarding the network perimeter should be physically different from those taking care of the internal security boundaries of the platform as per recommendation of the resource isolation separation principles.

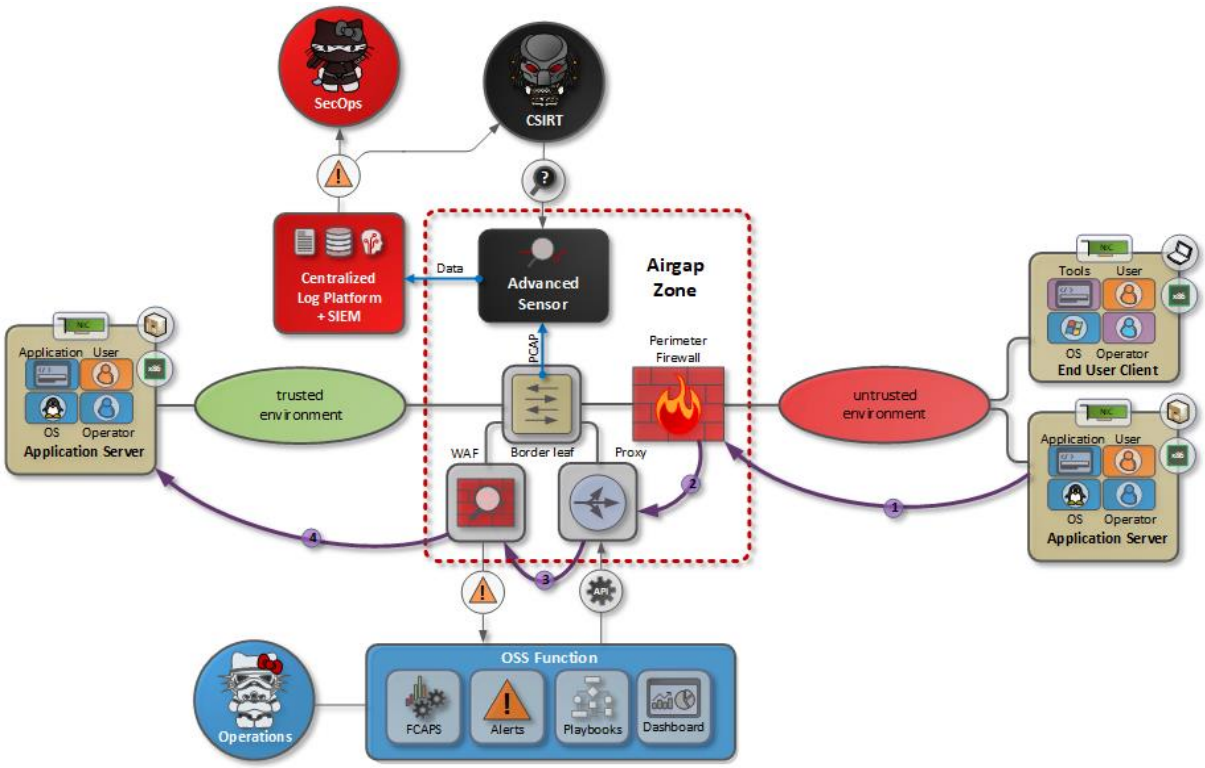


Figure 17. Perimeter security boundary with air gap functionality

At a **minimal** level of implementation, perimeter security boundaries are established only around external entry points such as internet access and using the built-in capabilities of the underlying network infrastructure such as switches and routers.

At **basic** implementation level, the network perimeter security boundary would utilize dedicated devices for the function, with the devices being stateful and capable of building security policies up to layer 4 with basic recognition of protocols and ports. Scope of implementation is at this level and beyond, expected to cover all internal and external entry and exit points.

At **standard** level of perimeter security boundaries, the security posture is further increased, all applications or services that are exposed to an untrusted or uncontrolled network would need to be protected by a layer 7 inspection capable device. Similar to the platform security boundaries, standard perimeter security boundaries include the ability to do deep packet inspection and discover vulnerabilities at protocol levels that a basic security device would not. In addition, an external network perimeter security boundary would include DDOS protection in some function, either integrated or external.

Perimeter security boundaries at this level would also be supported by functionality from one of the capabilities in the detection area, namely the specialized network IDS functions as shown in the figure above. The IDS will monitor all traffic crossing the perimeter to or from external networks, this enables the SOC teams to monitor traffic to known C&C destinations and help the CSIRT team during an ongoing incident to track progress and status of evicting a threat actor.

Advanced implementation level builds on the stateful security devices to include application specific detection and filtering capabilities. This can include threat prevention in firewalls, web application firewalls or malware detection capabilities. Capabilities for full layer 7 inspection of applications and SSL decryption are deployed in all perimeter security boundary devices.

At an **intelligent** capability level. The security boundary devices are equipped with the ability to consume external threat intelligence feeds and perform analysis of unknown files and patterns through malware detonation and community analysis.

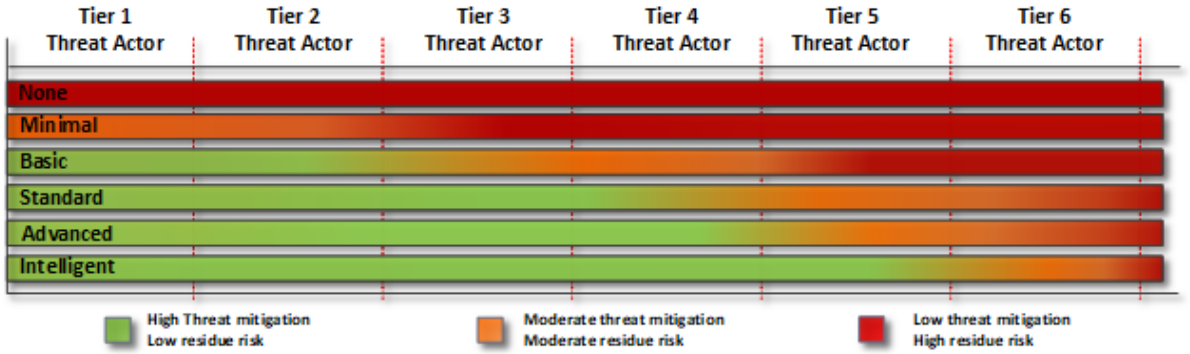


Figure 18. Perimeter Security boundaries mitigation efficiency

The mitigation efficiency for each of the types of deployment is measured in the figure above.

4.1.4 System Security

Hardening of the software and configuration of all deployed software is the act of configuring it securely, updating it, to create rules and policies to help govern the system in a secure manner, and by removing unnecessary applications and services that may be enabled by the default configuration.

This is done to minimize the components attack surface and will reduce the exposure to any potential threats.

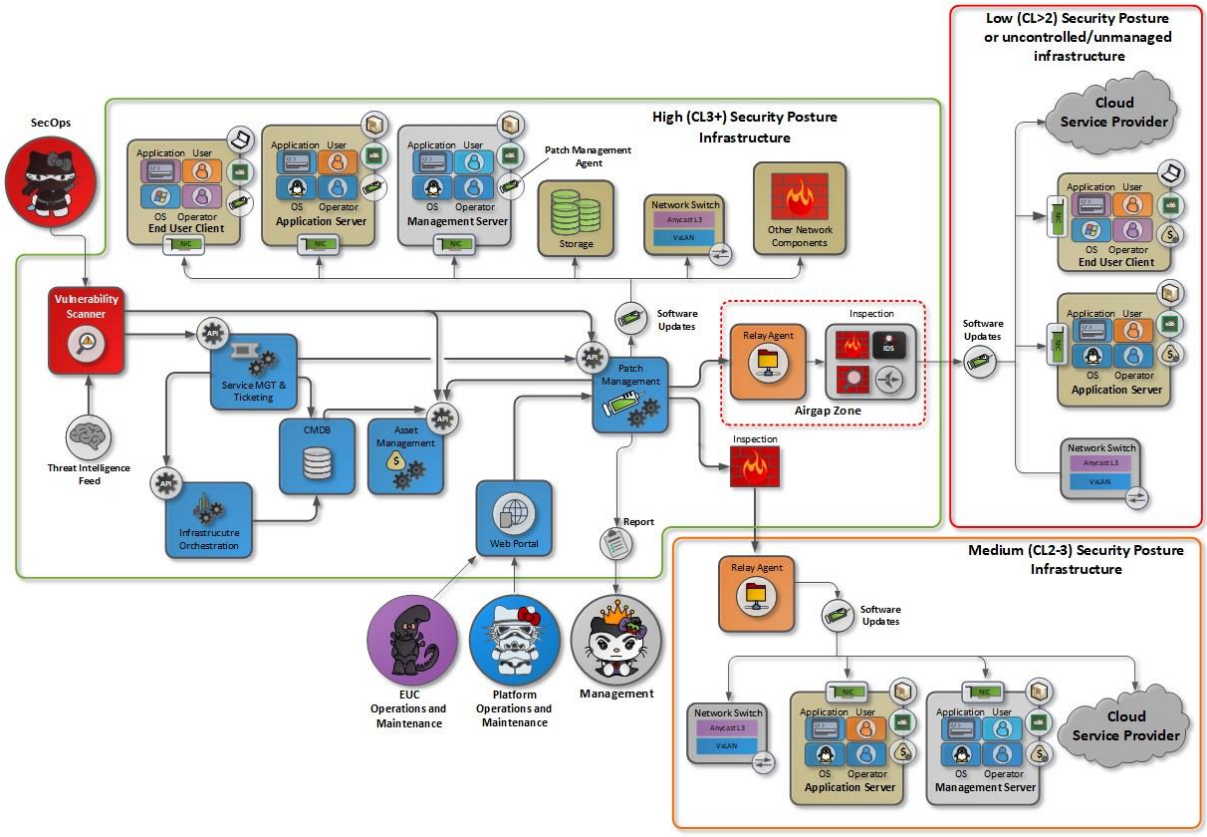


Figure 19. Patch Management Solution

Part of a **minimal** implementation of software security is to protect the services and systems exposed to the internet or other uncontrolled and/or high-risk environments. This implies, although limited, a deployment of configuration management processes to harden operating systems, network devices and security appliances and secure their configuration using hardening templates. This hardening should be according to best practices such as those given by CIS, SANS and NIST. Critical software updates are deployed ad-hoc on key assets.

Basic implementation level implies the functions around asset management have been introduced and covers at least all hardware components. All systems in management and service domains are hardened by default following industry best practices such as CIS. Configuration management at system level on critical assets. Critical software updates are deployed ad-hoc on all assets.

The **standard** implementation level implies asset management in place for all hardware and software assets to gather a comprehensive inventory of all its assets and regularly updating all software components through a central patch management system. Policies for patch remediation times based on asset criticality have been defined and software updates are regularly deployed on all assets. Asset and patch management is closely linked to the vulnerability discovery capability and will mitigate those vulnerable components that are discovered (preferably by the organization before a threat actor does!).

Configuration management capabilities are at this implementation level expected to be expanded and hardening of configuration is performed on all infrastructure components and systems in both management and service domains. Assets in the management domain such as access management

jumphosts are subject to more comprehensive configuration management. Key critical assets at the at standard level is to be considered to be protected by HW integrity checking through TPM.

If the environment is self-serviced and automated, then the requirement for full *multi-tenancy* becomes a critical function of the infrastructure to ensure that underlying weaknesses in the automation stack does not compromise the platform. Implementing the software security to the intermediate level implies that all critical components required to operate and automate the infrastructure is fully multi-tenant end to end in all critical components.

Advanced implementation level of software security moves the configuration management from the basic infrastructure platform and system level to the application tier. This area is more varied and complex and usually involves close cooperation with the tenants of the platform apart from the platform operators if they are doing deployment and maintenance of applications on their own. Application control in the form of black/whitelisting is also a part of the level of this capability and security control, locking down what applications, extensions and scripts that can be executed on a runtime environment. All systems in both service and management domains are subject to configuration management. High risk or and key systems throughout the management domain are additionally safeguarded by HW rooted integrity checking through TPM. At advanced level, the infrastructure is capable of hosting hostile tenants.

Intelligent level implementation of software security implies that the majority of the control functions in this capability area are automated and interlinked. Patch management, asset management and configuration management solutions that are deployed are also fully automated, with tiered policies applied to the different categories of assets. Auditing the configuration data of all the organization's assets configuration data is performed automated on a very frequent basis and all deviations are logged and alerted via the SIEM. The Organization's software assets have software updates automatically downloaded and depending on the asset type, also automatically applied to the target system. The vulnerability management system is integrated to the service management solution and based on automatic scans will submit tickets to target systems that are not part of the automated patch management scheme. Asset management is also automated using a combination of active and passive tooling being integrated with multiple 3rd party data sources such as infrastructure automation, dhcp servers, or ITSM CMDB.

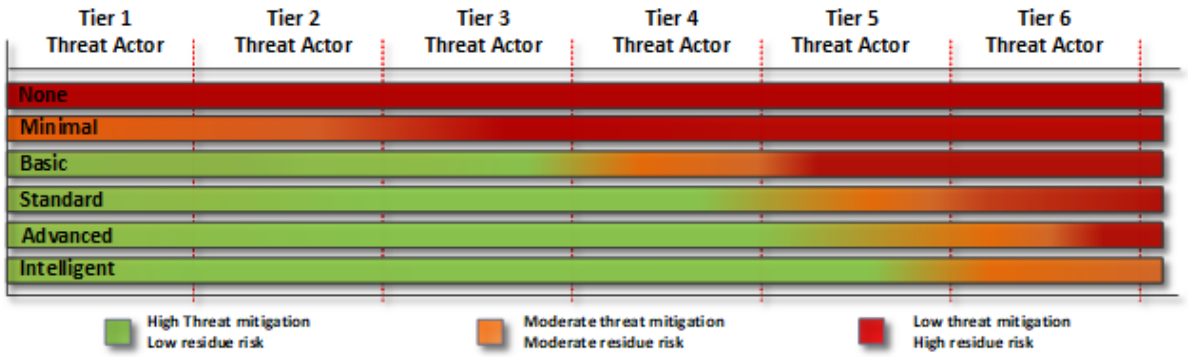


Figure 20. Software security mitigation efficiency

The mitigation efficiency for each of the types of deployment is measured in the figure above.

4.1.5 Data protection

Data security deals with the ability to secure and maintain the confidentiality, integrity and the availability of an organizations data, whether it be internal business data or the data of its customers and consumers of its services.

An effective **data security** architecture will protect data in all of its three states:

- In transit
- In use
- At rest

Data confidentiality and integrity are provided through the encryption of data and through the usage of and digital signatures and keys complementing the other preventive DA capability areas. Encryption protects data in transit, either via transport layer encryption (TLS), by message level encryption (e.g. XML-Encryption), or a combination of both. Network level encryption in the form of VPN can also provide an additional layer of security if data is traversing uncontrolled or untrusted networks. Encryption can also protect data at rest by encrypting the data on the media where it is stored such as disks and tapes. Encryption at rest will provide protection from any low level read operations that may have been able to any bypass application or database specific access controls.

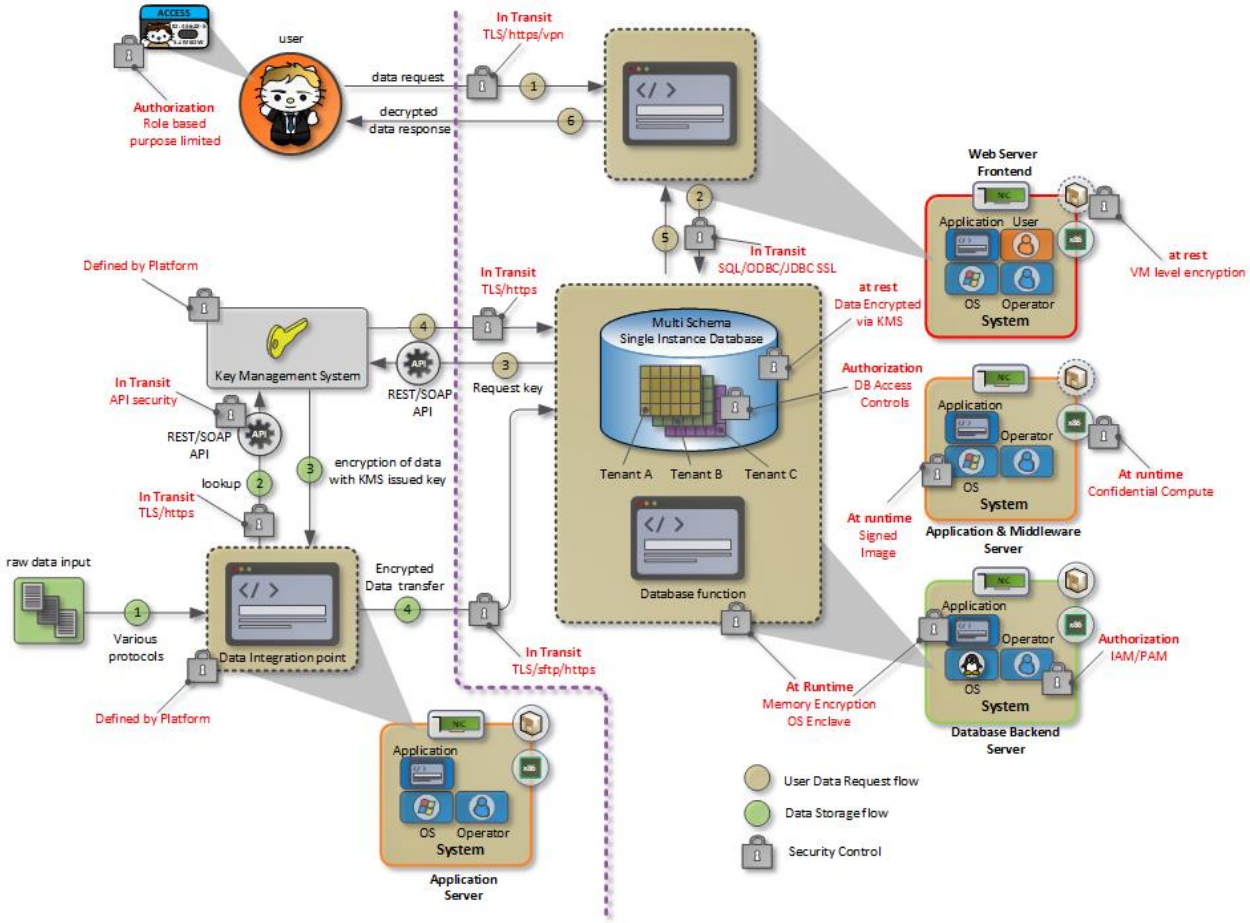


Figure 21. Data domain preventive security controls for confidentiality and integrity

In addition, comes the dimension of data privacy which is supported by technologies such as data masking, tokenization and similar where certain parts of the organization's stored data sets are subject to certain additional restrictions when applicable.

A security conscious organization should classify its data and apply different security controls according to the data's sensitivity and any relevant regulatory requirements.

It should be noted that depending on which industry the organization operates, the security controls and thus the implementation levels are dictated by regulatory requirements. I.e if the organization handles personal identifiable information, traffic data or other data falling under regulatory control or is managing critical information infrastructure (CII) the required security controls may be dictated externally and may by default require a higher implementation level than what only the business requirements of the organizations would like to implement to fulfill the regulatory requirements.

At a **minimum** level a process along with definitions for classification of data have been established. All services that are exposed to uncontrolled or external networks such as the internet are encrypted using TLS, although certificate management may be manual. Encryption of data at rest or in use is employed only as required by relevant regulatory legislation. Service classification and availability are defined but data protection policies in the form of backups are however only extended to systems and applications classified as mission critical at service level C1[39].

Basic level of data protection introduces the foundational components and functionality of a holistic approach to securing data. A Key management system is implemented for the management of keys throughout different systems in the organizations infrastructure. There may be multiple independent KMS systems for different service verticals if the organization owns or maintains a very large infrastructure. Data at rest in critical assets are encrypted at either filesystem or database level. Data protection policies assets for applications of service level C2 or above. Application level and configuration management usage of TPM is addressed under software security implementation levels.

Standard level introduces a certificate manager (private CA) into the organization for more streamlined management of certificates significantly improving on the manual management of earlier levels. Confidential compute us used for runtime protection of data for all assets storing or processing confidential or sensitive data classified at tier D4[40] or above. KMS systems are more consolidated or singular and/or federated deployment. The majority of the systems in the service and management domains with a REST API and/or web interface is encrypted using certificates. Data classification integrated into asset management system and can be included in the overall risk management evaluation of the organization similar to vulnerability management. Data protection policies extended to all assets at service tier C3 or higher. Restore tests done periodically on all critical assets, ad-hoc on other major systems.

Advanced implementation level of data security supports privacy related features such as tokenization or data masking features such as DB field level encryption supported by KMS. Certificate management of cloud native applications and platforms such as Kubernetes. At this level a secrets manager is expected to be implemented supporting the development processes and the CI/CD pipeline used for this purpose. Confidential compute for runtime protection is deployed for certain key critical assets and supported by TPM to preserve the integrity of the underlying hypervisors. Data protection services cover all assets at service level C4 and above and all backup media is encrypted

Intelligent level capability introduces the concept of automation and policy driven enforcement also to data security and protection. Through the tagging of data stored or processed in different systems and applications of the asset management system, the various security controls are automatically applied through policies where deviations to policies are detected. Confidential compute for runtime

[39] See DA-2021-003 Data protection documentation for service level definitions
[40] See DA-2021-003 data protection documentation for classification of data tiers

protection is deployed for most key critical assets and supported by TPM to preserve the integrity of the underlying hypervisors. Data protection is expected to be fully integrated with the rest of the detection capabilities to detect any data integrity violation and trigger an incident response.

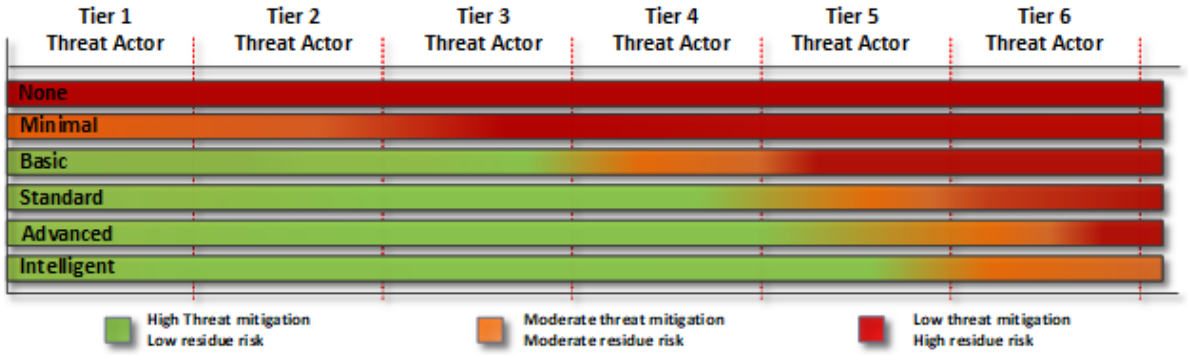


Figure 22. Data protection mitigation efficiency

The mitigation efficiency for each of the types of deployment is measured in the figure above.

4.1.6 Vulnerability management

Vulnerability management is another key capability that is vital to endpoint security and also one of the most proactive approaches to remove security weaknesses in the organization's systems before they are discovered by a threat actor and lead to a breach.

Vulnerability management is a continuous process, it includes proactive asset discovery, continuous monitoring of those assets, remediation of found vulnerabilities on the assets or deploying other mitigating measures to minimize the organization's attack surface and protect assets from potential breach and data loss. Vulnerability management is one of the very few ways the organization can be proactive in securing its assets and its importance as a function cannot be overstated.

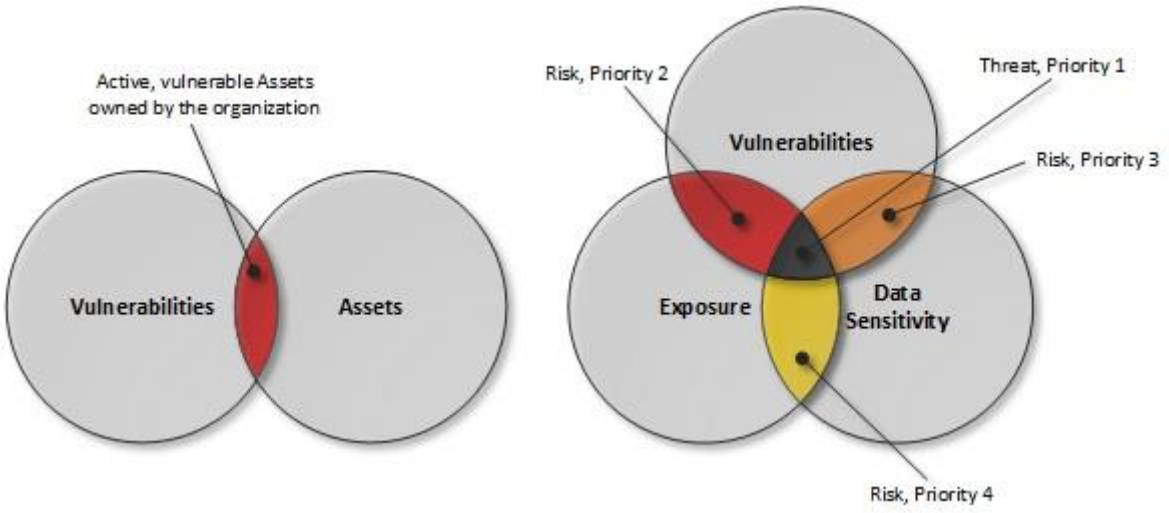


Figure 23. Risk-based Vulnerability management

Another key benefit possible from vulnerability management, given a sufficient implementation level is to add the asset management context and turn the VMS into a strategic analysis tool as part of the overall enterprise risk management process. Insight into the total amount of assets the organization has with the combination of the current state of vulnerabilities and likelihood of breach and potential impact of breaches can provides input into the overall risk picture the organization is facing.

Based on this insight, acceptable risk levels can be defined which in turn will decide on the prioritization of patch management, or the implementation of other additional security controls. Without actual data input and insight, the risk-assessment is both static and theoretical and may not represent the actual threat and risk picture the organization is facing, and most importantly it will not capture the dynamic nature of vulnerabilities and thus not be able to close high-risk vulnerabilities in time before an opportunistic threat actor finds it and exploits it.

The **minimal** implementation level of this capability is to implement vulnerability scanning and to scan the externally exposed parts of the infrastructure. These are the components that are most likely to first be probed and later attacked by a threat actor. There are vulnerability search engines such as Shodan[41] that continuously probe the internet looking for connected devices and classifying them based on type and software versions that threat actors can use to quickly find devices and exploit them, once a vulnerability in the software becomes known. At the minimum level, external vulnerability scans are either performed ad-hoc or regularly critical vulnerabilities in exposed systems are discovered but follow-up of findings may not be systematic.

With **basic** level of vulnerability scanning, the VMS function is still stand-alone, but focus is not only on the external parts of the infrastructure, but scope is also extended to all internal components. While increasing the number of components and possible also number of vulnerabilities significantly, it will give a complete overview of the infrastructure in regard to software running on various systems and infrastructure components which may be vulnerable.

Keeping all the software running in the different parts of the organization up to date will help limit lateral movement by a threat actor after an initial breach. Internal scans will also limit the attack surface of any insider threats whether they are deliberate or have their endpoints compromised which may in the case low maturity in the remote access capabilities have direct access to internal infrastructure components. For full effectiveness, all scans need support the ability to be authenticated.

From a process perspective, vulnerabilities are when they are discovered, documented and systematically followed up on, but not necessarily in a prioritized order from a business continuity perspective.

At **standard** implementation level, the VMS becomes Integrated with neighboring systems such as asset management systems/CMDB and SIEM. All newly deployed assets get added to the VMS scanning cycle and discovered assets are reported back to the asset management system for comparison. VMS is also integrated with the SIEM providing log data and the ability to use the SIEM as a single pane of glass for reporting. The context of the running software, data stored on the assets and their exposure is added to vulnerability management database enabling a risk-based prioritized software update and patch management schema. The combined data in the VMS database can be export to the enterprise risk management process for strategic assessment of the organization's overall risk. Integrated vulnerability management allows the security operations and OAM teams to follow a risk-based model as well as addressing a dynamic threat landscape.

At this implementation level, the visibility and data provided by the vulnerability scanning can be proactively used in determining organization overall risk.

At the **advanced** level of implementation for vulnerability management lifecycle management of all the vulnerabilities discovered are also expected to be in place to track the trends of the actual security posture verifying what vulnerabilities have been addresses and which are still open. Life cycle management may be manual but is tracked and reported on. To improve the overall security

[41] https://www.shodan.io/

posture, the number of vulnerabilities is required be kept as low as possible to limit threat actors' ability to gain an initial foothold. Vulnerability management is at this implementation level supported by threat intelligence feeds making the risk-based vulnerability management process much more precise

Integrating vulnerability management into an automated security response framework is the key objective to the **intelligent** implementation of the vulnerability scanning capability and thus supporting the ambition of automation in the security area. Scope cover is both internal and external, but the scans should also be policy based and automated, including discovery functions and the scanning of newly deployed assets, existing assets need to automatically be scanned at regular intervals at a weekly basis. The vulnerability scanner has an API to integrate with the SIEM and/or EDR solution to perform automated scans of assets if any anomalies are detected on them through security analysis.

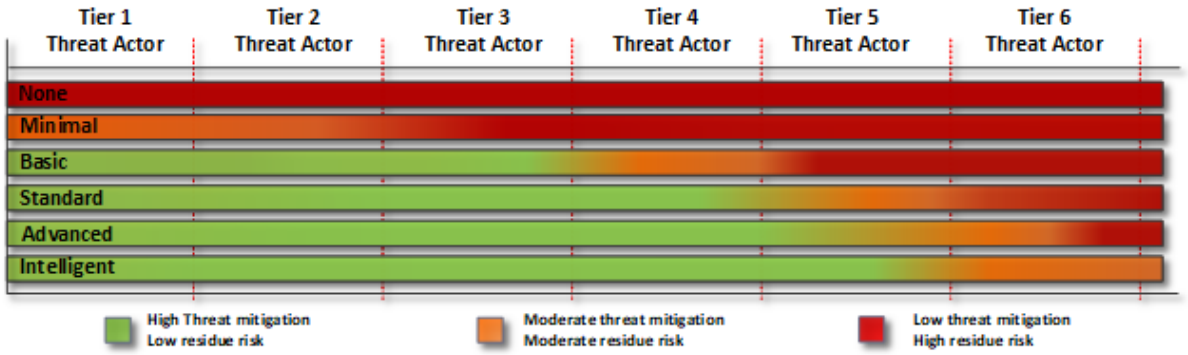


Figure 24. Vulnerability scanning mitigation efficiency

The mitigation efficiency for each of the types of deployment is measured in the figure above.

4.1.7 Integrated and automated risk management

The organization need to continually assess all their running workloads and underlying infrastructure everywhere it is running, whether it is on-premises or have been deployed to a public cloud service provider. Assets needs to be identified along with the security controls attached to them which are present, and which are missing.

Most large organizations have established a risk management program to meet compliance and regulatory requirements. As part of this program, continuous vulnerability management is performed to ensure all systems are identified, properly configured and they are running the latest version of software with no inherent vulnerabilities that can potentially pose a risk to the organization. Ultimately, asset management, configuration patch management makes up the response dimension to vulnerability management thus enabling organizations to properly address relevant business risks. The ability to map asset management, configuration management and patch management to the vulnerability and risk management processes is thus essential both increasing the overall security posture as well as showing compliance.

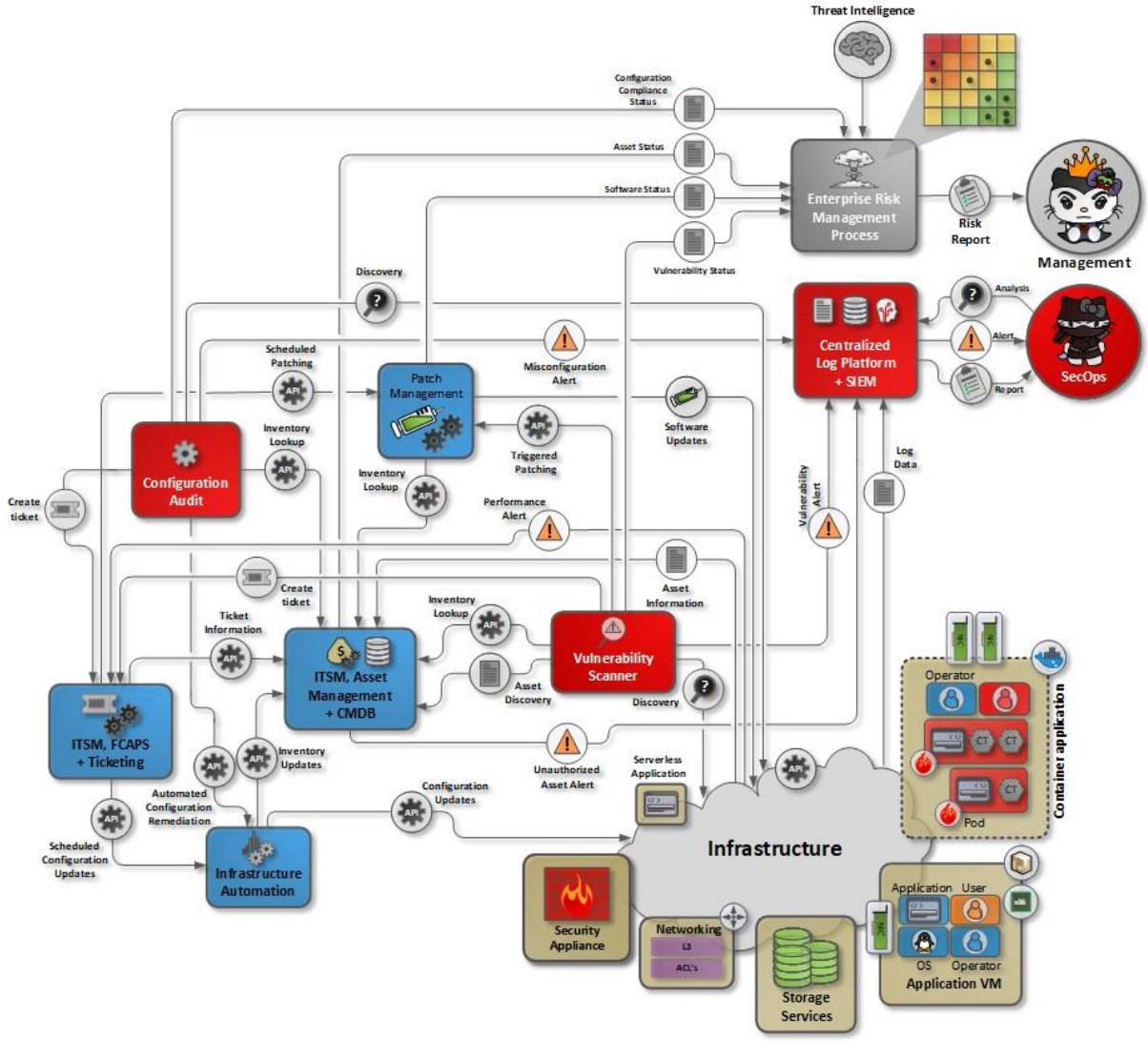


Figure 25. Integrated tooling ecosystem

By building an inventory of the entire infrastructure's assets, with its associated vulnerabilities, misconfigurations or compliance deviations. A strong understanding of the organization's overall exposure and risk may be established. Automating these functions and integrating with threat intelligence can make this insight both dynamic and in near real-time

Capability areas and their corresponding security controls should not be standalone but instead act together to complement and enhance each other.

Among the main security controls to address software, system and application security as part of defendable architecture the following have been identified:

- Asset management of all hardware, software and information components
- Software update and patch management
- Configuration management of endpoints, systems and devices
    - Endpoint hardening, OS
    - Endpoint Integrity Checking
    - Applications hardening + whitelisting
- Vulnerability Management
- Multi tenancy capabilities in shared software components

Asset management which is a key control and important baseline for all the other security controls is usually an integrated part of the larger ecosystem of IT service management but is highlighted here as part of the identify step of the automated patch management process. Further reduction of attack surface on all systems is performed via secure configuration management in the form of hardening of all operating systems, applications, appliances and devices. and then the subsequent automated auditing of that configuration to see that is following best practices and is not tampered with. Further adding whitelisting of which applications, libraries and functions regulates which executables that are allowed to run on a specific system. Coupled together with guidance on how to properly deploy multi-tenant software helps the everyday usage of the running software components to remain secure when being used in a multi-user environment.

Observation 002-4: *Asset management together with configuration management, patch management and vulnerability management are in combination a key to successful unified risk-based management of infrastructure and services*

Configuration and patch management is never as simple as merely identifying configuration gaps or that a software update is needed then distributing it to the system in question. It is a complex process that includes multiple steps including staging, testing, configuration management and more. Using multiple different technologies for vulnerability assessment, configuration management, patch management responding to them create a resource overhead, and require extensive integration efforts between the systems. A single, comprehensive solution that provides both visibility and control across the organization's complete infrastructure environment, including workloads deployed to public cloud should be considered to simplify and automate these functions.

When combined together, these security controls if correctly deployed and maintained over time, will greatly reduce the chance of any software assets to be breached by a threat actor and used as a pivot point to gain unauthorized access to the organization's information and sensitive data.

4.2 Detection Capabilities

Why it is necessary to include comprehensive and effective security monitoring and how this enables effective incident handling?

Detection and security monitoring is the second main area of defendable architecture in addition to preventive capabilities. Its complimentary to preventive capabilities that aim to make it as difficult as possible to perform lateral movement since a threat actor would need to perform much more varied and multiple methods of attack to freely move around and thus make more "noise" in their effort which is caught by the several methods of monitoring.

To detect the different types of attackers, the security monitoring needs to both multi-capability and multi-tiered. Multi capability as in that the different functions can are aimed at detecting different things.

Multi-capability would mean as an example that a basic endpoint security agent detecting malware using signatures would be effective in stopping a tier 1 or tier 2 threat actor but would be useless in stopping more advanced threat actors, which would require another defensive mitigating capability such as more advanced endpoint security agents. A similar approach would apply to network monitoring as well, basic signature-based IDS would catch known exploits and rootkits deployed by a less skilled threat actor while the significantly more advanced sensors developed by the CSIRT team would be required to detect a higher tier threat actor.

Multi-layered implies that monitoring takes place at different places in the infrastructure, where one layer is the various agents at the OS instance level, and another would be passive monitoring at network level. The agents would be visible from the OS instance that might be compromised and in

worst case tampered with or disabled so it would be unable to send an alert. The passive network monitoring however is not reachable from a potential compromised OS instance.

Similarly, the passive network monitoring comes with different capabilities with varying degrees of sophistication including machine learning and analytics capabilities to automatically trigger alerts based on endpoint behavior.

In general, the greatest threat towards the infrastructure and any sensitive data stored within it is a threat actor cannot be seen and not be detected until a significant foothold have been established or large amounts of sensitive data have been exfiltrated. Detecting, containing and evicting an attacker that have achieved either a significant foothold or worst, a total comprise of the infrastructure is a very time consuming and expensive effort.

The counter this threat, both proper monitoring and incident handling processes needs to be needs to be in place. Organizational capabilities and process are not in scope for this document, but the technical capabilities that can be implemented in the infrastructure is, and it needs to cover multiple areas of the infrastructure to ensure that any threats, advanced or not are detected.

4.2.1 Endpoint Detection and Response

The highest level and granularity of visibility in the infrastructure comes from the telemetry data collected directly from the endpoints and the capability referred to as Endpoint Detection & Response (EDR). With the ability to monitor the runtime environment both processes, memory and configuration data can be monitored for unauthorized changes by various forms of malware or exploits. The endpoints are also the infrastructure components that will be most vulnerable they are exposed to internet or other uncontrolled networks. The applications and operating systems contain millions of lines of code and is the most likely entry point for a threat actor by exploiting a weakness in the software.

There are different implementation levels of endpoint protection that can be deployed, the most basic type of endpoint protection are protective agents that both detect and remove malware. This is the traditional signature based anti-virus/anti-malware type of software that monitors all the processes and executables in a runtime environment and blocks and removes any known type of malware. These tools are signature based and act on what is known, so they will be very effective against tools and exploits that are known and added to the signature database, but not so much against unknowns, also in some cases you want to study the malware for its behavior and communication to identify C2 infrastructure instead of killing it outright. In general, an effective tool to defeat lower tiers of threat actors, but not so much for the more advanced ones.

The are available more feature rich and sophisticated endpoint agents available which are used for the higher implementation levels of EDR. These types of agents not only look at the checksum of the executables launched and does the same as the basic endpoint protection agents, but also monitors the entire runtime environment. The detection agent will be looking all types of events for anomalies whether it is someone trying to impersonate the local system account indicating access token theft, or a process reflectively loading a dll it is not supposed to trying to avoid regular anti-virus monitoring. While these more sophisticated software agents are not bullet proof, they are far better at detecting the malicious behavior that comes with more advanced TTP’s from the higher tiers of threat actors.

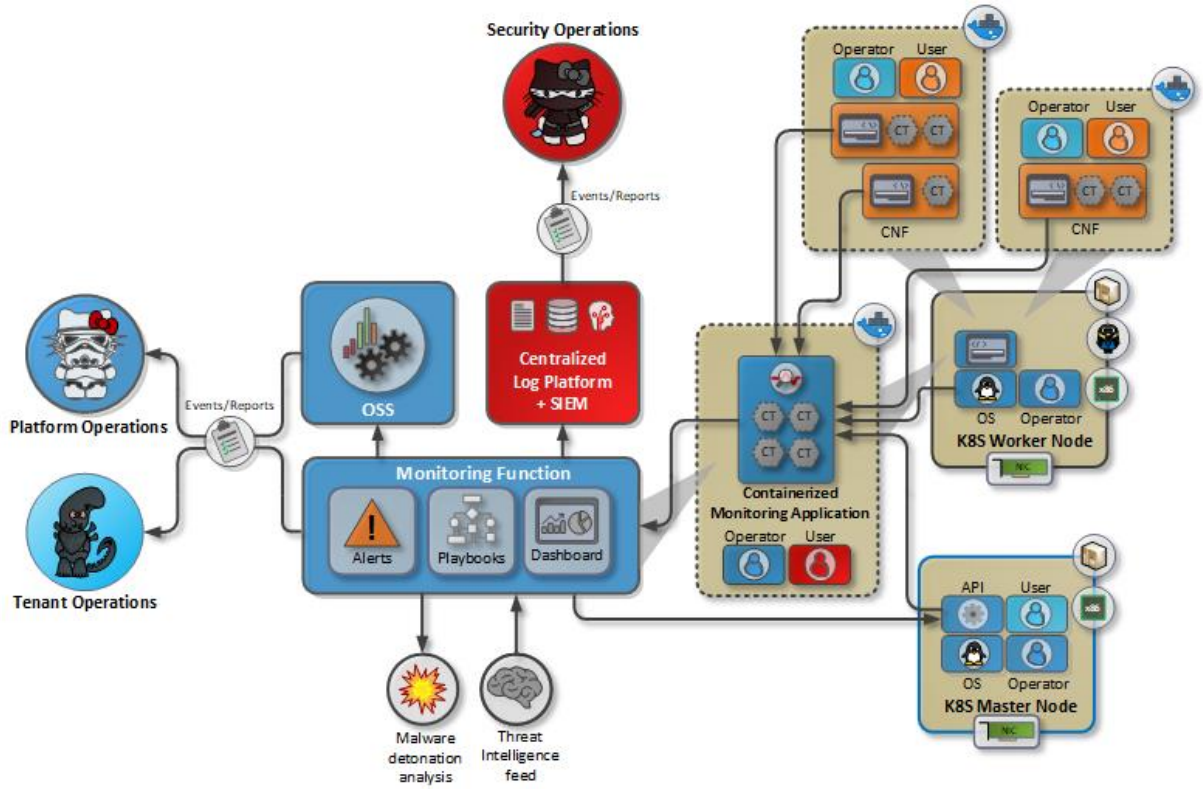


Figure 26. EDR on a container worker node using kernel event monitoring

There are different implementation levels of endpoint protection that can be deployed, at a **minimal** level, the type of agents is limited to the classic AV type of protective agents AND/OR scope of deployment is limited to critical assets only.

At the **basic** level of implementation, the type of agents being used are typically still dominantly of the protective AV type as at the minimal implementation level, but the scope is extended to the majority of the organizations running systems in the infrastructure. The AV system is also integrated with the asset management systemin which allows for consolidation of data and verification of the number of assets, vs those having AV agents installed. SIEM integration allows for a more holistic analysis of events also including endpoint data.

At **standard** implementation level the default agent type is no longer the basic signature-based protection agents but rather the event-based EDR agents. Installation scope at standard level is expected to cover the majority of systems and components in all security domains such as staging, management, service and security domains, including all critical assets. A fully functional EDR solution have been established at this point.

Certain key systems including PAWs used for remote access, central management systems and other critical assets use the more advanced behavioral-based EDR agents. Other less critical assets may still use standard AV solutions.

Application whitelisting is also enabled at this capability level, but implementation scope is typically limited to critical assets only

At the **advanced** level of implementation, the main job of collecting telemetry is handled by EDR alone, and all aspects of traditional AV have been phased out. Additional functionality is applied to make the EDR solution more dynamic and precise

Threat intelligence feeds enhances the detection capabilities of the deployed EDR agents to improve their efficiency by discovering known IOC's faster. Public and private intelligence feeds ensure that known event pattern that are identified as an indicator of compromise (IOC) that is part of a breach it gets fed to all the other users of the agents and thus sharing the gathered intelligence data across multiple organizations.

Key functionality in the form of automated malware detonation and subsequent analysis is also added, taking suspicious files and send to a sandboxed environment to understand what actions a specific file takes in a system and determine any risks associated with it and create response rules.

Application whitelisting is at this capability level extended to the majority of the organization's assets.

The organization's CSIRT team also makes use of dedicated forensics suite with their own set of agents to support all incidents. The forensics agent is only used during incident response processes, this is to gather endpoint data for forensics purposes such as files, memory dumps. All data from suspected compromised hosts are gathered in a central location to be analyzed for suspected indicators of compromise.

Intelligent endpoint detection and response expands the log collection, analysis and response capability across other domains in addition to only endpoints and analyze their behavior providing a more holistic visibility turning the EDR platform into an XDR solution. Coupled with threat intelligence feeds, this greatly increase zero-day vulnerability coverage and the Integration into other domains provides an automated defense grid.

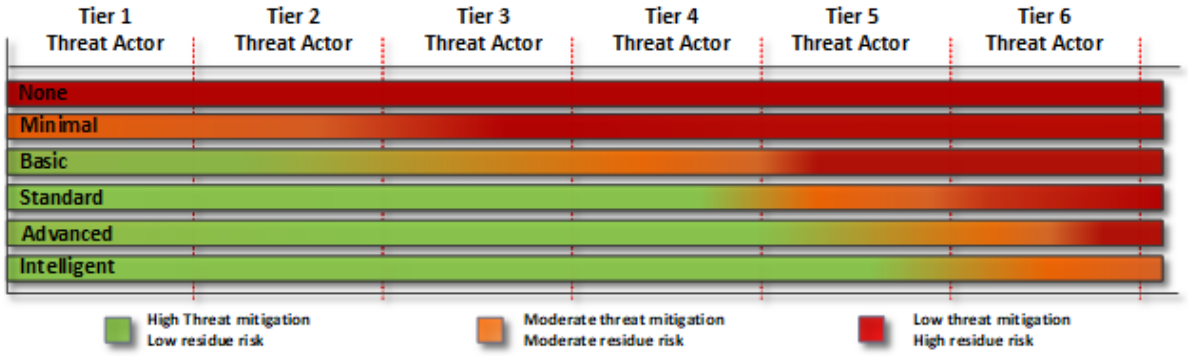


Figure 27. Endpoint Security mitigation efficiency

The mitigation efficiency for each of the types of deployment is measured in the figure above.

4.2.2 Flow based network monitoring

Note. A company that does not have any intention of mitigating the more advanced types of threat actors such as tier 4 and above, will most likely not have a sufficient budget justification for implementation of this capability.

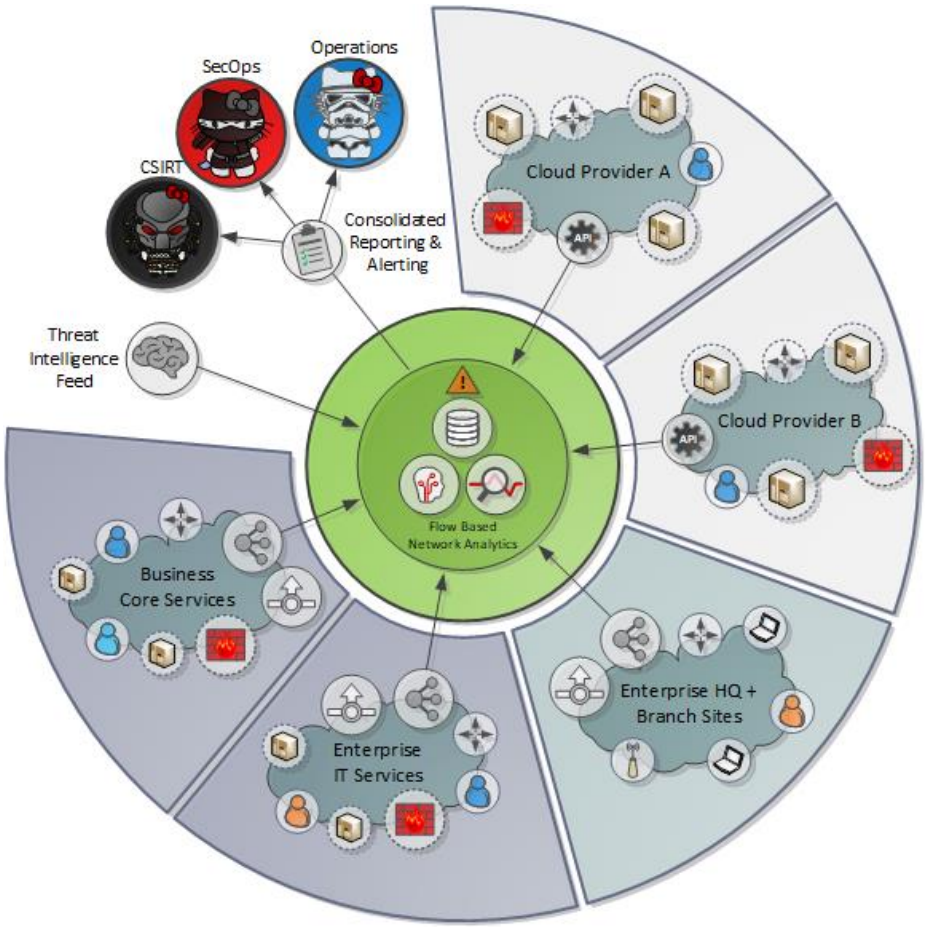


Figure 28. Flow based network monitoring across multiple infrastructure domains

Ideally, the flow-based monitoring would cover all assets, although as it is usually a costly implementation project, a staged approach would need to be taken. The capability implementation levels are addressing this from a scope perspective in the lower levels before building additional features on top.

Minimal capability level would mean a partially implemented flow monitoring system in the organizations network infrastructure mainly focusing on the organization's "crown jewels" defined as critical assets with a limited set of use cases to only monitor what is really important, but to provide good behavior-based traffic analysis on those critical assets. While the capability at this level is able to track the behavior of traffic to and from the critical assets, extended monitoring and the ability to track threat actor movement across the general infrastructure is limited.

Basic implementation of flow-based network monitoring would mean that the capability have been extended in regards to scope and can be considered to cover the majority of the systems in the management domain. As management systems are used to operate other system components and access resources and data in the service domain, higher priority should be given to these systems. The extended coverage enables the tracking of threat actor activities and movement across multiple within the management domain, which would be very helpful as a supporting tool in an incident response.

A **standard** implementation of flow-based monitoring would cover the entire network infrastructure of the organization. This would include both service and management domains in the on-prem production domain, the enterprise networks being used by corporate end users, and any public cloud deployments the organization are using if any workloads are deployed there. All the organization's

assets that thus be assumed to be covered under a single plane of glass and all anomalies in the infrastructure would trigger an alert. All assets discovered by the flow monitoring are also regularly matched towards the asset database.

Implementing the **advanced** scope of the flow-based monitoring would in addition to the full coverage of all assets also include the consumption of threat intelligence feeds to improve the effectiveness of the solution. External threat feeds provide intelligence data from multiple external sources to the flow analytics platform to help detecting advanced threats. At advanced levels, the flow monitoring solution should also be capable of analyzing encrypted traffic without decrypting it, which is becoming more challenging with the development of stronger and better encryption methods such as TLS 1.3. Detecting threats in encrypted traffic can discover the stealthier threat actors and in addition gives the ability perform analysis of the encrypted traffic can also ensure cryptographic compliance to know how much the deployed services that uses sufficiently strong encryption and to address and deviations.

Intelligent flow monitoring implies integrations towards the other security functions should also be implemented to trigger automated response. The flow-based monitoring solution can for instance be integrated to the infrastructure policy manager to automatically quarantine endpoints responsible for certain policy violations by reconfiguring network or security devices or it may trigger automated tapping of data via the SIEM solution

Implementing the **advanced** scope of the flow-based monitoring would in addition to the full coverage of all assets, also include the application of threat intelligence. An external threat feed provides intelligence data from multiple external sources to the flow analytics platform to help detecting advanced threats. Other integrations towards the other security functions should also be implemented to trigger automated response. The flow-based monitoring solution can for instance be integrated to the infrastructure policy manager to automatically quarantine endpoints responsible for certain policy violations by reconfiguring network or security devices or it may trigger automated tapping of data via the SIEM solution

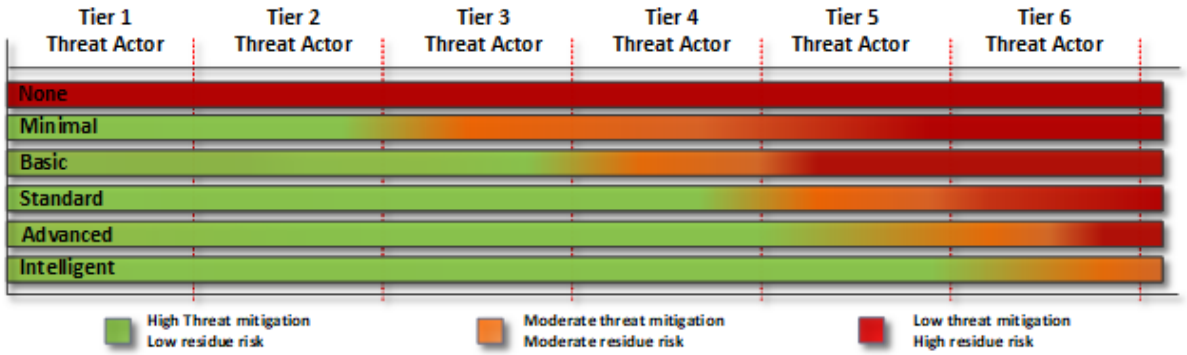


Figure 29. Flow based network monitoring mitigation efficiency

The mitigation efficiency for each of the types of deployment is measured in the figure above.

4.2.3 Logging & Auditing

Depending on requirements of what tiers of threat actors to mitigate overall risks and chosen operating model of the infrastructure, different levels of log infrastructure can be deployed.

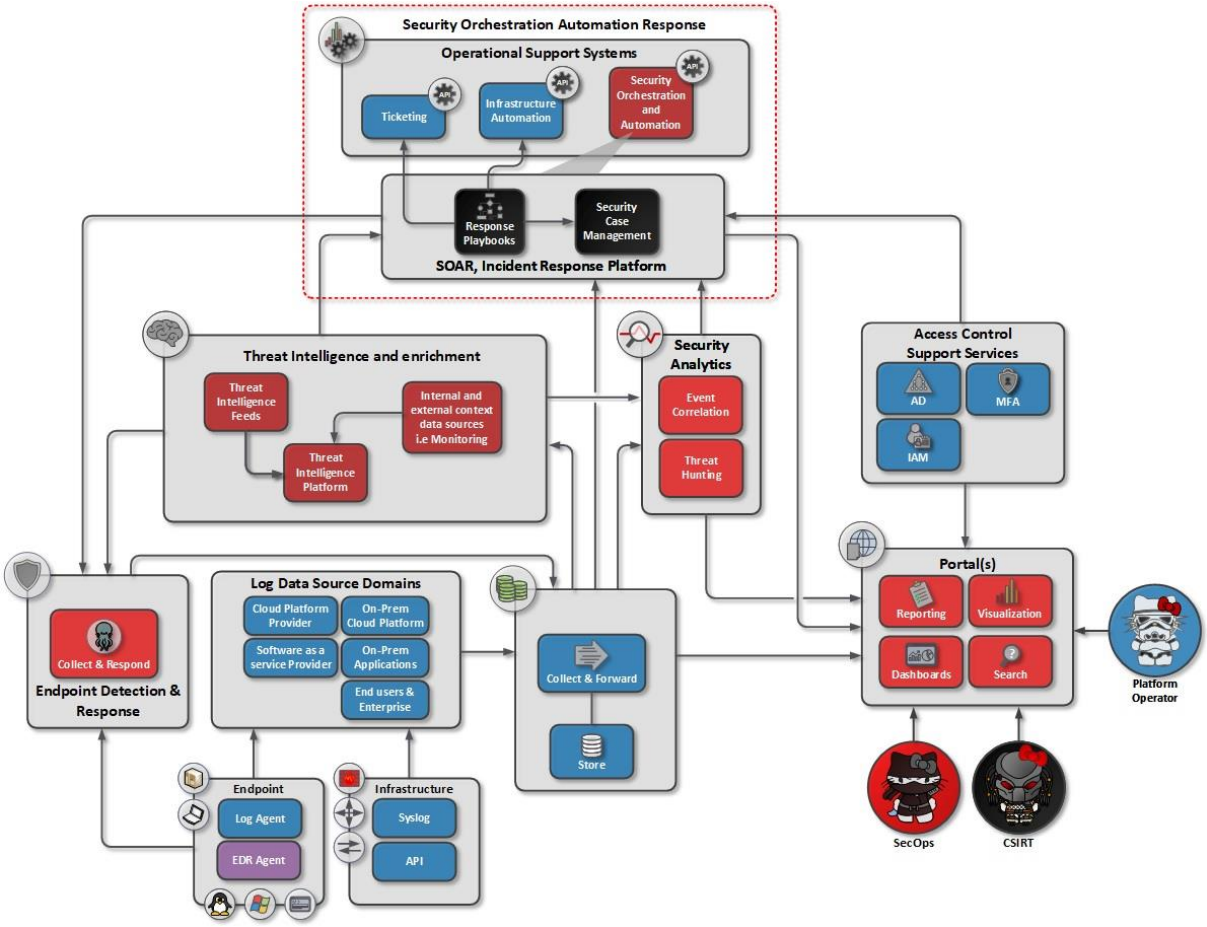


Figure 30. Functional components for Intelligent (CL5) logging and auditing

The deployment of logging and auditing is centered around the deployment of a log management solution where the target is to collect auditable information for all HW and SW components in the infrastructure and establish a process for mapping it against the inventory of known assets. Once all log data is being collected, this data can support incident response processes for both operational and security related incidents.

At the **minimal** level of logging, a centralized logging solution have been implemented that is that to the systems can send their logs to. Coverage at this level is considered to be partial though with only critical assets in scope and logs mostly collected at system level. No analysis on the logs takes places, and the information they provide is utilized in a reactive manner only.

At **basic** level, all systems in the service and management domain delivers log data to the centralized logging solution. Log coverage is considered to extend to most of the infrastructure. Application logs from critical systems are also collected in addition to ordinary logs from infrastructure components and system level logs from OS instances.

Standard implementation levels extend on the collected data with data-aggregation, correlation of events, dashboards for visualization and real-time alerting is the foundation for the standard capability in the logging and auditing space. It provides the basis of turning the collected data and

applying analytics to it to turn it into a data-driven incident response tool and a SIEM platform instead of only passive information source from logs.

Advanced level of logging and auditing also goes into the user behavior analytics space. UBA focuses on what the user is doing in addition to only system level activities, what application are launched, network activity, or most what files or other resources that are accessed. User behavior analysis greatly improves the ability to mitigate insider threats, or the unauthorized use of legitimate credentials.

The consumption of threat intelligence feeds at advanced level also widens up the number of known patterns by importing other known indicators of compromise across the greater footprint of industry communities and turns the log analysis into a collective venture that can increase its effectiveness.

For the "ordinary" system level analysis, application logs across both the service and management domain are also collected and subject to analysis.

The **intelligent** implementation level for logging introduces capabilities for logging and auditing that adds onto the SIEM implemented earlier with built-in tools automating and supporting the incident response process with specialized view, reports and known trigger points. Another key aspect of intelligent logging and auditing that it will make up the foundation of the automated defense grid. Using API driven interfaces and interconnecting it to other security functions, certain combinations of anomalies detected in the logs can trigger external actions such as an automated vulnerability scan, or automated on-demand tapping on hosts suspected of compromise. Further analysis of the collected data from the third-party functions can then determine if a full incident response needs to be triggered. Automated response is the best way of dealing with sophisticated upper-tier threat actors.

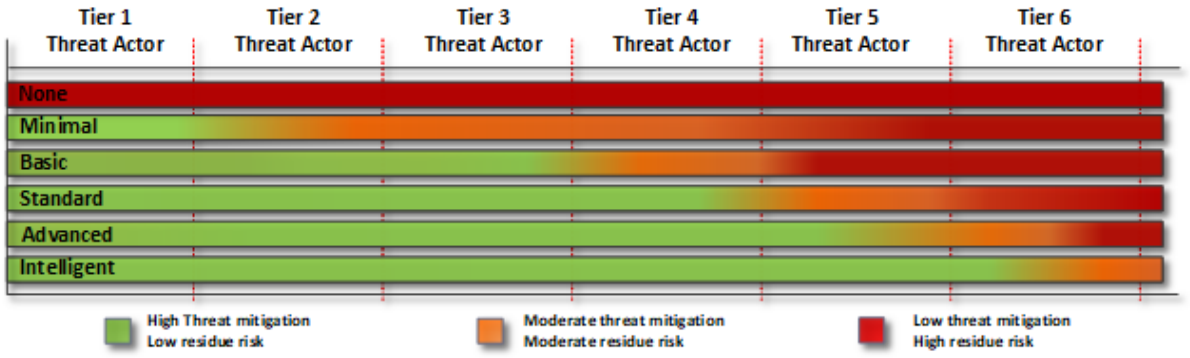


Figure 31. Logging & auditing mitigation efficiency

The mitigation efficiency for each of the types of deployment is measured in the figure above.

4.2.4 IDS/IPS

Network based intrusion detection (IDS) and prevention (IPS) systems have been around for a very long time. They plug into the network traffic either directly or are fed via a network tapping solution. Once hooked into the data stream they analyze the network data and searches all the payload that is part of the traffic for malware or other unknown or potentially hostile files. By being signature based, an IDS/IPS will always be one step behind those more sophisticated threat actors that either use zero-day exploits or who are able to create their own.

The **minimum** defendable architecture implementation of IDS is using a signature-based IDS at internet facing parts of the network. This will catch well known exploits or rootkits deployed by threat actors at the main entry point to the infrastructure.

The **basic** implementation of IDS is using a signature based IDS at the edge of the network covering entry points into the network segments hosting exposed system in the service domain and/or the internet access for the enterprise network. Select critical assets also have sensor coverage.

The IDS sensors that are deployed in the **standard** capability level implementation are more intelligent and feature rich. The more sophisticated IDS sensors utilizes in addition to normal pattern recognition also anomaly based detection capabilities which are enhanced with machine learning. . In addition to external network exits/entrances they also cover the standard level perimeter security boundaries (if this level is reached in that domain) in the form of air gap zones to also focus on internal threats in addition to the external ones as well as any defined critical assets. All main entry points into the network is covered, both internal facing legacy networks and enterprise network and external points such as partners or the internet

At an **advanced** level, the IDS sensors to be more effective comes with the capability to consume threat intelligence feeds continuously delivering TI data and IOC's to them closing the gap for malware or a set of events go from unknown to known threats. Malware detonation capabilities are to be also present to analyze unknown findings. The scope of IDS coverage with an advanced implementation level would cover all traffic passing through internal or external chokepoints bordering points external environments as well as select internal points in the network covering all key internal systems (domain controllers, IAM etc)

With the **intelligent** level of this capability, the IDS sensors are also used by the CSIRT to tap into the network traffic and record it for an extended period of time to support incident response. To investigate an incident that goes back in time the analysts can them look into the stored packet capture data and analyze it for file transfers etc to gather forensic evidence several weeks and months after an incident have actually occurred. IDS sensors are also integrated with the SIEM solution and other detection capabilities

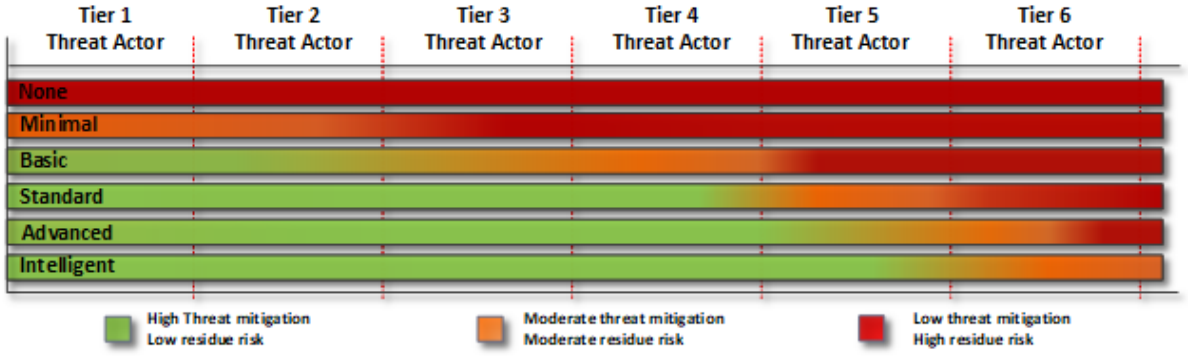


Figure 32. IDS/IPS tapping mitigation efficiency

The mitigation efficiency for each of the types of deployment is measured in the figure above.

4.2.5 Network tapping

Depending on the level of network coverage and automation deployed network tapping can provides excellent intelligence by providing an opportunity to listen in and do a detailed analysis on suspected threat actors traffic to support an incident response.

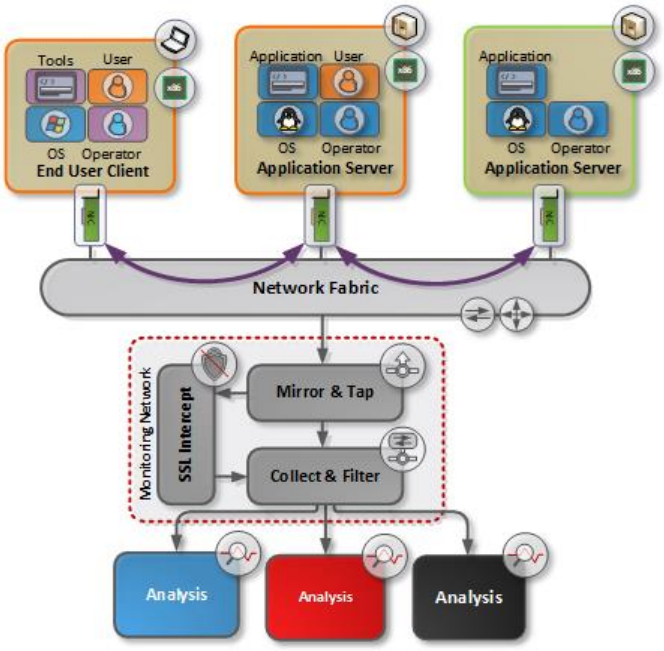


Figure 33. Network Tapping Architecture

Minimal implementation level includes leveraging only the port mirroring capabilities at network switch level with no dedicated monitoring network deployed. Focus for security purposes is mostly for internet traffic or analysis done ad-hoc in the case of operational issues of a security incident.

The **basic** implementation of network tapping would consist of monitoring network with a smaller number of packet broker switches which may or may not share a common topology and relying on a limited number of physical tap devices and port mirror sources for data input. This solution can effectively support only a few (1-2) tapping use cases in an efficient manner. Coverage of continuous tapping in the network would be a limited scope but should include the ability to tap traffic to and from endpoints in the management domain and other additional systems that have been classified as critical assets elsewhere in the infrastructure. Usage of physical taps for continuous tapping may be limited and setting up tapping outside the scope of the taps for an endpoint may require a manual process involving traffic redirect and mirror port on an ad-hoc basis. A single security monitoring station have been deployed and is used by the security teams to analyze on-demand packet capture for incident response.

A **standard** level deployment of a network tapping solution would include an expanded monitoring network that utilizes multiple packet broker switches in a unified topology and using aggregation layers to support scaling of network traffic while supporting multiple tapping use cases.

Continuous monitoring is ensured by both physical and virtual taps which are deployed across the entire production network infrastructure with both service and management domains under coverage. The network tapping capability at this level can support multiple continuous analysis functions (5+) and use cases in an efficient manner.

Network tapping is at this level expected to be complete, supporting continuous tapping covering most endpoints and assets in both service and management domains. Physical tapping points have been established across the infrastructure for continuous tapping of endpoints and selected key points in the network as required. Additional coverage can be achieved by manually modifying the deployed tap or mirror policies to cover any endpoint in the network.

Advanced level network tapping adds the implementation of SSL intercept capabilities natively into the monitoring network for all relevant tapping use cases, either continuous or ad-hoc. Tapping

points in form of physical taps are by default present across the network infrastructure and enables traffic all endpoints and/or network ports to be mirrored into the monitoring network for one or more continuously use cases without any configuration changes.

SSL intercept capabilities are implemented for selected tapping use cases either with dedicated appliances or natively in the monitoring network.

Multiple security monitoring stations, either physical or virtual have been deployed for usage by different teams to simultaneously working on operational or security incidents in parallel. The monitoring network shall at this stage also be multi-tenant and support partitioning among the groups of users to isolate the use cases from each other within the single topology of the monitoring network.

Intelligent Network tapping implementation include in addition to full network coverage and decryption capabilities also include automation and integration with the organization's chosen SIEM solution. Anomaly detection caught by the log management solution's analytic function should trigger an automated playbook that alerts the SOC team while immediately starting to tap the network traffic of the asset in question. Integration between the production network fabric the tapping function and the SIEM solution is thus required. The security monitoring station(s) would have a large storage pool available to be able to store recorded packet capture data for an endpoint for 6+ months or a defined set of time as defined by the organization's security policy.

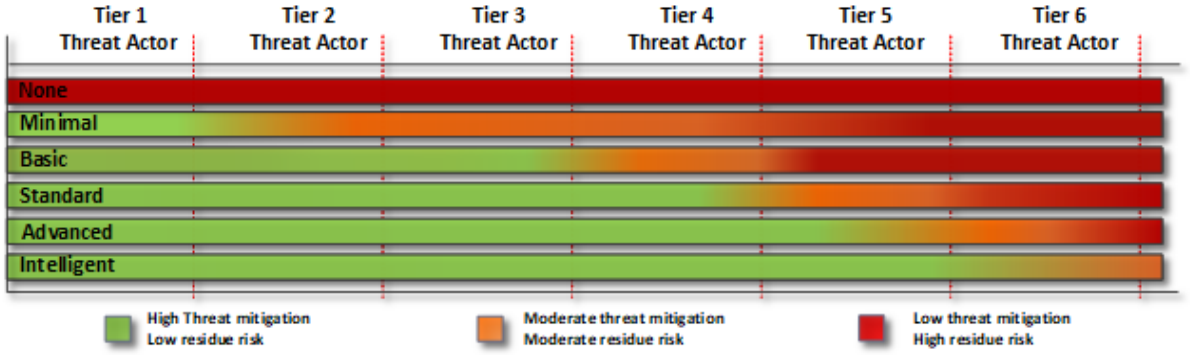


Figure 34. Network tapping mitigation efficiency

The mitigation efficiency for each of the types of deployment is measured in the figure above.

4.2.6 Integrated and automated detection and response

The figure below shows an overview of the different detection capabilities defined in defendable architecture along with supporting components in an integrated deployment. Modern tooling come with API's and the various integration points between them that can both enhance the efficiency of the security control, provide data output used for assurance or risk management processes as well as enabling capabilities for automated response.

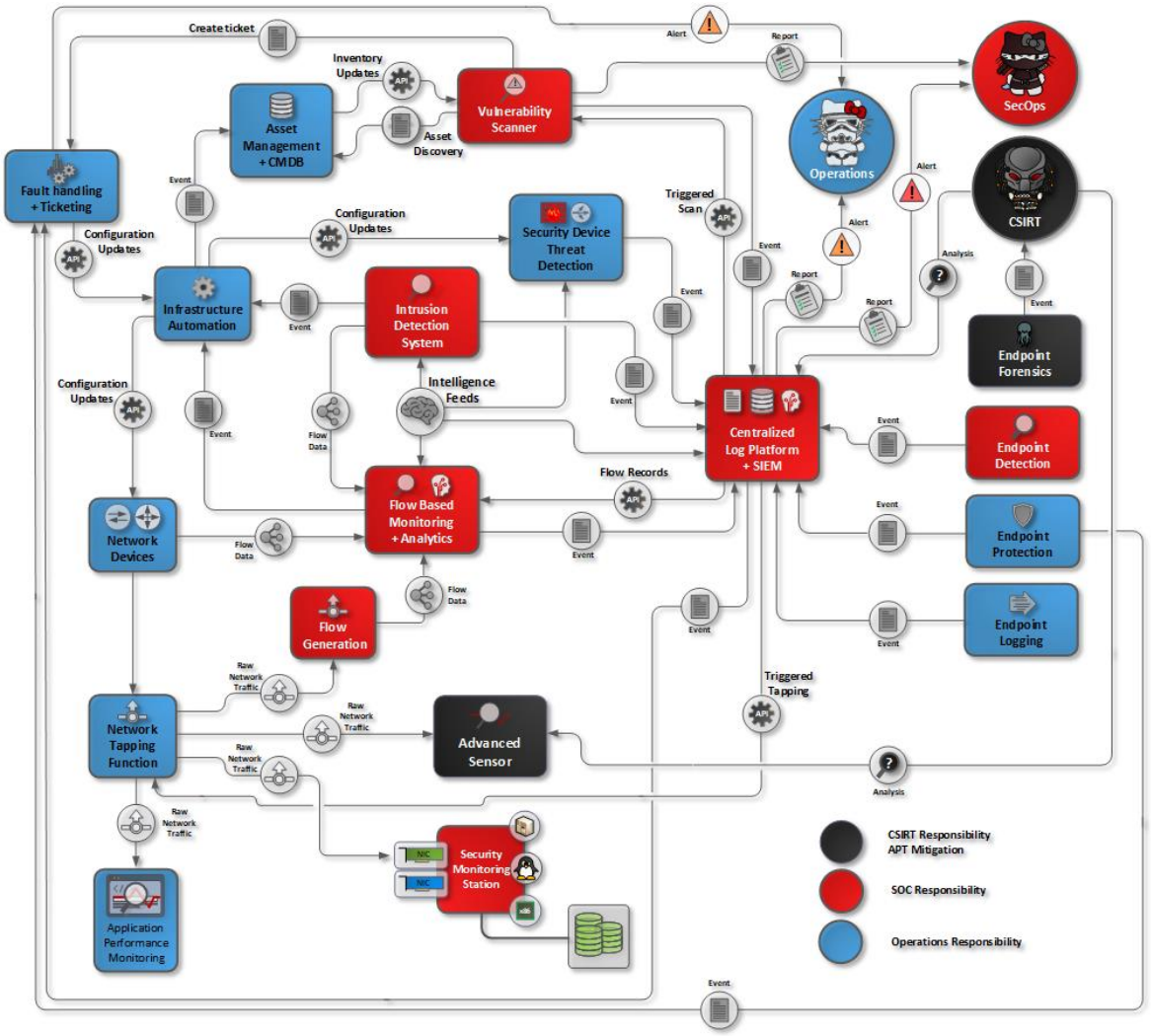


Figure 35. Security Monitoring Ecosystem

The tools that are supporting the detection, discovery and incident response process comes into 4 main categories which combines active and passive capabilities and are both in-band and out of band from the endpoint perspective. The difference in capabilities of the tooling while providing a partial overlap of functionality, provides complete coverage and to ensure that if a threat actor manage to either bypass one detection capability, or the capability would happen to suffer from a catastrophic failure, the threat actors' action should be captured by another. Multi-capability coverage supports the defense in depth principle and does not leave the discovery process blind in case of an outage of a single capability.

The currently described capabilities in DA which are utilized for security monitoring:

- Passive network-centric security monitoring capabilities

    - Continuous network tapping
    - Flow-based network monitoring
    - Signature or event-based IDS
    - Perimeter security boundaries with airgap zones
- Active, endpoint-centric security monitoring capabilities
    - Integrated vulnerability management
    - Endpoint detection & response (AV or EDR)
    - Software security with endpoint configuration audit and compliance
- Logging & Auditing
    - Centralized logging with security analytics
- Incident Response
    - Selected network tapping for affected endpoints
    - IDS with packet capture playback
    - Endpoint detection & response, forensic agents

It should be noted that the list above which focuses on the ICT platform, is not an exhaustive list of security controls to deploy, as there may be other controls in addition which are tailored to the workloads in specific use cases. The security controls described here have been defined through the defendable architecture foundation documentation as generic controls which are considered to be the most effective ones to deploy to mitigate the majority of scenarios in which a threats actors' is able to compromise the organization's infrastructure.

All of the defined security controls within defendable architecture shall be used to sufficiently protect sensitive data and to support an incident response process. The operational security team shall integrate their vulnerability management efforts along with endpoint security and application security efforts with network security monitoring to ensure that new threats are discovered and responded against across all the organization's assets.

Endpoint security and application vulnerability management is centered on the use of tools and capabilities such as software vulnerability scanners, endpoint agents and host/system integrity checking and configuration auditing to find weakness in applications in the infrastructure and to track if their state or configuration have been altered. This is particularly important for those applications placed in the exposed parts of the infrastructure.

Effective security enforcement for endpoint security also requires engagement at OS level, application level with using whitelisting mechanisms, by creating comprehensive audit trails of all activity as well as utilizing capabilities in the underlying network infrastructure for passive out of band monitoring.

In addition to using the endpoint centric tools, a vulnerability management program is a very effective pro-active security control. Frequent vulnerability scans should be run against the organization's infrastructure, as a minimum all exposed parts of the network, but preferably as many of the organization's assets as possible. This tests the network from a threat actor's perspective, allowing discovery of vulnerabilities before threat actors have the chance to exploit them. For this capability to be effective it is of course required for the operations team to have tools and processes in place to follow up on the vulnerabilities that the SOC team have discovered in a prioritized and timely manner and make sure that the software running on all the organization's systems gets updated and remains free of vulnerabilities.

Passive security monitoring management must include the use of tools such as centralized logging with security analytics (SIEM) , flow-based network monitoring with analytics, intrusion detection systems, and continuous network tapping.

Each of the different security controls in the form of tools and capabilities can be installed at different capability levels, with increased scope and efficiency, starting at a level of basic (CL2) functionality and then be further enhanced with at standard (CL3), advanced (CL4) or intelligent (CL5) feature sets that may be licensed addon features that added through over time through planned implementation according to defined risk levels and budgets.

As with all other security controls, it is important, that required processes are in place on proper usage, and the competency of the people operating the different security controls are in place to support the use of the deployed security controls to make them as effective as possible.

4.3 Access Capabilities

The third and equally important area to defendable architecture is access. By definition this area focuses on provide a secure way of accessing the infrastructure for the personnel authorized to operate it in a secure way as well as authenticating and authorizing business user access to applications.

At the core of securing the different types of operators access to the infrastructure is the operator remote access platform. The more advanced threat actors are known directly attack operations personnel, compromise their endpoints, steal their credentials and then use legitimate access methods to login to the platform and compromise data directly.

Advanced threat actors are known to compromise managed services providers (MSP) [42] to which operations have been outsourced and use their credentials to access data of their clients. For this reason, having an operator remote access platform that caters for outsourcing to different groups of MSP's using multi factor authentication for access and utilizing strictly controlled and monitored jump hosts also referred to as privileged access workstations (PAW) for their daily duties. Applying multiple layers of control on the operator access with jump hosts and MFA as the basic controls, more sophisticated features such as client security posture checking and a full-fledged VDI solution can additionally be applied with dynamically pooled desktops and complete isolation between the vendor groups.

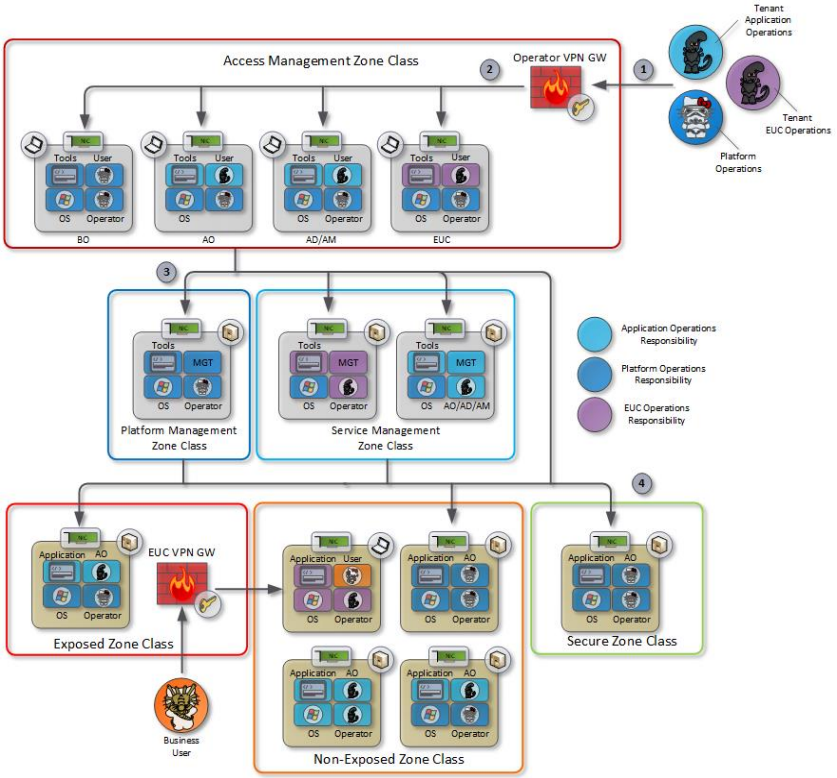


Figure 36. Operator remote access with PAW's

Key to the area of access is also a centralized mechanism of authentication and authorization for both system level access for the operators as well as application-level access for business users. A

[42] https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-cloud-hopper

central active directory or LDAP service will provide a single location for managing all levels of access and apply group policy objects to apply different settings across multiple groups of users. Using a central directory is the first step on applying a role based access control mechanisms across multiple sets of user groups and applications access.

Utilizing a central repository for users is key apply a “least level of privilege” and “need to know” access model with RBAC and can quite effectively mitigate in particular insider threats and the lower tiers of threat actors that are not able to exploit infrastructure components or applications directly.

Access capabilities is expected to include full lifecycle management of users with integration to HR systems where accounts belonging to users who no longer are engaged with the company to automatically have their access terminated.

The higher implementation levels of access capabilities would imply a higher degree of automation and analytics capabilities as well as the ability to authenticate access to resources based on policies, context and attributes utilizing a more dynamic ABAC scheme.

4.3.1 Operator Access

At **minimal** level remote operator access includes the least viable functionality for setting up secured connectivity to the infrastructure platform comes in the form of the usage of VPN, either client based or network based in the form of IPSEC, MPLS-VPN or similar. While direct access to system resources is from the operator endpoints may be possible through the vpn at this level of implementation, but the recommendation is to supplement the operator access capability with that of PAW’s.

Basic secure remote operator access also applies MFA to the minimal level vpn connectivity when client based. The remote access solution will then assure the identity of the remote access user and provide access to the privileged access workstations (PAWs) which themselves may be of different implementation levels independent of the level of operator access) for the various administrative tasks of the operators. All access to system level resources passes via the PAW's, no direct access. Authentication & authorization is typically performed locally per system and application with a limited deployment of centralized directories or AAA solutions.

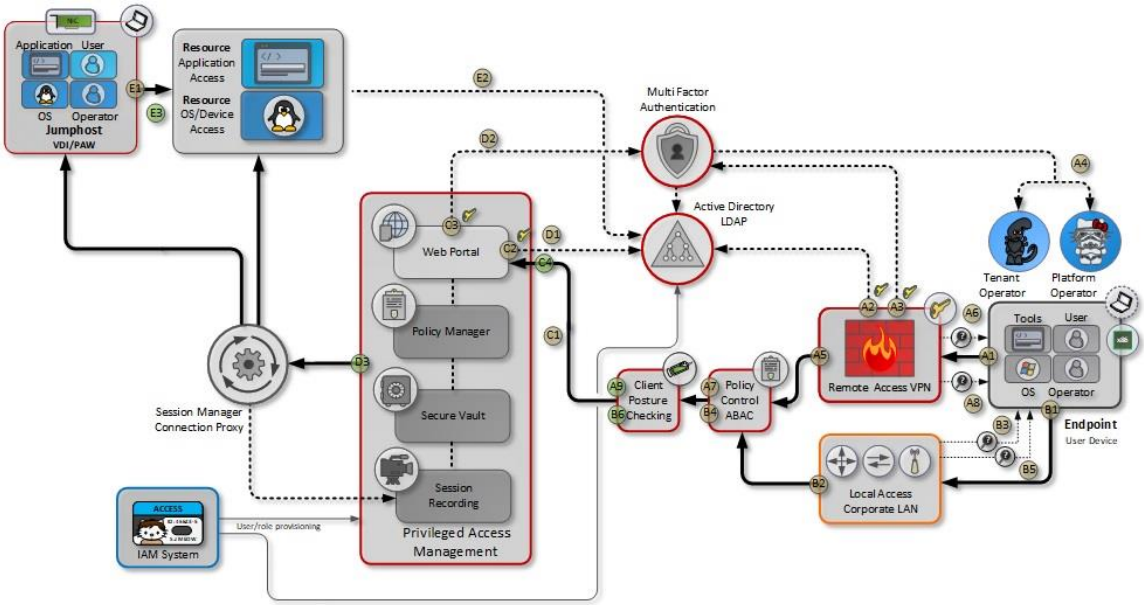


Figure 37. Functional components for Intelligent (CL5) operator access

A **standard** remote access solution adds the capability to perform posture checking of the clients trying to establish a remote connection through vpn. Based on policy, different user groups can have

their clients audited for certain parameters such as operating system patch levels, anti-virus or firewall software installed, or any other custom attribute as required before allowing the client access to the internal network. This is useful to determine if a remote client of either an employee or a vendor meets the required minimum standards to connect remotely to the infrastructure.

Implementing an operator access solution with **advanced** capabilities also include the implementation of a full privileged access management solution (PAM) that gives access to resources based on configured policy. The PAM solution would include password rotation capabilities to make sure that device logon credentials are not known to the remote operator and is dynamically changed at set intervals. Operators' session on the PAM solution would be subject to session recording of both CLI and GUI based access methods for later auditing and playback as required.

Intelligent level of implementation means the operator access is policy driven and authentication and authorization is context-based granting access based on various attributes such as location, endpoint type, time etc. The operator access is fully integrated with the IAM and PAM solutions for all forms identity life cycle management, role assignment and authorization.

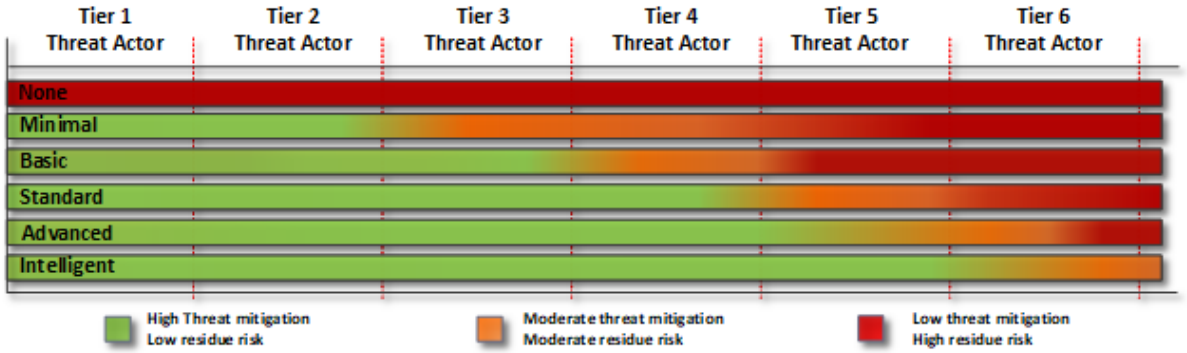


Figure 38. Operator Access Mitigation Efficiency

The mitigation efficiency for each of the types of deployment is measured in the figure above.

4.3.2 Privileged Access Workstations

Depending on requirements of what tiers of threat actors to mitigate, risks and chosen operating model of the infrastructure, different deployments of PAWs can be used, depicted here as basic, intermediate of advanced deployment models. The deployment chosen will reflect the requirements of the respective enterprise and the level of functionality, separation and threat mitigation required. The more advanced functionality and separation that is required, the higher the cost.

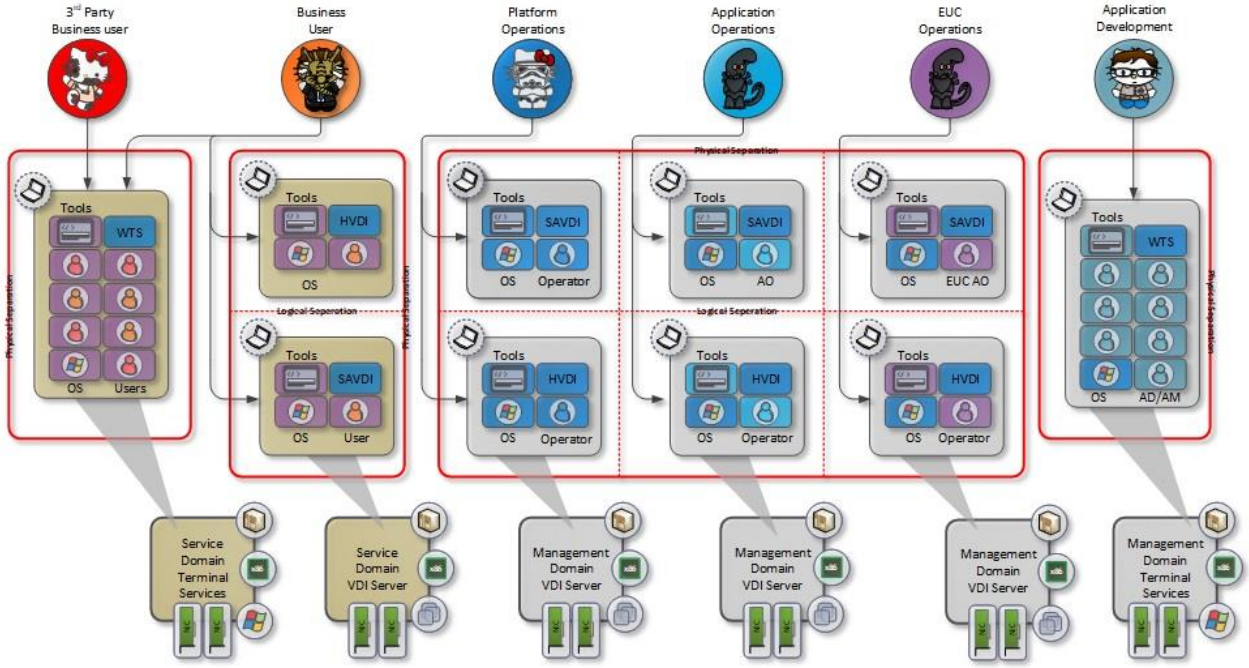


Figure 39. Intelligent level (CL5) PAW deployment

A **minimal** setup utilizes a shared desktop solution such as windows terminal server, but mixed for all user groups, operators and enterprise users. Deployed to the access management zone class if resource isolation is implemented at this level. EDR agents, logging etc present at the jumphosts if these capabilities are deployed to basic implementation level or higher.

The **basic** deployment model utilizes a simple windows terminal server setup similar to minimal level but are separating the business users from those of the operators. At this implementation level the solution does, however, not distinguish between the different operator types. Windows GPO's and OS parameters regulate which users can do what. Company issued physical PAWs are mandatory to be used by vendors and contractors performing initial base install of the infrastructure before remote access is established. It is also a requirement to have endpoint detection and response implemented at a minimum basic level since EDR capability is essential to securing the integrity of jumphosts

With a **standard** deployment model, windows terminal server may still be the software of choice for efficiency, but there are different pools of underlying physical servers serving different groups of operators such as platform operators, tenant operators, application operators etc. The main division should be between the platform operators who can access everything, and the tenant operators with a limited set of access. Other groups of tenant operators, such as operators of a corporate end user platform (EUC) can also be considered a candidate for physical separation.

Using the **advanced** deployment of PAW deploys a full-fledged virtual desktop infrastructure. It can contain a combination of terminal servers for lighter user groups with limited requirements for privileged access such as application developers, and more persistent virtual desktop machines that

are used by the operators as personal and dedicated environment for their daily operations works where the required management tools and applications are installed.

At an **intelligent** implementation level more sophisticated and dynamic functionality is added to the jumphosts, the VDI's can be either dynamic desktops that are created from an image on login and deleted after logging off, or hosted virtual machines that persists after logoff. The dynamic VDI's reduces the risk of malware taking root in the operators' desktops as the VDI is deleted on logoff, taking any eventual malware infection running on it on deletion.

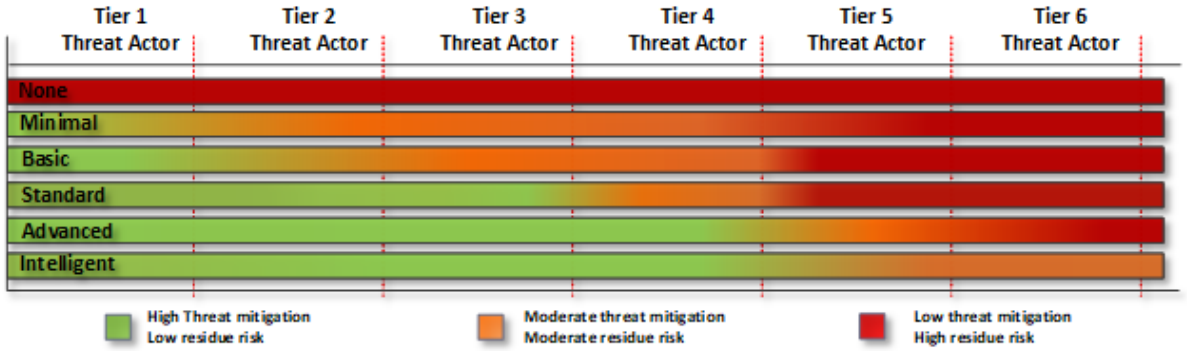


Figure 40. PAW Mitigation Efficiency

The mitigation efficiency for each of the types of deployment is measured in the figure above.

4.3.3 Identity & Access management

Identity and access management (IAM) is about defining and managing the roles and access privileges of individual users and the circumstances in which these users are granted (or denied) those privileges. In this context, it is the identity of employees that are the focus with the main objective of the IAM system being to provide **one** digital identity per individual. Once that digital identity has been established, it must be maintained, modified and monitored throughout each user's "lifecycle" and all forms of access granted should be surrounded around that single identity.

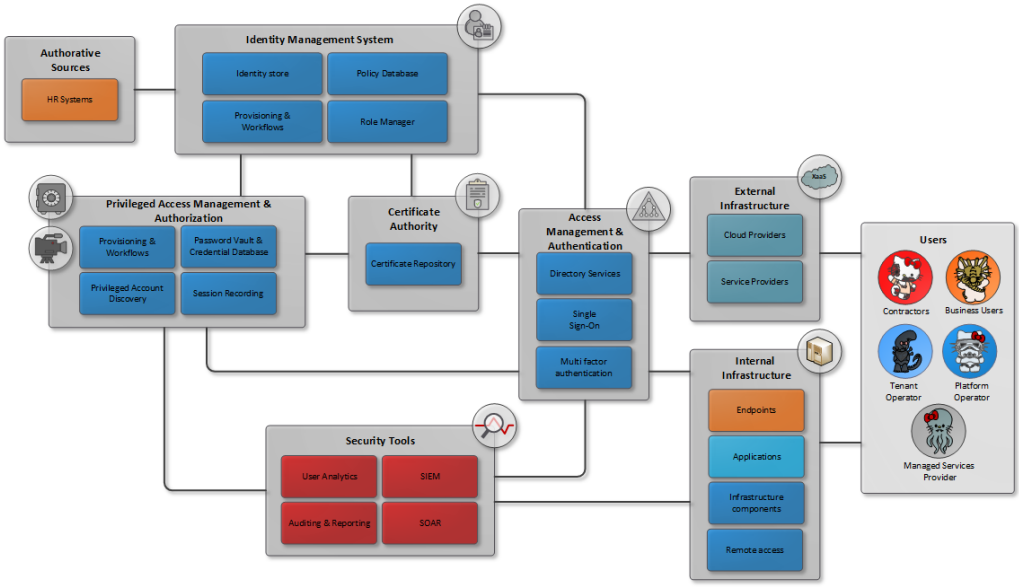


Figure 41. Identity and Access Management

At a **minimum** level access management and identity governance is at least IGA established at process wise. System support is not present using manual mechanisms to maintain overview, like an

access database or excel. Authentication is local to all systems, common directories for authentication are of limited usage

The **basic** level of an IAM implementation focused mainly on the life cycle and workflow management of employees and managed services providers from when they start and until the point where they leave the organization and further controls who have access to different applications, data or assets based on defined roles.

These roles are applied to the users based on their functions or changed when the user changes their job functions. Have logging of the approvals as to why they are created and who approved their creation. So, in the first basic step, the organization should simply bring the workflow of providing access to an application or update of access or deletion of access via an IAM tool rather than managing approvals through emails and manual processes.

Life cycle management of identities should be managed and preferably automated with the IAM system being linked to the relevant HR master databases system, so the organization's identities are automatically created or suspended on new hires and when the relationship with the organization is terminated.

It is important to understand that for a basic level of implementation, account creation within applications may be done manually however, user life cycle management and workflows have been implemented via IAM. With the basic functionality and process support implemented, the organization can move towards the next implementation level.

Technical integration for provisioning of accounts and credentials may be partially implemented or manual for the majority of the systems and applications, but from a process perspective, all access rights are granted via the established processes.

At the **standard** implementation level of IAM, key objective is to integration to directory services, systems and applications through connectors for the purpose of user provisioning and de-provisioning. Roles and authorization to the systems is managed through the role manager and audit and compliance reports can be produced quickly and accurate for all systems and/or users.

The standard implementation of identity and access management would require a full IAM system to be implemented. The IAM system would also be the authorizing part of granting access to resources applying multiple contexts to a request for access to a resource such as geo location, device type being used, time of the day, in addition to simple group GPO membership.

Authentication to resources is granted with a centralized directory services such as LDAP or Active Directory (AD). All users are provisioned into the directory and access to resources is granted via group memberships or so-called group policy objects (GPO). No local accounts should by default be used on any resource, server, service or application except for break the class credentials in case of emergencies. Lifecycle management would be process supported and authorization or context not in scope for basic capability.

All critical assets have their credentials managed via IGA and are expected to be integrated directly with the IAM systems along all key systems. Fully for the management domain, partially for the service domain.

The primary goal of an **advanced** IAM implementation should be reconciliation for as many systems as possible (both connected, that is, systems that interface with a component of the IAM system, and disconnected, where system account information is dumped from target system and imported to IAM system on a manual basis. This way all the orphaned accounts can be discovered, mapped to human users and clean up performed. After that is all done, the next step can commence which is the provisioning/de-provisioning/using IAM system for access management.

At **intelligent** implementation levels, it is expected that all access management is fully automated though intelligent workflows which support automated approval through policies. The majority of the assets are integrated with the IAM system for the provisioning of access rights and entitlements. The IAM system and all relevant authentication subcomponents are integrated towards user behavior analysis function (UBA) to monitor for abnormal or unauthorized behavior using automated playbooks and response capabilities on anomaly detection. Context based authentication mechanisms that grant differentiated access based on user, resource, device, location or other attributes is supporting the directory services for all types of access.

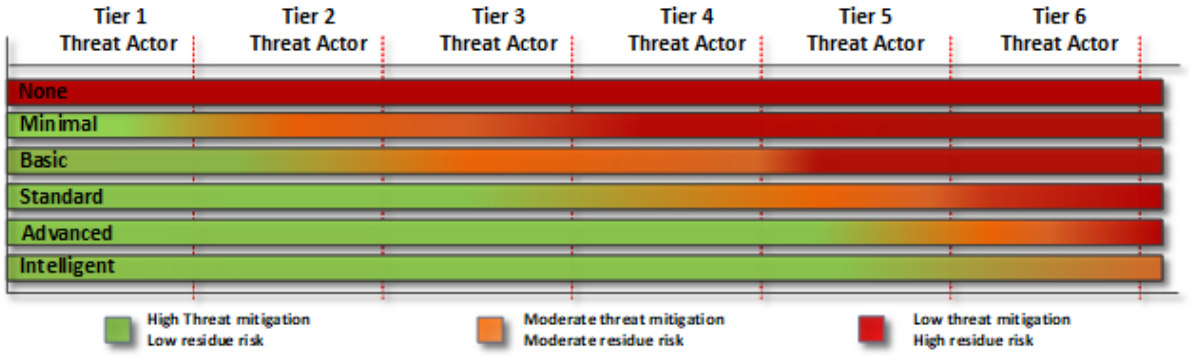


Figure 42. Identity & Access Management Mitigation Efficiency

The mitigation efficiency for each of the levels of capability deployment is measured in the figure above.

4.4 Considerations on cloud delivery models

The usage of cloud-based services for information and communications technology (ICT) infrastructure are now mainstream across most industry sectors. Purchasing and using services from an external provider for ICT however is not something new. The usage cloud services comes with associated risk levels that are essentially the same as that for outsourcing of traditional ICT operating services, where risk and vulnerability are associated with the choice of provider, location, communication channels and not at least architecture.

Depending on the chosen model of the cloud service from the service provider (SP), IaaS, PaaS or SaaS, there is a variable set of security controls that available

- Delivered, Operated and configured by the tenant
- Delivered and operated by the SP and configured by the tenant
- Delivered, operated and configured by the SP

Typically, tenant security controls are delivered and/or configured by the tenant while the provider have exclusive access to the underlying parts of the infrastructure. Even software as a service should have some basic integration with the tenant's infrastructure for items such as access control and be capable of providing basic audit trails to be integrated into the organization's security monitoring.

For IaaS/PaaS deployments the security controls that are provided by the SP is configurable by tenant for, thus tenant is still responsible for proper security of the configuration even if delivered by SP. There are numerous security breaches that have occurred due to misconfiguration in public cloud.

What public cloud service providers do:

- Protect themselves from tenants influencing their infrastructure
- Protect tenants from directly influencing each other through SP infrastructure
- Protect tenants from basic external DDOS

What public cloud service providers don't:

- Implement tenant security controls
- Configure tenant security controls
- Protect tenant infrastructure from any external or internal threats apart from DDOS

Since there are numerous configurable options available for public cloud services, security architecture and reference blueprints with valid design examples are still required for public cloud. There are many examples where misconfiguration or the misconception that default configuration in public cloud providers provide a sufficient level of security

Defendable Architecture is organized into the forementioned 14 capabilities with defined objectives and security principles attached to them. The valid design examples in the documentation are using many traditional on-prem components and building blocks to show how to achieve the security objectives, for a public cloud environment, different building blocks may be required to use public cloud in a cloud native way.

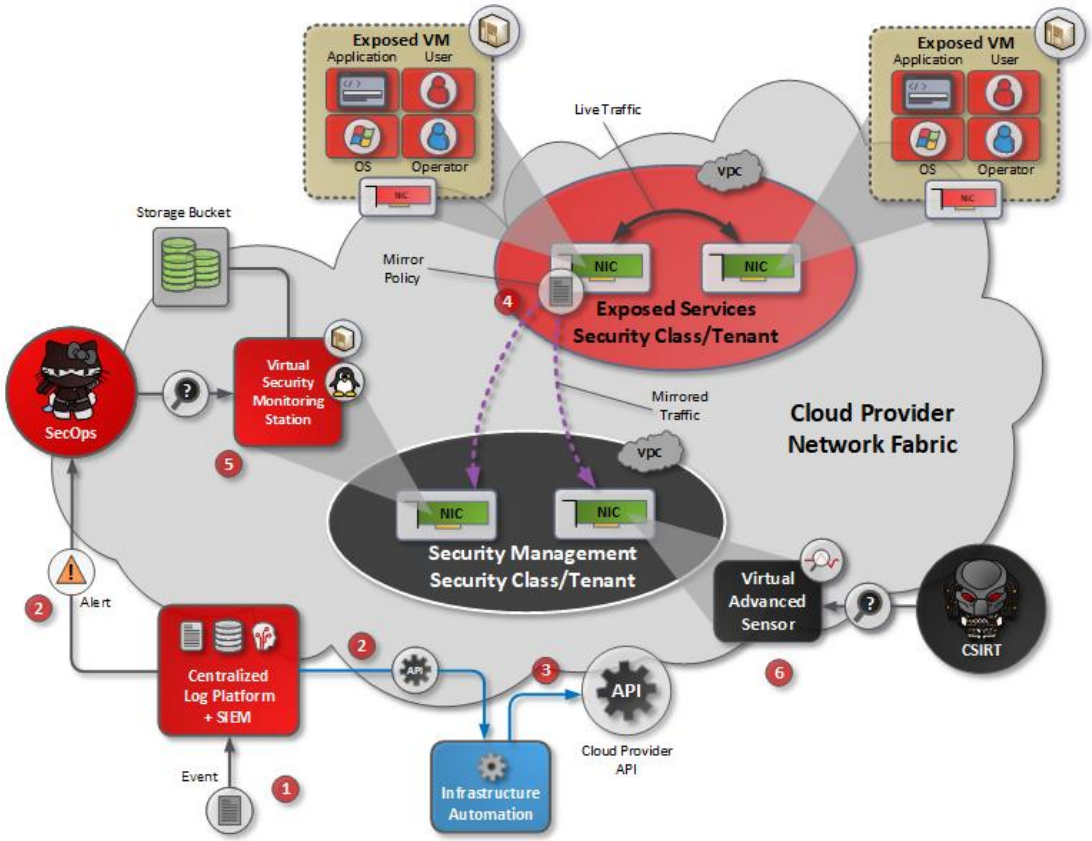


Figure 43. Automated network tapping playbook in public cloud

Observation 002-5: *While DA Objectives are valid across all environments on-prem design examples and artefacts are not always directly transferrable to public cloud environments. The modularity in the form of the implementation levels is also applicable to public cloud to balance cost vs risk and regulatory requirements and is of particularity importance as public cloud resources are billed on usage in an opex model.*

Observation 002-6: *ICT deployed to public cloud require the same control areas as on-prem to be considered defendable but public cloud security controls require different building blocks and design artifacts to achieve the same objectives*

5 Managing residue risk & tracking capability efficiency

After implementing different implementation levels of the defined security controls a measurement of the organization's overall security posture, the residue risk and a overall roadmap to track the development of security within the organization should be created.

The first topic on the list is to apply the threat mitigation levels of the defined controls towards those risks that were identified earlier in the process to see what risks are mitigated down to more tolerable levels and what is the remaining level of risk that remains within the organization. Remaining risks are those that remain after controls are applied through risk reduction actions, or the risk is either avoided, transferred or accepted and is referred to as residual risk.

Residual risk is the risk that remains after the risks have been treated. Proper risk management involves treating risks meaning that for each identified risk a choice is made to either avoid, reduce, transfer or accept it. To completely eliminate risk is difficult and normally there a residual risk that remains after each risk item have been mitigated with one of the approaches as mentioned above.

Risks as documented in this document are mostly subject to risk reduction as the main mitigating measure through the implementation of the different 14 capabilities and using the effectiveness ratings as explained in sections **3.10** and **3.11**.

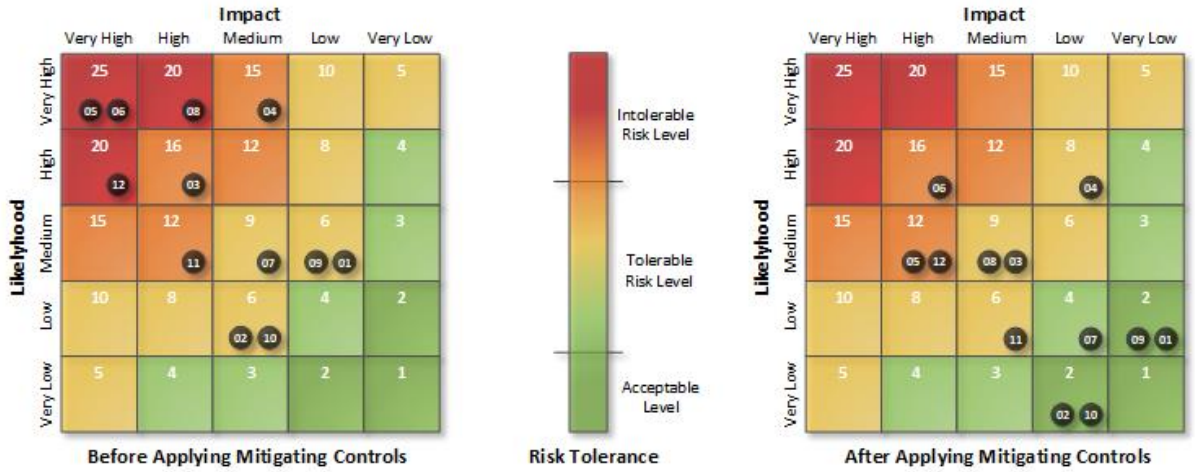


Figure 44. Overall Business Risk before and after mitigating controls

By applying the risk reducing security controls with their measured effectiveness gives an overview of residue risks as shown in Figure 44 above where the initial level of risk is brought down considerably by the implemented controls but still some remain in the intolerable regions. A roadmap needs to be developed on how to deal with these remaining risks. Any risk identified should be added to the organizations risk register [43] to track its development.

5.1 Tracking capability implementation quality

Just purchasing the tools required for the capabilities is not enough, there are many ways of doing the implementation and not all of them are equally good. Features might not be fully implemented, or not configured in the desired way for maximum outcome and competence or process might not be at adequate levels

[43] https://en.wikipedia.org/wiki/Risk_register

While mitigation is mainly tracked by the efficiency of the control to mitigate threat actor attacks as described in sections **3.10**, tracking the quality of the capabilities by measuring the implementation quality also adds to the overall effectiveness. This is done by measuring implementation quality, process maturity and the role definitions and competency of the people to use it and depending on the combined levels of these elements may either improve or drastically reduce the measured effectiveness.

5.1.1 Capability quality

To assist on implementing things right, security principles are added under the description of each capability in the ***detailed documentation packages*** describing the different capabilities. These security principles have a dual function, they act as both requirements and guide on implementing a capability in the correct way and also as checkpoints on measuring the quality of the implementation.

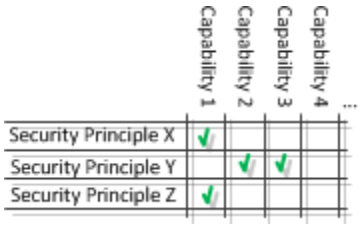


Figure 45. Security Principles Mapping

To use the security principles as KPI's they have been mapped to one or more of the 14 capabilities as shown in figure **Figure 45** above. The mapping is documented in supplementary excel spreadsheet DA_Assessment_template-v3-.xls and the design principles also have weighting applied to them since some of them are more important than others.

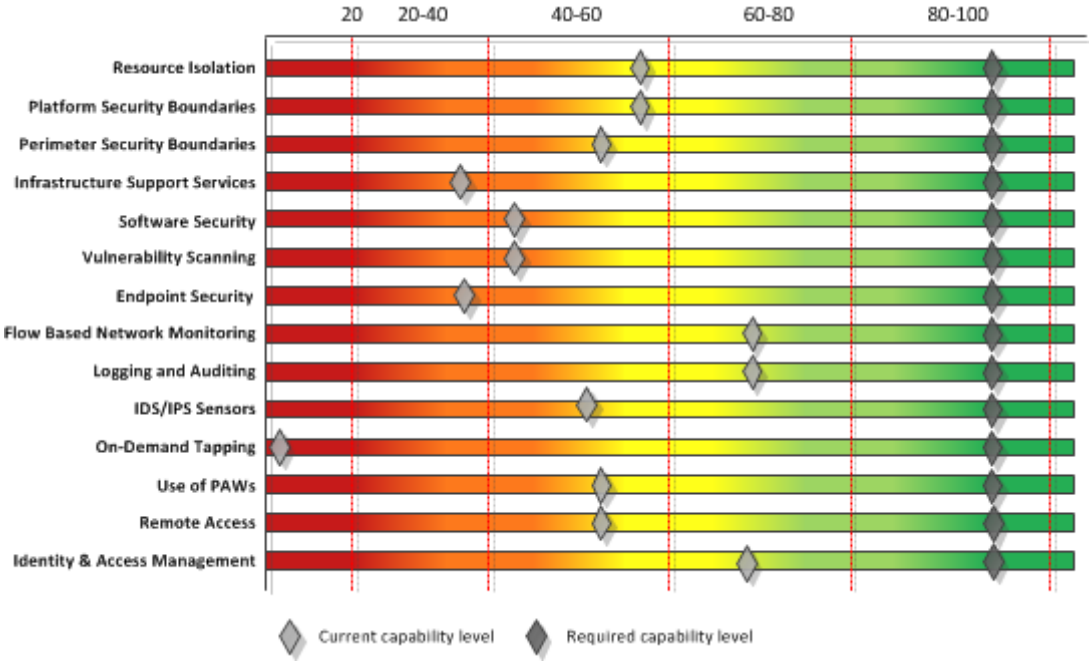


Figure 46. Security Principles Assessment

Choosing either fully, partially or not compliant to the security principles within a single category will result in a score for each of them that when summarized for all the security principles in a single

capability category will range from 0 to 100 depending on compliance status as shown in **Figure 46** below. This score will reflect the effectiveness of the control as highlighted in **Table 4**

Security Principle 002-21: *All infrastructure shall have its security controls regularly audited for implementation quality, no less than 1 time per year*

5.1.2 Capability Process maturity measurement

Security process maturity matters, as with all learning, organizations need to learn walk before being able to run and then can consider joining a full-length marathon. It is too often falsely assumed that an organization is able to quickly adapt to and implement sophisticated and effective defense-in-depth cybersecurity controls where no such capabilities have been before.

For the capability to be effective it needs to be supported by adequate processes. There is for instance little use of an IDS system if it is not properly integrated into the overall security operations center and/or operation support systems, or no one know what to do when an alert is triggered. A good example of this is the Target incident in 2013 [44] where sophisticated detection systems had been installed and the initial breach was detected but failed to properly respond to the incident. This failure from the security operations to properly respond resulted in the loss of 40 million credit card numbers and other customer related information and the legal settlements came up to 18,5M[45] USD in direct costs, and on top of that, the cost of the efforts to clean up.

The process maturity of an individual capability is directly reflected by the overall security maturity in an organization, which covers fields ranging from governance, security operations, and insights into assets threats and risks.

To properly measure the effectiveness of the defensive capability the supporting processes must be identified, if any, are processes defined at all? How mature are they? How is integration with OAM and SOC teams, both tool wise and process wise and have playbooks been defined. A mature process should have all these in place.

The process maturity also plays a major role if the ambition is to automate response capabilities (which is becoming a must to tackle the upper tiers of threat actors) to handle security incidents. It is simply not possible to automate something which is not properly defined, have acceptance criteria or playbooks attached to it.

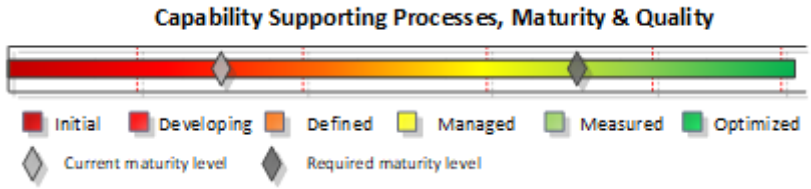


Figure 47. Capability Process Maturity

To help define the maturity of processes connected with a capability, 5 levels of maturity have been defined, which will affect the efficiency rating of a capability:

- Initial
- Developing

[44] https://www.reuters.com/article/target-breach/target-missed-early-alert-of-credit-card-data
[45] https://www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach

- Defined
- Managed
- Measured
- Optimized

At **initial** level, no formal security governance is in place in the organization and thus no supporting process is implemented either to support the capability, the capability integration with relevant support systems or monitoring functions is not in place. Effectiveness of a capability is considered to be severely lacking (-3 levels) due to defined processes and policies missing. No organization with the even the slightest level of responsibility to its customers should be at this level and it is provided for reference only.

At **developed** level, basic security governance has been established as part of the overall security maturity and the capability is supported by a defined policy, but process support is limited by missing clear definitions or proper anchoring in the organization. The capability or tool is freestanding with partial integration to the some of the major operational support systems for alerts. Effectiveness of a capability is considered to be sub-optimal (-2 levels)

At **defined** level, the capability is supported by processes that are acknowledged across the organization along with clearly defined policies for usage. There is however less focus on verification of results in the form of KPI's or other reporting. Integration with most operational support systems such as fault monitoring, alerting and logging is in place but is still considered partial and due to lacking integration with ticketing or other service management tools. Effectiveness of a control is considered to be less than optimal (-1 level)

At **managed** level, the supporting processes and policies for the capability are not only defined but also properly executed in the organization. The capability is fully integrated into all monitoring and service management systems. Playbooks, although manual, have been created for resolution of major categories of incidents. Beginning a SOAR[46] implementation is possible at this level. Effectiveness of a defined capability is assumed to be at 100%

At **measured** level, management processes and policies supporting the capability are not only defined but also have clear KPI's attached to them so their effectiveness can be measured and tracked over time. Some degree of automation also takes place at this stage. The capability is fully integrated into all operational support systems and service management tools having in addition analytics applied to see trends and support strategic planning. At least partial automation is expected to be in place for the capability at this level. Effectiveness of a defined capability is assumed to be optimal and at 100%

At **optimized** level, capability supporting processes are comprehensively implemented, using risk-based methodology and organization wide acceptance. Effectiveness is constantly monitored through a continuous improvement process. The capability is fully integrated into all relevant monitoring and service management systems and apply automated playbooks for most incident resolution using a SOAR framework. Effectiveness of a control is considered to be increased beyond the defined baseline (+1 levels).

Security Principle 002-22: *All infrastructure shall have its security controls regularly audited for process maturity, no less than 1 time per year*

[46] https://www.rapid7.com/solutions/security-orchestration-and-automation/

5.1.3 People skillset measurement

Equally important to the effectiveness of a security control and capabilities is the people making use of them on a daily basis and the competency of those people. A tool can only be as effective as the people using them, and if role descriptions and skillsets are missing the return of investment in a security control in the form of its mitigation effectiveness is drastically reduced. Similarly, to the process maturity, people also need to learn to walk before they can run and start to implement the more advanced versions of capabilities.

For example, implementing sophisticated SIEM features to perform threat hunting, or deploying privileged access management (PAM) solutions to their full effectiveness will be quite difficult if not the foundational skillset is present in the operations team. They need to develop the skillset to implement the basic version of the capabilities such as centralized logging and remote access with MFA and jumphosts or other basic IT functions like directory services, service ticketing, and asset management before being considered mature enough to support advanced capabilities.

People and competency mapping to measure capability effectiveness needs to be done on the team that are both the operators and users of the capabilities, and this may span both OAM and SOC teams depending on capability and organizational setup. CSIRT team is also directly involved in using the capabilities and is thus also required to be of sufficient maturity to make capabilities efficient

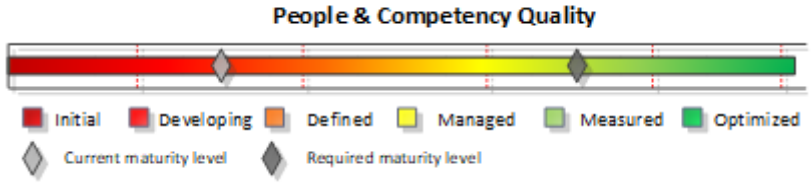


Figure 48. People & Competency Maturity

The same 6 levels of measurement as in the process maturity assessment can also be applied to people and competency maturity.

- Initial
- Developing
- Defined
- Managed
- Measured
- Optimized

At **initial** competency level capabilities activities are unstaffed and uncoordinated among the relevant functions of the OAM or SOC teams. Effectiveness of a specific capability is considered to be severely lacking (-3 levels) due to roles, responsibilities and competency missing.

At **developing** levels overall security maturity is increased resulting in information security leadership being established, with informal communication. Staffing attached to the capability is still considered unclear among the operations teams. Effectiveness of a capability is considered to be sub-optimal (-2 levels)

At **defined** levels, some roles and responsibilities are formally established within the operations teams along with competency and certification requirements. The effectiveness of a control is considered to be less than optimal (-1 level)

At **managed** levels the organization have developed significantly in the security maturity space resulting in increased resources allocated as well as organization wide awareness. Personnel

operating the capabilities have clearly defined roles and responsibilities. Effectiveness of a defined capability is assumed to be optimal and at 100%

At **measured** levels, all the capabilities are manned by specialist teams with clear role descriptions but are also measured for the competencies and development plans. The required certifications for each individual role have been developed for the specialists on the different teams and clear development roadmaps are in place for each individual person to meet the defined requirements and organization resources are made available to support those goals. Effectiveness of a defined capability is assumed to be optimal and at 100%

At **optimized** levels, the organization have developed a culture that supports continuous improvement, to security skills, process, technology. All capabilities have clearly defined roles that are manned by specialists that are always pro-active in the daily tasks and are actively and consistently encouraged by the organization to further develop their skills. Effectiveness of a control is considered to be increased beyond the defined baseline (1+ levels).

Security Principle 002-23: *All infrastructure shall have its security controls regularly audited for competency quality, no less than 1 time per year*

5.1.4 Visualizing mitigation gaps and risk

To further track the overall development of the defined security controls and defensive capabilities to provide an overview of risks, a chart can easily be produced based on the 14 capabilities. If the required target is to mitigate a tier 6 threat actor which require and advanced implementation of resource isolation as an example and the current implementation is only basic there is a challenge.

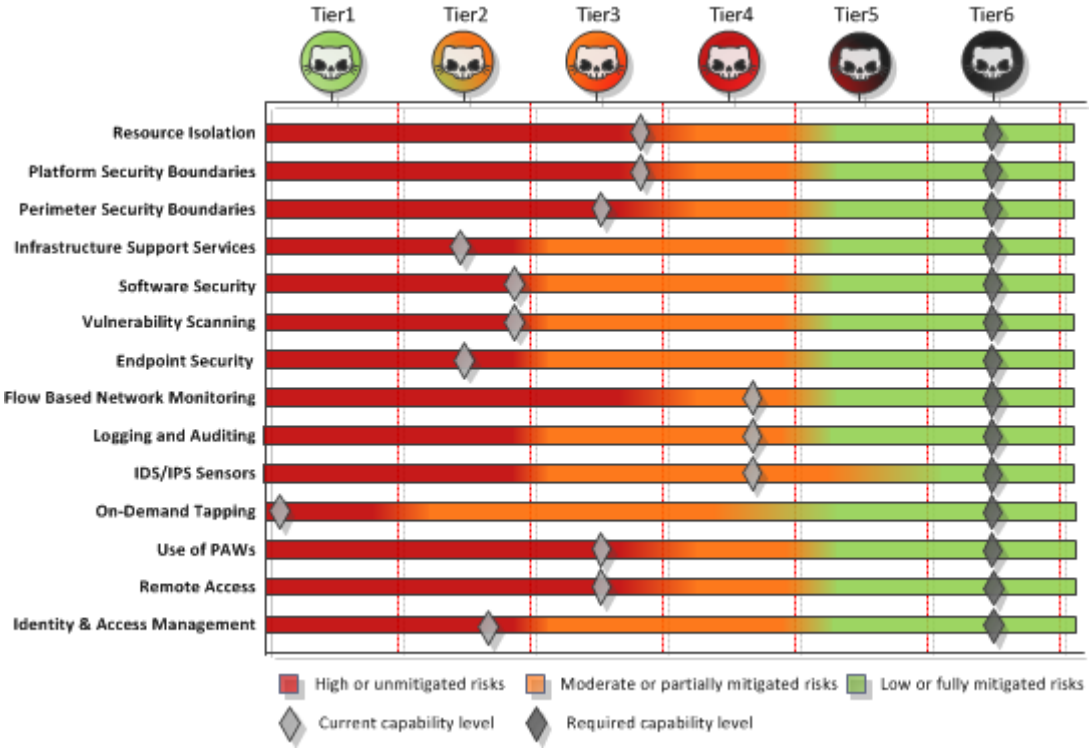


Figure 49. Example threat mitigation overview of Defensive Capabilities

The basic implementation which is assumed to mitigate only a tier 3 threat actor, provides a significant gap and lack of ability to limit breach of the infrastructure and corresponding lateral movement of tier 4 and above threat actors. Visualizing risk in this matter comes a long way when communicating to upper management and presenting the overall status of the enterprise's security

posture. The figure above reverse the coloring from **Figure 9** to display unmitigated risk as opposed to risk mitigation effectiveness.

5.1.5 Creating capability Scorecards

Adding the score for each of the capabilities together can present a total chart of the effectiveness of the implementation of each of them. Displaying this will show quite well if the implementation has been successful or not as per requirements stated in the security principles or if process support or competency is missing and needs to be developed. It can also be a checkpoint to see that individual functionality have been implemented and used as a signoff for any external vendor that may have been contracted to deliver the implementation in parts or whole of a capability to verify that everything is implemented according to scope of work and the requirements.

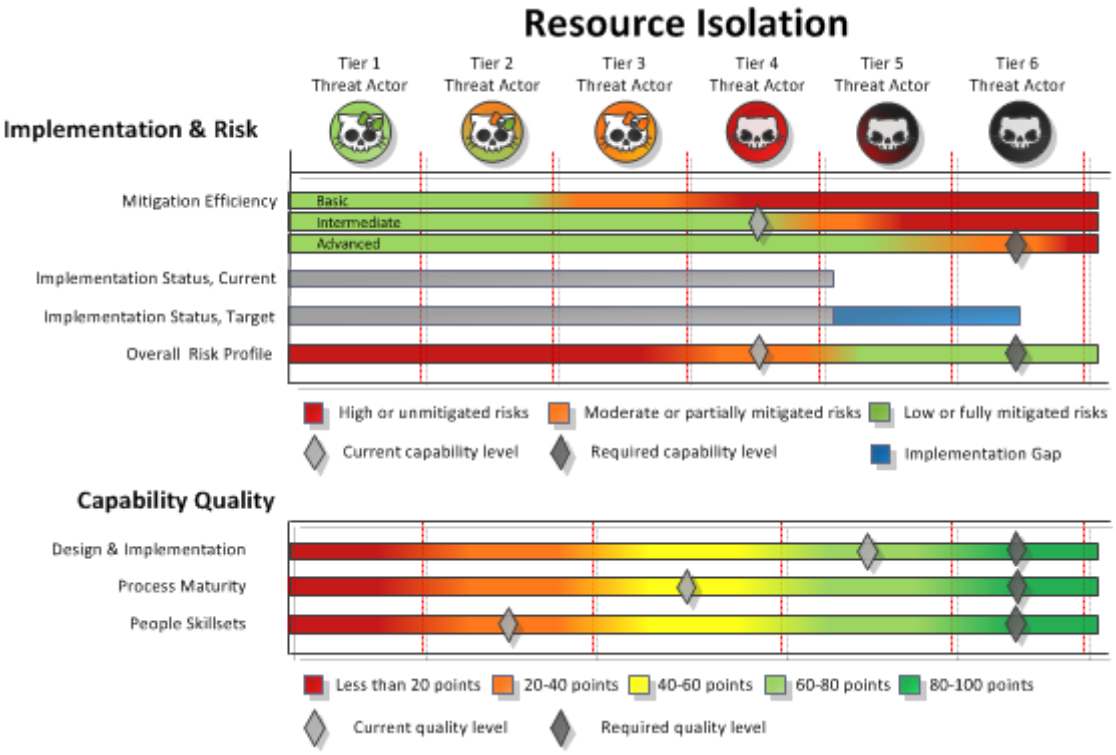


Figure 50. Capability Score Card

Combining all the information charts shown in the charts above can then be used to create a score card for each of the defined capabilities that make up defendable architecture to give a complete overview of both implementation status, implementation quality as well as process maturity and people skillsets required to make proper use of the capability.

Note that the full scope of security operations in the form of process maturity and people requirements and are not fully detailed in the defendable architecture documentation at this point in time, only the measurement requirements. The aim is to also add this over time in addition to the detailed security controls technology descriptions to provide an end-to-end overview of requirements for a proper security posture.

As the capabilities are implemented or upgraded, the overall security posture will increase as will the ability to either contain and detect and thus properly mitigate more advanced threat actor.

6 Building a defendable architecture

Going through the earlier document sections with acceptable risk levels defined, regulatory requirements, business requirements taken into account and the threat actor mitigation level target set, the planning for implementing the defined security controls can take place. Since most organizations have the budget or resources available to implement every capability at the same time, the investment and implementation of the capabilities need to be spread out in time as shown in **Figure 56** using a staged approach. It is for this reason that the implementation levels have been applied to each individual capability so they can be built on top of each other and be gradually implemented in a more budget friendly way.

6.1 Setting the stage, define goals

An important topic is to do a methodical approach to implementing and planning for the implementation of defendable architecture. This section highlights a method to measure and visualize implementation status, implementation quality and a gap analysis for how to reach the required threat mitigation level (TML) and reducing the risks discovered through the analysis phase.

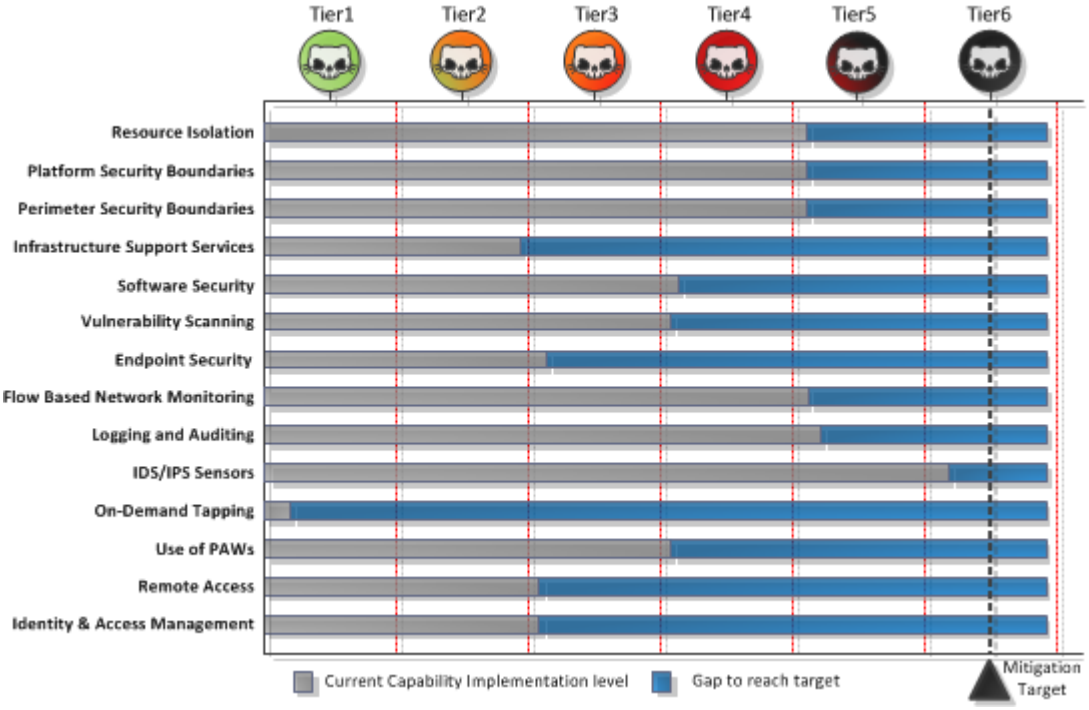


Figure 51. Example of Target and Gap Analysis of Defensive Capabilities

As mentioned in the earlier section about threat actors, the ability to mitigate certain levels of threat actors is defined by the number and level of the defensive capabilities implemented. The 3 core areas of defendable architecture, the 14 key capabilities with their feature-based sublevels is central to this. First the required mitigation level is defined for each of the 3 areas, then based on an assessment of implemented capabilities, a gap chart like the one shown in the figure above can be produced.

The chart above provides a clear overview on where the largest gaps are and based on cost levels, and available budgets a conscious decision can be made to which area to develop first. In addition to the technology aspects of the capabilities, similar development plans needs to be made in the areas of process maturity as described in section **5.1.2** and people & competency which is highlighted in

section **5.1.3**. The sum of technology, process and people make up the overall security posture of the organization as described in section **7.2**.

6.2 Design & build

During the build phase the implementation of capabilities needs to be planned so that a roadmap can be created, and resource planning and budgeting can be secured. To properly deploy the defined security controls in the form of defensive capabilities to mitigate a certain level of identified threats. Let's take a look at some sample use cases on how to apply the technology capabilities. Security operations-oriented capabilities such as process maturity and educating personnel will of course come in addition.

Company X is a standard enterprise, serving its customer services not covered by any particular regulatory law (such as PCI,HIPAA etc) except standard privacy laws such as GDPR . For this example, let's say TV and Broadcast services. The company is not targeted by any nation states or their proxies but have some experience with hacktivist and cybercrime threat actors who want to either abuse or disrupt broadcast services or steal data or information to sell.

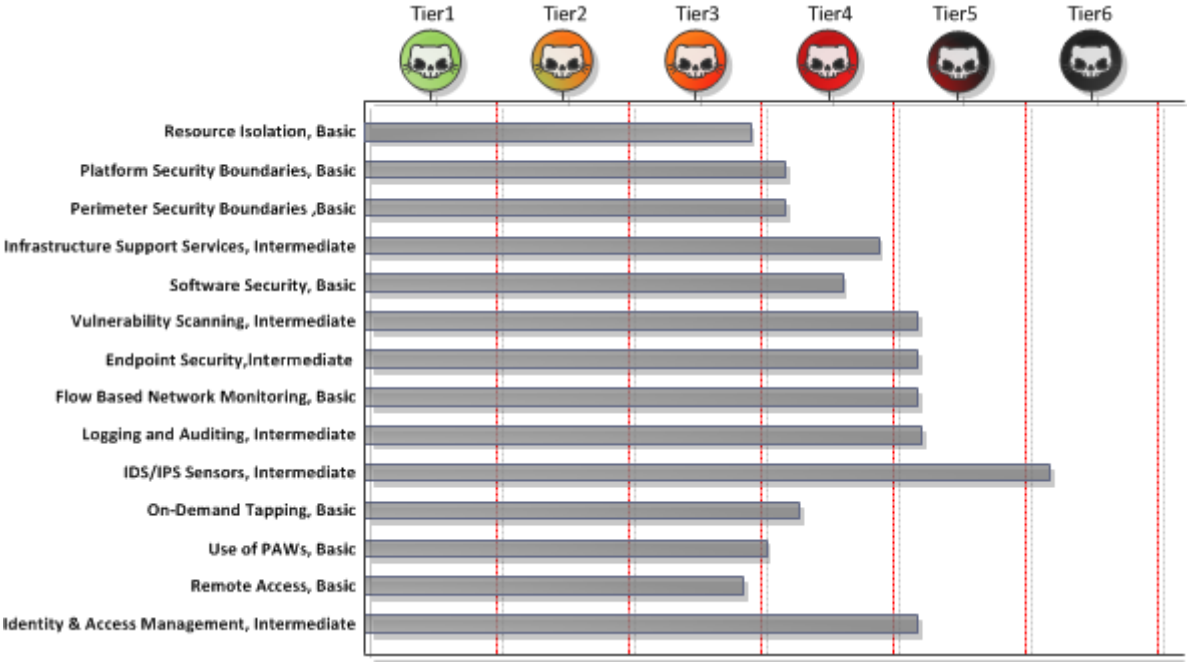


Figure 52. Usecase 1, Defensive Capabilities first phase

Based on this background, the management and security and operations teams aim to fully mitigate tier 4 threat actors as their strategic goal, but want to do it in a 2 step approach for their infrastructure. Preventive and access capabilities are initially built to mitigate tier 3 and tier 4 threat actors in the first step and further upgrading them later to be capable to fully withstand tier 4 threat actors.

On the detection side capabilities are deployed from the start to be able to detect threat actors up to tier 4 so that any breaches from the most likely risks will be detected and then responded upon by security operations and their incident management teams.

Based on the different capabilities and their levels to mitigate threat actors as shown earlier a set of capabilities and corresponding levels of implementation are chosen **Appendix 1** shows the estimated effectiveness of the different capabilities without adjustments for process maturity and competency.

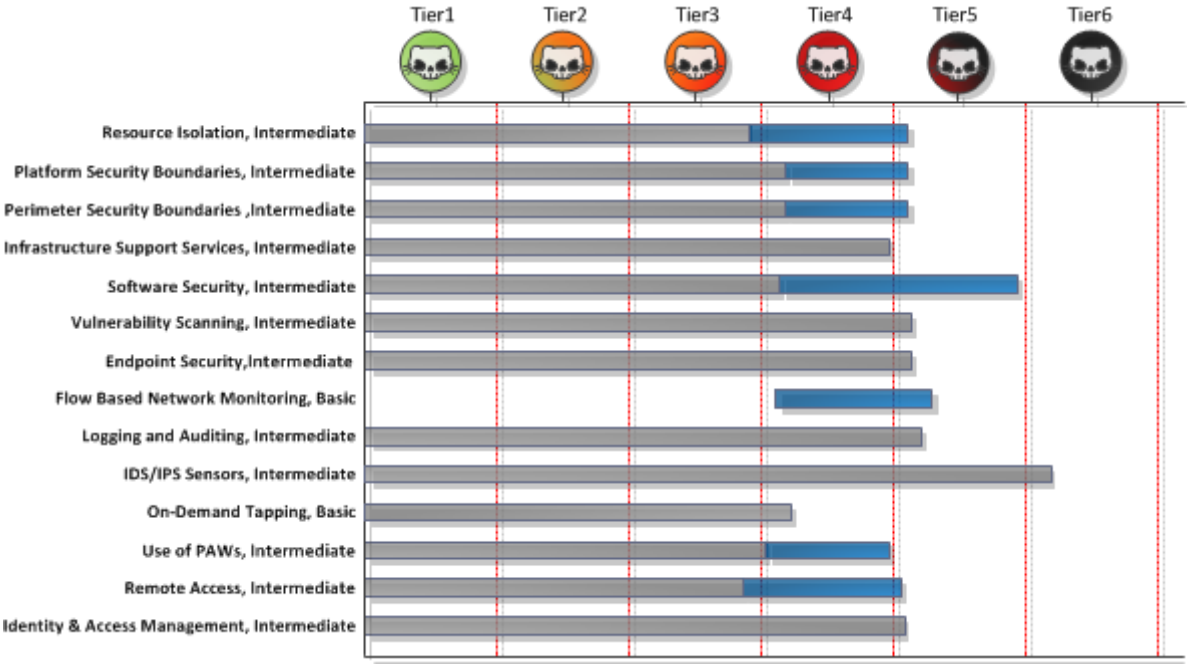


Figure 53. Usecase 1, Defensive Capabilities second phase

When planning for phase two of the upgraded security architecture, looking at the different capabilities again and their effectiveness makes it clearer to see what needs to be done in each of the different areas to fully mitigate tier 4 threat actors. The delta of existing vs required capabilities is shown in **Figure 53** above as blue colored. Knowing the gaps in the security posture makes it easier to do the proper planning and procurement as well as budgetary planning and make sure that over investment does not take place.

The second use case is about how the capabilities list can be used to measure risk in addition to assist with planning of increasing the security posture. In this use case the company in question is a provider of services that are under strong regulatory control, such as a mobile operator. Mobile operators a frequently targeted by the full specter of threat actors up to and including APT groups such as nation states and their proxies for their valuable information about their customers. Security capabilities in all areas should therefore be able to mitigate up to tier 6 attackers.

Figure 54. Usecase 2, Capabilities based mitigation overview

However, having neglected security planning and budgeting over a long period of time the company have fallen behind on keeping up with the required security posture. Measuring the currently implemented capabilities vs that which would be required, shows the delta that needs to be addressed.

The figure above also shows clearly what risk profile the company is currently running on based on the ability to either contain or detect a certain tier of attackers. In the example above, capabilities and controls have been implemented in some areas, but not nearly enough to properly mitigate the assumed risk picture, and it is expected that several data breaches have been performed by advanced threat actors, both detected and undetected.

The approach of mitigation also allows for flexibility and calculated risk, company Y have as shown in the figure above displaying their security uplift strategy decided that they want to run with some deliberate risk profile due to cost reasons, and thus not implementing the advanced versions of all capabilities, focusing more on some areas than others.

6.3 Assumptions on implementation

Based on the current threat landscape and the likelihood of exposure to one or more of the threat actor types as described in section **3.7**, the following assumptions have been used for the security design as described in this document in addition to industry best practices to build an architecture that is defendable:

1. There is at least one remotely exploitable vulnerability in the network.
2. There is at least one hostile entity in the network.
3. Security design and applied security measures are known by the attacker.
4. Attacks are likely from malicious internal hosts.

6.4 Guiding Principles for implementation

To properly define the different requirements needed to defend against threat actors and to scope the capabilities required to mitigate them, the following basic principles have been used when trying to describe the different areas in this document as given by the 20 main CIS security controls[47].

First of all is to evaluate the infrastructure and decide which assets who are the most critical ones and how to treat them:

- Which data is most important to protect?
- Which systems are most important to defend?
- Who needs access to these systems and data?

Answering these questions become critical if the ambition is to defend against APTs, the tier 5&6 threat actors since their attacks will be against specific targets of interest. System classification, business impact assessment and threat modelling can help in these assessments.

Define and implement security classes and security zones and implement adequate segregation and protection mechanisms between them applying defense in depth principles.

- Systems that need to be exposed to the Internet should have their own exposed security class and corresponding network
- Systems that need to be protected from the Internet and other sources of a lower Trust Level should have their own non-exposed security class and corresponding network zones
- Management systems that are used to control other systems should have their own management security class and corresponding network zones

How to understand and correctly apply the design principles above is at the core of this document:

Resource isolation utilizing the zone model and its usage to create security classes, security zones and to do system zoning is a foundation capability but is a complex topic requiring a lot of guidance so a reference architecture built on the zone model should be provided. Resource isolation techniques, infrastructure zoning and sharing principles for making the infrastructure both secure and efficient should be described, and software security in the form of multi tenancy principles for applications, databases and orchestration in a cloud environment is also key as this is the area where the actual breach happens.

Another critical design principle is to establish choke points for network access into and out of each security zone. These should be introduced to support sufficient level of visibility on network traffic and to avoid blind spots inside the infrastructure:

- Do not allow servers, end user endpoints or critical infrastructure components to communicate directly towards the Internet. Implement filtering gateways and proxies for each security class and ensure the only way to reach the Internet is via these gateways. Enable logging on the gateways and send the logs in real time to a secure and centralized log solution.
- Do not allow rulesets in firewalls that make it possible to log on to systems directly from the Internet. Use VPN gateways with jump hosts such as virtual desktop infrastructure (VDI) terminal servers or other intermediary systems to control and limit who gets access to what. Enable detailed logging of who has been accessing which systems, and what they do once they have accessed it. Collect the logs to a secure centralized system.

[47] https://www.cisecurity.org/controls/cis-controls-list/

Endpoints in the office network must not be allowed direct system level (e.g. OS or CLI) or privileged access to databases or other production system components in the data centers. If this type of access is allowed, all it takes for an attacker to get full control of a corporate PC and to obtain access to databases or other production systems is for to visit to a web site that exploits a hitherto unknown browser vulnerability or open an email containing a malicious attachment that exploits a security vulnerability in e.g. Microsoft Office or Adobe Reader.

Establish separate differentiated remote access solutions for the different user groups:

- All employees – for access to enterprise IT systems
- Some employees – for access to the IT & Telco infrastructure
- Vendors – for operations & support of the IT & Telco infrastructure

Use jump hosts as the only way to get access to critical systems:

- Use different jump hosts for granting access to different types of systems
- Each operator group shall have its own set of jump hosts
- The jump hosts need extended hardening, security monitoring and logging

Use Multi Factor Authentication:

- for all access from the Internet
- for access between different security domains (such from the EUC office network towards management domains of the datacenters)
- for access to critical systems or data

Last but not least, the security architecture shall be resistant to any deviations introduced to it.

6.4.1 Implementing the target security architecture

This document details the core architecture principles and blueprints for building infrastructure in accordance with the defined resource isolation requirements and also additional preventive, detection and access capabilities such as security boundaries, infrastructure support services, vulnerability management tools and security monitoring to support the required incident response processes. The difference between these two types is that the core architecture principles are best implemented when the infrastructure is being built and it will not be very cost effective to try to retrofit these capabilities later on, as it will be considerably more expensive than adding them from the start.

The additional security capabilities are more independent of nature and may be added as stand-alone functions either as a single add-on after the infrastructure is built or in a staged approach. However, some capabilities such as the flow-based network monitoring with behavioral have technical requirements for functionality in the underlying infrastructure that needs to be taken into consideration when planning the overall build. Planning for the future and having these requirements and the corresponding functionality to the infrastructure will be significantly more cost efficient than having to add them later and not having the full target architecture in mind may limit the available choices for implementing capabilities later.

As an example, not having the capability of generating netflow for the behavior-based network analysis capability natively present within the network switches would require additional mitigating capabilities to be added. Physical taps or port mirroring added to the infrastructure later will result in a higher total cost than having this functionally present from the start as some components may have to be replaced.

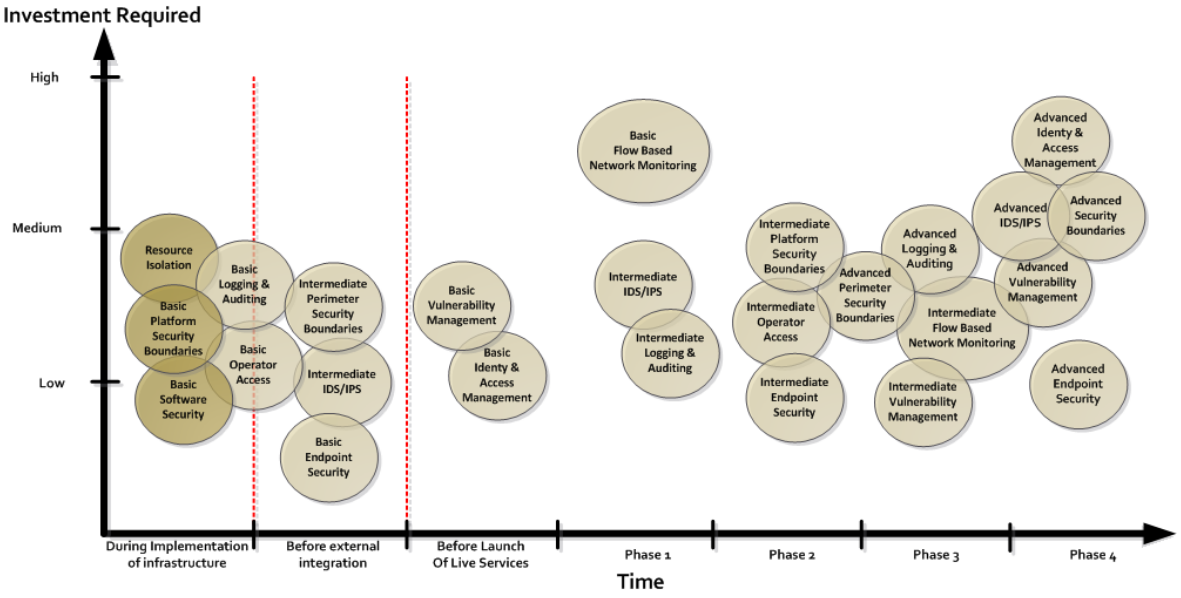


Figure 55. Baseline Architecture and capabilities

Since the capabilities are free-standing from a platform perspective these can be added separately from the underlying infrastructure. It may be spread out in time depending on risk evaluation and available capex. In the early phase of an implementation or in very small environment the separation principles might appear as high. But building the infrastructure in accordance with the architecture design principles, the scale will over time reduce the overhead of the zone class separation principles resulting in a security compliant as well as efficient infrastructure naturally.

Figure 55 shows the architecture principles and the additional capabilities that are described in different sections of this guideline document. Capabilities have been described to assist deployment by providing blueprints on how these can be built and to link the total set of requirements and apply them where they are relevant for the underlying infrastructure. This document is outlined as follows:

Architecture principles for preventive capabilities:

- Resource isolation using the zone model
- Resource isolation separation principles
- Reference architecture and topology for resource isolation mitigating up to tier 6 threat actors
- Software Security for platform multi tenancy

Capabilities:

- Preventive
  - Platform Security Boundaries
  - Perimeter Security Boundaries
  - Infrastructure support services
  - Software Security
  - Vulnerability Scanning
- Detection
  - Flow Based Monitoring with Analytics
  - Network tapping
  - Logging and auditing

  - Endpoint Security
  - IDS/IPS Sensors
- Access
  - Operator Remote access
  - Use of PAWs
  - Identity and Access Management

Security Principle 002-24: *Core architectural security principles are mandatory to follow*

Security Principle 002-25: *Capabilities are either mandatory or optional to implement, it is decided by the Business Security Officer in accordance with the specific risk picture, threat actor mitigation ambitions and any regulatory requirements if applicable.*

Security Principle 002-26: *Deviations to mandatory requirements shall be handled in accordance with the risk-based deviation process and be signed off by the relevant risk owners and added to the local risk register.*

6.4.2 Deviations to the defined architecture

Any deviations to an architectural specification as described in this document normally means that a requirement will not or cannot be complied with (e.g. for technical or business reasons). It is in the interest of the company and their eventual customers that the residual risk arising from non-compliance is kept to a minimum and that adequate compensating controls are implemented.

All deviations from the security requirements must be handled according to the defined procedure for “Deviation Handing”. The residual risk from implementing the deviation must be understood and accepted at the correct place(s) and level in the organization for the purpose of avoiding unacceptable risk to other assets.

Before considering deviations from these requirements, ask the following questions:

- What triggered the deviation?
- Is the deviation the correct one, for the right reasons?
- Are there any dependencies to other areas? What are the risks to these?
- Has Architecture and/or Security team(s) been included in the deviation process?
- Are there adequate compensating controls in place?
- Has the risk owner at the correct level signed off on the deviation?
- Is the deviation adequately documented and registered?
- Is there a defined time frame for closing the deviation?
- Have the residual risks of deviating from this policy been understood?

Security Principle 002-27: *Do not start the deviation process unless satisfactory answers can be given.*

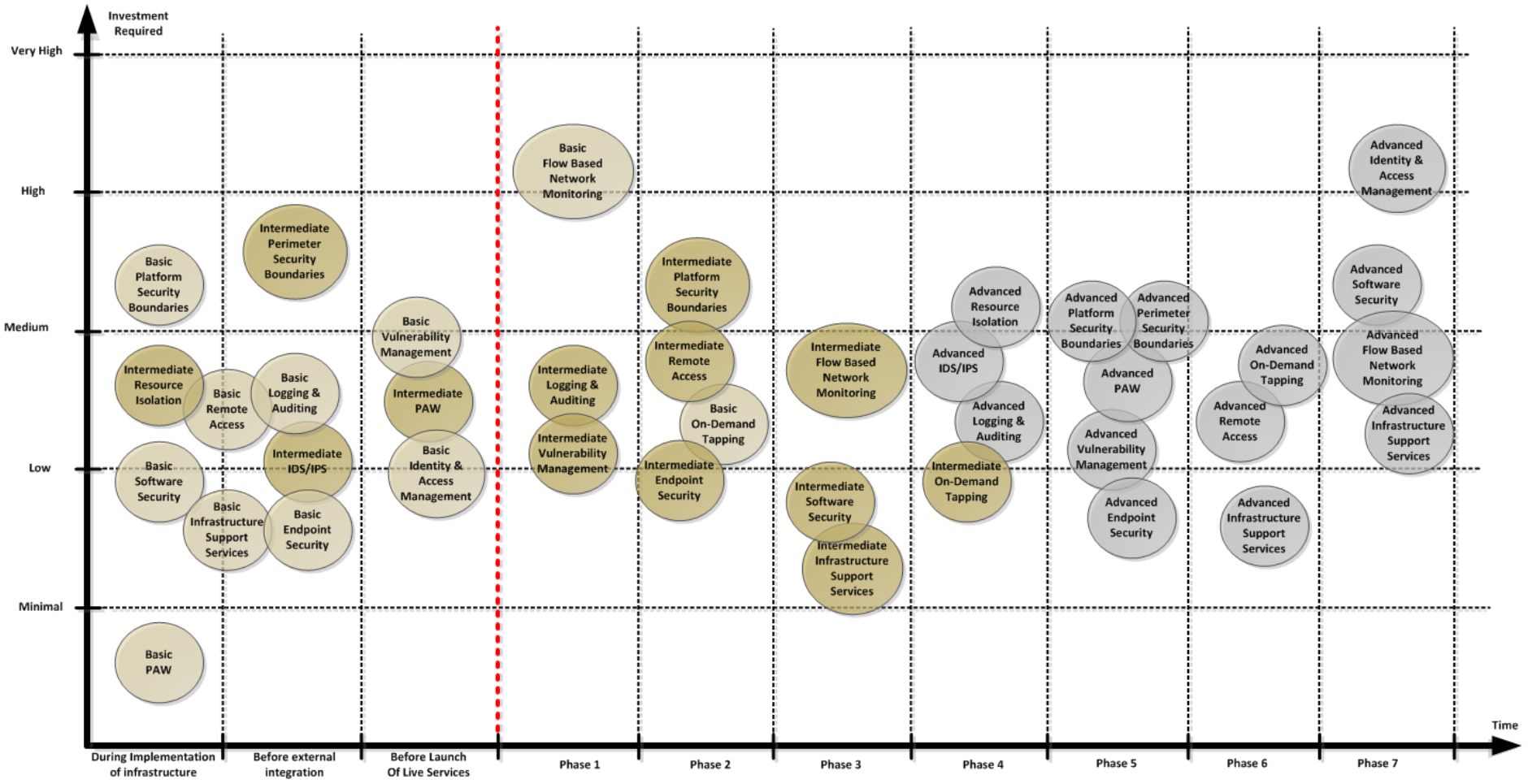


Figure 56. Sample Capability Implementation Plan

7 Defending the Architecture through Security Operations

Security operations is further detailed in document DA-2020-013 but high-level insight into the overall maturity of a security operations center is detailed here to show the different technology capabilities, process maturity and people competencies that are required to meet the different security posture maturity levels.

While implementing the technology-based security controls in the form of the defensive capabilities, these controls have little value if they are not operated and maintained by competent people who have clearly defined processes for both operations, change management, detection and incident response.

Security operation is also an area where the competence of individuals makes a significant impact to the expected outcome of the security operations function. The SOC should therefore in addition to clearly defined roles and responsibilities have formal description of required and desired competence and competence development plan for each role.

7.1 Defender incident response abilities.

Similar to the different tiers of threat actors along with their offensive capabilities that was shown by the threat actor pyramid in **Figure 5**, a similar pyramid can be defined for the defenders along with required defensive capabilities present within the organization and give an overview of what actions the SOC is actually capable of performing.

Figure 57. SOC requirements for incident response

Security operations abilities are based on what the operations teams are capable of performing of actions for incident response and is referred to as "the incident response hierarchy of need" [48]. What actions the SOC is able to perform plays directly into the ability to mitigate the different levels of threat actors in an efficient way. These abilities are built up by the different defined defensive capabilities in the form of tools and technologies, supported by effective processes and operated by competent people. All 3 needs to progress for security operations teams to be able to develop better abilities as required in incident response.

[48] https://github.com/swannman/ircapabilities

For the reasons mentioned, it is recommended to measure and stage the introduction of capabilities and create a clear roadmap to move up in the hierarchy of defensive capabilities. From the figure above it is possible to see that without a proper asset inventory, monitoring and detection capabilities it will become very difficult to build any kind of advanced response abilities and go threat hunting for instance. Having a proper foundation to build on becomes important when wanting to address the higher tiers of threat actors since the implementation of advanced capabilities relies on those foundational capabilities.

One also needs to consider the sequencing of tools, processes and organization. It is highly recommended to focus on the organizational aspects and staffing first, as one can expect that competent people will be able to identify and implement capable tools and processes.

Dependencies and sequencing of capabilities is directly connected to the ability to mitigate threat actors and will influence the mitigation efficiency as shown in **Appendix 1** about defensive capabilities and measured against the SOC maturity shown in **Figure 58**. In any case, it will be necessary to adapt this to the existing capabilities and particulars of each individual organization unit to create a specific implementation plan.

7.2 SOC maturity levels

Similarly, to the capability levels of the defined security controls, the of typical capability steps of a Security Operations Centre are listed as a set of incremental steps. The defined levels follow the maturity levels which are used to measure company overall security maturity.

Level 0, Blind

At this level focus is on only on preventive measures. Responsibility for detecting and handling incidents is not defined, and resources are not present. Few if any of the defined capabilities for detection to perform security monitoring are implemented.

- Detection capabilities implemented for this maturity level
  - None, preventive only
- Detection capability process maturity
  - Initial
- Detection capability people maturity
  - Initial

Any organization being at this level would certainly fail of an of audit or the most basic of compliance checks and would not be considered serious to its customers (if any) and be in violation of most countries' privacy regulations in. Consider this level for reference only, it's not possible to get any worse.

Level 1: Performed

At this level security is performed on an ad-hoc basis. The ability to protect company assets is considered to be limited.

- High level policies in place
- Key Processes (Patch, Vulnerability, Credentials) Performed Ad-Hoc
- Some detection capabilities are implemented

Security operation is mandated in the company as a function but is considered a non-important capability that receives minimal effort. Central security monitoring is in place, but only collecting logs from a small subset of assets and is not being regularly maintained. Incidents are discovered only through pre-set rules and indicators on an ad-hoc basis, and no formal process exists for incident handling.

- Detection capabilities implemented for this maturity level
  - vulnerability scanning: minimal
  - endpoint detection & response: minimal
  - logging and auditing: minimal
  - IDS/IPS sensors: minimal
- Detection capability process maturity
  - developing
- Detection capability people maturity
  - developing

Level 2: Planned

At this level, security is performed and is based on structured plans. The ability to discover basic incidents and lower tier threat actors is present.

- Security capabilities include certain security specialists
- Minimum security requirements implemented in processes in IT infrastructure (e.g. Patch, Credentials)
- Most detection capabilities are implemented at basic level and Basic Monitoring is in place.
- Reactive response is conducted

Security operation is compliance-focused only. No security operations charter and champions exist. There are no existing continuous improvement activities, and capacity and competence is at a required minimum. Logging is expanded to cover critical assets, and some additional monitoring tools are introduced. Forensics are not performed; re-imaging is the main cause of action. Incident response process exists on paper but is not followed consistently.

- Detection capabilities implemented for this maturity level:
  - vulnerability scanning: basic
  - endpoint detection & response: basic
  - flow based network monitoring: none
  - logging and auditing: basic
  - IDS/IPS sensors: basic
- Detection capability process maturity
  - defined
- Detection capability people maturity
  - defined

Level 3: Managed

Security systematically managed. Ability to protect against regular incidents.

- Security Risks are identified and managed. Security management system implemented
- Preventive defensive capabilities ensuring resilient technical security infrastructure
- All detection capabilities at basic or intermediate level are implemented
- Advanced Security Monitoring established. Can identify advanced threats
- Security operation is considered as important for the business.

Multiple tools in the form of detection capabilities with regularly updated threat intelligence feeds are introduced, and asset coverage if these capabilities is approaching 100%. Incident handling follows a

structured and measured process. Clear responsibilities are defined and anchored, and there is a dedicated department and individuals with competence and capability to handle security monitoring and incident response 24/7. Basic forensic analysis is performed on selected incidents. Threat hunting is done on an ad-hoc basis. Performance is measured. At this level a company is able to handle most incidents up to tier 4 threat actors, excluding APTs. (Tier 5 and above)

- Detection capabilities implemented for this maturity level:
  - vulnerability scanning: standard
  - endpoint detection & response: standard
  - flow based network monitoring: basic
  - logging and auditing: standard
  - IDS/IPS sensors: standard
- Detection capability process maturity
  - managed
- Detection capability people maturity
  - managed

Level 4: Measured & controlled

Security capabilities are measured. Company has the ability to protect and mitigate advanced threats

- Security organization with specialist functions.
- Infrastructure segmented and controlled
- Key processes measured, and controlled through KPIs and metrics

Security operation is delivering clear value to the business by effectively detecting and handling incidents before they can harm the business. A comprehensive and integrated toolset is used, managed by security engineering. Threat hunting finds incidents on a regular basis. Advanced forensic capabilities exist and are in regular use. A structured process exists to improve preventive measures from incident learnings. Threat intelligence provides valuable input to detection capabilities. Able to handle APT incidents.

- Detection capabilities implemented for this maturity level:
  - vulnerability scanning: advanced
  - endpoint detection & response: advanced
  - flow based network monitoring: advanced
  - logging and auditing: advanced
  - IDS/IPS sensors: advanced
- Detection capability process maturity
  - measured
- Detection capability people maturity
  - measured

Level 5: Tailored

Security subject to continuous improvement. Effectively protect and mitigate advanced threats

- Security fully integrated in all parts of the organization
- All infrastructure built with preventive capabilities implemented from start, with automated security supported by artificial intelligence and machine learning

The organization considers security to be a fundamental capability with high criticality for the organization and takes lead among peers in the area. Security operation has a high degree of automation, and continuous improvement processes are working well. Able to detect and evict most threat actors, including APTs, before they gain a foothold supported by IT architecture design.

- Detection capabilities implemented for this maturity level:
  - vulnerability scanning: intelligent
  - endpoint detection & response: intelligent
  - flow based network monitoring: intelligent
  - logging and auditing: intelligent
  - IDS/IPS sensors: intelligent
- Detection capability process maturity
  - optimized
- Detection capability people maturity
  - optimized

The sweet spot for at mature SOC is considered to be at either high 3 or a low 4, which should be both an acceptable and achievable target for a serious company. The approximately average seen across different sectors and verticals is assumed to be around 2.75 based on input from consultancies helping companies to mature their SOCs, which is quite low. On the other hand, some sectors being constantly on the front lines facing threats and under regulatory risk such as the finance sector is on average being more mature, being around 3.5. The more security conscious industry sectors like the defense industry or military organization being even higher than that having the security mindset fully integrated into all aspects of their organization.

To get started it is suggested that the first step is to perform a gap analysis of the recommendations in this document and make a phased improvement plan. It is recommended to set a specific target for improving maturity scores over a 1- 3 year time frame with concrete mile stones and deliveries, similar to the staged implementation of the capabilities as outlined in section **6.1**. With the assumption of starting at level 0 or 1, it is expected that that to achieve level 3 or above in SOC maturity, there is definitely no silver bullet, quick fix or free lunch. It is expected to take a significant amount of time, money and focused effort.

7.2.1 Security Operations Threat mitigation efficiency

Similarly, to the defensive capabilities, the maturity of the security operations center, the tools, processes and the number of competent resources available play directly into the ability to mitigate the different levels of threats.

*For a provider of services falling under regulatory constraints or defined as a national **critical information infrastructure** (CII) company, the recommendation is to mitigate an **absolute minimum of tier 4** threat actor level, with the best practice being tier 5 or above.*

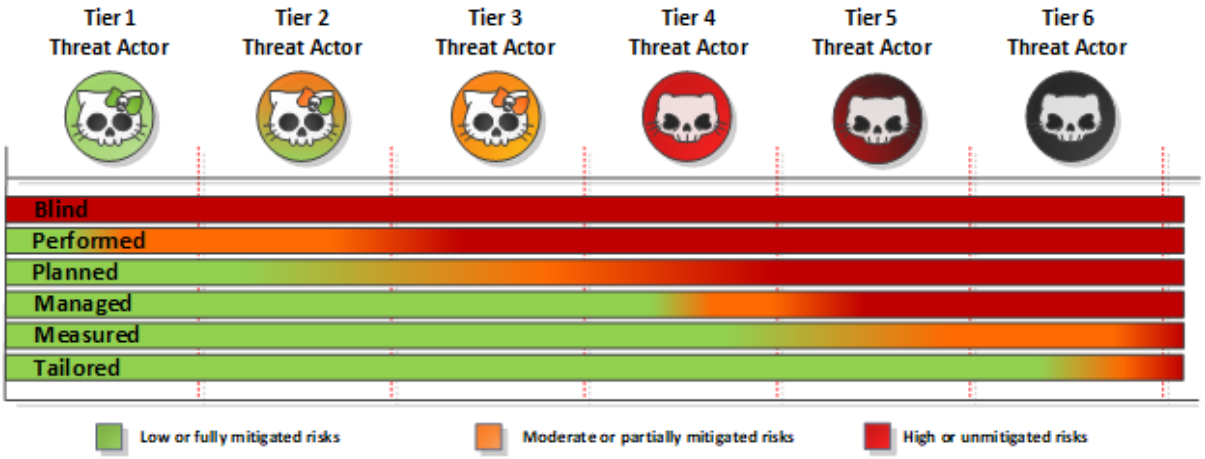


Figure 58. SOC threat actor mitigation efficiency

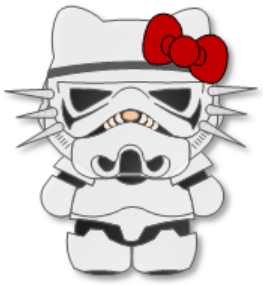
Building on the implemented defensive capabilities and tools the SOC will be able to detect more and competent threat actors. While the purpose of the implemented preventive security controls is to prevent threat actors from breaching the infrastructure, the main purpose is to be able to detect any threats that actually do. With thousands of components in the average infrastructure, this is inevitable to happen sooner or later and when it does, it is required to have all tools and capabilities, tools, processes and competencies in place to support an effective incident response process to evict them before any serious damage is caused to the enterprise.

7.3 Who is who on the defensive team?

Within an organization there are multiple teams with various roles that needs to interact with each other, and all pull in the same direction for an organization's security posture and incident response capability is to be at sufficient levels. Depending on the size of the organization multiple of these functions may be on the same teams, or there may be multiple teams of highly competent specialists. Security is all about teamwork and it is not all of the roles that perform security related functions which are directly attached to the security unit either. Specialists may be working in the technology domain or be in governance functions outside the environment of operational security but still play a crucial role in maintaining key security related functions.

The security organization itself can also often perform other roles relating to security in addition to the ones that are described in this section; roles and functions are influenced by the context in which the SOC operates inside the organization and what purpose it is created to serve.

7.3.1 Operations and Maintenance



OAM, the "regular" operations and maintenance teams also have an important role to play in an organization from a security perspective. These are the engineers who are network specialists, virtualization experts or application operators who can provide great and detailed insight into the underlying infrastructure based on their daily tasks. OAM personnel is in charge of all change and release into the infrastructure and is thus the source of all the information going into the asset inventory which is crucial for the security operations center and information security architects when defining the baseline of authorized assets.

Operations are also the engineering experts that sits with the detailed knowledge about the applications so that they can be decomposed when performing risk analysis and determining where the vulnerable spots in the various information systems are located.

Depending on the organizational layout OAM teams may also be directly responsible for operating some of the defensive controls as shown in Error! Reference source not found.. In particularly the preventive c ontrols, which are an integral part of the infrastructure such as regular anti-virus, the firewalls, network tapping function or maintaining the log servers that the SOC teams use for their analysis work.

OAM teams are also on the receiving end of the SOC's vulnerability scans and have the important job of upgrading all the software components that make up the infrastructure and keep the number of vulnerabilities as low as possible.

Roles may include Network specialist, Virtualization Specialist, Windows/Linux Administrators, Storage Specialist, Application Operators, Database Administrators, Active Directory Guru

7.3.2 Security Operations

The security operations teams are the eyes and ears of the organization in the security space. The main function of the SOC team is to protect the infrastructure and the confidentiality, integrity and the availability of the data either stored, processed or transported through it. In achieving this target is the role of the SOC needs to be considered in more detail, then the number of people and their competency and any specializations if applicable in the SOC and finally the process and procedures that are needed for a SOC to function properly. The exact roles and responsibilities will be determined by two factors, the overall security maturity of the organization as highlighted earlier as well as the size of the organization itself.

Monitoring can be considered to be the core responsibilities of the SOC, although it is often now subsumed into security information and event management. Here, the SOC is responsible for monitoring any security aspect of the IT system. There can be a large degree of overlap here with other parts of the organization, as it will obviously interface with physical security which is commonly looked after by a different part of the organization. There may be overlap with other parts of the OAM team, especially when it comes to issues of availability, which can be the responsibility of both the SOC team and the operations team.

At the heart of the detection capabilities ecosystems, you can find one of the main tools of the SOC team which is the Security Information and Event Management (SIEM) system. This system collects information from all the components in the infrastructure and utilizes it for the management and analysis of security-related data. This data can be collected from event related information through active or passive detection capabilities but also includes other security information such as external threat intelligence feeds and other similar information.

Vulnerability management is typically also a function that can be done by the security operations team, and then any discovered vulnerabilities is reported and submitted to the OAM teams to fix. Some organizations have the OAM team do both the scanning and patching, but having the same team being responsible for and being measured for both discovering and keeping the organization's threat level as low as possible by closing the discovered vulnerabilities may lead to some undesired behavior due to the potential conflict of interest between defined KPI's. Having this function assigned to the security operations teams will also make them aware of the potential ongoing threats through vulnerabilities and can enhance the value of gathered threat intelligence by being able to correlate the information much faster to known threats.

The SOC engineers are responsible for operating the detection capabilities themselves. While some of these (anti-virus, firewall etc) may be under the control of the OAM team the main detection controls such as the SIEM, Flow Based Analytics or the more advanced endpoint detection and response agents are managed directly by a dedicated team of engineers which are specialized in the use of those tools.

Any development of own internal capabilities, whether it is software or tools such as the advanced IDS sensors is done by the engineering function of the SOC.

A more advanced SOC team with competent specialists are also capable of going on the offensive in regard to monitoring and not rely passively on the detection capabilities. This more offensive approach is called threat hunting and refers to the process of proactively and repeatedly searching through the infrastructure to detect, isolate and evict higher tiers of threat actors in the form of advanced persistent threats that are capable evade existing security solutions. SOC team members involved in threat hunting are usually among the most skilled members of the team and may have double roles as being part of the CSIRT but performing threat hunting when not being involved in an incident response.

Threat intelligence gathering is also a common role that are part of larger and more mature SOC. Threat intelligence is used to help understand the nature of the potential threats to the organization. In order to do this, information needs to be collected.

Collecting threat intelligence data can be done in multiple ways and come from different sources:

- Social media
- Flash memos from other CERTs, either national or international
- Updates from vendors
- Security monitoring of organization's own infrastructure
- National cyber security authorities, defense, police

The collected intelligence data is used to assist in setting the direction that the security operations team needs to develop itself in the form of skills and competencies. This development may include potential tools that needs to be created, modified or updated to capture new threats by the engineers that are tasked with maintaining the SOC's tool stack.

SOC Managers, SOC Engineers, SOC Analyst, Vulnerability Experts

7.3.3 Cyber Security Incident Response Team

To respond to security incident response in a timely fashion is the main job of the CSIRT. Incident response involves detecting and responding to security incidents in a timely fashion and can either be responsive after being alerted by the SOC team of a possible breach, or pro-active through threat hunting by analyzing collected telemetry data from the various detection capabilities. The CSIRT team is often more specialized in certain field than the regular Security Operations teams and its permanent member are forensics experts that can conduct detailed forensics of assumed compromised assets. These forensic activities collect information during an incident to secure indicators of compromise for both dealing with the incident itself as well as securing evidence for any legal response following it. The CSIRT may also have virtual assignments from the OAM and/or SOC teams to gather specialists in certain relevant areas related to the incident or on a permanent basis.

It is of key importance that the CSIRT team have a dedicated manager and that the function operates with a solid mandate from the executive management with the ability to requisition resources, collect information for any relevant source and have the authority to temporarily suspend any activity.

Roles may include: CSIRT manager, forensic experts, incident analysts

7.3.4 Security Architecture

Best practice approaches encourage governance to be embedded at all levels and not only at C-level to allow specialist parts of the organization to handle appropriate parts of the governance process. For security governance, it is therefore logical for the security architects within the security organization to advise or take a lead in aspects of security governance. The security architecture functions does not necessarily have to be organized under the SOC and is often found attached to other similar architecture and governance functions in the technology division as security specialists within that domain.

The security architecture unit may take on responsibility for information risk management and for quantifying the amount of security risk the organization is exposed to, as well as defining and designing the capabilities and controls to manage the risks and measuring their effectiveness together with the SOC and OAM teams based on telemetry from monitoring and incident handling and response

Within the governance team also lies the function of compliance. After having identified the risk and defined the controls that are needed, it is needed to make sure that the controls are implemented and that they are effective as highlighted in section **3.10**.

Information security compliance is addressing the required compliance with both external regulation as well as any internal policies. The external regulation is often legal (such as GDPR, National cybercrime laws), but may also be sector standards such as the Payment Card Industry Data Security Standard (PCI DSS) which is the standard for all companies handling payment using credit card information. Compliance can in this context be regarded as the superset of information security as it covers any risk to availability, not just security risks.

Roles may include Security Architects, Information Security experts, risk managers, compliance analysts.

8 Definitions, Abbreviations and Legend

8.1 Definitions

This document adheres to requirement definitions as described in RFC 2119:

Term	Synonym(s)	Meaning
MUST	**REQUIRED, SHALL**	The definition is an absolute requirement of the specification.
MUST NOT	**SHALL NOT**	The definition is an absolute prohibition of the specification.
SHOULD	**RECOMMENDED**	There may be valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood, documented and carefully weighed before choosing a different course.
SHOULD NOT	**NOT RECOMMENDED**	There may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood, documented and the case carefully weighed before implementing any behavior described with this label.
MAY / OPTIONAL	**OPTIONAL**	An item is truly optional.

Table 9. Definitions

8.2 Abbreviations

Abbreviation	Full Term
CSIRT	Computer Security Incident Response Team
DA	Disaster Avoidance
DDOS	Distributed Denial of Service
DMZ	Demilitarized Zone
DNS	Domain Name System
DR	Disaster Recovery
HVD	Hosted Virtual Desktops
IAM	Identity Access Management
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
NFV	Network Functions Virtualization
NFVi	Network Functions Virtualization Infrastructure
NOC	Network Operations Center
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SIEM	Security Incident Event Management
SIP	Session Initiation Protocol
SLA	Service Level Agreement

SNMP	Simple Network Management Protocol
SOC	Security Operations Center
TLS	Transport Layer Security
URL	Universal Resource Locator
VDI	Virtual Desktop Infrastructure
VLAN	Virtual Local Area Network
VMS	Vulnerability Management System
VRF	Virtual Routing and Forwarding
WTS	Windows Terminal Server

Table 10. Definitions

8.3 Legend

Table 11. Legend

9 List of references

[1] Scott C. Fitch and Michael Muckin /Lockheed Martin, Defendable Architecture

[2] Scott C. Fitch and Michael Muckin /Lockheed Martin, A threat driven approach to Cyber Security

[3] Tony UcedaVélez & Marco M Morana Risk Centric Threat modelling with PASTA

[4] Marco Morana,OWASP Architectural Patterns in financial Web Applications

[5] Bruce Schneier, Attack Trees

[6] Shemlse Gebremedhin Kassa, IT asset evaluation, Risk assessment and control implementation model, IASCA Journal

[7] Mitre Atta&k Framework

[8] Randy Franklin Smith, Brian Coulson & Dan Kaiser, understanding Mitre Atta&k whitepaper

[9] Kevin Townsend, Using infection monkey with Mitre Atta&k framework

[10] Center for internet Security, 20 main CIS security controls

[11] John Kindervag/Palo Alto, Zero Trust Architecture

[12] Lillian Ablon, The motivations of cyber threat actors and their use and monetization of stolen data

[13] Recorded Future, Understanding threat actor types,

[14] ThaiCERT Threat Actor Encyclopedia

[15] Finjan Cyber Security Blog, Qualitative vs Quantitative risk assessment

[16] Trend Micro, Indicator of Compromise definition

[17] Jerome H. Saltzer & Michael D. Schroeder: The Protection of Information in Computer Systems

[18] European Union Agency for Network and Information Security (ENISA): ENISA Threat landscape 2014

[19] Workshop Report on Security Architecture by the Information Security Forum

[20] Common Weakness Enumeration (CWE)

[21] Open Web Application Security Project (OWASP)

[22] The CIS Security Metrics

[23] Microsoft PAW

[24] Katie Nickels, Mitre Atta&k, Getting started with Atta&k using threat intelligence

[25]

10 List of directional statements

In this section all the key objectives of this document are summarized in the form of principle statements and observations.

10.1 Summarized Security Principles

Security Principle 002-1: *Security control design shall address relevant regulatory requirements and mandatory industry frameworks that apply for the industry that the organization operates in*

Security Principle 002-2: *Security control design shall use threat modelling as part of the design process*

Security Principle 002-3: *Threat modelling shall be precisely scoped to the asset(s) it is meant to protect*

Security Principle 002-4: *All the assets internally or externally which are being used by the organization shall be identified and added to the asset inventory database (cloud services and the like also apply here)*

Security Principle 002-5: *All technologies, both SW and HW, that are used by each individual asset shall be identified, documented and added to the asset inventory database*

Security Principle 002-6: *Each asset shall have a dedicated system owner that can be identified*

Security Principle 002-7: *Documentation shall be created and maintained for all assets mapping out interfacing applications and protocols*

Security Principle 002-8: *All access to individual asset shall be documented and be traceable*

Security Principle 002-9: *information the asset is either processing, storing, transporting or otherwise is in contact with shall be identified and documented*

Security Principle 002-10: *Each asset's business criticality and its estimated value shall be documented*

Security Principle 002-11: *Possible attack vectors and known vulnerabilities for each assets shall be documented*

Security Principle 002-12: *Threat intelligence shall be gathered both internally and externally at regular intervals to assess threat landscape and design effective security controls*

Security Principle 002-13: *Attack trees should be created for assets as part of the security control design process*

Security Principle 002-14: *All security controls shall through the design process, apply risk analysis to measure the business impact it is meant to mitigate*

Security Principle 002-15: *For the security architecture to remain business driven, the cost of implementing a security control should not significantly exceed the estimated business impact of the risk it is meant to mitigate*

Security Principle 002-16: *Clear tolerance levels for acceptable risk should be defined*

Security Principle 002-17: *Risk tolerance levels should be anchored with senior management and/or the board of the organization*

Security Principle 002-18: *Security control effectiveness shall be measured at regular intervals and no less than on a yearly basis*

Security Principle 002-19: *Security control effectiveness shall always be measured after a successful breach is conducted*

Security Principle 002-20: *Clearly define the threat actor levels that are required to be mitigated to build the most efficient security controls to reach the targeted security posture*

Security Principle 002-21: *All infrastructure shall have its security controls regularly audited for implementation quality, no less than 1 time per year*

Security Principle 002-22: *All infrastructure shall have its security controls regularly audited for process maturity, no less than 1 time per year*

Security Principle 002-23: *All infrastructure shall have its security controls regularly audited for competency quality, no less than 1 time per year*

Security Principle 002-24: *Core architectural security principles are mandatory to follow*

Security Principle 002-25: *Capabilities are either mandatory or optional to implement, it is decided by the Business Security Officer in accordance with the specific risk picture, threat actor mitigation ambitions and any regulatory requirements if applicable.*

Security Principle 002-26: *Deviations to mandatory requirements shall be handled in accordance with the risk-based deviation process and be signed off by the relevant risk owners and added to the local risk register.*

Security Principle 002-27: *Do not start the deviation process unless satisfactory answers can be given.*

10.2 Summarized Observations

Observation 002-1: *Protecting the most critical assets by selecting the right security controls and providing guidance to implementing them in the correct way to mitigate unacceptable or unavoidable levels of risk is the core principle of a business driven security architecture.*

Observation 002-2: *From a defensive point of view, the objective of an attack tree is to identify possible attacks and implement defensive controls to increase the costs/risk to make them either unsustainable to achieve or to reduce the probability of them occurring.*

Observation 002-3: *The defendable architecture implementation levels can be used to create an overview of the implemented capabilities in the organization, so if investment doesn't allow for more than basic or minimal levels in certain capability areas, then the definitions can be used to document this so that relevant risks can be documented and addressed as per the organizations risk strategy.*

Observation 002-4: *While DA Objectives are valid across all environments on-prem design examples and artefacts are not always directly transferrable to public cloud environments. The modularity in the form of the implementation levels are also applicable to public cloud to balance cost vs risk and regulatory requirements and is of particularity importance as public cloud resources are billed on usage in an opex model.*

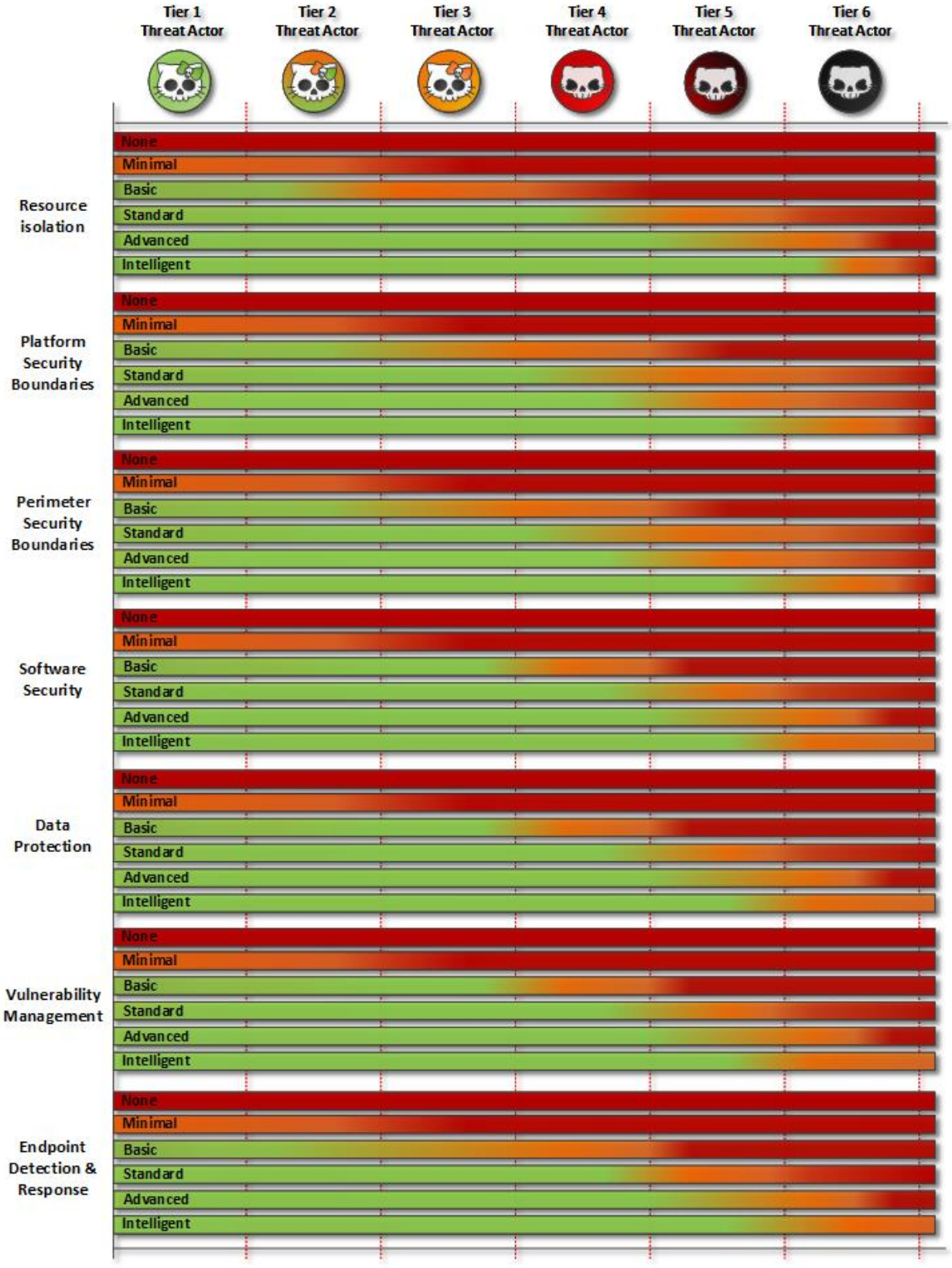
Observation 002-5: *ICT deployed to public cloud require the same control areas as on-prem to be considered defendable but public cloud security controls require different building blocks and design artifacts to achieve the same objectives*

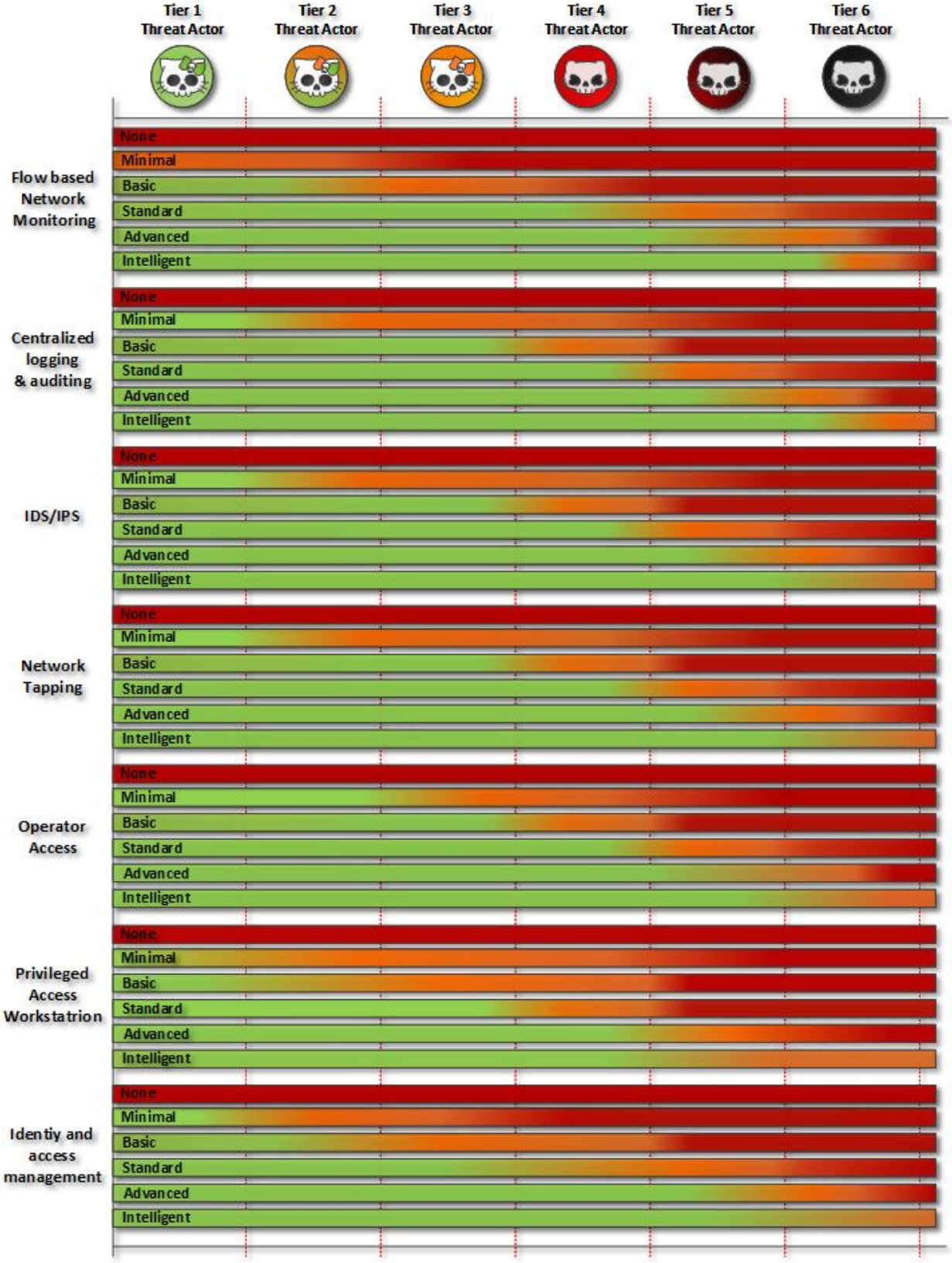
11 Document history

Document version	Version description	Version Responsible	Date
0.1	Inception	Erik Kvarvåg	10.12.2019
0.5	First Draft	Erik Kvarvåg	16.12.2019
0.5	First, limited peer review	Erik Kvarvåg	20.12.2019
0.8	Second draft	Erik Kvarvåg	28.12.2019
0.9	Second, extended review	Erik Kvarvåg	08.01.2020
1.0	Final version	Erik Kvarvåg	20.01.2020
1.01	Minor updates on preventive capabilities	Erik Kvarvåg	21.01.2020
1.1	Detailing of 14 Security Capabilities	Erik Kvarvåg	17.02.2020
1.2	Security Operations Maturity	Erik Kvarvåg	27.02.2020
1.3	Executive Summary	Erik Kvarvåg	14.04.2020
1.4	Full risk assessment process documented	Erik Kvarvåg	08.05.2020
1.5	New base template, Minor content updates	Erik Kvarvåg	01.06.2020
1.51	Added security principle statements	Erik Kvarvåg	07.07.2020
1.52	Added definitions	Erik Kvarvåg	21.07.2020
1.6	Revised implementation levels and capabilities	Erik Kvarvåg	07.11.2021
1.61	Public cloud considerations added	Erik Kvarvåg	23.11.2021
1.62	Revised zone class drawings	Erik Kvarvåg	07.01.2022
1.63	Security Management class added to intelligent level	Erik Kvarvåg	27.01.2022
1.64	Minor updates and error corrections	Erik Kvarvåg	24.05.2022
1.65	Revise capabilities level definition for detection	Erik Kvarvåg	16.08.2022
1.66	Unified capability level definitions	Erik Kvarvåg	26.08.2022
1.67	Updated access capabilities	Erik Kvarvåg	30.08.2022
1.68	Revised introduction section	Erik Kvarvåg	01.09.2022
1.69	Evaluation appendix added	Erik Kvarvåg	03.10.2022
1.7	Clarification on Zero-Trust and NIST/CSF/ISO elements	Erik Kvarvåg	16.11.2022
1.71	Updated drawings not following ZTA principles	Erik Kvarvåg	18.04.2023
1.72	Automated risk management with integrated controls	Erik Kvarvåg	19.04.2023
1.73	Applied concept of policy domains to resource isolation	Erik Kvarvåg	30.05.2023
1.74	Applied licensing	Erik Kvarvåg	26.10.2023

Appendix 1.

Defensive capabilities threat mitigation



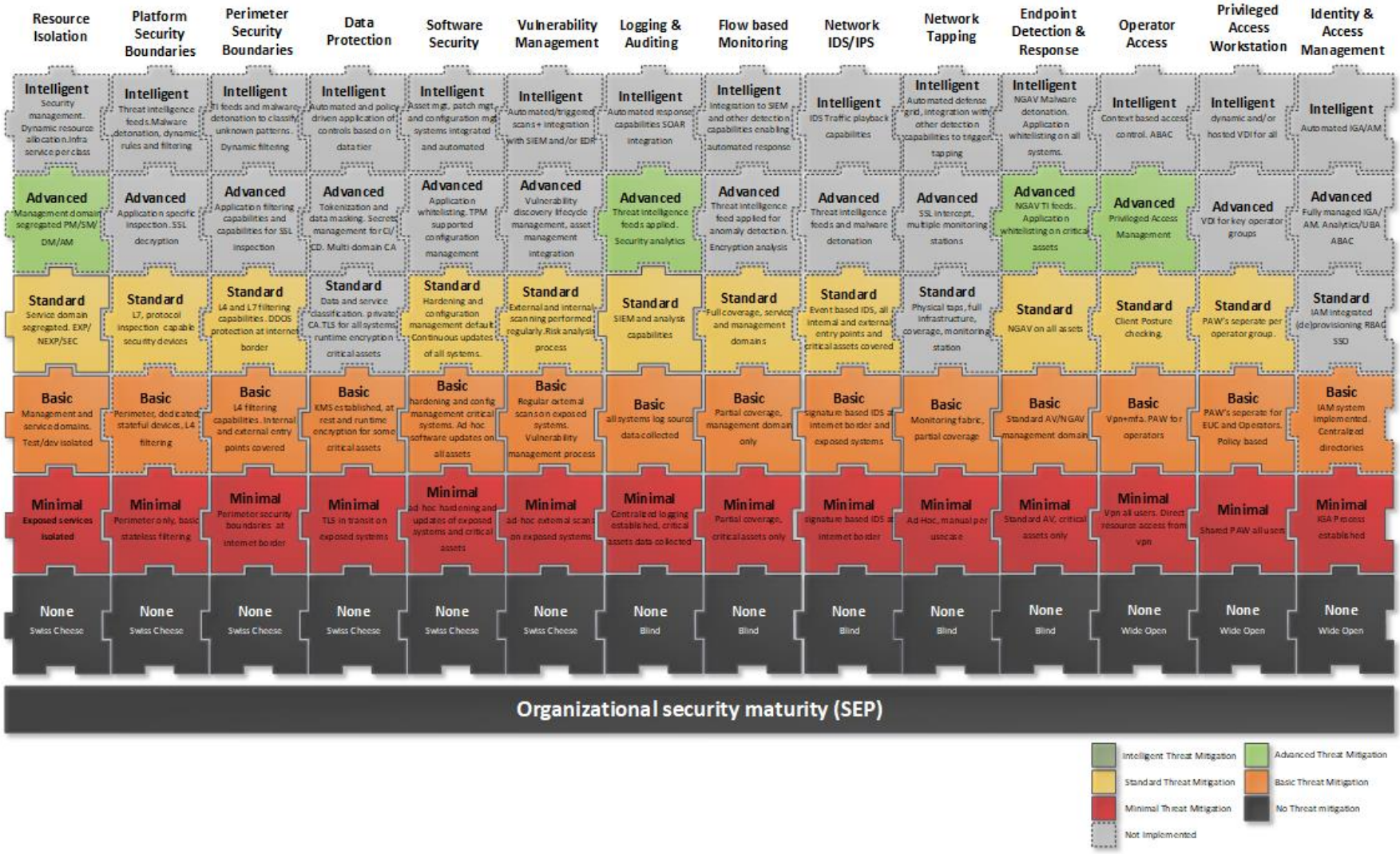

Tier 1 Threat Actor
Tier 2 Threat Actor
Tier 3 Threat Actor
Tier 4 Threat Actor
Tier 5 Threat Actor
Tier 6 Threat Actor
Flow based Network Monitoring
Centralized logging & auditing
IDS/IPS
Network Tapping
Operator Access
Privileged Access Workstatrion
Identiy and access management
None
Minimal
Basic
Standard
Advanced
Intelligent

Appendix 2.

The following table can be used for a simplified measurement of the technical security capabilities within an infrastructure platform or policy domain.

DA Capability	Implementation Level (minimal, basic, standard, advanced, intelligent)
Resource Isolation	
Platform Security Boundaries	
Perimeter Security Boundaries	
Software Security	
Data Protection	
Network Tapping	
Netflow based monitoring	
IDS/IPS	
Endpoint detection & response	
Logging & auditing	
Vulnerability Management	
Operator Access	
Privileged Access Workstation	
Identity & Access Management	

The figure below outlines a graphical representation of the table above


Resource Isolation
Platform Security Boundaries
Perimeter Security Boundaries
Data Protection
Software Security
Vulnerability Management
Logging & Auditing
Flow based Monitoring
Network IDS/IPS
Network Tapping
Endpoint Detection & Response
Operator Access
Privileged Access Workstation
Identity & Access Management
Intelligent
Advanced
Standard
Basic
Minimal
None
Organizational security maturity (SEP)
Intelligent Threat Mitigation
Advanced Threat Mitigation
Standard Threat Mitigation
Basic Threat Mitigation
Minimal Threat Mitigation
No Threat mitigation
Not implemented

Appendix 3. Next Steps

The defensive capabilities have been organized differently as opposed to earlier distributions of the defendable architecture framework. They are now organized into 3 main areas and a set of capabilities in total. Each volume of the defendable architecture documents highlights one more of the capabilities within each of the documents.

A3.1 Updates for next major version

Threat centric, situational awareness, mitre mapping