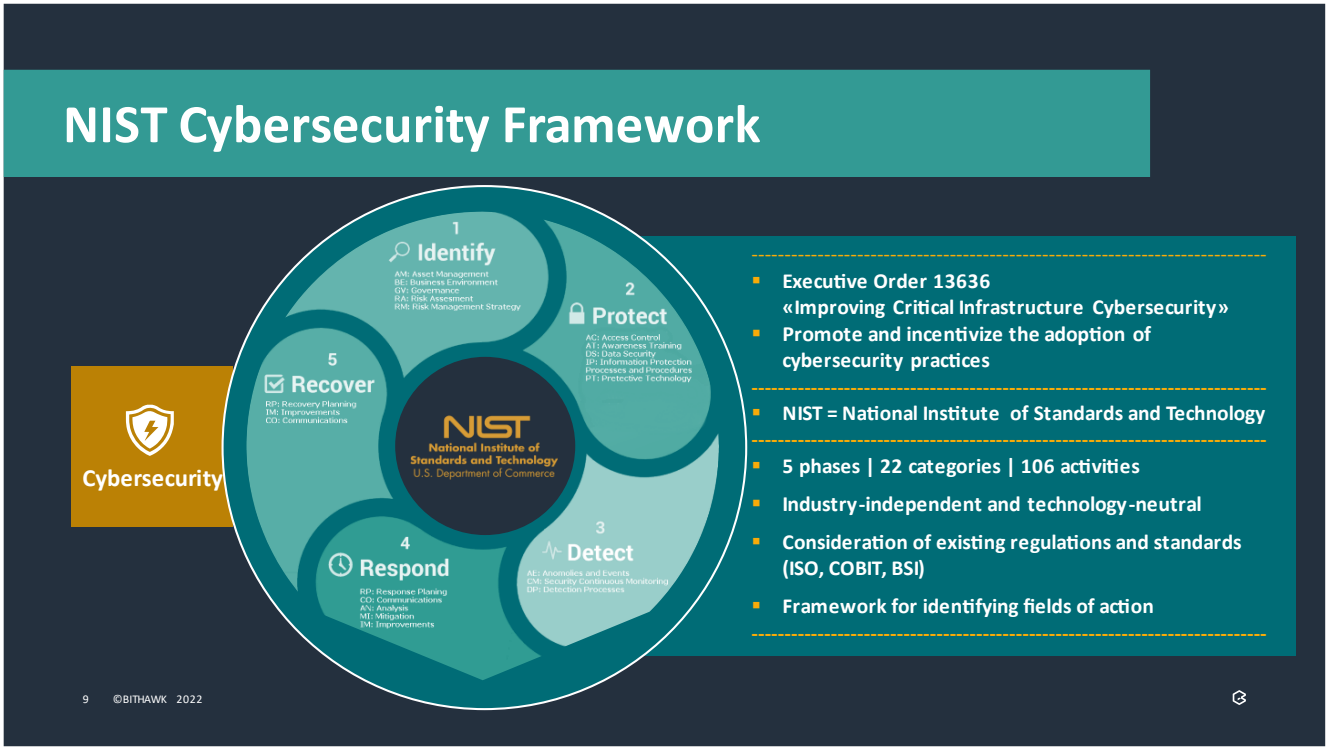
1 BitHawk Security Operation Center (SOC) Service

1.1 Starting Position

The current security situation and constantly increasing challenges regarding cybersecurity present companies with many challenges. These include organizational challenges on the one hand, but also technical challenges:

- Attacks are increasing and becoming more intelligent
- Vulnerability management is becoming more and more important
- Too few resources to run a SOC service
- No sensors or technology to detect attacks, abnormal behavior and vulnerabilities
- Too many events to respond quickly and professionally enough
- Lack of expertise to assess incidents
- Silo-based security solutions (not cross-cutting)
- Constantly adding new features to modern cloud solutions
- No logs when needed, as there are no tools that record and visualize incidents
- High operating costs of an own SOC and its tools

BitHawk works in the field of cybersecurity with the framework of NIST (National Institute of Standards and Technology). The framework describes with its activities the scope and best practices of cybersecurity in a company.
The SOC service is designed to support and relieve organizations, particularly in the following NIST activities:

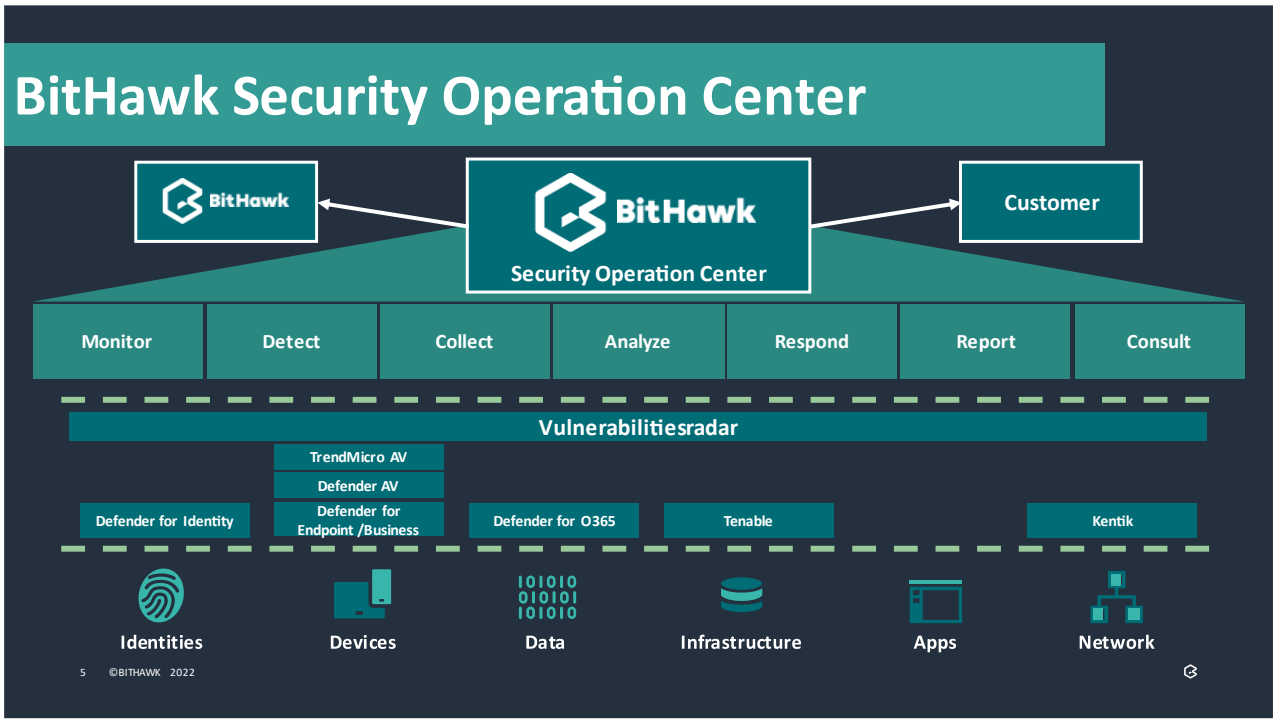


- DE.CM-3: Establish monitoring of employee cyber activities to detect potential cyber security incidents.
- DE.CM-7: Monitor your system on an ongoing basis to ensure that activities/accesses by unauthorized individuals, devices, and software are detected.
- DE.AE-2: Ensure that detected Cyber Security incidents are analyzed for their objectives and their methods.
- RS.AN-1: Ensure that notifications from detection systems are considered and follow-up investigations are triggered.
- RS.AN-2: Ensure that the impact of a cyber security incident can be correctly identified.

1.2 Service Design

The BitHawk SOC service operates on three levels.

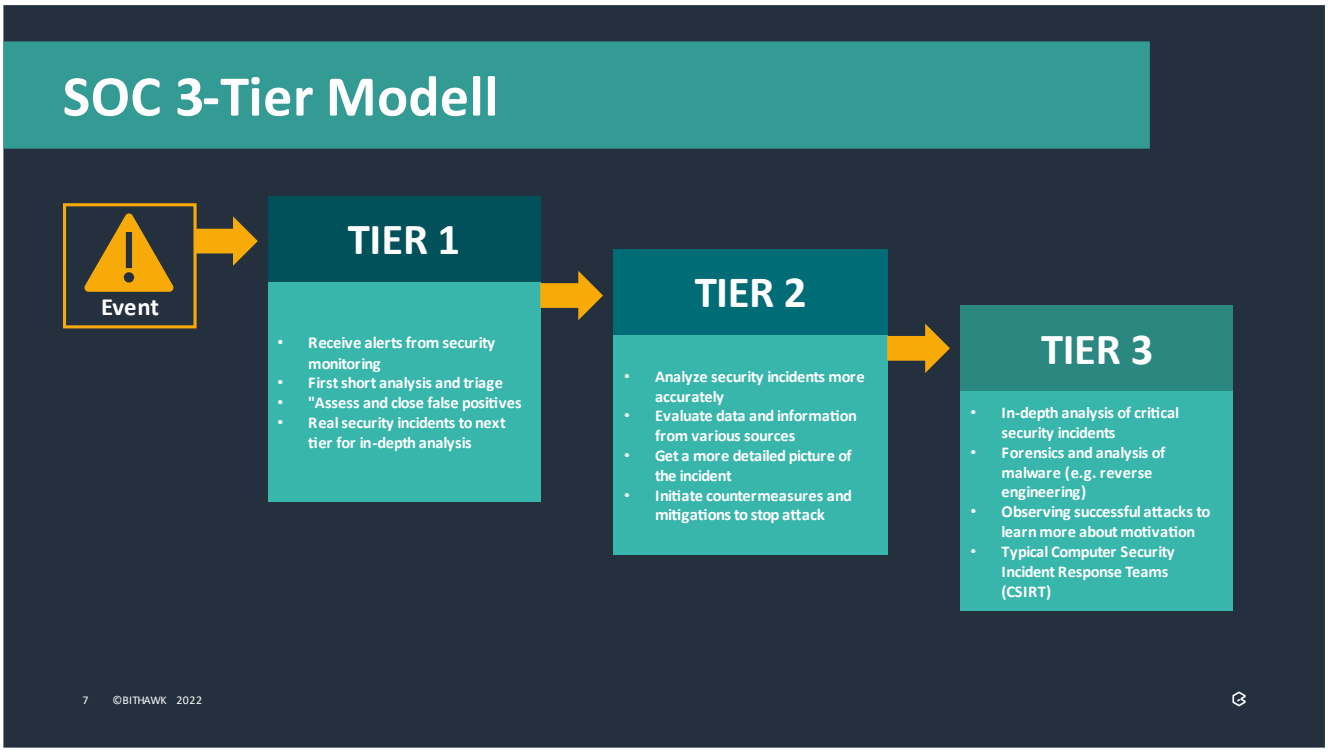
- Level 1: Areas to be monitored (Identities, Devices, Data, Infrastructure, Apps, Network)
- Level 2: Sensors (technical security solutions)
- Level 3: Organizational operation of the service with defined services



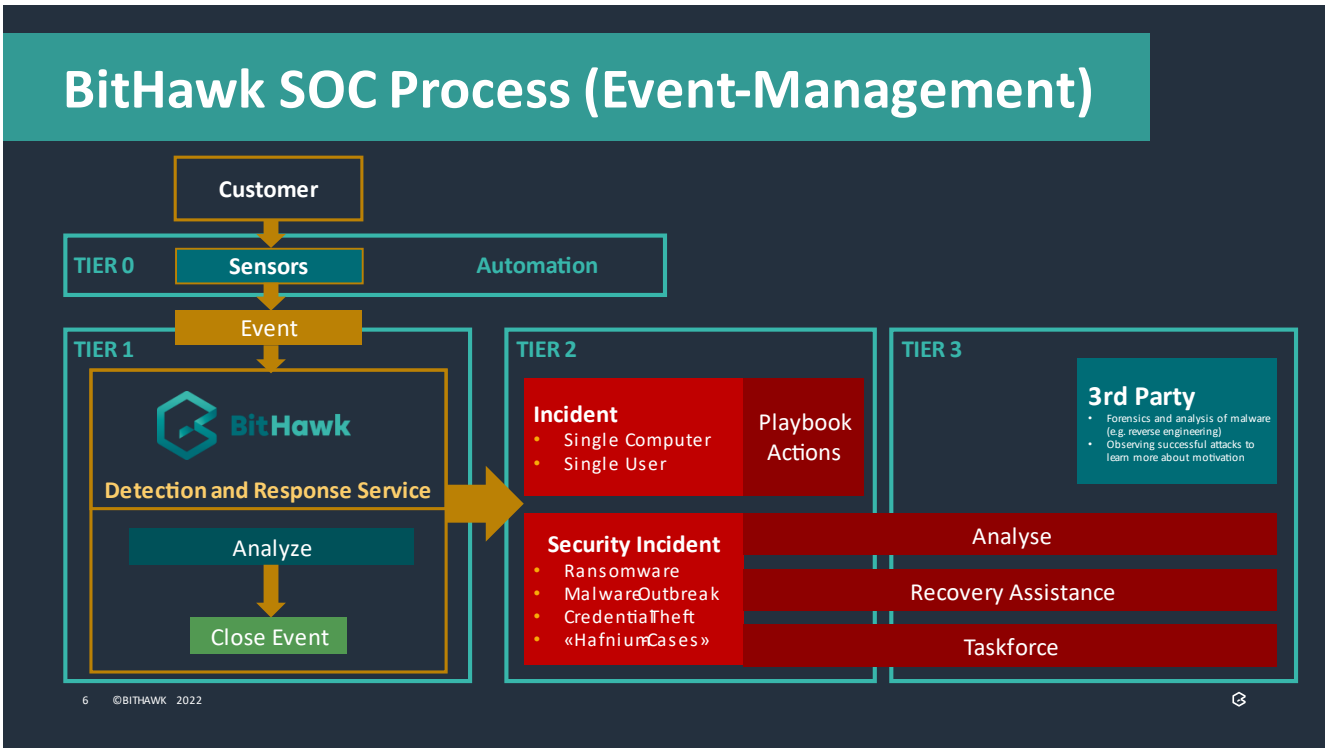
The service is structured in such a way that the definition of the detectable security incidents is based on the selected sensors. The customer thus decides for himself which sensors are to be used and monitored on his premises. All security-relevant incidents that a sensor can detect are then processed. Accordingly, all objects/areas that are equipped with a corresponding sensor are also in scope. Sensors can also be added at a later point in time.

The sensors are based on the modern IT security architecture with the Zero Trust Objectives. The sensors currently available are described in section 4.1.
In addition to the sensors, customers of the BitHawk SOC service benefit from the Vulnerability Radar. This alerts them to known vulnerabilities and provides recommendations on how to close them.

According to the definition for the Security Operation Center (SOC) process, an event from a sensor passes through three TIERs. The following areas of responsibility apply to the respective TIERs:



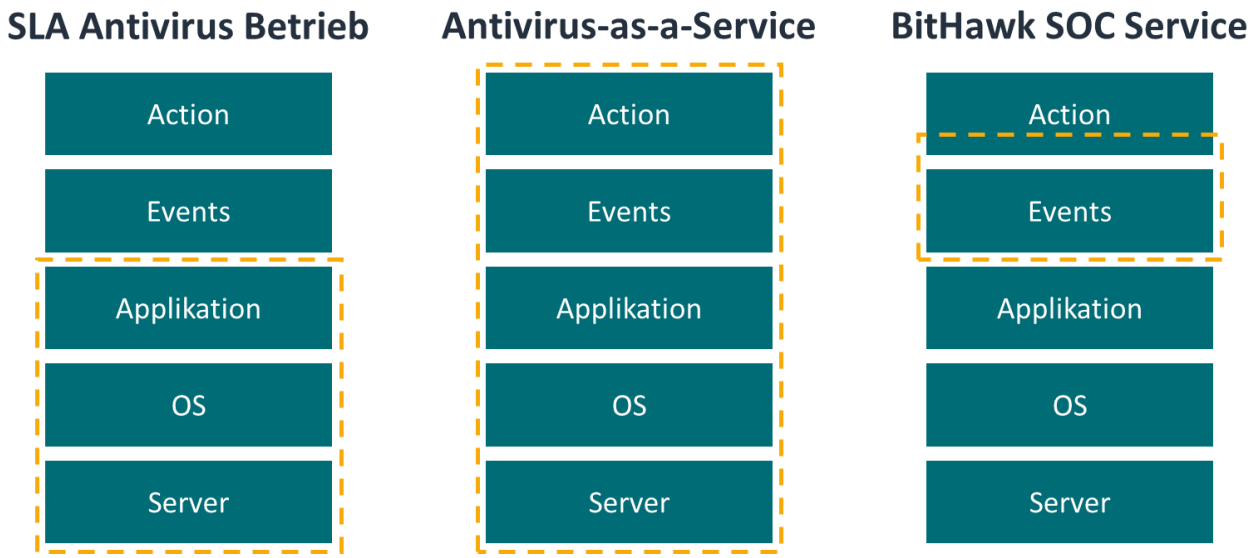
The BitHawk SOC service basically includes the services up to and including TIER 1. If necessary, a close exchange with the customer about further activities takes place. For further work, corresponding incidents or security incidents are created. This TIER 2 work is carried out in consultation with the customer and is charged according to the time and effort involved. In-depth forensics in TIER 3 is carried out with partners (if necessary, mediation by existing cybersecurity insurance).



The following services are provided in TIER 1 by the service as a lump sum for the selected sensors:

1.3 Shared Responsibility

Important to understand is the so-called shared responsibility, which can also be different between the sensors. Shared responsibility refers to the shared responsibilities for a service.
The responsibilities of a sensor can be outsourced to different parties. Often, the basic operation of a service and the event monitoring are assigned to separate organizations. Unless otherwise defined (e.g. an SLA is in place), the basic operation of the individual sensors is the responsibility of the customer. The BitHawk SOC service deliverables relate specifically to event handling and initial response. The graphic below illustrates the shared responsibility and different characteristics using the example of the "Antivirus" sensor:



1.4 Why BitHawk?

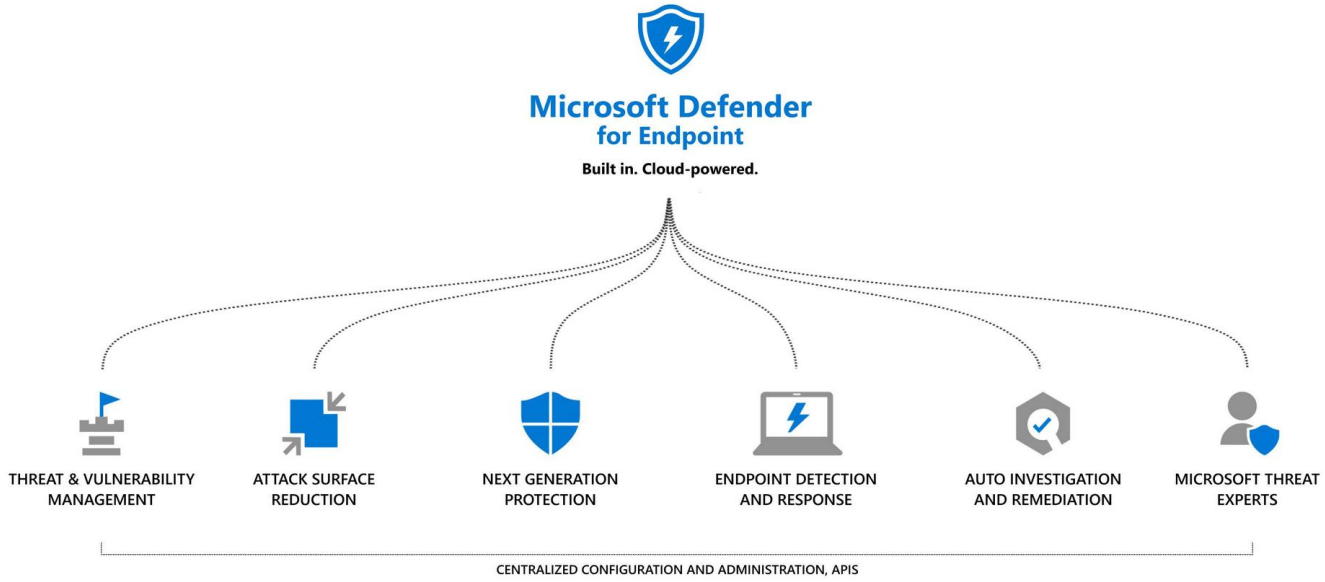
- Qualified and experienced security analysts
- Proactive monitoring and analysis using up-to-date threat data
- State-of-the-art security solutions from market leaders with AI, ML and automation
- Further development of sensors by specialists
- No local infrastructure required to operate the SOC service
- No additional maintenance costs
- Selective sensor choice (low entry costs)
- No in-house organization and know-how required
- Cybersecurity maturity level optimization
- SOC service suitable for SMEs
- Active vulnerability management with notification

2 SOC Sensoren

2.1 Product descriptions

2.1.1 Microsoft Defender for Endpoint (MDE)

Microsoft Defender for Endpoint (MDE) consists of six pillars, which are briefly explained below.



Threat & Vulnerability Management.
This integrated capability uses a revolutionary risk-based process to identify, prioritize and remediate endpoint vulnerabilities and misconfigurations.

Attack Surface Reduction.
Attack surface reduction capability is the first line of defense in the stack. By ensuring configuration settings are set correctly and applying exploit mitigation techniques, these capabilities resist attacks and exploits. These features also include network protection and web protection that restrict access to malicious IP addresses, domains, and URLs.

Next Generation Protection
To further enhance the security perimeter of the network, MDE uses next-generation protection mechanisms designed to intercept all types of threats.

Endpoint Detection and Response
Endpoint Detection and Response capabilities are designed to detect, investigate, and respond to advanced threats that may have overcome the first two layers of security. With Advanced Hunting, MDE provides a query-based threat hunting tool to proactively find breaches and create custom detection rules.

Auto Investigation and Remediation.
In addition to the ability to respond quickly to advanced attacks, MDE provides automatic investigation and remediation capabilities that help reduce the number of alerts. Auto Investigation and Remediation (AIR) uses algorithms and processes that are also used by security analysts. AIR examines alerts and takes immediate action to resolve violations. AIR's capabilities reduce the number of alerts, allowing security staff to focus on more challenging tasks.
AIR can be launched automatically (by triggering an alert and incident) or manually.

Microsoft Threat Experts
MDE's Threat Hunting services provide proactive search, prioritization, and additional context and insight that further enhance SOCs (Security Operations Center) ability to quickly and accurately identify and respond to threats (additional costs may apply).

2.1.2 **Microsoft Defender for Identity (MDI).**

Microsoft Defender for Identity (formerly Azure Advanced Threat Protection or Azure ATP) is a cloud-based security solution that leverages signals from the on-premises Active Directory instance to identify and detect complex threats, compromised identities, and malicious insider actions against the organization and assist in investigating these threats.
Microsoft Defender for Identity bietet beim Erkennen erweiterter Angriffe in Hybridumgebungen folgende Funktionen:

- Monitoring of users, entity behavior and activities with learning-based analysis.
- Protection of user identities and credentials stored in Active Directory
- Identify and investigate suspicious user activity and advanced attacks throughout the kill chain
- Provide unique information about an incident in a simple timeline for quick selection

Monitoring and profiling user behavior and activity.
Microsoft Defender for Identity monitors and analyzes user activity and information, such as permissions and group memberships, across networks, creating a behavioral baseline for each user. Microsoft Defender for Identity then identifies anomalies with built-in adaptive intelligence, giving you insight into suspicious activity and events. This gives you visibility into complex threats, vulnerable users, and insider threats to the organization. Microsoft Defender for Identity's proprietary sensors monitor the organization's domain controllers. This provides a comprehensive view of all user activity from any device.

Protect user identities and reduce the attack surface
Microsoft Defender for Identity provides valuable insight into identity configurations and provides recommended security best practices. Using Microsoft Defender for Identity, security reporting and user profile analysis can significantly reduce the organization's attack surface, which can also reduce the exposure of user credentials and the risk of an attack.
Microsoft Defender for Identity's visual lateral movement paths show how an attacker can move laterally within the organization to compromise sensitive accounts. The solution helps prevent these risks in advance. In addition, Microsoft Defender for Identity security reports can identify users and devices that authenticate with clear-text passwords. Additional insights enable you to improve your organization's security posture and policies.

Protecting ADFS in Hybrid Environments
ADFS (Active Directory federated services) plays an important role in modern infrastructure when it comes to authentication in hybrid environments. Microsoft Defender for Identity protects Active Directory federated services in the environment by locally detecting attacks on Active Directory federated services and providing visibility into authentication events generated by Active Directory federated services.
Identify suspicious activity and advanced attacks through the cyberattack kill chain.
Attacks are typically launched against any accessible entity, such as a user with minor privileges, and then quickly move laterally until the attacker gains access to valuable assets (e.g., sensitive accounts, domain administrators, and highly confidential data). Microsoft Defender for Identity detects these advanced threats from the ground up throughout the cyberattack kill chain.

Examine alerts and user activity
Microsoft Defender for Identity is designed to reduce the number of general alerts so that only rele-vant, important security alerts can be delivered in a clear time scale with attacks directed against the organization in real time. Microsoft Defender for Identity can be used to investigate threats without much effort and gain visibility across organizations for users, devices and network resources. Seamless integration with Microsoft Defender for Endpoint provides another advanced layer of security through additional detection and protection against advanced persistent threats to the operating system.

2.1.3 Microsoft Defender for Office 365 (MDO)

Microsoft Defender for Office 365 Plan 1 and Plan 2 are included in the Microsoft 365 E5 Security and Office 365 E5 license bundles. Additionally, Plan 1 as well as Plan 2 are available as separate add-ons. The table below lists the feature set of the two plans.

Microsoft Defender for Office 365 Plan 1	Microsoft Defender for Office 365 Plan 2
Safe Attachments	Safe Attachments
Safe Links	Safe Links
Safe Attachments for SharePoint, OneDrive und Teams	Safe Attachments for SharePoint, OneDrive und Teams
Anti-Phishing	Anti-Phishing
Real-time recognition	Real-time recognition
	Threat Trackers
	Threat Explorer
	Automated Investigation and Response
	Attack simulation Training
	Campaign Views

In addition to these features, Exchange Online Protection provides basic protection against malware, spam and phishing. Exchange Online Protection is included in all Exchange Online licenses.

Prevention (Plan 1 & Plan 2)
A reliable filtering function prevents attacks on small and large target groups as well as targeted attacks, e.g. by fraudulent e-mails, spied credentials, ransomware and sophisticated malware. To prevent attacks, Microsoft Defender for Office 365 offers several configuration options. These are:

Anti-phishing.
Various features enable the reduction of phishing emails. For example, spoof intelligence, anti-phishing policies, black lists and implicit email authentication (via SPF, DKIM and DMARC) are used to block spoofed senders.
Anti-Spam
The anti-spam rules help to filter spam e-mails. Different technologies are used, such as connection filtering and content filtering. In addition, outgoing emails are also checked for possible spam content.
Anti-Malware
Anti-malware policies are used to detect known malware based on signatures and heuristic detection. In addition, the Microsoft Anti-Malware team updates detection rules every two hours when an attack is detected.
Safe Attachments
Safe Attachment policies provide zero-day protection by scanning email attachments for malicious content. Sa-fe Attachment routes all messages and attachments that do not have a virus/malware signature to a dedicated environment and then uses machine learning and analysis techniques to detect malicious intent. If no suspicious activity is found, the message is forwarded to the mailbox.
Safe Links
Enables URLs to be checked at the time of click, for example in emails and Office files. Protection is continuous and applies to the entire messaging and Office environment. Links are scanned on every click: safe links remain accessible, malicious links are blocked dynamically.

Detection (Plan 1 & Plan 2)
Innovative AI detects dangerous and suspicious content and correlates attack patterns. This enables detection of attackers trying to bypass protection mechanisms.

Investigation and Hunting (Plan 1 & Plan 2)
Powerful tools facilitate threat detection, prioritization and investigation to track down attackers across the Office 365 environment using innovative hunting capabilities.

2.1.4 Tenable

Internal services are published against external because this is needed to meet requirements. (Examples: Skype for Business, ConfigMgr, CRM tool, etc.). Publishing and its configuration may create vulnerabilities that allow an attacker to gain

improper access to the systems from the outside (examples: RDP, TLS, etc.). Newly discovered vulnerabilities or so-called dangerous zero-day vulnerabilities may pose an additional threat.

To check the publications for security best practices and to monitor for new vulnerabilities, the vulnerability scanning tool Tenable is used.