Sentinel

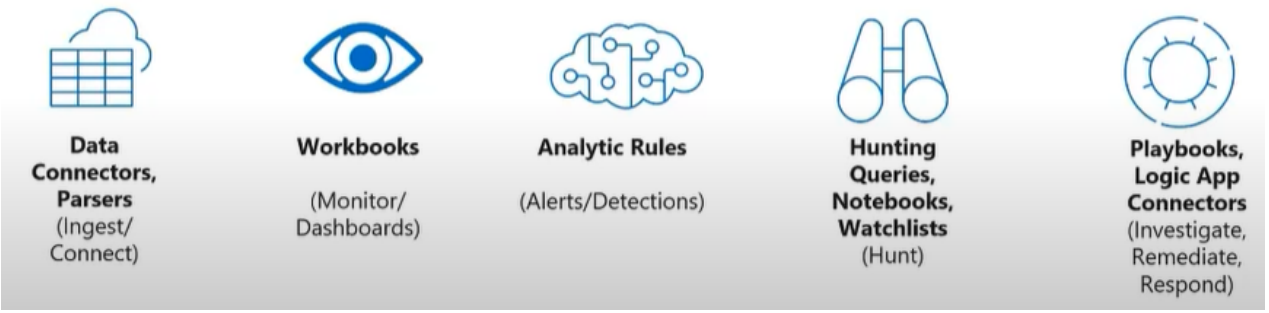
Index

Defender for Cloud and Sentinel

- Defender for cloud :
  - Used for protection and governance of azure and hybrid workloads.
- Sentinel :
  - Sentinel is a #SIEM and #SOAR solution of Microsoft.
  - **SIEM** is basically a data aggregator where you can collect data from all the sources including on-premises and other cloud providers and analyze it using *threat intelligence* and *advances analytics*.
  - It uses AI for *Threat intelligence*.
  - It is also a **SOAR** solution allows to automate and orchestrate common tasks and workloads using built-in or custom *playbooks*.
  - You can also integrate Sentinel with multiple services like *Service now* which is a tool for automations like automated remediation, Unified view of incidents
- Sentinel is a cloud native SIEM and SOAR
  - Security Information and Event Management.
  - Security Orchestration Automation and Response.
- You can improve your security posture by collection of the data, detection of undetected threats, Investigate and respond.
- Sentinel supports #Lighthouse :
  - Lighthouse is a multitenant management service which lets a service provider use his own tenant to manage the subscriptions and resource groups that are delegated by the customer.

Microsoft Sentinel Solution

- Packed integrations that deliver end-to-end product value and enable customers to easily *ingest data*, *monitor data*, *hunt*, *investigate*, *respond and connect* with different products , platforms and services
- These integrations are the collections of multiple components of Microsoft Sentinel content, such as:



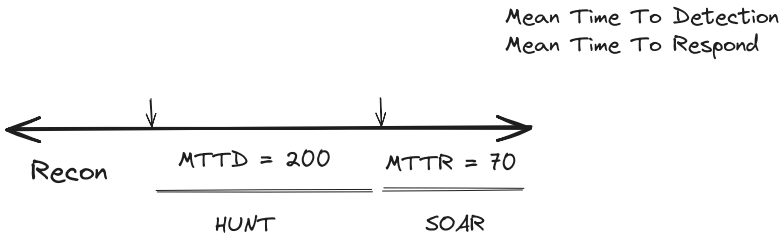
What is SIEM

- SIEM - Security Information and Event Management.
- Hackers need one blind spot and use that vulnerability to exploit.
- The Security analysts always deal with disconnected tools, 100s of tools which are not communicating with each other. So they're going back and forth, checking all these different tools, which creates 100s if not 1000s alerts daily.
- SIEM is the solution which provides *High-Fidelity Alerts*.
- The SIEM is a tool which pulls in sources all the places.
- Aggregates the data,
- Consolidates the data,
- Sorts and Prioritizes to identify threats.

Inputs to SIEM

- Logs
- Threat intel
- Vulnerability feeds
- Network Detection and Response (NDR)
- Endpoint Detection and Response (EDR)
- The SIEM is infused with AI, ML and Analytics which will correlate all the different data in the real time.
- The SIEM outputs High-Fidelity (better alerts) Alerts and they are going to prioritize based on the priority.
- So basically SIEM is a *case management* system which is detected and attach the appropriate artifacts.

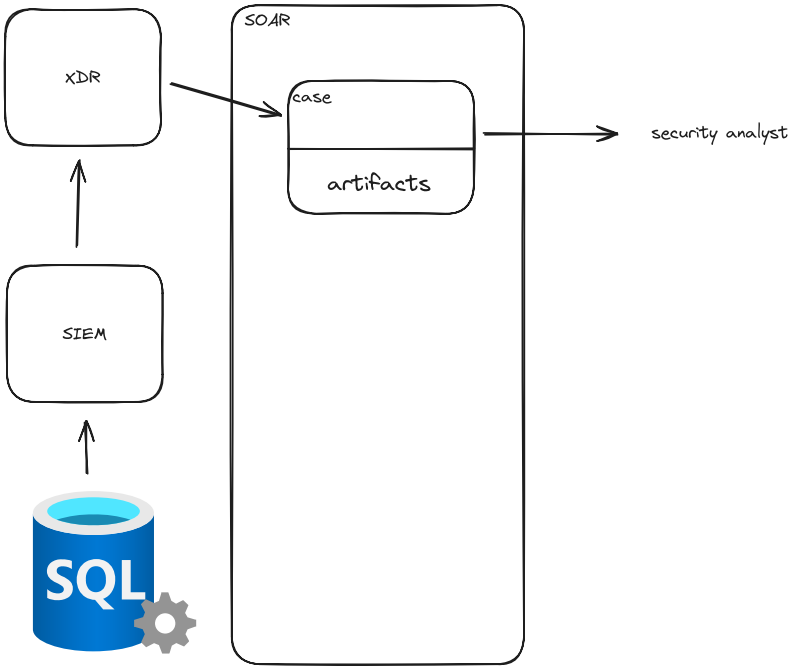
What is SOAR



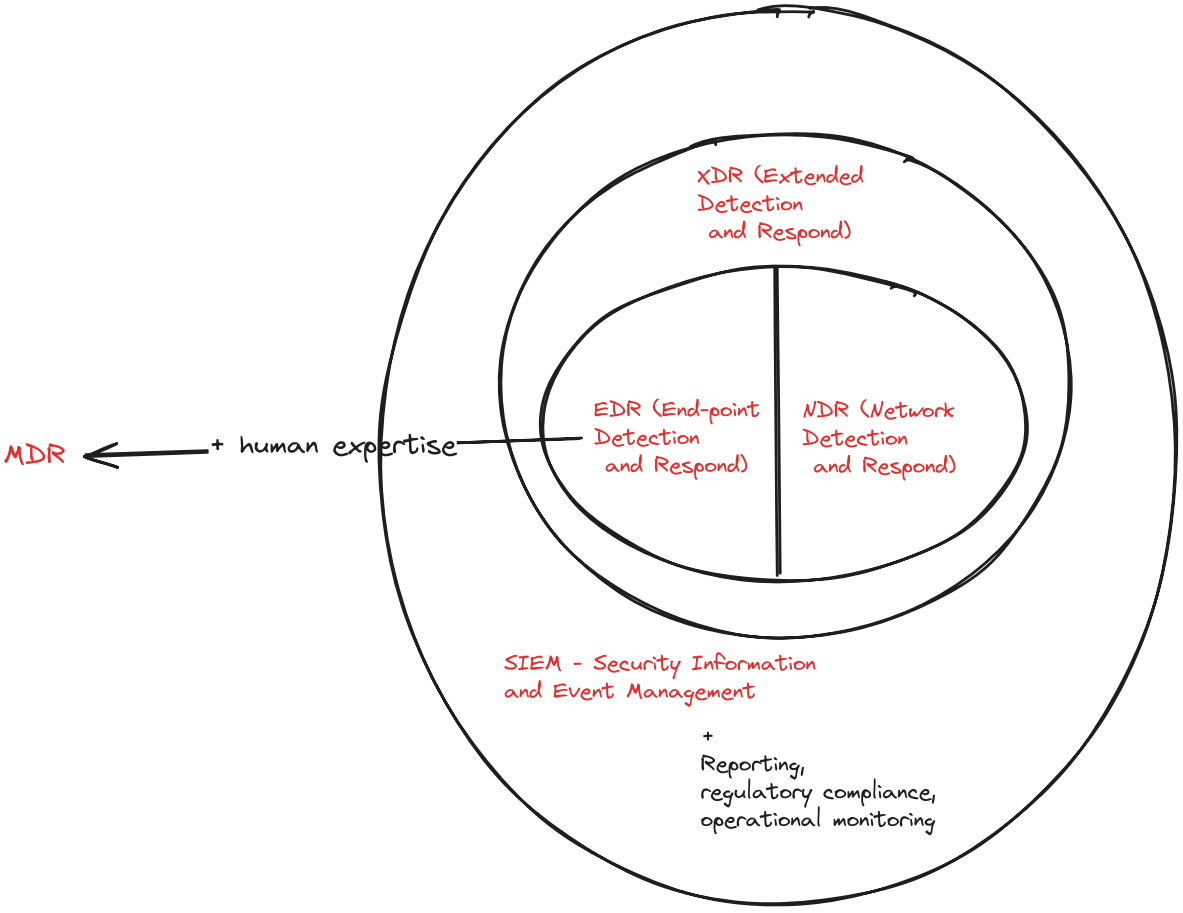
- There are two scenarios, where you manually detect and respond, 2ns is automation.
- The problem is that we can do automation only for what you seen before.
- The concept of *orchestration* is the way you handle these first of the kind. We still have a human involved, but just guiding the actions but not doing every action. It's like semi-automated.
- Manual to a more automated or orchestrated response.

- Lets assume we have a breach in a database.
- It sends an indication up to the SIEM.
- Takes the incident and give a real time alarm and sends it either within the SIEM and have it managed, or sends it up to *XDR*.
- XDR then sends a message over to the *SOAR* to open a case..
- Case is the thing that we're going to use to manage this all the way through to completion and track it along the process.
- The case is then attached with many artifacts which have all the information of compromised resources and source IP and all.
- This case is then assigned to a security analyst.

- So basically SIEM is a *case management* system which is detected and attach the appropriate artifacts.
- Now the analyst have the necessary info on the breach, they can do investigation and they need something to guide them along the way.
- The *playbook* is basically a set of steps where are created in advanced and running them when needed.
- What you do as the second step will depend on the output of the first step. S



EDR, MDR, XDR and SIEM and SOAR.



EDR

> EDR stands for endpoint detection and response, and its primary goal is to identify malicious activity occurring at the endpoint.

- ! EDR technology provides a great view of threats occurring at the endpoint.

- If a user browses to a malicious website and some sort of malware is downloaded, EDR can stop that threat before it turns into something like a ransomware attack.
- Focus is on malicious behavior.
- It monitors activities and events on devices, looks for patterns that may indicate malicious action.
- This provides data for future investigation and this data is vital when the breach is detected.
- The EDR provides details on how the breach occurred and what the attackers actually did.
- This is the part of *Detection* part
- *Response*: can proactively take action to mitigate attacks before they have a chance to cause damage.
- If events are recorded that indicate a system has been breached, EDR can automatically isolate the system from the network in order to cut off the network.
- ! The challenge with EDR is the amount of information it produces.
- EDR provides way more alerts for investigation than a traditional AV. It is a bit hard to detect a definitely good or definitely bad information.

NDR

> Network detection and response (NDR), identifies malicious activity traversing hosts; for example, detecting lateral movement across the network.

- This primarily focused across the network.
- ! It tells you what is occurring on your network, who is coming across it, and what anomalies are happening across your network.
- NDR also gives you the ability to respond to a threat.
- *Microsoft 365 Defender*, specifically the XDR (*Extended Detection and Response*) component, offers NDR capabilities.

XDR

- XDR gives you a combination of EDR and NDR.
- It merges these two technologies and looks at what is happening at the endpoint and then checks the movement of attackers or malware across a network.

> It combines EDR and NDR functionality with some elements of #UEBA User and Entity Behavior Analytics (UEBA)

- EDR focuses on endpoints. XDR solutions integrate data from other systems as well.
- It is an EDR solution while pull in the logs from other sources like firewalls.

Domain boundaries of Applications, Endpoints, Identity and Data. Defending a domain can be challenging. An attacker can establish

1. Alert Fatigue

XDR Vs SIEM and SOAR

> It’s like comparing a speedboat to a warship. Both go in the water and do similar things, but one takes a lot more feeding and watering and provides a lot more protection. One’s very easy to drive, but you can’t do as much with it. So you get there quicker, but you won’t be able to see as much

- SIEM is used for threat detection, compliance, operational risk, and many other things. SIEM collects information from many different sources and as a result, it is a broad and shallow approach.
- It consumes information from solutions such as NDR, UEBA, and EDR.

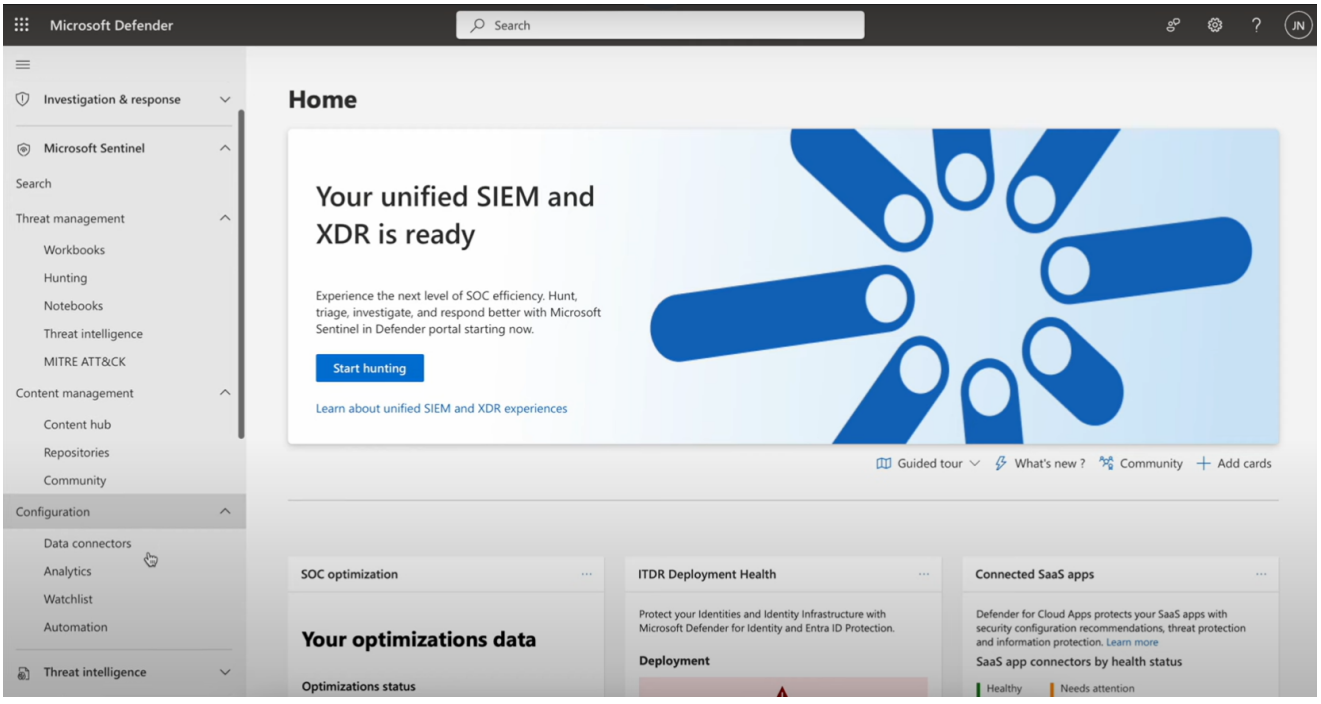
- EDR + additional capabilities, like **reporting**, **compliance**, and **operational monitoring**.
- Provides actionable response, but doesn't provide any kind of automated remediation.
- SOAR can orchestrate and automate the common tasks and remediations.
- XDR does the same sort of things as both SIEM and SOAR.
- XDR is not so comprehensive compared either of these two tools.
- XDR is more focused on endpoints and data ingestion and analytics of XDR is not as powerful as SIEM tool.
- The orchestration capabilities are limited compared to SOAR.
- The XDR tools are cheap than SEAM and SOAR tools.

MDR and MXDR

- The provider uses tools like *EDR and XDR* along with *human expertise*, to monitor your security environment.

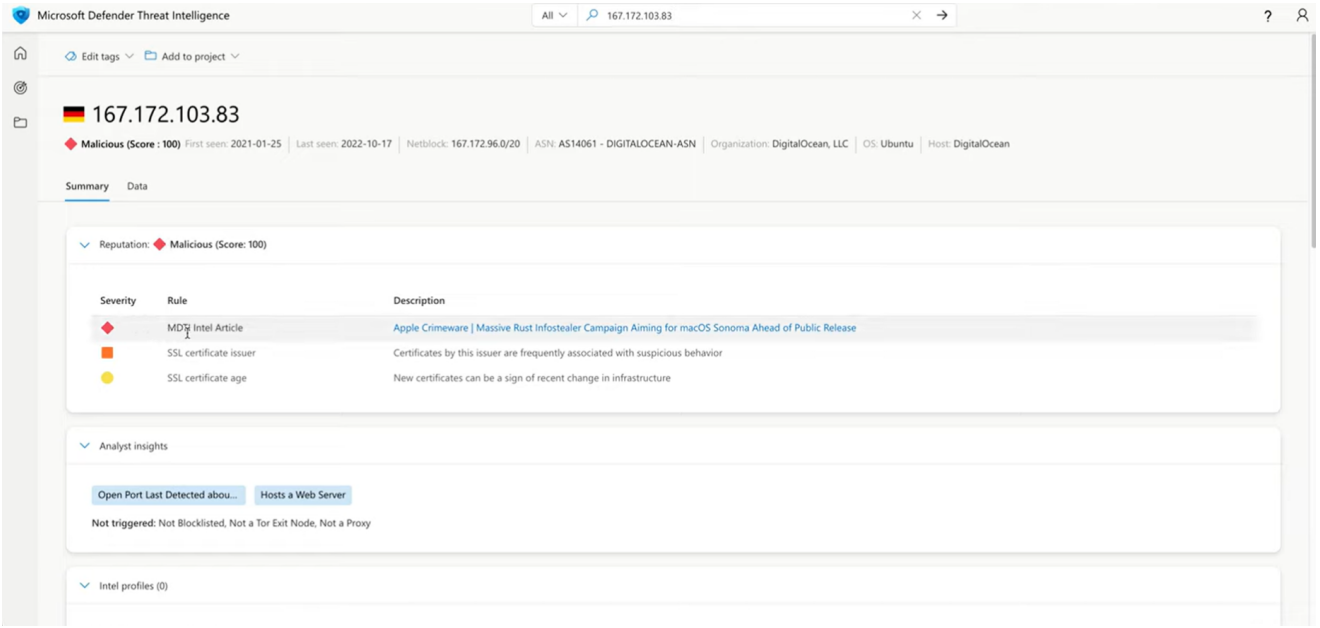
- A *Log Analytic workspace* is required to get ready for sentinel as it ingest all of its detections, analytics and other features.
- Sentinel workspace and its related resources in a dedicated resource group.

> Unified security operations platform which unifies sentinel and MDE. (announced at ignite)



Threat Intelligence in Sentinel

- defender for threat intelligence decreases the time to respond to an incident. It will also gives info on compromised resources in the environment.
- If you have a suspicious login from an IP, if you want to know more about that IP, like who it belongs, Defender threat intelligence will help you investigate on it.



Threat intelligence can be integrated to sentinel to further enrich the incidents. Like in the above image. We can have information of Malicious score of an IP address. This info can be extracted from threat intelligence to sentinel.

A free trial is available for threat intelligence and it provides licensing for both

- Portal features of defender for Threat intelligence.
- Defender for Threat intelligence API.

Analytic Rules in Sentinel

There are two kinds of Analytic rules in Sentinel

1. NRT - analytic rules
2. Scheduled analytic rules

NRT Analytic Rules

Limitations

- There is a limit on using these rules. We can only use 50 NRT Analytic rules.
- We cannot use joins or union statements. We can only use one table for NRT Analytic rules.