Create detections and perform investigations using Microsoft Sentinel.

# Sentinel Analytics

Allows us to analyse historical data collected from your workstations, servers, networking devices, firewalls, intrusion prevention and sensors. By using analytics rules you can trigger alerts based on the attack techniques that are used by known malicious actors.

Common use cases include:

* Identification of compromised accounts
* UEBA to detect potentially suspicious patterns
* Network traffic analysis to locate trends indicating potential attacks
* Detection of data exfiltration by attackers
* Detection of insider threats
* Investigation of incidents
* Threat hunting

You an access the analytics page from the navigation pane. The analytics home page has three main parts:

* The header bar contains information on the number of the rules that are currently in use
* The list of rules and templates contains all the rule templates that Microsoft has preloaded from the Microsoft Sentinel GitHub Repository
* The details pane contains additional information that explains each template and rule that you can use in detection.

We can filter rule template using:

* **Severity**. Use to filter the rules by levels of severity
* **Rule Type**. There are currently four types of rules: Scheduled, Fusion, Microsoft Security, Machine Learning Behaviour Analytics, Anomaly
* **Tactics.** Use to filter the rules based on 14 specific methodologies in ATT&CK model
* **Data Sources.** Use to filter the rules by data source connector that generates the alert.

# Alert types

**Anomaly** – identify anomalous behaviours

**Fusion** – Fusion alerts identify and suspicious activities at various stages of the cyber kill chain. Fusion correlates multiple security alerts from various products and uses machine learning to detect advanced multistage attacks.

For fusion and anomaly detection you must configure the following data connectors:

* AAD Identity Protection
* Microsoft Defender for Cloud Apps
* Microsoft Defender Advanced Threat Protection
* Palo Alto Networks

Some common attack detection scenarios that fusion alerts identify include:

* **Data exfiltration.**  Suspicious activity detected, such as suspicious forwarding rule in Microsoft 365 mailbox after a suspicious sign-in to Azure AD account can indicate compromised user account.
* **Data destruction.** Anomalous number of unique files that were deleted after a suspicious sign-in to Azure AD account can signal a compromised user account was used to destroy data.
* **Denial of service.** Significant number of Azure VMs deleted after a suspicious sign in to AAD account can signal a compromised user account that can be used to destroy the organisations assets.
* **Lateral movement.** Significant number of impersonation actions that occur after a suspicious sign in to azure ad account can indicate a compromised user account that was used for malicious purposes
* **Ransomware.** After a suspicious sign in to an AAD account unusual user behaviour used to encrypt data can trigger a ransomware execution alert.

**Microsoft Security –** The following security solutions pass their alerts to sentinel:

* Microsoft Defender for Cloud Apps
* Microsoft Defender for Server
* Microsoft Defender for IoT
* Microsoft Defender for Identity
* Microsoft Defender for Office 365
* AAD Identity Protection
* Microsoft Defender for Endpoint