1. Microsoft Sentinel

Microsoft Sentinel is a cloud-native Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) solution. It provides a comprehensive view of your organization's security posture. Here's a breakdown of its key features:

**Core Capabilities:**

* **Data Collection:**
  + Sentinel can collect security data from a wide range of sources, including:
    - Microsoft Azure services
    - Microsoft 365
    - On-premises infrastructure
    - Other cloud providers
    - Third-party security solutions

* + It offers built-in connectors for seamless data ingestion.
* **Threat Detection:**
  + Sentinel uses advanced analytics and machine learning to detect known and unknown threats.
  + It leverages Microsoft's threat intelligence to identify malicious activity.
  + User and Entity Behavior Analytics (UEBA) helps detect anomalous behavior.
  + It provides customizable detection rules.
* **Threat Investigation:**
  + Sentinel provides tools to investigate security incidents, including:
    - Incident management
    - Visual investigation graphs
    - Powerful search and query capabilities (Kusto Query Language - KQL)

* + It helps security analysts understand the scope and impact of attacks.
* **Threat Response (SOAR):**
  + Sentinel automates security responses using playbooks, which are based on Azure Logic Apps or Azure Functions.
  + This enables rapid containment and remediation of threats.
  + It allows for automated tasks like isolating compromised systems or blocking malicious IP addresses.
* **Threat Hunting:**
  + Sentinel provides proactive threat hunting capabilities, allowing security analysts to search for potential threats before they cause damage.
  + It includes built-in hunting queries and allows for custom queries.
  + Hunting bookmarks allow for the saving of interesting events.
* **Cloud-Native Scalability:**
  + As a cloud-native solution, Sentinel can scale to handle large volumes of security data.
  + This eliminates the need for on-premises infrastructure.
* **Cost-Effectiveness:**
  + Sentinel offers flexible pricing options, including pay-as-you-go and capacity reservation tiers.
  + It also provides cost savings by eliminating the need for infrastructure maintenance.
* **Workbooks:**
  + Sentinel integrates workbooks, which allow for the monitoring, measuring, and controlling of data. These workbooks are highly customizable.

**Key Benefits:**

* Improved threat visibility
* Faster threat detection and response
* Reduced security operations costs
* Enhanced security posture

In essence, Microsoft Sentinel empowers organizations to modernize their security operations and effectively defend against evolving cyber threats.

1. MICROSOFT Sentinel
   * SIEM – Detection
   * SOAR – Automate Response

A diagram of a computer

AI-generated content may be incorrect.

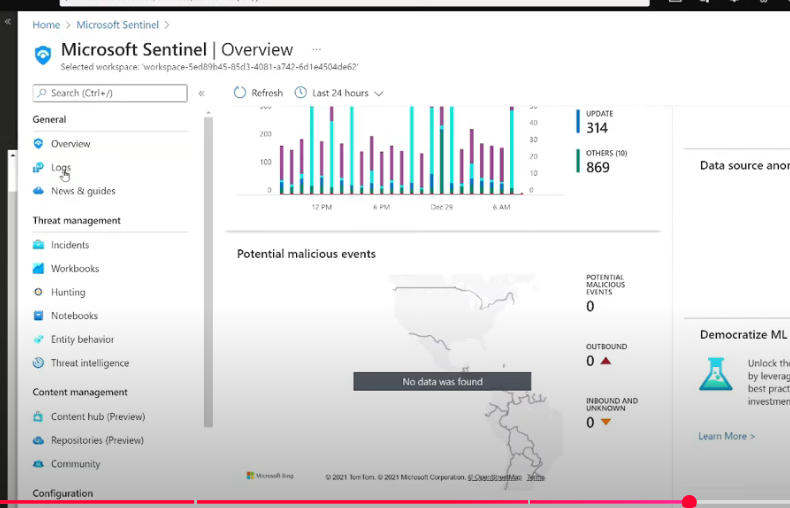
* + Sentinel works by using Microsoft Azure monitor – Log Analytics workspace.
    - Sentinel sits on top of Log Analytics workspace
    - Logs can be Security Logs, Signals etc
    - Sentinel gathers its logs from Azure Resources, On Premises, Other Clouds, Network Equipments, Identity (Azure AD)
  + Azure Sentinel Workspace
  + A screenshot of a computer

    AI-generated content may be incorrect.
  + Connectors – lists all like all azure services, network components, on prem devices etc

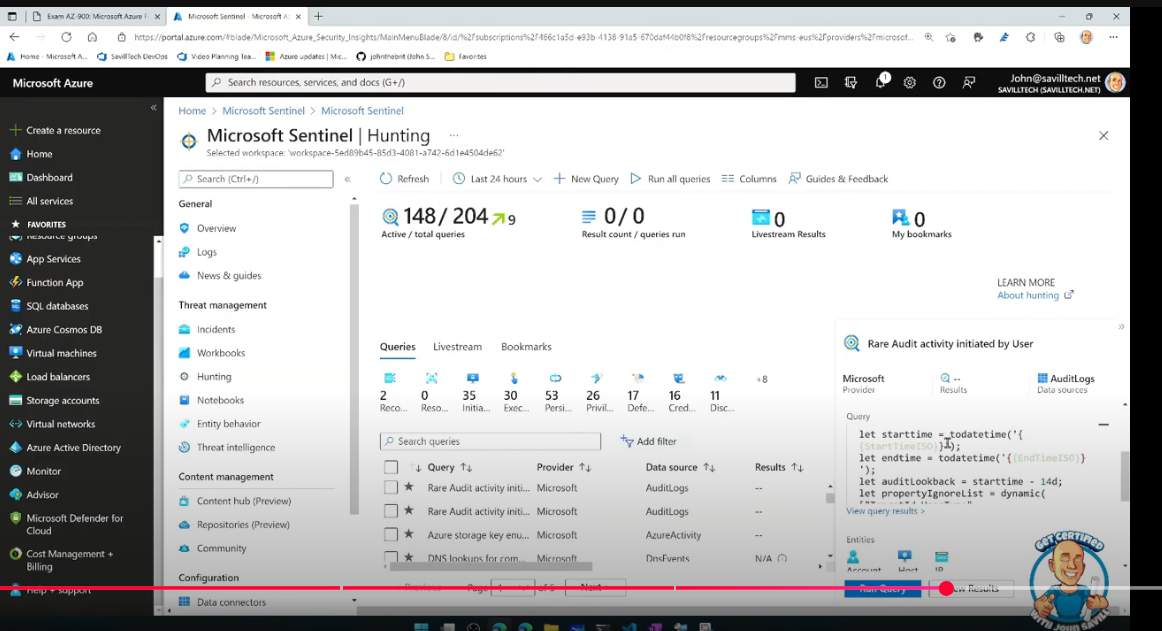
A screenshot of a computer

AI-generated content may be incorrect.

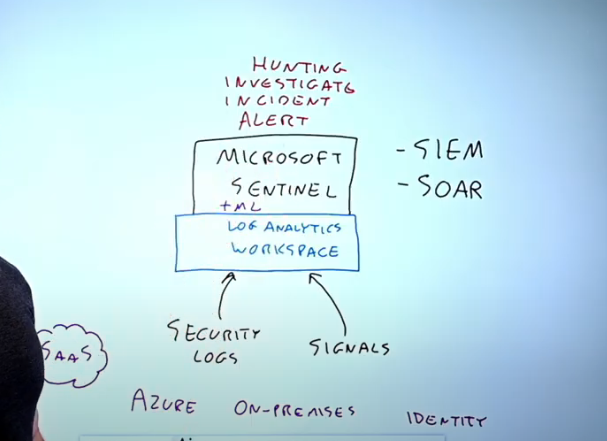
* + Malicious events



* + Hunting



* Entity behaviour – UEBA
* Threat Intelligence
* Automation
* SIEM + SOAR



1. Sentinel basics

A black and white text on a black background

AI-generated content may be incorrect.

A black and white sign with white text

AI-generated content may be incorrect.