MICROSOFT DEFENDER Mind Map

SIEM + XDR

Now, we are extending these XDR capabilities to non-Microsoft data brought in through the SIEM, starting with SAP.

- **Features**
  - Unified Platform with M365D + Sentinel
  - Embedded Security Copilot
  - Automatic Attack Disruption
  - Tailored recommendations
- **Ignite 2023 annoucements**
  - Blog
  - Solution Landing Page

Former RiskIQ

- **Defender Threat Intelligence (MDTI)** — Maps the entire internet to expose threat actors and their infrastructure
- **Defender External Attack Surface Management (EASM)** — Discover unknown and unmanaged resources that are visible and accessible from the internet (outside-in view)

Microsoft Defender Services

- **Microsoft Defender Experts for Hunting** — Augment your SOC team with leading end-to-end protection, threat intelligence, and expertise.
- **Microsoft Defender Experts for XDR** — MXDR - Give your SOC team coverage with leading end-to-end protection and expertise. / Defender Experts for XDR also includes the proactive threat hunting offered by Defender Experts for Hunting
- **Microsoft Incident Response Retainer** — Note: Not a Defender brand but it's part of the service and I am adding to the context here.

Microsoft Defender XDR

- **Microsoft Defender for Cloud Apps (MDA)**
  - App Governance
  - Add-on - Microsoft Defender Vulnerability Management
- **Microsoft Defender for Endpoint (MDE)** — Compare P1xP2
  - MDE P1
  - MDE P2
- **Microsoft Defender for Identity (MDI)**
  - Security Alerts in MDI
- **Microsoft Defender for Office (MDO)** — Compare P1xP2
  - MDO P1
  - MDO P2
- **Secure Score**
- **XDR Automatic Attack disruption**
- **Interactive Guide**
- **Security Copilot in M365 XDR**
- **Documentation**

Defender for IoT

- Overview
- Architecture
- OT sensor cloud connection
- Enterprise IoT Network Security
- Defender for IOT Solution for Microsoft Sentinel

Defender Ninja Trainings

- M365 Defender XDR
- Defender for IoT
- Defender for Cloud
- Defender for Identity
- Defender for Endpoint
- Defender for Office 365
- Defender for Cloud Apps
- Defender Threat Intelligence
- Defender EASM

Microsoft Defender for Cloud (MDC)

CSPM - Cloud Security Posture Management

- **Foundational CSPM - Free**
  - Free (Secure Score)
  - Recommendations
- **CSPM Plan** — Compare CSPM plans
  - Attack Path Analysis
  - Cloud Security Explorer
  - Agentless Scanning for machines
  - Governance & Compliance
  - Agentless Container Posture (Preview)
  - EASM insights in network exposure
  - Data-aware security posture (preview)
- **2023 CSPM Leadership Compass - KuppingerCole**

CWP - Cloud Workload Protection

- **Defender for Servers** — Compare P1 x P2
  - Defender for Servers P1
  - Defender for Servers P2
  - FAQ
- **Defender for App Services**
- **Defender for Databases**
  - Defender for Azure SQL
  - Defender for SQL servers
  - Defender for open-source relational databases
  - Defender for Azure Cosmos DB
- **Defender for Storage**
  - Malware Scanning add-on
- **Defender for Containers**
- **Defender for Key Vault**
- **Defender for Resource Manager**
- **Defender for DNS**
  - *As of August 1, customers with an existing subscription to Defender for DNS can continue to use the service, but new subscribers will receive alerts about suspicious DNS activity as part of Defender for Servers P2.*
- **Security Alerts**
  - **Security alerts - a reference guide**

CNAPP + DevSecOps

- MDC, a Cloud-Native Application Protection Platform (CNAPP) - Blog Post
- **Defender for DevOps**
- **Defender for APIs**

Other Features & Integrations

- Automation
- Workbooks
- Microsoft Cloud Security benchmark
- Azure Policies integration
- SIEM integration
- External Attack Surface Management
- Entra Permissions Management

Multi-Cloud Protection

- Azure
- AWS
- GCP
- Non-Azure VMs (Arc)

Pricing

How to Effectively Perform a MDC PoC

Labs

Microsoft Security Copilot in Defender for Cloud

Note: This mind map aims to be a tool for clarifying the Microsoft Defender product family only. This is not an official Microsoft document. Don't forget to click on the LINKS to access the contents.
Author: Tiago Souza - https://cybergeeks.cloud

Revision date: November, 2023 (post Ignite event)