THE PARTNER MASTERS

Microsoft Sentinel Migration and Modernization

Migrate from legacy SIEM to Microsoft Sentinel a cloud native SIEM + SOAR

Engagement Overview

Conduct a discovery to better understand the current state of your SIEM. Collect monitoring and alerting use cases and requirements.

Create a comprehensive design that aligns with the current security portfolio and existing data sources.

Implement the design phase: Integrate data sources that will connect to Microsoft Sentinel; ensure that Microsoft Sentinel works as designed.

Operationalize Microsoft Sentinel Investigation and Response within existing security monitoring, alerting, and incident response processes.

While legacy SIEMs can maintain good coverage of on-premises assets, on-premises architectures may have insufficient coverage for cloud assets, such as in Azure, and other cloud hyper-scalers. SOC teams face a set of challenges when managing a legacy SIEM:

- **Slow response to threats.** Legacy SIEMs use correlation rules, which are difficult to maintain and ineffective for identifying emerging threats. Analyzing this data slows down SOC teams in their efforts to respond to critical threats in the environment.
- **Scaling challenges.** As data ingestion rates grow, SOC teams must invest in infrastructure setup and maintenance, and are bound by storage or query limits.
- **Manual analysis and response.** SOC teams need highly skilled analysts to manually process large amounts of alerts. SOC teams are overworked and new analysts are hard to find.
- **Complex and inefficient management.** SOC teams typically oversee orchestration, infrastructure, manage connections between the SIEM and various data sources, and perform updates and patches. These tasks are often at the expense of critical triage and analysis.

Our Approach to Microsoft Sentinel

Our goal is to simplify and streamline the deployment of Microsoft Sentinel so you can get up and running as soon as possible. Our consulting service is customized based on your needs and on average takes up 2-4 weeks to deploy Microsoft Sentinel.

Determine the data sources to ingest, items to migrate, compliance and storage requirements.	Deploy data connectors, import Analytic Rules and configure UEBA, Watchlists, etc	Migrate existing historical logs, dashboards, etc. Setup starter Playbooks, Workbooks, Threat Hunting queries	Tune analytic rules and alerting processes. Setup retention and archiving, setup cost management

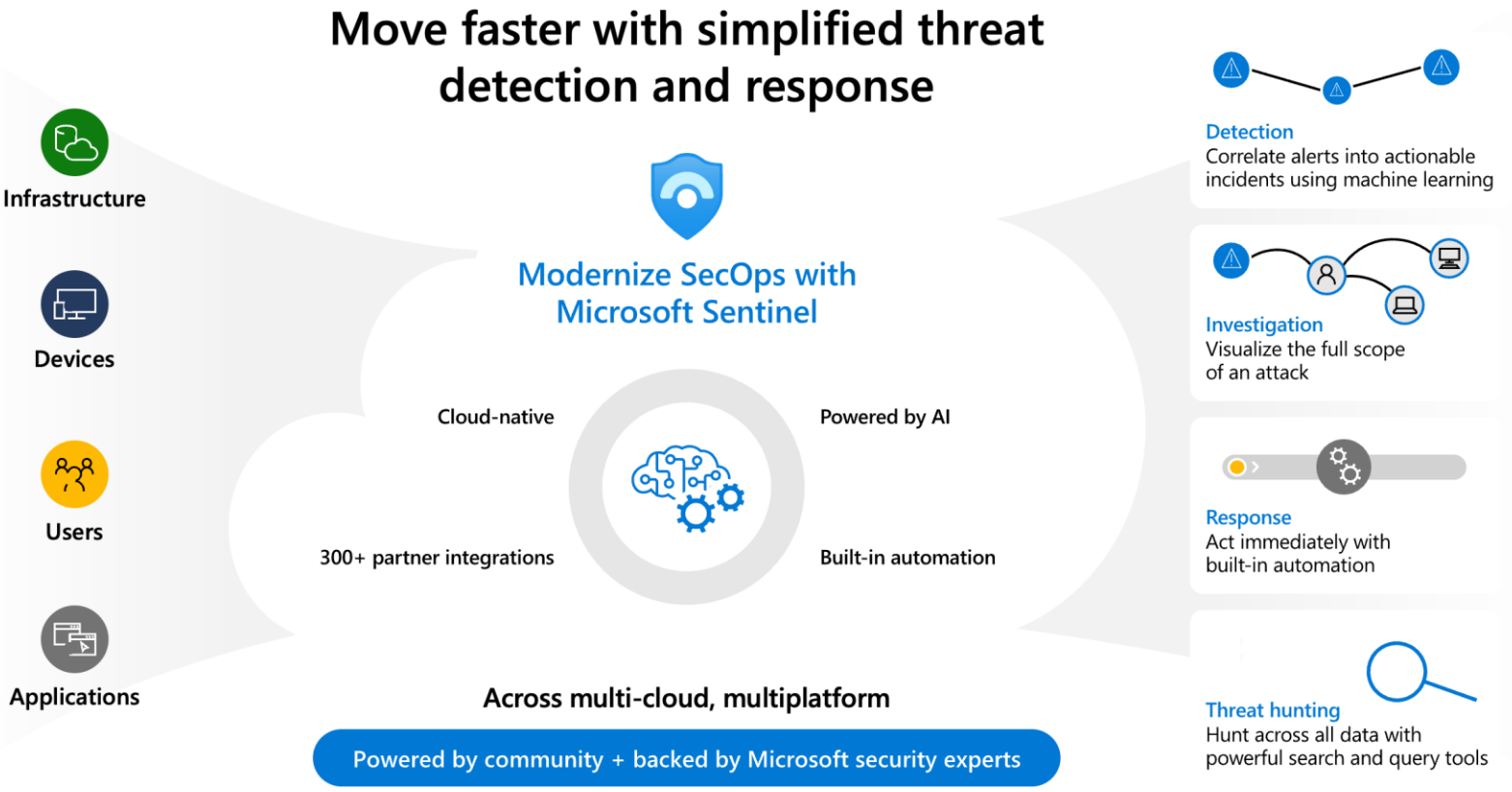
What to expect

During this engagement, we'll partner with you to help you get Microsoft Sentinel properly designed, deployed and configured according to your requirements.

- We will collaborate with your team on the design of Microsoft Sentinel, documenting requirements and decision points along with building architecture diagrams.
- During the migration deployment we will work alongside your teams to transfer knowledge on Microsoft Sentinel and document screenshot by screenshot how the environment is configured and why.
- Long-term recommendations from Microsoft experts about your security strategy specific to Microsoft Sentinel, with key initiatives and tactical next steps.

About Microsoft Sentinel

Microsoft Sentinel is a cloud-native SIEM (Security Information and Event Management) solution that offers intelligent security analytics and threat detection across an organization's digital estate. Organizations can use it to collect security log data at scale, detect and respond to threats swiftly, and minimize false positives with the help of Microsoft's advanced analytics and threat intelligence. It seamlessly integrates with other Microsoft security products, providing a unified security operations platform that enhances the capabilities of extended detection and response (XDR) and SIEM for a more robust defense strategy.



THE PARTNER MASTERS

Get started by contacting us via Azure Marketplace!
https://tpm.ms/SentinelMigrationOffer
sales@thepartnermasters.com