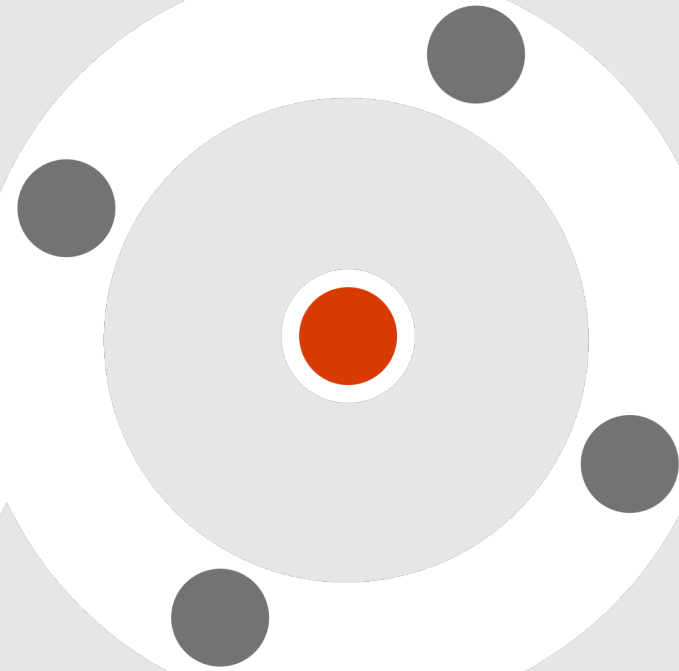


THE
PARTNER
MASTERS



Microsoft Sentinel Accelerator



Triggers of the need for a modern SIEM solution



Attack surface is expanding due to growing digital estates and hybrid work



Rapid acceleration and increasing sophistication of cybercrime



Rising costs of silos, licenses and staff




Complex set-up and maintenance of on-premises infrastructure

Move faster with simplified threat detection and response


Infrastructure


Devices


Users


Applications



Modernize SecOps with Microsoft Sentinel



Cloud-native

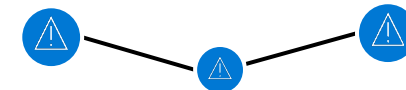
Powered by AI

300+ partner integrations

Built-in automation

Across multi-cloud, multiplatform

Powered by community + backed by Microsoft security experts



Detection

Correlate alerts into actionable incidents using machine learning



Investigation

Visualize the full scope of an attack



Response

Act immediately with built-in automation



Threat hunting

Hunt across all data with powerful search and query tools

Save money and reduce time to value

201% ROI
over three years¹

80% reduction
in investigation effort¹

48% less expensive
compared to legacy SIEMs¹

79% decrease in false
positives over three years¹

56% reduction in management effort
for infrastructure and SIEM¹

67% decrease in time to deployment
with pre-built SIEM content and
out-of-the box functionality¹



- » Cloud-native SAAS solution, with benefits like automatic updates, no on-premises infrastructure to set up and maintain and elastic scalability.
- » Unified SIEM solution with SOAR, UEBA and TI

- » Unparalleled integration with out-of-the-box solutions enabling value on day one. Don't spend time and money on set up
- » Mature and feature-rich SecOps platform built on top of core SIEM capabilities with native XDR integrations

Flexible collecting and archiving options

Eliminate blind spots with affordable solutions to collect, store, and analyze all your security data



Analytics logs

Security and activity logs

- » Used for continuous threat monitoring, near real-time detections, and behavioral analytics
- » Available for 90 days, with option to archive
- » Affordable pay-as-you-go pricing with volume discounts and predictable commitment tiers



Basic logs

High-volume, investigation logs

- » Accessed on-demand for ad-hoc querying, investigations, and automation
- » Supports ingestion-time parsing and transformation
- » Available for eight days, with option to archive



Archive

Low-cost, long-term storage

- » Meet compliance requirements
- » Archive data up to seven years
- » Easily search and restore archived logs

Solve the SOC's hardest challenges while managing the total cost of operations

Objectives



Plan and Prepare

Understand how you intend to use Microsoft Sentinel, define single or multi-tenant architecture and define compliance requirements for data collection and storage. Determine which data sources you need and the data size requirements to help you accurately project your deployment's budget and timeline.

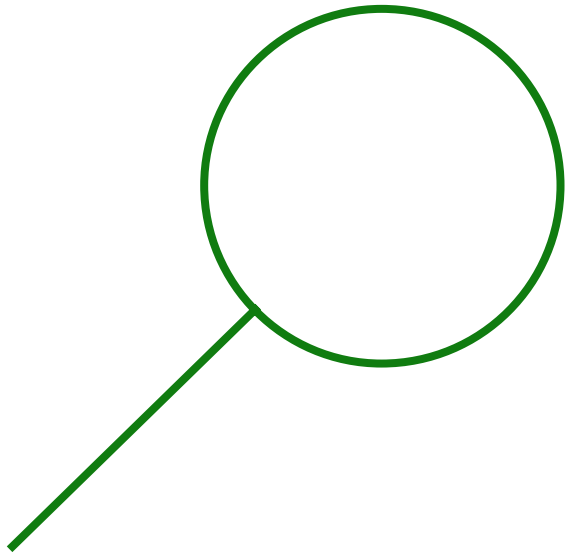
Deploy

Configure and deploy Log Analytics, Data Connectors, Analytic Rules, Playbooks, Workbooks, UEBA, Threat Hunting, Threat Intelligence, Watchlists and all capabilities of Microsoft Sentinel.

Optimize

Tune analytic rules based real world feedback to reduce false positives. Configure data retention and archiving for the Log Analytics workspace for cost optimization of Sentinel. Setup cost management workbook for ongoing analysis of data ingestion and processing to manage Sentinel costs.

Out of Scope



- » Incident Response of any threats discovered during deployment
- » Sentinel Notebooks
- » Multi-workspace / multi-tenant with Azure Lighthouse
- » Development of custom Analytic rules, Playbooks and Workbooks
- » Managed services to monitor Sentinel
- » Migration from 3rd party SIEM

Next Steps

Schedule your implementation today!

sales@thepartnermasters.com



Security

