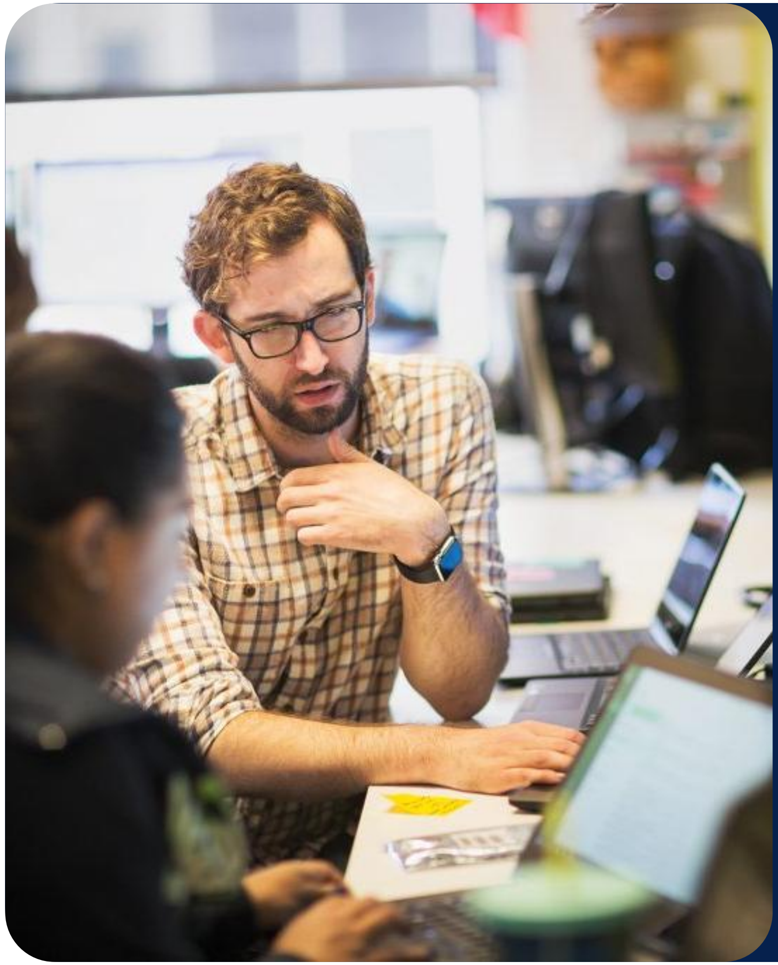

Microsoft Sentinel Migration and Modernization

Migrate from legacy SIEM to Microsoft Sentinel, the cloud-native SIEM solution powered by AI and automation

isacybersecurity.com

ISA CYBERSECURITY

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 cyber crime

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

Multi-cloud, multi-platform compatibility

Powered by community and 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

Improve Security, Metrics and Efficiency

201% ROI
over three years*

79% decrease
in false positives over three years*

80% reduction
in investigation effort*

56% reduction in management effort
for infrastructure and SIEM*

48% less expensive
compared to maintaining legacy SIEMs*

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

- Cloud-native SAAS solution, with benefits like automatic updates, elastic scalability, and no on-premises infrastructure to set up and maintain
- 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

* The Total Economic Impact™ of Microsoft Azure Sentinel from Forrester Consulting

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 behavioural 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

- Designed to meet compliance requirements
- Archive data up to seven years
- Easily search and restore archived logs

Microsoft Sentinel Migration

Phases & Key Activities

Discovery

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

Key Activities

- Identify requirements and detailed use cases
- Identify and document your existing automation, remediation, and alerting tools and processes
- Identify your existing SOC processes, including investigation, automation, and remediation
- Identify critical security assets
- Assess existing security portfolio
- Identify integrations with IT service management (ITSM), threat intelligence, and automation solutions

Deliverables

- Project plan
- Current state analysis
- Business and technical requirements
- Use cases

Design

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

Key Activities

- Design integration of Microsoft and third-party sources
- Map rules to Microsoft Sentinel built-in rules
- Map dashboards to Microsoft Sentinel workbooks
- Map automation to Microsoft Sentinel playbooks
- Design custom alerting for Microsoft Sentinel features
- Map existing SOC processes to Microsoft Sentinel features
- To migrate historical logs, review the available target platforms and data ingestion tools

Deliverables

- Design workshops
- Design documentation
  - Data source integration
  - Automation
  - Custom alerting

Implement

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

Key Activities

- Connect Microsoft sources, could logs (AWS/GCP), network devices, and third-party security solutions
- Deploy Azure Monitor Agent to collect logs from VMs (Windows/Linux) and network devices
- Review your MITRE ATT&CK® coverage
- Implement automation via Azure Logic Apps
- Convert remaining rules to Microsoft Sentinel rules
- Deploy/create playbooks and automation rules
- Deploy playbooks for ITSM platforms, SOAR, and threat intelligence platform integration
- Deploy workbooks and convert dashboards to workbooks
- Review SOC operations migration best practices

Operationalize

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

Key Activities

- Assist with refining monitoring and alerting processes
- Assist with security incident management processes
- Assist with triage/investigation processes
- Assist with alerting use cases refinement
- Define SOC processes based on the mapping done in the design phase

Committed Migrating to Microsoft Sentinel

Deliverables

- Microsoft Sentinel PoC plan
- Connect Microsoft data sources
- Connect external data sources
- Deploy Azure Monitor agent
- Implement workbooks and playbooks

Deliverables

- Microsoft Sentinel configuration documentation
  - Workbooks
  - Playbooks
  - Custom alerts
  - Kusto Query Language (KQL) queries

Schedule your migration and implementation today

☎ 1-877-591-6711

✉ info@isacybersecurity.com

🌐 isacybersecurity.com

ISA CYBERSECURITY