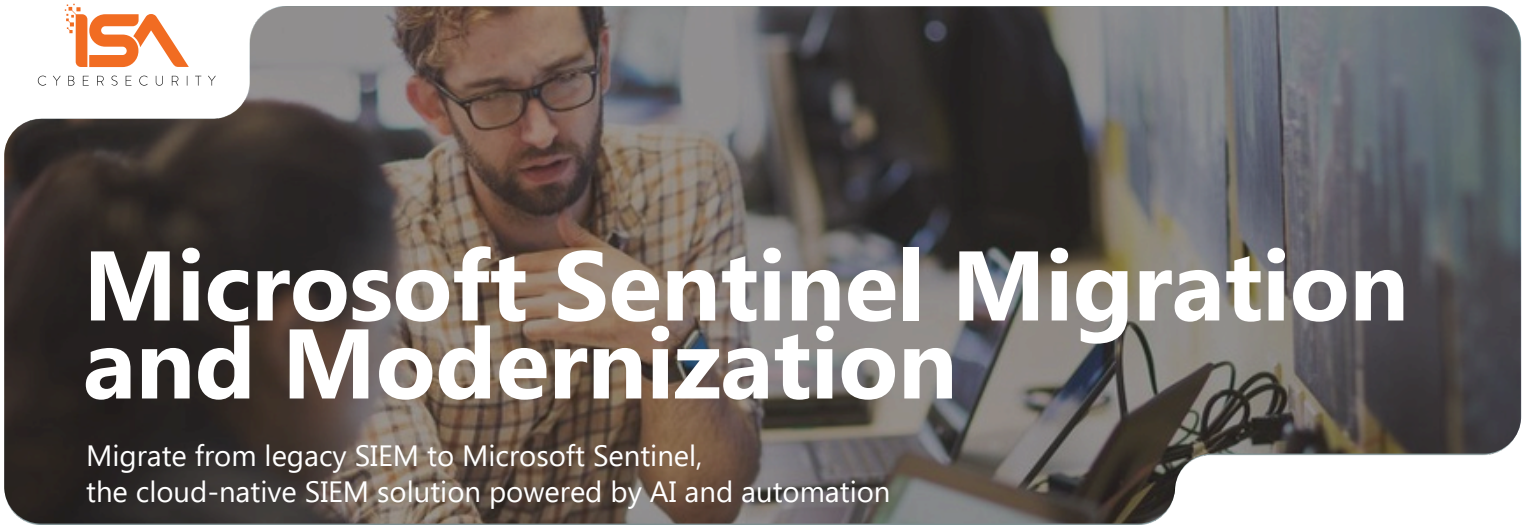


Microsoft Sentinel Migration and Modernization

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

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 your 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 incident investigation and response within existing security monitoring, alerting, and incident response processes.

While legacy, on-premises, hardware-based SIEMs can maintain adequate coverage of local assets, these architectures may have insufficient coverage for cloud assets, such as those in Azure and other cloud hyperscalers. This is just the beginning: SOC teams face a series of additional challenges when asked to manage legacy, on-premises SIEMs:

- **Slow response to threats:** Legacy SIEMs use correlation rules, which are difficult to maintain and ineffective for identifying emerging threats. When a SIEM analyzes data this way, the alert triggers can be delayed, slowing down a SOC team's ability to respond to critical threats in the environment.
- **Scaling challenges:** As the volume of data collected increases, security teams - often bound by storage, performance, or query limits - must plan and invest in adding costly infrastructure that requires setup and maintenance.
- **Complex and inefficient management:** Security teams are often responsible for managing the SIEM infrastructure, overseeing orchestration and managing connections between the SIEM and various data sources, in addition to performing updates and patches. These tasks are often at the expense of critical triage and analysis, exposing the business to the risk of being blind to attacks in progress.

THE ISA CYBERSECURITY APPROACH TO MICROSOFT SENTINEL

Our goal is to simplify and streamline the deployment of Microsoft Sentinel so you can have a best-in-class security monitoring solution to defend your organization. ISA Cybersecurity's consulting services are customized based on your needs and can take as little as two weeks for Microsoft Sentinel to have visibility into your environment.

Determine the data sources to ingest, items to migrate, compliance and storage requirements

Deploy data connectors and import analytic rules. Configure UEBA, watchlists, etc.

Migrate existing historical logs, dashboards, etc. Set up starter playbooks, workbooks, threat hunting queries

Test the implementation to validate user acceptance based on design

Tune analytic rules and alerting processes. Set up retention, archiving, and cost management

+1 877 591 6711
info@isacybersecurity.com
isacybersecurity.com

Microsoft Sentinel Migration and Modernization

WHAT TO EXPECT

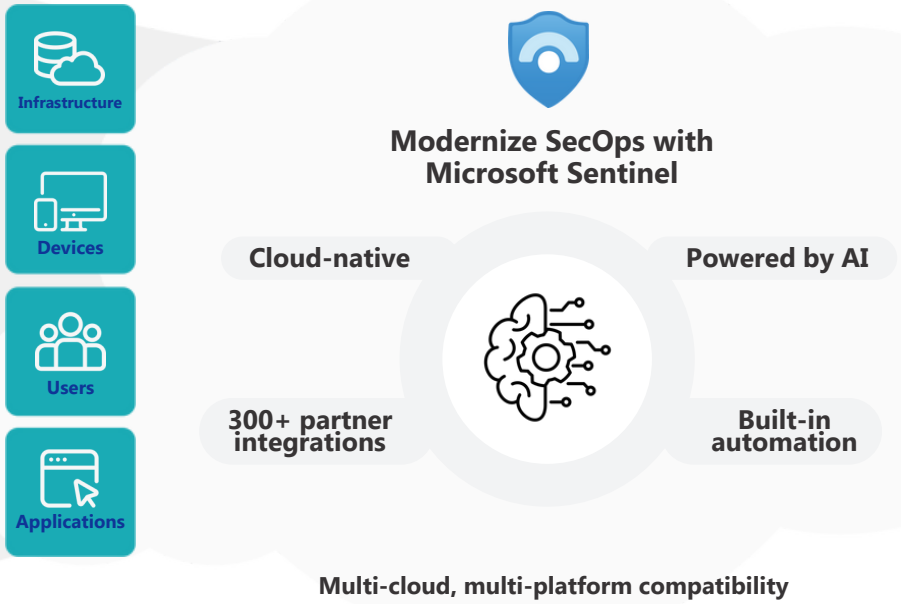
During this engagement, ISA Cybersecurity will partner with you to get Microsoft Sentinel properly designed, documented, configured, deployed and operationalized according to your requirements. During the migration deployment:

- We will work alongside your teams to transfer knowledge on Microsoft Sentinel and document runbooks on how the environment is configured.
- We will provide strategic recommendations from Microsoft experts about your security program 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, threat detection and automation across an organization's digital estate. Organizations use Microsoft Sentinel 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. Microsoft Sentinel 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.

MOVE FASTER WITH SIMPLIFIED THREAT DETECTION AND RESPONSE



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

Powered by community and backed by Microsoft security experts

Get in Touch

+1 877 591 6711

info@isacybersecurity.com

isacybersecurity.com

Head Office: 1100 - 3280 Bloor Street West Toronto, ON M8X 2X3