Microsoft

Sentinel Migration

Security Operations

Why it matters?

Migrating from legacy SIEMs like Splunk or QRadar to Microsoft Sentinel is a strategic move to modernize security operations. With the right expertise, it unlocks cloud-native analytics, AI-driven threat detection, and scalable automation—empowering your team to stay ahead of evolving threats and drive long-term growth.

Partnering with ISD simplifies your migration to Microsoft Sentinel—reducing complexity, minimizing downtime, and accelerating value. We ensure a smooth transition by automating the migration of detection rules, SOAR playbooks, and dashboards—modernizing your SOC for long-term success.

Outcomes

Enable

Microsoft Sentinel
Log Analytics workspace

Rules

Up to 25 rules migrated, deployed and operational (Small size)

Workbooks

Up to 5 Sentinel built-in workbooks enabled, deployed and operational. (Small size)

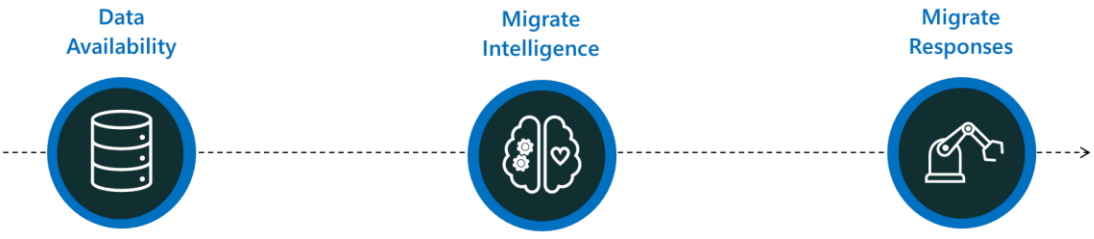
Playbooks

Up to 3 SOAR automation playbooks deployed and operational (Small size)

Available in Small/Medium/Large sizes

Capabilities and Offer Overview

The Sentinel Migration service focus on an efficient migration of use cases from your existing SIEM implementation to Microsoft Sentinel.



- Setup Sentinel instance
- Setup new log pipelines
- Optional: Historical Data export

Migrate SIEM Analytics (Detections, Dashboards, etc.)

Migrate automated responses

2025 © Microsoft Corporation. All rights reserved. This data sheet is for informational purposes only.
This material is for informational purposes only and is subject to change.

Scope

From 10 to 40 weeks

Start — **Delivery**

Readiness, Discovery, Design & Plan

- Security product workshops
- Analyze data infrastructure, ingestion logic, and use cases
- Design workshops, migration workshops, migration planning, build the backlog

Migration Sprints

- Configure the Microsoft Sentinel Solution
- Enable Defender XDR integrations with Sentinel
- Migrate use cases and dashboards
- Validate migrated rules, reduce false positives, sign-off on migrated rules

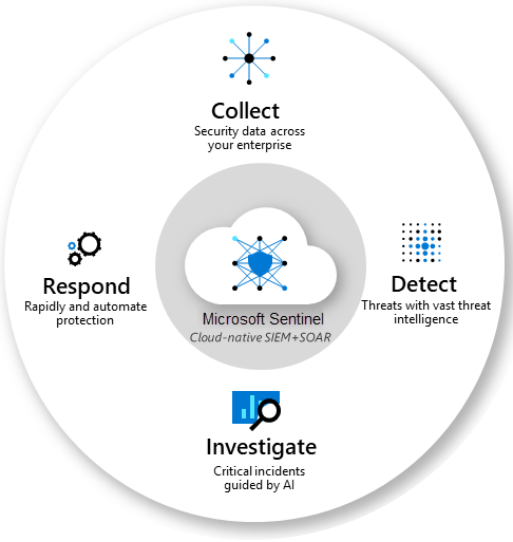
Transition

- Handover to operation
- Handover to continued migration
- Documentation handover
- Data protection cleanup
- Engagement closeout meeting

Benefits

- **Team Readiness**
- **Verified Design**
- **Factory Approach**
- **Repeatable Methodology**
- **Time- and cost-effective migration**
- **Improved security operations**

Why



Microsoft Industry Solutions Delivery accelerates and simplifies your transition from legacy SIEMs to Microsoft Sentinel with a proven, enterprise-ready approach. We deliver fast, secure migrations—including detection rules, SOAR playbooks, dashboards, and Defender XDR integration—enabling rapid value, reduced overhead, and a future-ready security posture.

Next steps

Contact your Microsoft representative to learn how you can migrate your SIEM effortlessly with Sentinel Migration.

2025 © Microsoft Corporation. All rights reserved. This data sheet is for informational purposes only.
This material is for informational purposes only and is subject to change.