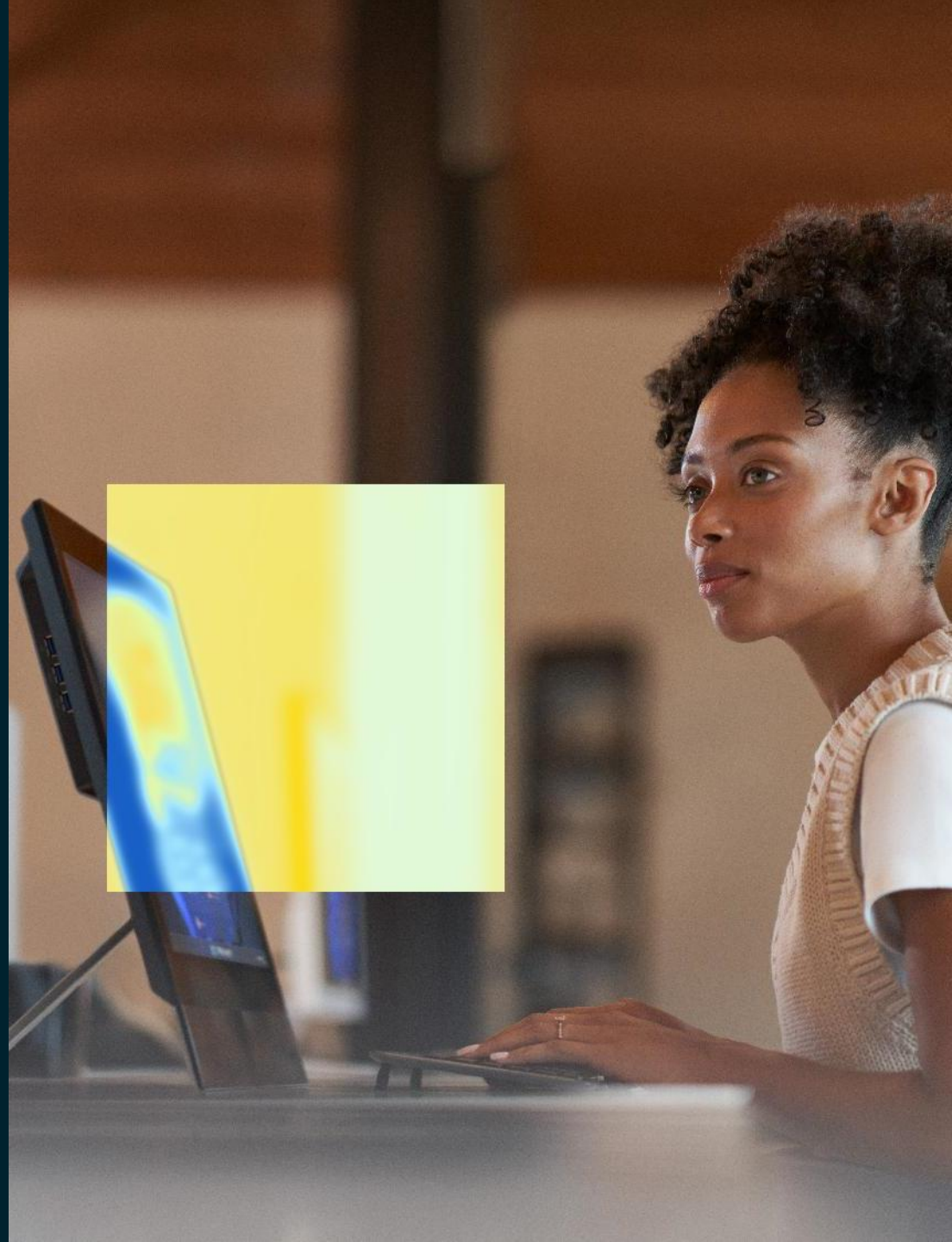
Microsoft Security

Sentinel SIEM Migration decision and planning guide

Powered by the AI-powered SIEM migration experience

Clarify scope, coverage, ownership, and next steps before execution



Customer proof point

“The tool helps turn a Splunk to Sentinel migration into a practical decision process. It gives clear visibility into which detections are relevant, how they align to real security use cases, and where it makes sense to enable or prioritize coverage—especially with cost and data sources in mind.”

Deniz Mutlu
Director, Swiss Post Cybersecurity Ltd.

Microsoft Sentinel: A modern, AI-powered SIEM

A unified SIEM and XDR platform for scale, clarity, and control

Security data foundation



Data lake storage for scale, retention, and cost control

Unified SecOps workflow



Detection, investigation, and response in one experience

AI-assisted response



Less noise, faster investigations

Why SIEM migrations get complex

Teams stall early when priorities, scope, and ownership aren't clear

Unclear priorities



Teams try to migrate everything at once

Undefined requirements



Discovery of missing connectors and data gaps late in process

Vague ownership



No clear decision on who executes and when

Removing ambiguities before any migration execution begins can simplify the process

Simplify SIEM migration in three stages*

Analyze first. Migrate with validation. Optimize continuously.

STAGE 1

Analyze and scope

- Analyze existing detections from Splunk/QRadar exports
- Compare existing detections that map cleanly vs. require redesign
- Review recommendation cards and CSV report of data source and connector requirements

Decision checkpoint: proceed to execution?

STAGE 2

Migrate and validate

(after decision checkpoint)

- Enable required data connectors
- Enable or customize recommended Sentinel detections
- Migrate in phases and validate coverage before cutover

After migration goes live

STAGE 3

Optimize

(after migration)

- Improve coverage and reduce noise
- Optimize cost and data usage
- Continuously tune detections, coverage, and signal quality

*Decision-stage view of the SIEM migration experience. Stage 1 does not start migration or enable any data sources or detections. Detailed product workflows are covered in Microsoft Learn, TechCommunity, and the demo video.

AI-powered SIEM migration experience

Plan and scope Splunk and QRadar migrations with a guided, automated experience

Simplify scoping

Analyze exports, map what translates vs. needs redesign, and identify connector gaps *before* execution

Define your targeted coverage

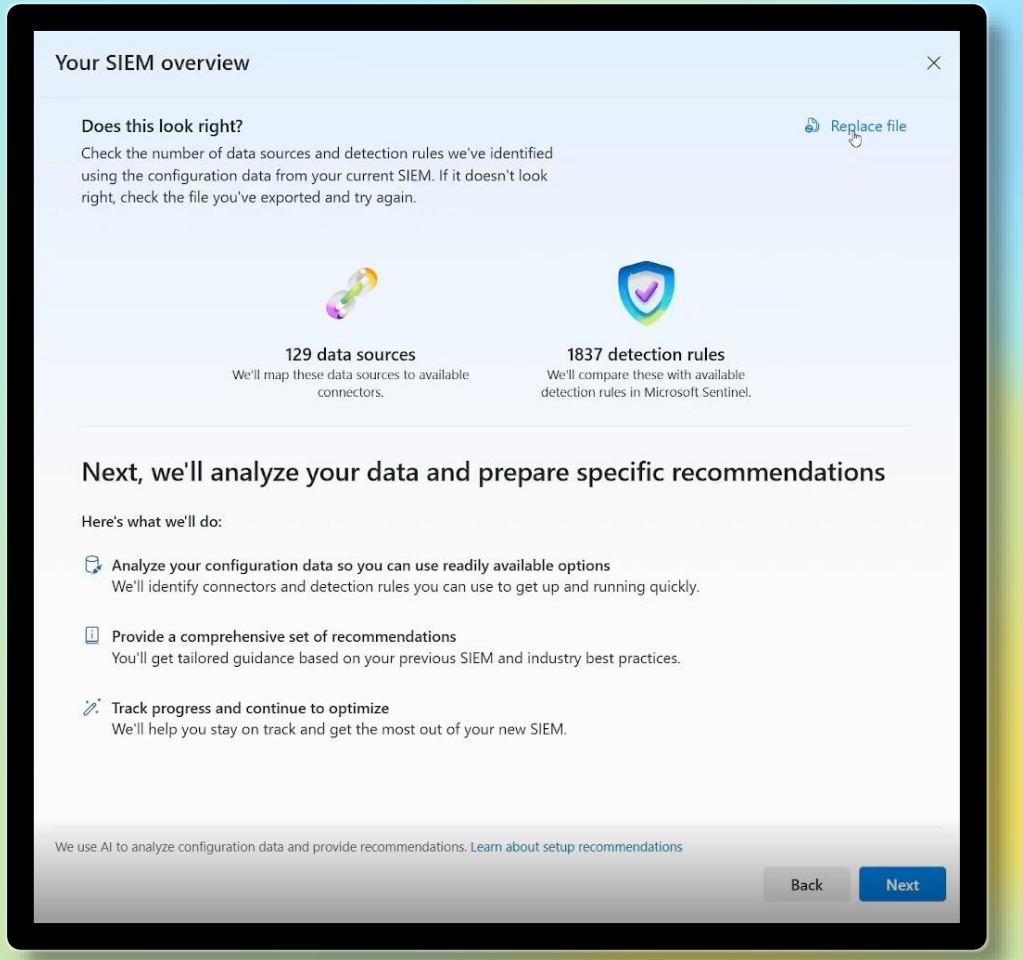
Establish a modern coverage baseline without inheriting legacy complexity

Design for continuous optimization

Improve coverage, signal quality, and cost as your SIEM matures

Learn more:
aka.ms/Sentinel/SIEM_Migration

The experience generates recommendations; no connectors or detections are enabled automatically



STAGE 1

Analyze and scope

Clarify priorities, scope, and ownership—before committing to migration



1

Prioritize work

- Existing detections that map cleanly vs. needing redesign
- Detection comparisons by security domains (Identity, Endpoint, etc.) against Sentinel mappings

2

Scope requirements

- Downloadable CSV with full detection mapping, including unmatched detections
- Required data connectors and gaps surfaced upfront

3

Identify owners

- Microsoft-led, partner-led, or customer-led execution
- Appointed owner before execution

Bottom line: a decision-ready baseline—before any migration execution begins

STAGE 1

Outputs

What you get before deciding



1. **Detection mapping**
   Comparison of legacy SIEM detections to recommended Sentinel detections, down to rule-level details
2. **Downloadable CSV report**
   Full mapping of existing detections, translation status, and required connectors, including unmatched detections
3. **Recommendation cards**
   Review of detection and connector tracking with status (no enablement)
4. **Connector actions**
   Lists of required connectors and their status, with link to Content Hub for connector installation

STAGE 1

Ownership options

This decision determines who executes migration. Microsoft provides guidance for all options.



Microsoft-led (Cloud Accelerate Factory)

- Best for guided execution and hands-on support (where eligible)
- You own access, decisions, and sign-off
- Next step: account team confirms eligibility and scope

Partner-led

- Best for using a chosen partner to execute data onboarding, detection tuning, SOC operations
- You own approvals and validation
- Next step: Microsoft/account team helps identify the right partner and/or align the scope

Customer-led

- Best for strong in-house SOC engineering capacity
- You own enabling of connectors, detections, and outcome validation using the worklist
- Next step: execute in phases using recommendation cards

AFTER STAGE 1

Decision checkpoint

Proceed to migration?



You now know

- What to migrate first
- What data is required
- Who should run the migration

Options

- Proceed to Stage 2: migrate and validate
- Pause and re-scope
- Change ownership model

Bottom line: The migration experience does not automatically enable connectors or detections. You decide when to proceed, what to enable, and who executes the migration.

STAGE 2

Migrate and validate

After the decision checkpoint, migration execution begins*

Enable required data connectors

Based on Stage 1 recommendations and chosen migration path

Enable or tune recommended Sentinel detections

Use the recommendation worklist: start with out-of-the-box, customize where needed

Migrate in phases and validate coverage

Pilot and validate alert behavior before cutover

*Execution approach depends on the chosen ownership option (Microsoft-supported, partner-led, or customer-led)

STAGE 3

Optimize

After migration, in-product SOC optimization improves coverage and reduces cost over time





Improve detection coverage

Identify gaps and expand coverage across prioritized use cases



Tune data ingestion

Refine what data is ingested and how it is used for detections and hunting



Optimize cost over time

Surface opportunities to reduce ingestion cost without reducing security value

Sentinel Adoption Factory

After Stage 1: Optional Microsoft-supported execution model

What it is

Microsoft delivery support for Sentinel adoption and SIEM migration execution (where eligible, scope varies)

When it is used

After Stage 1 analysis—once priorities, scope, and ownership are confirmed

What you get

- Guidance from Microsoft Sentinel specialists
- Outcome-based migration and deployment support
- Delivered remotely and coordinated through your account team

How to engage

Work with your Microsoft account team to confirm eligibility and align scope

Click here for more resources

Get started with the SIEM migration experience

Understand scope, effort,
and ownership–before execution

1. **Open**
   Microsoft Defender portal → SOC optimization* → Set up your new SIEM

2. **Upload**
   Splunk or QRadar export

3. **Run Stage 1 analysis for scope and ownership decisions**
   - Recommended Microsoft Sentinel detections
   - Required data connectors
   - Trackable recommendation cards to plan and sequence work

*Prerequisites: Microsoft Sentinel and Security Copilot enabled



Resources and next steps

Start here

Run the SIEM migration experience to understand scope, effort, and ownership

aka.ms/Sentinel/SIEM_Migration

Learn more

Accelerate your move to Microsoft Sentinel with the new AI-powered SIEM migration experience (TechCommunity)

aka.ms/MigratetoSentinelBlog

Want hands-on help?

Contact the Cloud Accelerate Factory for Microsoft-supported execution (conditions apply)

aka.ms/FactoryCustomerPortal