Microsoft Security

Azure Sentinel Migration Fundamentals

Considerations for transitioning to Microsoft's cloud-native SIEM for scalable, intelligent security analytics across your entire organization.

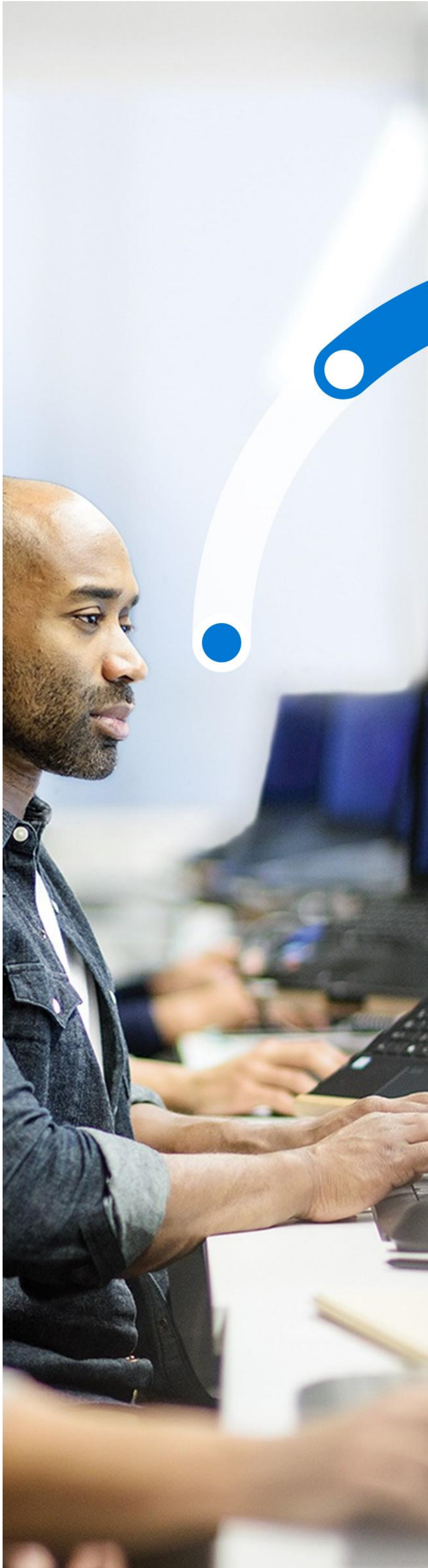
About this whitepaper

This white paper is designed to give you an overview of best practices and considerations for transitioning your security operations to Microsoft Azure Sentinel. We'll look at processes for a direct migration, as well as how to run Azure Sentinel in a side-by-side configuration with your legacy security information and event management (SIEM) solution. This paper also provides guidance on migrating completely away from your legacy solution, enabling you to enjoy the benefits of lower infrastructure costs, real-time threat analysis, and the easy scalability that comes with operating a cloud-native SIEM.

The information in this white paper is derived from experience we've gained in assisting numerous Microsoft customer migrations, as well as the experience of Microsoft's own security operations center (SOC) in protecting our IT infrastructure.

This whitepaper will cover:

- ✓ Planning your migration to Azure Sentinel
- ✓ Starting your migration to the cloud
- ✓ Operating side by side with a legacy SIEM
- ✓ Finishing the migration away from a legacy SIEM
- ✓ Next steps and additional resources



Contents

Introduction

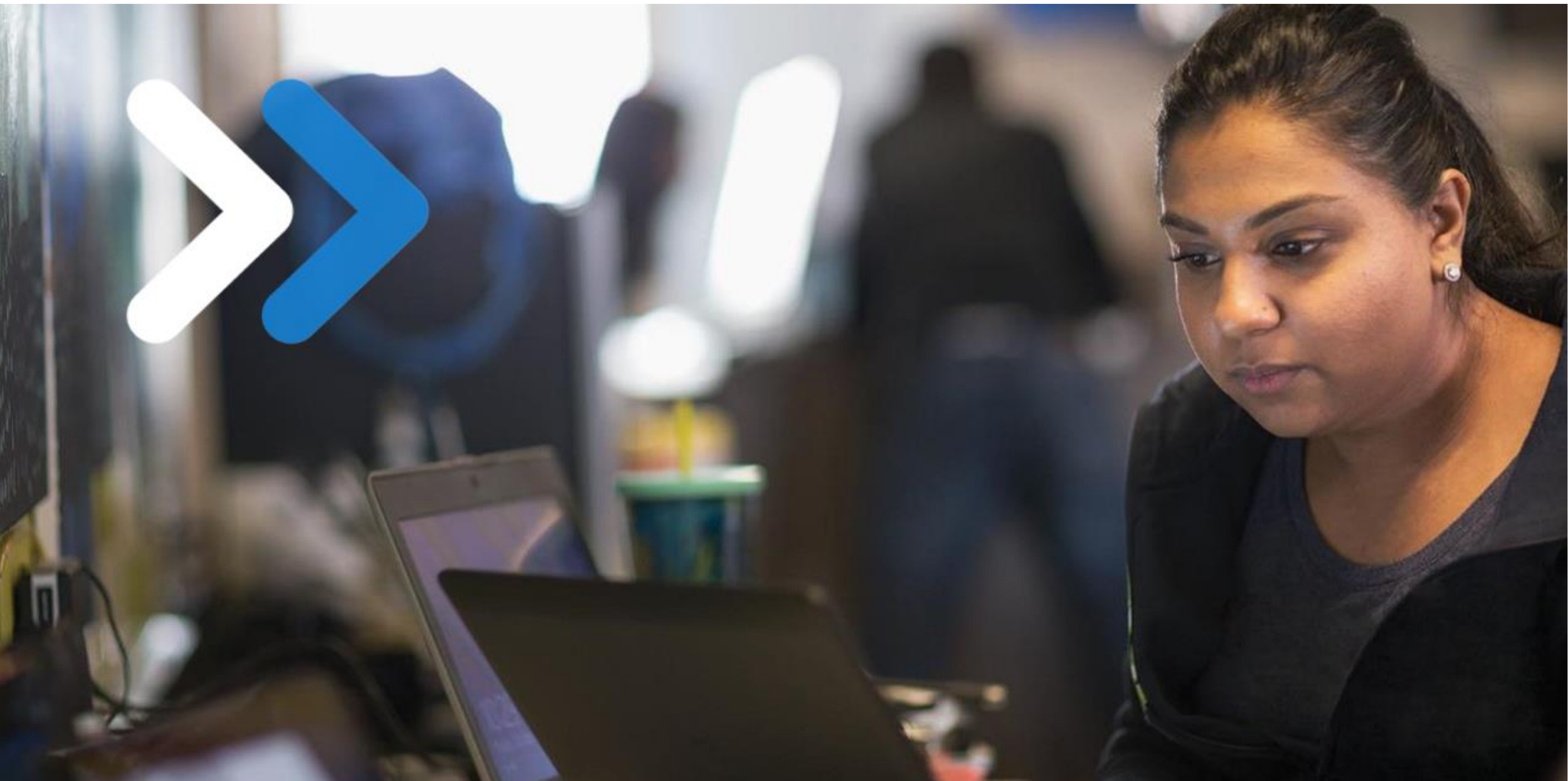
With today's widespread adoption of cloud and remote work, organizations need a solution for centralized security visibility and automation that can meet their growing needs across a decentralized digital estate. Azure Sentinel is designed to fill that need, providing the scope, flexibility, and real-time analysis that today's business demands. This white paper was put together by Microsoft Security experts and provides an overview of Azure Sentinel's core capabilities—how you can rapidly adopt it as a single solution, or use Azure Sentinel in a side-by-side configuration with your existing SIEM.

Planning and staging

We start by examining the features that differentiate Azure Sentinel from other SIEM solutions in the marketplace, including Azure Sentinel's cloud-native capabilities and AI for providing quick correlation—leading to cost savings, greater visibility, and faster time to resolution. We also examine the three basic architecture configurations currently in use for any SIEM, then look at some best practices for enabling your migration to get maximum value from your investment in Azure Sentinel. You'll learn about each step of the migration process, beginning with the decision to initiate a direct or gradual transition, according to your business needs and available resources.

Migration and operation

We'll look at the pros and cons of operating a side-by-side configuration combining Azure Sentinel and a legacy SIEM; specifically, whether a transitional or medium-to-long-term side-by-side configuration would be right for your business. We'll also break down key criteria for comparing Azure Sentinel to your existing SIEM. Finally, you'll learn about the benefits of moving to a fully cloud-native model. You'll also get a checklist covering tasks to complete before deprovisioning your legacy SIEM, as well as some tips for getting the most from Azure Sentinel after onboarding.



Azure Sentinel: Cloud-native SIEM to modernize your SOC

As the industry's first cloud-native SIEM+SOAR (security operation and automated response) solution on a major public cloud, Azure Sentinel provides intelligent security analytics across your entire organization—powered by AI and enhanced with automation. Using machine learning (ML) distilled from customer security data and more than eight trillion signals from Microsoft each day, Azure Sentinel dramatically reduces false positives. Its cloud-native nature helps secure your entire digital estate without the costly infrastructure and time-consuming maintenance required by a legacy or on-premises SIEM.

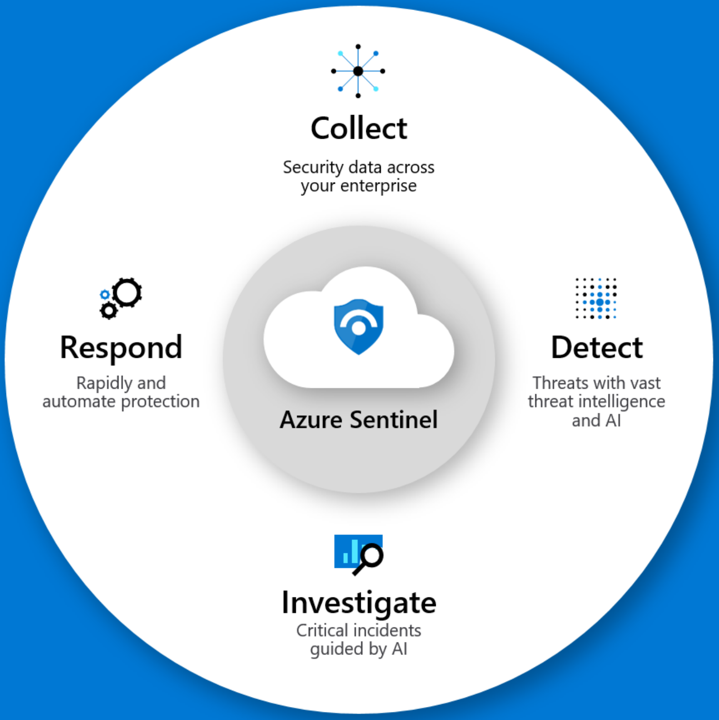

Collect
Security data across your enterprise
Respond
Rapidly and automate protection
Azure Sentinel
Detect
Threats with vast threat intelligence and AI
Investigate
Critical incidents guided by AI

Figure 1: Azure Sentinel functions

Azure Sentinel can receive data in real time from sources across your enterprise, including on-premises systems, software-as-a-service (SaaS) applications, and non-Microsoft cloud environments such as Amazon Web Services (AWS), Linux, or firewalls. Azure Sentinel enables your team to engage in proactive threat hunting using pre-built queries based on Microsoft's decades of security experience, helping you stop threats before they cause harm. You can even modify our ML models or bring your own for tailored detections. With built-in automation for common tasks and workflows, you'll be able to free up more of your analysts' time to focus on tasks that require human attention.

Ranked as a “Leader” in The Forrester Wave™ for security analytics platform providers in Q4 2020, Azure Sentinel helps organizations across IT, financial services, e-commerce, big data, and other verticals modernize their security operations.

> **“With Azure Sentinel, the false positive rate has dramatically improved and we’re now down to responding within minutes; whereas with our legacy solution, our average response time was eight hours.”**
> CISO, eCommerce / fashion industry
> The Forrester Total Economic Impact™ of Microsoft Azure Sentinel report

Why move to Azure Sentinel?

Today’s security operations (SecOps) teams are asked to do more with less, all while protecting an increasingly decentralized digital estate. Organizations are making do with siloed, patchwork security solutions just as cyber threats are becoming more sophisticated and relentless.

The ongoing shortage in security professionals—estimates indicate 3.5 million unfilled security jobs in 2021—has meant that 44 percent of security alerts never get investigated. Meanwhile, the mean time to detect a threat has increased to 197 days, while the time needed to contain it has stretched to 69 days. Add the high volume of noisy alerts, the increasing volume of logs from cloud services, rising infrastructure costs… It’s understandable that security teams are turning to cloud-native SIEMs to mitigate these challenges.

Moving to Azure Sentinel provides real benefits that help make security operations (SecOps) teams more efficient. It frees up your team’s time and resources for dealing with security, not infrastructure. A cloud-native SIEM also translates to significant cost savings. The Forrester Total Economic Impact™ (TEI) of Microsoft Azure Sentinel found that Azure Sentinel is **48% less expensive** than traditional on-premises SIEMs.

Moving to the cloud also allows for greater flexibility—data ingestion can scale up or down as needed, without requiring time-consuming and expensive infrastructure changes.

In addition, Azure Sentinel’s AI and automation capabilities offer significant time-saving benefits for SecOps teams. By combining low fidelity alerts about different entities into potential high-fidelity security incidents, Azure Sentinel helps **reduce noise and alert fatigue**. In fact, Forrester’s TEI report showed that deploying Azure Sentinel led to a **79 percent decrease in false positives** over three years—reducing SecOps workloads and generating $2.2 million in efficiency gains.

The benefits of migrating to a cloud-native SIEM are manifest. That leaves an important question: how do you make the journey?

STEP
1

STEP 1: Planning and approaching your migration

Getting started with your SIEM migration project can seem daunting, considering the sheer amount of data and content that need to be migrated. It’s important to handle your migration in a manner that doesn’t introduce gaps in coverage, which could put the security of your organization in jeopardy.

As we discuss the best ways to approach your migration journey, we’ll be talking about three different architecture stages of the migration process:

On-premises SIEM architecture: This is the classic model with analytics and database functions both residing on-premises. This type of SIEM usually has limited scalability and is typically not designed with AI; so, it may overwhelm your SOC with a large volume of alerts. For the purposes of this paper, we’re considering the on-premises SIEM to be your “before” state prior to the migration.

Side-by-side architecture: In this configuration, your on-premises SIEM and your cloud-native SIEM are used at the same time. We’ll discuss the various configurations of this stage, but typically the on-premises SIEM is used for local resources, while cloud-based analytics are often used for cloud resources or new workloads.

Cloud-native architecture (full Azure Sentinel deployment): In this model, both security analytics and data storage use native cloud services. For the purposes of this guidance, we’re considering this to be the end state, unless you choose to engage in a long-term side-by-side configuration.

If your organization has limited or zero investment in an existing on-premises SIEM, moving to Azure Sentinel can be a straightforward, direct migration.

For an enterprise that’s heavily invested in a legacy SIEM, maintaining good coverage of on-premises assets is usually attainable. However, those same organizations are often lacking security coverage for their cloud assets—Microsoft Azure, AWS, Google Cloud Platform (GCP), or Microsoft Office 365—due to the scale limitations of physical hardware and the pace of innovation in cloud technologies.

For an organization using a legacy SIEM, migration typically requires a three-stage process to accommodate transition tasks:

1. Planning and starting the migration.
2. Running Azure Sentinel and an on-premises SIEM side by side.
3. Completing the migration (moving completely off the on-premises SIEM)

Part of step one involves planning the side-by-side phase. This can be a medium-to-long-term operational model, or a short-term transitional phase leading to a completely cloud-hosted SIEM architecture.

While many organizations previously shied away from running multiple on-premises analytics solutions because of cost and complexity, Azure Sentinel makes this option simpler with its pay-as-you-go pricing model and lack of infrastructure requirements, allowing for greater flexibility. Running a side-by-side configuration as a transitional phase will give your SecOps team time to adapt to the change, migrating and testing content at a pace that works best for your organization.

Identify your key core capabilities and use cases

As you set out on this migration journey, you'll first want to identify your key core capabilities, aka "P0 requirements." Evaluate the key use cases deployed with your current SIEM, as well as which detections and capabilities are vital to maintaining effectiveness with your new SIEM. You may have an overwhelming amount of detections and use cases in your current SIEM; so, use this time to decide which ones are actively useful to your business (and which don't need to be migrated). A good starting place—look at which detections have actually produced results within the last year.

Best practice: Compare and contrast SIEMs

If you're evaluating Azure Sentinel, or plan to use it alongside your legacy SIEM for an extended period; use this time to compare Azure Sentinel to your current traditional SIEM. This will allow you to refine your criteria for completing the migration, as well as help you understand where you can extract more value by leveraging Azure Sentinel.

Based on our experience with responding to a high volume of real-world attacks, we've built this list of key areas to evaluate:

Attack detection coverage	Compare how well each SIEM is able to detect the full range of attacks using MITRE ATT&CK or a similar framework.
Responsiveness	Measure the mean time to acknowledge (MTTA), which is the time between when an alert appeared in the SIEM and when the analyst first started working on it. This will likely be similar between any SIEMs.
Mean time to remediate (MTTR)	Compare incidents investigated by each SIEM (with analysts at an equivalent skill level).
Hunting speed and agility	Measure how fast your teams can hunt—starting from a fully formed hypothesis, to querying the data, to getting the results on each SIEM platform.
Capacity growth friction	Compare the level of difficulty in adding capacity as your cloud use grows. This is particularly important because cloud services and applications tend to generate more log data than traditional on-premises workloads.

STEP
2

STEP 2: Operating side by side with a legacy SIEM

There are several models you can choose from to approach the side-by-side phase of the migration process. Common scenarios that we've addressed in conversations with customers include:

- Moving logs from Azure Sentinel to your legacy SIEM.
- Moving logs from your legacy SIEM to Azure Sentinel.
- Using Azure Sentinel and your legacy SIEM side by side, as two separate panes of glass.
- Sending alerts from Azure Sentinel to your existing SIEM, typically using Azure Sentinel to analyze your cloud data sources.
- Sending alerts from your existing SIEM to Azure Sentinel.

Some of these approaches are very effective, while others introduce significant problems. We'll walk through each of these approaches and their potential pros and cons.

Approach 1: Moving logs from Azure Sentinel to your legacy SIEM—*Not recommended*

In this configuration, organizations use Azure Sentinel only as a log relay, forwarding logs to their existing on-premises SIEM. This approach is not recommended, since running Azure Sentinel strictly as a log-relay means you'll continue to experience the same cost and scale challenges as with your on-premises SIEM. In addition, you'll be paying for data ingestion in Azure Sentinel along with storage costs in your legacy SIEM.

Furthermore, this approach won't allow you to get full value from your Azure Sentinel investment. Using Azure Sentinel merely as a log relay means that you won't be taking advantage of Azure Sentinel's full SIEM + SOAR capabilities, including detections, analytics, AI, investigation, and automation tools—key value-added benefits that Azure Sentinel provides in one platform.

Approach 2: Moving logs from your legacy SIEM to Azure Sentinel—*Not recommended*

In this approach, your SecOps team forwards logs from your legacy SIEM to Azure Sentinel. For reasons similar to the above, this isn't an ideal approach. While you'll be able to benefit from the full functionality of Azure Sentinel without the capacity limitations of an on-premises SIEM, your organization still will be paying for data ingestion to two different vendors. Beyond adding architecture complexity, this model can result in higher costs for your business.

Approach 3: Using Azure Sentinel and your legacy SIEM side by side as two separate solutions—*Not recommended*

In this model, your team uses Azure Sentinel to analyze certain data sources, typically your cloud data, and continues to use your on-premises SIEM to analyze others. Rather than send alerts between the two, SecOps uses both solutions as two separate panes of glass.

This setup allows for clear boundaries regarding when to use which solution, and it avoids the duplication of costs seen with the previous two configurations. However, cross-correlation becomes difficult in this scenario, and it's impossible to investigate attacks that cross between the two sets of data sources. In today's landscape—where threats often move laterally across the organization—such gaps in visibility pose a significant risk to your organization's security.

Approach 4: Sending alerts and enriched incidents from Azure Sentinel into your legacy SIEM—*Suboptimal*

In this model, you'll analyze data in Azure Sentinel (typically starting with your cloud data), then send the alerts generated to your legacy SIEM. There, you can continue to use your legacy SIEM as your single pane of glass and do any cross-correlation on the alerts generated by Azure Sentinel. Your team can then leverage Azure Sentinel for any deeper investigation needed on those alerts.

This configuration has several benefits. It's cost effective because it allows you to move your cloud data analysis to Azure Sentinel without duplicating costs or paying for data twice, while still giving you the freedom to migrate at your own pace. As you continue to shift content over to Azure Sentinel (data sources, detections, etc.), it will become easier to make a complete migration to Azure Sentinel as your single pane of glass and primary interface.

However, there are several downsides to this approach as well. Simply forwarding enriched incidents to your legacy SIEM does limit the value you get from Azure Sentinel's investigation, hunting, and automation capabilities (though you can, and should, leverage these capabilities when investigating and responding to incidents generated by Azure Sentinel).

Learn More:

- Learn how to send enriched Azure Sentinel alerts to your legacy SIEM.
- Learn how to send enriched Azure Sentinel alerts to IBM QRadar.
- Learn how to ingest Azure Sentinel alerts into Splunk.

Approach 5: Sending alerts from your legacy SIEM to Azure Sentinel—*Recommended*

In this configuration, your SecOps team sends alerts from your existing SIEM to Azure Sentinel. Typically, customers will ingest and analyze cloud data within Azure Sentinel; while alongside, they would continue using their legacy SIEM to analyze on-premises data and generate alerts. From there, you'll forward alerts from your on-premises SIEM into Azure Sentinel to maintain your single pane of glass. This can be done using different tools and methods, such as with Logstash, APIs, or Syslog. Any of these methods can send alerts to Azure Sentinel and store them in JSON format in the Azure Log Analytics workspace.

By sending alerts from your legacy SIEM to Azure Sentinel, your team is free to do cross-correlation and investigation on those alerts within Azure Sentinel, and still access your legacy SIEM for deeper investigation if needed. Meanwhile, you can continue migrating data sources over an extended transition period.

This is our **recommended side-by-side migration method**, because it allows you to get full value from Azure Sentinel while also migrating data sources at the pace that's right for your organization. Plus, it avoids duplicating costs for data storage and ingestion while allowing you to move your data sources over quickly.

Learn More: Get more information on how to send alerts or data from your legacy SIEM to Azure Sentinel in the following resources:

- Learn how to migrate QRadar offenses to Azure Sentinel.
- Learn how to export data from Splunk to Azure Sentinel.

Pro tip: Case-management tools

Because dividing the analytics in the above scenarios will add complexity to the investigation process, we strongly recommend setting up a **case-management tool**. Letting software manage the workflow and capture the investigation history and insights will take this burden off your analysts, allowing them to focus on attackers rather than processes. Azure Sentinel can provide basic workflow management, and third-party offerings are also available.

Transitional vs. medium-to-long-term side by side

For most of our customers, side-by-side is a temporary step in their migration journey as they shift to using Azure Sentinel as their primary SIEM. However, some organizations that are not ready to move away from their current SIEM may choose to use Azure Sentinel in a side-by-side configuration with their legacy SIEM as a long-term solution. Typically, these organizations will use Azure Sentinel to analyze their cloud data.

Transitional side by side (recommended): This approach involves running Azure Sentinel side by side with your legacy SIEM just long enough to complete the migration, with the end goal of moving permanently to Azure Sentinel.

> **Pros:** Gives your staff time to adapt to new processes as workloads and analytics migrate. Gains deep correlation across all data sources for hunting scenarios; eliminates having to do swivel-chair analytics between SIEMs or author forwarding rules (and close investigations) in two places. Also enables your SecOps team to quickly downgrade legacy SIEM solutions, eliminating infrastructure and licensing costs.
>
> **Cons***:* Can require a shortened learning curve for SOC staff.

Medium-to-long-term side by side: Involves using Azure Sentinel alongside your legacy SIEM for a longer period of time; leveraging both SIEMs to analyze different subsets of data indefinitely until you're ready to make a permanent full migration.

> **Pros**: Leverage Azure Sentinel's key benefits—including AI, ML, and investigation capabilities—without moving completely away from your legacy SIEM. Saves money compared to your legacy SIEM by analyzing your cloud or Microsoft data in Azure Sentinel.
>
> **Cons**: Separating analytics across two different databases results in greater complexity, i.e., split case management and investigations for multi-environment incidents. Greater staff and infrastructure costs. Requires staff to be knowledgeable in two different SIEM solutions.

Longer-term side-by-side deployment is a potential starting point for an organization that wants to take advantage of Azure Sentinel's strengths, but isn't yet ready to move away from its existing SIEM. Moving to Azure Sentinel over time provides more opportunities to modernize your SIEM while taking advantage of the cost-savings and flexibility the cloud provides. In addition, you'll get the full value of Azure Sentinel's correlation and investigation capabilities across all your data sources.

While short-term transitional side-by-side deployment is our recommended approach, Azure Sentinel's cloud-native nature makes it easy to run side-by-side with your traditional SIEM as long as needed—giving you the flexibility to approach migration in a way that best fits your organization.

STEP 3

STEP 3: Migrating your content

So, how do you approach this migration journey? **Most of our customers migrate in three phases: Starting with data, then detection rules, and finally automation.**

Best practice: Migrating data

Azure Sentinel comes loaded with many built-in data connectors that make it easy to ingest data from across your organization. Start by considering your key priorities and use cases. This is a refrain you'll read several times throughout this guidance, and for good reason. You don't want to invest time or money migrating resources that aren't adding value. Migration is a prime opportunity to re-evaluate your security needs and cull content that's no longer useful. This is especially important when dealing with a SIEM, where the amount of data ingested has a cost implication for your business.

Begin by prioritizing your data sources. Ask yourself: Is this data source valuable? Think holistically about your use cases, then map the data required to support them. Identify any lingering gaps in visibility from your legacy SIEM and determine how you can close them.

Most of our customers begin by ingesting their cloud data into Azure Sentinel. Another good starting point is ingesting data from other Microsoft products, since many of these data sources are free. Azure activity logs and Office 365 audit logs are free to ingest and give you visibility into Azure and Office 365 activity.

You can also ingest alerts from Microsoft Defender products, Azure Security Center, Microsoft Cloud App Security, and Azure Information Protection—all for free. For security products like these, consider whether enriched alerts provide enough context for your key use cases, or if you need to ingest raw logs, which can be costly. In many cases, security teams will ingest enriched data from their security products across the organization while using Azure Sentinel to correlate across them, without needing to also ingest raw logs from the data sources themselves.

As you migrate detections and build out your use cases in Azure Sentinel, always be mindful of the data you ingest and verify its value to your key priorities.

Best practice: Migrating detection rules

Another key task for your migration involves translating existing detection rules into those that map to Azure Sentinel (view the full blog post for more information). Azure Sentinel provides a powerful query language, Kusto Query Language (KQL), that can be used across other Microsoft solutions, such as Microsoft Defender for Endpoint and Application Insights.

Azure Sentinel has four built-in rule types:

Alert grouping
The goal of alert grouping is to reduce alert fatigue by grouping up to 150 alerts occurring within a given timeframe. Azure Sentinel has three options for grouping: matching entities, alerts triggered by the scheduled rule, and matches of specific entities.

Entity mapping
This enables SOC engineers to define entities as part of the evidence to be tracked during the investigation. Entity mapping also makes it possible for SOC analysts to take advantage of the intuitive Investigation Graph to reduce time and effort compared to legacy SIEMs.

Evidence summary
This feature surfaces events, alerts, and any bookmarks associated with a particular incident within the incident preview pane. Additionally, entities and tactics also show up in the incident pane. This provides a snapshot of essential details needed by an analyst to judge how to begin a particular investigation; making it easier to conduct triage.

Kusto Query Language
KQL is based on read-only requests to process data and return results. The request is sent to a Log Analytics database and is stated in plain text, using a data-flow model designed to make the syntax easy to read, author, and automate. Because several other Microsoft services also store data in Azure Log Analytics or Azure Data Explorer, this reduces the learning curve needed to query or correlate, regardless of the source.

Rule migration flow

Rule migration across SIEMs requires a clear strategy and a detailed implementation plan to achieve your business goals while reducing security risks. The rule-migration/process-flow diagram shown here provides an overview of key elements, decision points, and interrelationships among the steps.

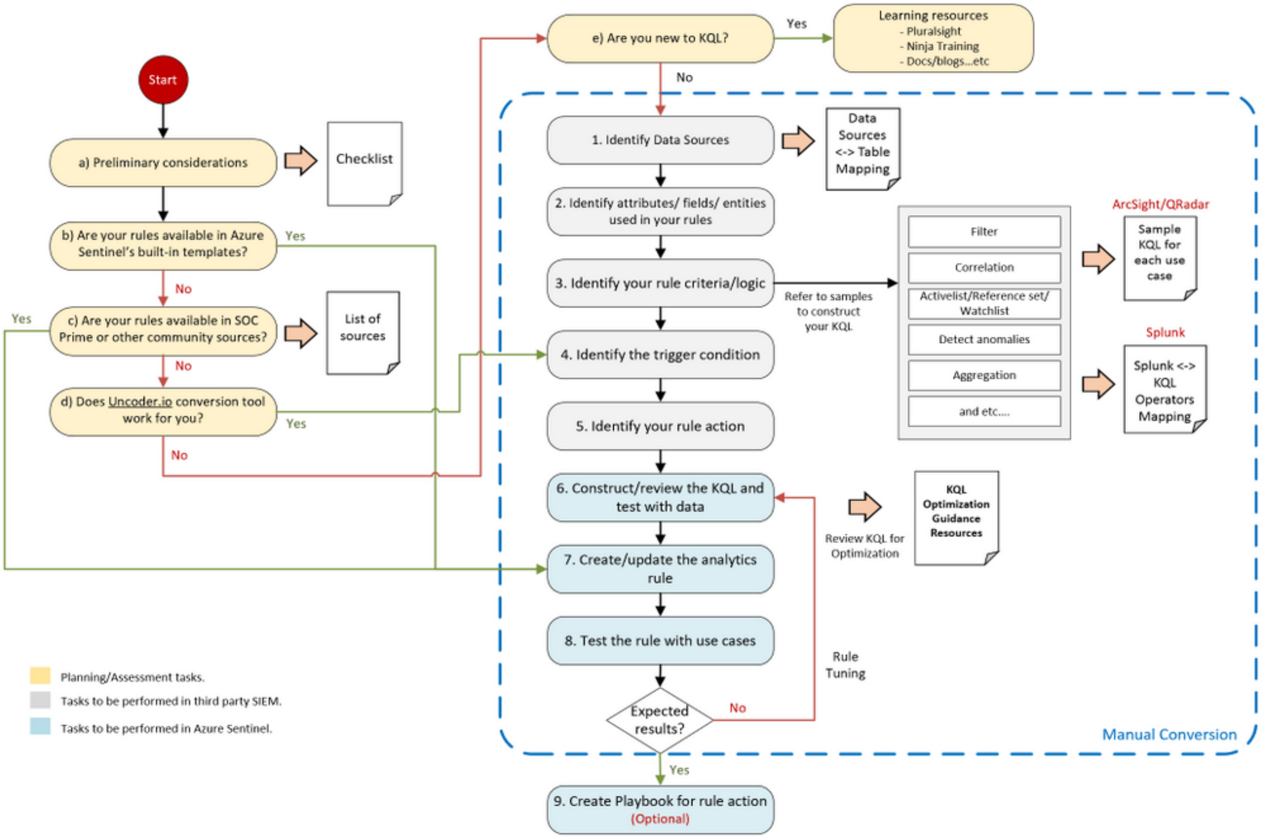

Start
a) Preliminary considerations
Checklist
b) Are your rules available in Azure Sentinel's built-in templates?
Yes
No
c) Are your rules available in SOC Prime or other community sources?
Yes
List of sources
No
d) Does Uncoder.io conversion tool work for you?
Yes
No
e) Are you new to KQL?
Yes
Learning resources
- Pluralsight
- Ninja Training
- Docs/blogs...etc
No
1. Identify Data Sources
Data Sources <-> Table Mapping
2. Identify attributes/ fields/ entities used in your rules
3. Identify your rule criteria/logic
Refer to samples to construct your KQL
Filter
Correlation
Activelist/Reference set/ Watchlist
Detect anomalies
Aggregation
and etc....
ArcSight/QRadar
Sample KQL for each use case
Splunk
Splunk <-> KQL Operators Mapping
4. Identify the trigger condition
5. Identify your rule action
6. Construct/review the KQL and test with data
Review KQL for Optimization
KQL Optimization Guidance Resources
7. Create/update the analytics rule
8. Test the rule with use cases
Rule Tuning
Expected results?
No
Yes
Manual Conversion
9. Create Playbook for rule action (Optional)
Planning/Assessment tasks.
Tasks to be performed in third party SIEM.
Tasks to be performed in Azure Sentinel.

Figure 2: Rule migration process flow

When planning your detection migration, create checklists and important points to consider before you begin the rule-migration steps. Also, include useful resources to help prepare your team for the journey. Because Azure Sentinel uses ML analytics to produce high-fidelity and actionable incidents, it's likely that some of your existing detections won't be required anymore.

Remember:

- Don't migrate all the rules blindly; focus on quality, not quantity.
- Leverage available resources. Review all the [Azure Sentinel built-in rules]() to identify out-of-the-box rules that can address your use cases. Explore community resources such as [SOC Prime Threat Detection Marketplace]().
- Confirm connected data sources and review data connection methods. Revisit data collection conversations to ensure data depth and breadth across the use cases you plan to detect.
- Ask yourself: What problems are we trying to solve? Select use cases that justify rule migration in terms of business priority and efficacy:
    - Review rules that haven't triggered any alerts in the last 6 - 12 months and determine whether they're still relevant.
    - Eliminate low-level threats or alerts you routinely ignore.
    - Prepare a validation process: Define test scenarios and build a test script to be used for rule validation.

Learn More: For detailed guidance on the rule migration process, including specifics on how to migrate detection rules from a variety of other SIEMs, view our **rule migration best practices**.

Leveraging automation

Automating workflows can streamline both common and critical tasks for your SOC. Where do you really need to save time? Automated workflows enable you to group and prioritize alerts into a common incident, then modify its priority. Also, automated playbooks in Azure Sentinel enable easy integration with third-party ticketing solutions, such as ServiceNow.

But automation isn't just about running tasks in the background. From within the investigation, your SOC team can use an automated playbook to gather additional information or apply remediation action; helping an analyst to accomplish more in less time. You're also free to iterate and refine over time, moving to full automation for response. Browse the GitHub playbooks to get new ideas and learn about the most common automation flows.

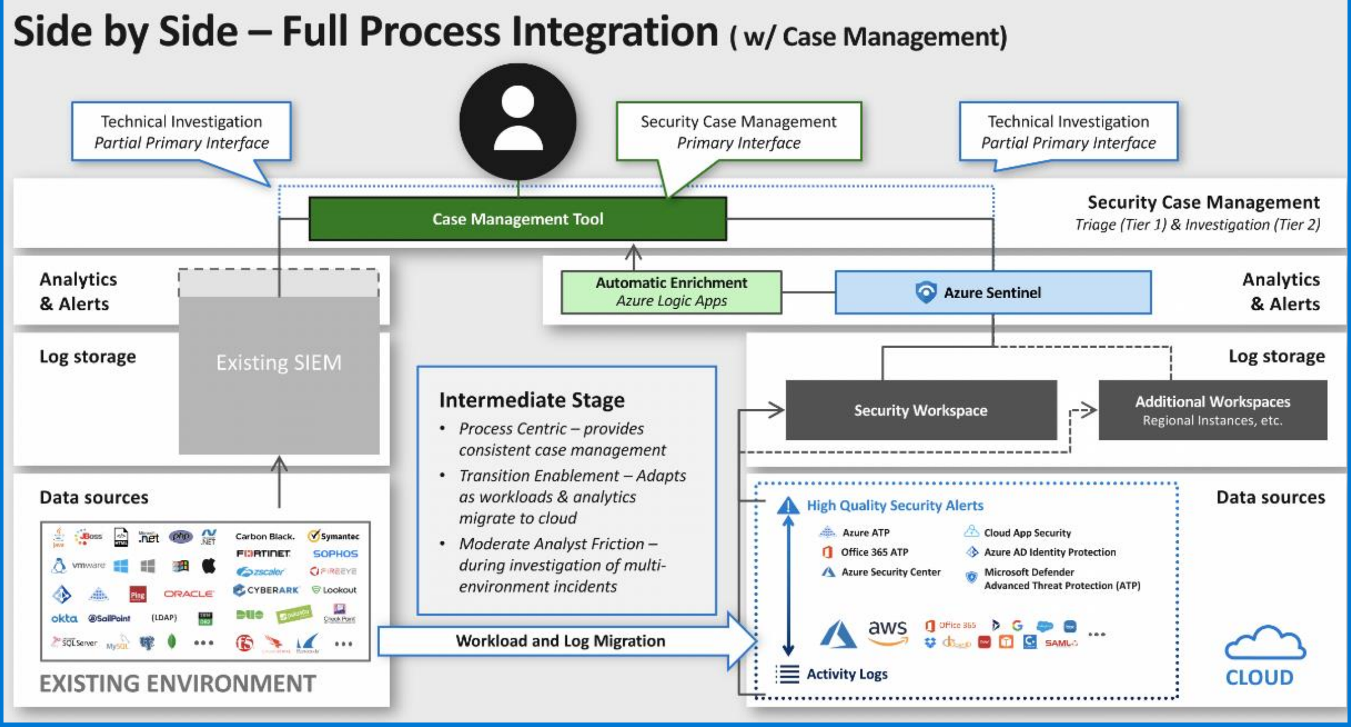


Figure 3: Side-by-side deployment—full process integration

STEP
4

STEP 4: Finishing the migration (retiring the legacy SIEM)

Why should you retire your old SIEM? By moving completely to Azure Sentinel, your organization may enjoy significant savings on infrastructure, licensing, and staff hours. Additional benefits of fully transitioning to Azure Sentinel include a SecOps team that is:

Process centric	Fully modernized	Savings enabled	Friction reduced
A unified SIEM solution allows for consistent case management.	Azure Sentinel applies machine learning, threat intelligence, and behavior analytics across all your data sources, both on-premises and in the cloud.	Retiring the legacy SIEM enables reduced infrastructure, licensing, and staff costs.	Keeping analysts trained on multiple SIEMs can be challenging. By migrating completely to Azure Sentinel, your SOC can now create queries and conduct threat hunting from a single pane of glass.

Checklist for retiring your legacy SIEM

Based on your criteria, P0 priorities, and the use cases that you've defined throughout this migration process, you'll develop a strong sense of when you're ready to retire your legacy SIEM. Still, making the break from your legacy SIEM completely requires that you've fulfilled several criteria across technology, processes, and people.

Based on our experience, we find that customers are ready to retire their legacy SIEMs once the following requirements have been fulfilled:

Technology

- **Check critical data:** Make sure sources and alerts are available in Azure Sentinel.
- **Archive all records:** Save critical records of past incidents and cases (raw data optional) to retain institutional history.

Processes

- **Playbooks**: Update investigation and hunting processes for Azure Sentinel.

- **Metrics:** Ensure that all key metrics can be obtained completely from Azure Sentinel. Create custom workbooks, or use built-in workbook templates to quickly gain insights as soon as you connect to data sources.
- **Cases:** Make sure all current cases are transferred to the new system (including required source data).

People

- **SOC analysts:** Make sure everyone on your team is trained on Azure Sentinel and feels comfortable leaving the legacy SIEM.

What next?

You're invited to explore Microsoft's resources for Azure Sentinel, all of which are designed to expand your skills and help you get the most out of Azure Sentinel's capabilities.

Expand your Azure Sentinel skills

Become an Azure Sentinel Ninja with the complete 400-level training. This training program includes 16 modules covering workspace and tenant architecture; workbooks, reporting, and visualization; KQL; and much more.

Visit Microsoft Learn courses to further familiarize yourself with Azure Sentinel and its capabilities. Check out the Azure Sentinel Learning Path to get more information about security incident management, threat hunting, connecting data sources, and more.

Get certified with the SC-200 Microsoft Security Operations Analyst certification. This exam measures your ability to work with Azure Sentinel, as well as Microsoft 365 Defender and Azure Defender.

Improve your SOC efficiency

Learn more about utilizing automation features, including how automation rules can deliver more streamlined orchestration.

Continue to measure and improve your SOC efficiency in Azure Sentinel with built-in efficiency tools, like the SOC efficiency workbook. Learn more about optimizing your SOC efficiency with Azure Sentinel.

Expand your threat detection with integrated SIEM & XDR

Once you've moved onto Azure Sentinel, consider the increased threat protection you'll gain by using it alongside Microsoft 365 Defender and Azure Defender for integrated threat protection. With this combination, you'll benefit from the breadth of visibility that Azure Sentinel delivers while easily diving deeper into detailed threat analysis. See how the process works in this interactive guide.

Coming soon…

The Azure Sentinel Migration Cookbook—an all-in-one guide for technical guidance that takes you from start to finish in your migration.

References and further reading

More about Azure Sentinel

Azure Sentinel on Azure.com

The Total Economic Impact™ Of Microsoft Azure Sentinel

The Forrester Wave™: Security Analytics Platforms, Q4 2020

Azure Sentinel learning resources

Azure Sentinel documentation

Azure Sentinel interactive guide

Investigating a hybrid attack with Azure Sentinel

Microsoft Security Technical Content Library

Azure Sentinel MS learning paths

More migration guidance

Running Azure Sentinel side by side with Splunk

Running Azure Sentinel side by side with QRadar

How to export data from Splunk to Azure Sentinel

Sending enriched Azure Sentinel alerts to third-party ticketing systems

Webinar: Best Practices for Converting Detection Rules

More best practices

Become an Azure Sentinel Ninja: The Complete 400 Level Training

Azure Sentinel: An end-to-end SOC scenario

Azure Sentinel Technical Playbook for MSSPs

Azure Sentinel Best Practices: Strategies for success in data ingestion and incident response

KQL learning resources

KQL online course: The Basics of Kusto Query Language | Pluralsight

SC-200 part 4: Create queries for Azure Sentinel using Kusto Query Language (KQL) - Learn | Microsoft Docs

Azure Sentinel webinar: KQL part 1 of 3 - Learn the KQL you need for Azure Sentinel – YouTube

Microsoft Azure Data Explorer - Advanced KQL

Other resources

Top 7 Case Management Tools in 2020

MITRE ATT&CK®

Managing and Responding to Security Events Using Azure Sentinel | Pluralsight

Appendix

Terminology

SIEM: Security information and event management

SOAR: Security orchestration and automated response

SOC: Security operations center

SecOps: Security operations

ML: Machine-learning

On-premises SIEM architecture: The classic model with analytics and database functions both residing on-premises.

Side-by-side architecture: In this configuration, an on-premises SIEM is used for local resources, while cloud-based analytics are often used for cloud resources or new workloads. This side-by-side model can use native cloud analytics or infrastructure as a service (IaaS). Cloud-native is preferable to IaaS because of its reduced need for infrastructure management.

Cloud-native architecture: In this model, both security analytics and data storage use native cloud services.

Alert: technical indicator of anomalous activity

Event log: Raw data on activity in the environment

Case ticket: Process elements for managing incidents (owner, activity history, etc.)

Incident: Discrete adversary attack operation

MTTR: Mean time to remediate

MTTA: Mean time to acknowledge

KQL: Kusto Query Language