



Solving Key Challenges for Multi-Vendor Security Environments

A guide to overcoming security burnout and bolstering
your defenses with Insight and Microsoft Sentinel

Security under stress

42%

of respondents in Cisco's 2020 CISO Benchmark Survey say they are suffering from cybersecurity fatigue (defined as virtually giving up on proactively defending against malicious actors).

Of those suffering, 93% receive more than

5,000 alerts every day,

indicating that complexity appears to be one of the main causes of security burnout.¹

To manage a complex threat environment, most organisations are leveraging several security solutions. But managing and orchestrating alerts from several disparate sources is not only challenging — it also exposes organisations to more risk.



An overabundance of alerts means there may be simply too many to address, impacting the team's awareness and visibility, and potentially exposing the business to bigger, more damaging threats down the road.

According to Fady Younes, cybersecurity director at Cisco, "Failure to integrate multiple security solutions can also leave gaps in coverage, or create a situation where the IT team doesn't properly understand what protection a particular solution is providing or how it works, impacting visibility and awareness into the true security state of the network."²



Knowing which risks and alerts to prioritise becomes less clear in these environments.

Not all alerts are of the same severity, and the best security strategies tailor security controls and allocate resources based on risk level.



In diverse, multicloud environments, disaster recovery becomes incredibly complex, necessitating a proactive vs. reactive security culture.

"Dealing with integration issues and a high volume of security alerts can distract security engineers from tackling other challenges they face..."

— Fady Younes, Cybersecurity Director, Middle East & Africa at Cisco

SIEM and SOAR

Security teams have two main objectives: to know what's going on in their IT environments, and to respond to that information. Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) solutions exist to help achieve these goals.



SIEM tools gather and aggregate event data from various sources within an IT environment, then analyze and rank events in order of priority or criticality. Security teams carry the responsibility of threat hunting and response, as well as tuning and remediation of the SIEM platform.

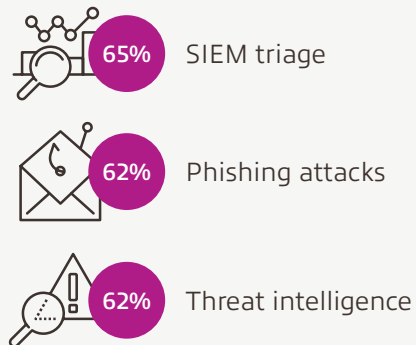


SOAR tools provide advanced analytics and automation that builds on the capabilities of SIEM tools, for more autonomous threat response. SOAR tools leverage as much real-time data as possible and are sensitive to the proficiency of managers — these tools are more or less effective based on how they're used.



say **SOAR** is very or extremely
important to their organisation's
overall security posture.

Key use cases for SOAR:



Outcomes from SOAR deployments:



What sets Microsoft Sentinel apart?

“SOAR is the functionality of Sentinel that differentiates it from competitors. It allows security teams to write code or playbooks within Sentinel to automatically respond to threats as they come in — helping the SOC team reduce alert fatigue and focus on things you actually need to focus on.

Our clients really like that you can cross-correlate alerts and incidents, drawing a map of each incident associated with a specific entity. What I'll typically show clients in a demo is a scenario where a random attacker has gained access to the environment, elevated their privileges, performed a mass download of business data, and then deleted their account. Those are four separate alerts that you'd get within any SOAR or a SIEM. But within Microsoft Sentinel, you can see a graph of one entity with four different lines to each alert they've generated, as well as a chronological timeline of those events. Microsoft Sentinel really makes threat hunting easier.”

— Associate Consultant, InfoSec, Insight

The case for Microsoft Sentinel

Microsoft Sentinel™ combines the power of a SIEM and a SOAR into one solution. If you've already invested in Microsoft® Sentinel, you're on the path to stronger security.

The Sentinel platform can help you:



Identify threats before they impact your business.



Respond quickly and with more accuracy.



Simplify security across hybrid, multicloud, server-less, and other modern environments.



Reduce costs over legacy SIEM solutions for threat investigation, licensing, storage, infrastructure, management, and deployment.

The tool is built upon Microsoft's deep experience in security and the latest artificial intelligence capabilities, and works harmoniously with other Microsoft products. It's quick to set up and easy to scale.

One hub, many data points

Multi-vendor solution environments become less complex to manage with Microsoft Sentinel. Sentinel's ability to pull data sources from the entire ecosystem of multi-vendor security solutions gives organisations visibility and control to simplify threat hunting, reduce alert fatigue, and capture a true picture of your security posture.

Best practices for implementation

Getting started with Microsoft Sentinel is relatively simple. Prior to implementation, we advise establishing clear governance and policies. Considerations include compliance standards, cost requirements, plans for storage, disaster recovery, security team staffing, and incident response plans.

Day 1:



Enable Microsoft
Sentinel.



Connect data
sources.



Start building queries to
investigate the data.

Like many other SIEM tools, Syslog and CEF serve as ingestion points. You may use any Linux® distro preferred, including Microsoft's own Linux distro, and install CEF and Syslog forwarders to forward logs to Microsoft Sentinel for ingestion.

Microsoft has built Sentinel to accommodate generic formatting logs in common event format as well, so that even logs from legacy or specialised devices can be integrated and analyzed.

Secure across the board.

Microsoft Sentinel is most effective when part of a broader, programmatic approach to cybersecurity. Make sure your organisation is employing best practices across the entire cybersecurity spectrum: Identify, Protect, Detect, Respond, and Recover.

INSIGHT SOLUTION

Mitigate risk and protect your organisation.

Insight has a robust security practice and the pulse on the IT security landscape. We have helped organisations secure their data and networks for more than 30 years. As a group of advisors, solution providers, and technical specialists, we maintain certification and immersion in the latest security technologies and best practices.



Day 2+:

The flexibility and dynamism of the platform will become evident at this point. Here are several ways you can drastically maximise Microsoft Sentinel's benefits for your organisation's specific needs and risk profile.

1.

Check your log forwarders.

If you don't pay close attention to the health of your log forwarder and the capacity of your VAR log directory, things can quickly break down and log ingestion will cease. When Insight consultants perform Microsoft Sentinel deployment, we use Linux distros with a partition for the VAR log mount point that's separate from the OS. This way, if the directory fills up, it doesn't impact the OS as much.

3.

Minimise false positives.

Many out-of-the-box rules that report on administrative functions using behavior analytics can generate false positives. Microsoft has published a Sentinel feature called Watchlist to help reduce these false positives, the resulting noise, and alert fatigue. Watchlist lets you bake queries (or CSVs of different attributes) into analytics rules that examine a watchlist, or key identifier pair, and does not alert on specific activities.

2.

Look at your ingestion rates.

Estimating how many logs you may ingest right at the beginning is difficult — but after a month or two, you'll have enough historical data to support better decision-making around an appropriate data ingestion rate. This will help you attain a better cost output.

4.

Use a centralised tenant.

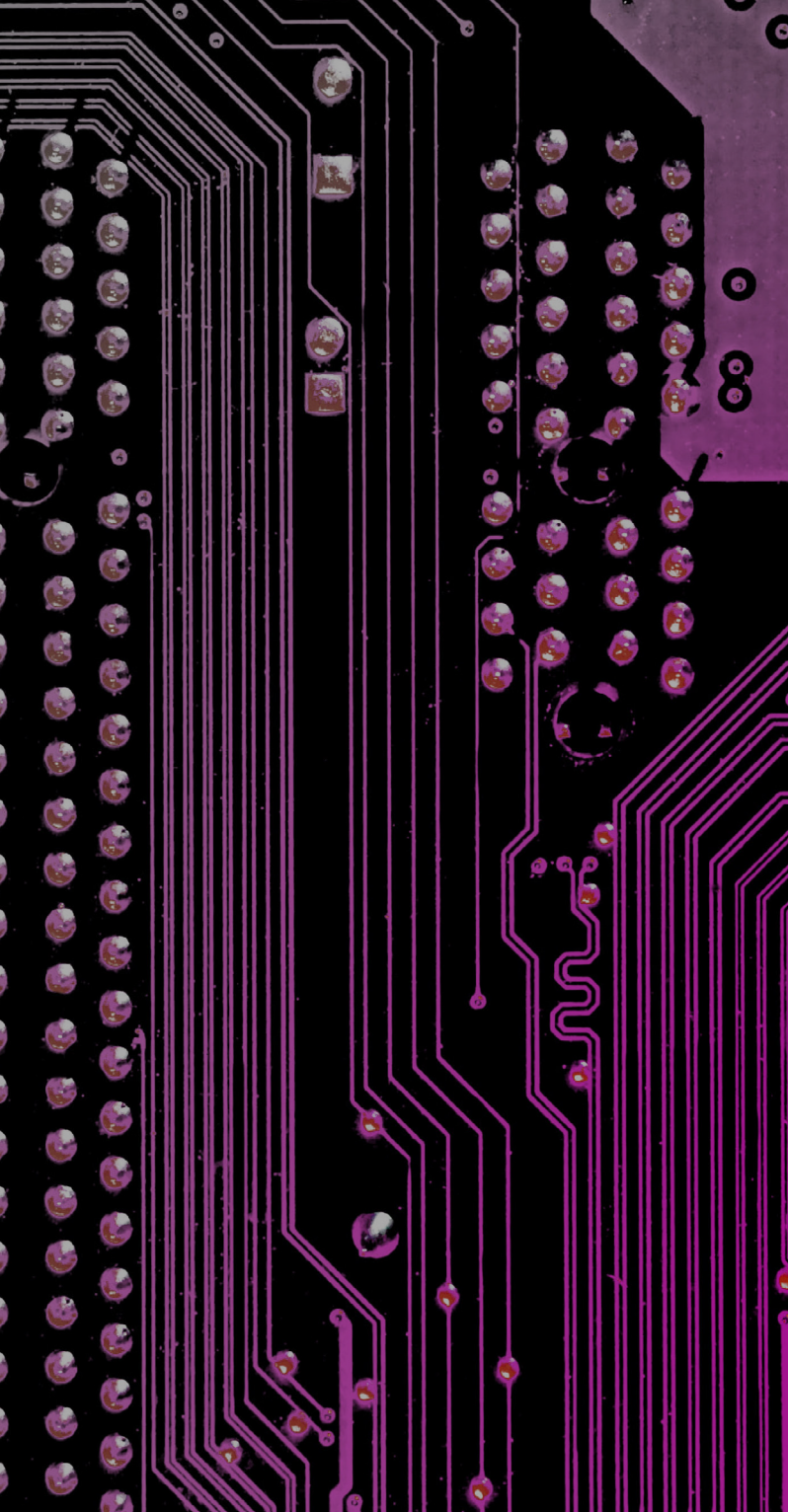
If you're monitoring different Azure® tenants, you need to create different Microsoft Sentinel installs and log analytics workspaces in each of those tenants. By using Azure Lighthouse to monitor these workspaces in a centralised tenant, you can tune analytic rules, get to the source of truth, and deploy rules to all tenants. This will help you establish a consistent baseline for thresholds, running frequency, and other settings.



Did you know?

If you use Microsoft Sentinel, any data from Microsoft infrastructure — Office 365®, Microsoft Azure, etc. — does not have to be ingested and is therefore free.

This is a major price advantage over other SIEM and SOAR solutions in which every message incurs costs. Organisations can also leverage Microsoft storage for more affordable retention solutions.



5.

Perform out-of-the-box detuning.

Microsoft Sentinel offers the distinct benefit of integrating fluidly with your Microsoft ecosystem. Our consultants regularly advise clients to use Microsoft Defender for Identity (MDI) for on-premises Active Directory® (AD), for example. However, when you plug MDI into Sentinel, the default setting will automatically forward all alerts coming out of MDI. You'll likely want to go into the plugin connector and detune it so that you aren't being alerted on non-urgent information and only receive alerts within a specified severity range.

Also examine the severities of existing analytic rules and escalate, deescalate, or remove them, based on your needs. Many out-of-the-box analytic rules run on a set frequency that may be too often to manage. We advise using analytic rules running every 15 or 30 minutes for high-severity alerts, and running them just once a day for low-severity or informational alerts that don't carry much business impact. Ultimately, detuning will help you minimise alert fatigue and noise.

6.

Evaluate for parity.

What were you using to secure your IT environment prior to Microsoft Sentinel? What are the similarities and differences? Our consultants suggest looking side by side at your old system and the Microsoft Sentinel environment and comparing visual output, dashboards, alerts, log sources, and other key attributes to ensure you're getting parity. No data source should be left behind. This also helps you ensure that you fully understand the new scope of day-to-day tasks, care and feeding, and staffing requirements for supporting the new platform.

7.

Consider Microsoft's guidance.

Microsoft has published recommendations for regular activities to perform to ensure Sentinel is giving you the best security possible. Review them for suggestions on daily, weekly, and monthly tasks, integrations to set up, and processes for managing and responding to incidents.

Opportunities for automation

One of the strengths of the Microsoft Sentinel platform is its automation capabilities. Take advantage of automation to achieve optimal efficiency and security.

Here are a couple of ways you can automate with Sentinel:

Retention

Every organisation has different needs surrounding data retention, based on industry and legal and compliance requirements. Microsoft Sentinel offers the ability to automate storage for set periods of time — making it incredibly easy for your team to tick that box without having to set reminders or worry about capacity.

Playbooks

For more intricate automations, playbooks are an excellent option. Playbooks within Microsoft Sentinel can be set up for a range of tasks, such as:

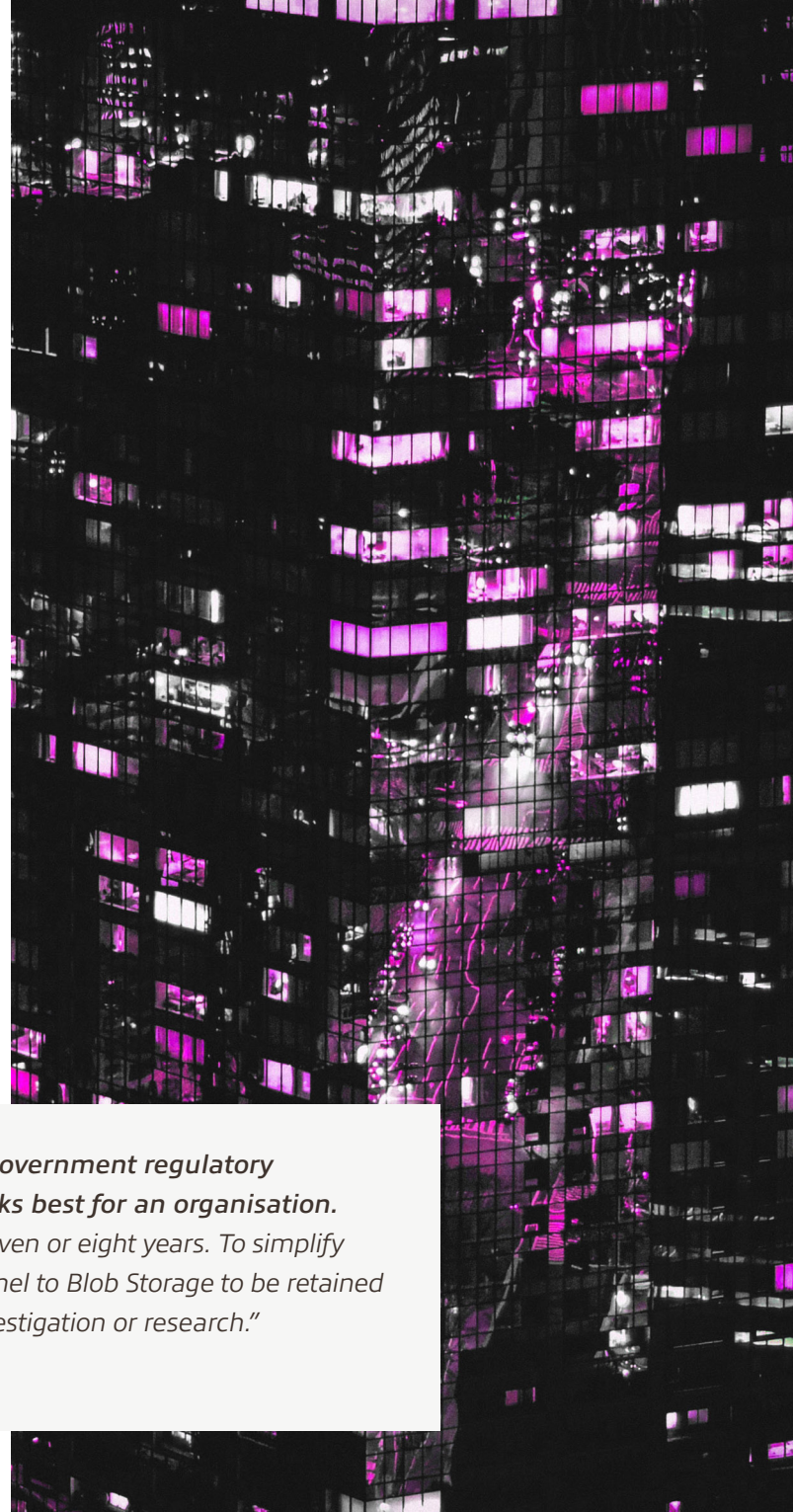
- Blocking a user after a failed login alert
- Creating a ServiceNow® incident that feeds into your ticketing system
- Modifying the CMDB in ServiceNow upon changes to blocked devices on the network

Microsoft-owned GitHub hosts many playbooks and ideas for customisations, as well as vendor-specific automations within Microsoft Sentinel to explore.

“

We have clients that want seven years of data retention for HIPAA, or one year for a government regulatory compliance or NIST, let's say. It's a challenge to figure out what retention scheme works best for an organisation. Microsoft's Blob Storage is a good option — it lets you cost-effectively retain logs for up to seven or eight years. To simplify this, we create Azure Logic Apps that automatically move ingested logs from Microsoft Sentinel to Blob Storage to be retained for seven years. Organisations still have access to the logs if they're needed for a security investigation or research.”

— Associate Consultant, InfoSec, Insight





Looking ahead

There are countless ways to expand and enhance Microsoft Sentinel — and the opportunities keep growing as the platform and user community mature.



BYO ML

Bring Your Own Machine Learning (BYO ML) is an area that's getting a lot of attention. This [Microsoft GitHub page](#) acts as a repository for the latest information and a growing library of sample training notebooks. Organisations are using BYO ML to spin up Databricks and bring training and analytics through a Spark environment pulling all data from Sentinel, building models for remote access or anomalous behavior, and so much more.



***You don't have to be a Ph.D. to be doing this.** A lot of the community-based training and models are a pretty good approximation that just need to be customised for your environment. Other SIEMs have something similar to this, but the idea that you can have a very data science-native experience, where you basically have a Jupiter notebook, a bunch of Python data science libraries, and you're pulling data directly from the environment where the notebook is running — that is pretty interesting to me."*

— Principal Architect (Cybersecurity, Networking, Data Science), Insight



Advanced visualisation

Azure Monitor Workbooks within Microsoft Sentinel offer rich data visualisation. Of course, this is extremely useful for security teams. Seeing the data can make it easier to identify points of weakness and vulnerabilities, helping security teams prioritise. Visualisation can also help security teams justify budgets to the C-suite with quick impact. In the future, we believe data visualisation will be a key focus, with communities of users developing custom workbooks to address any security or business need.

INSIGHT SOLUTION

Our Security Services consultants can help you consider the security implications of your business activities and adopt solutions aligned with your needs and objectives. We begin by assessing your current environment, challenges and requirements.





Managed services

Due to a lack of time and resources, today's organisations are only able to remediate



50%

of legitimate security threats.¹

Many organisations are finding it difficult to attract and retain experienced security professionals who are up to date on the latest SIEM, SOAR, and Security Operations Center (SOC) tool sets. We're already seeing an overall consolidation of security talent within services organisations that can proficiently manage security environments — as well as provide critical support around ransomware readiness, security architecture, incident response, and remediation.

In many instances, time management is the central challenge. Learning about ways to increase automation or leverage machine learning to improve threat hunting may be overshadowed by the countless day-to-day demands of running a security team.

The key to amplifying your security? Managed services.

Insight offers Managed Security Services (MSS) that build on the capabilities of Microsoft Sentinel and provide 24/7 monitoring of your environment. By combining industry-hardened best practices with cutting-edge techniques for risk minimisation, we help clients offload the heavy burden of caring for and enhancing a dynamic security environment.

An advanced approach.

Our Security Services consultants can help you consider the security implications of your business activities and adopt solutions aligned with your needs and objectives. We begin by assessing your current environment, challenges, and requirements.

16 years

of incident
and threat
management
experience

1,500+

architects, engineers
& subject matter
experts in security
& service delivery

Managed security outcomes:



Faster response times



Stronger governance
and compliance



Richer context and visibility



Improved threat detection



Reduced security team burden

Sky's the limit

Microsoft Sentinel is easy to implement — but takes additional skill to optimise well.

Luckily, there are few limits to how far the platform can take you toward complete security — and with a trusted team such as Insight, it's easier than ever to unearth the value of your investment. Our consultants, technicians, and architects have industry-leading expertise around Microsoft Sentinel across a wide variety of client environments.

No matter where you are along the Sentinel path, you can leverage Insight for:



Evaluation of your current security environment



Managed Security Services to manage Microsoft Sentinel



A Microsoft Sentinel readiness assessment



Microsoft Sentinel optimisation, automations, and advanced feature tuning



Microsoft Sentinel deployment, integration, and customisation

Contact our team today to discuss your needs

About Insight

Insight Enterprises, Inc. is a Fortune 500 solutions integrator with 11,500 teammates worldwide helping organisations accelerate their digital journey to modernise their business and maximise the value of technology. We enable secure, end-to-end transformation and meet the needs of our clients through a comprehensive portfolio of solutions, far-reaching partnerships and 33+ years of broad IT expertise. Rated as a Forbes World's Best Employer and certified as a Great Place to Work, we amplify our solutions and services with global scale, local expertise and a world-class e-commerce experience, realising the digital ambitions of our clients at every opportunity.

Learn more at: uk.insight.com



Sources:

¹ Cisco. (2020). Securing What's Now and What's Next: 20 Cybersecurity Considerations for 2020. CISO Benchmark Survey.

² Younes, F. (2021, Jan 21). Complexity Still Remains Cybersecurity Worst Enemy. Techeconomy.ng.

³ Rockett, J. (2020, June 25). 2020 SOAR Report Highlights Key Drivers and Impacts. Swirmlane.