AUJAS CYBERSECURITY
An NSEIT Company

Microsoft Sentinel

Transform your security operations center with **Aujas powered Sentinel**

e-Book

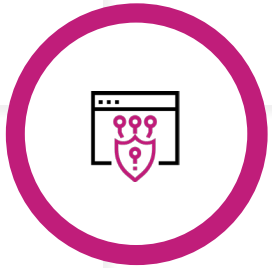
Traditional SIEMs are inefficient

Cyberattacks are increasing in frequency and intensity, with criminals taking advantage of evolving strategies and vulnerabilities. Even simple ransomware can now take down entire networks. Security teams need new ways to integrate cybersecurity with business continuity strategies.

Traditional Security Information and Event Management (SIEM) solutions, once the backbone of organizational security, are struggling to meet modern demands. These legacy systems face several critical limitations:

Scalability issues in the face of exponential data growth.

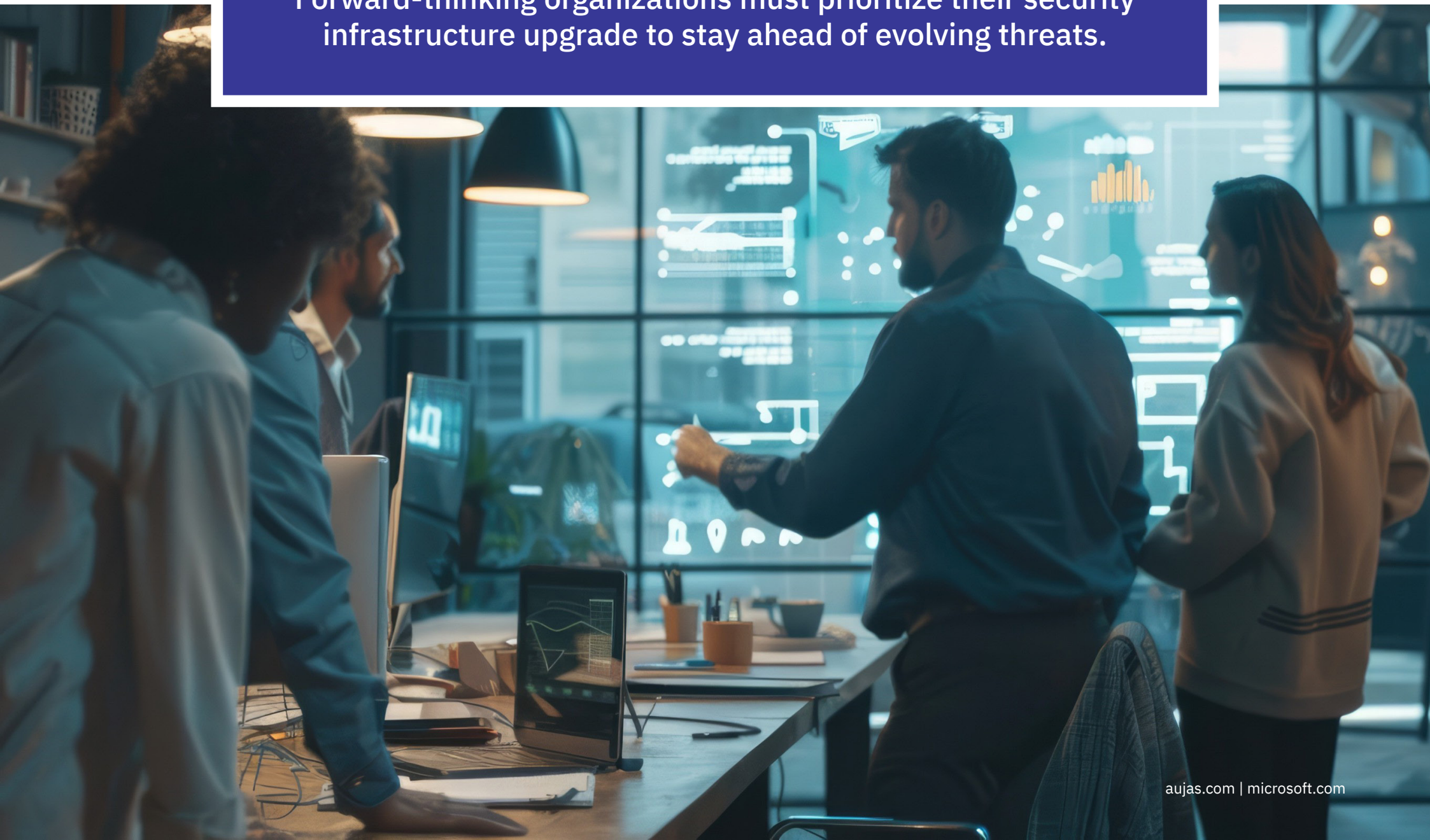
Limited capabilities in detecting and responding to advanced threats.



High costs associated with maintenance and expansion, particularly in terms of data storage.

Operational silos leading to potential security blind spots.

Forward-thinking organizations must prioritize their security infrastructure upgrade to stay ahead of evolving threats.



Why Cloud SIEM is better?

SIEM Model	Overhead Cost and Expense	Operational Efficiency	Control and Ownership	Real-time Visibility and Security	Support and Maintenance
On-Premise	▲ Higher	▼ Lower	▲ Higher	▼ Lower	▼ Lower
Cloud Native SIEM	▼ Lower	▲ Higher	▼ Lower	▲ Higher	▲ Higher

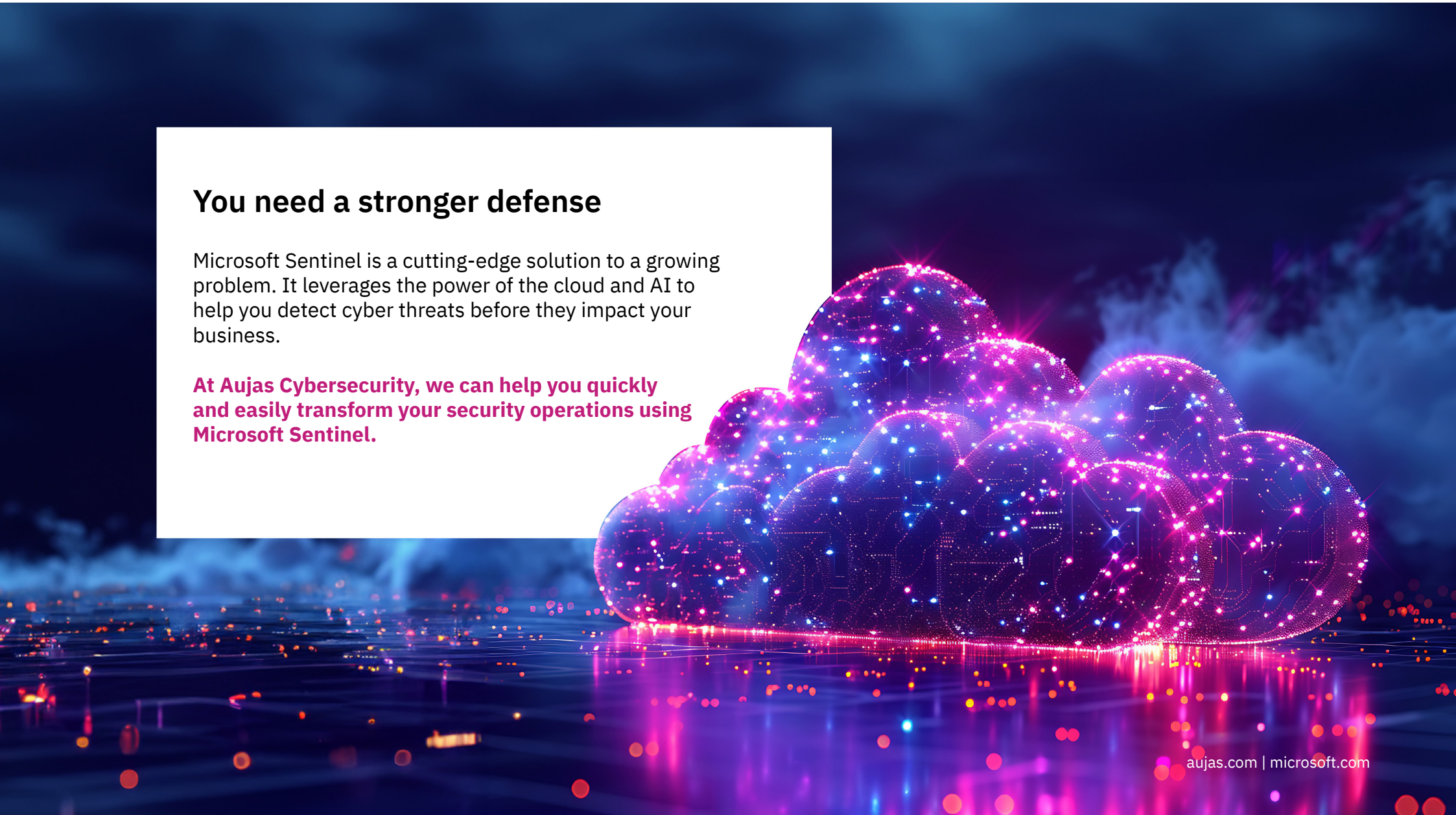
Outdated SIEM solutions in your Security Operations Center (SOC) can be a significant bottleneck, creating excessive workloads and elevating risk levels. The vast amounts of generated data can overwhelm your security teams, forcing them to rely heavily on manual analysis while sifting through countless alerts—many of which are false positives.

The Impact:

Your SOC may be missing critical insights due to:

Incomplete visibility	**Lack of contextual awareness**	**Inability to handle big data**	**No threat intelligence integration**	**Slow analysis and limited integration**
Gaps in monitoring can leave threats undetected.	Alerts without context make it harder to prioritize real threats.	Struggling to process large volumes of data efficiently.	Missing out on crucial external threat data.	Delayed response times and difficulty integrating with other tools.

Addressing these issues is vital to enhance your SOC's effectiveness and safeguard your organization against evolving threats.



You need a stronger defense

Microsoft Sentinel is a cutting-edge solution to a growing problem. It leverages the power of the cloud and AI to help you detect cyber threats before they impact your business.

At Aujas Cybersecurity, we can help you quickly and easily transform your security operations using Microsoft Sentinel.

Aujas powered Microsoft Sentinel: the next-gen SIEM solution

Aujas MDR provides comprehensive 24x7 incident management services and offers transformational services through Next-Gen Cyber Defense Center (CDR) capabilities in an increasingly complex technology landscape.

Aujas Cybersecurity is deeply involved in the security space, and as a technology advisor to businesses, we recommend Microsoft Sentinel. Microsoft Sentinel is a next-generation, cloud-native SIEM solution that utilizes the power of AI, automation, and deep-threat intelligence. It is designed to be proactive rather than reactive. Our customers using Microsoft Sentinel have a solution that helps protect large digital estates before threats occur—and it works across data, apps, infrastructure, or any custom data or use case.

Unlike traditional SIEM solutions with scalability and integration issues, Aujas leverages Microsoft Sentinel for real-time monitoring, to detect and respond to threats across complex, hybrid environments. This unified Security Operations platform for your SOC team provides a complete view of the entire data estate in one location enabling them to efficiently hunt and resolve critical threats at machine speed.

Microsoft Sentinel is highly integrated with Microsoft XDR solutions—Microsoft 365 Defender, Microsoft Defender for Cloud, and Microsoft Defender for IoT. This integration keeps incidents synchronized between both portals for complete visibility from within Microsoft Sentinel.

25+

ASC Trained
Professionals

30+

Azure Sentinel
Trained Professionals

140+

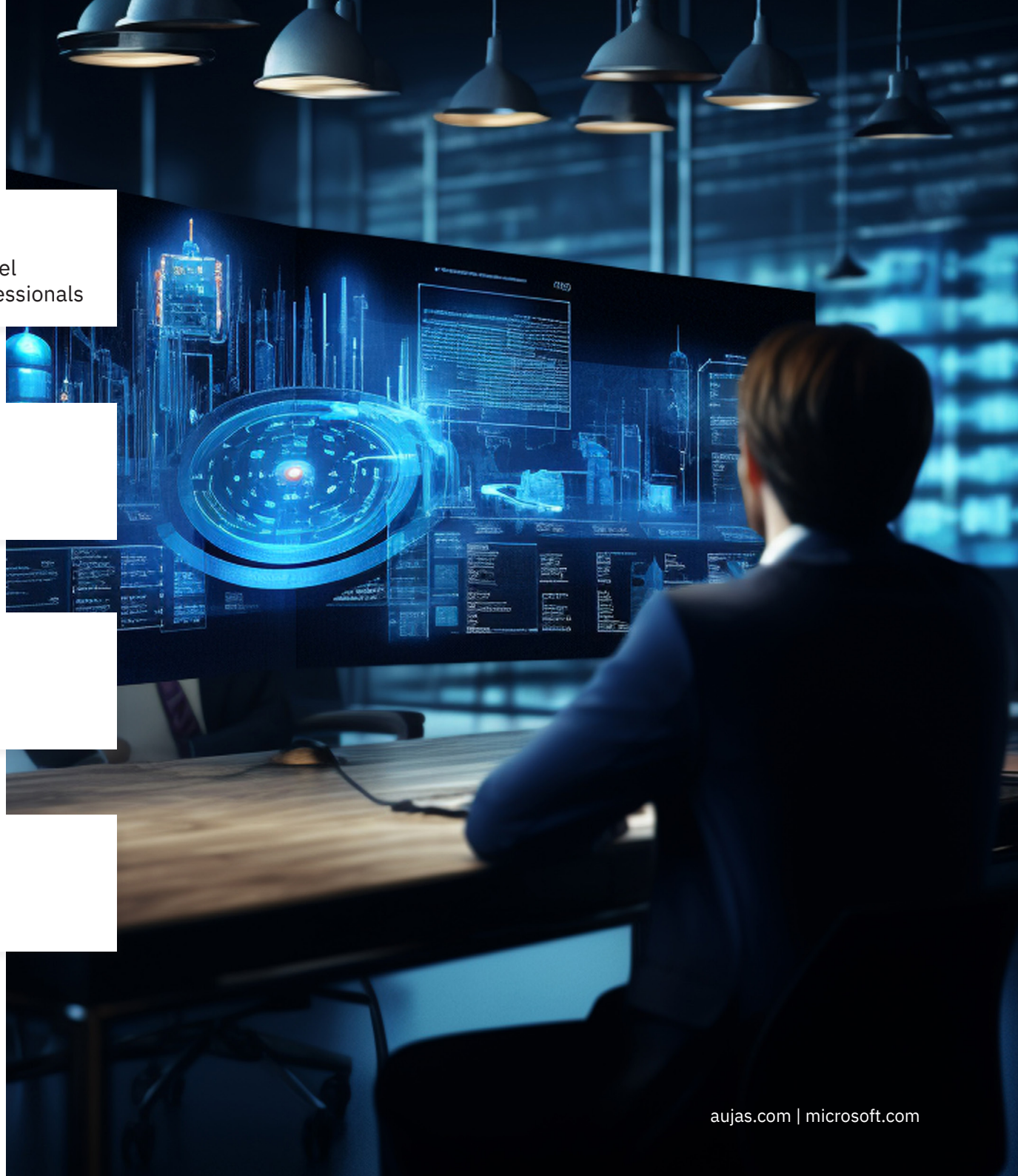
NextGen Cyber Defense
Professionals (includes MS)

15+

AZ500 Certified
Professionals

15+

Microsoft ATP
Trained professionals



aujas.com | microsoft.com

Why Aujas Cybersecurity for your SOC?

Aujas MDR delivers comprehensive 24x7 incident management services and offers transformational services through Next-Gen Cyber Defense Center (CDR) capabilities in an increasingly complex technology landscape.

2.7 Billion/day

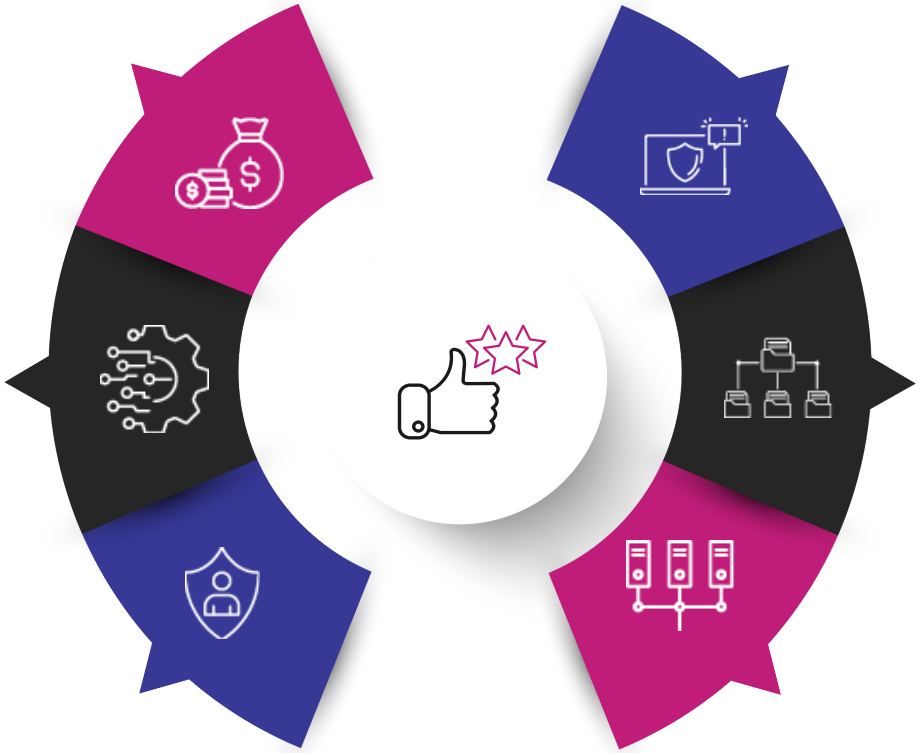
Events analysed for large SIEM & security analytics installations

350+

Custom parsers developed to integrate niche log sources

200+

Security defense Professionals



80+

Security certified professionals

700+

Use cases designed for security monitoring scenarios

2

Global CDCs
India: Mumbai, Bangalore

Help protect your digital estate

Secure more of your digital estate with scalable, integrated coverage for a hybrid, multi-cloud, multiplatform business.

Empower your SOC with Microsoft intelligence

Optimize your SecOps with advanced AI, world-class security expertise, and comprehensive threat intelligence.

Detect, investigate, and respond effectively

Stay ahead of evolving threats with a unified set of tools to monitor, manage, and respond to incidents.

Lower your total cost of ownership

Get started faster while reducing infrastructure and maintenance with a cloud-native SaaS solution.

It’s time to simplify your defense against threats

Aujas Cybersecurity, in partnership with Microsoft Sentinel, enhances SOC efficiency by consolidating security tools, eliminating silos, and improving threat detection. This approach offers a cost-effective alternative to traditional SIEM systems and is well-suited for organizations with hybrid workstyles or multiple cloud platforms.

Secure more, stress less

Aujas Cybersecurity enhances Microsoft Sentinel’s native capabilities and offers extensive features and proficiencies to help your SecOps team be more efficient, strategic, and effective.

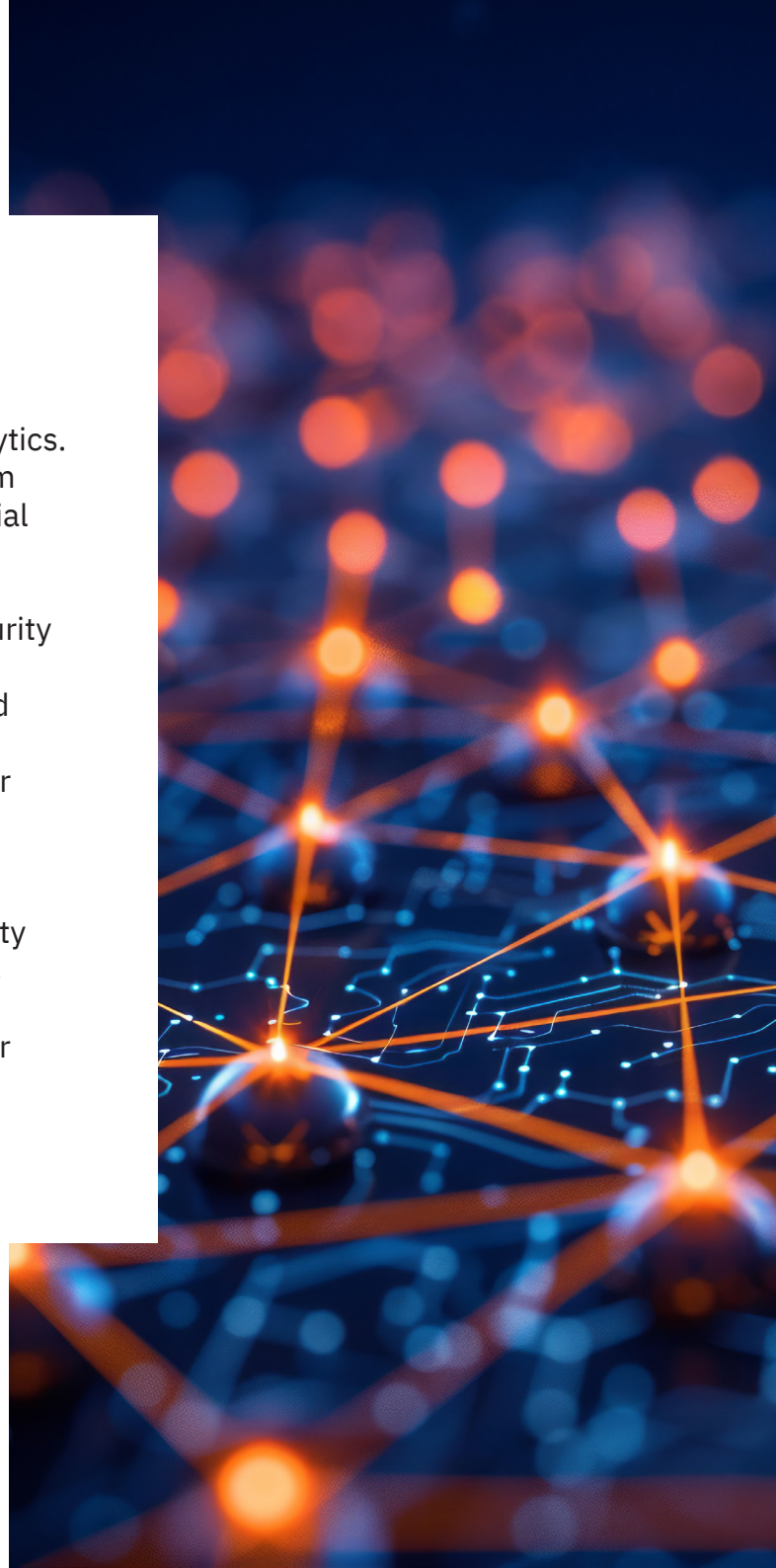
	Cloud Foundation Security	Azure Sentinel	Azure XDR
BUILD	• Azure Firewall, Application gateway, Azure Monitor, Anti-malware, Azure Security Center, Key Vault, Azure Audit logs, Azure Load Balancer, Azure Policy, Virtual Network, Azure backup, Azure Container Service	• Azure Sentinel Subscription • Define and integrate the log sources, threat intel, Alerts, workbooks, playbooks, data connectors, log parsers, Dashboard and Reporting	• Uninstallation of existing AV and Windows Defender agent deployment • Base Policy Configuration, custom rules • Build Defender for M365, IOT and Identity • Enable Defender for EDR capabilities • Report and Dashboard Configuration
MANAGED SERVICES	• 24*7 Monitoring Security Alerts • Configuration and Change Management	• Define incidence response SOP • 24*7 threat hunting, monitoring, and Compliance Reporting • Define the auto-containment policies	• 24x7 monitoring of alerts and policy exceptions, endpoints, IOT agents reporting to the console • Manage user access

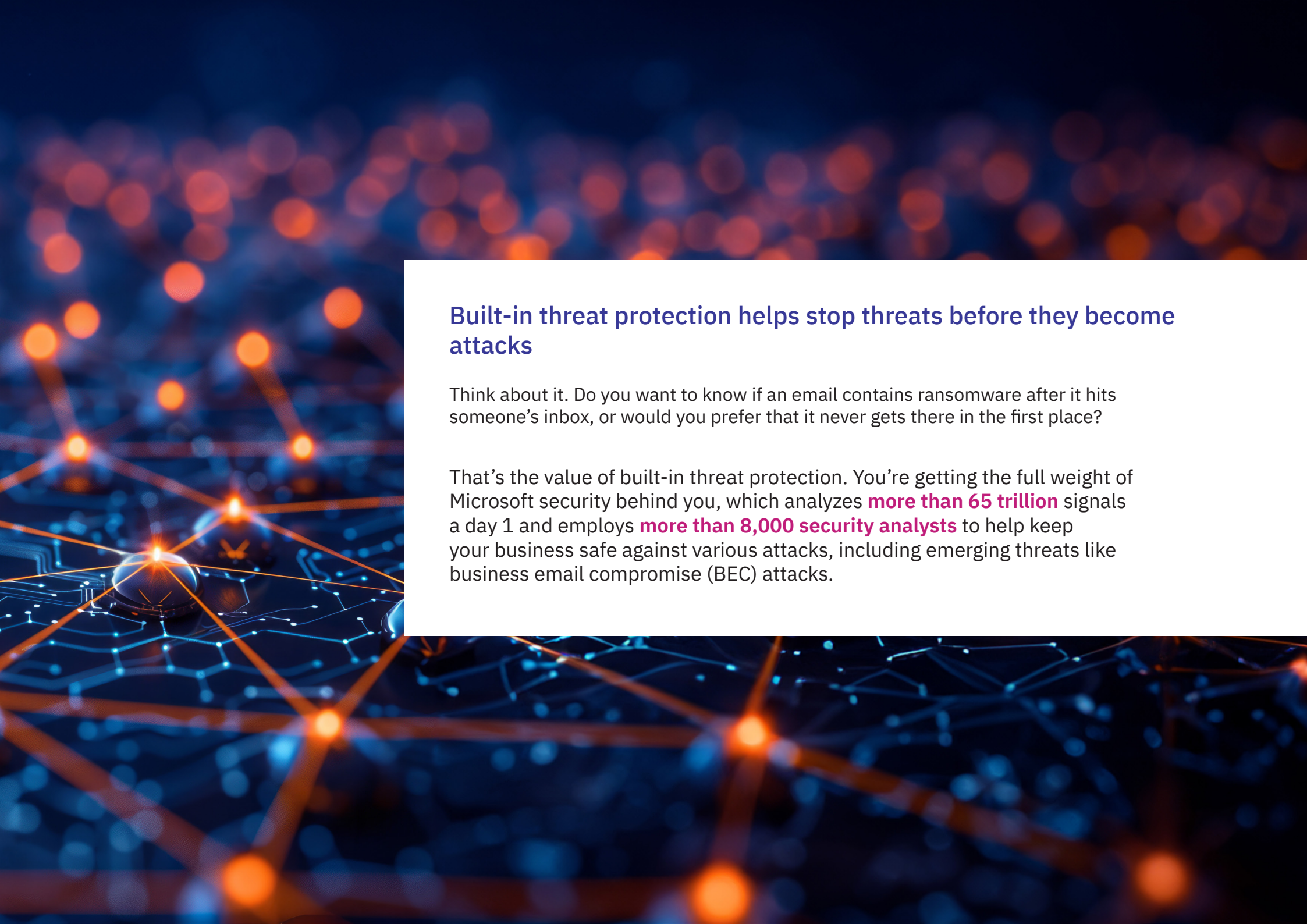
Easily eliminate those blind data spots

Effective security strategies in the modern world require large-scale data collection and analytics. Aujas Cybersecurity leverages Microsoft Sentinel's capability to ingest and correlate data from various sources, including endpoints, networks, servers, applications, cloud services, industrial infrastructure, and even third-party applications where data is stored.

As a unified SIEM solution with built-in SOAR, UEBA, and threat intelligence, Aujas Cybersecurity enhances Microsoft Sentinel's native capabilities with advanced threat detection techniques like behavioral analytics, machine learning, and threat intelligence. A variety of playbooks and integrations make it simpler and faster to deploy. You can access over 3,000 out-of-the-box and customizable standalone content and packaged solutions and even integrate it with other applications, like SAP.

Aujas and Microsoft Sentinel continuously improve security by actively hunting for threats, planning for incident response, and optimizing security policies. This ensures that new security blind spots are identified and mitigated. Microsoft Sentinel also provides comprehensive logs and documentation, making them more reliable. Basic logs can be used for post-event threat investigation at scale and for querying and automation on demand. Analytics logs are used for continuous threat monitoring, near real-time detection, and behavioral analysis.





Built-in threat protection helps stop threats before they become attacks

Think about it. Do you want to know if an email contains ransomware after it hits someone's inbox, or would you prefer that it never gets there in the first place?

That's the value of built-in threat protection. You're getting the full weight of Microsoft security behind you, which analyzes **more than 65 trillion** signals a day 1 and employs **more than 8,000 security analysts** to help keep your business safe against various attacks, including emerging threats like business email compromise (BEC) attacks.

What are we delivering?

The combined strength of Microsoft's advanced security infrastructure and Aujas' specialized MDR services create an impenetrable shield for your business. Our solution offers proactive defense, comprehensive coverage against a wide range of cyber threats, and adaptive protection that evolves in real-time.

Sentinel implementation and incident management

SIEM implementation

- Log ingestion from in scope cloud and on-prem log sources
- Enablement of out of box and custom use cases

24* monitoring and Incident Response Mgmt.

- 24*7 monitoring and on-time response to detected incidents
- Mitigate the threat – provides auto and manual remediation steps for security incident. Exploration of Sentinel SOAR capabilities to automate most of activities and responses
- Prevent future attacks - provides security recommendations to help reduce the attack surface, increase security posture, and prevent future attacks

Log source management

- Verify data collection and log continuity
- Perform device on-boarding and log source addition

Analysis, reporting, dashboard, visualization

Analysis and reporting

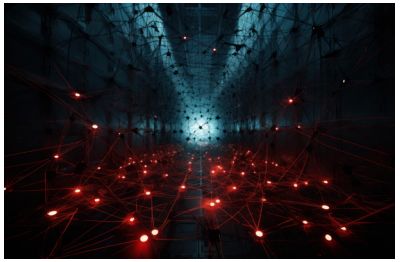
- Get started quickly without managing an infrastructure
- Review and analyze reports.
- Visualize & report your data using Sentinel workbooks

Dashboard and visualization

- Visualizations can be pinned to dashboards from multiple Azure pages
- Supports both metrics and logs
- Combine data from multiple sources including output from Metrics Explorer, log queries, and maps and availability inapplication insight
- Parametrized metrics dashboards with timestamp and custom parameters

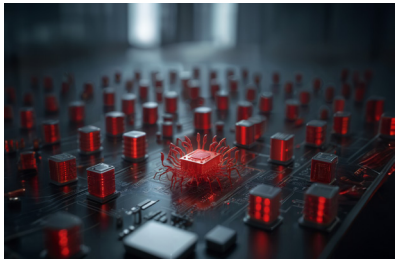

aujas.com | microsoft.com

Microsoft Sentinel use cases



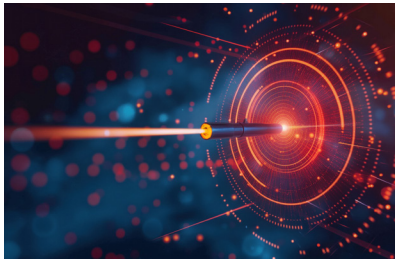
Increasing attacks

To stop and prevent an attack, you must have visibility of your entire digital attack surface and the ability to secure it. That means your SIEM must be able to ingest any type of data known today or yet to come. As a software-as-a-service offering, Microsoft Sentinel can ingest any data stored for up to seven years for compliance and quickly that can easily be augmented and customized with out-of-the-box content, connectors, additional solutions, workbooks, and more.



Lurking threats hidingin your organization

Security analysts want to be more proactive about looking for security threats. That means you need to be able to hunt and see if anything comes back as unusual. Microsoft Sentinel provides powerful hunting search and query tools across all your data sources.

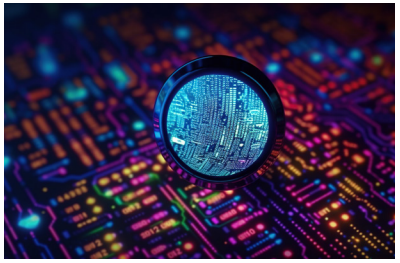


Multiple regions,any industry

You cannot be everywhere and observe everything, but your organization needs to have the latest threat intelligence information to help prevent and detect threats and attacks. Microsoft processes more than 65 trillion signals every day, which, combined with AI and the expertise of more than 8,000 dedicated security professionals, provides deep security insights to prevent catastrophic breaches. All this information is embedded into Microsoft Sentinel to help prevent and detect attacks. The affected pieces are isolated for simpler remediation if an attack gets in.

Faster, more sophisticated attacks

Every minute matters in your investigation. Microsoft Sentinel uses cutting-edge Microsoft AI and ML, trained at scale to give your SOC enhanced tools to speed their threat detection and remediation. Built-in intelligence can reduce signal noise, and pinpoint attacks, correlate the mass amounts of alerts into incidents that can span the entire attack kill chain in an attack. Then, ML prioritizes alerts can be taken right from the incident page.



Quick identification of whether something is malicious or benign

To remediate threats, you first need to know if something is malicious or not—and finding that out often takes the most amount of time. Microsoft Sentinel features investigation tools that help you understand the scope and root case of threats. Plus, an identity mapping graph enables analysts to ask interesting questions for a specific entity and drill down more deeply.

The flexibility you need, at an affordable total cost of ownership

Your enterprise needs modern security solutions—and to be their best, your SecOps team needs a full-featured, cloud native SIEM solution that enables flexibility and nimbleness. That solution is Microsoft Sentinel, and it's much more cost-effective than you might think.

Aujas and Microsoft Sentinel reduce TCO by integrating security operations, improving efficiency through automation, and providing comprehensive security coverage across IT environments. For another, you get more—like low-cost storage that meets compliance regulations and native XDR integration.

Lastly, you'll be able to eliminate multi-vendor solutions, which can save up to 60 percent on security technology expenditures.

67%
decrease in time to deployment with pre-built SIEM content and out-of-the-box functionality

201%
ROI over three years

48%
less expensive compared to on-premises SIEMS

80%
reduction in investigation effort

56%
reduction in management effort for infrastructure and SIEM

79%
decrease in false positives over three years

Case study: Leading telecommunication solution provider company

Leading global player offering managed services solutions, business process management, and technological advancements to organizations seeking higher operational effectiveness, greater flexibility, and cost savings.

The Company offers network access control and mobile security solutions, data analytics, business process management, and consulting services.

Business problem

The Client wanted to integrate their wide range of devices like servers, network devices, security tools and other Microsoft products available, into Azure Sentinel and keep track on the security alerts that get generated from these log sources. With a wide experience in the field of Managed Detection and Response area and a team with required skillsets, Aujas would be a trusted partner and would help client to set-up and manage the operations of Azure Sentinel.

- Identify threats in the organization and ways to improve
- Identify suspicious activities within the ecosystem
- Perform process improvement for preventive measures

Scale

- Fortinet Firewall
- Cisco Switches
- Azure VMs
- Windows and Syslog Servers

Continued....

Solution

In partnership with Microsoft, Aujas delivered a Managed detection and response environment to the customer so that the customer could scale up their business with maximum cyber assurance. Microsoft is providing an SIEM solution through the SAAS-based model in addition to the SOAR platform to automate many repetitive tasks.

They take care of the infrastructure and build the required things. Aujas created the required connections, automated them as needed, and provided continuous support as Managed detection and response services.

Heuristic approach

- Used Rule Based Alert Decision
- Explore various log ingestion sources like firewalls and Windows servers

Machine learning approach

- Algorithm-based alert detection
- Framework for automated tracking and monitoring
- Anomaly Detection using advanced machine learning
- Auto-alerts for investigations with minimal false alarms

Achievements

- Successfully Implemented Azure Sentinel
- Detected various threats for the organization from various data sources like Firewalls, Switches, Windows servers, etc
- Automated the incident response using Azure Sentinel

We’re here to help you transform your security operations center

Now is the time to stop cyberattacks and coordinate response across all your assets. Give your SOC a true command and control center designed with AI front and center. Benefit from our experience as a trusted Microsoft partner who understands best practices and can create and customize a solution specifically for your needs.

In essence, Aujas Cybersecurity and Microsoft Sentinel are uniquely positioned to help you streamline all your security operation modernization projects. Whether you need assessment, migration, hunting expertise, incident response, or managed security services, our experienced team and robust security service offerings can help strengthen your cybersecurity posture and defend against evolving threats effectively.

Contact us today!

For more information, visit us at
www.aujas.com or
write to us at **contact@aujas.com**