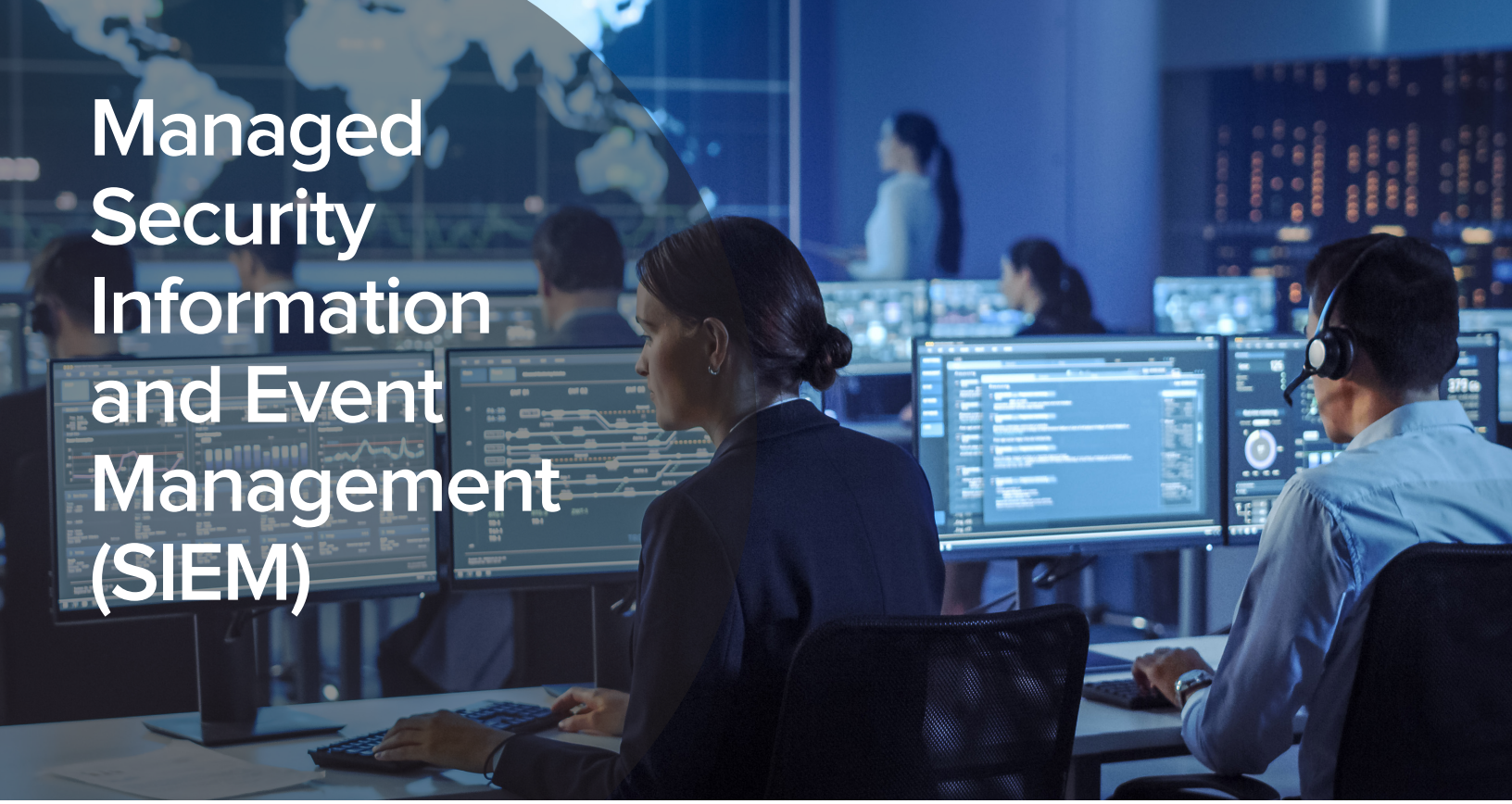


Managed Security Information and Event Management (SIEM)

What is Managed Security Information and Event Management (SIEM)?

Our managed SIEM is the perfect solution for small to medium-sized businesses that require top-notch cybersecurity but lack the resources to handle it in-house. You can now focus on growing your business while we take care of all your cybersecurity needs. Our cost-effective and intelligent solution provides you with a seamless and comprehensive approach to safeguarding your enterprise against cyber threats.

Our cutting-edge SIEM and SOC work together seamlessly to offer a holistic approach to safeguarding your organization against cyber threats. Our team is dedicated to efficiently monitoring security events, detecting and neutralizing potential risks, and ensuring that your organization meets compliance standards. With our expert guidance, you can make well-informed choices to boost your organization's security stance. By centralizing security event data, our solution eliminates any blind spots, effectively managing potential risks and keeping your enterprise safe and secure.

Begin your journey to safeguarding your enterprise today with a no-cost consultation from one of our cybersecurity professionals.

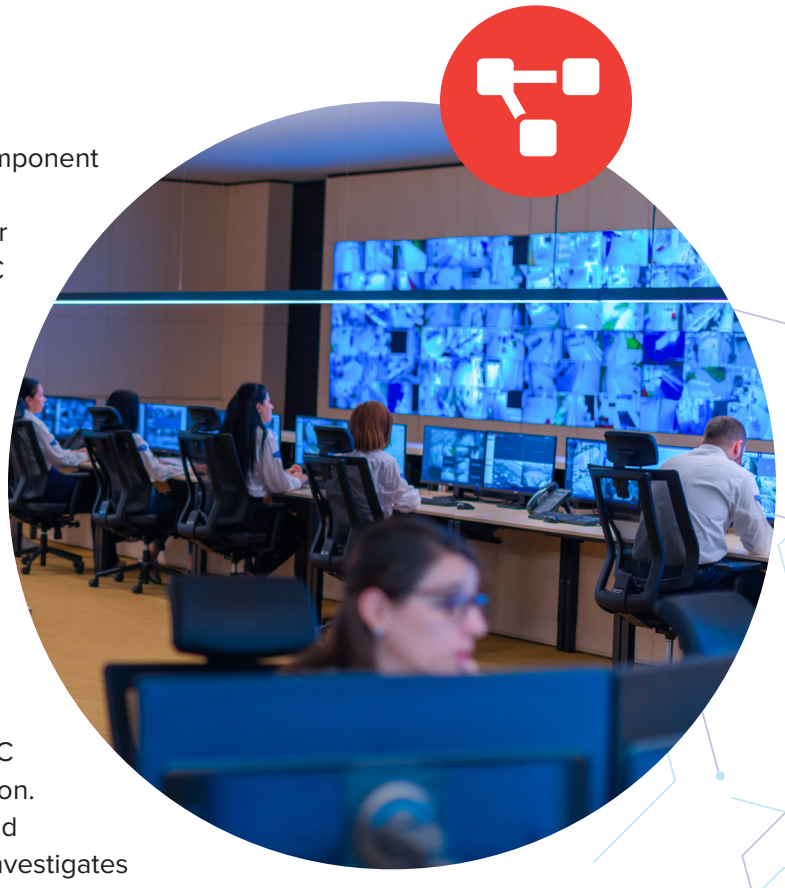
SIEM is a powerful tool that gathers security notifications and event data to provide a comprehensive view of potential threats.

What is a SIEM?

SIEM is a powerful tool that gathers security notifications and event data to provide a comprehensive view of potential threats. It ensures compliance and generates compliance reports by collecting data from all systems. SIEM automatically cross-correlates and analyzes all event logs across your network, including the server type, applications, and configuration, to prevent false positives. It integrates threat intelligence feeds, blacklists, and geolocation data to reduce false positives and detects hidden cybersecurity issues, making it an essential component of any robust security posture.

What is a SOC?

A Security Operations Center (SOC) is an essential component for effectively examining and responding to IT security incidents. While smaller organizations may rely on their IT staff for this task, larger organizations require a SOC to manage the sheer volume of events. To effectively manage these alerts, the SOC leverages a SIEM that incorporates alerts from various components, such as endpoints, network equipment, firewalls, servers (internal or web), cloud resources, virtual devices, mobile devices, and applications.



How Do a SIEM and a SOC Work Together as a Managed SIEM?

The seamless integration of a SIEM (Security Information and Event Management) system and a SOC (Security Operations Center) is a formidable combination. The SIEM acts as the first line of defense, collecting and analyzing security data, while the SOC validates and investigates alerts, taking prompt and effective action for incident response and remediation. With the SIEM's crucial role in reporting, compliance, and continuous improvement, security incidents can be detected and resolved efficiently. Together, they form a collaborative and efficient security operations framework that leaves no room for vulnerabilities. Although larger organizations have their own SOC staff, most SMBs lack the necessary resources to manage in-house.

In our managed SIEM, the SIEM and SOC seamlessly collaborate to provide a comprehensive and affordable approach to safeguarding SMBs against cyber threats. Our team is committed to monitoring security events efficiently, detecting and mitigating potential risks, and ensuring compliance standards are met. With our expert advice, you can make informed decisions to enhance your organization's security posture. By centralizing security event data, our solution eliminates any blind spots, effectively managing potential risks and keeping your enterprise secure.

What challenges are addressed by a Managed SIEM?

SIEM solutions address a variety of business challenges, including:

- Addresses compliance with regulatory requirements
- Cost-effective choice for SMBs that don't have resources to manage their security posture
- Streamlines incident response/mitigation with real-time alerts and actionable insights for cyber threats
- Automates the aggregation, cross-correlation, and analysis of event logs from across your network to identify threats
- Provides valuable security intelligence and actionable insights for informed decisions
- Ability to scale to meet your business requirements without costly infrastructure

Reasons for a SIEM

A Security Information and Event Management (SIEM) solution is critical for organizations seeking to strengthen their security posture. By consolidating all security and event data into a central location, SIEM eliminates blind spots and provides a comprehensive view of potential threats. With SIEM, suspicious activities can be detected quickly, reducing the chances of false positives. This ensures that potential security problems are identified and dealt with before they escalate into a full-blown security breach. Additionally, SIEM allows for comprehensive monitoring and enforcement of corporate policies, ensuring compliance with regulatory requirements such as PCI, HIPAA, and FFIEC. With SIEM, organizations can rest easy knowing that their security is strengthened and they are well-prepared to tackle any potential security threats.

What Makes GSI's Managed SIEM Different?

Application Expertise

Industry-leading enterprise application experts with an average of 18+ years of application, security, industry, cloud, business, and managed services experience.

Sub-5-Minute Response Time

Average sub-5-minute response time to tickets and alerts.

100% Signature Guarantee

All Services Backed by GSI's Signature 100% Guarantee.

AICPA SOC 2 Certified

GSI is SOC 2 certified by the American Institute of CPAs (AICPA) which demonstrates that GSI has specific security controls in place.

Certified ISO 27001 Lead Implementer

Certified ISO 27001 Lead Implementer resources on staff. GSI is certified to implement the formal structure, governance, and policy of an ISO 27001 conforming to the Information Security Management System (ISMS) standards.

Certified CISO & vCISO Resources

GSI has certified Chief Information Security Officer (CISO) and virtual Chief Information Security Officer (vCISO) resources.

Challenges Facing Organizations Without a SIEM

Challenge
Limited Resources / Expertise

Solution
Managed SIEM/SOC services provide access to a team of experienced security professionals and who possess the knowledge, skills and tools to manage and respond to security incidents effectively. This helps SMBs leverage specialized expertise without the need for extensive hiring or training.

Challenge
Difficulty Meeting Compliance, Regulatory, Supply Chain Requirements

Solution
The SIEM's powerful capabilities enable businesses to effortlessly showcase their compliance with various security standards and regulations like PCI DSS, HIPAA, GDPR, and more. By leveraging these capabilities, businesses can generate compliance reports with utmost efficiency, ultimately saving valuable time and effort.

Challenge
Business Email Compromise Trend

Solution
A SIEM can play a major role in helping organizations detect and respond to Business Email Compromise (BEC) attacks through log monitoring, analytics, user behavior analysis, event correlation, and integration with external threat intelligence feeds.

Challenge
Lack of Access to Threat Intelligence & Its Potential Impact on Business

Solution
SIEM solutions integrate with external threat intelligence feeds, enhancing its ability to detect attacks by cross-referencing events with known activity indicators.

Challenge
Data overload from multiple systems creates alert fatigue and log data

Solution
A SIEM offers a centralized hub that effortlessly gathers, organizes, and oversees logs from various origins. This streamlines log management, empowering technical teams to effortlessly delve into logs, swiftly address problems, and thoroughly investigate security incidents.

For more information:

Contact us today to learn more. You can also email us or call (855) 474-4377.

GSI, Inc.

GSI is a forward-thinking organization that aligns and optimizes your digital footprint with your business goals. We combine our deep business and industry experience with our expert knowledge of enterprise applications, automation, cloud and cybersecurity to deliver secure and flexible systems that allow your business to thrive and not just survive.

GSI's comprehensive suite of solutions includes: AppCare, a 24/7 managed service that includes EaaSy with flexible "on-demand" services and dynamic pricing; GENIUS AI, an Application Intelligence Platform (AIP) for creating application health and user experience monitors; GENISYS, a solution for optimizing system performance; RapidReconciler®, its inventory reconciliation software; GENOME, which automatically Detects, aNalyzes and Automates the process of converting customizations into Orchestrations; and GatewayNow, low-cost, accelerated time-to-value ITSM solution using the industry-leading ServiceNow platform in a fully managed environment.

GSI consulting and managed services are backed by its signature 100 percent guarantee. Founded in 2004, the rapidly growing company is headquartered in Atlanta with worldwide resources. With over 100 employees, GSI consultants average over 15 years of real-world experience and are certified experts in business, industry, and enterprise applications. GSI provides comprehensive 24/7 global support.