FourNet®

Quick Guide to

Security Incident and Event Management (SIEM)

Welcome to our Quick Guides to Cyber Security.

These guides have been created to give you an overview of the key pillars and solutions needed to overcome the challenges arising from Cyber threats.

Other guides in our security series:

- **Secure Infrastructure |** Quick Guide on Edge/Perimeter Security
- **Secure Infrastructure | Quick Guide to SIEM**
- **Secure Infrastructure |** Quick Guide to Cloud Security
- **Secure Infrastructure |** Quick Guide to Data and Compliance
- **Secure Infrastructure |** Quick Guide to Socially Engineered
- **Secure Infrastructure |** Quick Guide to Endpoint Security

In these guides, we outline all the major risks and threats, security trends, common challenges, and impacts. Finally, we consider the best ways to calculate and mitigate the risks to your organisation, the key measures which should be introduced, and outline how FourNet's best-in-class security solutions can help.

If you take one concept from this series, it is that effective cyber security requires a layered approach to be successful. Also be mindful that compliance does not make an organisation secure and relying solely on technology to provide the solution won't combat the inherent risks humans pose.

Building the right security culture and strategy is like Lego, needing many pieces to intersect and interplay to help mitigate the increasing level of risk our organisations face.

This guide focuses on Security Incident and Event Management otherwise known as SIEM and how this solution is helping to shape the cyber security landscape, providing organisations with visibility, Threat intelligence and the tools needed to combat and respond to threats in the new digital landscape.

Contents

Overview of SIEM and Background to the Technology

Security Information and Event Management (SIEM) is a comprehensive security solution that combines two key functions: Security Information Management (SIM) and Security Event Management (SEM). SIEM technology collects, analyses, and correlates security data from across an organisation's IT environment, providing real-time monitoring, threat detection, and incident response capabilities. It serves as a centralised platform that consolidates logs and event data generated by applications, networks, devices, and security systems to identify potential security incidents and enable rapid response.

The origins of SIEM can be traced back to the need for improved security monitoring and incident response capabilities in complex and distributed IT environments. With the increasing volume and sophistication of cyber threats, organisations needed a more efficient way to detect and respond to security incidents. Early security tools focused on log management and event correlation, but they were often siloed and lacked the ability to provide comprehensive insights into the entire security landscape. SIEM evolved as a solution to address this gap by integrating security information management and real-time event monitoring into a unified system.

Today, SIEM platforms leverage advanced technologies such as artificial intelligence (AI), machine learning (ML), and big data analytics to enhance threat detection, automate incident response, and provide actionable security insights. SIEM is widely adopted across industries to strengthen an organisation's cybersecurity posture by detecting known and unknown threats and supporting compliance efforts.

81% of organisations that use SIEM say that it has helped them enhance their threat detection abilities

Security challenges that have led to SIEM

Several key security challenges have driven the adoption of SIEM solutions

Increased Volume of Security Data

Modern IT environments generate massive amounts of security data from various sources, such as firewalls, intrusion detection systems (IDS), endpoint devices, and applications. Manually analysing and correlating this data to detect security incidents is impractical, leading to the need for automated solutions like SIEM that can handle large-scale data aggregation and analysis.

Resource Constraints

Security teams are often understaffed and overburdened, making it challenging to keep up with the constant influx of security alerts. SIEM systems help by automating threat detection and response processes, allowing security teams to focus on the most critical incidents.

Sophisticated Cyber Threats

Cyber attackers have become more advanced, employing complex tactics such as phishing, malware, ransomware, and zero-day exploits. These threats often go undetected by traditional security tools. SIEM's ability to correlate disparate events and detect anomalies allows organisations to identify these sophisticated threats before they cause significant damage.

Regulatory Compliance

Many industries are subject to stringent regulatory requirements regarding data security and privacy (e.g., GDPR, HIPAA, PCI-DSS). Organisations need to demonstrate compliance by monitoring security events, generating audit logs, and maintaining incident response capabilities. SIEM platforms help streamline compliance efforts by automating log collection, reporting, and alerting on policy violations.

Lack of Centralised Visibility

In complex IT environments, security events are often dispersed across multiple systems and locations. Without centralised visibility, security teams struggle to detect and respond to incidents in a timely manner. SIEM provides a unified view of security events across the entire organisation, enabling better situational awareness and faster incident response.

How SIEM works for organisations

SIEM platforms play a vital role in an organisation's cybersecurity strategy by providing the following key functionalities

Data Collection

SIEM solutions collect and aggregate security data from multiple sources, including network devices, security appliances, servers, applications, cloud environments, and endpoints. This data includes logs, events, and other security-related information that provides visibility into the organisation's security posture.

Threat Intelligence Integration

Modern SIEM solutions integrate with external threat intelligence feeds to enhance detection capabilities. By correlating internal security events with known threat indicators (e.g., malicious IP addresses or malware signatures), SIEM systems can detect emerging threats and provide context for faster investigation.

Real-Time Monitoring and Alerts

SIEM continuously monitors security events in real-time, using predefined rules, behavioural analytics, and threat intelligence feeds to detect suspicious activities. When a potential threat is detected, the system generates alerts that are prioritised based on severity, helping security teams respond quickly to high-risk incidents.

Compliance and Reporting

SIEM solutions generate detailed reports and audit logs to help organisations meet compliance requirements. These reports provide insights into security incidents, user activity, policy violations, and other key metrics required for regulatory audits.

Data Normalisation and Correlation

Once data is collected, SIEM systems normalise it to ensure consistency and compatibility across different formats. This enables the platform to correlate events from various sources, identifying patterns, trends, and potential security incidents that might otherwise go unnoticed. For example, an anomalous login attempt followed by unusual data access could indicate a potential breach.

Incident Response and Automation

SIEM platforms often include incident response capabilities that enable security teams to investigate and remediate incidents. This can involve automating specific responses, such as blocking an IP address, disabling a user account, or isolating a compromised device. Advanced SIEM solutions integrate with Security Orchestration, Automation, and Response (SOAR) tools to further streamline incident response processes.

Considerations for implementing SIEM

Organisations considering implementing a SIEM solution should take the following factors into account

Scalability and Performance

SIEM platforms must be able to scale with the organisation's growth. Consider how much data the SIEM system will need to handle as the organisation expands. The solution should be capable of processing high volumes of data without performance degradation.

User Interface and Usability

A user-friendly interface is critical for ensuring that security teams can effectively monitor and manage security events. The platform should offer intuitive dashboards, visualisations, and reporting tools that make it easy for security analysts to detect threats and take action.

Ease of Integration

Ensure that the SIEM platform can integrate with your existing IT infrastructure, including security tools, network devices, cloud services, and applications. Seamless integration is essential for collecting comprehensive security data and ensuring effective threat detection.

Cost and Total Cost of Ownership (TCO)

Implementing and maintaining a SIEM solution can be costly. Consider the upfront licensing costs, ongoing subscription fees, and additional costs for scaling, training, and support. Assess the total cost of ownership (TCO) and compare it with the expected security benefits and potential cost savings from preventing data breaches.

Customisation and Flexibility

Different organisations have unique security requirements. Look for SIEM solutions that offer customizable rules, dashboards, and workflows that can be tailored to your organisation’s specific needs. This flexibility is crucial for adapting the platform to your security policies and priorities

Incident Response and Automation

Look for SIEM solutions that offer built-in incident response capabilities and automation features. Automation can significantly reduce the time and effort required to respond to incidents, helping to contain threats faster and more efficiently.

Threat Detection and Analytics Capabilities

Evaluate the threat detection capabilities of the SIEM platform. Advanced solutions should offer behavioural analytics, machine learning, and integration with threat intelligence to detect both known and unknown threats. Additionally, the platform should provide powerful search and query functions to enable deep investigations.

01 Overview of SIEM

02 Security Challenges that have led to SIEM

03 How SIEM works for organisations

04 Consideration when looking to implement SIEM

05 The Benefits of SIEM

06 How FourNet can Help

The Benefits of SIEM

SIEM solutions provide a range of benefits that can help organisations strengthen their cybersecurity posture

Improved Threat Detection

SIEM systems enhance an organisation's ability to detect and respond to threats by correlating security events from multiple sources, identifying anomalies, and triggering alerts. This reduces the time it takes to detect potential threats, allowing security teams to respond before a breach occurs.

Faster Incident Response Times

With real-time monitoring, automated alerts, and incident response workflows, SIEM solutions help security teams respond to incidents faster and more efficiently. By automating repetitive tasks and prioritising critical alerts, SIEM reduces the time and resources required for incident handling

Centralised Visibility and Control

SIEM platforms provide a centralized view of an organisation's security environment, enabling security teams to monitor and manage security events across the entire infrastructure. This unified visibility is critical for detecting incidents and coordinating response efforts effectively.

Proactive Security Posture

SIEM solutions enable organisations to take a proactive approach to cybersecurity by continuously monitoring for threats, identifying vulnerabilities, and responding to incidents before they escalate. This proactive approach helps prevent data breaches and minimise damage from cyberattacks.

Supporting Regulatory Compliance

SIEM can help organisations meet compliance requirements by providing automated logging, monitoring, and reporting capabilities. These features make it easier to demonstrate adherence to industry regulations and security standards, reducing the risk of compliance violations.

Enhanced Forensics and Investigations

In the event of a security incident, SIEM systems provide detailed logs and event data that can be used for forensic analysis. This information helps security teams understand the root cause of the incident, trace the attacker's actions, and prevent future occurrences.

In Conclusion

Security Information and Event Management (SIEM) solutions have become an essential component of modern cybersecurity strategies. By providing centralised visibility, real-time threat detection, and automated incident response, SIEM platforms empower organisations to stay ahead of evolving cyber threats.

While implementing a SIEM system requires careful planning and consideration, the long-term benefits, such as improved threat detection, compliance support, and faster incident response, make it a valuable investment for organisations looking to enhance their security posture.

How FourNet can help

Our clients benefit from our experience working with some of the biggest names in government, healthcare, and finance. We have delivered solutions that have been recognised as Best of Breed by industry bodies such as Government Digital Service (GDS).

At FourNet, our solutions are designed to always protect your organisation from downtime - whether it's network failure or an attack on your infrastructure - so you can concentrate on what matters most: keeping people safe.

Trusted by Mission Critical Organisations

FourNet are trusted by some of the most secure and mission critical organisations in the UK including Whitehall, Downing Street, Cheshire Fire and Rescue, South Coast Ambulance Service, and others. Offering a diverse portfolio of solutions for both public sector and private enterprise with cloud solutions like ANTENNA and Agile Cloud.

We also provide highly available contact centre solutions delivering 999 & 111 services to the public and back-office solutions to support a flexible, agile workforce and have highly accredited and security cleared engineers and consultants.

Helping You to Understand Security Posture

FourNet's security specialists are here to help your organisation detect, defend, and repel threats from whatever threat vector they emerge. Our team of experts will work alongside you to identify and remediate areas of concern or risk. We work with you to build a business case to demonstrate ROI and payback periods based on your current costs and KPIs. Get in touch to schedule an initial discovery call.

Managed Security to Remove the Worries

We offer a range of managed solutions from the world's leading security vendors all underpinned by SC and DV level security cleared engineers and consultants. Our best-in-class security cleared service management from our dedicated secure Service Desk, FourNet provides a fully managed service desk and Security Operations Centre (SOC) with 24/7 phone support and multi-factor authenticated ITSM access.

Whether you are looking to secure and control access to critical systems or wanting to outsource security to a managed SOC we can help. We work with you to create an understand your organisation and provide the help, solutions, and support where it is needed most.

Discover if your Network is Ready for Emerging Threats

Discover whether your security solutions are keeping pace with the threat landscape with a FourNet Cyber Assessment.

Get in touch to arrange your assessment

Check out our Other Guides to Cybersecurity

Click Here >>

FourNet®

Manchester Office (HQ)
3 Scholar Green Road,
Cobra Court,
Manchester. M32 0TR
Tel: 0845 055 6366

hello@fournet.co.uk
fournet.co.uk

FourNet PR & Media Office
Tim Reid
e-mail: treid@fournet.co.uk