Security Incident & Event Management (SIEM)

LOGICALIS
Business and technology working as one

intel Security

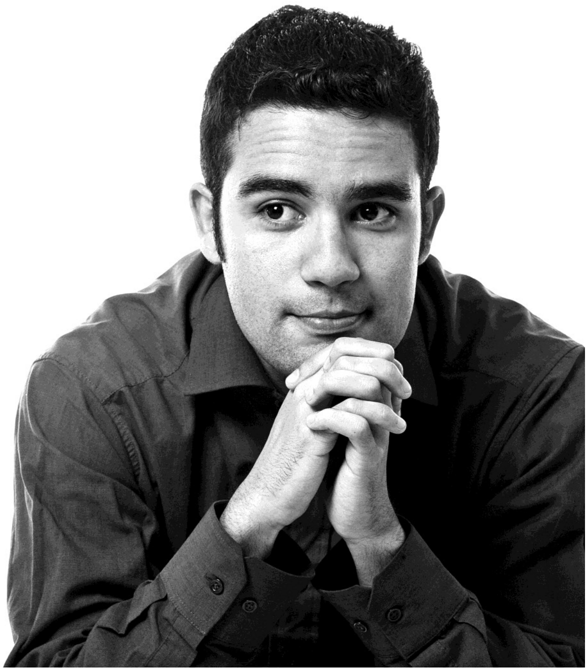
Business Requirement

Gain visibility into security events on your whole security posture.

Payment Card Industry Data Security Standard (PCI DSS) compliance has traditionally driven SIEM adoption in large enterprises. Concerns over Advanced Persistent Threats (APTs) have led smaller organisations to look at the benefits a SIEM Managed Security Service Provider (MSSP) can offer.

ISO27001 and a desire to improve the organisations' overall security posture, coupled with mitigating risk by utilising real time views of security and other related events, has caused many customers to look at SIEM solutions.

SIEM can be a challenging and expensive solution if it's not delivered as a service to a customer by dedicated experts .

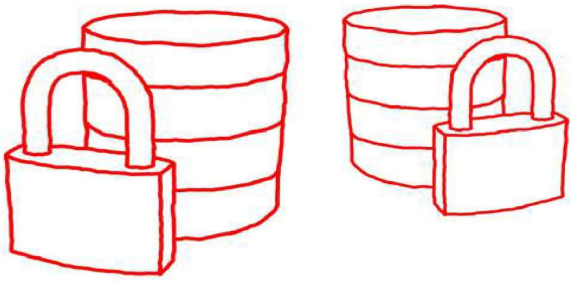


Logicalis Solution

Security Information and Event Management (SIEM) is an approach to security management that seeks to provide a holistic view of an organisations information technology security posture. SIEM combines Security Information Management (SIM) and Security Event Management (SEM) functions into one security management system. SIEM offers a single pane of glass in which to view an organisations current security.

The underlying principle of a SIEM system is to relay relevant data about an enterprise's security posture. The correlation of log data produced from devices in multiple locations is organised in a centric fashion. This allows security professionals to spot trends and work out patterns that are out of the ordinary and potentially suspicious.

Mitigating the risk by utilising real time views of security and other related events, are key to improving the organisations overall security posture.



Business Benefits

- ✓ Allows monitoring and logging of access to systems with regulated information.
- ✓ Retains details of all logs allowing easy search for analysis as well as time-stamping to aid forensic investigations.
- ✓ Flexible and hybrid delivery options include physical and virtual appliances.
- ✓ A single architecture for analysing log, flow, vulnerability, user and asset data.
- ✓ Near real-time correlation and behavioural anomaly detection to identify high-risk threats.
- ✓ High-priority incident detection among billions of data points.
- ✓ Full visibility into network, application and user activity.
- ✓ Automated regulatory compliance with collection, correlation and reporting capabilities.
- ✓ Continuously monitor, identify, investigate and resolve threats.
- ✓ Fight advanced threats with real-time SIEM.

Logicalis' Managed Security Services

Logicalis has a unique capability to build, host, support and manage any size of communications and computing infrastructure. Accredited by the leading security vendors and managed service providers, Logicalis operates UK Managed Service Centres and in-house UK Tier 3 managed hosting facilities.

Overview

The non-intrusive design of the Logicalis SIEM solution supports your expanding compliance, auditing and reporting requirements.

Logicalis' SIEM solutions delivers non-intrusive, detailed security analysis and monitoring, showing all access to sensitive corporate and customer data. With minimal deployment effort, you can have visibility into your systems and devices logs providing advanced alerting and warning of any incidents.

With advanced reporting included as standard, Logicalis' SIEM solution helps drive your compliance goals such as PCI-DSS compliance.

Logicalis SIEM solutions will help you understand your network and gain advanced visibility into any issues in real time.

Features

- ✓ Monitors and logs all activity.
- ✓ Support compliance efforts such as PCI –DSS
- ✓ Wide device compatibility.
- ✓ Increased accountability.
- ✓ Monitor all paths to data, including:
  - Applications
  - Users
  - Malware
  - Utilities
  - Logon failures
  - Firewalls / Routers alerts
  - IDS/IPS systems alerts
  - Availability and file integrity monitoring
- ✓ Capture valuable security metrics for monitored devices.
- ✓ Alerting on objects, events and policy violations.

Visit Jersey www.je.logicalis.com	Visit Guernsey www.gg.logicalis.com
Call Jersey +44 (0) 1534 288019	Call Guernsey +44 (0) 1481 737 000
Email Jersey Solutions@je.logicalis.com	Email Guernsey solutions@gg.logicalis.com

LOGICALIS
Business and technology working as one

About the Team

Our dedicated security professionals are certified and trained in security disciplines and methodologies. The Value that the Logicalis Managed security Services security adds is not limited to our extensive security team in the SOC Security Operations Centre that help with correlation of endpoint security events. Our seasoned team are skilled in deploying, maintaining, alerting and reporting on security events that could potentially result in security incidents.

Provides real-time analysis of security alerts