Security Information and Event Monitoring for SMEs

What is SIEM?

SIEM is an acronym for Security Information and Event Management. It is a software solution which allows businesses to detect, analyse and respond to potential security threats across their organisation.

Security threats are detected by analysing behaviours and activities which are considered to be abnormal or suspicious, using threat rules and threat intelligence. Once a potential threat is detected, alerts are automatically created to allow security personnel to investigate and respond to the threat.

The SIEM solution allows businesses to understand the risks and threats to their environment, to manage and evaluate these, and put in place suitable responses to protect their digital assets and reduce security risks.

Can I use SIEM to meet all my security needs?

No. When used, SIEM should form part of an overall security strategy which may include, but not necessarily be limited to:

- Configuration of routers, firewalls, user and system security
- Regular patching and update of operating systems and software
- Backup and recovery strategies for all mission-critical systems and data
- End-point protection including anti-virus and anti-malware solutions
- Multi-factor authentication for logging into systems
- Cyber-security awareness

"SMEs are especially vulnerable to cyber security threats. Feedback from consultation shows SMEs often lack the resources or expertise to defend themselves and that there can be a large impact on regional communities when cyber criminals target SMEs."

- Australia's Cyber Security Strategy 2020

For more information call 1300 736 953
www.bluebloodsolutions.com.au

Who needs SIEM?

Data breaches and cybercrime can bring businesses to a standstill and damage brand, customer loyalty and the partnerships that a business has. All businesses are vulnerable to cybercrime. Gone are the days when you could just put in place a firewall and some anti-virus software, the cybersecurity threats of today are evolving and have become more sophisticated.

Reasons why an organisation may require a SIEM solution:

- To meet compliance requirements, where reports which address security events or reporting on data breaches is required. Without SIEM, the organisation would need to manually retrieve logs and compile reports.
- To protect sensitive data and systems which are managed by the business. Often businesses are unaware of attempted infiltrations until it is too late, and they do not have systems in place to detect and respond to malicious activities. The quicker the threats are identified, the quicker the response is, and therefore the more secure IT systems will be, reducing the overall risks to the business.

Why would an SME require SIEM?

SMEs (Small to Medium Enterprises) tend to be more vulnerable as they have far less resources to protect themselves than larger businesses. SMEs also face a number of challenges. Typically, SMEs don't have the budget for enterprise security solutions or the inhouse expertise required to implement IT solutions. Hackers target SMEs as they can be easier to infiltrate, sometimes they are the weak point in a supply chain, and a way to penetrate larger enterprises who have stronger security.

Implementing SIEM can assist SMEs in spending their limited budgets on the areas which represent the highest degree of risk.

Why Blueblood SIEM?

We realise that SMEs don't have the big budgets that larger businesses have, so we have put together a cost-effective solution, using Microsoft's Azure Sentinel technology. Our solution includes pre-built threat rules from Microsoft as well as a set of customised rules and reports which we believe are essential for SMEs. We continually add to the threat rules as the threat landscape changes and new requirements are identified.

The Blueblood SIEM Solution

The Blueblood SIEM solution provides a solution which collects, monitors, detects, investigates, communicates and reports on potential security threats.

Collect

Event data is collected from your applications and infrastructure. This data may include data from servers, routers, web-based systems, Microsoft 365 and other systems.

Detect

Potential security threats are detected using pre-built and custom alerts which generate incidents for investigation and reporting. As the cyber security landscape and systems change, Blueblood adds new alerts to the environment to detect new threats.

Monitor

Dashboards, email alerting, analytics queries and more, are used by Blueblood staff to monitor any potential security threats.

Investigate

A combination of dashboards, investigation panels, log data, pre-built and custom analytics queries help us investigate potential security threats.

Communicate

We liaise with you and your Managed Service Provider or IT support team to assist in the resolution of any security threats or incidents.

Report

Monthly reports allow you to see trends in security threats and specific incident information. These allow you to assess the security threats that represent the greatest risk to you, and therefore where further action would provide the most benefit.

For more information call 1300 736 953
www.bluebloodsolutions.com.au