Managed SIEM Solution

solve solutions

Managed SIEM Solution

Our managed SIEM solution ensures quick and effective detection and response to security threats, while reducing operational costs, improving compliance, and providing better visibility into your security posture.

With a managed SIEM solution, organisations can benefit from advanced analytics and machine learning algorithms to detect even the most sophisticated threats, as well as reduce the time it takes to detect and respond to security incidents.

Our Managed SIEM solution provides organisations with a number of different deliverables, including:

- Reports and dashboards providing insight into the organisation's security posture and compliance with security regulations.
- Real-time alerts and notifications regarding potential security threats and incidents.
- Automated log collection and analysis to detect suspicious activity.
- Automated incident response processes to respond quickly and effectively to security incidents.

Managed SIEM solutions provide organisations with the peace of mind that their data is being monitored and protected 24/7, ensuring the highest level of security. Investing in a managed SIEM solution can help organisations reduce the risk of a security incident and keep their data safe.

Use Cases

Threat detection and incident response:

We facilitate collection and analyse log data from various sources, such as network devices, servers, and applications, to detect potential security threats and help with incident response.

- Malware
- Ransomware
- Reconnaissance
- Phishing

Network and security monitoring:

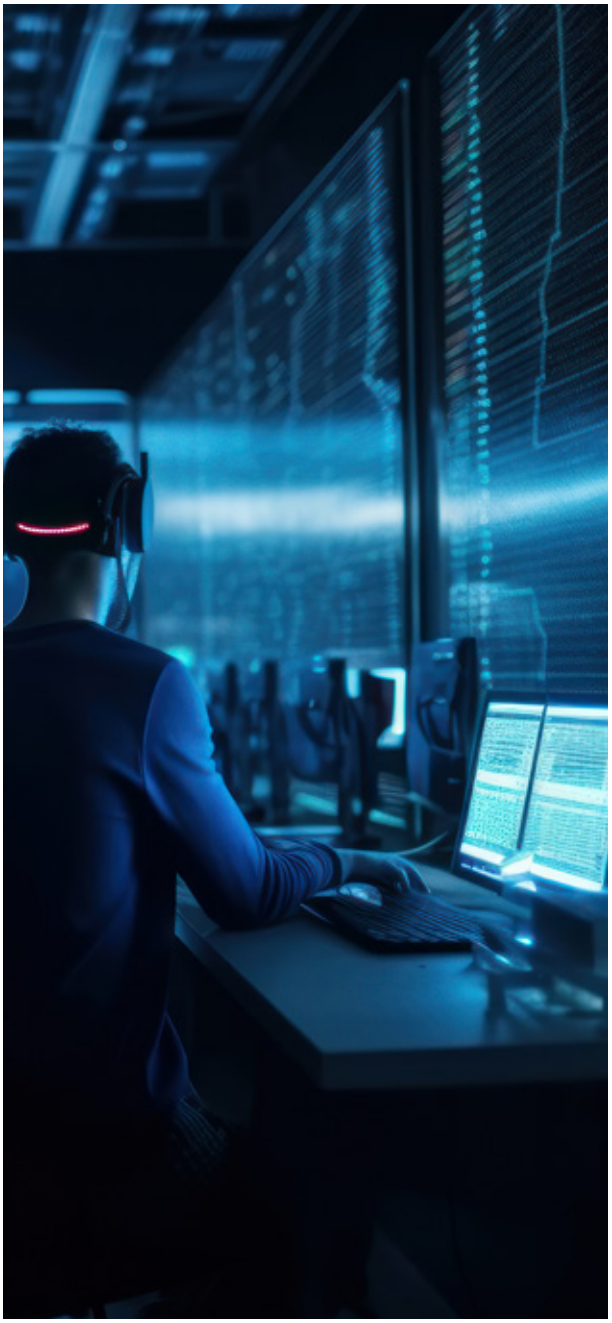
A SIEM can provide real-time visibility into network traffic and events, helping to identify and respond to potential security threats. Some of the possible event sources include:

- Intrusion Detection System (IDS): A SIEM can be used to detect malicious network traffic, such as malware, port scans, and denial of service attacks.
- Network Access Control (NAC): A SIEM can be used to monitor and enforce access control policies and ensure only authorised users and devices have access to the network.
- Data Loss Prevention (DLP): network traffic for sensitive data, such as credit card numbers, social security numbers, and other confidential information.
- Network and Host availability: Monitor the operational state of your key service infrastructure for visibility and early warning of potential failures.

Business Benefits:

With a managed SIEM solution, organisations can benefit from the following advantages:

- Reduced operational costs: By outsourcing implementation and management, organisations can reduce the costs of implementing and maintaining a SIEM system.
- Increased efficiency: Reduce the time it takes to detect and respond to security incidents, enabling fast and effective response.
- Better visibility: Provide organisations with improved visibility into their security posture, allowing them to identify and address potential security threats with speed.



Service Overview

Our engagement is workshop-led and aligned to best practices and industry standards. During the workshop we will assist in the discovery of the required event sources, log management architecture and security.

Scope of work includes:

- Establish a process for logging and monitoring of events.
- Establish procedures for regularly reviewing logs.
- Establish procedures for responding to detected security incidents.
- Ensure that logs are stored in a secure and tamper-proof manner.
- Ensure that logs are backed-up regularly.
- Ensure that logs are retained for a sufficient amount of time.
- Ensure that access to logs is restricted to authorised personnel.
- Ensure that processes are in place to detect and respond to suspicious log activity.

After the workshop, we provide a proposal containing the architecture, pricing and detailed services configuration.

About Solve Solutions

Solve Solutions is your managed cybersecurity business partner. We provide 24/7 monitoring, threat detection, and response services to ensure network uptime and data protection. Our team of experienced professionals will work with you to create a customised plan that addresses your unique security needs and compliance requirements. Now you can focus on your core business while we handle the cybersecurity risks.

Don't let cyber resources compromise your business's success – contact us today to learn more about our managed cybersecurity solutions.

Block A Knightsdridge office park, 33 Sloane Street, Bryanston
+27 82 902 6261 | kevin.smith@solvesolutions.co.za
www.solvesolutions.co.za