SOLUTION BRIEF

Managed SIEM

Comprehensive Visibility without the Complexity

Reduce the time to detect and respond to threats in your environment.

Despite your organization's best efforts, threats can break through your security defences. And when they do, you need to stop them fast, before they can cause damage.

A security information event management (SIEM) tool is foundational to the visibility and context that fuel effective threat detection and response. A SIEM collects and consolidates security data from devices across your modern distributed environment and normalizes it so that it can be analysed and monitored for threats.

SIEM tools are costly and complex to implement, manage, and tune in-house, especially without the right skills and with constantly changing security threats to your business. Misconfigurations are common and can result in the SIEM generating too many false alerts which can hide real threats. Importantly, a SIEM can't tell you how you should respond to an alert. With Managed SIEM, you get all the advantages of a SIEM without the complexity – and with flexible options that scale according to your needs.

SilverSky leverages FortiSIEM technology to deliver on the most advanced SIEM capabilities on the market:

Broad Visibility

We configure FortiSIEM to ensure that optimal logs, endpoint data, and network and system activity from across your distributed environment are collected in real-time, consolidated, and unified.

Innovative Tools

Automation tools, threat intelligence feeds, and deep analytics assist our security operations center (SOC) team in surfacing and analysing alerts from FortiSIEM to determine risk to your business.

Machine Learning/UEBA

Our advanced machine learning engine evaluates the FortiSIEM data and detects unusual user and entity behaviour (UEBA) that traditional defences can miss.

Actionable Results

Our SOC analysts rapidly prioritize, triage, and correlate alerts and respond to confirmed threats based on your custom playbook.

Continuous Monitoring

The streamlined activity data is monitored for threats and indicators of compromise by our seasoned SOC analysts 24x7x365.

Strong Fortinet Partnership

We've been a top Engaged Fortinet partner for 20 years. With our deep experience working with Fortinet technology and its capabilities, SilverSky is the partner of choice for managing FortiSIEM.

SOLUTION BRIEF

SilverSky Managed SIEM

We help you achieve optimal SIEM performance

A SIEM can help you detect and respond to threats in your environment before they can cause damage to your business. SilverSky Managed SIEM offers flexible service levels that can take over wherever your team's bandwidth and skills leave off. Whether you have your own instance of FortiSIEM or use ours, SilverSky skilled analysts and engineers work with your team to configure and tune FortiSIEM to your security criteria so that it accurately identifies, prioritizes, and alerts on suspicious activity and indicators of compromise.

Our SOC team is well-trained to investigate and act on positive alerts. We take the time to develop custom response playbooks and train your team on the use of our outSOC portal which provides real-time insights and reporting, so that together, you and your team can action those alerts based on your business.

While a SIEM leverages automation, threat intelligence, and machine learning to analyse security data activity and generate alerts, it can only take that analysis so far. Guided by your custom playbook, SilverSky experts act on severe threats and either remediate them directly or provide you with actionable advice. With more than 20 years of experience delivering global SOC services to more than 4,000 customers, you can be confident in our delivery in partnership with your security team.

Take your protection to the next level

- Real-Time Telemetry
- Threat Intelligence
- Machine Learning / UEBA
- Integrated Technology Stack
- Skilled Analysts
- Active Monitoring
- Customised Response Playbooks

In partnership with our highly skilled and certified SOC team, SilverSky Managed SIEM optimizes your ability to detect and respond to threats – protecting your business with actionable security insights.

Call SilverSky 1-800-234-2175

linkedin.com/company/silversky

twitter.com/silversky

www.silversky.com

SILVERSKY

1-800-234-2175
learn@silversky.com

3015 Carrington Mill Boulevard
Suite 400
Morrisville, NC 27560