SOLUTION BRIEF

Managed SIEM

For Those About to SOC

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

Despite your organization's best efforts, threats can break through your security defenses. 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 analyzed and monitored for threats.

Managing a SIEM in-house requires staffing, yet an industry talent shortage is underscored by the constantly evolving threats to your business. Misconfiguration is common and can result in the SIEM generating excessive false alerts, which mask real threats. Not to mention, a SIEM alone can't tell you how you to respond to an alert...

With PatientLock Managed SIEM, you get all the advantages of a SIEM without the complexity.

PatientLock 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.

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.

Continuous Monitoring

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

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.

Actionable Results

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

Strong Fortinet Partnership

With our deep experience working with Fortinet technology and its capabilities, PatientLock is the partner of choice for managed FortiSIEM.

SOLUTION BRIEF

PatientLock 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 or patients. PatientLock Managed SIEM offers flexible service levels that can take over wherever your internal team's bandwidth or skills leave off. Whether you have your own instance of FortiSIEM or use ours, PatientLock 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 will work with you 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, we have an alert-handling playbook that matches your business needs. While a SIEM leverages automation, threat intelligence, and machine learning to analyze security data activity and generate alerts, it can only take that analysis so far.

Guided by your custom playbook, PatientLock experts act on threats and either remediate them directly or provide you with actionable advice.

Take your security to the next level

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

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

Call PatientLock 866-938-4250

linkedin.com/company/patientlock

twitter.com/patientlock

www.patientlock.net

866-938-4250

info@patientlock.net

Corporate Woods - Building 51
9393 W. 110th Street, Ste. 500
Overland Park, KS 66210