Cyber Lantern Next-Generation SIEM

The Business Challenge

To meet compliance standards, most organizations rely on a Security Information and Event Management (SIEM) platform to manage their security needs. While there are many security products available for large enterprise organizations, they are often too costly and complex for deployments by Small to Medium Size Businesses (SMBs), or Managed Service Providers (MSPs) who manage several security deployments. Without having any real affordable options, many of these organizations become primary targets for hackers. While there are many security products available for large enterprise organizations, they are often too costly and complex for deployments by Small to Medium Size Businesses (SMBs), or Managed Service Providers (MSPs) who manage several security deployments. Without having any real affordable options, many of these organizations become primary targets for hackers.

The Cyber Lantern next-generation SIEM creates prioritized cyber security tasking so you can spend less time and money managing security, and more time focusing on making your business successful.

The Cyber Lantern Approach

At Cyber Lantern, we believe every organization should have access to affordable and reliable security, regardless of size or budget. The Cyber Lantern next-gen SIEM allows you to have the expertise of an entire security team built into one platform. Cyber Lantern incorporates enhanced data contextualization and the Adaptive Security Model to

BUSINESS BENEFITS

Effortless and Affordable Security

Cyber Lantern next-gen SIEM runs as your security operations center without the cost of building one, giving you all the capabilities of an expert team at a fraction of the cost.

Reduce time spent managing security

Ensure faster threat detection and remediation with correlated and prioritized alerting and tasking, helping you minimize the downtime, costs and business impact of a breach.

Lower cyber risks and improve brand protection

Protects your organization and brand name from breaches which can cripple your company's business operation.

KEY FEATURES

Network and Device Visibility

Understand your environment to help protect the most important systems and data first.

Network Protection

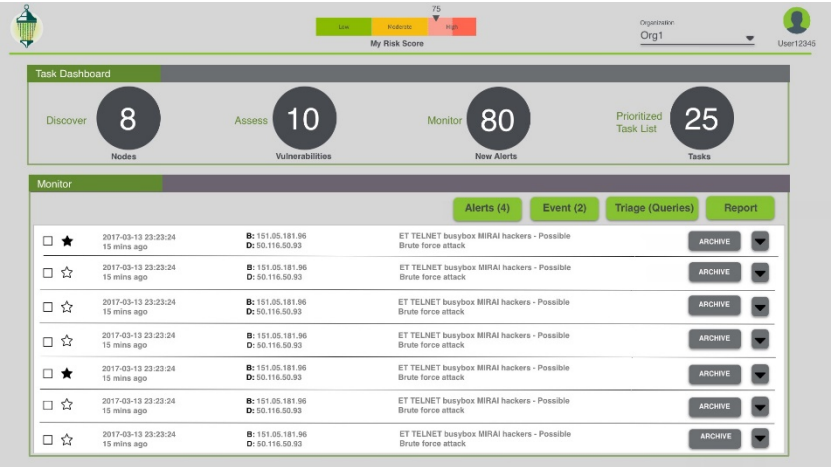
Correlated alerts that help identify vulnerabilities, threats to your network, data, and applications.

Prioritized Actions

Dashboard of current company risk score and prioritized action items and recommendations to help identify what action to take first and how to continuously improve your security posture.

Cyber Lantern Next-Generation SIEM vs. Traditional SIEM

Traditional SIEMs pose many obstacles for SMBs and MSPs alike. High costs and implementation are the most common challenges, however there are additional challenges that make these products difficult to manage and use daily.



Cyber Lantern's Next-Gen SIEM creates prioritized tasking based on an Adaptive Security Model focused on Prevention, Detection, Prediction and Response for easy management of security operations.

Traditional SIEM Challenges

Steep Learning Curve

Traditional SIEMs are only as effective as the person managing and operating them. These SIEMs often require hours if not days of training for analysts to properly learn how to effectively manage and operate these tools since they require a significant amount of manual tuning to operate.

Unreliable Correlation and Alerting

SIEM operators rely on event correlation and alerting mechanisms within the SIEM to help filter out non-threatening events. This helps ensure analysts are only looking at relevant alerts and using correlation of several data sets to help reduce incident analysis time. With traditional SIEMs, these alerts and correlations are heavily reliant on a continuous “tuning”, normally requiring full time resources. As networks, data sets, and IT environments rapidly change within an organization, the traditional SIEM will require rule and data management to minimize false positives and maintain high fidelity alerting.

Lack of Analytic Flexibility

Many SIEMs provide pre-defined analytics and dashboards to assist in investigations and reporting. While these reports are helpful, they often do not consider the ever-changing threatscape and security standards businesses experience, leaving little room for explorative analysis and dynamic reporting.

Cyber Lantern Next-Gen SIEM Features

Asset identification and alignment with security.

- Agentless aggregation of the assets on your network
- Integrated asset criticality tagging and management with event alerting to ensure your critical devices are prioritized during threats.
- Enables you to rapidly identify and remediate breached devices

Task management and integration.

- Prioritized tasking based on your most critical security needs first.
- Rapidly enables event and incident response.
- Rapid data integration and association helps decrease resource time for deployment and analytic interpretation.
-

Advanced Analytics and contextual correlation

- Simple signature based and security device alerting is insufficient for today's evolving threats.
- Anomaly detection through unsupervised learning finds threats that your security devices missed.
- Advanced analytics piece together seemingly disparate and unimportant events into a cohesive view of major events.