Cyber Observer **Technology Partners**

splunk> turn data into doing™

CYBER OBSERVER

Solution Brief

Cyber Observer and Splunk Integration

Unified cybersecurity management and awareness

Challenge

Today's challenging cybersecurity landscape offers an over-abundance of cybersecurity tools. As the number of breaches proliferates, so do the solutions and technologies designed to stop them. The state of cybersecurity is not getting easier to manage, and enterprises and organizations are spending more money than ever on new technologies and solutions.

CISOs, CIOs, and other enterprise executives need a unified view of their entire cybersecurity ecosystem. Comprehensive visibility and monitoring is the only way to continuously maintain proper **cyber hygiene**.

Solution

Designed for security and risk management leadership, **Cyber Observer** empowers decision makers with a unified dashboard of their organizations' entire cybersecurity ecosystem. **Cyber Observer** can be fully deployed within an enterprise in a few hours, enabling easy **identification** of **weaknesses**, reduction of **mean-time-to-detect (MTTD)**, **prevention of breaches**, and **advancement of cybersecurity posture** and **maturity**. Through Cyber Observer's partnership with Splunk, leaders receive alerts from Cyber Observer on key aspects and issues in Splunk Enterprise Security such as **configuration**, **incident and investigation management**, **password policies**, **user and role administration,** and more. This integration helps enterprises manage their cybersecurity environment and **continuously monitor their cybersecurity ecosystem posture**.

KEY FEATURES

- Identifies cybersecurity tools that are misconfigured, malfunctioning, or missing
- Finds security gaps and provides recommendations for fixing
- Builds ongoing security program to ensure alignment with new threats
- Uses continuous analytics to send alerts when there are deviations from normal behavior
- Automatic reporting

splunk> turn data into doing™

CYBER OBSERVER

The integration between Cyber Observer and Splunk offers CxOs powerful and effective **resilience visibility** along with **compliance validation** and **controls**, to secure and monitor Splunk Enterprise Security in an unprecedented manner.

Cyber Observer deploys to the corporate network automatically, in a matter of a few hours, predefined with security domains and CSC measurements to deliver three unique cybersecurity ecosystem views:

- First, it provides organizations the best indicators of the cybersecurity tools that may be **misconfigured**, **malfunctioning**, or **missing** and should be added in order to provide complete cybersecurity protection.
- It then **reveals the security gaps** that exist in each security domain and **delivers continuous proactive recommendations to close these gaps**.
- Finally, Cyber Observer's machine learning analytics engine continuously calculates online measurements that represent normal behavior, and then **alerts when a deviation from normal behavior is detected**.

Fast and Secure Deployment

The Cyber Observer connector for Splunk Enterprise Security receives security and configuration data from the Splunk server via a secure REST API.

splunk> turn data into doing™

CYBER OBSERVER

Key Features & Benefits of This Integration

- **Security Analysis and Reporting for Managers:**
  Alerts and reporting of current configuration status, based on the vendor's recommendations and security standards best-practices. This includes Splunk's security configuration issues, incidents and investigations management, insecure password policies, user and role administration, and more.
- **Customizable Views and Reports:**
  Cyber Observer is highly customizable – all views and reports can be copied and modified to an organization's specific needs and structure. The integration between Cyber Observer and Splunk offers CxOs powerful and effective resilience visibility, as well as compliance validation and controls.
- **Reduced Incident Analysis Time:**
  Cyber Observer provides continuous alerts on deviations from normal behavior regarding Splunk implementation and effectiveness, along with near real-time continuous monitoring of relevant security issues.
- **Continuous Incident Response:**
  CISO and other relevant managers in the organization, along with the Splunk technical owners, receive continuous mitigation recommendations and steps to improve as well as ways to secure and monitor Splunk implementation, effectiveness, maturity, and resilience, in an unprecedented manner.

Key Use Cases

1 High Severity Incidents and Investigations Issues

- High risk incidents
- High count incidents
- Unresolved incidents
- Unassigned incidents
- Current open investigations
- Current unresolved investigations
- Objects with a high-risk score

2 User, Role and Password Management

- Administrator users
- **ess** admins users
- Users
- **ess** analysts
- Users changes
- Users with failed login attempts
- Users who were recently locked out
- Minimum password length less than X characters
- Password policy does not include at least X numerals
- Lockout disabled
- Failed login attempts set to more than X attempts
- Roles
- External authentication configuration

3 Licensing and Token Issues

- Licenses that are due to expire soon
- Expired licenses
- Current token details
- Tokens that were never used
- Tokens that were issued recently
- Tokens that have expired

splunk> turn data into doing™

CYBER OBSERVER

About Splunk

Splunk (NASDAQ: SPLK) is the world's first Data-to-Everything Platform, designed to remove the barriers between data and action for everyone to thrive in the Data Age. We're empowering IT, DevOps and security teams to transform their organizations with data from any source and on any timescale. Splunk helps organizations ask questions, get answers, take actions and achieve business outcomes from their data. Organizations use market-leading Splunk solutions with machine learning to monitor, investigate and act on all forms of business, IT, security, and Internet of Things data.

About Cyber Observer

Cyber Observer is holistic cybersecurity management and awareness solution. It continuously measures the cybersecurity status of an organization's security environment by retrieving and analyzing Critical Security Controls (CSCs) from relevant security tools. Developed for CISOs, InfoSec and IT managers, Cyber Observer provides extensive cybersecurity understanding for all stakeholders.