SOLUTION BRIEF

Enhancing Cybersecurity with Pure Storage and Cisco Splunk

Streamline Security Operations and Enhance Data Protection.

As technology advances, the need for secure systems emerges, especially for protecting sensitive information from constant cyber threats. Automated and easy-to-implement security solutions are the need of the hour for real-time data protection. Integrating Pure Storage® with Splunk Enterprise offers comprehensive security insights about storage, proactive threat detection, and optimized incident response, resulting in improved visibility and agility to address evolving cybersecurity challenges. Splunk Enterprise SIEM and SOAR offer a unified platform for monitoring, detecting, and responding to threats, enabling comprehensive asset protection for organizations.

Solution Overview

In the evolving cybersecurity landscape, prioritizing security is essential, as systems storing sensitive data are frequently targeted by cyber threats. Therefore, organizations require high-performance security solutions that are both automated and straightforward to implement, ensuring real-time protection of critical data.

Pure Storage provides high-performance data storage solutions. When integrated with Splunk, it enhances threat detection and response capabilities by enabling seamless access to critical security event data. This integration empowers security teams to act swiftly and effectively against emerging threats.

Splunk Enterprise SIEM (security information and event management) and Splunk SOAR (security orchestration, automation, and response) deliver comprehensive protection through a unified platform. Together, they enable organizations to monitor, detect, and respond to security threats efficiently, ensuring robust protection of their critical assets.

Technology Overview

Deploying Splunk Enterprise as a SIEM solution on virtualized or on-premises platforms provides organizations with a robust foundation. Integrating Pure Storage with Splunk Enterprise enhances these capabilities by delivering:

- Comprehensive insights into the storage environment
- Proactive identification of potential security threats
- Optimized incident response efforts

Reduced Manual Intervention

Automates repetitive tasks, freeing security teams to focus on higher-priority challenges.

Accelerated Response Times

Automation and streamlined workflows minimize delays in addressing threats.

Scalability and Flexibility

Customizable playbooks and API integrations ensure adaptability to evolving security needs.

Enhanced Security Posture

Comprehensive insights and proactive measures ensure robust protection of critical assets.

This integration ensures enhanced visibility and agility in addressing evolving cybersecurity challenges.

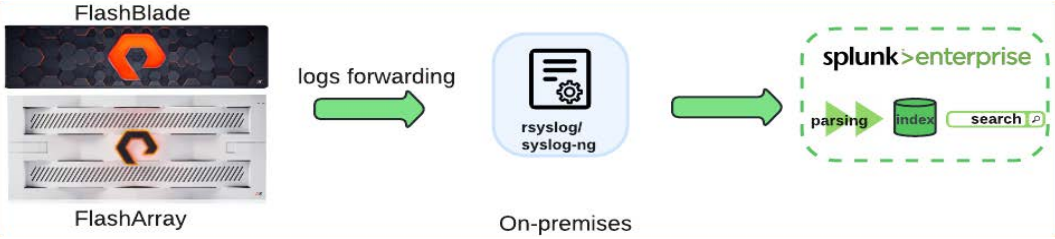

FIGURE 1 Splunk Enterprise SIEM integration with Pure Storage FlashArray and FlashBlade

Technical Components

Pure Storage

Pure Storage is a leading data storage company specializing in innovative solutions to support modern business demands, ensuring speed, simplicity, and efficiency while maintaining robust data security and integrity.

FlashArray™: An all-flash storage solution designed for databases, virtualized environments, and enterprise workloads.

FlashBlade®: An unified fast file and object storage platform built for unstructured data workloads. It excels in delivering rapid data access and high throughput, making it suitable for analytics, artificial intelligence (AI), and machine learning (ML).

Log Forwarding

A Syslog server in the centralized system receives and stores log messages which are forwarded from a FlashArray or FlashBlade system. It enables real-time monitoring, troubleshooting, and analysis of system events for improved security and performance.

Splunk Enterprise SIEM and SOAR

Splunk Enterprise SIEM provides real-time threat visibility by aggregating and analyzing infrastructure data, enabling effective monitoring and incident response. Splunk SOAR enhances incident workflows by automating actions such as isolating compromised systems, blocking malicious IPs, and creating Pure Storage snapshots for threat mitigation

Streamlined Alert Response: Integrating Pure Storage, Splunk SIEM, and SOAR

Integrating Pure Storage with Splunk Enterprise allows organizations to forward storage logs for comprehensive monitoring. Key capabilities include:

- **Syslog ingestion**: You can configure Pure Storage arrays to forward syslog messages to Splunk Enterprise, ensuring real-time visibility into storage-related activities and potential security events.
- **Log parsing with the Pure Storage Unified SIEM app**:
  Use pre-built regex patterns to extract relevant fields from Pure Storage logs. This enables detailed alerting and analysis, with custom alerts based on specific thresholds for prompt identification of potential threats.
- **Automated responses with Splunk SOAR**:
  The workflow begins with Splunk Enterprise SIEM identifying a specific alert type by the logs and forwarding it to Splunk SOAR, where machine learning evaluates their severity and triggers tailored playbooks for investigation, containment, eradication, and recovery. Predefined Custom lists enable proactive security by defining critical resources like storage volumes, protection groups, and access users. Assets act as connectors, integrating with external systems to streamline actions. Automated playbooks perform tasks such as creating snapshots or removing unauthorized users, enhancing storage infrastructure security. Organizations can also create custom playbooks for API-driven actions, ensuring adaptability to evolving threats. This seamless automation reduces manual intervention, accelerates response times, and fortifies overall security posture.

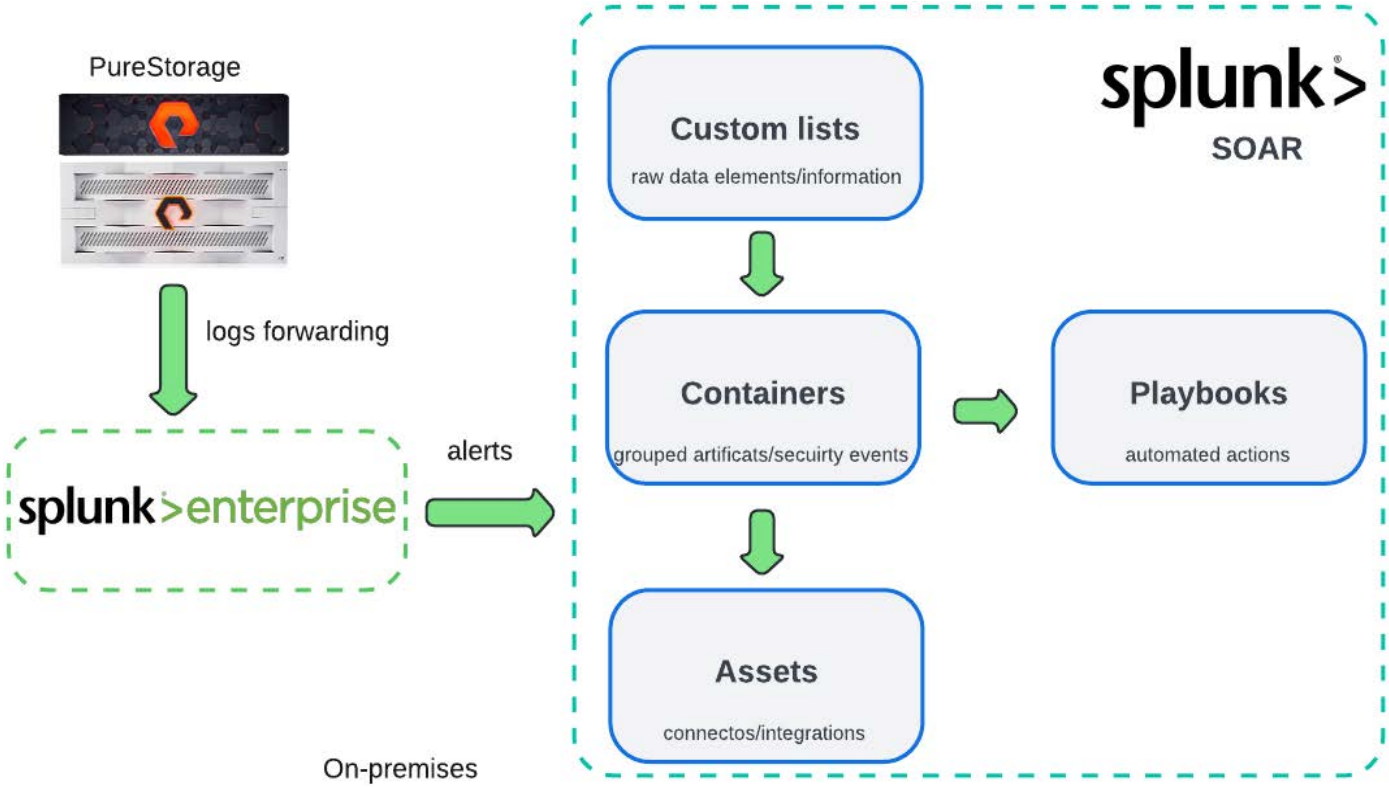

FIGURE 2 Splunk SOAR automated response

Use Case Scenarios

The following table lists a few common use case scenarios.

Target	Action	Description	Use Case
FlashArray	Take protection group snapshot	Creates a snapshot of all volumes within a protection group.	An attack is detected and a SafeMode™ snapshot is taken to secure critical data.
	Take volume snapshots	Creates a snapshot of the volume.	An attack is detected and a SafeMode Protected snapshot is taken to secure critical data. Note: Volume level snapshots are only protected by SafeMode snapshots if SafeMode is enabled array-wide.
	Remove local user	Removes a local user from the FlashArray system.	A user account has been compromised and is trying to dump or delete critical data.
FlashBlade	Take file system snapshots	Creates a snapshot of the FlashBlade File systems.	An attack is detected and a file system snapshot is taken to secure critical data.

TABLE 1 Common Pure Storage and Splunk SIEM use cases.

PureStorage SIEM App for Splunk: Enhancing Storage Security

To simplify and enhance the integration of Pure Storage with Splunk Enterprise, the PureStorage SIEM App for Splunk is now available on the Splunkbase Portal. This app provides users with a powerful, pre-configured toolset for gaining actionable insights into their Pure Storage environments. For more information, you can visit the PureStorage SIEM App for Splunk.

Conclusion

The integration of Pure Storage FlashArray and FlashBlade with Cisco Splunk Enterprise SIEM and SOAR represents a significant advancement in enhancing infrastructure visibility and security. By leveraging advanced technologies, organizations can achieve comprehensive data aggregation and analysis, improving threat detection and response times.

This integration not only strengthens an organization's security posture but also enables security teams to operate more efficiently in the face of evolving cyber threats. As organizations navigate the complexities of cybersecurity, the collaboration between Pure Storage and Cisco Splunk provides a robust solution for safeguarding critical data and infrastructure, ensuring both operational resilience and enhanced protection against potential risks.

Additional Resources

- Learn about how comprehensive data protection solutions from Pure Storage help safeguard critical data.
- Discover how SafeMode secures data from ransomware attacks.
- Learn how Splunk Enterprise enhances data analysis.
- Learn how Splunk SOAR orchestrates workflows and automates tasks.
- Learn about SOAR integration
- PureStorage SIEM App for Splunk

PS2718-01-en 02/25