Commvault + splunk> a cisco company

SOLUTION BRIEF

Enhanced threat detection and response with Commvault and Splunk SOAR

Commvault Cloud integrates with Splunk SOAR to help improve threat detection and drive faster, more automated response.

CHALLENGE

As organizations face an overwhelming volume of security threats, they're faced with the challenge of managing the triage and response to the daily onslaught of threat indicators and events generated. Manual incident response processes are time-consuming and error-prone, making it difficult to manage and prioritize incidents effectively. Additionally, siloed management of various security tools and systems can be a significant hurdle, as disjointed systems hinder efficient threat detection and response. These issues can strain IT and security teams, impacting their ability to protect the organization from evolving cyber threats.

SOLUTION OVERVIEW

The integration of Commvault Cloud with Splunk Security Orchestration, Automation, and Response (SOAR) provides a powerful solution that enhances data management, security operations, and incident response. This integration enables Security Ops teams to respond swiftly to threats using pre-built integrations and playbooks to secure and audit backups and backup software ecosystems. It allows organizations to monitor anomaly alerts from Commvault Cloud and respond with orchestrated actions to help fortify how critical data is secured and protected. Commvault Cloud and Splunk can help organizations improve their security posture and deliver faster, more coordinated response after a cyber attack or security incident.

Automate to Simplify

With Splunk SOAR you can streamline complex workflows with support for over **2,800** automated actions.

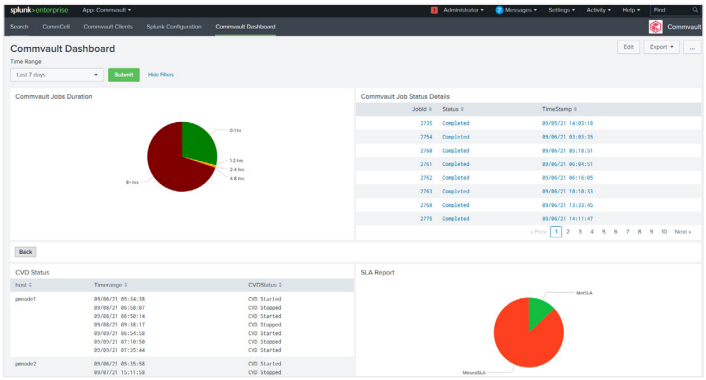
SOLUTION BENEFITS

Integrating Commvault Cloud and Splunk SOAR can help organizations simplify operations and see the following benefits:

- **Accelerated incident response**
- **Expanded threat detection**
- **Enhanced information sharing**
- **Better cross-team coordination**
- **Streamlined workflows**
- **Improved security posture**

SOLUTION CAPABILITIES / USE CASES

By integrating Commvault Cloud with Splunk SOAR, organizations improve their incident response processes. With this integration, Commvault sends threat detection and backup intelligence directly to Splunk, enriching security events and alerting SecOps teams to incidents.



Highlight	Description
Enriched threat intelligence	Security operations team are alerted via Splunk to Commvault-detected threats such as malware infections or threat actors interacting with traps.
Consolidated security event data	Threat detection details generated by Commvault can be collected and alerted by Splunk alongside incident/alert info from hundreds of other ecosystem partner technologies.
Automated threat response	Respond to security incidents with meaningful actions (playbooks) that fortify and protect data within Commvault Cloud. Actions like disabling data aging, disabling users, or disabling IDP.
Improved cross-organizational collaboration	Bridge the gap between SecOps and ITOps and facilitate better, more coordinated response and management of security incidents.

ABOUT SPLUNK ENTERPRISE

Splunk Enterprise is a Security Orchestration, Automation, and Response (SOAR) system that combines security infrastructure orchestration, playbook automation, and case management capabilities to integrate your team, processes, and tools to help you orchestrate security workflows, automate repetitive security tasks, and quickly respond to threats.

splunk.com

ABOUT COMMVAULT

Commvault (NASDAQ: CVLT) is the gold standard in cyber resilience, helping more than 100,000 organizations to uncover, take action, and rapidly recover from cyber attacks—keeping data safe and businesses resilient and moving forward. Today, Commvault offers the only cyber resilience platform that combines the best data security and rapid recovery at enterprise scale across any workload, anywhere with advanced AI-driven automation—at the lowest TCO.