Trusted Cyber Technologies

THALES

Thales TCT and Splunk:

Identifying complex security and compliance threats that puts your data at risk

splunk>

Security Intelligence solution for Splunk

- Alerts when unusual or improper data access is detected
- Offers detailed user and process information to help investigation
- Protects across heterogeneous environments, including file systems, databases, big data implementations, VMs, cloud environments and SAN/NAS devices

The Problem: Threat Landscapes Have Drastically Changed

With advanced persistent threats (APTs), now common—hackers are actively seeking to steal credit card data, personally identifiable information (PII), critical intellectual property (IP), and other legally protected information to sell to the highest bidder. Some of the most effective tools for fighting these attacks are the security intelligence and threat detection capabilities of Security Information and Event Management (SIEM) solutions. SIEM solutions monitor both real-time events and track long-term data to find anomalous patterns of usage, qualify possible threats to reduce false positives, and alert organizations when risks are detected. The CipherTrust Manager from Thales enhances SIEM solutions by providing an additional data feed on events that are occurring on the internal network and provides rich data points about protected data-at-rest.

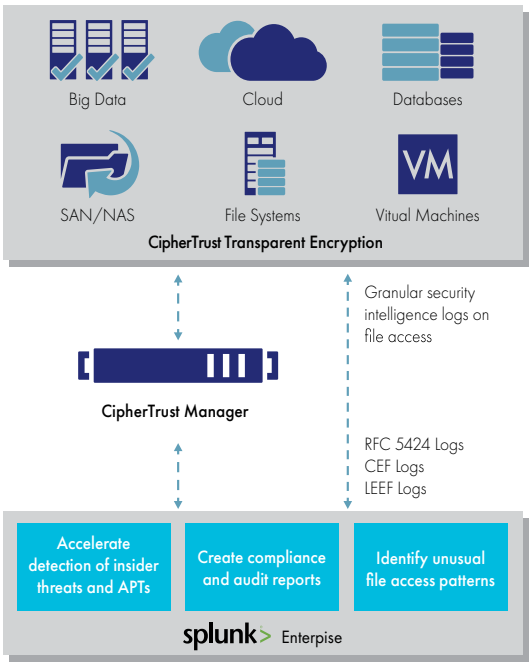

Figure 1:CipherTrust Manager feeds Splunk with the insider file access intelligence needed to identify and stop complex security and compliance threats.

Splunk and Thales simplifies security and minimizes risk

The solution: CipherTrust Data Security Manager and Splunk

- When used with an Operational Intelligence platform such as Splunk, the CipherTrust Data Security Platform not only encrypts and controls access to your files and databases, but also provides information that is utilized by Splunk Enterprise. Whether the deployment is physical or virtual, the CipherTrust Security Intelligence Solution for Splunk can alert you when unusual or improper data access is detected, and can offer detailed user and process information to help investigation. You will gain insight to not only see what is happening from the "outside-in," but also from nefarious activity that may be due to the insider threat. This capability is available as part of the extensible CipherTrust Data Security Platform, providing protection across heterogeneous environments—file systems, databases, big data implementations, VMs, cloud environments and SAN/NAS devices. This capability helps to catch bad actors in action, which includes: Identifying anomalous process and user access patterns for investigation. CipherTrust logs detail the processes and users accessing protected data. Splunk then performs an analysis of log information, which identifies usage patterns that are inconsistent with that user or process profile. This could identify an ATP attack or malicious insider action.
- Visualizing unauthorized access attempts to protected data. CipherTrust Data Security identifies and controls access, including privileged users. When attempts are made to access protected data by an unauthorized user or process, data is logged and made available to Splunk. Even privileged users logged in with authorized user credentials (e.g., using Switch User commands) are controlled and logged.

The CipherTrust Security Platform is available for sale to the U.S. Federal Government exclusively through Thales Trusted Cyber Technologies.

Why Use CipherTrust Data Security Platform with Splunk?

The CipherTrust Data Security Manager strengthens and simplifies security by automatically feeding logged information to Splunk Enterprise, which proactively monitors activity and alerts when it detects irregularities. These irregularities are usage or login patterns that fall outside of a user's credentials. This proactive automation can help thwart malicious attacks or actions before they cause harm.

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., protects the most vital data from the core to the cloud to the field. We serve as a trusted, U.S. based source for cyber security solutions for the U.S. Federal Government. Our solutions enable agencies to deploy a holistic data protection ecosystem where data and cryptographic keys are secured and managed, and access and distribution are controlled.

For more information, visit www.thalestct.com

Splunk

Splunk was founded to pursue a disruptive new vision: make machine data accessible, usable and valuable to everyone. Splunk's Security and Compliance solutions provide real-time security monitoring, historical analysis and visualization of massive data sets, providing security intelligence for both known and unknown threats. Splunk facilitates data exploration of incidents in real time to perform comprehensive incident investigations, maintain a proactive defense and support the creation of ad hoc reports in minutes.

3465 Box Hill Corporate Center Drive, Suite D, Abingdon, MD 21009 • 443-484-7070 • info@thalestct.com
thalestct.com