splunk>

TECH BRIEF

SPLUNK® FOR CDM PHASE 2

Introduction

The Department of Homeland Security (DHS) and General Services Administration (GSA) created the Continuous Diagnostics and Mitigation (CDM) program to enhance and modernize the security posture for Federal Departments and Agencies (D/A). Phase 1 of the program was targeted on endpoint security and was rolled out in 2014/2015. Phase 2 of the program, rolling out late 2015 and 2016, monitors and manages user-based accounts and services, moving from endpoint to internal network activity. The four functional tool areas of CDM Phase 2—TRUST, BEHAVE, CRED and PRIV—will be deployed to verify trust levels, training, credentials and access rights according to established D/A policies.

DHS and GSA have approved Splunk® Enterprise and Splunk Enterprise Security (Splunk ES) for all four functional areas of Phase 2. The software will correlate multiple data sources to create and monitor the Master User Record (MUR)—the central repository of attributes for all four tool areas—to alert and remediate instances, in real time, when the MUR reflects a delta from the "desired state" as defined by D/A policy.

Splunk Enterprise and Splunk ES have also been approved for Phase 1. The Splunk platform can serve as the Master Device Record (MDR) of Phase 1, which is hardware asset, software asset and configuration settings management, and integrate these with the MUR. The Splunk platform is the **only solution that can fully integrate Phase 1 and Phase 2 technologies into a single, holistic view of the enterprise.**

The Splunk Platform: Delivering Operational & Security Intelligence Worldwide

Splunk Enterprise collects machine-generated and other data from virtually any source and indexes the information without the need for normalization or fixed schemas. Data can be flexibly sorted, collated and visualized in dashboards and reports for both historical and real-time visibility into any and all network activities.

The Master Record for All Tools & Data

CDM envisions the creation of a MUR for every D/A user. Because the MUR houses the data elements defining the real state of user activity, it can help identify deltas between the desired and real states to reveal potential risks.

Splunk Enterprise serves as the MUR by ingesting data from all Policy Decision Point (PDP) and Policy Enforcement Point (PEP) tools. It communicates bi-directionally with PDPs to exchange data on desired and actual states to determine if deltas or defects exist. If the Splunk platform or a PDP detects a defect based on policy, Splunk software can generate an alert and/or run a script to bring the user into compliance with the defined policy. The Splunk platform integrates with all known approved Phase 2 tools. It indexes and monitors data in real time and provides alerting and reporting based on defined thresholds.

The Splunk platform is highly scalable and can support large-scale environments of 500,000 endpoints or more, and can ingest terabytes of data from individual tools and deliver appropriate streams to the CDM dashboard. As a result, Splunk software can break down data silos in even the largest agencies. Rather than monitor separate systems, agencies will gain unified, real-time views of their data and processes.

The Splunk Solution for Phase 2 Tool Areas

TRUST—the trust accorded to users

Users within D/A environments must have levels of trust commensurate with the sensitivity of the data and resources they access. Splunk can use identity information from sources like asset databases and Active Directory (AD) to maintain a list of known identities. It then correlates incoming information against this record. Splunk will build a master record of data on all **Currently granted trust levels for each person employed by the D/A** including:

- Status of Trust Level (i.e., Pending, Authorized, Suspended, Revoked, Expired)
- Date initially authorized
- Date last authorized
- Date revoked
- **Values of local enhancements** including date of last status change, or any other data to compare with locally-defined desired state specifications.

BEHAVE—the behavior of users

Users should be granted access to facilities, systems and information only when they possess the appropriate security training, skills, knowledge or certification. Without proper training, they can pose risks by engaging in behaviors that jeopardize systems, expose sensitive data or subvert security policies. In real time, Splunk will identify the **Level of training completion for each authorized user** including:

- Training identifier
- Status
- Date first trained
- Date of most recent training

CRED—the credentials assigned to users

Poor credential management and authentication practices increase the risk of unauthorized users accessing buildings, networks and information. Examples of faulty practices include weak passwords, unsecured physical tokens or not enforcing two-factor authentication for remote access to restricted information. The Splunk platform can correlate data from HR databases or repositories like Active Directory or e-learning systems with TRUST and BEHAVE information to determine which users require security awareness training. For example, Splunk searches can identify when additional training is required by comparing data like web access and proxy logs with such behaviors as visiting inappropriate websites, accessing resources with default/shared account names and clicking on phishing emails. Splunk will build a master record on all **Issued credentials for each authorized user employed by the D/A** including:

- Credential ID
- Person credential is issued to
- Status
- Date initially authorized
- Date last authorized
- Date revoked

Additionally, Splunk will build a record of **Information for every user account** including:

- Date/time account was established
- Date/time account was last accessed
- If the password must be reset at next login and date requirement was placed on account
- If multifactor authentication is required
- If a hardware token is required or enabled (or both) for authentication
- If a password is required or enabled (or both) for authentication
- If biometrics are required or enabled (or both) for authentication
- Credential ID if one is associated with account access

- If a password complexity enforcement mechanism was used for the account (if passwords are enabled) and which one
- If the default password is still valid for any known default accounts
- Date/time password was last changed
- Date/time account was last accessed

PRIVILEGES—the access rights granted to users
Agencies assign privileges based on access requests, but as jobs and missions change, privileges are rarely removed, resulting in the risk of improperly accessed resources. Splunk Identity Correlation will capture and log attempted access across a multitude of platforms and network devices, tracking unwanted users with repeated login failures, unauthorized access attempts and inappropriate privilege escalation. By monitoring the use of credentials across multiple domains and authorization granted to those credentials, Splunk software ensures that identities on the network are who they claim to be and are only accessing resources for which they are entitled. Splunk will build a master record of **Any authorized physical accesses for each person employed by the D/A** including:

- Status
- Date initially authorized
- Date last authorized
- Date revoked

Information for every user account includes:

- Date/time account was established
- If the account is disabled and date disabled
- If the account is locked and date locked
- Date/time account was last accessed
- Access restrictions applied to account
- Privileges enabled by account.

Dynamic Correlations Across the Enterprise

The power to correlate disparate data sources is the key to CDM. D/As often deploy PDPs and collect data from identity, credential, access management and e-learning systems, but often without implementing a correlation engine. As a result, they are limited to the visibility and awareness of each individual tool and the attributes it collects. They are unable to correlate data across multiple tools for comprehensive visibility and awareness.

The Splunk platform provides true situational awareness of risk by dynamically correlating data from all four Phase 2 tool areas. Every attribute of desired and real states—not just those siloed in one tool area—are compared and analyzed for compliance and defects. By correlating different data types across diverse toolsets in real time and without requiring normalization, Splunk software ensures there are no gaps in views of the holistic enterprise. For example, log data may represent a user as an employee number, but the HR system may use the employee's full name. By collating data from both sources, the solution presents a unified perspective of the employee and eliminates false alerts.

The Splunk platform issues alerts when it detects any anomaly. Someone who logs into the network might be confirmed to have Trust and Privileges, but not Credentials. Splunk software will alert this action as someone seeking to access the network without proper credentials. Other examples of behavior that would trigger alerts include:

- A user's clearance has lapsed
- A user is accessing file systems for which they are not entitled
- A user has not completed mandatory training
- A user is logging in from a geographic area outside of policies or improperly using a VPN

Splunk ES strengthens the monitoring of user behavior with advanced anomaly detection and enhanced risk scoring. It prioritizes risks based on rules and policies, and enables the most serious incidents to be remediated promptly—before they impact the organization.

Investigations & Remediation

The value of the Splunk platform extends beyond identifying deltas between desired and actual states. Its unified views of all data sources eliminate the need to manually gather data across individual point solutions for analyses. The solution not only correlates data between all Phase 1 and Phase 2 sources, it also can integrate data from Phase 3 sources for holistic visibility, or tools deemed outside the scope of CDM. Without this visibility, agencies could lack the insights to even know that remediation is necessary.

Splunk software also provides deep-dive search functionality for forensic investigations. Analysts can examine patterns of data, trends in network and host access behaviors, and rapidly identify activity and patterns that lie outside of the norm. They then can drill down to the original source events for corroboration and further granularity.

The solution can also take precautionary measures proactively or when analysts detect issues. For example, analyst can use the Splunk Search Processing Language (SPL®) to deny access to a particular resource or the entire network. If they detect suspicious activity, they can trigger enhanced monitoring, including video monitoring, for a forensic record.

Only the Splunk software offers a complete platform for the CDM program. It uniquely tracks all other toolsets used for CDM, for identifying potential security risks and issues, and for remediation to ensure compliance.

With the Spunk platform, governments can gain the visibility and intelligence to lower costs, improve security, streamline IT operations and better serve the public. Learn more

splunk> sales@splunk.com www.splunk.com