splunk>

FACT SHEET

Splunk® for Cisco Identity Services Engine AddOn

Using Splunk Enterprise to Extract Additional Value From Cisco ISE Deployments

Cisco Identity Services Engine (ISE)

Cisco ISE offers a centralized control point for comprehensive policy management and enforcement of bring your own device (BYOD) policies in a single RADIUS-based product. It starts with rigorous identity enforcement that includes an automatic device feed service to keep the product populated and up-to-date with the latest smartphones, tablets, laptops, and even specialized network-enabled devices used in the retail, healthcare and manufacturing industries.

Cisco ISE offers an easy onboarding experience for BYOD and guest workers, so that personal devices can meet security policy and be secured and granted access via a simple self-service portal. Cisco ISE reduces operational costs and improves efficiency by leveraging existing network visibility and policy control to streamline efforts for secure access.

Implementing Cisco ISE allows the enterprise to:

- Accurately identify and assess all users and devices connecting to the network
- Grant, limit and quarantine network access in alignment with the company's appropriate business policy or security compliance requirements and guidelines
- Ensure seamless onboarding, roaming and network access control throughout any multi-vendor infrastructure that is 802.1X-compliant
- Apply business policy enforcement via network access controls, MDM device

Why Splunk for Cisco ISE?

Splunk Enterprise takes in any data without upfront normalization, scales to collect and analyze hundreds of terabytes of data per day, and applies a 'late binding schema' based on the kinds of questions you want to ask of your data. The flexibility and scalability of Splunk Enterprise makes it uniquely suited to correlate data from Cisco ISE with other data sources, including firewalls or application data, for deeper operational and security visibility (see Figure 1).

Splunk Enterprise supports complex correlations across structured and unstructured data types, the creation of exact match searches and searches that monitor for statistical outliers and trends in real time. The software also embraces the concept of 'lookups' to other data stores that may contain important context for security events, such as employee schedule management data, supervisor information or even marital status changes as additional context important to understanding insider threats. Splunk software can access this data from traditional databases, files and Hadoop (HDFS) based systems. Easy access to the data without the cost of connector lifecycle

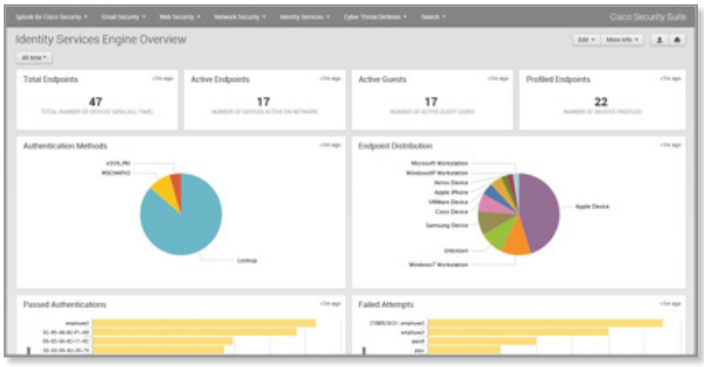

Figure 1. Cisco Identity Services Engine.

maintenance encourages IT security professionals to construct IT risk-based scenarios and freely ask questions of their data.

Splunk Enterprise has out-of-the-box support for Cisco ISE with the Splunk for Cisco ISE AddOn and the Splunk App for Cisco Security Suite (see Figure 2).

Sample scenarios and use cases:

- Compare the total number of active endpoints in the environment against known baselines
- Track contractors separately from regular employees, including their movements and access based on where they login to the network
- Monitor logins by device type to understand unusual or rare device type authentications
- Baseline successful and unsuccessful logins to identify anomalies
- See real-time and historical changes by user, applied to security rules on all security appliances
- Determine where a person was when a device that used that person's credentials was involved in a security issue in real time
- Monitor changes to policies implemented in ISE to know if any changes happened outside of specific change windows
- Monitor and troubleshoot the health of the ISE appliance

Visibility Into Custom Application Logs

For comprehensive investigations and effective root-cause analysis, a review of data from traditional security sources typically isn't enough. Security events and their impact on mission-critical applications need to be reviewed as part of the attack timeline.

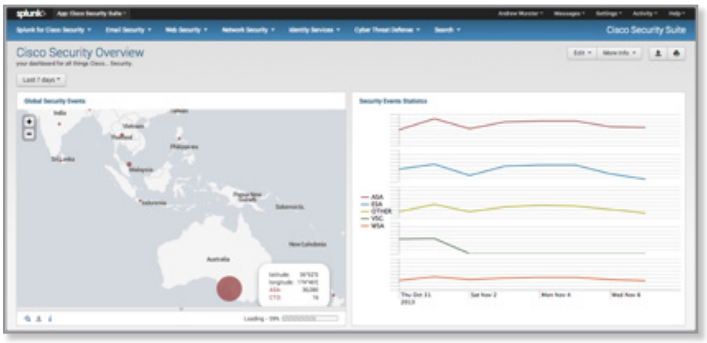

Figure 2. The Splunk for Cisco Security Suite.

The Splunk for Cisco ISE AddOn can correlate access data from custom applications with other critical business applications. This can help to support insider threat and fraud use cases.

Splunk software's ability to accept multi-line application logs, its freeform search language and its interactive interface let you see the complex characteristics of an incident. For example, you can know that an attacker gained access to the network but was blocked at the application-level, avoiding further exploit. The security picture is not complete without visibility into virtually all the data, including applications. If a successful attack occurs, the security team should know the full extent of any data loss.

Baseline Activity and Identify Outliers

Monitoring activities represented in machine-generated data allows you to build baselines around user identity and watch for statistical outliers. These outliers can either be the triggers for an investigation or supporting evidence of a data breach from an advanced threat. Tracking credentialed activity throughout the IT infrastructure allows for better employee accountability and process tracking for compliance purposes.

Cisco Data and Beyond

The Splunk for Cisco ISE AddOn leverages the native capabilities of the core Splunk engine. Splunk Enterprise provides the ability to search, report, monitor and analyze real-time and historical machine-generated data—physical or virtual. Splunk works across vendor environments, all from a single interface, to provide a comprehensive view of security and application data on the same timeline.

Free Download

Download Splunk for free. You'll get a Splunk Enterprise 6 license for 60 days and you can index up to 500 megabytes of data per day. After 60 days, or anytime before then, you can convert to a perpetual Free license or purchase an Enterprise license by contacting sales@splunk.com.

Try Out the App, it's Free!

To download the Splunk for Cisco ISE AddOn, Cisco Security Suite, or any other Cisco apps and AddOns please visit apps.splunk.com.

250 Brannan St., San Francisco, CA 94107 info@splunk.com | sales@splunk.com 866-438-7758 | 415-848-8400 www.apps.splunk.com

Item # FS-Splunk-CiscoISE-101