# Table of Contents

Introduction ............................................................................................................................................3
Stovepipe Systems and Cybersecurity Risk.................................................................3
Introducing CSCA .................................................................................................................................4
Ingestion ............................................................................................................................................4
Correlation .........................................................................................................................................5
Search & Visualizations .......................................................................................................................6
Advanced Analytics .............................................................................................................................6
Architecture .........................................................................................................................................7
Conclusion ...............................................................................................................................................7
Introduction

In the modern connected world, public and private enterprises are facing ever-growing cyber threats. Companies can make significant investments using a litany of tools and still not have the full, real-time visibility into their data they need to effectively analyze all their activity. As companies grow via mergers and acquisitions, they have a limited view of external threat actors, insider threats, and vulnerability information across their enterprise. The questions that keep CISOs up at night include:

» When I become aware of a potential issue how quickly and effectively can I analyze and report on it?

» Do I have visibility into all of my assets?

» How fast can I spot threats to my organization?

» How does a newly-discovered vulnerability affect my enterprise?

To answer these questions, companies need to stand up a central data lake before they are asked. Situational awareness is impossible when data is dispersed geographically or in multiple systems and tools. Centralization is only the first step, though. The data has to be collected, correlated, tied to your infrastructure, and configured to power the right visualizations and analytics. What if a platform did all these things and let you answer the questions above in near real-time? Introducing Sierra Nevada Corporation’s Cybersecurity Correlation and Analytics (CSCA) platform.

CSCA is a massively scalable security orchestration and analytic platform.

It centralizes and automates the collection, triage and detection of cyber threats so you can search, visualize, report and respond to them efficiently and with greater accuracy.
Stovepipe Systems and Cybersecurity Risk

Many companies have invested in multiple cybersecurity tools such as IPS (Intrusion Prevention System), IDS (Intrusion Detection System), firewalls, SIEMS, threat intelligence feeds etc. Each application across the enterprise has its own set of users, from SOC analysts to management, and disparate pockets of data that exist in many different places. The end result is stovepipe systems that lead to a lack of situational awareness. With no centralized repository in place, logs are reported in scattered locations, resulting in latency that can be the difference between a stopped attack and huge security breach. Companies lack insight into possible lateral threats. Imagine a company has a security breach in their French branch, which then moves to their branch in Germany and then the US. This attack could have been stopped at the French location if a centralized system was in place.

Stovepipe systems restrict ability to view data across the enterprise.
Introducing CSCA

In 2014 Sierra Nevada Corporation (SNC) entered into a partnership with one of the world’s largest international banking institutions to take their cybersecurity architecture to the next level. This joint effort became the CSCA platform. It was designed to provide security teams with centralized visibility into full network and security data in order to enable rapid analytics, detection, and reporting capabilities that are essential in today’s fight against advanced threats and determined threat actors.

Today, CSCA leverages leading-edge, open-source technologies to provide visibility of unknown threats, and increase productivity in both cyber security and business processes.

A centralized data lake provides a comprehensive view to all users regardless of their role in the organization.
Ingestion

CSCA can scale to any organization large or small. On the high end of the scale CSCA has proven ingest speeds of over 250k records per second, can handle over 20 terabytes per day, and has a maximum storage capacity of over 2.5 petabytes. CSCA indexes all data at the time of ingestion, which delivers superior query performance. The ingestion process is customizable to any data source.

Data is ingested using pipelines composed of generic, reusable stages. You can create a pipeline to ingest just about any data you wish. Below is a subset of data sources that are typically ingested and correlated:

- Firewall Logs
- Intrusion Detection Logs
- Intrusion Prevention Logs
- Web Content Filtering / Proxy Logs
- Router Logs
- Email Logs
- Print Logs
- Netflow and Packet Capture
- Any other data sources
Correlation

Infrastructure and threat data are also ingested using pipelines and are combined with other sources to link cyber activity with specific company information like user data, asset data or threat data. This provides context to your data and enhances your situational awareness to better understand threats. Below is a subset of possible correlation sources:

» Active Directory
» Threat Database
» Geolocation/IP2Location
» Who Is
» Virus Total
» pDNS
» Access Control Lists
» Alexa top websites
» Looking Glass
» Cyvailance
» iSight
» MaxMind
» MACOUIDB
» Any other data enrichments
Search & Visualizations

Data is indexed at ingestion to support ultra high speed searching. You can search hundreds of terabytes of data in seconds or minutes. Options to search include Basic, Template Queries or Advanced Search. Basic Search has a point and click interface to help non-technical analysts search for data of interest without knowing any programming languages. Template Queries provide fast answers to frequently asked questions. Advanced Search provides a SQL like language that lets the more technical analysts ask complicated questions at any level of detail.

Near real time searching enables near real time visualizations. Many SIEMs offer visualizations and reports but these reports can take a long time to run and update data. CSCA lets you see developing cyber situations in near real time. Visualizations generated with CSCA show the situation as it was minutes or even seconds ago.
Advanced Analytics

CSCA is an open analytic platform supporting many analytics, from simple out-of-the-box, rules-based analytics, to complicated and custom analytics that find threats unique to your organization. Analytics results are themselves a searchable data source in CSCA providing a historical view into how threats and key metrics are connected and develop over time. Analytics support customized alerts based on user defined criteria. Below are common examples of analytics provided by CSCA.

**Threat Match**
Trigger an event on any data matching threat databases.

**Geographic anomalies**
Find users connecting from Detroit and Denver 30 minutes apart.

**Data exfiltration**
Find users exfiltrating data from the company.

**Web Browsing**
Find unethical browsing habits/destinations

**Terminated Employees**
Find activity by former employees.

**Baseline Analysis**
Find behavior that significantly deviates from the norm for your company.

**Risk Scoring**
CSCA helps summarize and prioritize the risk your organization faces, so you can investigate the largest threats first. Sum all events across activity, infrastructure, geography, business units, threat databases, or any other dimension to show where your greatest risks are, so you can prioritize them.

**Forensics**
When an incident has occurred, CSCA provides a correlated, searchable, and comprehensive database from which related information can be quickly established and documented. For instance, when an individual has violated policy exposing the company to risk, CSCA provides a central location from which to quickly discover the other assets, individuals, and activities potentially involved.

**Visibility**
CSCA helps you identify gaps and incongruities in your coverage. For instance, an internal IP address talking to the outside world but not otherwise audited, a terminated employee still using company resources, or employee activity indicating two different physical locations at the same time are all suspicious activities that would be easily identifiable in CSCA.

**Anomaly Detection**
CSCA analyzes cyber behavior along any measurable dimension to establish “baseline” behavior. Then it uses that baseline behavior to find deviations and alert on them. A prominent example is finding websites that are being used by the company without a valid EULA (End Use License Agreement) in place.
Architecture

CSCA is an integrated solution leveraging open source technologies to minimize long term costs and maximize capability. The figure below shows the architecture.

The CSCA platform can be implemented on or off premises.
Conclusion

CSCA centralizes and automates the collection, triage and detection of cyber threats so you can search, visualize, report and respond to them efficiently and with greater accuracy. It is the clear choice for companies looking to centralize their cyber-security strategies.

FOR MORE INFORMATION ABOUT CSCA OR FOR A PRODUCT DEMONSTRATION, PLEASE CONTACT SIERRA NEVADA CORPORATION AT csca@ncontext.com

© 2015 – 2019 Sierra Nevada Corporation All Rights Reserved.