Hewlett Packard
Enterprise

Case Study

HPE Cyber Defense Center safeguards global resources every minute, every day

Largest showcase deployment of HPE security technologies and operational excellence

Objective

Protect worldwide enterprise resources while serving as an operational best-practices model for innovation in enterprise security

Approach

- Deploy HPE ArcSight products and integrate data feeds from Intrusion Prevention Systems and other sources
- Analyze big data sources to conduct advanced analytics and alerting with the HPE Vertica Analytics Platform

IT Matters

- ArcSight products monitor about one billion events per day, reducing the event flow to a volume that can be managed by a handful of analysts—something that would take an army of over 30,000 analysts to perform manually.
- Events are correlated from about 600 TippingPoint IPS platforms and dozens of other sources to proactively detect threats. TippingPoint IPS actively detects and blocks about five million attacks per day.
- Vertica Analytics Platform allows the CDC to correlate over two billion records each day, and enables the staff to perform queries 50-1,000 times faster than possible with traditional databases, using a fraction of the hardware.

Business Matters

- HPE enterprise data is protected on a global scale for about 250,000 employees with a staff of only 22 security professionals.
- The CDC serves as a framework for global enterprise security to keep HPE security best practices continuously refreshed and highly effective.
- Innovations in CDC security practices are transferred into HPE security products and services to keep customers steps ahead of cyber threats.

The HPE Cyber Defense Center (CDC) offers world-class capabilities in operations, engineering, intelligence, and incident management for all of Hewlett Packard Enterprise (HPE). The CDC deployed much of the HPE ArcSight product family and integrated data feeds from approximately 600 Intrusion Prevention Systems (IPS), and performs complex analytics on massive quantities of web and syslog data with the HPE Vertica Analytics Platform for advanced analytics and alerting. This real-world testing ground not only protects the HPE global IT infrastructure, but also provides a framework to help HPE customers stay steps ahead of cyber attacks and seamlessly conduct business.

After analyzing over 90 customer security operations centers (SOCs) throughout the world and accumulating the largest dataset of its kind, HPE has taken industry best practices and lessons learned and applied them to its own Cyber Defense Center.

The CDC demonstrates not only HPE's ability to gain a collective 3D view of the entire enterprise, but it also serves as a showcase for enterprise security innovation, protecting one of the company's most important assets: data.

The CDC, which opened in the fall of 2013, leverages the lessons HPE has learned from more than 10 years of security operations implementations. It is already one of the largest SOCs in the world, protecting the HPE global IT infrastructure from cyber attacks while providing a forum to showcase HPE security expertise to customers and partners. For example, it has protected HPE from attack types such as Heartbleed and Shellshock, malwares that could have resulted in extreme vulnerabilities and exploitation if not detected and patched.

In alignment with the “HPE on HPE” vision that HPE IT should be the company’s foremost showcase, the CDC team has deployed the majority of products within the HPE ArcSight product family and integrated data feeds from approximately 600 Intrusion Prevention System platforms deployed worldwide. HPE also collects logs from web servers and other sources and conducts advanced analytics and alerting with the HPE Vertica Analytics Platform.

This real-world testing ground allows HPE to secure its own IT infrastructure, and it also allows HPE to analyze cyber threats while translating insights into future advances

in HPE security products and consulting services.

It represents a major accomplishment in security intelligence at a massive scale, since HPE currently has:

- 20,000 network devices
- 37,000 servers
- 330,000 employees
- 450,000 managed endpoints

Correlating data across dozens of platforms

The TippingPoint IPS platform is deployed at HPE locations worldwide and managed locally, with the CDC serving as the primary consumer of their intrusion prevention events to provide proactive network security for HPE network traffic and data centers.

ArcSight solutions centrally correlate logs from various sources so the CDC can proactively detect threats.

According to Marcel Hoffmann, senior manager of the HPE Cyber Defense Center, “At HPE, approximately five million attacks are actively detected and blocked per day. When a serious threat is detected, we sanitize the traffic and actively block those attacks.”

“We receive high-volumes of alerts from firewalls, but many of them are background noise,” Hoffmann explains. “Having a robust IPS platform provides a low-volume, high-fidelity feed of actionable alerts that we actively investigate.”

HPE ArcSight Enterprise Security Manager (ESM), HPE ArcSight Logger, and the IPS platforms work together to create a powerful, comprehensive cyber defense system. Each element plays a critical role in ensuring the security of HPE valuable information assets, which includes enterprise applications, customer information systems, intellectual property assets, and all the critical information resources available on the HPE enterprise network.

The IPS monitors and detects activity on the network, blocks malicious activity at the application layer, and feeds event data to ArcSight ESM. ArcSight Logger categorizes and stores the event information from the IPS and other sources.

ArcSight enables monitoring of logs from dozens of platforms from a single console and performs advanced correlation of events from multiple sources, including firewalls, Microsoft® Windows® Server Active Directory, HPE-UX, VMware, Microsoft.net, and VPNs, network devices and switches, web proxies, open source solutions, and databases. “We’re able to capture logs from most of the sources using ArcSight’s out-of-the-box connectors, and we use the HPE FlexConnector framework to build collection logic and contextualize logs for any others,” says Jorge Alzati, senior manager of ArcSight Engineering & Production Management.

> “The CDC has already detected and deflected thousands of potential attacks in just less than a year. Our cyber security program provides accurate security data to help management make fact-based decisions while helping us continue to implement a predictive security strategy.”
>
> — Marcel Hoffmann, Senior Manager, Cyber Defense Center, Hewlett Packard Enterprise

ArcSight ESM filters and correlates the data, arming analysts with the robust, high-quality information they need to perform effective security intelligence analysis. Implementation of the HPE security products followed the HPE Software Professional Services deployment methodology and incorporates high availability, disaster recovery, fault tolerance, and load-balancing properties.

Detecting and deflecting attacks

An enterprise the size of HPE receives probes for vulnerabilities and attempts to exploit vulnerabilities hundreds of times per second. The HPE ArcSight solution processes an average of one billion events daily, reducing the event flow to a volume that can be managed by the handful of analysts that are active during each CDC shift.

Those analysts further refine the alerts to 15-20 incidents that are referred for follow-up and remediation action. It would take an army of over 30,000 analysts to perform an equivalent function manually. Without ArcSight in place, that analysis would not be performed and those events would be left unexamined, leaving attacks in progress to remain undetected.

The ArcSight solution detects patterns of activity, correlates them, and creates alerts based on use-case rules. HPE manages an enormous amount of sensitive data that needs to be protected, including data from systems, employees, and customers.

ArcSight ESM provides the CDC with a centralized point to conduct all security monitoring. The CDC leverages ArcSight to detect threats in real-time so they can be mitigated quickly, and uses ArcSight to collect and correlate vast amounts of security data, which greatly improves the ability of CDC analysts to pinpoint and thwart genuine threats.

“The ArcSight solution provides a single view into the threat landscape and helps us maximize our security resources,” says Hoffmann. “Our analysts’ time and efforts can now be focused on filtered security events that indicate actual threats, instead of sifting through reams of raw data from separate monitoring systems.”

The data analysis provided by ArcSight supports faster and more effective mitigation, and presents a strong case to affected-assets owners, which is key for speedy and effective remediations. When an attack is detected, ArcSight helps CDC analysts document the facts and provide the proof needed to effectively engage asset owners and gain their buy-in on a solution.

Data feeds are centrally correlated across business units and geographies, providing the CDC with unique visibility into cyber threats.

"Large enterprises need the ability to quickly cross-correlate attack data across multiple planes so they can rapidly identify potential threats occurring across the company that individual business units or regions might not recognize," explains Alzati.

Hoffmann adds, "ArcSight offers a highly sophisticated correlation engine, and it enriches the event data to provide faster context analysis. This allows our analysts to work more efficiently and effectively, and enables quicker action to mitigate threats.

"ArcSight also allows us to detect reconnaissance activities when attackers are searching for weaknesses in our systems so we can block potential attacks before they occur."

The CDC continuously leverages its experiences to develop use cases to filter the data feeds and sharpen the alerting process. "It's important to proactively develop use cases to make sure the CDC team receives the proper automated alerts," Alzati says. "Operations staff reviews reports on a daily basis to ensure that the proper controls and instrumentation are in place, but once they have the right use cases, ArcSight serves as a single pane of glass that helps them make sense of all the log information to understand the security status of the organization."

The combination of the ArcSight ESM and TippingPoint IPS solutions has helped CDC analysts detect and deflect thousands of potential attacks. For example, the CDC proactively prevented attacks from the Padding Oracle On Downgraded Legacy Encryption (Poodle) exploit.

According to Hoffmann, "When we first heard about the Poodle vulnerability, we wrote a use-case rule in ArcSight to detect activity attempting to exploit the vulnerability. We blacklisted about 250 IP addresses based on ArcSight alerts resulting from the new rule, potentially blocking attackers from exploiting vulnerabilities."

Within moments of the Shellshock announcement in September 2014, CDC analysts learned that attackers were scanning HPE systems looking for vulnerabilities through alerts displayed on ArcSight ESM dashboards. "ArcSight showed us in real-time where the scans were coming from and what they were targeting," says Hoffmann. "In a short timeframe, we were able to report on HPE's vulnerabilities to Shellshock and drive prioritization of system patches to remediate them."

Big data correlation and analysis

Partnering with HPE Labs, the CDC implemented domain name server (DNS) logging appliances to collect logs from all six internal DNS clusters, which are then sent to the HPE Vertica Analytics Platform for advanced analytics and alerting. The Vertica Analytics platform manages massive amounts of data quickly and reliably, giving the CDC real-time business intelligence for advanced, big data analytics.

Customer at a glance

HPE Security Solution

- HPE ArcSight Enterprise Security Manager
- HPE ArcSight Logger
- TippingPoint Intrusion Prevention System & Thread Digital Vaccine
- HPE Vertica Analytics Platform

With Vertica, the CDC is able to perform queries 50–1,000 times faster than possible with traditional databases, using a fraction of the hardware. Unlike traditional relational databases designed for processing business data, Vertica is built from the ground up specifically for complex analytic workloads, and can easily handle the velocity and volume of data that is collected within a SOC.

"The CDC needs a big data analytics platform because traditional technology can't meet the velocity and fast data access demands necessary for swiftly analyzing big data," says Lin Li, cyber security enterprise architect for HPE. "For example, the CDC analyzes log files from over 130 internal web servers. With Vertica, we can store and inject these files as an hourly batch and process them so the CDC team can run the analytics."

The correlated logs from ArcSight are also ingested into Vertica, allowing the CDC to swiftly perform sophisticated big data analysis to mitigate threats and prevent future attacks. "Vertica allows the CDC to correlate over two billion records each day, with log files coming in from a wide variety of formats," Li explains. "With Vertica, the CDC can normalize and cleanse the data, and correlate it with other reference data. This allows the CDC to put the whole picture together so the team can understand the traffic coming into the HPE global network and efficiently secure enterprise resources."

Li continues, "Since Vertica is easy to use and compresses the data very well, it allows the CDC to cost-effectively store data and conduct historical analysis of past events. Most of the detailed queries against over 100 billion log records in Vertica return within one minute. This was impossible under the old architecture because this kind of throughput would simply be impossible with a conventional DBMS of comparable scale. This level of historical analysis enables the CDC to understand whether users may be exposed to previously unknown malware and perform proactive security improvements."

Preparing for the future

The CDC is in the first of a three-phased implementation strategy. The initial phase has focused on securing the perimeter by leveraging threat intelligence and reducing the attack surface. Phase 2 will concentrate on securing the application while Phase 3 will secure the business. The CDC's roadmap calls for complete deployment across the enterprise by 2017, and HPE continues to evolve best practices that can be leveraged by other large enterprises.

"Start small, don't try to boil the ocean," advises Hoffmann. "It's best to deploy enterprise security in phases, especially for very large enterprises with multiple divisions. Prior to deployment, identify the most critical assets, train your people on the products, and develop mature remediation processes."

The CDC is also planning for emerging security threats to ensure it is well prepared to address these future challenges—today.

With a focus on continuous improvement, the CDC continues to evolve while serving as a real-world testing ground for HPE products and services and a framework for operating an agile SOC with a relatively small staff of only 22 security professionals.

By operating one of the largest SOCs in the world, HPE is learning to extract even more value from each security dollar so that it can be passed onto HPE customers.

Learn more at
hpenterprisesecurity.com/

Sign up for updates

★ Rate this document

Hewlett Packard
Enterprise

4AA5-8767ENW, May 2016, Rev. 2