Hewlett Packard Enterprise

HPE Cyber Defense Center schützt globale Ressourcen rund um die Uhr

Größte Vorzeigebereitstellung der Sicherheitstechnologien und Operational Excellence von HPE

Ziel
Schutz der Unternehmensressourcen weltweit und Modellfunktion für betriebliche Best Practices für Innovationen im Bereich der Unternehmenssicherheit.

Ansatz
- Bereitstellung von HPE ArcSight Produkten und Integration von Datenfeeds aus dem HPE TippingPoint Intrusion Prevention System und aus Drittquellen.
- Analyse von Big-Data-Quellen zur Ausführung erweiterter Analyse- und Warnfunktionen mit der HPE Vertica Analytics Platform.

Herausforderungen der IT
- ArcSight Produkte überwachen rund eine Milliarde Ereignisse pro Tag. Dadurch wird der Ereignisfluss auf eine Menge reduziert, die von einer Handvoll von Analysten bewältigt werden kann. Normalerweise wären für die manuelle Überwachung über 30.000 Analysten erforderlich.
- Ereignisse werden von rund 600 TippingPoint IPS Plattformen und anderen Quellen aus korreliert, um Bedrohungen proaktiv erkennen zu können. TippingPoint IPS erkennt und blockiert aktiv rund fünf Millionen Angriffe pro Tag.
- Die Vertica Analytics Platform ermöglicht dem Cyber Defense Center (CDC) die Korrelation von über zwei Milliarden Datensätzen pro Tag. Dadurch können Mitarbeiter Abfragen 50 bis 1.000 Mal schneller durchführen als bei herkömmlichen Datenbanken. Zudem wird dazu nur ein Bruchteil der normalerweise benötigten Hardware verwendet.

Herausforderungen des Unternehmens
- Der Schutz der Unternehmensdaten von HPE erfolgt auf globaler Ebene für rund 250.000 Mitarbeiter durch nur 22 Sicherheitsfachleute.
- Das CDC dient als Rahmen für die globale Unternehmenssicherheit, mit dessen Hilfe die Best Practices von HPE für die Sicherheit ständig aktualisiert und so effizient eingesetzt werden können.
- Innovationen in Sachen Sicherheitspraktiken im CDC werden auf Sicherheitsprodukte und Services von HPE angewendet, damit Kunden den Bedrohungen aus dem Internet immer einen Schritt voraus sind.

Das HPE Cyber Defense Center (CDC) bietet erstklassige Funktionen in den Bereichen Betrieb, Engineering, Intelligence- und Incident-Management für das gesamte Hewlett Packard Enterprise (HPE). Das CDC stellt einen Großteil der HPE ArcSight Produktreihe bereit und hat Datenfeeds von rund 600 HPE TippingPoint Intrusion Prevention System (IPS) Plattformen integriert. Zudem werden mit der HPE Vertica Analytics Platform komplexe Analysen großer Mengen von Web- und Syslog-Daten durchgeführt, um erweiterte Analyse- und Warnfunktionen nutzen zu können. Durch diese realistische Testumgebung wird nicht nur die globale IT-Infrastruktur von HPE geschützt, sondern auch ein Rahmen bereitgestellt, der dafür sorgt, dass HPE Kunden Angriffen aus dem Internet immer einen Schritt voraus sind und einen unterbrechungsfreien Betrieb gewährleisten können.

Nach der Analyse von über 90 Sicherheitszentralen (Security Operations Centers, SOCs) von Kunden weltweit und der Erfassung des größten Datensatzes seiner Art hat HPE die Best Practices der Branche und die gewonnenen Erkenntnisse auf das eigene Cyber Defense Center angewendet.

Das CDC veranschaulicht nicht nur die Fähigkeit von HPE, eine 3D-Gesamtübersicht des ganzen Unternehmens zu erstellen, sondern dient auch als Vorzeigeobjekt für die Sicherheitsinnovationen des Unternehmens, die dem Schutz der wichtigsten Unternehmensressource dienen: den Daten.

Das CDC wurde im Herbst 2013 eröffnet und profitiert von den Erkenntnissen, die HPE in über 10 Jahren im Bereich Sicherheitsimplementierungen sammeln konnte. Das CDC ist heute schon eines der größten Security Operation Center (SOC) der Welt und schützt die globale IT-Infrastruktur von HPE vor Cyber-Angriffen. Zudem ist es ein Beweis für das Sicherheits-Know-how, das HPE seinen Kunden und Partnern bietet. Das CDC hat HPE bereits vor Angriffstypen wie Heartbleed und Shellshock geschützt – Malware, die zu einer extremen Gefährdung und Ausnutzung hätte führen können, wäre sie nicht entdeckt und beseitigt worden.

Im Einklang mit der Vision „HPE on HPE", was bedeutet, dass die IT von HPE als Paradebeispiel für das Unternehmen dienen soll, hat das CDC-Team einen Großteil der Produkte der HPE ArcSight Produktreihe eingesetzt und Datenfeeds von rund 600 HPE TippingPoint Intrusion Prevention System Plattformen weltweit bereitgestellt. Darüber hinaus sammelt HPE Protokolle von Webservern und anderen Quellen und führt mit der HPE Vertica Analytics Platform erweiterte Analyse- und Warnfunktionen aus.

Diese realistische Testumgebung ermöglicht HPE den Schutz der eigenen IT-Infrastruktur und sorgt dafür, dass HPE Cyber-Bedrohungen analysieren und Erkenntnisse zukünftig in seinen Sicherheitsprodukten und Beratungsservices umsetzen kann.

Dies stellt im Hinblick auf die Security Intelligence eine erhebliche Verbesserung dar, denn HPE verfügt über:

- 20.000 Netzwerkgeräte
- 37.000 Server
- 330.000 Mitarbeiter
- 450.000 verwaltete Endpunkte

Korrelation von Daten über eine Vielzahl von Plattformen hinweg

Die TippingPoint IPS Plattform wird an HPE Standorten weltweit bereitgestellt und lokal verwaltet. Dabei dient das CDC als primärer Nutzer der Ereignisse zur Angriffsvorbeugung. TippingPoint IPS bietet In-Line-Schutz in Echtzeit sowie proaktive Netzwerksicherheit für HPE Netzwerkverkehr und Rechenzentren.

ArcSight Lösungen sorgen für die zentrale Korrelation von Protokollen aus TippingPoint und anderen Quellen, damit das CDC Bedrohungen proaktiv erkennen kann. Alle TippingPoint Plattformen basieren auf dem HPE TippingPoint Threat Digital Vaccine (ThreatDV) Abonnementservice, der wöchentlich ein Malware-Filterpaket bereitstellt, das Unternehmen vor den neuesten Bedrohungen schützen, Malware-Aktivitäten verhindern und hemmen, vertrauliche Daten schützen und die Netzwerkleistung optimieren soll.

Marcel Hoffmann, Senior Manager des HPE Cyber Defense Center, erläutert: „TippingPoint erkennt und blockiert bei HPE aktiv über fünf Millionen Angriffe pro Tag. Unser CDC betreibt die drittgrößte TippingPoint IPS Installation weltweit. Wird eine schwerwiegende Bedrohung erkannt, wird sie aus dem Netzwerkverkehr entfernt und aktiv blockiert."

Trotz der Größe der TippingPoint Bereitstellung erhält das CDC relativ wenige TippingPoint Warnungen.

„Wir erhalten zahlreiche Warnmeldungen von Firewalls, bei vielen handelt es sich jedoch um unbedeutende Störungen", erklärt Hoffmann. „TippingPoint IPS bietet einen kleinen, zuverlässigen Feed umsetzbarer Warnhinweise, denen aktiv nachgegangen wird."

HPE ArcSight Enterprise Security Manager (ESM), HPE ArcSight Logger und HPE TippingPoint IPS Plattformen bilden zusammen ein leistungsstarkes, umfassendes System zur Abwehr von Cyber-Angriffen. Jedes Element spielt bei der Gewährleistung der Sicherheit wertvoller Informationsressourcen von HPE eine wichtige Rolle, dazu gehören Unternehmensanwendungen, Kunden-informationssysteme, geistiges Eigentum und alle kritischen Informationsressourcen, die im Unternehmensnetzwerk von HPE zur Verfügung stehen.

TippingPoint IPS überwacht und erkennt Aktivitäten im Netzwerk, blockiert bösartige Aktivitäten auf der Anwendungsebene und leitet Ereignisdaten an ArcSight ESM weiter. ArcSight Logger kategorisiert und speichert die Ereignisinformationen von TippingPoint und anderen Quellen.

Mit ArcSight können Protokolle zahlreicher Plattformen von einer zentralen Konsole aus überwacht und erweiterte Korrelationen der Ereignisse aus mehreren Quellen durchgeführt werden. Abgesehen von der Übernahme von Protokolldaten von TippingPoint IPS Plattformen nimmt ArcSight zudem Protokolle von Firewalls, Microsoft® Windows® Server Active Directory, HPE-UX, VMware, Microsoft.net und VPNs, Netzwerkgeräten und -Switches, Webproxys, Open-Source-Lösungen und Datenbanken auf. „Wir sind in der Lage, mit den sofort einsatzbereiten Konnektoren von ArcSight Protokolle aus den meisten Quellen zu erfassen. Mit dem HPE FlexConnector Framework wird dann eine Sammlungslogik erstellt und die Protokolle werden für andere Nutzer in einen Kontext gesetzt", erläutert Jorge Alzati, Senior Manager von ArcSight Engineering & Production Management.

„Das CDC hat bereits in weniger als einem Jahr Tausende von potenziellen Angriffen erkannt und verhindert. Unser Programm für Cyber-Sicherheit stellt genaue Sicherheitsdaten zur Verfügung, mit denen das Management faktenbasierte Entscheidungen treffen kann. Gleichzeitig haben wir so die Möglichkeit, auch in Zukunft eine vorausschauende Sicherheitsstrategie zu implementieren."

– Marcel Hoffmann, Senior Manager, Cyber Defense Center, Hewlett Packard Enterprise

ArcSight ESM filtert und korreliert die von TippingPoint IPS und anderen Quellen gesammelten Daten und gibt Analysten somit zuverlässige, hochwertige Informationen an die Hand, um effiziente Sicherheitsanalysen durchführen zu können. Bei der Implementierung von HPE Sicherheitsprodukten wurde die Bereitstellungsmethode für HPE Software Professional Services angewendet. Dazu gehören hohe Verfügbarkeit, Disaster-Recovery, Fehlertoleranz und Lastausgleichseigenschaften.

Erkennen und Umlenken von Angriffen

Ein Unternehmen der Größe von HPE erhält pro Sekunde Hunderte von Sondierungsversuchen auf Schwachstellen und Exploit-Versuche. Die HPE ArcSight Lösung verarbeitet durchschnittlich eine Milliarde Ereignisse täglich und verringert somit den Ereignisfluss auf ein Volumen, das von einer Handvoll von Analysten bewältigt werden kann, die während einer Schicht im CDC arbeiten.

Diese Analysten verfeinern die Warnmeldungen auf 15 bis 20 Vorfälle, für die Folge- und Korrekturmaßnahmen ergriffen werden. Die manuelle Durchführung dieser Tätigkeiten würde normalerweise über 30.000 Analysten erfordern. Ohne ArcSight könnte diese Analyse nicht durchgeführt werden. Diese Ereignisse würden folglich nicht untersucht werden, wodurch aktive Angriffe nicht entdeckt würden.

Die ArcSight Lösung erkennt Aktivitätsmuster, setzt sie in Beziehung und erzeugt anhand von Anwendungsfallregeln Warnungen. HPE verwaltet eine riesige Menge an vertraulichen Daten, die geschützt werden müssen, u. a. Daten von Systemen, Mitarbeitern und Kunden.

ArcSight ESM stellt dem CDC eine zentrale Stelle zur Durchführung der gesamten Sicherheitsüberwachung bereit. Das CDC erkennt mithilfe von ArcSight Bedrohungen in Echtzeit, um diese schnell abwehren zu können. Zudem werden mit ArcSight große Mengen an Sicherheitsdaten gesammelt und korreliert, wodurch die Analysten im CDC echte Bedrohungen noch wirksamer lokalisieren und verhindern können.

„Die ArcSight Lösung erstellt eine zentrale Übersicht über die Bedrohungslage und trägt zur Maximierung unserer Sicherheitsressourcen bei", so Hoffmann. „Unsere Analysten können sich somit ganz auf gefilterte Sicherheitsereignisse konzentrieren, die auf tatsächliche Bedrohungen hinweisen, und müssen nicht mehr Unmengen von Rohdaten aus separaten Überwachungssystemen durchforsten."

Die Datenanalyse von ArcSight unterstützt eine schnellere und effizientere Angriffsvermeidung und liefert betroffenen Nutzern konsequente Strategien, die für eine schnelle und effiziente Behebung entscheidend sind. Bei der Erkennung eines Angriffs unterstützt ArcSight die CDC-Analysten bei der Dokumentierung der Fakten und der Lieferung des entsprechenden Nachweises, um Anlagenbesitzer wirksam einbeziehen zu können und sie von einer Lösung zu überzeugen.

Datenfeeds werden zentral über Geschäftseinheiten und Regionen hinweg korreliert und liefern dem CDC somit einen einzigartigen Einblick in Cyber-Bedrohungen.

„Große Unternehmen müssen in der Lage sein, Angriffsdaten über mehrere Ebenen hinweg schnell zu korrelieren, um potenzielle Bedrohungen, die im gesamten Unternehmen auftreten und von den einzelnen Geschäftseinheiten oder Regionen möglicherweise nicht erkannt werden, umgehend identifizieren zu können", erklärt Alzati.

Hoffmann fügt hinzu: „ArcSight verfügt über eine hoch entwickelte Korrelations-Engine und ergänzt die Ereignisdaten, um eine schnellere Kontextanalyse zu ermöglichen. Dadurch können unsere Analysten effizienter und effektiver arbeiten und schneller auf Bedrohungen reagieren.

„ArcSight ermöglicht zudem die Erkennung von Sondierungsaktivitäten, bei denen Angreifer nach Schwachstellen in unseren Systemen suchen. Auf diese Weise können wir potenzielle Angriffe bereits vor ihrem Auftreten unterbinden."

Das CDC greift bei der Entwicklung von Anwendungsfällen kontinuierlich auf seine Erfahrungen zurück, filtert Datenfeeds und optimiert den Warnprozess. „Die proaktive Entwicklung von Anwendungsfällen ist wichtig, um sicherzustellen, dass das CDC-Team angemessene automatisierte Warnmeldungen erhält", so Alzati. „Unsere Mitarbeiter überprüfen Berichte täglich, um sicherzustellen, dass die geeigneten Kontrollen und Instrumente greifen. Wenn jedoch erst einmal die richtigen Anwendungsfälle vorliegen, kann ArcSight als zentrale Konsole dienen, die eine Verbindung zwischen allen Protokollinformationen herstellt und einen Einblick in den Sicherheitsstatus des Unternehmens gibt."

Die Kombination aus ArcSight ESM und TippingPoint IPS Lösungen unterstützt CDC-Analysten bei der Erkennung und Abwehr Tausender potenzieller Angriffe. So konnte das CDC beispielsweise proaktiv Angriffe durch den Exploit Padding Oracle On Downgraded Legacy Encryption (Poodle) abwehren.

„Als wir von der Poodle-Schwachstelle erfuhren, haben wir in ArcSight eine Anwendungsfallregel erstellt, um Versuche zur Ausnutzung der Schwachstelle zu identifizieren. Aufgrund der ArcSight Warnmeldungen, die durch die neue Regel ausgelöst wurden, haben wir rund 250 IP-Adressen auf die schwarze Liste gesetzt und so verhindert, dass potenzielle Angreifer Schwachstellen ausnutzen."

Innerhalb kürzester Zeit nach der Shellshock-Ankündigung im September 2014 wurden CDC-Analysten von TippingPoint durch Warnmeldungen in ArcSight ESM Dashboards darüber informiert, dass Angreifer nach Schwachstellen in HPE Systemen suchen. „ArcSight zeigte in Echtzeit die Quelle und das Ziel dieser Scanversuche an", führt Hoffmann aus. „Wir konnten Shellshock innerhalb kürzester Zeit über Schwachstellen in HPE Systemen informieren und dafür sorgen, dass entsprechende System-Patches vorrangig entwickelt wurden."

Korrelation und Analyse von Big Data

In Zusammenarbeit mit HPE Labors hat das CDC Protokoll-Appliances für Domain Name Server (DNS) implementiert, um Protokolle von allen sechs internen DNS-Clustern erfassen zu können, die dann zwecks Durchführung erweiterter Analyse- und Warnfunktionen zur HPE Vertica Analytics Platform gesendet werden. Die Vertica Analytics Platform verwaltet riesige Mengen an Daten schnell und zuverlässig und versorgt das CDC so mit Business-Intelligence-Informationen in Echtzeit für eine erweiterte Big-Data-Analyse.

Fallstudie
HPE Cyber Defense Center

Branche
Technologie

Übersicht über den Kunden

HPE Sicherheitslösung

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

Dank Vertica kann das CDC Abfragen 50 bis 1.000 Mal schneller durchführen. Zudem wird dazu nur ein Bruchteil der normalerweise benötigten Hardware verwendet. Im Gegensatz zu herkömmlichen relationalen Datenbanken, die für die Verarbeitung von Unternehmensdaten konzipiert wurden, wurde Vertica von Grund auf speziell für komplexe Analyserechenlasten entwickelt und wird somit problemlos mit der Geschwindigkeit und der Menge der Daten fertig, die in einem Security Operation Center (SOC) erfasst werden.

„Da die herkömmliche Technologie den hohen Geschwindigkeits- und Datenzugriffsanforderungen bei der Analyse von Big Data nicht gerecht werden kann, benötigt das CDC eine spezielle Analyseplattform für Big Data", so Lin Li, Cyber Security Enterprise Architect bei HPE. „Im CDC werden beispielsweise Protokolldateien von über 130 internen Webservern analysiert. Mit Vertica lassen sich diese Dateien in Batches stundenweise speichern und einspeisen sowie verarbeiten, damit das CDC-Team die Analyse durchführen kann."

Die korrelierten Protokolle aus ArcSight werden ebenfalls in Vertica eingespeist und ermöglichen dem CDC so die schnelle Durchführung anspruchsvoller Big-Data-Analysen, um Bedrohungen abzuwehren und zukünftige Angriffe zu verhindern. „Vertica ermöglicht dem CDC die Korrelation von über zwei Milliarden Datensätzen täglich, wobei Protokolldateien in einer Vielzahl verschiedener Formate vorliegen können", erklärt Li. „Dank Vertica kann das CDC die Daten normalisieren, bereinigen und in Beziehung zu anderen Referenzdaten setzen. Dadurch erhält das CDC-Team ein Gesamtbild des eingehenden Datenverkehrs in das globale HPE Netzwerk und kann die Unternehmensressourcen wirksam schützen."

Li weiter: „Da Vertica benutzerfreundlich ist und die Daten sehr gut komprimiert, kann das CDC Daten kosteneffizient speichern und historische Analysen vergangener Ereignisse durchführen. Die meisten detaillierten Abfragen in über 100 Milliarden Protokolldatensätzen in Vertica können innerhalb einer Minute durchgeführt werden. In der alten Architektur war dies undenkbar, da ein solcher Durchsatz in einem herkömmlichen DBMS von vergleichbarer Größe schlichtweg nicht möglich ist. Dank dieser Möglichkeiten der historischen Analyse kann das CDC erkennen, ob Benutzer zuvor unbekannter Malware ausgesetzt sind, und proaktiv Sicherheitsverbesserungen durchführen."

Für die Zukunft gerüstet

Das CDC befindet sich in der ersten der drei Phasen der Implementierungsstrategie. Bei der Anfangsphase lag der Schwerpunkt auf der Absicherung der Netzwerkumgebung durch die Nutzung von Bedrohungsinformationen und die Verkleinerung der Angriffsfläche. In der zweiten Phase soll der Schwerpunkt auf der Absicherung der Anwendungen liegen, die dritte Phase konzentriert sich auf die Absicherung des Unternehmens. Der Strategieplan des CDC sieht eine umfassende Bereitstellung im gesamten Unternehmen bis 2017 vor. Und HPE wird weiterhin an der Entwicklung von Best Practices arbeiten, die auch von anderen großen Unternehmen genutzt werden können.

„Fangen Sie klein an und übernehmen Sie sich nicht", rät Hoffmann. „Es ist besser, Unternehmenssicherheit in Phasen bereitzustellen, insbesondere bei sehr großen Unternehmen mit mehreren Unternehmensbereichen. Vor der Bereitstellung müssen Sie Ihre wichtigsten Ressourcen identifizieren, Ihre Mitarbeiter in der Verwendung der Produkte schulen und ausgereifte Behebungsprozesse entwickeln."

Das CDC bereitet sich zudem auf neue Sicherheitsbedrohungen vor, um bereits heute gut für die Herausforderungen von morgen gewappnet zu sein.

Das CDC bemüht sich um kontinuierliche Verbesserung und entwickelt sich immer weiter, um als realistische Testumgebung für HPE Produkte und Services zu fungieren und den Rahmen für den Betrieb eines flexiblen SOC zu schaffen, das auch mit einem relativ kleinen Mitarbeiterstab von nur 22 Sicherheitsfachleuten auskommt.

HPE verfügt über eines der größten Security Operation Center der Welt und zieht aus jeder Sicherheitsherausforderung Erkenntnisse und Erfahrungen, die an HPE Kunden weitergegeben werden.

Weitere Informationen finden Sie unter hpenterprisesecurity.com/

Neuigkeiten abonnieren

★ Dieses Dokument bewerten

Hewlett Packard Enterprise

4AA5-8767DEE, Dezember 2015, Version 1