Gefahren sichtbar machen, IT-Security unter der Lupe mit HPE ArcSight ESM

Hewlett Packard Enterprise

Unternehmen ertrinken in einer Flut von Informationen aus ihrer IT-Landschaft. Versteckt in dieser Datenflut sind Anomalien, Bedrohungen und tatsächlich stattfindende Angriffe gegen die IT-Infrastruktur und sensitive Daten.

Zeitnahe Aufbereitung, Analyse und kontinuierliche Beobachtung von Log-Daten der (IT-) Geräte ist der Schlüssel für die erfolgreiche Abwendung von Schäden und Datenverlust. Findet dies nicht statt, fehlt der fundierte Überblick über die aktuelle (Sicherheits-) Lage innerhalb der Organisation und effiziente Maßnahmen zur Beseitigung von Vorfällen können nicht eingeleitet werden.

Der Datenstrom ist mittlerweile so stark gewachsen, dass es allein durch Menschenhand nicht mehr möglich ist, früh- und rechtzeitig Gefahren zu erkennen. Ohne Automatisierung ist der Zeitraum bis zur Erkennung und Beseitigung eines Vorfalls so groß, dass z. B. sensitive Daten wie F&E-Dokumente, Passwörter oder Kreditkarteninformationen bereits lange das Unternehmen verlassen haben können.

Hier fehlt es an einem Ansatz, der alle Log-Daten zentral automatisiert sammelt und analysiert. An dieser zentralen Stelle werden die Log-Daten dann normalisiert, aggregiert, korreliert, archiviert und visualisiert sowie ggfs. Incident-Response-Aktionen eingeleitet. SIEM-Lösungen (Security Information and Event Management) erfüllen genau diese Aufgabe.

Dazu muss ein SIEM in der Lage sein, die Informationen einer Vielzahl von Log-Datenquellen verschiedenster Hersteller – darunter Betriebssysteme, Anwendungen, Datenbanken und IT-Sicherheitssysteme – zu erfassen und zu verarbeiten. HPE ArcSight ESM bewerkstelligt dies problemlos.

HPE ArcSight ist eine modulare SIEM-Plattform, die alle wesentlichen Komponenten einer ausgereiften Security Information and Event Management Lösung beinhaltet. HPE ArcSight bildet das zentrale System für die Erfassung, Korrelation, Auswertung und Speicherung aller sicherheitsrelevanten Log Events. Der Einhaltung von Policy und Compliance-Anforderungen kommt man so einen deutlichen Schritt näher. Dabei ist es unerheblich, ob zunächst nur Log-Daten zentral erfasst und archiviert werden sollen oder ob zusätzlich eine intelligente Korrelation der Log-Daten im Vordergrund steht.

Funktionsweise

HPE ArcSight ESM schafft Transparenz über das Unternehmensnetzwerk, insbesondere über etwaige Sicherheitsrisiken und Bedrohungen, welche ohne HPE ArcSight ESM nicht erkannt werden würden.

HPE ArcSight SmartConnectors/FlexConnectors sammeln Log-Daten ein (oder bekommen sie gesendet), verarbeiten diese und versenden sie anschließend komprimiert und gesichert (verschlüsselt) in einem einheitlichen Format (CEF, Common Event Format) an den HPE ArcSight ESM Manager.

Bereits auf *HPE ArcSight SmartConnector/FlexConnector*-Ebene werden nicht relevante Log-Daten/Ereignisse herausgefiltert und/oder zusammengefasst; somit ist eine effiziente Nutzung der zur Verfügung stehenden Bandbreite gewährleistet und die Analyse am Manager findet tatsächlich nur über die relevanten Daten statt.

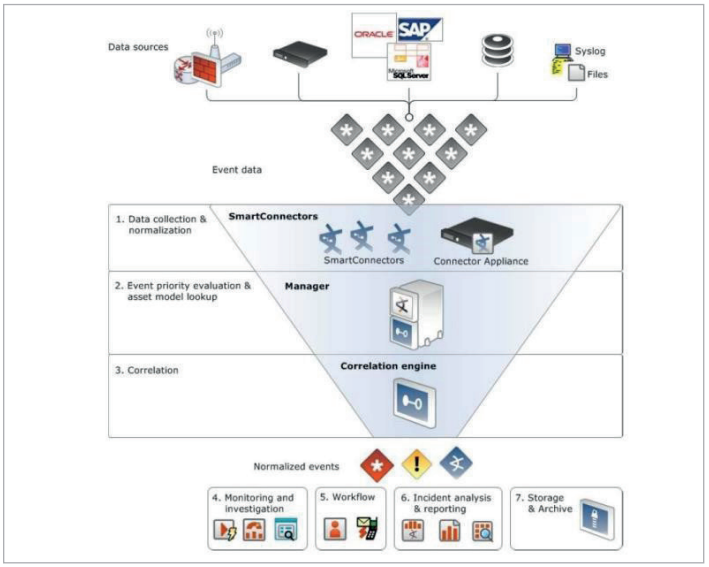

Abbildung 1: Funktionsweise

Die *HPE ArcSight SmartConnectors/FlexConnectors* normalisieren, kategorisieren und fügen den Log-Daten Netzwerkinformationen hinzu.

Treffen die Log-Daten am *HPE ArcSight ESM Manager* ein, werden sie auf Basis der enthaltenen Informationen priorisiert und durch weitere Informationen (wie z. B. Asset Informationen) angereichert.

Diese sogenannten „Basisevents" werden sicher (d.h. unveränderbar) in der Datenbank des HPE ArcSight Managers abgespeichert.

Eintreffende Log-Daten werden gegen hinterlegte Regeln geprüft. Falls bestimmte Kriterien erfüllt sind (Anomalie erkannt, Compliance Verstöße, etc.) generiert HPE ArcSight ESM, bzw. die CORRE Engine einen Alarm, und es werden die zuständigen Stellen/Mitarbeiter informiert.

Die Kategorisierung der Log-Daten durch die *HPE ArcSight Connectoren/FlexConnectoren* ermöglicht es, herstellerunabhängige Regeln zu definieren und eine herstellerübergreifende Korrelation von Log-Daten zu erlangen.

Regeln werden über einen Editor in der HPE ArcSight Java Console erstellt und können verschiedenste Ressourcen verwenden (z. B. Listen, Variablen, Filter oder auch Skripte). Neben den eigenen Regeln bietet HPE ArcSight ESM eine Vielzahl an bereits vorinstallierten Inhalten (Regeln, Listen, Berichte etc.), die direkt genutzt werden können.

Über die von Regeln erzeugten Alarme lassen sich verschiedene Aktionen ausführen: vom einfachen Benachrichtigen per E-Mail bis hin zu der Ausführung von Skripten oder auch dem automatischen Einleiten von Maßnahmen, wie z. B. dem Blockieren von Ports. Das integrierte Case Management-System kann in den eventuell existierenden Workflow für die Bearbeitung von Vorfällen integriert werden oder den Startpunkt darstellen, um einen solchen zu planen.

HPE ArcSight ESM bietet unter anderem eine mächtige Echtzeit-Korrelations-Engine (CORRE- Engine, Correlation Optimized Retention and Retrieval Engine) und eine herstellerunabhängige Korrelation (Cross-Device Correlation). Out-of-the-Box HPE ArcSight SmartConnectors erlauben das Einsammeln von mehr als 350 verschiedenen Typen von Logs von tausenden von Geräten.

Das Log-Format wird in ein einheitliches Format (Common Event Format, CEF) via HPE ArcSight SmartConnectors umgewandelt. Für z. B. Custom-Applikationen oder Log-Quellen, die (noch) nicht out-of-the-box unterstützt werden, steht SDK (Software Development Kit) zur Entwicklung von eigenen HPE ArcSight FlexConnectoren zu Verfügung.

Die Log-Daten werden dank Dashboards übersichtlich und verständlich visualisiert. Für die Verwaltung verschiedener Komponenten steht ein zentralisiertes Management über ArcMC zur Verfügung. Zusätzlich bietet HPE ArcSight ESM Case Management und die variable Speicherung der Log-Daten, basierend auf Compliance-Anforderungen (SOX, PCI DSS, HIPPA, FISMA, u.a.) an. Außerdem wird die Skalierbarkeit, Hochverfügbarkeit und Mandantenfähigkeit gewährleistet.

Sind Langzeitdatenspeicherung und forensische Analysen ein Hauptkriterium, bietet sich die Anbindung einer dedizierten Logmanagement-Lösung wie HPE ArcSight Logger an. Hier können die Daten über lange Zeiträume vorgehalten und durchsucht werden.

Log-Daten werden in diesem Fall am Besten im Parallelbetrieb zu HPE ArcSight ESM und HPE ArcSight Logger gesendet. Zusätzlich können die Ergebnisse der Korrelation von Log-Daten (Alarme) von HPE ArcSight ESM an HPE ArcSight Logger weitergeleitet werden.

Architekturmodell

HPE ArcSight ESM ist sehr flexibel implementierbar und skaliert sowohl horizontal (Hinzufügen von HPE ArcSight ESM Managern, Hinzufügen von HPE ArcSight SmartConnectoren oder auch mehrere HPE ArcSight Logger) als auch vertikal (Verbesserung der zugrunde liegenden Hardware).

HPE ArcSight ESM Manager:

Die Kernkomponente ist ein JAVA-basierter Server. Hier laufen alle Log-Daten, die zuvor von den HPE ArcSight SmartConnectors/FlexConnectors verarbeitet (normalisiert, gefiltert und aggregiert) werden zusammen und werden mit Hilfe der CORRE-Engine analyisiert und korreliert. Der Manager ist die zentrale Reporting- und Analyse-Plattform. Die HPE ArcSight Console und das HPE ArcSight Command Center dienen als Interfaces.

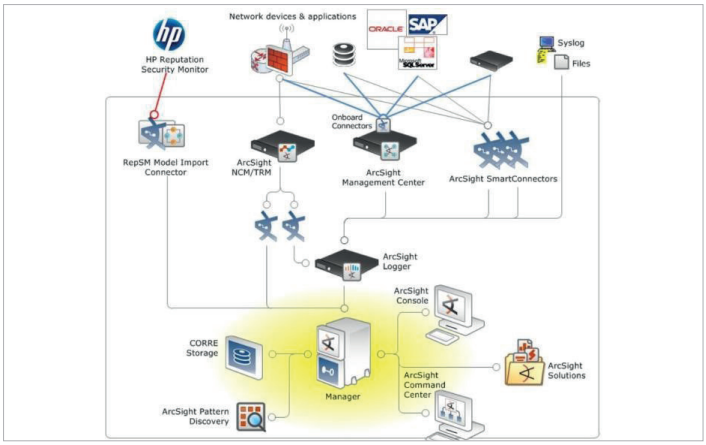

Abbildung 2: Architekturmodell

HPE ArcSight ESM Interfaces:

HPE ArcSight Java Console – Die Konsole ist ein Fat Client und wird von Analysten und Entwicklern (Regel- & Reporterstellung, etc.) als primärer Einstiegspunkt genutzt. Über die Konsole werden die Log-Daten im Detail analysiert (Active Channels) und Inhalte erstellt sowie exportiert und importiert. Ebenso ist es möglich, im begrenzten Umfang die Konfiguration von Komponenten (z. B. HPE ArcSight SmartConnectors) vorzunehmen.

HPE ArcSight Web – Web-basierter Zugang/Interface zum Manager. Über HPE ArcSight Web kann ebenfalls, wie bei der Java Konsole nach Events gesucht und diese analysiert werden. Reports und Dashboards können betrachtet und/oder ausgeführt werden. Es ist jedoch nicht möglich, Inhalte (Regeln o.ä.) zu erstellen.

HPE ArcSight Command Center – Das HPE ArcSight Command Center übernimmt die Funktionalität (administrativ) der Java-Konsole und von HPE ArcSight Web. Ein neues Feature des HPE ArcSight Command Centers ist die Volltextsuche ähnlich zu HPE ArcSight Logger.

HPE ArcSight SmartConnectors:

HPE ArcSight SmartConnectors sind die Interfaces zu den Log-Quellen. Sie können entweder Log-Daten empfangen oder sie aktiv einsammeln. Das Java-basierte Connector Framework unterstützt 32- und 64-Bit und verschiedene Plattformen (OS). Funktionen und Features der *HPE ArcSight Smart-Connectoren* beinhalten:

- Normalisierung
- Kategorisierung
- Forward look up von Customer- und Zoneninformationen
- Filterung von Events
- Aggregation von Events
- Komprimierung der Daten
- Kontrolle der Bandbreitennutzung
- Anonymisierung/Pseudonymisierung von Daten
- Auflösen von DNS-Informationen
- Mapping von zusätzlichen Informationen (über Map files)

HPE ArcSight ESM Ressources:

HPE ArcSight ESM Ressourcen werden in der Datenbank des Managers abgelegt und zentral über die Interfaces (HPE ArcSight Java Console / HPE ArcSight Web) verwaltet und geteilt.

Als „Resource" wird jeglicher Inhalt, der über die Konsole erstellbar, ist bezeichnet (Listen, Assets, Regeln etc). Ressourcen können paketiert (ArcSight Resource Bundles) und zwischen verschiedenen HPE ArcSight ESM-Instanzen geteilt werden (Import/Export).

Um maximale Ausfallsicherheit zu gewährleisten (aufgrund von z. B. internen Richtlinien und/oder Compliance), bietet HPE eine HA (High Availability)-Lösung an, d. h. ein gespiegelter Betrieb des HPE ArcSight Managers.

Leistungen

iT-CUBE SYSTEMS steht Ihnen rund um das Thema SIEM / HPE ArcSight ESM zur Verfügung. Wir unterstützen Sie bei der Konzeption und Planung und führen einen PoC (Proof of Concept) durch. Darüber hinaus implementieren wir HPE ArcSight ESM in Ihre bestehende Infrastruktur und integrieren Ihr SAP® ins SIEM. Mit unserer Hilfe werden stets neue Security Use Cases entwickelt und in Ihr System umgesetzt. Ist Ihnen der Betrieb eines SIEM zu aufwendig, bieten wir diese Leistung auch als Managed Security Service an. Dank zertifizierter Workshops und offiziellen HPE ArcSight Trainings schulen wir Ihre Mitarbeiter weiter, um immer den aktuellsten Wissensstand zu gewährleisten.

Durch Threat Modelling sind wir in der Lage, Angriffsvektoren (Attack Trees, O-WASP) und Risiken zu erkennen und zu bewerten. Auf dieser Basis erarbeiten und implementieren wir Abwehrmaßnahmen (Use Cases). Um einen Überblick über Ihre Daten zu bekommen, analysieren die Experten der iT-CUBE Ihre Log-Daten und bereiten diese visuell in Dashboards und Reports auf.

Durch unsere langjährige Erfahrung im SIEM-Umfeld und dem Umgang mit einer Vielzahl anderer Security-Produkte (wie Palo Alto Networks Firewalls, FireEye, HPE Fortify) ist iT-CUBE SYSTEMS in der Lage, diese Produkte in kürzester Zeit an Ihr SIEM anzubinden und einen Mehrwert in Ihr Monitoring zu bringen.

iT-CUBE SYSTEMS bringt die Kenntnisse mit, um Use Cases verlässlich umzusetzen. Damit später automatisch auf Ereignisse reagiert werden kann (Automated Reponse), müssen Sie sich sicher sein, dass tatsächlich ein realer „Incident" vorliegt und kein „false positive". Durch unsere Implementierungserfahrung mit über 60 realisierten SIEM-Integrationen wissen wir, welche Use Cases realisierbar und verlässlich sind und welche nicht.

agileSI™ applied ERP security

iT-CUBE SYSTEMS hilft Ihnen dabei, Ihre Applikationen und Server an ein SIEM-System wie HPE ArcSight ESM anzubinden und Anomalien frühzeitig zu erkennen. Durch agileSI™ erhalten Sie eine 360° Rundumsicht im SIEM-System durch die Integration relevanter SAP® Security Logs. Dadurch wird das Security Monitoring auf das nächste Level gehoben, da nun die Vorgänge außerhalb der Applikationswelt mit den Vorgängen innerhalb dieser korreliert werden können.

Nutzen

HPE ArcSight skaliert für Unternehmen jeder Größe (flexibles Deployment), angefangen bei kleineren Unternehmensumgebungen mit breitem Spektrum an Quellgeräten und -anwendungen bis hin zu großen Enterprise-Lösungen mit anspruchsvollen Anforderungen und bietet umfangreiche Möglichkeiten der Log-Sammlung: rohe sowie optimierte Log-Daten können out-of-the-box von über 350 unterschiedlichen Arten von Logquellen abgeholt werden.

Ein weiterer Nutzen ist die fortschrittliche Korrelation. Der Kontext zwischen Benutzern, Geräten, Anwendungen und Netzwerken wird hergestellt, um gezielte Angriffe auf kritische Assets zu erkennen.

HPE ArcSight deckt Compliance-Anforderungen perfekt ab. Vorgefertigte Reporting-Packages für PCI, IT Governance, SOX, HIPAA, FISMA, NERC und viele andere Kontrollrahmen sind vorhanden und ermöglichen ein einfaches Audit-Reporting.

Darüber hinaus wertet die Lösung reputationsbasiert Eventinformationen von Firewalls, DNS, Proxy, etc. aus. Diese Daten können durch Reputation Security Monitor (RepSM) gegen Malware Domain Lists abgeglichen werden. Diese Listen werden von den HPE DVLabs gepflegt und sind stets aktuell.

Mit Hilfe von Threat Detector können komplexe Angriffsmuster innerhalb der Event-Daten erkannt und darauf reagiert werden.

Dank UBA (User Behavior Analytics) ist eine Regel- und verhaltensbasierte Analyse und Alarmierung von Nutzeraktivitäten garantiert.

HPE ArcSight ESM ermöglicht einen unternehmensweiten Echtzeit-Überblick über die IT-Landschaft und bietet eine herstellerübergreifende Korrelation und Report-Erstellung. Die Lösung existiert als Software Lösung für größere Installationen und Enterprise Umgebungen oder als Appliance (HPE ArcSight Express) für mittelgroße/kleine Installationen und Unternehmen.

Durch das Zusammenspiel mit anderen Security Produkten kann die Funktionalität von HPE ArcSight ESM erweitert werden und komplexere Szenarien sind denkbar. HPE ArcSight ESM wird zu dem zentralen Kommandoposten Ihrer IT-Security:

- Durch die Integration eines NAC (Network Access Control) können Befehle von HPE ArcSight ESM direkt an die Netzwerkgeräte gesendet werden z. B. schnellere und automatische Reaktion (Automated Response) auf zeit- und sicherheitskritische Vorfälle.
- Ein an ArcSight angeschlossenes DLP (Data Leak Prevention)-System wie Digital Guardian erkennt das Kopieren von Daten auf externe Speichermedien. Durch Korrelation mit anderen Daten in HPE ArcSight ESM wird nun z. B. erkannt, dass der Mitarbeiter, welcher die Daten kopiert, gekündigt hat und es kann zeitnah reagiert werden.
- Vulnerability Scanner (McAfee NSP) zeigen nicht gepatchte Computer im Netzwerk auf. Diese Information kann in HPE ArcSight ESM weiter verwendet werden und bei der Korrelation und insbesondere bei der Kritikalität von Ereignissen berücksichtigt werden.

Referenzen / Projekte

Evaluierung und Machbarkeitsuntersuchung der Einführung einer weltweiten SIEM- und Logmanagement-Lösung

Kunde: Multinationales Unternehmen aus der Antriebs- und Fahrwerktechnik

Tätigkeiten:

- Evaluierung von HPE ArcSight ESM und HPE ArcSight Logger als SIEM und Logmanagement-Lösung zur Integration von Use Case-relevanten Devices an mehr als 100 weltweit verteilten Standorten

Erstellung eines SIEM Konzepts

Kunde/Branche: Informationstechnologie, Deutschland

Tätigkeiten:

- Mehrtägiger SIEM Workshop zur Evaluierung der Kundenanforderungen

  Themen: SIEM vs. Logmanagement, SIEM Implementation Best Practice, SIEM/SOC Processes, SIEM Requirements, SIEM Architecture, SIEM Products, SIEM Use Cases (Conceptual/Technical), SIEM Reports & KPIs, SIEM "Make or Buy", Technical Specifications, Cost Estimation, Rollout Planning
- Erstellung eines SIEM Konzepts

Aufbau eines SOC sowie einer zentralen SIEM und weltweit verteilten Logmanagement-Infrastruktur basierend auf HPE ArcSight ESM und HPE ArcSight Logger.

Kunde: Multinationaler Konzern aus der Arzneimittel und Kunststoff Industrie, Deutschland

Tätigkeiten:

- Unterstützung beim Aufbau eines Security Operation Centers (SOC)
- Implementierung eines zentralen SIEM-Systems (HPE ArcSight ESM (500 GB/Day))
- Implementierung einer weltweit verteilten Logmanagement-Infrastruktur – 9x HPE ArcSight Logger-Instanzen
- Implementierung einer weltweit verteilten HPE ArcSight SmartConnector/FlexConnector-Infrastruktur inkl. zentraler Management-Einheit
- Konfiguration & Adaption der SIEM und Logmanagement-Lösung
- Log-Integration: Security & Network Devices, Operating Systems, Web Applications, Custom Applications, Databases
- Umsetzung diverser Security Use Cases inkl. HPE ArcSight Identity View mit über 100.000 Actors
- HPE ArcSight Workshops/Hands-On
- Projektmanagement

Monitoring von Zugriffen auf klassifizierte Daten unter Verwendung des SAP®-Application Security Monitoring-Produktes agileSI™.

Kunde: Konzern aus der Rüstungsindustrie, Deutschland/Frankreich

- Planung und Implementierung von HPE ArcSight Express
- Planung und Integration des Logging von OS und DB in HPE ArcSight Express für Cross Device Korrelation mit SAP®-Logging
- Planung und Integration des agileSI™ (SAP®) Logging in HPE ArcSight Express
- Entwickeln von benutzerdefinierten Anwendungsfällen für das Monitoring von Zugriffen auf klassifizierte Daten unter Verwendung des agileSI™-Loggings
- Anbindung der entwickelten Korrelation an das zentrale Security Operations Center
- Schulung von Mitarbeitern
- Projektmanagement

Zertifizierungen

- iT-CUBE SYSTEMS ist zertifizierter HPE Gold-Partner für ArcSight-Integration und Training
- Wir sind Board Member im HPE ArcSight Technical Advisory Board und dem HPE ESP EMEA Partner Advisory Board sowie Gründungsmitglied der SIEM Alliance.
- Ausbildung von offiziellen HPE ArcSight Trainern
- Akkreditierte HPE ArcSight Trainer
- HPE Accredited Technical Professional (ATP)
- HPE Accredited Solutions Expert (ASE)
- HPE ArcSight ESM Security Analyst (AESA)
- HPE ArcSight ESM Integrator/Administrator CORRE (AEIA)

Hewlett Packard Enterprise

Gold Partner

iT-CUBE SYSTEMS AG

Paul-Gerhardt-Allee 24
81245 München, Germany

T: +49 89 2000 148 00
F: +49 89 2000 148 29

info@it-cube.de
www.it-cube.de