splunk> turn data into doing™

CASE STUDY

Intel erhöht Sicherheitsniveau mit innovativer Data Intelligence

Zentrale Herausforderungen

Intel musste auf ein datenzentriertes Geschäftsmodell wechseln, das den Wert der Daten erhöht und gleichzeitig die Anfälligkeit verringert.

Wichtige Ergebnisse

Auf der Grundlage von Splunk® und Apache Kafka liefert die Cyber Intelligence Platform (CIP) einen vollständigen Einblick in die InfoSec-Organisation von Intel, was das Information Security Management drastisch verändert hat.

Branche: Technologie

Lösungen: Security, IT Operations

Datengestützte Ergebnisse

- Beschleunigt die Datenanalyse und erkennt ausgeklügelte Bedrohungen in Minuten oder Stunden statt in Tagen oder Wochen
- Bietet einen kollaborativen, einheitlichen Ansatz zur Verwaltung der Cybersicherheit
- Bietet Stream Processing- und Machine Learning-Tools, die in weiteren Bereichen, wie Security Operations und System Health, zusätzlichen Mehrwert bringen

Der Beitrag, den Intel mit seiner Technologie für unsere Gesellschaft leistet, ist nicht zu unterschätzen.

Die technische Expertise des Unternehmens bildet die Grundlage für Milliarden von Geräten und die Infrastruktur der intelligenten, vernetzten Welt und trägt zu deren Sicherheit und Verzahnung bei. Im Lauf der Zeit hat sich Intel von einem PC-zentrierten Unternehmen zu einem datenorientierten Unternehmen gewandelt. Sie entwickeln neue Produkte, erschließen neue Märkte und gewinnen auf innovative Weise neue Kunden.

„Daten sind alles, Daten sind Trumpf. Sie bilden die Grundlage unseres Unternehmens, die Grundlage für alles“, sagt Brent Conran, Chief Information Security Officer bei Intel. „Sie transformieren traditionelle Branchen und solche, die in der Cloud zu Hause sind. Die Fähigkeit, Erkenntnisse aus Daten zu gewinnen, unterscheidet erfolgreiche Unternehmen von Unternehmen, die den Anschluss verlieren.“

Aufgrund dieser stärkeren Ausrichtung auf Daten musste Intels Abteilung für Informationssicherheit (InfoSec) eine umfassende „Defense-in-Depth“-Strategie entwickeln und verfolgen. Das Team automatisierte Präventions- und Erkennungstools auf vielen Ebenen, darunter die Perimeter-, Netzwerk,- Endpunkt-, Anwendungs- und Datenebene, und konnte damit 99 % der Bedrohungen für Intels Umgebung in den Griff bekommen.

Die Jagd nach dem einen Prozent

Komplexe Bedrohungen werden immer zahlreicher und ausgefeilter. Und das Unternehmen mühte sich ab, mit einer veralteten SIEM-Lösung (Security Information and Event Management), die den aktuellen Anforderungen einfach nicht mehr gewachsen war. Nur eine Handvoll Experten kannte sich mit der bestehenden SIEM-Lösung aus, die nicht mehr auf die stetig steigende Anzahl neuer Datentypen skalierbar war.

Intel InfoSec (Intels Abteilung für Informationssicherheit) brauchte eine Strategie zur Erkennung von hochkomplexen Bedrohungen für die Umgebung des Unternehmens – intern die Jagd nach dem einen Prozent genannt. Diese Strategie war ausschlaggebend für die Entwicklung von Intels Cyber Intelligence-Plattform (CIP), die auf Spitzentechnologien wie Splunk und Apache Kafka aufbaut. Mit Hochleistungsservern, die auf Intel® Xeon® Platinum Prozessoren, Intel 3D NAND Solid State Drives (SSDs) und Intel® Optane™ SSDs basieren, erfasst die neue CIP-Plattform ein Datenvolumen von mehr als 12 Terabyte pro Tag und speichert 15 Petabyte. Die Daten fließen aus Hunderten Quellen in einen Kafka Message Bus und dann in die Splunk-Plattform, auf der Benutzer mehr als 1,3 Millionen Suchvorgänge pro Woche ausführen.

Mit Splunks Data-to-Everything Plattform und Hunderten von Drittanbieter-Tools verfügt Intel InfoSec nun über umfassende Transparenz und eine gemeinsame Arbeitsoberfläche. So konnte die Effektivität in der gesamten InfoSec-Organisation gesteigert werden. Das Team ist nun in der Lage, Bedrohungen innerhalb von Stunden bzw. Minuten anstelle von Wochen bzw. Stunden zu erkennen und abzuwehren

> Daten sind alles, Daten sind Trumpf. ... Sie transformieren traditionelle Branchen und solche, die in der Cloud zu Hause sind. Die Fähigkeit, Erkenntnisse aus Daten zu gewinnen, unterscheidet erfolgreiche Unternehmen von Unternehmen, die den Anschluss verlieren."
>
> **Brent Conran,** Chief Information Security Officer

Skalieren der Cyber Intelligence-Plattform von Intel

Die Ergebnisse der CIP führten zu weiteren Datenquellen, neuen Use Cases und vielen weiteren Datenmodellen. Schon bald wurde die Nutzung der CIP auf Bereiche wie Schwachstellenmanagement, Compliance und Enforcement sowie Risikomanagement ausgeweitet, was zusätzliche Anforderungen an die Infrastruktur stellte und noch schnellere Rechen- und Speichervorgänge erforderte. Um die Performance der Plattform zu maximieren, mussten Intels Sicherheitsarchitekten und Ingenieure sich noch eingehender mit der Splunk-Plattform und den Intel-Technologien auseinandersetzen.

> Wir erkennen das Potenzial, und weil wir das Potenzial erkennen, investieren wir Zeit, Energie und Ressourcen. Denn wir möchten unbedingt, dass es ein Erfolg wird, da wir überzeugt sind, dass es uns dabei helfen wird, unsere Mission zu erfüllen."
>
> **Brent Conran,** Chief Information Security Officer

Splunk und Intel arbeiteten als Team zusammen, um eine gemeinsame Referenzkonfiguration zu entwickeln und so die Erweiterung der CIP in Sachen Rechenleistung, Arbeitsspeicher und Speicherkapazität mit den neuesten Produkten und Technologien von Intel zu unterstützen. Splunk und Intel lassen nun IT-Kollegen an ihrem Erfolg teilhaben und helfen anderen, ihre Splunk- und Apache Kafka-Implementierungen zu skalieren, um Rohdaten effektiver in aussagekräftige Informationen zu Betrieb, Business und Sicherheit zu verwandeln.

Nachhaltige Wertschöpfung

Das InfoSec-Team von Intel ist dabei, die Nutzung von Splunk und Kafka auszuweiten. Die Analysten und Datenwissenschaftler befassen sich mit dem Transformieren, Anreichern, Verknüpfen, Filtern und Bearbeiten von Daten im Datenstrom. Darüber hinaus fügt das Team weitere Machine Learning-Tools für unterschiedlichste Anwendungsfälle hinzu – von Incident Response, Betriebs- und Systemintegrität bis hin zur Workflow-Orchestrierung und Warnmeldungen. In Zusammenarbeit mit Splunk setzt Intel nachhaltige Wertschöpfungspotenziale frei.

„Intel Information Security ist viel agiler als früher", so Conran. „Wir haben einen brandneuen Splunk-Data Lake integriert und unsere Tools modernisiert. Mit den Daten am richtigen Ort und durch die Schulung unserer Mitarbeiter konnten wir Kräfte bündeln und einen Multiplikatoreffekt erzielen. Jetzt verwenden wir Machine Learning, um die Tiefe und Geschwindigkeit unserer Cyber-Intelligence signifikant zu steigern.

20-14330-TransformingIntel_sSecurityPostureWithInnovationsinDataIntel-A4-104-CS_DE