ASICS automatisiert Management und Behebung von Incidents mit Echtzeit-Log-Analysen

Kurzfassung

ASICS ist ein multinationales Unternehmen aus Japan, das aus der Fusion von Onitsuka, GTO und Jelenk hervorgegangen ist. Asics wartet mit einer vollständigen Palette von Sportartikeln und -ausrüstung auf und schafft mit intelligenter Sporttechnologie hochwertige Lifestyle-Produkte. Um Cyberbedrohungen zu bekämpfen und Incidents ohne Zeitverlust zu lösen, benötigte ASICS eine zentrale Plattform zur Verwaltung, Korrelation und Analyse von Logs aus mehreren Systemen. Seit der Einführung von Splunk® Enterprise verzeichnet das Unternehmen deutliche Verbesserungen, wie etwa:

- Echtzeitsichtbarkeit von Incidents und Bedrohungen durch automatisierte Log-Analysen
- Verbesserung im Bereich Social Accountability durch mehr Sicherheit und Transparenz
- Mehr Effizienz und Produktivität aufgrund von optimierten Geschäftsabläufen

Warum Splunk?

ASICS hat im Laufe der Jahre proaktive Schritte zum Schutz des Unternehmens eingeleitet. Unter anderem wurden ein Information Security Committee und ein Information Security Office eingerichtet, ein Computer Security Incident Response Team (CSIRT) zusammengestellt und ein Security Operations Center (SOC) installiert. Doch auch mit diesen Ressourcen war das Unternehmen noch nicht in der Lage, Logs aus internen, über verschiedene Standorte verteilten Systemen wie Firewalls, Proxy-Servern und Systemen zur Endpunkterkennung und -behandlung zentral zu verwalten und zu analysieren und gleichzeitig die Nachweisführung im Rahmen der Social Accountability sicherzustellen. All diese Aufgaben waren mit vielen manuellen Prozessen verbunden und entsprechend zeitintensiv.

Ein weiteres wichtiges Anliegen war es, Endpunktbedrohungen in Gestalt von E-Mail-Betrug, Cyberangriffen oder anderen Problemen und Attacken durch ein Rund-um-die-Uhr-Monitoring treffsicher zu erkennen und frühzeitig darauf zu reagieren. Zur Krisenprävention benötigte ASICS darüber hinaus einen zuverlässigen Mechanismus zum Extrahieren anormaler Muster und Identifizieren verdächtiger Geräte durch Korrelation und historische Analysen von Log-Daten. Splunk Enterprise erfüllt all diese Anforderungen und konnte bei ASICS außerdem mit seiner Flexibilität und der nahtlosen Integration in eine kleine kommerzielle SOC-Umgebung sowie mit geringem Investitionsaufwand und schneller Inbetriebnahme punkten.

Branche

- Fertigung

Splunk-Anwendungsfälle

- Log-Management
- Cyber Security und Betrugsbekämpfung

Herausforderungen

- Keine frühzeitige Reaktion auf Incidents und Bedrohungen
- Keine zentralisierten Log-Management- und -Analyseprozesse
- Unwirtschaftliche Prozesse bei Incident Response und Incident Resolution aufgrund von hohem manuellem Aufwand
- Herausforderungen im Bereich Social Accountability aufgrund möglicher Datenschutzverletzungen und Sicherheitsrisiken

Auswirkungen für das Unternehmen

- Mehr Sicherheit durch Echtzeit-Sichtbarkeit von Incidents und Bedrohungen
- Optimierte Prozesseffizienz dank automatisiertem, zentralisiertem Log-Management mit minimalen manuellen Eingriffen
- Verbesserung im Bereich Social Accountability mit sicheren und transparenten Abläufen
- Nachhaltiges geschäftliches Wachstum mit dem Potenzial, mit Splunk noch einen Schritt weiterzugehen

Datenquellen

- Firewalls der nächsten Generation
- Cloud-Proxys
- Proxy-Server
- Endpunkterkennungs und -Response-Systeme
- Event-Logs von Cloud-Servern

Splunk-Produkte

- Splunk Enterprise

Automatisierung der Log-Analyse mit Echtzeittransparenz und operativen Erkenntnissen

Die Splunk-Software wird in einer Virtual Private Cloud innerhalb des Rechenzentrums von ASICS ausgeführt, konsolidiert Log-Daten aus allen Systemen und analysiert sie auf einer zentralen Plattform. Die Folge: wertvolle Erkenntnisse und Echtzeittransparenz aller Abläufe. Auf der Grundlage von Korrelationssuchen werden Risikobewertungen erstellt und Anomalien und Bedrohungen in Echtzeit erkannt. Die SOC-Mitarbeiter können nun jederzeit und überall über eine intuitive Web-Konsole auf den Analysestatus zugreifen und bei Notfällen Warnmeldungen auf ihren Smartphones empfangen. Außerdem kann das CSIRT von ASICS die Aktivitäten nach einem Incident problemlos verfolgen.

Da alle diese Prozesse automatisiert sind, ist ASICS in der Lage, sein Rechenzentrum rund um die Uhr mit minimalen manuellen Eingriffen zu überwachen. Durch die Automatisierung des Log-Managements sparen das Unternehmen und deren Mitarbeiter wertvolle Zeit ein, sodass die Fachkräfte sich auf wirklich wichtige Tätigkeiten konzentrieren können.

Social Accountability durch frühzeitige Verfolgung von Incidents und verbesserte Cyber Security

Als börsennotiertes Unternehmen ist ASICS verpflichtet, seinen Stakeholdern ein klares Bild des Unternehmens zu vermitteln. Beispielsweise ist Rechenschaft darüber abzulegen, wie Daten erfasst und die einzelnen Prozesse wie Schuhkonstruktion und Fertigung ausgeführt wurden. Mit Splunk Enterprise kann ASICS potenzielle Beeinträchtigungen rasch verfolgen, Problemen vorgreifen und die Sicherheit erhöhen. Darüber hinaus hat das Unternehmen die Möglichkeit, über eine benutzerfreundliche Oberfläche operative Erkenntnisse aus Logs zu gewinnen, Events zu identifizieren und umgehend Berichte für Top-Management und Stakeholder zu erstellen. Die Fortschritte im Bereich Social Accountability ermöglichen es ASICS seinen Ruf bei internen und externen Stakeholdern zu verbessern, seine Attraktivität für Fachkräfte zu steigern und seine Mitarbeiter zu motivieren.

„Als Allround-Analysetool unterstützt Splunk Enterprise effizient unsere Geschäftsabläufe und bietet uns große Vorteile. Wir glauben, dass Splunk eine Art „Energizer“ für die Sportbranche sein könnte.“

— Shigekazu Tanimoto, Global Security Lead, ASICS Corporation

Mehr Effizienz und Produktivität aufgrund von optimierten Geschäftsabläufen

Mit Splunk Enterprise als Dreh- und Angelpunkt der Sicherheitsinfrastruktur profitiert ASICS von einem korrelierten Netzwerk von Daten und nie dagewesenen Prozessoptimierungen. Die Lösung ist vollständig kompatibel mit bestehenden Anwendungen, lässt sich problemlos in alle Bereiche des Unternehmensumfelds integrieren und ermöglicht eine reibungslose Zusammenarbeit zwischen unterschiedlichen Abteilungen. Die Folge sind Steigerungen von Prozesseffizienz und Produktivität.

Inzwischen prüft ASICS auch die Umsetzung kreativerer Konzepte mit Splunk Enterprise, zum Beispiel die gezielte Bekämpfung von Insider-Bedrohungen und Datenschutzverletzungen zum Schutz verschiedener Unternehmens-Assets sowie der Privatsphäre der Mitarbeiter. Zu diesem Zweck evaluiert das Unternehmen gerade Splunk User Behavior Analytics für einen möglichen zukünftigen Einsatz. Geplant ist darüber hinaus die Ausweitung der Splunk-Lösung auf einen größeren geographischen Raum durch die Implementierung einer regionalen SIEM (Security Information and Event Management)-Strategie für andere Länder.

Außerdem ist ASICS bestrebt, die Vorzüge des Big Data-Analysemoduls der Splunk-Software für eine größere Bandbreite von Geschäftsanwendungen zu nutzen. Eines der Produkte ist beispielsweise ein Baseball mit eingebauten Sensoren zur Messung von Wurfdaten. Die über die Sensoren erfassten Daten könnten Sportlern wertvolle Erkenntnisse liefern und so dabei helfen, neue Rekorde aufzustellen. Bei ASICS ist man überzeugt davon, dass mit Splunk Enterprise das Beste noch bevorsteht und eine nachhaltige Zukunft zum Greifen nah ist.

20-13538-Splunk-SEC-ASICS-A4-101-CS