splunk>

CASE STUDY

OhioHealth beschleunigt Incident-Untersuchungen mit Datenanalysen in Echtzeit

OhioHealth

Kurzfassung

OhioHealth wurde 1891 gegründet und ist eine gemeinnützige Gesundheitsorganisation mit 28.000 Mitarbeitern, Ärzten und Freiwilligen sowie einem Netzwerk aus 11 Krankenhäusern, mehr als 50 ambulanten Einrichtungen, Hospizen, Einrichtungen zur häuslichen Pflege, medizinischen Geräten und weiteren Services aus dem Gesundheitswesen in einem 40 Landkreise umfassenden Gebiet. OhioHealth nutzt eine vernetzte Umgebung, um nahtlosen und sicheren Zugang zu Patientendaten, Telemedizin und anderen Gesundheitsdiensten zu ermöglichen. Seit der Einführung von Splunk Enterprise verzeichnet das Unternehmen deutliche Verbesserungen, wie etwa:

- Schnellere Incident-Untersuchungen
- Einsparungen von ca. 5.000 USD pro Phishing-Sitzung
- Vermeidung von jährlichen Kosten in Höhe bis zu 30.000 US-Dollar für die Wartung von Active Directory-Audit-Software

Warum Splunk?

Das Gesundheitsnetzwerk verfügt über zahlreiche Soft- und Hardware-Tools zum Schutz seiner IT-Umgebung, darunter Firewalls, DLP-Software (Data Loss Prevention), Vulnerability Scanner, Active Directory-Domänencontroller, Viren- und Malwareschutz sowie eine SIEM-Lösung (Security Information and Event Management). Zwar sind diese Tools jedes für sich wirksam, es gibt aber wenig Integration zwischen ihnen, was die Ad-hoc-Analyse zu einer Herausforderung macht und wenig Möglichkeiten bietet, aus verschiedenen Quellen stammende Sicherheitsdaten zu aggregieren und zu korrelieren OhioHealth suchte eine Lösung, die über Datensilos hinweg eingesetzt werden konnte, um Sicherheits-Tools zu konsolidieren, ein branchenweit führendes Sicherheitsprogramm aufzubauen und eine einfache Methode zur Bekanntmachung potenzieller Risiken für das Unternehmen zu bekommen.

Das Security Operations-Team von OhioHealth setzte Splunk Enterprise ein und installierte Splunk Forwarder auf allen Firewalls, Domänencontrollern, Switches und anderen Geräten. Splunk-Forwarder bieten eine zuverlässige und sichere Erfassung und Übermittlung von Daten an die Splunk-Plattform zur Indizierung, Speicherung und Analyse. Sobald die Einspeisung von Protokollen und anderen Daten in Splunk Enterprise begann, nutzte das Team die Lösung, um den Schutz seiner Infrastruktur zu verbessern und die Einhaltung gesetzlicher Vorschriften gemäß HIPAA usw. sicherzustellen. Mithilfe der Splunk-Software wurden Incident-Untersuchungen beschleunigt, die Event-Korrelation verbessert und automatisierte Echtzeit-Datenanalysen bereitgestellt.

Branche

- Gesundheitswesen

Splunk Use Cases

- IT Operations
- Sicherheit

Herausforderungen

- Geringe Integration zwischen den aktuellen Sicherheitstools
- Schwierige Ad-hoc-Analyse
- Fehlende Fähigkeit zum Sammeln und Korrelieren unterschiedlicher Sicherheitsdaten
- Wunsch nach dem Aufbau eines branchenführenden Sicherheitsprogramms

Auswirkungen für das Unternehmen

- Möglichkeit zu plattformübergreifender Sicherheitskorrelation und -analyse
- Schnellere Untersuchung von Incidents
- Automatisierte Metriken und Datenanalyse in Echtzeit
- Einsparungen von ca. 5.000 USD pro Phishing-Sitzung
- Vermeidung von bis zu 30.000 USD an Kosten pro Jahr für die Wartung von Active Directory-Überwachungssoftware
- Erwartete Einsparungen durch Wegfall von Lizenzgebühren für die bisherige SIEM-Lösung

Datenquellen

- Firewall- und Domänencontroller-Logs
- Switches, Router und andere Netzwerkgeräte
- Antivirensysteme für Endpunkte
- Vulnerability Scanner
- Apache Webserver-Zugriffs-Logs
- Logs der Datenverlust-Verhinderung

Splunk-Produkte

- Splunk Enterprise
- Splunk Enterprise Security

Sensibilisierung für Phishing und Risikominimierung

OhioHealth hat Services evaluiert, um Überprüfungen auf Phishing in seinem Gesundheitsnetzwerk durchzuführen. Das Sicherheitsteam zog die Beauftragung eines Dienstleisters in Erwägung, der 5.000 USD pro Phishing-Testsitzung gekostet hätte. Stattdessen wurde ein interner Phishing-Webserver an Splunk Enterprise angebunden und ein einfaches Skript erstellt, das Phishing-E-Mails an 700 zufällig ausgewählte Empfänger im gesamten OhioHealth-Netzwerk sendete. Nach monatelangen Tests führte das Team eine Live-Demo für das obere Management durch, bei der die Ergebnisse über Splunk-Dashboards in Echtzeit angezeigt wurden. Es ließ sich genau ablesen, wer auf die E-Mail geklickt hatte – und wären die Phishing-E-Mails echt gewesen, hätte dies zu einer möglichen Infektion oder gestohlenen Anmeldeinformationen geführt.

„Die Splunk-Live-Demo hat das Bewusstsein unserer Führungskräfte für die Bedeutung von Risikoanalyse und -minimierung geschärft“, sagt der Manager für Infrastrukturtechnologien bei OhioHealth. „Splunk hat uns nicht nur geholfen, unser eigenes Phishing-Testsystem zu entwickeln, sondern wir sparen auch das Geld, das wir für einen externen Dienstleister eingeplant hatten“.

Große Einsparungen bei Active Directory-Audits

Bei der Implementierung eines neuen biometrischen Zugangssystems für OhioHealth-Mediziner und andere Kliniker wurden versehentlich kritische Benutzerblöcke aus dem Active Directory gelöscht. Während das Implementierungsteam die Benutzer schließlich wiederherstellen konnte, blieb die Ursache der Löschungen unbekannt. „Wir haben uns für eine führende Sicherheits- und Compliance-Lösung entschieden, aber wir haben erkannt, dass sie nicht genau das ist, was wir brauchen, und sie hätte uns etwa 30.000 USD pro Jahr gekostet“, sagt der Manager. „Wir brauchten eine Möglichkeit, unsere Active Directory-Dienste zu überprüfen und festzustellen, was wann passiert ist. Dann fanden wir heraus, dass wir das System mit Splunk Enterprise praktisch kostenlos erstellen können.“

„Unser SIEM war immer nur einfach ein SIEM, während Splunk eine Datenanalyse-Plattform mit SIEM-Funktionalität ist. Besonders, wenn man sich durch Logs wühlen oder Berichte über die Internetnutzung durchsehen muss, dann geht dies mit Splunk Enterprise viel schneller. Wir können praktisch jede Frage stellen und sie – mit den richtigen Daten – mithilfe der Splunk-Software beantworten. Wenn es um die Erkennung von Anomalien geht, erreichen wir mit Splunk Enterprise Security genau das.“

Manager Infrastructure Technologies
OhioHealth

Durch den Einsatz von Splunk-Forwardern auf jedem Domänencontroller, die Informationen von diesen Geräten sammeln und sie sicher und zuverlässig zur Analyse an die zentrale Splunk-Instanz senden, konnte das Security Operations-Team den gesamten Active Directory Forest in Echtzeit überwachen, einschließlich aller Änderungen an Verzeichnissen und Benutzerkonten. Als das gleiche Zugriffsproblem erneut auftrat, konnte das Team dank Splunk die Ursache des Problems innerhalb weniger Minuten finden.

Tieferer Einblick in den Netzwerkbetrieb

Das Netzwerk-Team von OhioHealth übermittelt Logdaten von allen Routern und Switches zur Indizierung an Splunk Enterprise. Umgehend wurde das Team mit tieferen Einblicken in den Netzwerkbetrieb belohnt. Alle unentdeckten Betriebsdetails – wie z.B. deaktivierte Lüfter – sind nun leicht zu erkennen und zu korrigieren. Das Netzwerk-Team plant nun, die Splunk-Lösung als Teil ihres NOC (Network Operations Center) der nächsten Generation einzusetzen. OhioHealth plant darüber hinaus auch, seine SIEM-Lösung durch Splunk Enterprise Security zu ersetzen, welches standardmäßig Incident-Überprüfung und -Klassifizierung, Berichte und Sicherheitsmetriken, risikobasierte Analysen, ein Threat Intelligence Framework, einen einheitlichen Sucheditor, statistische Analysen und flexible Dashboards bietet.