splunk> turn data into doing™

CASE STUDY

Dänemarks größtes Versorgungs- und Telekommunikationsunternehmen spart dank beschleunigter Incident Response 35 Stunden pro Woche

Zentrale Herausforderungen

Nach dem Aufbau eigener Log-Analyse- und Incident-Response-Funktionen sah sich das Norlys-Team zahlreichen Herausforderungen gegenüber, darunter mühsame Routineaufgaben, zu viele Tools, langsame Web-Oberflächen und schwerfällige Prozesse.

Wichtige Ergebnisse

Mit der Splunk-Plattform ist es Norlys gelungen, Bedrohungsinformationen zu integrieren, Routineaufgaben zu automatisieren und Untersuchungen zu zentralisieren. Dadurch verkürzte das Unternehmen seine Reaktionszeiten und steigerte die Produktivität seiner Mitarbeiter.

NORLYS

Branche: Energie- und Versorgungsunternehmen

Lösungen: Security

Für Grundversorger hat Sicherheit oberste Priorität.

Norlys ist Dänemarks größtes Energie-, Versorgungs- und Telekommunikationsunternehmen und bedient 1,5 Millionen Kunden. Den Verantwortlichen ist daher bewusst, dass eine schnelle Reaktion auf Sicherheitswarnungen zwingend erforderlich ist. Als die Sicherheitsabteilung geschaffen wurde, hatte das Unternehmen jedoch keinerlei Incident-Response- oder Sicherheitsfunktionen. Das Norlys-Team musste daher praktisch bei Null anfangen und eigene Log-Analyse- und Incident-Response-Kapazitäten entwickeln.

Dieser unternehmenseigene Ansatz brachte allerdings Herausforderungen mit sich, darunter aufwändige manuelle Workflows, umständliche Routineaufgaben, zu viele Tools, fehlender Kontext, langsame Web-Oberflächen und wartungsintensive Prozesse. Um diese Probleme zu lösen, entschied sich Norlys für Splunk – mit Splunk Enterprise Security (ES) als SIEM-Tool und Splunk SOAR als Plattform für SOAR-Aufgaben (Security Orchestration, Automation and Response).

Angreifer entdecken

Norlys verfügt heute über aussagekräftige Informationen, um Bedrohungen zu bekämpfen, und setzt Splunk ES für verschiedenste Zwecke ein – von der Bedrohungserkennung über die Erfassung von Feeds bis hin zu Dashboards für Untersuchungen und Korrelationssuchen. „Bei verdächtigen Aktivitäten an einem Endpunkt schauen wir uns das entsprechende Dashboard in ES an und sehen sämtliche Bewegungen“, erklärt Tibor Földesi, Security Automation Analyst bei Norlys. „Ich gebe einfach den Hostnamen eines Rechners ein und sehe alle Antwort-Logs des Endpunkts. Mit ES können Sie alles sehen, was in Ihrer Umgebung vor sich geht, um die bösen Jungs zu finden.“

Um maximalen Nutzen aus ihrer Investition zu ziehen, lässt sich Norlys vom Splunk Professional Services Team beraten. „Wenn wir glauben, etwas nicht bestmöglich lösen zu können, wenden wir uns an das Team von Splunk Professional Services. Professional Services sind wirklich ein entscheidender Erfolgsfaktor“, so Földesi. „Durch das Professional Services Team haben wir erfahren, dass wir sofortigen Nutzen aus ES und Splunk SOAR ziehen können, indem wir Tickets in anderen Systemen automatisieren. Ich möchte nicht jeden Tag Tickets öffnen, und jetzt muss ich das auch nicht mehr.“

Datengestützte Ergebnisse

35 Std.
werden pro Woche eingespart

30 Sek.
Prozessdauer, anstatt zuvor 30 Minuten

98 %
weniger Zeitaufwand für das Öffnen von Tickets

35 Stunden Ersparnis pro Woche

Dank der Automatisierungs- und Orchestrierungsfunktionen von Splunk SOAR kann Norlys Sicherheitsprobleme heute schneller lösen.

Földesi erstellte mit Splunk SOAR zunächst ein eigenes Playbook für die Reaktion auf eine Antivirus-Warnmeldung. Wenn eine Warnmeldung eingeht, löst das Splunk SOAR-Playbook automatisch ein EDR-Tool (Endpoint Detection and Response) aus, das den Endpunkt auf verdächtige Aktivitäten analysiert. Die unter Quarantäne gestellte Datei wird dann abgerufen und zur Detonation und Analyse an eine Malware-Sandbox gesendet, anschließend wird ein Bericht für den Sicherheitsanalysten erstellt – alles automatisch. Vor der Erstellung dieses Playbooks musste das Norlys-Team solche Security-Warnungen mehrmals täglich mit großem Aufwand manuell bearbeiten.

„Es handelt sich um ein sehr umfassendes Playbook", erklärt Földesi. „Die Untersuchung ist zu 100 Prozent automatisiert, es ist keinerlei menschliches Eingreifen erforderlich. Vorher habe ich diese Aufgabe manuell erledigt, aber mit Splunk SOAR muss ich erst am Ende der Analyse aktiv werden und dann nur noch eine informierte Entscheidung über die erforderlichen Maßnahmen treffen."

Das Security-Team von Norlys arbeitet nach dem Motto: Wenn Aufgaben lästig sind, automatisiere sie. Folgerichtig nutzt das Team inzwischen täglich 20 verschiedene Playbooks, um Zeit und Geld zu sparen. „Splunk SOAR spart uns 35 Stunden pro Woche – etwa fünf Stunden pro Tag. Wir können uns jetzt endlich auf die wichtigen Aufgaben konzentrieren", sagt Földesi.

> Die Automatisierung verändert die Art und Weise, wie Teams üblicherweise ein SIEM nutzen. Wir verlassen uns stark auf Splunk SOAR und Enterprise Security. Sie ergänzen sich auf sehr gute Weise und ermöglichen es uns, die Security-Fähigkeiten für das gesamte Unternehmen zu verbessern."
>
> **Tibor Földesi,** Security Automation Analyst, Norlys

> „Früher haben wir 10 Minuten gebraucht, um ein Ticket zu erstellen, heute geht es im Nu. Und bei einigen Tickets wird automatisch eine Anreicherung gestartet, die nur 30 Sekunden dauert. Manuell haben wir früher 30 Minuten dafür gebraucht."
>
> **Tibor Földesi,** Security Automation Analyst, Norlys

Gute Workflows, hohe Sicherheit

Durch die Einbindung von Splunk in alltägliche Workflows können die Sicherheitsanalysten von Norlys ihr Unternehmen nun besser schützen. „Die Automatisierung verändert die Art und Weise, wie Teams üblicherweise ein SIEM nutzen", erläutert Földesi. „Wir verlassen uns stark auf Splunk SOAR und Enterprise Security. Sie ergänzen sich auf sehr gute Weise und ermöglichen es uns, die Security-Fähigkeiten für das gesamte Unternehmen zu verbessern."

Laden Sie Splunk kostenlos herunter oder probieren Sie die kostenlose Cloud-Testversion aus. Egal, ob Sie mit großen oder kleinen Teams, in der Cloud oder lokal arbeiten – Splunk hat das passende Bereitstellungsmodell für Sie.

splunk>

Mehr erfahren: www.splunk.com/asksales

www.splunk.com

21-15232-Splunk-Norlys-A4-CS-103