Bewertung und Zitate des Auftraggebers:

„Die Zusammenarbeit war sehr partnerschaftlich und äußerst professionell.“

„Die Experten sind wahnsinnig gut ausgebildet und entsprechen sowohl fachlich als auch menschlich hohen Ansprüchen.“

„Nicht nur die Qualität überzeugt, sondern auch der Einsatz der Experten, der weit über das normale Maß hinausgeht.“

„Wir freuen uns auf die weitere Zusammenarbeit mit euch.“

canacoon Case Study

Internationaler SIEM Roll-out

Der Kunde in Stichpunkten

- internationaler, US-stämmiger Konzern, der bereits 1833 gegründet wurde und sowohl organisch als auch durch sehr viele Zukäufe rasant gewachsen ist
- diverse Töchter verschiedener Branchen mit unterschiedlichen Geschäftsmodellen
  - Pharmahandel
  - Apotheken (Onlinehändler und Filialen)
- 208 Milliarden US Dollar Umsatz weltweit (unkonsolidiert ca. 320 Mrd.)
- in Europa:
  - 17.1 Mrd. € mit apothekenspezifischen Lösungen
  - 3.9 Mrd. € mit Patienten- und Kundenlösungen

Das Unternehmen unterliegt einer Vielzahl von Compliance- und Datenschutzvorgaben, unter anderem PCI-DSS, HIPAA, SOC und SOX, sowie besonderen Vorgaben im Europäischen Datenschutz. Zudem gibt es weitere Vorgaben in einzelnen Ländern aufgrund der dortigen Handhabung von Patientendaten, sprich „besonderer Personenbezogener Daten“ nach DSGVO Artikel 4.

Die Aufgabenstellung

Die Aufgabenstellung war zunächst, 2.000 Systeme und rund 100 Datenbank- und Applikationslayer von 37 dedizierten Applikationen der dreizehn europäischen Tochterunternehmen, in einen zentralen SIEM Betrieb zu überführen. Ziel war die Implementierung eines SIEM Loggings, dass als Grundlage eines Security Operation Centers alle zu Grunde liegenden Compliance-Anforderungen zu erfüllen hatte. Herausfordernd waren die unterschiedlichen, heterogenen IT Umgebungen in verschiedenen Reifegraden, die zudem bei 3 Zentralen und 6 länderspezifischen Hostern betrieben wurden. Hinzu kamen diverse SaaS und PaaS Provider, die überwiegend von den landesspezifischen Geschäftseinheiten gesteuert wurden und zunächst keine direkten Zugriffe zuließen. Zu den Herausforderungen zählte zudem das im Projektzeitraum noch rechtlich unklare Umfeld von GDPR (DSGVO), und dabei besonders landesspezifische Sonderregelungen wie beispielsweise in Dänemark.

Die Definition von Lösungsmöglichkeiten für das Logging von Systemen, Datenbanken, Applikationen, besonderen Sicherheits-komponenten wie z. B. Firewalls, von Routern, Switches und vielem mehr gehörte ebenso zur Aufgabenstellung der Integration des Loggings durch die canacoon Berater wie auch die Gewährleistung der sicheren Transporte der Daten. Besonders herausfordernd waren die speziell für den Kunden entwickelten Applikationen. Für diese war ein Logging und eine Dateninterpretation auf SIEM-Seite gemäß der Kundenvorgaben abzustimmen, zu entwickeln, zu testen und in Betrieb zu nehmen.

Die Lösung

Die canacoon wurde mit der Projektleitung und technischen Unterstützung beauftragt. Nachdem canacoon die Business Units für ihr geplantes Vorgehen gewinnen konnte, wurden alle verbliebene Projektteile - unter Verwendung eines aus verschiedenen, agilen Vorgehensweisen (für die Role-outs) und klassischen Projekt-management-Methoden zusammengesetzten Ansatzes - geplant und durchgeführt. canacoon unterstützte auch in rechtlichen Fragestellungen, um die zeitnahen Role-outs sicherstellen zu können. Parallel zu den Klärungen im rechtlichen Bereich wurden in Kooperation mit dem SIEM Anbieter standardisierte Lösungen für Betriebssystem-logging und Datenbanklogging geschaffen. Diese wurden ergänzt um spezielle Lösungen, die die canacoon für Standard Applikationen (z. B. SAP) entwickelte. Da bei dem Kunden eine gewachsene, noch nicht konsolidierte IT Infrastruktur vorlag, musste eine Vielzahl unterschiedlichster Standard-Lösungen definiert, getestet und zum Role-out abgestimmt bzw. geplant werden. Im Vordergrund der Role-outs standen dann die Koordinationen mit den internationalen Providern und internen IT Teams der verschiedenen Geschäftseinheiten des Kunden. Dies inkludierte auch Abstimmungen mit Betriebsräten, indirekt mit Gewerkschaften und vergleichbaren Organisationen sowie Funktionsbereichen der Geschäftseinheiten innerhalb Europas.

Das Projekt wurde innerhalb des Zeitplans und vollständig dokumentiert übergeben. Die Dokumentation umfasste auch Anleitungen für zukünftige Implementierungen. Jedes Logging-Objekt, die Netzwerk- und Sicherheits-komponenten, die Datenbanken, Systeme und Applikationslayer wurden im kundeneigenen Architekturtool auf allen Detailebenen dokumentiert, verknüpft und an den Betrieb sowie das SOC übergeben. Sollte es zu Vorfällen kommen, sind so alle relevanten Daten an einem Ort zu finden. Das ermöglicht dem Kunden eine schnelle Reaktion, um weitere mögliche Folgeschäden zu minimieren bzw. auszuschließen. Der Kunde gewann hierdurch eine bestmögliche Nachvollziehbarkeit und ein messbares und transparentes Projektergebnis.

Mit Abschluss des Projektes erfolgte nahtlos eine Nachfolgebeauftragung zum Anschluss weiterer 3.000 Komponenten, Systeme, Datenbanken und Applikationen (diese nun überwiegend GDPR relevant) an das SIEM. Diese Beauftragung beinhaltete auch eine bereits frühzeitig geplante Weiterentwicklung der international verteilten SIEM Umgebung zur Abbildung zukünftiger Anforderungen des Security Operation Centers.