ConSecur GmbH hat für einen Kunden aus dem Bankwesen 50 IT-Security-Analysten ausgebildet

BEI DIESER KUNDENREFERENZ AUS DEM BANKWESEN ERKENNEN SIE WEDER KUNDENLOGO NOCH KUNDENNAMEN WIR HABEN UNS AUS GRÜNDEN DAFÜR ENTSCHIEDEN, SODASS WIR IHNEN UNSERE LEISTUNGEN BEI DER AUSBILDUNG VON 50 IT-SECURITY-ANALYSTEN VORSTELLEN KÖNNEN.

ConSecur

[security and consulting]

Zum eigenen Cyber Defense Center in 7 Monaten

Ein US-amerikanisches Finanzdienstleistungsunternehmen hat die eigene Cyber-Sicherheit selbst in die Hand genommen. Innerhalb kürzester Zeit hat der Kunde Hochschulabsolventen und IT-Kräfte ohne IT-Security-Bezug rekrutiert, die im Cyber Defense Center mit Sitz in den USA und Irland das interne Netzwerk überwachen sowie Cyber-Bedrohungen identifizieren und ihre Folgen neutralisieren sollen. Die ConSecur GmbH hat alle 50 neuen Team-Mitglieder zu IT-Security-Analysten ausgebildet.

Nach einer fünfmonatigen Trainingsphase hat das neu eingerichtete Cyber Defense Center seinen Betrieb aufgenommen.

Aus Talenten sind innerhalb eines halben Jahres IT-Security-Fachkräfte geworden.

Aus Talenten sind innerhalb eines halben Jahres IT-Security-Fachkräfte geworden.

Fachkräftemangel – welche Optionen gibt es?

Ein Jahr vor dem Go-Live-Termin des eigenen Cyber Defense Centers hat unser Kunde entschieden, die bisher an einen externen Managed Security Service Provider vergebene Dienstleistung der Cyber Defense im eigenen Hause als Kompetenz zu etablieren.

Aufgrund des IT-Fachkräftemangels ist es keine echte Option gewesen, etablierte Fachkräfte anzuwerben. Welche Option bliebe stattdessen? Wäre es möglich, junge Menschen innerhalb weniger Monate zu IT-Security-Spezialisten auszubilden? Könnte es gelingen, im eigenen Haus eine schlagkräftige Allianz aus IT-Abteilung und IT-Security-Analysten zu bilden, die Cyber Defense als eingespieltes Team umsetzt?

Der Kunde spielte diese Alternative gedanklich durch, welche Schritte und Partner dafür nötig wären, ein auf zwei Kontinenten arbeitendes Cyber Defense Center aufzubauen, das alle Anforderungen vollständig erfüllt.

Rekrutierungskampagne zur Gewinnung von Hochschulabsolventen

Das Unternehmen startete eine Rekrutierungskampagne, um Hochschulabsolventen für das neue Cyber Defense Center zu begeistern. Für diesen Ansatz, Cyber Defense mit einem frischen Team aufzubauen, hat der Kunde ein Umfeld geschaffen, das Karriereentwicklungsmöglichkeiten für alle Mitarbeiterinnen und Mitarbeiter anbietet. Im Zuge dessen sind Tools entwickelt und bereitgestellt worden, Berufs- und Privatleben in Einklang zu bringen.

Diese Form der Wertschätzung ist dem Kunden ein hohes Anliegen gewesen, sodass jeder Einzelne sein ganzes Potential im Cyber Defense Center ausschöpfen kann.

„Wir haben diesen Ansatz gewählt, um die zur Verfügung stehende Zeit bestmöglich zur Qualifizierung zu nutzen“

CHRISTOPH KRONABEL

EDR-Infrastruktur für das Cyber Defense Center (24/7)

Die Zielvorgabe für das neue Cyber Defense Center war, jedes Gerät im Unternehmens-Netzwerk sicher zu betreiben sowie Anomalien schnellstmöglich zu erkennen, zu neutralisieren und ihre Folgen zu beseitigen.

Der Kunde registrierte zu diesem Zeitpunkt zweihundert potentielle Sicherheitsvorfälle in 24 Stunden, die von IT-Security-Analysten einzeln untersucht worden sind. Insbesondere außerhalb der Geschäftszeiten und an Feiertagen verzeichnete das Unternehmen eine größere Zahl verdächtiger Ereignisse, sodass das neue Cyber Defense Center in großer Personalstärke 24/7 betrieben werden sollte.

Für die schnelle und gründliche Analyse jedes Ereignisses sollte das hohe Schutzniveau des Unternehmens-Netzwerks von einer EDR-Infrastruktur unterstützt werden: Endpoint Detection and Response (EDR) ermöglicht den direkten Zugriff auf einzelne Clients. Über EDR können IT-Security-Analysten im Falle einer Cyber-Attacke auf jedes Endgerät der 32.000 Mitarbeiter zugreifen, um Angriffsmuster nachvollziehen zu können: Wie hat es Angreifern gelingen können, sich unbefugten Zugang zum Unternehmensnetzwerk zu verschaffen?

IT-Security-Analysten können mit EDR erkennen, ob Aktionen am Endgerät eine Cyber Attacke begünstigt haben und über welche Wege die Angreifer in das Unternehmens-Netzwerk vorgedrungen sind. Dieses Konzept der Cyber Defense schließt auch Endgeräte ein, die aus dem Homeoffice, dem öffentlichen Netz oder mobil auf das Netzwerk zugreifen und dort nicht durch die Unternehmens-IT geschützt sind.

Das Unternehmen startete eine Rekrutierungskampagne, um Hochschulabsolventen für das neue Cyber Defense Center zu begeistern.

Kombination von Bootcamp und Remote-Schulung in der IT-Security-Analysten-Ausbildung

Mit einer Vorlaufzeit von neun Wochen haben IT-Security-Consultants der ConSecur GmbH mit den ausgearbeiteten Trainings der Hochschulabsolventen begonnen. Innerhalb von fünf Monaten sollte die Ausbildung aller neu eingestellten Mitarbeiter abgeschlossen sein, sodass diese im Team die Arbeiten im Cyber Defense Center vom externen Dienstleister übernehmen können.

Die Planung hat vorgesehen, zeitversetzt in zwei Gruppen auszubilden. „Wir haben diesen Ansatz gewählt, um die zur Verfügung stehende Zeit bestmöglich zur Qualifizierung zu nutzen“, sagt Christoph Kronabel, Lead IT-Security-Consultant der ConSecur GmbH. Parallel hat die Rekrutierungskampagne weiterlaufen können, bis die gewünschte Personalstärke für das Cyber Defense Center zu 100 Prozent erreicht worden ist.

In den modulbasierten Trainings hat ConSecur die gemeinsame Präsenzzeit im Bootcamp vor Ort mit Remote-Schulungen kombiniert. Über die reine Vermittlung der fundierten Kompetenz eines IT-Security-Analysten hinaus sollten mit diesem Ansatz das Wir-Gefühl sowie die Teamarbeit innerhalb der Gruppe initiiert und gefördert werden.

Stufenweise zum IT-Security-Analysten

Die Module der viermonatigen Trainings haben jeweils mit einem Test abgeschlossen, der das Erlernte über Aufgabenstellungen abgefragt hat. In Breakout-Sessions nach den Prüfungen sind die Aufgabenstellungen in der Gruppe sowie bei Bedarf in Einzelsitzungen aufgearbeitet worden.

Inhaltlich haben die neuen Mitarbeiter stufenweise ihr Handwerk als IT-Security-Analysten erlernt. Von grundlegenden Inhalten aus, der Basic IT Security, haben sich die künftigen Analysten in die Netzwerk-Analyse eingearbeitet, das Vorgehen im Falle einer Cyber-Attacke simuliert, Kommunikations- und Dokumentationstrainings durchlaufen und die Tools im Cyber Defense Center kennengelernt. Zum Abschluss hatten die Analysten mit einem „Capture-the-Flag“ die Aufgabe, in etwa 20 Leveln den Login einer virtuellen Maschine zu „knacken“.

MODULE DES IT-SECURITY-ANALYSTEN TRAININGS

- Basic IT Security
- Monitoring & Analysis
- Incident Handling
- Tool based Training
- Capture the Flag - Login einer virtuellen Maschine in etwa 20 Leveln „knacken“
- Training on the Job - Begleitung

Fazit

Nach fünf Monaten Training haben die ausgebildeten IT-Security-Analysten als hauseigenes Team den externen Dienstleister abgelöst und die Cyber Defense übernommen.

Das ambitionierte Ziel, ein junges Team ohne Berufserfahrung selbst auszubilden, hat der Kunde durch eine erfolgreiche Rekrutierungskampagne erreicht und mit der Expertise ConSecurs umgesetzt.

Gemeinsam ist es gelungen, innerhalb des engen Zeitfensters eine leistungsfähige neue Fachabteilung aufzubauen, die Zukunft hat.

ConSecur GmbH

Als herstellerunabhängiges Beratungs- und Dienstleistungsunternehmen befasst sich die ConSecur GmbH mit der Planung und Umsetzung von Maßnahmen zur Informationssicherheit. Unsere Leidenschaft ist die Entwicklung, Bewertung und Realisierung von IT-Sicherheitskonzepten für Unternehmen. So beschützen wir die Information, die Sie täglich für Einkauf, Produktion, Dienstleistung, Logistik und Korrespondenz benötigen. ConSecur hat sich darauf spezialisiert Informationssicherheit an die Geschäftsprozesse im organisatorischen und informationstechnischen Umfeld anzubinden. Hierbei setzen wir auf die bestehenden unternehmerischen Prozesse und eingesetzten Technologien unserer Kunden auf. Wir etablieren lösungsorientierte, standardisierte und effiziente Maßnahmen, die unsere Kunden in die Lage versetzen, ihre informationstechnischen Risiken zu beherrschen und bestehenden regulatorischen Vorgaben zu genügen. Ziel unserer Arbeit ist es, nur berechtigten Personen den Zugriff auf Informationen zu gewähren und Informationen vor Übergriffen Unbefugter zu schützen

ConSecur – next level information security

ConSecur
[security and consulting]

ConSecur GmbH
Nödiker Straße 118
49716 Meppen

TEL.: +49 5931 9224-0
info@ConSecur.de
www.ConSecur.de