CS_PORTFOLIO

ConSecur
Cyber Defense Center

ConSecur
[security and consulting]

Der Sicherheitsdienst für Ihre IT

Unsere vernetzte Welt hat in den vergangenen Jahren in einem beeindruckenden Tempo an Mobilität und Flexibilität gewonnen. Wir rufen Informationen dort ab, wo wir uns gerade befinden, und teilen sie mit Kunden, Partnern und Kollegen. Allerdings erfordert diese Freiheit gleichermaßen unsere erhöhte Wachsamkeit. Denn überall dort, wo etwas rausgeht, kann eben auch immer jemand hereinkommen.

Damit genau das nicht passiert, gibt es das Cyber Defense Center der ConSecur GmbH. Hier überwachen unsere Security-Analysten rund um die Uhr die Sicherheit von IT-Infrastrukturen. Sie behalten Ihre Systeme permanent im Auge und analysieren sämtliche sicherheitsrelevanten Vorgänge. Im Zusammenspiel mit der bestehenden Sicherheitsarchitektur bietet das Cyber Defense Center einen Hochleistungsschutz für Ihre IT. Darüber hinaus erkennen unsere Analysten Schwachstellen und identifizieren Sicherheitsvorfälle aller Art.

PERMANENTE SICHERHEIT FÜR IHRE INFORMATIONEN

Damit haben Sie die Gewissheit, dass ausschließlich berechtigte Personen Zugang zu Ihrem Netzwerk und damit auf Informationen, Daten und Dokumente haben. Das gilt sowohl für Angreifer, die von außen auf Ihr Netzwerk zugreifen wollen, als auch für Innentäter aus den eigenen Reihen. Das Cyber Defense Center erkennt diese Angriffe rechtzeitig und leitet gezielte Abwehrmaßnahmen ein. Deshalb ist Ihre IT bei der ConSecur GmbH in den besten Händen.

FRAGEN ZU MANAGED SECURITY SERVICES?

Rob Suurland
PRODUKTMANAGER UND
SENIOR BERATER

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

Berechtigte Zugriffe erlauben – Angriffe abwehren

Die IT steuert und verwaltet den Informationsfluss in Unternehmen. Im Cyber Defense Center spüren wir Anomalien auf, die diesen Informationsfluss stören.

Anomalien bzw. Sicherheitsvorfälle können z. B. Angriffe von Außen sein, fehlerhafte Konfigurationen von einzelnen Systemen, Zero-Day-Exploits, aus dem LAN initiierte, unautorisierte Datenabflüsse, nicht Policy konformes Passwort-Sharing, Konfigurationsmanipulationen an z. B. Datenbanksystemen und vieles mehr. ConSecur fasst dies in UseCases zusammen und dokumentiert in diesen UseCases das dazugehörige Risiko sowie die notwendigen Log- und Informationsquellen. Die Kreativität bei der Entwicklung von UseCases ist nur durch die zur Verfügung stehenden Log- und Informationsquellen begrenzt. Die Identifizierung der Sicherheitsvorfälle geschieht in Echtzeit. So können wir Schaden von Unternehmen abwenden bzw. minimieren.

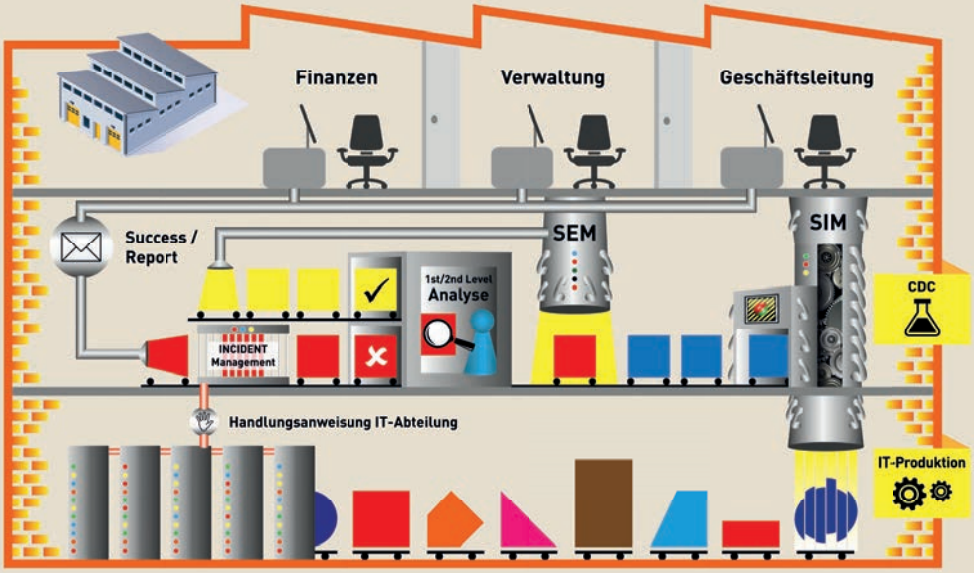
Täglich kommen leicht hunderttausende von Log-Informationen und Events zusammen. Um dieser Datenflut Herr zu werden, nutzen wir in unserem Cyber Defense Center das SIEM-Tool QRadar von IBM. Das SIEM-Tool überprüft nach einem von uns entwickelten Regelwerk, basierend auf den definierten UseCases, ankommende Logs und Events, die aus unterschiedlichen Quellen stammen, in zwei Schritten.
Im ersten Schritt, dem SIM, werden die Log-Daten und Events gesammelt, gespeichert, normalisiert und analysiert. Dieses ist die Voraussetzung für den zweiten Schritt. Im zweiten Schritt, dem SEM, werden diese normalisierten Informationen korreliert und z. T. um weitere Informationen angereichert. Bei der Korrelation der Daten werden dann auf Grund des Regelwerks Sicherheitsvorfälle identifiziert. Diese meldet das SIEM-Tool dann an unseren Analysten.

Unsere Analysten untersuchen dann den Vorfall und erkennen, ob sich hinter der Anomalie ein tatsächlicher Sicherheitsvorfall verbirgt. Liegt ein Sicherheitsvorfall vor, löst der Analyst Alarm aus und übergibt den Fall mit allen relevanten Informationen an das Incident Management, das mit den verantwortlichen Fachabteilungen entsprechende Gegenmaßnahmen einleitet.

Alle Sicherheitsvorfälle dokumentieren wir ausführlich. Die Dokumentation dient zum einen dazu, dieses Wissen bei nachfolgenden Ereignissen als Wissensbasis heranzuziehen. Zum anderen gewinnen wir mit der Dokumentation ein stetiges und aktuelles Bild der Sicherheitslage des Unternehmens.

Features des Cyber Defense Centers

- Maximale Investitionssicherheit
- 24x7-Monitoring
- Log- und Eventanalyse
- Einsatz eines SIEM-Systems
- Permanente Weiterentwicklung



ConSecur

[security and consulting]

ConSecur GmbH
Nödiker Straße 118
49716 Meppen

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