Cyber Defense Services

Cyberangriffe stellen eine der größten Bedrohungen für Unternehmen und Verwaltungseinrichtungen dar. Lag bisher der Fokus auf präventiven Schutzmaßnahmen, liegt dieser heute auf der Detektion und Bewertung von Angriffen. Es existiert mittlerweile quasi ein kontinuierlicher Wettbewerb zwischen Herstellern, die ihre Sicherheitslösungen permanent weiterentwickeln, und Angreifern, die als Antwort darauf neue Angriffsmechanismen konzipieren.

Bereits das Erkennen dieser Angriffe ist für IT-Abteilungen intern kaum noch leistbar. Hinzu kommt, dass es – neben dem Einsatz einer geeigneten Detektionslösung – vor allem wichtig ist, den Kontext eines Angriffs zu verstehen, um angemessen reagieren zu können.

Die Controlware Cyber Defense Services enthalten – abhängig vom individuell gewählten Leistungsumfang – die Erkennung von Cyber-Gefahren, Schwachstellen und Anomalien durch unterschiedliche Risikoerkennungsmodule in Verbindung mit Dienstleistungen zur Analyse, Bewertung und Priorisierung von Security Incidents. Ein besonderer Schwerpunkt liegt unter anderem auf der ständigen Beobachtung der weltweiten aktuellen Bedrohungslage, um Angriffsmuster zu verstehen und die Detektionsmechanismen kontinuierlich darauf anzupassen.

Auf Basis dieser Services lassen sich die folgenden Herausforderungen des IT-Betriebs erfolgreich adressieren:

- Wie schaffe ich Risikotransparenz?
- Wie kann ich moderne, gezielte Angriffs-szenarien erkennen?
- Wie kann ich Korrelation über Ereignisse oder Ereignisketten herstellen?
- Wie erhalte ich anwendbare Anleitungen für die Behandlung von Risiken?
- Wie kann überprüft werden, ob Verbesserungen erfolgreich waren?

Das Controlware Cyber Defense Center (CDC)

Mit seinem ISO 27001 zertifizierten Cyber Defense Center mit Standort in Deutschland, ist Controlware optimal für die Erkennung, Bewertung und Abwehr von Cyber Gefahren in den IT-Umgebungen unserer Kunden aufgestellt.

In Kombination mit unseren Leistungen im Bereich der Systemintegration und Beratung, können Handlungsempfehlungen gemeinsam mit dem Kunden umgesetzt werden.

Die Controlware Cyber Defense Services Module

Vulnerability Management Service (VMS)

Im Rahmen dieses Moduls wird eine Plattform bereitgestellt und betrieben, die der Identifizierung und Inventarisierung von Assets sowie der Erkennung und Nachverfolgung von Schwachstellen innerhalb der IT-Infrastruktur dient. Die Schwachstellen werden priorisiert dargestellt und mit Handlungsempfehlungen versehen.

Advanced Log Analysis (ALA)

Die bei diesem Modul zur Sammlung und Auswertung von Log-Daten bereitgestellte Plattform dient der Erkennung Security-relevanter Ereignisse. Über spezielle, von Controlware entwickelten Use Cases, können Angreifer-Verhalten und eingesetzte Techniken in den unterschiedlichen Phasen eines Angriffs sicher erkannt und in einen Zusammenhang gebracht werden. Gleichzeitig ermöglicht dieses Modul eine Bewertung von Security Incidents im kundenspezifischen Kontext. Dabei verbleiben alle Daten grundsätzlich beim Kunden. Die Verarbeitung erfolgt im Rahmen der EU-Datenschutzbestimmungen.

Advanced Threat Detection (ATD)

Im Rahmen dieses Moduls wird eine Plattform zur Erkennung von Anomalien im Netzwerk-Datenverkehr, im Benutzerverhalten oder in E-Mails bereitgestellt und betrieben. Die Plattform liefert auch Hinweise auf Cyber Security-relevante Vorgänge und Ereignisse.

Analyse – „SOC as a Service“

Auf die Risikoerkennungsmodule aufbauend erfolgt die Security Analyseleistung durch unsere zertifizierten Cyber Security Analysten im Cyber Defense Center. Diese analysieren, bewerten und priorisieren die gefundenen Risiken, um anschließend konkrete Handlungsempfehlungen zu geben und den Kunden bei der Beseitigung der Cyber-Gefahren oder -Risiken zu unterstützen.

Cyber Defense Einstiegsoptionen

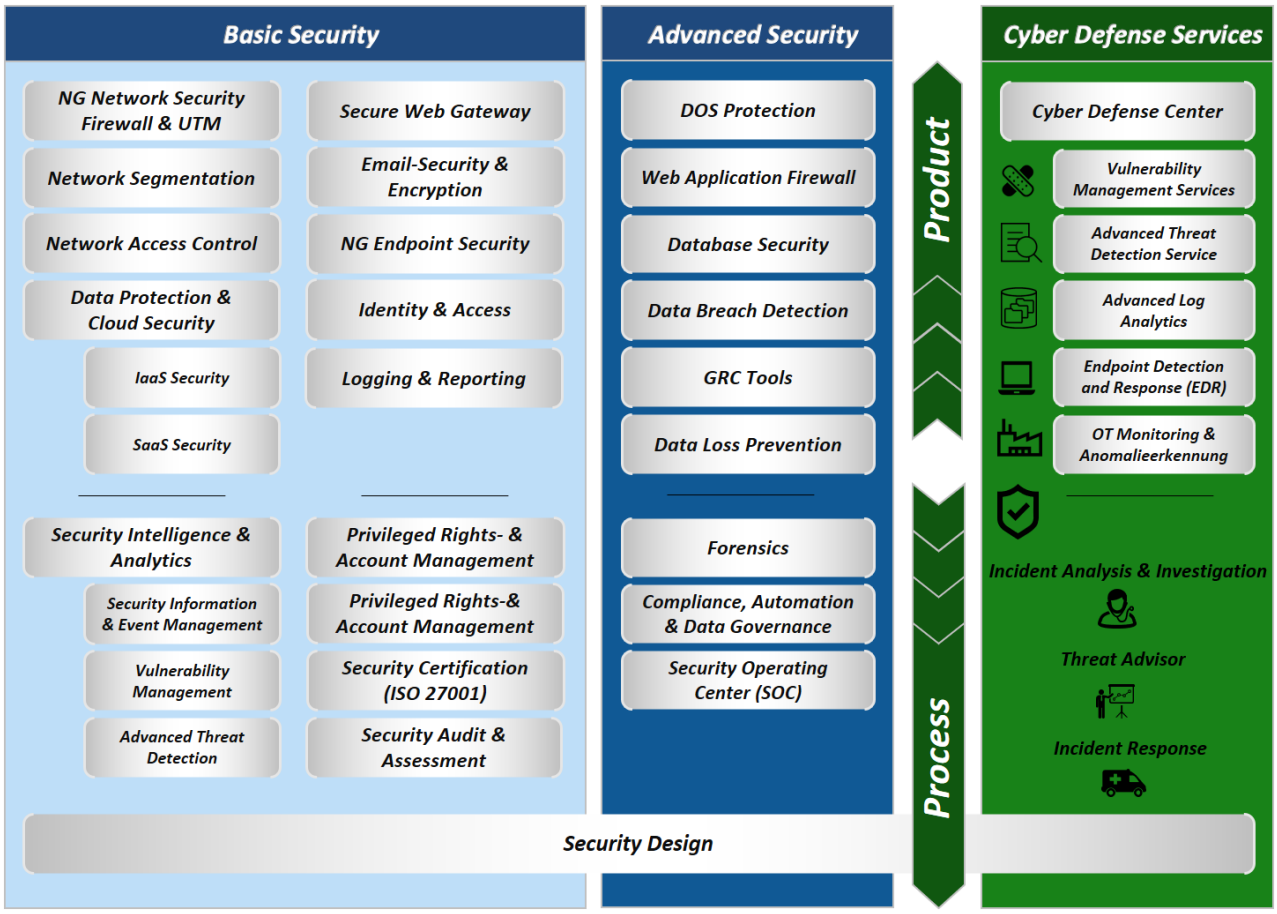
Security Assessment

Zur Ermittlung des tatsächlichen Bedarfs und des optimalen Leistungsumfangs der Cyber Defense Services, empfehlen wir die Durchführung eines gemeinsamen Security Assessments. Dieses ermöglicht kurzfristig und mit geringem Aufwand eine initiale Erfassung des aktuellen Sicherheitsniveaus Ihrer IT-Landschaft und gibt einen Überblick über vorhandene Schwachstellen und Verwundbarkeiten.

Compromise Assessment

Künstliche Intelligenz (KI) und Machine Learning (ML) haben sich im Bereich der IT-Sicherheit als treibende Kräfte etabliert. Durch KI-gestützte „Compromise Assessments“ verhilft Controlware seinen Kunden zu genauen Einsichten in ihre Infrastrukturen und zeigt Bestands-Kompromittierungen auf.

Controlware Cyber Defense Services – Maßgeschneiderte Security für Ihr Unternehmen



Zentrale

Controlware GmbH
Waldstraße 92
63128 Dietzenbach

Tel. +49 6074 858-00
Fax +49 6074 858-108

info@controlware.de
www.controlware.de