DE

Kapsch BusinessCom

Kapsch Cyber Defense Center.

Ein Kapsch-Service, bei dem international zertifizierte und bestens ausgebildete Analysten von Kapsch Cyberkriminellen den Kampf ansagen. Und das bereits bei zahlreichen Kunden sehr erfolgreich.
Als wesentlicher Bestandteil von IT-Prozessen müssen die Detektion von Angriffen und die schnelle Reaktion darauf im Vordergrund stehen. Durch das Kapsch Cyber Defense Center (Kapsch CDC) kann die Prävention zielgerichtet und kontinuierlich verbessert werden.

Das Kapsch Cyber Defense Center ermöglicht eine zielgerichtete Prävention.

Zusätzlich zu den klassischen Security-Lösungen wie z. B. Firewalls, die automatisiert das Netzwerk schützen, bietet Kapsch mit seinem Cyber Defense Center ein Service an, bei dem Analysten eine intensive Überwachung der Sicherheitssysteme zur Erkennung von Vorfällen durchführen. Dies kann auf 4 verschiedene modulare Weisen passieren: Netzwerkanalyse, Endpoint-Analyse, Log-Analyse und Threat Intelligence.

Die Module

Netzwerkanalyse

Bei der Netzwerkanalyse werden Kapsch Server mit eigens entwickelten Applikationen genutzt. Diese zeichnen direkt im Netzwerk des Kunden den kompletten Verkehr auf. Dieser Traffic wird von den Analysten von Kapsch untersucht, um Angriffe und Anomalien festzustellen.

Log Analyse

Bei der Log-Analyse werden Logs von diversen Geräten innerhalb des Netzwerks gesammelt, um einen Gesamtkontext herzustellen und Angriffe und Anomalien genauer identifizieren zu können.

Endpoint-Analyse

Für die Endpoint-Analyse wird ein forensischer Endpoint Client genutzt. Dabei werden alle Events auf Servern und Endgeräten (ausgenommen Mobile Devices Android/iOS) aufgezeichnet. Im Bedarfsfall können die Analysten umgehend darauf zurückgreifen.

Threat Intelligence

Threat Intelligence bietet die Möglichkeit, im Darknet und in geschlossenen Foren nach Informationen zu suchen, die auf einen Angriff auf den Kunden hinweisen können.

Network Security Monitoring

Track network traffic
Automated and manual analysis
Threat detection
Network forensic

Endpoint Detection & Response

Endpoint visiblity
Live remote analyse
Remote data collection
Quarantine endpoints

Log Analysis

Log aggregation and assessment
Statistical analysis
Data correlation

Threat Intelligence

Brand & Credential Monitoring
Trend Analysis and Threat Research
Indicator enrichment

Was sind unsere Unique Selling Points?

- Analysten des Kapsch CDC sind militärisch sicherheitsüberprüft
- Hinter Kapsch CDC steckt ausschließlich österreichische Dienstleistung
- Kapsch CDC nutzt Quellen aus der gesamten Welt, inklusive teurer bezahlpflichtiger Quellen
- Beim Kapsch CDC verlassen die Daten des Kunden sein Netzwerk nicht
- Kapsch CDC gibt sofort klare und belegte Inputs, wie der Kunde seine interne Security verbessern kann
- Kapsch CDC analysiert permanent – im Gegensatz zu Marktbegleitern, die teilweise nur einmal pro Woche Alarme auswerten
- Kapsch CDC übermittelt nicht einzelne Alarme, sondern einen Gesamtkontext zu Vorfällen, um dem Kunden einen klaren und verständlichen Überblick zu geben

Welche Probleme löst das Kapsch CDC?

- Ressourcenmangel beim Kunden
- Hochspezialisiertes, schwer verfügbares Wissen wird durch das Kapsch CDC verfügbar gemacht (durch Mitgliedschaft in relevanten Communities, Nutzung von spezialisierten Quellen etc.)
- Visibilität im Netzwerk wird ermöglicht – einen Großteil der Vorgänge würde der Kunde sonst nicht sehen

Die Top-3-Benefits für Kunden:

- Stetige Verbesserung seiner internen Security durch Rückmeldungen aus dem Kapsch CDC
- Direkter Ansprechpartner in Österreich
- Gesamte Expertise von Kapsch steht dahinter

Kapsch BusinessCom AG | Wienerbergstraße 53 | 1120 Wien | Österreich | T +43 50 811-0 | F +43 50 811-9995 | kbc.info@kapsch.net | www.kapsch.net | www.kapschbusiness.com