

KONDRA

SIEM, MDR, CTI FÜR KMU



KONDRA:

ÜBERWACHUNG RUND UM DIE UHR, OHNE EIGENES SOC.

Ihre Firewalls, Windows-Rechner und Ihr Microsoft-365-Tenant protokollieren bereits, was im Netzwerk geschieht. Gelesen wird davon kaum etwas. Um diese Daten rund um die Uhr zu überwachen, braucht es ein Security Operations Center (SOC) mit Analysten im Schichtbetrieb, und das können sich nur wenige KMU leisten.

So stapeln sich die Logs, und einen Einbruch bemerkt man meist erst am Schaden.

Kondra sammelt diese Logs, indexiert sie beim Eintreffen und schneidet zusätzlich den Netzwerkverkehr über einen Mirror-Port an Ihrem Switch mit. Erkennungsregeln und Threat Intelligence filtern daraus die Alarme heraus, und die Analysten von EXYS bearbeiten sie 24 Stunden am Tag.

Alles läuft auf einer Appliance in Ihrem eigenen Netzwerk. Die Analysten greifen dort auf Ihre Daten zu; die Daten selbst verlassen Ihr Haus nicht.

**SICHERHEIT WIE IM KONZERN.
KOSTEN WIE IM KMU.**

Die Appliance hört den Verkehr passiv über einen Mirror-Port am Switch mit und versteht mehr als 20 Netzwerkprotokolle. Ungewöhnliche Verbindungen, falsch konfigurierte Hosts und abfliessende Daten fallen auf, auch bei Geräten, auf denen nichts installiert ist.

Ombra, der Endpoint-Agent von Kondra, ergänzt, was das Netzwerk nicht sieht: die installierten Anwendungen und die Konfiguration jedes Geräts. Auch Änderungen an Benutzern, Gruppen und Gruppenrichtlinien im Active Directory werden erfasst, so kann schon ein neues Admin-Konto einen Alarm auslösen.

Nach jedem Vorfall wollen Revision und Aufsicht dasselbe wissen: was passiert ist, wann, und was unternommen wurde. Mit Kondra ist das bereits dokumentiert. Jedes Ereignis ist durchsuchbar, das EXYS SOC eröffnet einen Fall mit Logs und Indicators of Compromise (IoC), und der forensische Bericht entsteht aus denselben Daten. Die Aufbewahrungsdauer wird pro Kunde festgelegt, je nachdem, was Revision, Aufsicht oder interne Richtlinien verlangen. EXYS selbst ist nach ISO 27001 zertifiziert.



WAS SIE BEKOMMEN:

- Appliance vor Ort, dimensioniert nach Anzahl Endpunkte, die Logs bleiben bei Ihnen
- Überwachung und Reaktion rund um die Uhr durch Analysten des EXYS SOC
- Passive Netzwerküberwachung über einen Mirror-Port am Switch, mehr als 20 Protokolle
- Logs von Firewalls verschiedener Hersteller, Microsoft 365, Windows-Ereignissen, Netzwerk und IDS, dazu eigene Quellen auf Anfrage
- Korrelation mit Open-Source- und eigener Threat Intelligence
- Vorgefertigte Dashboards, eine Netzwerkkarte der Problem-Hosts und Alarmierung über mehrere Kanäle
- Endpoint-Agent Ombra für Software-Inventar und Endpoint-Konfiguration
- Änderungsverfolgung im Active Directory: Benutzer, Gruppen, Gruppenrichtlinien und Organisationseinheiten
- Fallbearbeitung im EXYS SOC, mit verknüpften Logs, IoCs und forensischen Berichten
- MITRE-ATT&CK- und RE&CT-Matrizen zur Abdeckung von Erkennung und Reaktion
- Malware-Analyse, mit isolierten Dateien und PCAP-Mitschnitten für die Untersuchung
- Erweiterungen für OT-Ereignisse
- Log-Aufbewahrung, Integritätsprüfung und Backup für Compliance-Audits

MIR SIND FÜR SIE DA.

ADRESSE

EXYS SA
Strada Regina 16
CH-6934 Bioggio
Tessin, Schweiz

KONTAKT

Telefon +41 (0)91 220 52 00

www.exys.swiss
office@exys.swiss

EXYS SA ist nach ISO/IEC 27001 zertifiziert



EXYS
WHERE PASSION
MEETS TECHNOLOGY
EXYS7950 - KONDRA