XDR as a Service (by Palo Alto Networks)

Über 70 % der Cyberangriffe starten auf dem Endgerät, entweder über eine Webseite oder über ein E-Mail.

Security Operations wird aufgrund einer wachsenden Angriffsfläche, einer gefährlichen Bedrohungslandschaft und der zunehmenden Nutzung von Cloud Computing schwieriger. Präventive Schutzmassnahmen wie Antivirensoftware reichen deshalb nicht aus. Dagegen kann XDR as a Service (by Palo Alto Networks) Anomalien erkennen und den End-Benutzer und die IT-Infrastruktur vor Attacken schützen.

XDR as a Service basiert auf einer einheitlichen Plattform zur Erkennung und Reaktion auf Sicherheitsvorfälle. Die Daten werden automatisch von mehreren Sicherheitskomponenten und Quellen gesammelt und ausgewertet. Bei einer Attacke werden Security Alerts oder Incidents erstellt. Um False Positives erkennen oder auf Security Incidents reagieren zu können, haben Security Analysten das Dashboard immer im Blick.

Ihr Nutzen mit XDR as a Service (by Palo Alto Networks)

Alles im Blick

End-to-End-Sichtbarkeit der Vorgänge, Prozesse, Applikationen, Memory, Files über alle Endpunkte, Identitäten, Netzwerke und externe Daten. ✓

Umfassender Schutz

Schutz vor dateibasierter und dateiloser Malware, Ransomware, Attacken sowie Zero-Day-Exploits. ✓

Ausführliche Analyse

Sammeln, analysieren und korrelieren von Daten aus verschiedenen Quellen und Events. ✓

Entlastung

Dank automatisierter Untersuchungen und Behebungen von Alerts wird das Security-Betriebsteam entlastet. ✓

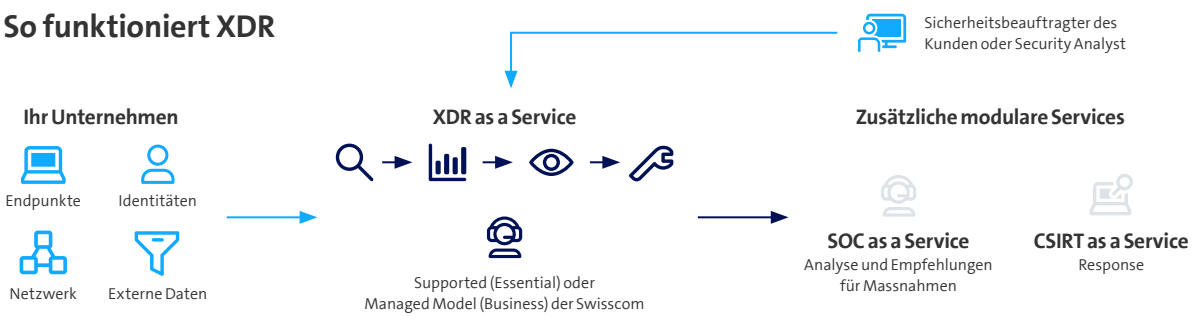
Übersichtliches Dashboard

Das XDR Dashboard bietet Advanced Threat Hunting sowie Remote Remediation Capabilities. ✓

Managed Service

Swisscom bietet das ganze Swisscom Cybersecurity Portfolio und Management an sowie die Integration in andere Swisscom Security Services. ✓

So funktioniert XDR



swisscom

XDR as a Service (by Palo Alto Networks)

Swisscom-Leistungen

	Essential	Business
Projektleistungen für das Setup des Services und das Onboarding der Komponenten	●	●
Das Management des Kunden-Tenants	—	●
Review und quartalsweise proaktive Kommunikation von neuen Features und Funktionalitäten, Einschätzung und Empfehlung durch Swisscom	—	●
Konfiguration der Security Policies und Onboarding, Lifecycle und Release Management des Agents auf den Endpoints	—	●
Jährliches Assessment der implementierten Security Policies	●	●
Incident Management von betrieblichen Incidents über den Swisscom Service Desk	○	●

XDR Features, Optionen und Komponenten

Next-Gen Endpoint Protection (EPP)	—	●
Endpoint Detection and Response (EDR)	—	●
Data Retention Time 30 Tage	—	●
Zusätzliche Data Retention Time von 30 Tagen	—	○
USB Device Control	—	●
Host Firewall und BitLocker Disk Encryption	—	●
Threat & Vulnerability Monitoring (Host Insights)	—	○
Anbindung externe Daten per TB	—	○
Digitale Forensik (Forensics)	—	○

Lizenzen

Lizenzen und Lizenzmanagement	—	●

● Standard (im Projektpreis inbegriffen)
○ Gegen Aufpreis
— Nicht erhältlich

Kombinierbare Zusatzservices

Threat Detection & Response – SOC as a Service
Mit Threat Detection & Response – SOC as a Service erhalten Sie via Dashboard einen Überblick über potenzielle und bestätigte Sicherheitsvorfälle aus definierten Log-Daten Ihrer Unternehmung. Zusätzliche Analysen mit konkreten Handlungsempfehlungen helfen Ihnen, auf kritische Security Incidents selbstständig zu reagieren.

Threat Detection & Response – CSIRT as a Service
Mit Threat Detection & Response – CSIRT as a Service ziehen Sie Experten von Swisscom zur Analyse und Bewältigung von Vorfällen bei. Wir leiten den Security-Incident-Management-Prozess remote oder bei Ihnen vor Ort, unterstützen Sie bei der Beweissicherung sowie der Kommunikation zu Kunden und Partnern.

Enterprise Workspace, Smart, Connected oder Rich Workplace
Enterprise Workspace oder Smart, Connected oder Rich Workplace: vom digital smarten Arbeitsplatz, den die Benutzer selbstständig ohne IT einrichten können, bis hin zu einem ganzheitlich gemanagten Client-Arbeitsplatz, inklusive Software-Verteilung, Software-Paketierung, Asset-Management und Good Practice Security.

Swisscom (Schweiz) AG Enterprise Customers, Postfach, CH-3050 Bern, Tel. 0800 800 900, www.swisscom.ch/enterprise