Microsoft XDR as a Service

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 Microsoft XDR as a Service Anomalien erkennen und den End-Benutzer und die IT-Infrastruktur vor Attacken schützen.

Microsoft 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 Microsoft XDR as a Service

Alles im Blick

End-to-End-Sichtbarkeit der Vorgänge, Prozesse, Applikationen, Memory, Files über alle Endpunkte, Identitäten, Apps, E-Mails, Daten und Cloud-Workloads. ✓

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. ✓

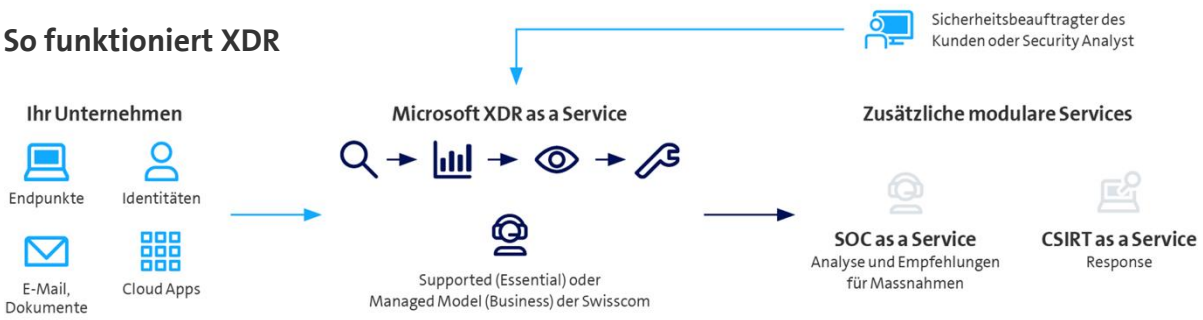
Übersichtliches Dashboard

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

Microsoft XDR as a Service im Überblick

Swisscom-Leistungen

	Essential	Business
Projektleistungen für das Onboarding	●	●
Jährliches Security Policy Assessment	●	●
Tenant Management durch den Kunden	–	–
Review und Kommunikation von neuen Features und Funktionalitäten	–	●
Security Policy Konfiguration und Agent Lifecycle	–	●
Monitoring der Betriebs- und Health Alerts	–	●
Incident Management von betrieblichen Vorfällen	○	●

XDR Komponenten

Microsoft Defender for Endpoint (MDE) • Next-Gen Endpoint Protection (EPP) • Endpoint Detection and Response (EDR) • Threat & Vulnerability Monitoring • Attack Surface Reduction • Device Control	–	○
Microsoft Defender for Office (MDO) Schutz und Monitoring von E-Mails	–	○
Microsoft Defender for Identity (MDI) Schutz und Monitoring der Identitäten auf dem Active Directory (AD) und AD FS	–	○
Microsoft Defender for Cloud Apps (MDCA) Erkennt und schützt vor Shadow IT	–	○

Lizenzen

Lizenzen und Lizenzmanagement	–	–

● Standard (im Projektpreis inbegriffen)
○ Optional erhältlich
– 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.

Microsoft 365 Management
Überlassen Sie uns das Management von Microsoft 365 und fokussieren Sie sich auf Ihr Kerngeschäft. Das Management des Kunden-Tenants und die Lizenzen sind hier verfügbar.

Die Informationen in diesem Dokument stellen kein verbindliches Angebot dar. Änderungen sind jederzeit vorbehalten.

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

swisscom