Network Detection and Response as a Service

Hochgradig verteilte und hybride Netzwerke lassen sich aufgrund ihrer Komplexität nur schwer analysieren und überwachen. Der Netzwerkverkehr selbst ist oft verschlüsselt und kaum einsehbar, was Sicherheitstools die Malware-Erkennung erschwert.

Die Bedrohungserkennung im Netz mit statischen Indicators of Compromise für bekannte Schadsoftware reicht nicht mehr aus. Neue und veränderte Angriffsformen benötigen eine verhaltensbasierte Abwehr.

Was ist NDR as a Service?

Verschlüsselter Netzwerkverkehr und eine Bedrohungserkennung mit statischen IOC öffnen Cyberangreifern zu viele Schlupflöcher. Der erforderliche Schutz ist damit nicht mehr gewährleistet.

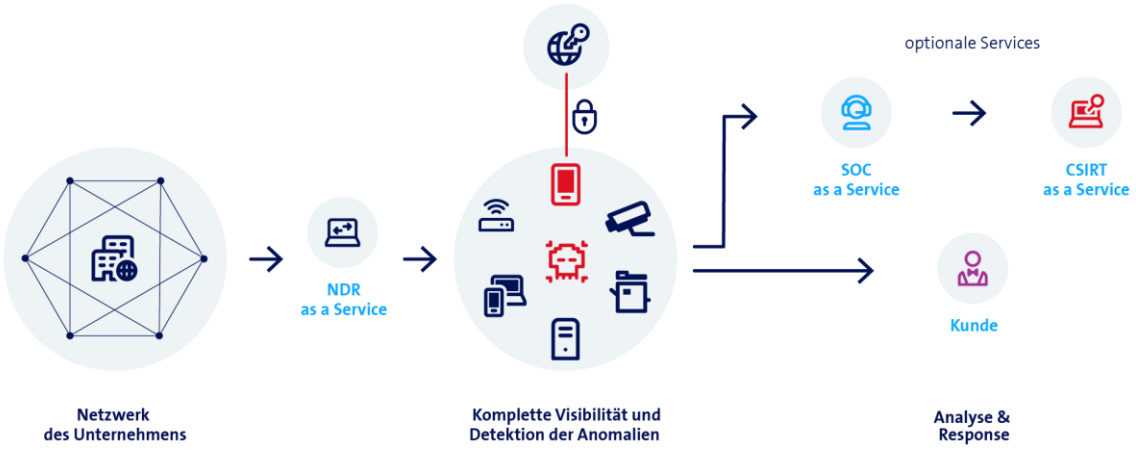
Network Detection and Response (NDR) bietet leistungsstarke und fortschrittliche KI-Algorithmen, um Unternehmensnetzwerke verlässlich zu sichern. Cyberattacken lassen sich schnell erkennen und beseitigen.

Maximale Visibilität über alle Netzwerkaktivitäten steht dabei im Vordergrund von NDR.

Ihre Nutzen mit NDR as a Service

- **Visibilität in Ihrem Netzwerk**
  Schwachstellen identifizieren, bevor sie von Angreifern ausgenutzt werden (beispielsweise exponierte Dienste, Schatten-IT).
- **Einsicht in verschlüsselten Netzwerkverkehr**
  Automatisierte Erkennung von Angreifern in Ihrem Netzwerk, bevor Daten exfiltriert oder verschlüsselt werden.
- **Vorgefertigte Anwendungsfälle und ML-Modelle**
  Automatisierte quellenübergreifende Korrelation und intuitive Visualisierungen.
- **Schnelle Bereitstellung**
  Keine zusätzliche Hardware und auch keine Agenten notwendig.

So funktioniert Network Detection and Response



swisscom

Facts & Figures

Basisleistungen	On-Premises: Die NDR-Appliance wird vor Ort beim Kunden gehostet und vom Kunden überwacht. Sicherheitspatches werden in Absprache mit Kunde und Hersteller eingepflegt. Sofern der Kunde die Leistung Security Analytics as a Service (SAaaS) und Security Operation Center as a Service (SOCaaS) bezieht, kann ein Software-basierter Forwarder auf der Kundenumgebung installiert werden, um die Incidents von der Appliance ans SOC zur Analyse weiterzuleiten. Bei verdächtigen Sicherheitsvorfällen wird der Kunde informiert.
	Managed by Swisscom: Die NDR-Appliance wird zusammen mit einer Logging-Plattform in einem Swisscom Rechenzentrum gehostet und überwacht. Sicherheitspatches werden von Swisscom eingepflegt. Sofern der Kunde die Leistung SAaaS und SOCaaS bezieht, stellt Swisscom sicher, dass Incidents von der Appliance ans SOC zur Analyse weitergeleitet werden. Bei verdächtigen Sicherheitsvorfällen wird der Kunde informiert.
Zusatzservices	Security Analytics as a Service (SAaaS): Wir sind Fachleute in den Themen Security und Big Data und stellen Ihnen unsere bewährte Security-Analytics-Infrastruktur zur Verfügung. Schliessen Sie weitere Logquellen aus der Cloud, On-Premises oder von einem Managed Provider an und erhalten Sie im Dashboard einen Überblick über potenzielle Sicherheitsvorfälle. Analyse und Reaktion auf Sicherheitsvorfälle übernehmen Sie selbst.
	SOC as a Service (SOCaaS): Sie erhalten via Dashboard einen Überblick über potenzielle und bestätigte Sicherheitsvorfälle aus definierten Logdaten Ihrer Unternehmung sowie Analysen mit konkreten Handlungsempfehlungen. Auf kritische Security Incidents reagieren Sie selbständig.
	CSIRT as a Service (CSIRTaaS): Zur Analyse und Bewältigung von Sicherheitsvorfällen ziehen Sie Fachleute von Swisscom bei. Wir leiten den Security-Incident-Management-Prozess remote oder bei Ihnen vor Ort und unterstützen Sie bei der Beweissicherung sowie der Kommunikation mit Kunden und Partnern.
	Digital Risk Protection as a Service (DRPaaS): Sie werden proaktiv informiert über das Vorkommen von sensiblen Geschäfts- und persönlichen Informationen Ihres Unternehmens in öffentlichen und geschlossenen Netzen (z.B. Darknet). Unsere Handlungsempfehlungen für bestätigte Sicherheitsvorfälle setzen Sie selbständig um.

Mehr Informationen und den Kontakt zu unserem Experten finden Sie auf **swisscom.ch/ndr**

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

swisscom