



Oltre il 70 % dei cyber-attacchi parte da un terminale, attraverso un sito web o una e-mail.

Le operazioni di sicurezza diventano sempre più difficili a fronte di una maggiore vulnerabilità, un panorama di minacce oltremodo pericoloso e l'utilizzo crescente del Cloud Computing. Ecco perché misure di protezione preventive come i software antivirus non bastano più. Invece, XDR as a Service (by Palo Alto Networks) è in grado di riconoscere le anomalie e proteggere l'utente finale e l'infrastruttura IT dagli attacchi.

XDR as a Service si basa su una piattaforma unitaria per l'individuazione e la reazione a eventi critici per la sicurezza. I dati vengono raccolti e valutati automaticamente da varie fonti e componenti di sicurezza. Nel caso di un attacco vengono attivati Security Alerts o Incidents. Per riconoscere i falsi positivi o per poter reagire ai Security Incidents, gli analisti della sicurezza tengono sempre sotto controllo il dashboard.

I vostri vantaggi con XDR as a Service (by Palo Alto Networks)

Tutto sotto controllo

Visibilità end-to-end delle operazioni, processi, applicazioni, memoria, file da tutti gli endpoint, identità, rete e dati esterni.



Protezione completa

Protezione da file-based e fileless malware, ransomware, attacchi ed exploit zero-day.



Analisi dettagliata

Raccolta, analisi e correlazione dei dati da varie fonti ed eventi.



Riduzione del carico di lavoro

Grazie ad analisi automatizzate ed eliminazione degli alert, si riduce il carico di lavoro per il team operativo addetto alla sicurezza.



Dashboard funzionale e ben strutturato

L'XDR dashboard offre Advanced Threat Hunting e anche Remote Remediation Capabilities.

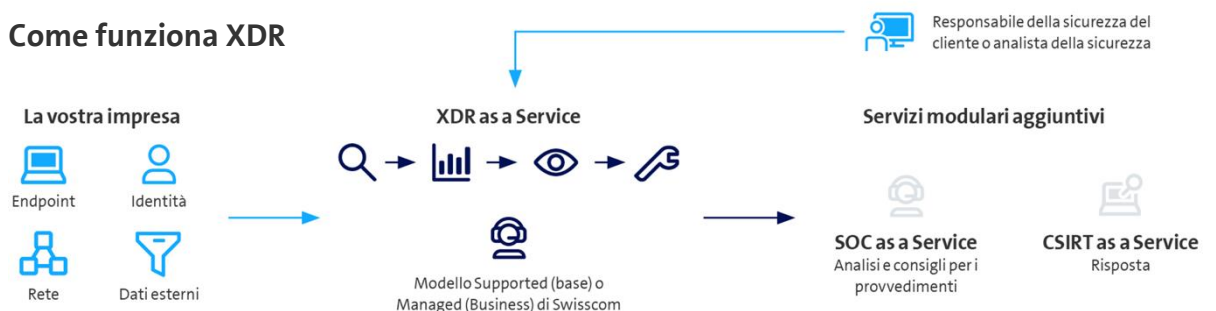


Servizi gestiti

Swisscom offre l'intero Swisscom Cyber Security Portfolio e Management, oltre all'integrazione in altri servizi di sicurezza Swisscom.



Come funziona XDR





Le informazioni contenute in questo documento non rappresentano un'offerta vincolante. Con riserva di modifiche in qualsiasi momento.

Swisscom (svizzera) SA Enterprise Customers, Casella postale, CH-3050 Berna, tel. 0800 800 900, www.swisscom.ch/enterprise

XDR as a Service (by Palo Alto Networks)

Prestazioni di Swisscom

	Essential	Business
Servizi di progetto per l'onboarding	●	●
Valutazione annuale delle security policies implementate	●	●
Gestione tenant cliente	–	●
Revisione e comunicazione di nuove caratteristiche e funzionalità	–	●
Configurazione della politica di sicurezza e ciclo di vita dell'agente	–	●
Monitoraggio degli allarmi operativi e sanitari	–	●
Incident Management degli incidenti aziendali	○	●

Opzioni e componentistica XDR

Next-Gen Endpoint Protection (EPP)	○	●
Endpoint Detection and Response (EDR)	○	●
USB Device Control	○	●
Data Retention Time 30 giorni	○	●
Ulteriore Data Retention Time	○	○
XDR Pro Host Insights	○	○
Extended Threat Hunting (XTH)	○	○
Identity Threat Detection and Response (ITDR)	○	○
XDR PRO per GB Hot Storage	○	○
Digital Forensics	○	○

Licenze

Licenze e gestione licenze	○	○
----------------------------	---	---

- Standard (incl. nel prezzo del progetto)
- A pagamento
- Non disponibile

Servizi aggiuntivi abbinabili

Threat Detection & Response – SOC as a Service

Con **Threat Detection & Response – SOC as a Service** ricevete attraverso il dashboard una panoramica degli eventi critici per la sicurezza sia potenziali che confermati da dati log definiti della vostra impresa. Ulteriori analisi con raccomandazioni per misure concrete da adottare vi aiuteranno a reagire autonomamente a Security Incidents critici.

Threat Detection & Response – CSIRT as a Service

Con **Threat Detection & Response – CSIRT as a Service** fate intervenire gli esperti Swisscom per l'analisi e per far fronte agli incidenti. Guidiamo il processo di Security Incident Management da remoto in loco presso di voi, vi aiutiamo nella raccolta delle prove nonché nella comunicazione con clienti e partner.

Enterprise Workspace, Smart, Connected oppure Rich Workplace

Enterprise Workspace oppure **Smart, Connected** oppure **Rich Workplace**: dalla postazione di lavoro smart digitale, che gli utenti possono allestire autonomamente, senza IT, fino alla postazione Client completamente gestita, inclusa distribuzione software, software packaging, asset management e good practice security.

Threat Detection & Response – NDR as a Service

Threat Detection & Response – NDR as a Service offre algoritmi AI potenti e avanzati per proteggere in modo affidabile le reti aziendali. Gli attacchi informatici possono essere rapidamente identificati ed eliminati.