Extended Detection and Response (XDR) - Guida introduttiva

SOPHOS
Cybersecurity evolved.

Che cosa significa XDR?

Siccome vengono utilizzati vari modi per descrivere questa funzionalità, cominciamo con una definizione di Extended Detection e Response (XDR).

- **Extended Detection and Response** (rilevamento e risposta estesi) è la definizione utilizzata più frequentemente, nonché quella adottata da diversi analisti e vendor di cybersecurity. Il termine "Extended" (esteso) si riferisce al concetto di non fermarsi agli endpoint e ai server, ma di andare oltre, raccogliendo dati da altre origini quali firewall, e-mail, cloud, dispositivi mobili e altro.
- **Cross-product Detection and Response** (rilevamento e risposta su prodotti multipli) è un'altra definizione che si riferisce all'integrazione dei dati provenienti da prodotti e livelli di sicurezza multipli.
- La terza interpretazione utilizza la "X" di XDR come variabile matematica che rappresenta tutte le origini di dati utilizzati per la soluzione.

Qualsiasi sia la definizione di XDR scelta per descriverla, tutte le opzioni fanno riferimento e utilizzano gli stessi concetti principali, ovvero la capacità di accedere e formulare query su un'ampia gamma di origini di dati, per garantire maggiore visibilità e contesto alla propria organizzazione.

Come funziona l'XDR?

L'XDR è una soluzione progettata per offrire alle organizzazioni una prospettiva olistica dello stato di sicurezza e dell'ambiente IT, con la capacità di passare a indagini più approfondite laddove necessario.

Secondo Gartner:

"Le principali proposte di valore di un prodotto XDR sono le capacità di incrementare la produttività delle operazioni di sicurezza e di ottimizzare le funzioni di rilevamento e risposta alle minacce, includendo un maggior numero di componenti di sicurezza in un sistema unificato e in grado di offrire varie opzioni di telemetria con diverse alternative per forme di rilevamento multiple, abilitando nel contempo l'utilizzo di diversi metodi di risposta."

Gartner, "Innovation Insight for Extended Detection and Response" (2020).

Una domanda frequente è: "Quali differenze presenta rispetto all'EDR?". Le soluzioni XDR devono, a tutti gli effetti, includere le stesse capacità di risposta a domande critiche per le organizzazioni che utilizzando EDR (Endpoint Detection and Response). Devono infatti essere in grado di raccogliere dati in tempo reale direttamente da un endpoint o server e devono permettere di accedere ai dati nel cloud quando un dispositivo è off-line.

L'XDR parte da queste solide basi e aggiunge ulteriori dati e contesto, per incrementare la visibilità e fornire all'utente maggiori approfondimenti durante un'indagine. I risultati sono maggiore rapidità e precisione nel rilevamento e nella risposta agli incidenti. Le origini di dati aggiuntive possono includere firewall, e-mail, cloud e dispositivi mobili. Ad esempio, arricchire le informazioni con dati provenienti dal firewall semplifica la correlazione tra il traffico dannoso del firewall e un endpoint compromesso; può anche aiutare a identificare un'applicazione che rallenta la connessione della rete in ufficio.

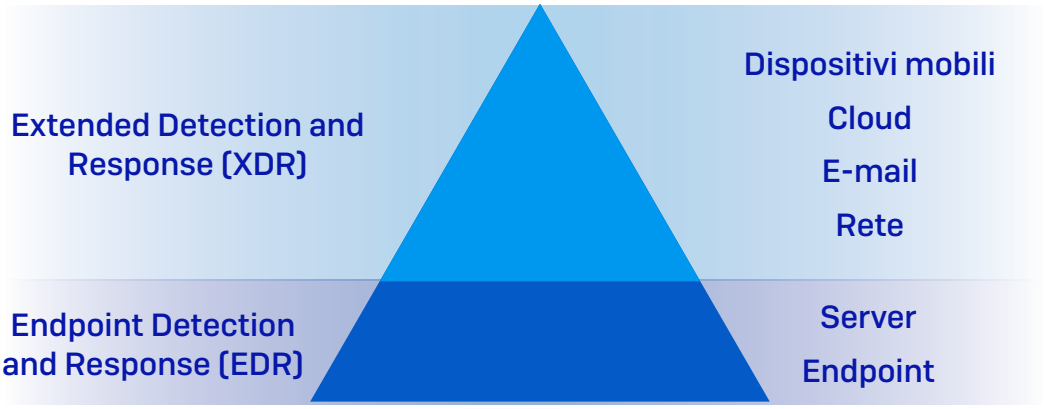
Uno dei metodi migliori per utilizzare l'XDR è cominciare dalle "macroanalisi", che offrono strumenti di scansione dell'intero ambiente in grado di mettere in evidenza eventuali attività sospette, comportamenti anomali o altri problemi informatici. Quando viene identificato un problema, è quindi possibile agire su un dispositivo in particolare, raccogliendo dati in tempo reale o effettuando l'accesso al dispositivo da remoto per affinare le indagini e intraprendere azioni correttive.

Origini di dati estese

Per quanto siano potenti, gli strumenti EDR sono pur sempre limitati al rilevamento e alla risposta su endpoint e server. Questa non è necessariamente una caratteristica negativa. Se si deve selezionare un unico ambito su cui focalizzare le attività di rilevamento e risposta dell'organizzazione, endpoint e server sono decisamente un'ottima scelta.

Tuttavia, ci sono azioni che non è possibile svolgere su questi sistemi in isolamento. Dopotutto, l'ambiente IT è una struttura interconnessa di reti, strumenti di comunicazione, dispositivi mobili, applicazioni cloud e molto di più. Per proteggere l'infrastruttura IT in maniera più completa, un elemento essenziale è un sistema integrato di rilevamento e risposta. Ed è qui che entra in gioco l'XDR.

XDR estende l'idea di EDR. Va oltre gli endpoint e i server, per integrare dati provenienti da altri strumenti di sicurezza quali firewall, gateway di posta,
strumenti per il cloud pubblico e soluzioni di gestione delle minacce dei dispositivi mobili. L'XDR è una tecnologia emergente, per cui le origini di dati e le funzionalità variano da vendor a vendor. Tuttavia, questo diagramma costituisce un buon punto di partenza per capire quali sono gli elementi aggiuntivi dell'XDR rispetto all'EDR.



Casi di utilizzo di XDR

Il modo migliore per spiegare i vantaggi concreti dell'XDR è osservare come questa funzionalità può aiutare le organizzazioni a svolgere le proprie attività quotidiane di IT operations e threat hunting. Abbiamo incluso anche esempi di EDR, poiché una soluzione XDR deve essere in grado di gestire anche questi casi.

	IT operations	Threat hunting
EDR	• Perché un computer è particolarmente lento? • Su quali dispositivi sono presenti vulnerabilità note, servizi sconosciuti o estensioni del browser non autorizzate? • Ci sono programmi in esecuzione che dovrebbero essere rimossi?	• Quali processi stanno cercando di stabilire una connessione di rete su porte non standard? • Visualizzazione dei processi che hanno recentemente modificato file o chiavi di registro • Elenco degli indicatori di compromissione (Indicator of Compromise, IoC) mappati al framework MITRE ATT&CK
XDR	• Identificazione dei dispositivi non gestiti, IoT e appartenenti a utenti guest • Perché la connessione di rete in questo ufficio è lenta? Qual è l'applicazione responsabile? • Possibilità di indagare sugli ultimi 30 giorni di attività di un dispositivo smarrito o reso inutilizzabile, per rilevare eventi anomali	• Estensione delle indagini a 30 giorni senza bisogno che il dispositivo sia on-line • Utilizzo dei rilevamenti ATP e IPS del firewall per svolgere indagini sugli host sospetti • Confronto tra dati nell'intestazione delle e-mail, SHA e altri indicatori di compromissione, per identificare il traffico diretto verso un dominio pericoloso

Sophos vi può aiutare, ecco come

Sophos XDR fornisce alle organizzazioni una prospettiva ampia e olistica del loro intero ambiente di cybersecurity, con la possibilità di svolgere approfondimenti, se richiesto. In altre parole, offre sia una prospettiva generale della situazione vista "dall'alto", sia dettagli granulari, a seconda delle esigenze del momento.

Le soluzioni predisposte per l'XDR inviano dati provenienti da endpoint, server, firewall, e-mail e altre origini* al Sophos Data Lake, un repository cloud di dati critici di XDR e dati off-line dei dispositivi. È un punto centralizzato di raccolta di tutti i dati, che permette di rispondere rapidamente a domande critiche per l'organizzazione, correlare eventi provenienti da varie origini e intraprendere azioni basate su decisioni più informate.

Grazie alla raccolta di query precompilate e completamente personalizzabili, cominciare a utilizzare questo sistema è semplice: basta scegliere una categoria, aggiungere dispositivi ed è subito possibile cominciare a rispondere alle domande sulle IT operations e sul threat hunting.

Gartner Innovation Insight for Extended Detection and Response, Peter Firstbrook, Craig Lawson,19 marzo 2020.

Gartner non appoggia non sostiene alcun fornitore, produttore o servizio citato all'interno delle sue pubblicazioni di ricerca e non consiglia agli utenti delle tecnologie di selezionare solo i fornitori con le valutazioni più alte o altre designazioni. Le pubblicazioni di Gartner riflettono solamente le opinioni dell'organizzazione, e non devono pertanto essere considerate come affermazioni di fatto. Gartner rinuncia a qualsiasi garanzia, implicita o esplicita, in merito a questa ricerca, incluse le garanzie sulla commerciabilità o sull'idoneità a un particolare scopo.

* Cloud Optix e Sophos Mobile saranno disponibili prossimamente

Per saperne di più, visitate: sophos.it/xdr

SOPHOS

06/04/21 WP (NP)