CROWDSTRIKE

CHE COS'È ESATTAMENTE XDR?

XDR sta per "extendend detection and response", o rilevamento e risposta estesa, ed è l'ultima frontiera per bloccare le minacce sofisticate di oggi.
Rappresenta un approccio olistico che ottimizza l'acquisizione, l'analisi e i flussi di lavoro relativi alla sicurezza dei dati per tutte le operazioni di sicurezza dell'organizzazione.

Extended (Estesa)

Amplia il rilevamento e risposta agli endpoint (EDR) con la telemetria a pieno spettro ricavata e integrata per tutte le operazioni di sicurezza

Detection (Rilevamento)

Identifica e individua le minacce più rapidamente con gli indicatori di attacco, le informazioni utili e gli avvisi per più piattaforme in un'unica console unificata

Response (Risposta)

Trasforma le informazioni utili XDR in azione e design orchestrati e automatizza i flussi di lavoro di risposta multipiattaforma per il ripristino chirurgico e ottimizzato

PERCHÉ XDR PROPRIO ADESSO?

I dati di sicurezza e i sistemi isolati generano punti ciechi

45

il numero medio di strumenti relativi alla sicurezza informatica distribuiti sulle reti aziendali[1]

I team di sicurezza devono muoversi in modo rapido e agile per rispondere alle minacce di oggi

92

i minuti prima che gli attaccanti inizino a spostarsi lateralmente dopo avere ottenuto l'accesso[2]

Massimizza il valore della tecnologica esistente per contenere il rischio

59%

la percentuale di responsabili globali delle decisioni che ha segnalato la compromissione dei dati sensibili della propria azienda almeno una volta nello scorso anno[3]

NON FARTI INGANNARE DA FAUXDR

Molti fornitori propongono un "XDR" che non è affatto tale:

NON XDR:

- ☒ NDR ≠ XDR
- ☒ SOAR ≠ XDR
- ☒ SIEM ≠ XDR
- ☒ NDR + SOAR + SIEM ≠ XDR

XDR – L'ORIGINALE

RILEVAMENTO PIÙ RAPIDO AD ALTA FEDELTÀ
Estendi le tecnologie di protezione alle origini dei dati di terzi per rilevamento, indagine e individuazione ad alta fedeltà su tutta la superficie di attacco

ECOSISTEMA DI PUNTA
Riunisci la telemetria pertinente proveniente da più tecnologie e domini per consentire una risposta accelerata alle minacce, ovunque esse avvengano

RIDUCI IL COSTO TOTALE DI PROPRIETÀ
Amplia il valore delle tue operazioni di sicurezza facendole collaborare

RISPOSTA OTTIMIZZATA
Consenti ai team di sicurezza di progettare e automatizzare i flussi di lavoro della risposta multiambiente e multipiattaforma per il ripristino chirurgico delle operazioni complete

SECOPS PIÙ EFFICIENTI
Crea correlazioni in modo intelligente tra i dati provenienti da più origini, rapidamente e su larga scala, per fornire informazioni utili di sicurezza attuabili da un'unica console

PRONTI PER IL VERO XDR?

Inizia con questa lista di controllo di preparazione XDR:

- ☑ La soluzione dispone di funzionalità **native di rilevamento e risposta agli endpoint**?
- ☑ Sono disponibili **informazioni unificate incentrate sulle minacce** per risposte di rilevamento e ottimizzazione accurate?
- ☑ Il **rilevamento automatico** è disponibile su tutti gli ambienti IT, i flussi di lavoro cloud, le reti, l'email e gli endpoint al fine di **ridurre il tempo di triage** e **accelerare la risposta**?
- ☑ È disponibile un numero sufficiente di **integrazioni basate sul cloud** per acquisire registri ed eventi da più origini dati e terzi?
- ☑ Esiste un'**alleanza tra partner strategici** consolidata con i fornitori di soluzioni leader del settore?

> "UN XDR VALIDO È INDISSOLUBILMENTE LEGATO AL FONDAMENTO DI UN EDR VALIDO."[3]
>
> — Report Forrester: Adapt Or Die: XDR Is On A Collision Course With SIEM And SOAR —

La soluzione definitiva per il rilevamento, l'indagine, l'individuazione e la risposta unificati multipiattaforma.

FALCON XDR

Estendi oltre l'endpoint

Ulteriori informazioni

FONTI:

[1] https://www.zdnet.com/article/the-more-cybersecurity-tools-an-enterprise-deploys-the-less-effective-their-defense-is/
[2] https://www.darkreading.com/threat-intelligence/attackers-moving-faster-inside-target-networks-report
[3] https://reprints2.forrester.com/#/assets/2/482/RES165775/report

CROWDSTRIKE

WE STOP BREACHES