CROWDSTRIKE

WAS GENAU IST XDR?

Extended Detection and Response (XDR) steht für „erweiterte Erkennung und Reaktion“ und ist eine innovative Lösung zum Stoppen aktueller hochentwickelter Bedrohungen. Der ganzheitliche Ansatz vereinfacht die Erfassung und Analyse von Sicherheitsdaten sowie Workflows in der gesamten Sicherheitsumgebung eines Unternehmens.

X

Extended
(Erweiterte)

Optimieren Sie Ihre Maßnahmen zur endpunktbasierten Detektion und Reaktion (EDR) mit umfassenden Telemetriedaten, die aus der gesamten Sicherheitsumgebung erfasst wurden und mit dem gesamten Stack integriert werden können.

D

Detection
(Erkennung)

Identifizieren und suchen Sie Bedrohungen schneller mithilfe plattformübergreifender Angriffsindikatoren, Einblicke und Warnmeldungen, die Sie auf einer zentralen Konsole abrufen können.

R

Response
(Reaktion)

Verwandeln Sie XDR-Einblicke in koordinierte Maßnahmen und entwickeln sowie automatisieren Sie Reaktions-Workflows, die mehrere Plattformen umfassen und gezielte, optimierte Behebungsmaßnahmen ermöglichen.

WARUM IST XDR JETZT WICHTIG?

Isolierte Sicherheitsdaten und -systeme führen zu erheblichen blinden Flecken.

45

Durchschnittliche Anzahl von Cybersicherheitstools, die in Unternehmensnetzwerken eingesetzt werden[1]

Sicherheitsteams müssen schnell und flexibel auf aktuelle Bedrohungen reagieren.

92

Minuten, bis Angreifer sich nach dem Erstzugriff lateral durch das Netzwerk bewegen[2]

Nutzen Sie alle Vorteile Ihrer vorhandenen Technologie, um Risiken zu minimieren.

59 %

Anteil der weltweiten Entscheidungsträger, die berichten, dass die vertraulichen Daten ihres Unternehmens im vergangenen Jahr mindestens einmal kompromittiert wurden[3]

FALLEN SIE NICHT AUF FALSCHE XDR-LÖSUNGEN HEREIN

Anbieter verkaufen „XDR“, das die Anforderungen nicht erfüllt.

KEIN **XDR**:

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

ECHTES XDR

SCHNELLE, ZUVERLÄSSIGE ERKENNUNG
Decken Sie mit den Schutztechnologien auch externe Datenquellen ab, um zuverlässige Erkennung, Untersuchung und Suchfunktionen für die gesamte Angriffsfläche zu erhalten.

ERSTKLASSIGES ÖKOSYSTEM
Vereinheitlichen Sie relevante Telemetriedaten aus mehreren Technologien und Domänen, um überall schneller auf Bedrohungen reagieren zu können.

GERINGERE GESAMTBETRIEBSKOSTEN
Lassen Sie Ihre Sicherheitslösungen zusammenarbeiten und verbessern Sie sie so deren Mehrwert.

VEREINFACHTE REAKTION
Unterstützen Sie Ihr Sicherheitsteam bei der Entwicklung und Automatisierung von Workflows für mehrere Stufen und Plattformen, die gezielte, optimierte Behebungsmaßnahmen ermöglichen.

EFFIZIENTE SICHERHEITSPROZESSE
Führen Sie schnell und in großem Maßstab intelligente Korrelationen von Daten aus mehreren Quellen durch, um über eine zentrale Konsole verwertbare Sicherheitserkenntnisse zu erhalten.

BEREIT FÜR ECHTES XDR?

Anhand dieser XDR-Checkliste können Sie es prüfen.

- ✓ Verfügt die Lösung über **native Funktionen für endpunktbasierte Detektion und Reaktion**?
- ✓ Stehen einheitliche **Bedrohungsinformationen und -analysen** für zuverlässige Erkennung und vereinfachte Reaktionen zur Verfügung?
- ✓ Gibt es **automatisierte Erkennung** für alle IT-Umgebungen, Cloud-Workloads, Netzwerke, E-Mails und Endgeräte, um die **Zeit für die Triagierung zu verkürzen** und die **Reaktion zu beschleunigen**?
- ✓ Stehen **cloudbasierte Integrationen** zur Verfügung, mit denen Protokolle und Ereignisse aus mehreren internen und externen Datenquellen erfasst werden können?
- ✓ Gibt es bereits eine **strategische Partner-Alliance** mit branchenführenden Lösungsanbietern?

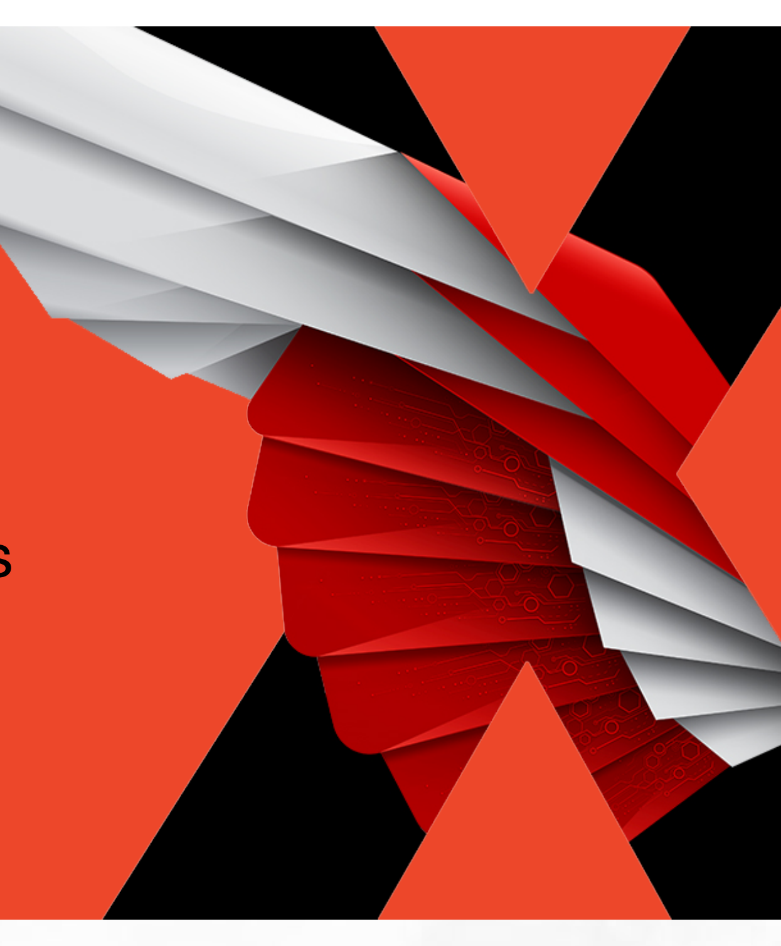
> „GUTES XDR STEHT UND FÄLLT MIT GUTEM EDR ALS GRUNDLAGE.“[3]
>
> – Forrester-Bericht: „Adapt or Die: XDR is on a Collision Course with SIEM and SOAR“

Die ultimative Lösung für einheitliche, plattformübergreifende Erkennung, Untersuchung, Suche und Reaktion

FALCON XDR

Schutz über Endgeräte hinaus

Weitere Informationen



QUELLEN:

[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