XDR GEGEN SIEM

DAS IST XDR

WAS IST ES?

XDR steht für “Extended Detection and Response”. Es wird generell als Weiterentwicklung von bestehenden Lösungen am Markt angesehen.

WARUM GIBT ES DAS?

Es wendet proaktive Maßnahmen an, indem es die Transparenz von Daten über Systemkomponenten hinweg in Kombination mit Analyse und Automatisierung gewährleistet.

WIE FUNKTIONIERT ES?

Durch das Sammeln und Analysieren von Daten aus mehreren Quellen können XDR-Lösungen Warnungen besser validieren, wodurch Fehlalarme reduziert und die Zuverlässigkeit stark erhöht werden kann.

WER VERWENDET ES?

XDR unterstützt Sicherheitsteams bei der Behebung von Vorfällen, indem Sicherheitsdaten normalisiert und ganzheitlich korreliert werden.

WANN MACHT ES SINN?

Wenn du die Erkennungsgenauigkeit erhöhen möchtst, indem du Signale über mehrere Lösungen hinweg korrelieren und die Effizienz und Produktivität verbessern willst, ist XDR genau das Richtige für dich.

DAS IST DER UNTERSCHIED

FAKT 1

XDR kann vor vielen Bedrohungen warnen, diese erkennen und sogar direkt darauf automatisch reagieren.

FACT 2

SIEM bietet dir einen ganzheitlichen Blick auf das Unternehmen und hilft dabei Bedrohungen schnell zu erkennen.

////// Danke //////

Dieses Poster wurde von Patrick in Kollaboration mit Heike Ritter erstellt.

Mehr zu Microsoft’s XDR & SIEM Lösung findest du unter aka.ms/SIEMandXDR

AFRAIT

DAS IST SIEM

WAS IST ES?

SIEM ist ein weiteres Akronym und steht für “security information and event management”. Es kombiniert Signale aus deinem Unternehmen.

WARUM GIBT ES DAS?

Der Hauptzweck von SIEMs besteht darin, Daten wie Protokolle von verschiedenen Tools für Aktivitäten, Sichtbarkeit und Untersuchungen zu sammeln und zu aggregieren.

WIE FUNKTIONIERT ES?

SIEM ist im Kern ein Datenaggregator. Es sammelt immense Datenmengen aus dem Unternehmen und der gesamten Netzwerkumgebung, konsolidiert diese Daten und macht sie für den Menschen zugänglich.

WER VERWENDET ES?

SIEM hilft Sicherheitsteams, Vorfälle schneller, einfacher und effizienter zu identifizieren, zu überprüfen und darauf faktenbasiert zu reagieren.

WANN MACHT ES SINN?

Wenn dein Ziel die Protokollierung und Protokollverwaltung ist, ist SIEM für dich. Ein weiterer Anwendungsfall ist die ganzheitliche Unterstützung zur Einhaltung von Vorschriften wie HIPAA, PCI, SOX und auch GDPR.