2022

WHITEPAPER

BARRACUDA SKOUT MANAGED XDR

MSP

Barracuda.

Your journey, secured.

BARRACUDA SKOUT MANAGED XDR

24/7 Cybersicherheit für Ihre Kunden

Bedrohungen im Netzwerk Ihrer Kunden sofort erkennen und zuverlässig reagieren

Bieten Sie mit **Barracudas Managed XDR** einen Service für Ihre Kunden an, mit denen Sie Bedrohungen sofort erkennen - und zwar bevor sie zum Problem werden. Echte Analysten im SOC lassen Ihnen umgehend praktikable Lösungsvorschläge zukommen. Optimieren Sie so Ihre Reaktionszeit.

DER FAKTOR ZEIT

Ein Cyberangreifer hat in der Regel 193 Tage Zeit, sich ausgiebig durch Systeme und Daten zu wühlen. Denn so lange bleiben Angriffe im Durchschnitt unbemerkt. Das ist ausreichend, um Daten zu manipulieren, abzuziehen und im Darknet zu verkaufen. Der ausschlaggebende Faktor bei der Bekämpfung von Cyberbedrohungen ist deshalb die Reaktionszeit.

Diese ist bei den meisten Unternehmen – selbst bei Unternehmen mit umfassender IT-Sicherheitsinfrastruktur – immer noch deutlich zu langsam. 2019 hatten **weniger als 5% der Unternehmen Services** im Einsatz, die Bedrohungen erkennen, untersuchen und aktiv darauf reagieren.

Ein Umstand, der zu Pandemiezeiten Tür und Tor für Cyberkriminelle geöffnet hat. Cyberangriffe befinden sich auf einem Rekordhoch. Es ist daher nicht verwunderlich, dass die **Allianz Cyberangriffe als Nr. 1 Business Risiko im Jahr 2022 nennt**. Schützen Sie Ihre Kunden zuverlässig mit einer Rundum-Sicherheitslösung, die State of the Art am globalen Markt ist.

XDR UND SOC FÜR HÖCHSTE SICHERHEIT

Der globale Markt für Cybersicherheit bewegt sich im Jahr 2022 weiter hin zu serviceorientierten Tools. Sicherheitslösungen müssen nicht nur zuverlässig und flexibel sein, sondern Kunden nach höchsten Standards umfassend unterstützen. XDR und SOC sind die wichtigsten Bausteine dieses Ansatzes.

193
TAGE

bleiben Cyberangriffe in der Regel unentdeckt

WAS IST SOC?

Ein SOC (=Security Operations Center) ist ein internes oder externes Team von Cyber Security Experten. Es operiert in vier Phasen: Monitoring, Analyse, Abwehr, Prävention. Die Aufgabe des SOC ist es, die gesamte IT-Infrastruktur zu überwachen und Cyberbedrohungen in Echtzeit zu erkennen.

Sobald eine Bedrohung erkannt wurde, reagiert das Team sofort und setzt umgehend Lösungsvorschläge auf. Die Grundlage für ein SOC ist ein SIEM (=Security Information and Event Management). Im Gegensatz zu vielen Konkurrenzlösungen werden die Lösungsvorschläge im SOC von Barracuda Managed SKOUT von echten Menschen erarbeitet und basieren nicht nur auf einer KI.

WAS IST XDR?

XDR steht für Extended Visibility Detection Response. Schon der Name zeigt, was XDR kann: „Extended Visibility“ bedeutet eine größere Sichtbarkeit, „Detection“ heißt mögliche Bedrohungen werden schneller als üblich in allen Netzwerkebenen erkannt und mit „Response“ ist eine schnelle Reaktionszeit gemeint. Es handelt sich dabei um ein SaaS-basiertes Tool, das verschiedene Sicherheitsprodukte in ein Gesamtsystem integriert. Dabei kann es flexibel auf bereits vorhandener Infrastruktur aufbauen.

Es gibt zahlreiche Vorteile beim Einsatz von XDR. So werden etwa viel mehr Daten als nur beim SIEM überwacht. XDR kann zusätzlich Clouds, E-Mails und SaaS-Lösungen überwachen. Es erfasst Daten ganzheitlich und bewertet sie über mehrere kritische Ebenen hinweg. Bei der Bewertung werden künstliche Intelligenzen eingesetzt, um Warnungen nach Priorität zu verdichten und so gezielte Reaktionen zu ermöglichen.

LEISTUNGEN DES BARRACUDA SKOUT MANAGED XDR

Mit Barracuda SKOUT Managed XDR holen sie sich eine höchst effiziente und flexible Lösung ins Haus, die zu 100% zu Ihren Kunden passt. Als MSP müssen Sie Ihren Kunden eine Lösung bieten, die zu ihm passt und nicht umgekehrt. Unser XDR ist unabhängig von Herstellern. Es ist deshalb nicht notwendig, von Unternehmen zu verlangen, bestimmte Anwendungen oder Dienste zu nutzen, um XDR einzusetzen.

XDR-PLATTFORM

Unsere Plattform bündelt die notwendigen Tools zu einem Gesamtsystem. So werden Kosten für das Konfigurieren und Verwalten von Sicherheitsprodukten reduziert.

SOC

Barracuda bietet einen der ausgereiftesten SOC-Services. Unser SOC operiert rund um die Uhr, 7 Tage die Woche und 365 Tage im Jahr. Dabei werden enorme Volumen an Daten KI-gestützt aufbereitet und von Experten analysiert und interpretiert.

ADVANCED CYBERTHREAT PREVENTION & DETECTION

Integrieren Sie die XDR Plattform mit weiteren Lösungen, um Zero-Day- und Ransomware-Angriffe aufzudecken und zu bekämpfen.

SIEM-ANALYSE

Unsere Analytiker gleichen Millionen von Datenpunkten miteinander ab, um jegliche Anomalien in den Systemen von Kunden aufzudecken.

EINFACHSTE EINRICHTUNG

Ihre Kunden richten Sie schnell und remote ein. Dafür nutzen Sie unser Self-Service oder den 24h-Support. Ihre Kunden können problemlos weiterarbeiten, während Sie im Hintergrund Bedrohungen verhindern und aufdecken.

REPORTING

Unsere maximale Flexibilität findet sich auch im Reporting wieder. Erstellen Sie benutzerdefinierte Berichte, um Ihren Kunden anhand von leicht lesbaren PDFs oder XLXS-Formaten zu demonstrieren, wie diese durch die Zusammenarbeit profitieren können.

DASHBOARD

Unser mandantenfähiges Dashboard bietet MSPs die Möglichkeit, alle Kunden anhand einer einzigen Ansicht im Überblick zu halten.

RESSOURCEN SPAREN

Mit dem Einsatz von Barracuda SKOUT Managed XDR sind Sie nicht nur auf dem neuesten Stand in Sachen Cybertechnologie, sondern sparen auch wertvolle Ressourcen.

Unser XDR integriert Cybersecurity-as-a-Service Lösungen flexibel und effizient. So sparen Sie sich Koordinationsaufwand und Ausgaben für zusätzliche Tools. Sie können unser Service wirklich jedem Kunden anbieten, da unser XDR unabhängig von Herstellern arbeitet.

Durch unser SOC wird es überflüssig, zusätzliches Personal aufzubauen. Sie müssen nicht mehr in Training und Neuanstellungen von Technikern investieren.

Die Reaktionszeit auf Cyberbedrohungen und -angriffe wird auf ein Minimum verkürzt. Schäden für das Unternehmen und daraus resultierende Zeit- und Geldaufwände werden so effektiv reduziert.

KI-gestützte Verfahren reduzieren die Arbeitslast enorm und erlauben die zuverlässige Analyse von sehr großen Datenmengen ohne Zusatzkosten.

Wer auf SOC-Lösungen setzt, erhält bei Cyberrisk-Versicherungen deutlich bessere Konditionen.

Sie erhalten von uns für jeden Alarm Berichterstattung und Runbooks bereitgestellt.

BIETEN SIE IHREN KUNDEN DEN OPTIMALEM CYBERSCHUTZ

DAS WICHTIGSTE IM SECURITY BUSINESS IST DIE CYBER HYGIENE.

Nur gepflegte Systeme überdauern auch groß angelegte Angriffsversuche. Dafür reicht kein punktueller Schutz, es gilt die Gesamtheit der Infrastruktur zu überwachen. Das sieht auch der Gesetzgeber so. Das IT-Sicherheitsgesetz verpflichtet Betreiber von kritischer Infrastruktur ab 01.05.2023 Sicherheitssysteme zur Erkennung von Cyberangriffen auf den neuesten Stand der Technik zu bringen. Je früher Unternehmen darauf vorbereitet sind, desto besser.

WIR FREUEN UNS, IHNEN DIESEN SERVICE IN EINER DEMO ODER TESTVERSION ZU ZEIGEN.

JETZT DEMO VEREINBAREN

JETZT TRIAL STARTEN