eBOOK

www.security-insider.de

SECURITY INSIDER

Security Operations Center für den Mittelstand

Cortex XDR: das Security Operations Center aus der Cloud, professionelle Hilfe für kleine Security-Teams

Powered by:

paloalto NETWORKS®

DTS Systeme

Inhalt

Powered by:

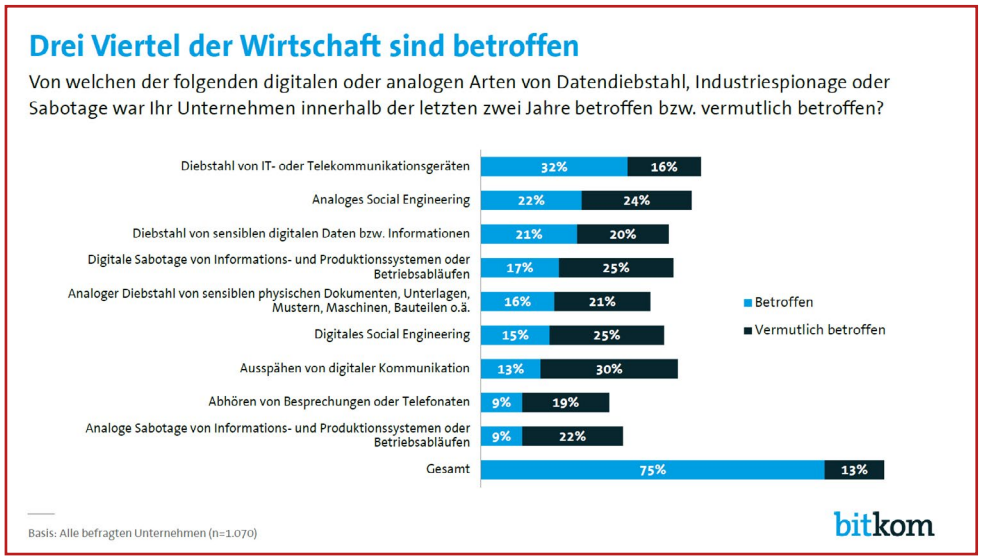
paloalto NETWORKS

Palo Alto Networks
Rosenheimer Str. 143c, 81671 München
E-Mail contact_salesEMEA@paloaltonetworks.com
Web https://www.paloaltonetworks.de

Vogel IT-Medien GmbH
Max-Josef-Metzger-Str. 21
86157 Augsburg
Telefon +49 (0) 821/2177-0
E-Mail redaktion@security-insider.de
Web www.Security-Insider.de
Geschäftsführer: Werner Nieberle
Chefredakteur: Peter Schmitz, V.i.S.d.P., peter.schmitz@vogel-it.de
Erscheinungstermin: Januar 2020
Titel: d1sk/stock.adobe.com

Der Mittelstand im Fadenkreuz der Cyber-Attacken

Nicht nur Konzerne und Großunternehmen sind den Bedrohungen durch Hacker und Internetkriminelle ausgesetzt. Der Mittelstand in Deutschland gilt als Know-how-Träger der Wirtschaft, das wissen auch die Angreifer. Doch während große Unternehmen ihr eigenes Security Operations Center (SOC) betreiben können, um Angriffe besser zu erkennen und abzuwehren, haben die Unternehmen im Mittelstand bisher kaum die Chance, ein eigenes SOC aufzubauen. Das muss sich ändern.



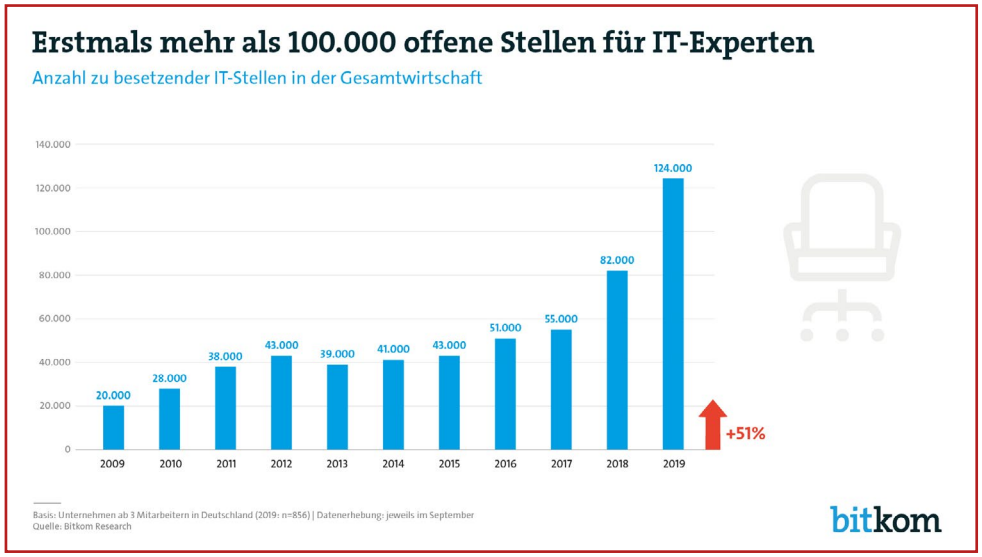
3 von 4 Unternehmen in Deutschland wurden bereits Opfer von Sabotage, Datendiebstahl oder Spionage. Besonders gefährdet ist der Mittelstand. (Bild: Bitkom)

Der Mittelstand ist vielen Attacken ausgesetzt

„Gerade der Mittelstand als Rückgrat unserer Wirtschaft und vielfacher Innovationstreiber ist im Visier von Cyber-Angreifern", erklärt Arne Schönbohm, Präsident des BSI (Bundesamt für Sicherheit in der Informationstechnik). „Viele KMU benötigen Unterstützung bei der Planung und Umsetzung von Maßnahmen der Prävention, Detektion und Reaktion", so Arne Schönbohm weiter.

Das erhöhte Risiko für den Mittelstand sollte nicht nur als Warnung verstanden werden. Die Cyber-Attacken auf die Unternehmen in Deutschland finden Tag für Tag statt. Durch Sabotage, Datendiebstahl oder Spionage entsteht der deutschen Wirtschaft jährlich ein Gesamtschaden von 102,9 Milliarden Euro, wie eine Umfrage des Digitalverbandes Bitkom Ende 2019 ergab. Der Schaden ist damit fast doppelt so hoch wie noch vor zwei Jahren. Drei Viertel der Unternehmen waren in den vergangen beiden Jahren von Angriffen betroffen, weitere 13 Prozent vermuten dies.

Für die Zukunft prognostiziert eine breite Mehrheit der Unternehmen eine weitere Verschärfung der Sicherheitslage. 82 Prozent gehen davon aus, dass die Zahl der Cyber-Attacken auf ihr Unternehmen in den nächsten zwei Jahren zunehmen wird.



Die Zahl der offenen Stellen für IT-Fachkräfte erreicht eine neue Rekordmarke. Der Fachkräftemangel in der Security trifft den Mittelstand hart. (Bild: Bitkom)

Der Fachkräftemangel ist im Mittelstand besonders spürbar

Nicht nur die Zahl der Cyber-Angriffe und der wirtschaftliche Schaden dadurch sind weiter gestiegen. Auch die Zahl der offenen Stellen für IT-Fachkräfte hat eine neue Rekordmarke erreicht, wie der Digitalverband Bitkom ebenfalls berichtet. In Deutschland gibt es aktuell 124.000 offene Stellen für IT-Spezialisten. Das entspricht einem Anstieg um 51 Prozent verglichen mit dem Vorjahr. Innerhalb von zwei Jahren hat sich damit die Zahl der unbesetzten IT-Stellen mehr als verdoppelt.

Laut dem Marktforschungsinstitut Gartner ist gerade der Security-Fachkräftemangel ein beständiges Problem, das regelmäßig dazu führt, dass Sicherheitstechnologien nicht effektiv ausgerollt werden können. Die Analysten erwarten, dass die Anzahl unbesetzter Stellen in der IT-Sicherheit bis Ende 2020 weltweit auf 1,5 Millionen steigen wird.

Unternehmen aus dem Mittelstand haben besondere Probleme damit, geeignete Security-Experten zu finden und dann langfristig an sich zu binden. Großunternehmen werden von Bewerbern häufig bevorzugt, da man dort höhere Gehälter und Budgets sowie spannendere Aufgaben erwartet.

Security-Lösungen sind häufig Insellösungen

Eine weitere Herausforderung für die Cyber-Sicherheit im Mittelstand kommt noch hinzu: Die Cyber-Attacken sind inzwischen sehr professionell und komplex und erfolgen auf verschiedenen Angriffswegen zeitgleich oder zeitversetzt. Die Security-Maßnahmen im Mittelstand sind aber oftmals nicht aufeinander abgestimmt. Viele Unternehmen setzen eine Vielzahl verschiedener Security-Werkzeuge parallel ein, die weitgehend nicht integriert sind, sondern Insellösungen bilden. Anzeichen für Angriffe, die eine Security-Lösung wahrnimmt, werden nicht an die anderen Abwehrlösungen übermittelt.

So gibt es häufig Einzellösungen für Endpoint Detection and Response (EDR), Network Traffic Analysis (NTA)

und User and Entity Behavior Analytics (UEBA), anstatt diese zu integrieren. Um die Cyber-Attacken jedoch schneller und besser erkennen und abwehren zu können und um die richtigen, präventiven Maßnahmen zu ergreifen, müssen die verschiedenen Security-Lösungen zusammen arbeiten, Daten austauschen, in einen Workflow eingebunden werden und wie aus einer Hand priorisiert, gesteuert und automatisiert werden können.

Stattdessen leiden gerade Unternehmen aus dem Mittelstand unter komplizierten Security-Prozessen und mangelnder Abstimmung zwischen den Security-Maßnahmen bei gleichzeitig knappen Personal-Ressourcen und Budgets in der Security. Cyber-Angreifer haben deshalb oftmals leichteres Spiel, wenn sie ein kleines oder mittleres Unternehmen angreifen.

Security-Teams sind überlastet

Komplexe Cyber-Angriffe, kleine Team-Größen und die Vielzahl an Insellösungen führen dazu, dass sich die Security-Mannschaft in einem mittelständischen Unternehmen häufig überfordert fühlt. Die Zahl der Security-Warnungen der verschiedenen IT-Sicherheitslösungen wächst und wächst, Verbindungen zwischen den Warnungen lassen sich nicht ohne weiteres feststellen. Es ist vielfach nicht möglich, wichtige von unwichtigen Warnungen zu unterscheiden und die Warnungen manuell miteinander in Verbindung zu bringen, geschweige denn, allen relevanten Security-Alerts nachzugehen.

Als Folge davon entsteht in den Security-Teams eine Ermüdung gegenüber den zahlreichen Alerts, man beginnt damit, diese als gegeben zu akzeptieren und nicht weiter zu verfolgen. Man spricht von einer „Alert Fatigue“. Anzeichen für Angriffe in den verschiedenen Alerts werden nicht mehr entdeckt, denn die Zusammenhänge müssten in den einzelnen Security-Lösungen händisch gesucht werden – ein Aufwand, der nicht erbracht werden kann.

Die Folgen für die Cyber-Security im deutschen Mittelstand sind hochriskant: Es bestehen Lücken in der Angriffserkennung, das Aufdecken von Attacken dauert zu lange, die Security-Teams sind überlastet und unzufrieden, denn trotz ihrer großen Bemühungen haben die Cyber-Angreifer immer häufiger Erfolg.

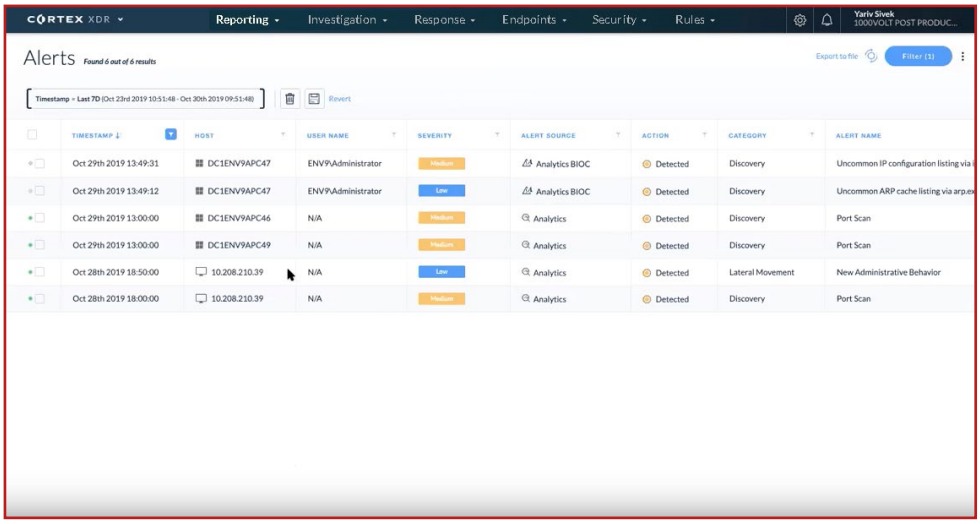
Ein Security Operations Center könnte helfen, aber …

Großunternehmen haben oftmals eine Antwort auf die beschriebenen Probleme des Mittelstands, sie betreiben ein SOC (Security Operations Center), um Security-Wissen, Tools und Prozesse zu bündeln. Doch kleine und mittlere Unternehmen schaffen es bisher nicht, ein SOC für sich aufzubauen, denn die Rekrutierung von SOC-Analysten und Cyber-Sicherheitsexperten ist eine echte Herausforderung, gerade für den Mittelstand. Zudem bindet der Aufbau und Betrieb eines SOC erhebliche Investitionen, die ein Unternehmen aus dem Mittelstand kaum leisten kann.

Deshalb müssen neue Wege in der Cyber Security gefunden und beschritten werden.

Die Alternative zum eigenen Security Operations Center

Unternehmen aus dem Mittelstand können auch dann ihre Herausforderungen in der Cyber-Security meistern, wenn sie kein eigenes Security Operations Center betreiben. Möglich wird dies mit Cortex XDR. Damit erhalten kleine und mittlere Unternehmen die Vorteile eines SOC, ohne ein eigenes Security Operations Center zu haben.



Cortex XDR von Palo Alto Networks wertet Security-Warnungen eigener IT-Sicherheitsfunktionen und von Drittlösungen aus und bietet den Kontext zur besseren Bewertung des bestehenden Risikos und möglicher Angriffe. (Bild: Palo Alto Networks)

Welche Funktionen der Mittelstand braucht

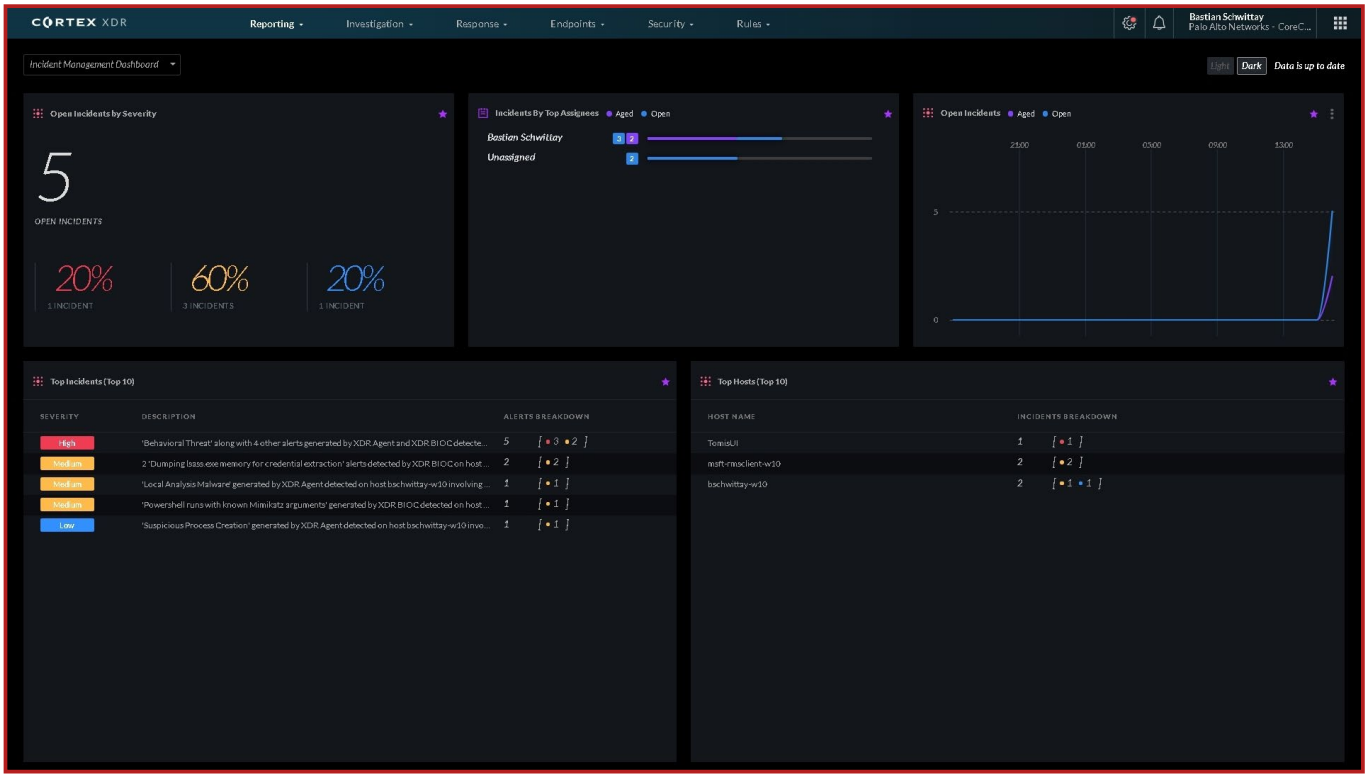
Unternehmen aus dem Mittelstand brauchen kein eigenes SOC, sondern die Funktionen und Vorzüge, die ein SOC bieten kann:

- Insellösungen in der Security müssen ersetzt und Datensilos aufgebrochen werden, damit Angriffe systemübergreifend erkannt und abgewehrt werden können.
- Die komplette IT-Infrastruktur mit allen genutzten Endgeräten und Cloud-Diensten muss überwacht und geschützt werden.
- Relevante Sicherheitswarnungen aus anderen Security-Lösungen müssen importiert und zusammen mit den eigenen Alerts ausgewertet werden.
- Security-Alerts müssen bewertet und priorisiert werden, damit die tatsächlichen Risiken minimiert werden können.
- Die Security muss in eine aktive Rolle gebracht werden, hin zum „Jäger", heraus aus der reinen Verteidigerrolle.

Was Cortex XDR leisten kann

Cortex XDR von Palo Alto Networks ist eine Alternative zum eigenen SOC und übernimmt die Optimierung der Security-Prozesse, gerade für Unternehmen aus dem Mittelstand:

- Cortex XDR bricht die Datensilos auf, die Sicherheitssysteme voneinander

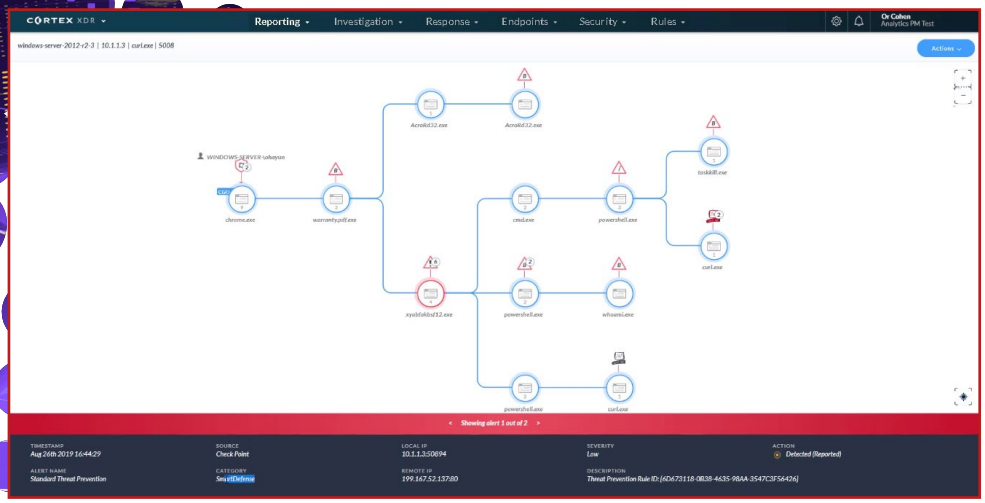


Security-Ereignisse werden bewertet und priorisiert, sodass sich das Security-Team auf die echten Risiken konzentrieren kann. (Bild: Palo Alto Networks)

isolieren und Incident-Response-Prozesse ausbremsen. Dies geschieht mithilfe nativer, auf maschinellem Lernen basierender Funktionen für die Zusammenführung und Analyse von detaillierten Netzwerk-, Endpunkt- und Cloud-Daten. Auf diese Weise unterstützt Cortex XDR die Optimierung sämtlicher Sicherheitsprozesse.

- Mit Cortex XDR können Bedrohungen in allen Netzwerk-, Endpunkt- und Cloud-Ressourcen erkannt und abgewehrt werden. Alle sicherheitsrelevanten Daten werden in Cortex Data Lake, einem skalierbaren, cloudbasierten Daten-Repository, gespeichert, um die Einschränkungen der lokalen Protokollspeicherung zu vermeiden.
- Auch Alerts der Lösungen von Drittanbietern können in den Cortex Data Lake einfließen und werden bei den Analysen automatisch einbezogen und ausgewertet.
- Die Daten aus den verschiedenen Quellen werden zusammengeführt, abgeglichen und analysiert. Mithilfe von maschinellem Lernen werden Anomalien identifiziert, die auf bisher unerkannte Angriffe hinweisen. Die Ursachen, der bisherige Verlauf und der Kontext werden automatisch ermittelt und zusammengetragen, damit die Mitarbeiter des Sicherheitsteams das potenzielle Risiko genau einschätzen können.
- Des Weiteren erhalten Sicherheitsteams eine Funktion zur proaktiven Suche (Hunting) nach verborgenen Bedrohungen und die Möglichkeit zur Erstellung eigener Regeln, sodass die

gewonnenen Erkenntnisse für künftige Untersuchungen und zur Aufdeckung ähnlicher Bedrohungen genutzt werden können.



Angriffe lassen sich systemübergreifend nachvollziehen, digitale Spuren in den richtigen Zusammenhang bringen. (Bild: Palo Alto Networks)

- Cortex XDR bietet alle Funktionen traditioneller Produkte für Endpoint Detection and Response (EDR), Network Traffic Analysis (NTA) und User and Entity Behavior Analytics (UEBA). Da Cortex XDR standardmäßig Traps-Endpunktschutz-Agents enthält, erhält man außerdem einen Endpunktschutz.
- Cortex XDR spart nicht nur Geld durch Konsolidierung, sondern verbessert auch die IT-Effizienz, indem Daten dynamisch zusammengefügt werden, was zu schnelleren und besseren Untersuchungen führt. Das Sicherheitsteam kann von Funktionen wie der Ursachenanalyse von Vorfällen, Ein-Klick-Untersuchungen von Warnmeldungen und Arbeitsabläufen zur Vorfallverwaltung (Case Management) profitieren.

Funktionen, die selbst SOC-Analysten vermissen

Mittelständische Unternehmen haben mit Cortex XDR Sicherheitsfunktionen zur Hand, die selbst SOC-Analysten oftmals noch vermissen müssen. Demisto, ein Unternehmen von Palo Alto Networks, gibt mit einem Report Einblicke zum Status von SOAR (Security Orchestration, Automation and Response).

Der Bericht zeigt, dass Sicherheitsanalysten auf breiter Front mehr Automatisierung in Security-Operation-Centern fordern, da sie weiterhin zu viel Zeit damit verbringen, manuell Regeln zu aktualisieren und Warnungen zu verwalten.

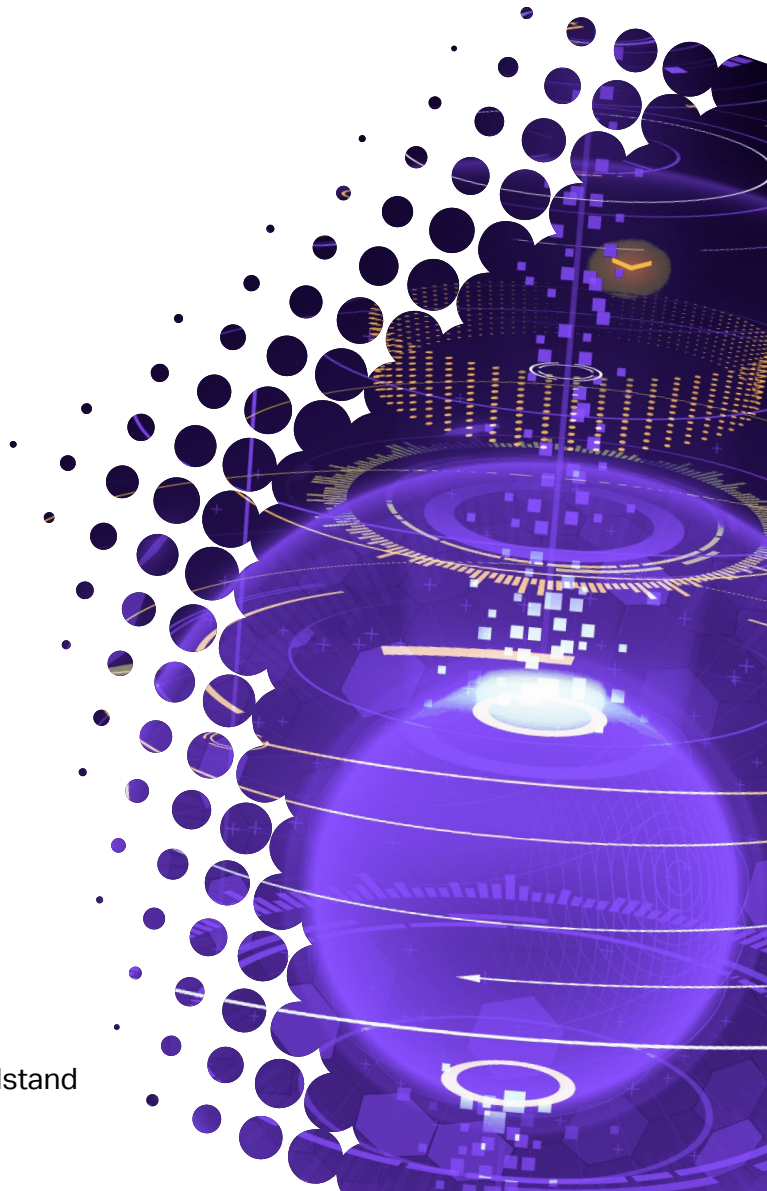
Zu den wichtigsten Ergebnissen des Reports gehören:

- Notwendigkeit einer Automatisierung mit aktualisierten Regeln und Überprüfungen nach einem Vorfall: Nahezu 60,5 Prozent der Befragten aktualisieren manuell Regeln von punktuellen Sicherheitsprodukten und verdeutlichen damit eine potenzielle Zeitersparnis. Bei vielen Sicherheitsprodukten ist die Automatisierung immer noch nicht erfolgreich umgesetzt. Mehr als 60 Prozent der Befragten wünschten sich Tools, die automatisch Informationen für die Überprüfung nach einem Sicherheitsvorfall erfassen.
- Notwendigkeit von maschinellem Lernen zur Verbesserung der Sicherheitsabläufe: Rund 61 Prozent der Befragten

wünschen sich Empfehlungen auf Basis von maschinellem Lernen zur Verbesserung der Sicherheitsabläufe. Nur 30 Prozent der Befragten gaben an, dass diese Funktion bereits in ihren Sicherheitsprodukten enthalten sei.

- Fortschritte bei automatisierten Playbooks (Praxisanleitungen, „Security-Kochbücher"): Nur 52 Prozent der Befragten gaben an, entweder automatisierte Playbooks oder eine Kombination aus automatisierten und manuellen Playbooks für die Implementierung von Incident-Response-Prozessen zu verwenden.

Damit sind Unternehmen aus dem Mittelstand dank Cortex XDR bei ihrer Security mit großen Unternehmen gleichauf, teils sogar überlegen.



Wie Cortex XDR dem Mittelstand helfen kann

Cortex XDR deckt automatisiert Angriffe auf und wendet maschinelles Lernen auf Netzwerk-, Endpunkt- und Cloud-Daten an. Cortex XDR deckt bekannte und unbekannte Schadsoftware auf, indem Angriffsverhalten und ungewöhnliche Aktivitäten erkannt werden. Cortex XDR erkennt die ungewöhnlichen Aktivitäten der Angreifer, noch während sie sich im Netzwerk bewegen und nach wertvollen Daten suchen.

Die Vorteile von Cortex XDR (Bild: Palo Alto Networks)

Entlastung für das Sicherheitsteam

Auch ein kleines Sicherheitsteam kann Bedrohungen schnell beseitigen, wenn es sie sofort von der Cortex XDR-Konsole aus eindämmt. Cortex XDR zeigt automatisch die Abfolge von Ereignissen, die mit der Bedrohung verbunden sind, und ermöglicht es so auch weniger erfahrenen Security-Mitarbeitern, einen Vorfall schnell zu untersuchen.

Cortex XDR ermöglicht:

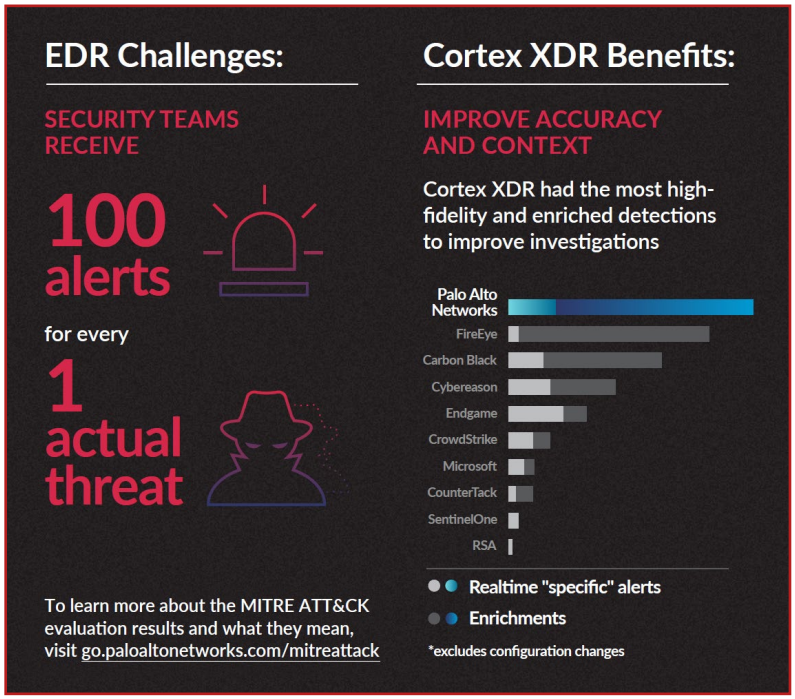
- Automatisches Erkennen komplexer Angriffe durch Analyse von Netzwerk-, Endpunkt- und Cloud-Daten
- Vereinfachen von Untersuchungen mit automatisierter Ursachenanalyse und Timeline-Analyse
- Optimieren der Bedrohungssuche mit leistungsstarken Suchfunktionen für Verhaltensbedrohungen

Unternehmen, die Cortex XDR einsetzen, automatisieren dadurch die Bedrohungserkennung und beschleunigen die Untersuchung von Cyber-Vorfällen:

- Die auf maschinellem Lernen basierende Lösung nutzt detaillierte Daten- und

Verhaltensanalysen sowie individuell anpassbare Erkennungsregeln, um Malware-Infektionen, gezielte Angriffe und Insider-Bedrohungen aufzudecken. Dadurch werden Bedrohungen mit hoher Genauigkeit automatisch erkannt, sodass sich Sicherheitsteams auf die Aufgaben konzentrieren können, die unbedingt manuell erledigt werden müssen.

- Wenn ein Alarm ausgelöst wird, kann das Security-Team mit einigen Klicks die Ursache und den Verlauf des Sicherheitsvorfalls ermitteln. Dank der bereitgestellten Kontextinformationen zu den Aktivitäten im Netzwerk, auf den Endpunkten und in der Cloud gestaltet sich die Analyse der Ereignisse erheblich einfacher. Dadurch wird das Team entlastet und die Untersuchung insgesamt beschleunigt.



Cortex XDR ist führend in der Erkennung von tatsächlichen Angriffen bzw. False Positives und entlastet dadurch das Security-Team erheblich. (Bild: Palo Alto Networks)

Schnelle Bereitstellung statt langwierigem SOC-Aufbau

Auch bei der Bereitstellung der neuen Security-Funktionen haben die Unternehmen einen Zeitvorteil dank Cortex XDR: Da es sich bei Cortex XDR um eine cloudbasierte App handelt, gestalten sich die Einrichtung, Verwaltung und Skalierung sehr viel einfacher als bei On-Premises-Lösungen.

Als Datengrundlage für Cortex XDR fungiert der Cortex Data Lake, eine Umgebung, in der große Volumen an Netzwerk-, Endpunkt- und Cloud-Daten für Verhaltensanalysen vorgehalten werden können.

Es zeigt sich: Cortex XDR ist für Unternehmen aus dem Mittelstand eine Alternative für ein eigenes SOC. Es erkennt automatisiert Bedrohungen und leitet die Abwehr ein, optimiert die Security-Prozesse, verkürzt die Zeit der Angriffserkennung und Abwehr, entlastet das Security-Team und senkt die Ausgaben für Security im Vergleich zu den zahlreichen Einzellösungen und Datensilos.

Urgestein und Vorreiter in der Cloud und IT-Sicherheit

DTS Systeme steht als erfolgreicher IT-Dienstleister seit über 35 Jahren deutschland- und europaweit für Innovation, Kompetenz sowie Leidenschaft.

Hinter dem Namen steht eine Technik Company, bestehend aus den 3 Kernbereichen Datacenter, Technologies und Security. Über 300 Mitarbeitende an 13 Standorten stellen mit zwei eigenen deutschen Rechenzentren ganzheitliche Lösungen und Services zur Verfügung, rund um die Uhr an 365 Tagen.
Wir sind sowohl Urgestein als auch Vorreiter in der Cloud und IT-Sicherheit. Mit unserem hybriden Baukastenkonzept und der Managed Multicloud entwickeln wir Made in Germany Know-how in der Wolke. Zudem haben wir uns als IT-Security-Hersteller, Security Operations Center und Managed Services Experten etabliert.

Auf der Datenbasis von Cortex XDR

Wir unterstützen unsere Kunden als Security Service Provider indem wir ihre Sicherheitsplattform kontinuierlich weiterentwickeln. Dies beinhaltet z. B. den Betrieb von Plattformen, Health Checks und Managed Detection & Response Services auf der Datenbasis von Cortex XDR durch unser eigenes Security Operations Center. Unser hochqualifiziertes, deutsch- und englischsprachiges Expertenteam ist 24/7 für Sie im Einsatz. Sie sparen wertvolle Zeit und Ressourcen, können sich auf die wesentlichen Geschäftsprozesse im betrieblichen Ablauf konzentrieren und profitieren von der langjährigen Erfahrung der DTS.
Cortex XDR eignet sich ideal für alle Unternehmen, die sich gegen zielgerichtete und komplexe Security-Bedrohungen schützen wollen. Wir ermöglichen Ihnen genau das und noch mehr.
Potenziale optimal nutzen, sämtliche Anforderungen erfüllen, kundenindividuelle Services – das ist die DTS Systeme.

Kontaktinformationen

DTS Systeme GmbH
Schrewestraße 2
32051 Herford

Telefon +49 5221 1013-000
Web www.dts.de

DTS Systeme