SICHERHEIT NEU DEFINIERT MIT XDR

Die Bedrohungserkennung und -abwehr nur am Endpunkt greift zu kurz

Einleitung

Jedes Sicherheitsteam hat das Ziel, die Infrastruktur und die Daten seines Unternehmens vor Schäden, unbefugtem Zugriff und Missbrauch zu schützen. Dazu wird in der Regel ein mehrschichtiger Ansatz verfolgt. Da Hackerangriffe stärker automatisiert und komplexer geworden sind, setzen auch die Produkte zur Erkennung und Reaktion auf mehrschichtige Transparenz, etwa bei der Erkennung und Abwehr von Bedrohungen (Endpoint Detection and Response, EDR), der Analyse des Netzwerkverkehrs (Network Traffic Analysis, NTA) und bei SIEM-Lösungen.

Der Zugewinn an Transparenz wird allerdings mit einem hohen Aufwand an Zeit und Know-how erkauft. Unterschiedliche Erkennungs- und Abwehrprodukte geben immer mehr Benachrichtigungen aus, was zusätzliches Fachwissen erfordert und die Sicherheitsteams an den Rand ihrer Leistungsgrenze bringt: ein endloser Strom von Ereignissen, immer mehr Tools und immer längere Erkennungszeiten. Gleichzeitig steigen die Kosten immens an. Wir reagieren nur noch und geraten dadurch immer weiter ins Hintertreffen.

Viele Unternehmen wie Ihres stellen sich dieselbe drängende Frage: Wie gelingt der Wechsel vom Reagieren auf eingehende

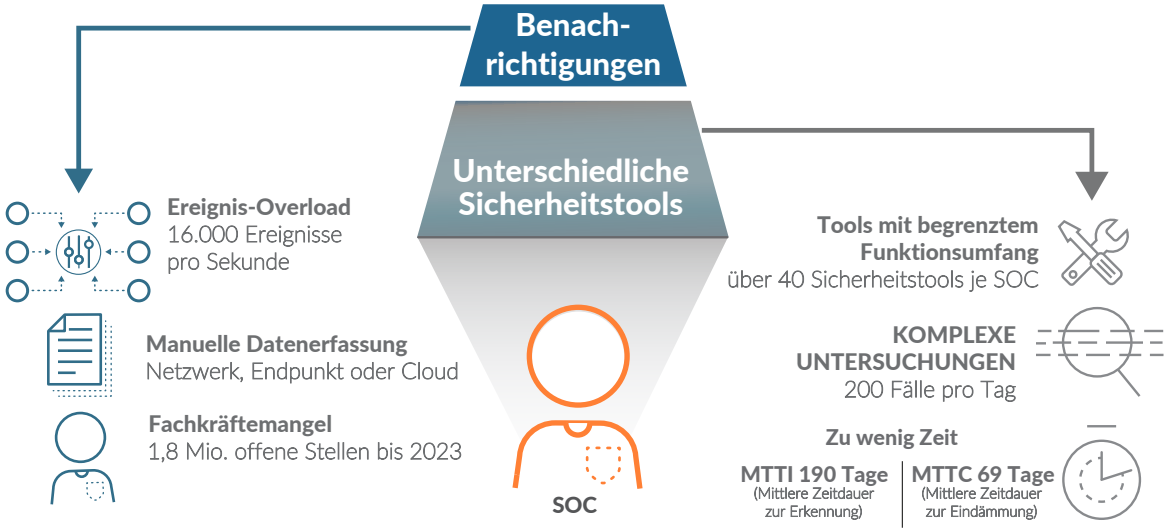


Abbildung 1: Netzwerk, Endpunkt oder Cloud

Benachrichtigungen hin zu einer aktiven Threat Prevention?

Es ist Zeit für eine neue Herangehensweise, die das Sicherheitsteam unterstützt anstatt es zu belasten, die Abläufe vereinfacht und eine schnelle Erkennung und Bekämpfung selbst der ausgefeiltesten Bedrohungen in der gesamten IT-Umgebung ermöglicht.

Konventioneller Ansatz: Beim Lösen eines Problems entstehen mehrere neue

Sicherheitsteams arbeiten hart, um ihr Unternehmen zu schützen, können Datendiebstähle aber nur mit Mühe verhindern. Die fünf größten Herausforderungen sind dabei:

- Zu viele Ereignisse
- Zu wenige Sicherheitsfachkräfte
- Begrenzter Funktionsumfang der Tools
- Fehlende Integration
- Zu wenig Zeit

Abbildung 2: Die fünf größten Herausforderungen für SOC-Teams

Sehen wir uns die einzelnen Problembereiche näher an:

1. Zu viele Ereignisse

Sicherheitsanalysten bekommen viel mehr Ereignisse gemeldet als sie effektiv bearbeiten können. Bei 55 Prozent der Sicherheitsteams oder Security Operations Center (SOC) gehen täglich durchschnittlich über 10.000 Ereignisse ein.[1] Diese sind jedoch nicht alle gleichwertig: Die meisten müssen nach Priorität eingestuft, abgeglichen oder normiert und zum Benachrichtigungspool hinzugefügt werden. Auch wenn das SOC-Team diese Datenflut mithilfe von SIEM durchkämmt, ist es weiterhin erforderlich, manuell Daten zu sammeln, Analysen durchzuführen und Falschmeldungen auszusortieren – und das möglichst schnell, damit Zeit für die wirklich kritischen Benachrichtigungen bleibt. Allzu oft passiert es dabei, dass die Wachsamkeit nachlässt (Stichwort „Warnungsmüdigkeit“) und wichtige Benachrichtigungen in der Datenflut übersehen werden. Aufgrund des hohen Aufkommens übersehen 54 Prozent der Sicherheitsexperten mitunter Benachrichtigungen, die sie untersuchen müssten.[2]

2. Fachkräftemangel

Viele Unternehmen würden der steigenden Arbeitsbelastung gern durch Neueinstellungen begegnen, aber es besteht bereits heute ein weltweiter Mangel an geschulten Sicherheitsfachkräften, der laut Vorhersagen von Analysten bis 2022 auf 1,8 Millionen ansteigen wird.[3] Besonders Fachleute mit Kenntnissen im Bereich Netzwerk- oder/und Endpunktforensik sind rar. Sicherheitsteams sind daher mit der Priorisierung und Untersuchung von Benachrichtigungen und der Gefahrenabwehr hoffnungslos überlastet. Sie verbringen übermäßig viel Zeit mit mühevoller Kleinarbeit wie Datenerfassung, manueller Analyse und dem Einpflegen von Bedrohungsdaten. Selbst der Umstieg auf eine automatisierte Bearbeitung bringt zusätzliche Arbeit. Lernen und das Weitergeben von Informationen leiden darunter, weil Wissen und Beispielfälle isoliert bleiben und anderen Gruppen nicht zur Verfügung stehen.

Die Kombination aus zu vielen Benachrichtigungen, komplexen Untersuchungen und Personalknappheit führt zu menschlichem Versagen und löst einen Schneeballeffekt aus: Weil die erforderlichen Kontextinformationen fehlen, wird manchen Benachrichtigungen eine zu hohe oder zu niedrige Dringlichkeitsstufe zugewiesen. Das führt zu unnötiger Arbeit für das Untersuchungsteam, das dann möglicherweise Kollegen um Hilfe bitten muss, die eigentlich proaktiv nach Bedrohungen suchen sollten.

3. Zu viele Tools mit zu geringem Funktionsumfang

Eine Lösung zur Bewältigung solcher Herausforderungen ist die Anschaffung weiterer Tools, um schneller und besser informiert entscheiden zu können. Man kann aber auch zu viele Tools haben. Die meisten Sicherheits-Tools wurden entwickelt, um eine ganz bestimmte fehlende Funktion zu bieten. Die Einbettung in die Arbeitsumgebung wurde dabei meist nicht genügend berücksichtigt, sodass viele Tools ihre Nutzer nun eher daran hindern, sich einen ganzheitlichen Überblick zu verschaffen. Sie arbeiten isoliert voneinander, berücksichtigen nur Daten aus einer bestimmten Quelle und sind daher nur für wenige Fachleute nützlich, während sie andere eher noch überlasten.

Manche regelmäßig in der Erkennung und Abwehr eingesetzten Tools sind in ihrem Bereich durchaus von Wert:

- **EDR** kann die Untersuchungsdauer für erfahrene Incident-Response-Teams verkürzen, arbeitet jedoch nur mit Daten von Endpunkten, auf denen man einen Agenten installieren kann. EDR kann zudem das Benachrichtigungsaufkommen drastisch erhöhen. Darüber hinaus ist selbst die Automatisierung einfacher Aufgaben nur mithilfe individuell entwickelter Lösungen möglich und führt oft zu einer zusätzlichen Belastung für andere Teammitglieder.
- **NTA** erfordert die richtige Platzierung von Sensoren, um keine Datenströme zu übersehen, verfügt selten über Abwehrfunktionen und bezieht keine Endpunktdaten in die Erkennung von Anomalien oder Untersuchung von Bedrohungen mit ein.
- **UEBA** (User and Entity Behavior Analytics) konzentriert sich hauptsächlich auf Logdateien und lässt wichtige Details aus der Tiefenanalyse des Netzwerks außen vor, ganz zu schweigen von Endpunkten und der Cloud. Darüber hinaus generiert UEBA viele Fehlalarme, was die Analysten noch zusätzlich belastet.

Alle diese Tools verbessern die Transparenz, aber da sie neue Probleme mit sich bringen, sind Spezialkenntnisse erforderlich, um praktisch anwendbare Rückschlüsse aus den Ergebnissen zu ziehen.

4. Daten-Puzzle statt ganzheitlichem Überblick

Für die Erkennung komplexer Hackerangriffe müssen Daten aus den verschiedensten digitalen Quellen abgeglichen werden. Da die meisten Tools für die Erkennung und Abwehr von Bedrohungen nur Daten aus einer Quelle berücksichtigen, beispielsweise von einem Endpunkt, entgehen ihnen wichtige Hinweise aus anderen relevanten Quellen. Das mühevolle Zusammenpuzzeln der Bedrohungsanalyse überlassen sie dem Sicherheitsteam. Da im SOC eines typischen Großunternehmens über 40 unabhängig voneinander arbeitende Tools verwendet werden, erhalten die Analysten Daten oft „scheibchenweise“. So müssen sie von Bildschirm zu Bildschirm schalten und relevante Informationen zu einem Gesamtbild zusammensetzen, um echte Bedrohungen abwehren zu können. Würden die Daten zusammengeführt, ergäben sie ein ganzheitliches Bild der Umgebung – dafür müssten sie aber normalisiert und nach Datum, Uhrzeit und Ereignis abgeglichen werden. Außerdem wäre die Kenntnis der Untersuchungstechniken für verschiedene Bereiche wie Netzwerk und Endpunkte erforderlich.
Das ist nicht einfach und muss bis heute manuell erledigt werden.

1. „Survey: 27 Percent of IT professionals receive more than 1 million security alerts daily“, Imperva, 28. Mai 2018, https://www.imperva.com/blog/2018/05/27-percent-of-it-professionals-receive-more-than-1-million-security-alerts-daily/.
2. „2017: Security Operations Challenges, Priorities, and Strategies“, ESG, März 2017, http://resources.siemplify.co/hubfs/PDF%20Downloads/ESG-Research-Insights-Report-Siemplify.pdf?hsCtaTracking=4303efc5-9f7b-4a8a-9438-263c0588b898%7C6043fb9a-2881-4940-9a0e-6239a8686b81.
3. „2017 Global Information Security Workforce Study“, Frost & Sullivan, abgerufen am 8. Januar 2019, https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf.

5. Die Zeit arbeitet gegen uns

Der wichtigste Faktor von allen ist die Zeit. Je schneller eine Bedrohung identifiziert werden kann, desto größer ist die Chance, sie abzuwehren. Teams, die durch zu viele Ereignisse, zu wenige Mitarbeiter und fehlenden Datenabgleich überlastet sind, laufen Gefahr, unscheinbare Benachrichtigungen zu übersehen, die auf echte Gefahren hinweisen. Auch für die proaktive Suche nach unbekannten Bedrohungen bleibt oft zu wenig oder gar keine Zeit. Derzeit vergehen durchschnittlich 6 Monate zwischen dem Beginn einer Sicherheitsverletzung und ihrer Entdeckung,[4] Tendenz steigend. Die mittlere Dauer bis zur Erkennung eines Angriffs (Mean Time to Identify, MTTI) hat sich von 190 Tagen im Jahr 2017 auf 197 Tage im Jahr 2018 verlängert. Die mittlere Zeit von der Erkennung bis zur Eindämmung (Mean Time to Contain, MTTC) verlängerte sich zwischen 2017 und 2018 von 66 Tagen auf 69 Tage.[5]

Dies alles geschieht zu einer Zeit, in der sich Unternehmen EDR, NTA und UEBA anschaffen und ihr SIEM überarbeiten und in der fast 60 Prozent des IT-Budgets für Sicherheit ausgegeben werden.[6] Trotz dieser Tools verbringen Analysten noch einen großen Teil ihrer Zeit mit manuellen Tätigkeiten wie dem Schreiben von Abfragen, dem Abgleich von Benachrichtigungen mit Logdateieinträgen und dem Zusammentragen und in Beziehung setzen von Informationen aus unterschiedlichen Quellen. Aufgrund dieser ständigen Überlastung ist es kein Wunder, dass nur wenige Sicherheitsteams die Zeit für strategisch wichtige Aufgaben wie die Suche nach komplexen Bedrohungen, grundsätzliche Erwägungen und das Lösen kniffliger Sicherheitsprobleme haben, die auch mit raffinierten Programmen und Automatisierung nicht lösbar sind.

Ihr SOC hat etwas Besseres verdient

Ein SOC-Team braucht einen Ansatz, mit dem es diese Herausforderungen bewältigen kann. Dieser muss das Team in allen Stadien seiner Arbeit – Priorisierung von Benachrichtigungen, Untersuchung von Sicherheitsvorfällen und Suche nach Bedrohungen – unterstützen, damit es Bedrohungen aller Art rasch abwehren kann. Aus praktischer Sicht muss der ideale Ansatz folgende Anforderungen erfüllen:

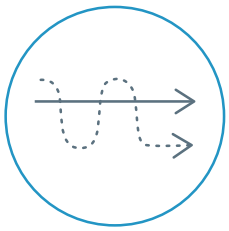
- Verfolgen aller Aktivitäten im gesamten Netzwerk, auf Endpunkten und in Clouds zur Erkennung, Priorisierung, Untersuchung und Abwehr von Bedrohungen.
- Integration der Tools, die Benachrichtigungen erzeugen oder Informationen bereitstellen, damit die Präsentation von Informationen, das Ziehen von Schlussfolgerungen und möglichst auch die Einleitung von Maßnahmen automatisch erfolgen können.
- Abgleich von Daten aus allen Quellen mithilfe umfangreicher Analysen, sodass auch gut getarnte Bedrohungen automatisch oder manuell aufgedeckt werden können, ohne dass zu viele Fehlalarme generiert werden.
- Vereinfachen von Untersuchungen, um weniger erfahrene Analysten zu unterstützen, erfahrene Fachkräfte zu entlasten und alle Analyseschritte im SOC erheblich zu beschleunigen.
- Rasche Weiternutzung von Erkenntnissen aus jeder Untersuchung für die Verbesserung der Abwehr, beispielsweise als Hintergrundinformation für zukünftige Untersuchungen, zur Verringerung der Zahl der Benachrichtigungen und zum Schließen neuer oder bekannter Sicherheitslücken.

Dadurch würde die mittlere Zeit bis zu Erkennung und Abwehr von Bedrohungen erheblich verkürzt, Sicherheitsteams kämen weg vom reinen Reagieren auf Benachrichtigungen und hin zum proaktiven Schutz des Netzwerks.

Eine neue Dimension der Erkennung und Abwehr mit XDR

Palo Alto Networks stellt einen bahnbrechenden neuen Ansatz für die IT-Sicherheit vor, der die Transparenz verbessert und die Aufdeckung, Untersuchung und Abwehr von Bedrohungen beschleunigt: XDR, ein Ansatz, der neue Maßstäbe für die Erkennung und Abwehr von Hackerangriffen setzt. Das „X“ steht dabei für beliebige Datenquellen, im Netzwerk, auf Endpunkten oder in einer Cloud. Zentrales Anliegen ist die drastische Steigerung der Produktivität von SOCs durch

Schnellere Bedrohungserkennung durch netzwerk-, cloud- und endpunktübergreifende Analysen



Einfachere Untersuchung und Abwehr bekannter und neuer Bedrohungen

Stärkere Sicherheit und größerer ROI der Sicherheitsinvestitionen

Abbildung 3 : Drei große Vorteile von XDR

4. „2018 Cost of a Data Breach Study“, Ponemon Institute, Mai 2018, https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=55017055USEN&.
5. Ebd.
6. „Infographic: 2018 IT budgets are up slightly; spending focus is on security, hardware, and cloud“, ZDNet, 2. Oktober 2017, https://www.zdnet.com/article/infographic-2018-it-budgets-are-up-slightly-spending-focus-is-on-security-hardware-and-cloud.

Automatisierung. Die Verknüpfung von Daten aus all diesen Quellen sorgt für umfassende Transparenz. Sicherheitsexperten können sich ein vollständiges Bild der Aktivitäten im Unternehmen machen, ohne die dazu erforderlichen Daten erst manuell zusammentragen und zueinander in Beziehung setzen zu müssen. Und Angreifer können sich nicht mehr verstecken. Auch Daten aus externen Quellen wie Sicherheitshinweisen und globalen Bedrohungsdaten werden dabei mit einbezogen. Die automatisierte Funktion führt wichtige Daten zusammen und wertet sie für die Sicherheitsteams aus – so liegen innerhalb weniger Sekunden Ergebnisse vor, für die hochqualifizierte Analysten sonst Stunden benötigen. Das vereinfacht die Untersuchungen im gesamten IT-Sicherheitsbereich und verkürzt die Zeit für die Erkennung und Suche nach allen Arten von Bedrohungen, ihre Untersuchung und die Einleitung von Gegenmaßnahmen. Mit XDR beginnt eine neue Ära der Heuristik, Analytik und Modellierung, dank künstlicher Intelligenz und maschinellen Lernens lassen sich selbst die raffiniertesten Angriffe zügig erkennen und abwehren. XDR wertet alle Quellen und Standorte der IT-Infrastruktur eines Unternehmens aus und kann dadurch die Eindämmung von Bedrohungen automatisieren, den Ablauf eines Angriffs rekonstruieren, diesen mit bekannten Bedrohungsdaten vergleichen und im Verlauf der Untersuchung aufgedeckte Sicherheitslücken schließen. Damit beschleunigt XDR die Behebung sicherheitsrelevanter Vorfälle und nimmt Analysten sehr aufwendige Tätigkeiten ab. Wichtiger Hinweis: Um die Bereitstellung zu vereinfachen, sollte XDR idealerweise als reine Cloudlösung genutzt werden.

Vorteile der Erkennung und Abwehr mit XDR

XDR arbeitet für das und mit dem SOC. Es bietet drei wesentliche Vorteile: konkurrenzlose Transparenz, vereinfachte Sicherheitsabläufe und einen deutlich höheren ROI für Sicherheitsinvestitionen.

Konkurrenzlose Transparenz: Getarnte Bedrohungen schneller finden

XDR entdeckt von der Norm abweichende Aktivitäten, indem es Angaben zum Anwenderverhalten, zu Ressourcen und Aktivitäten aus allen Datenquellen zueinander in Beziehung setzt. Es senkt die Komplexität der Bedrohungssuche durch leistungsstarke Suchfunktionen, belastbare Rückschlüsse auf mögliche Urheber und den Abgleich aller verfügbaren Daten. XDR automatisiert die Erkennung aktiver oder früherer Bedrohungen mithilfe von Big-Data-Analysen der Daten von Endpunkten, aus dem Netzwerk, aus diversen Clouds und aus externen Quellen und führt sie an einer zentralen Stelle für die SOC-Mitarbeiter zusammen.

Vereinfachte Sicherheitsabläufe bei Priorisierung, Untersuchung und Abwehr

XDR beschleunigt und vereinfacht Untersuchungen durch Visualisierung der Aktivitätskette für ein beliebiges Ereignis: Das macht automatisch die Ursachen sichtbar und liefert aussagekräftige forensische Details für alle Sicherheitsanalysten. Warnungsmüdigkeit ist kein Thema mehr, denn die Untersuchungsergebnisse werden mit allen Sicherheitsbenachrichtigungen verschiedener Tools abgeglichen, wodurch auch weniger erfahrene Analysten in kürzerer Zeit mehr leisten können. XDR reagiert auf aktive Bedrohungen und vereitelt zukünftige Angriffe durch die koordinierte Durchsetzung von Maßnahmen im Netzwerk und auf den Endpunkten. Das nimmt den Teammitgliedern manuelle Analysen ab und gibt ihnen mehr Zeit für die Bedrohungserkennung.

Erheblich höhere Rendite der Sicherheitsinvestitionen

XDR vervielfacht die Leistungsfähigkeit des Teams für Sicherheitsanalysen, strafft Arbeitsabläufe, verkürzt und vereinfacht die Priorisierung von Ereignissen, die Untersuchung von Sicherheitsvorfällen, die Abwehr und die proaktive Suche. Es ermöglicht die Zusammenarbeit unterschiedlicher Sicherheitstools zur automatischen Reaktion auf Probleme unter Berücksichtigung verschiedenster interner und externer Daten und Bedrohungsdaten. XDR nutzt die Erkenntnisse aus jeder Untersuchung zur Verbesserung der Prävention. Das stärkt die Sicherheit, reduziert die Anzahl der Warnmeldungen und hebelt ähnliche Bedrohungen in Zukunft von vornherein aus.

Was kann XDR Ihrem SOC bieten?

Sie legen Wert auf Prävention. XDR unterstützt diesen Ansatz mit einer Erkennungs- und Abwehrtechnologie, die Ihren Sicherheitprofis den Übergang von einer reaktiven zu einer proaktiven Arbeitsweise ermöglicht. Die Auswertung sämtlicher Datenquellen und die angemessene Bewertung aller Prozesse, von der Priorisierung von Benachrichtigungen bis zur Bedrohungssuche, ermöglicht Ihnen die erhebliche Verbesserung Ihres Sicherheitsmanagements. Ihr Sicherheitsteam wird von der erdrückenden Flut der Warnmeldungen befreit, kann Fehlalarme in Rekordzeit herausfiltern und schneller fundierte Entscheidungen treffen. So können Ihre hochqualifizierten Experten, von manueller Kleinarbeit befreit, endlich ihrer eigentlichen Arbeit nachgehen, nämlich der Suche nach noch unbekannten Bedrohungen und der souveränen Abwehr bekannter Angriffsmethoden. Mit Automatisierung und einem umfassenden Überblick über Ihre Sicherheitslage trägt XDR dazu bei, dass Ihr SOC seine Leistungsfähigkeit voll entfalten kann. Fragen Sie bei der Suche nach einer Technologie für die Erkennung und Abwehr von Bedrohungen gezielt nach dem „X“, denn eine eindimensionale Perspektive auf Ihre IT-Infrastruktur reicht nicht mehr aus.

Palo Alto Networks,
Oval Tower, De Entrée 99-179,
1101HE Amsterdam,
Niederlande

Telefon: +31 20 888 1883

www.paloaltonetworks.de

redefine-security-operations-with-xdr-wp-012219