CyberCompare Whitepaper

Wie Sie die richtige Lösung für den Schutz Ihrer Endgeräte finden – die Welt aus EDR, XDR und MDR verstehen

Endpunktsicherheit ist ein Dauerbrennerthema – und eine tragende Säule der IT-Sicherheit. Antivirus(AV)-Software dagegen ist Schnee von gestern, und selbst die Popularität von Next-Gen-Antivirus (NGAV), also Antivirenlösungen der nächsten Generation, lässt nach. Ganz oben auf der Buzzword-Liste der Anbieter stehen heute EPP, EDR und XDR (sowie natürlich Verhaltensanalyse und künstliche Intelligenz). Wir unterstützen unsere Kundschaft regelmäßig beim Klären ihrer Anforderungen sowie bei (neuen) Ausschreibungen und entsprechender Marktforschung. In manchen Fällen liegen der Kunschaft bereits Angebote vor, aber sie brauchen einen unabhängigen Blick von außen oder geeignete Alternativen.

Einleitung

Bezeichnungen (vereinfacht, Anbieterdefinitionen können abweichen)

NGAV
Next-Generation Antivirus

Nutzen Softwareauskundschaftende auf einem Host, um (in der Regel dateibasierte) Angriffe zu verhindern (signatur- oder reputations-basiert).

EDR
Endpoint Detection & Response

Funktioniert über Anomalieerkennung, die Korrelationen in den Daten mehrerer Endpunkte erfasst und (nahezu) in Echtzeit analysiert; dies ermöglicht sogar die Erkennung komplexer Angriffsszenarien. Zu den Reaktionsmöglichkeiten zählen nicht nur Warnmeldungen, sondern auch erste Gegenmaßnahmen auf Endgeräteebene.

EPP
Endpoint-Protection-Platform

Kombiniert klassische AV-Funktionen mit Intrusion-Prevention-Systemen und anderen Firewall-Funktionen wie Data Loss Prevention und Verschlüsselung. Diese Lösungen dienen in erster Linie der Prävention und stützen sich vor allem auf Signale eines einzelnen Hosts. Dies gilt aber nicht für alle Lösungen; manche EPP bieten auch umfassende EDR-Kapazitäten.

XDR
Extended Detection & Response

XDR-Lösungen bieten den vollen EDR-Funktionsumfang, nutzen darüber hinaus aber auch Events aus Cloud-Anwendungen und anderen Protokollquellen (Firewalls, Domain Controller, Vulnerability Scanner, Network Traffic Analysis etc.), um Anomalien zu erkennen (einschließlich Log Data Lake und unter Umständen weiterer Sicherheitsfunktionen wie Honeypots).

NDR
Network Detection & Response

Netzwerküberwachung (Network Traffic Analysis, NTA) zur Erkennung bösartiger Aktivitäten auf Basis von Signaturen oder Anomalien; die Lösungen unterscheiden sich z.B. in der Nutzung von Metadaten oder Deep Packet Inspection. Sie basieren in der Regel auf Sensoren/Agenten, die an Routern, Switches oder Firewalls angedockt sind und sowohl den East-West-Traffic als auch den North-South-Traffic überwachen.

MDR
Managed Detection & Response

Service für die Überwachung und den Betrieb einer technischen Lösung wie EDR/XDR/NDR, in der Regel in einem 24/7- oder 8/5-Modus; im Grunde genommen ein eingeschränktes Security Operations Center (SOC). Der Service kann je nach Vertrag Threat Hunting und Incident Response mit unterschiedlichen Stufen der Eindämmung und Beseitigung von Bedrohungen umfassen.

1. Wählen Sie die richtige Lösung für Ihre Situation

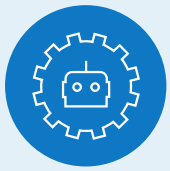
EDR allein reicht nicht aus

Richtig konfiguriert können moderne EDR-/XDR-Lösungen sowohl Angreifenden als auch Penetration-Testenden das Leben richtig schwer machen. Es ist praktisch unmöglich, ein System oder Netzwerk anzugreifen, ohne Spuren zu hinterlassen, die bei der forensischen Datenanalyse ans Licht kommen.

Gleichzeitig reicht es nicht aus, sich nur auf Erkennung und Reaktion zu konzentrieren; „klassische“ Hash-/signaturbasierte AV-Systeme bieten noch immer den schnellsten Schutz gegen die am weitesten verbreiteten Formen der Schadsoftware. Fehlen diese Funktionen in Sicherheitslösungen, kann zwar die Erkennung besser werden (d.h., es wird häufiger Alarm ausgelöst), aber die Reaktion erfolgt in vielen Fällen verzögert oder bleibt aus.

Wer reagiert auf welche Alarmmeldungen?

Wann und wie erfolgt die Ursachenforschung – auch bei Alarmmeldungen außerhalb der Arbeitszeiten, in anderen Ländern oder bei Home-Office-Geräten?



Vollautomatische Ansätze über Playbooks oder Lösungen wie Hunters.AI haben sich bis heute noch nicht als praxistauglich erwiesen.

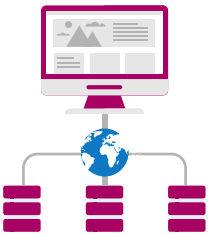
Zudem muss immer geklärt werden, ob Scans „on Demand“ durchgeführt werden können (z.B. Scans von Datenspeichermedien, für die weder Baselining noch Anomalieerkennung durchgeführt wurde). Außerdem sollten die Funktionen eines Tools für offline betriebene Geräte überprüft werden.

Welche EDR-/XDR-Lösung ist die beste?

Alle Herstellenden – selbst ohne Kaspersky gibt es mehr als zwanzig ernstzunehmende Anbietende auf dem Markt – werben mit herausragenden Ergebnissen bei AV- und Labortests, MITRE-Analysen oder mit beeindruckenden Stimmen der Kundschaft. Selbst kleinere Anbietende können Unternehmenskundschaft mit 50.000 Installationen oder mehr vorweisen. Trotzdem gibt es keine perfekte Lösung, die entsprechend geschulte und motivierte Angreifende nicht überwinden oder umgehen könnten.

Deshalb ist das Erfüllen der individuellen Kundschaftanforderungen in der Regel wichtiger als die konkreten technischen Funktionen oder ein Testergebnis. Wir empfehlen, sich bei der Beurteilung von Lösungen sowie MDR-Service auf Alleinstellungsmerkmale zu konzentrieren. Ausführliche Vergleiche des gesamten Funktionsumfangs führen sonst dazu, dass alle Lösungen zwischen 95 und 99% liegen und die entscheidenden Punkte, die einen Unterschied machen und die Kaufentscheidung beeinflussen sollten, in der Masse der geprüften Punkte untergehen. Eines der wichtigsten Entscheidungskriterien könnte z.B. die Auswahl der unterstützten Betriebssysteme sein. Zur Zeitpunkt der Entstehung dieses Whitepapers, boten die meisten Lösungen bei manchen Linux-Distributionen nur einen begrenzten Funktionsumfang, und wir kennen nur einen Anbietenden, der IBM Power, IBM AIX oder Oracle Solaris unterstützt.

Welche EDR-/XDR-Lösung ist die beste? *(fort.)*



Die Kompatibilität (z.B. mit Ticketsystemen, Protokollquellen, Token für Multifaktorauthentifizierung oder anderen Sicherheitsprodukten) fällt je nach Lösung sehr unterschiedlich aus. Bedeutet Kompatibilität eine Integration in beide Richtungen, d.h., lassen sich Reaktionsmaßnahmen auslösen? Anbindungen über API müssen gründlich geprüft werden: Wer ist für die Aktualisierung der Schnittstelle verantwortlich, wenn die API aktualisiert wird? Welcher Aufwand ist in der Regel zu erwarten? Bei Protokollquellen bedeutet die Speicherung von Syslog-Daten natürlich noch lange nicht, dass benutzerdefinierte Erkennungsregeln auf Basis der berücksichtigten Logs erstellt werden können. Zudem lassen sich programmierte Regeln bei einem Wechsel der NGAV-Lösung nicht immer übertragen.

Ein technischer Faktor, der das Feld von Anbietenden deutlich ausdünnen kann, ist die Möglichkeit, die zentralen EDR-Server bei der Kundschaft zu betreiben. Manche Lösungen mögen diese Option theoretisch anbieten, lassen sich in der Praxis jedoch nicht den Anforderungen des Unternehmens entsprechend skalieren. Für die meiste Kundschaft ist es kostengünstiger, wenn Anbietende ein System (mit kurzen Updatezyklen) über die Cloud bereitstellen. Deshalb sind die Sicherheitsvorteile von lokal bei der Kundschaft betriebenen Servern (für den Fall, dass der Cloud-Anbieter gehackt wird) bislang eher gering: Da bei den meisten Unternehmen IT und IT-Sicherheit eher dünn besetzt sind, würde der Vor-Ort-Betrieb des EDR-/XDR-Systems wertvolle Ressourcen von anderen Sicherheitsaufgaben abziehen.

Vorhaltezeit von Daten ist in der Regel ein starker Kostentreiber. Hier lohnt es sich, Fragen wie diese zu stellen: Welche Daten werden im Rahmen des angebotenen Pakets wie lange gespeichert? Die beworbenen Speicherzeiten beziehen sich häufig nur auf die Erkennungsdaten bei Alarmmeldungen, nicht auf die vollständigen Telemetriedaten wie Dateiveränderungen, Registry-Veränderungen, Prozessaufrufe oder Netzwerkverbindungen. Vor dem Hintergrund, dass Angreifende in manchen Fällen bis zu einem Jahr im Netzwerk verbleiben, sind sieben Tage zu kurz, um nach dem Erkennen eines Vorfalls den Patienten Null oder einen Datenabfluss aufzuspüren. Das BSI empfiehlt z.B. eine Vorhaltezeit von 90 Tagen.

In der Praxis überwachen die meisten Unternehmen und öffentlichen Stellen die EDR/XDR Lösung nicht selbst, sondern kaufen sich einen 24/7 Überwachungsservice (MDR) ein. Falls das Tool tatsächlich selbst betrieben wird, ist ein entscheidendes Kaufkriterium häufig, wie intuitiv sich ein Tool durch die Fachleute der Kundschaft konfigurieren und bedienen lässt. Kompetenz und Kapazitäten des internen Teams an Analysierenden sind ebenfalls ein entscheidendes Kriterium: Lösungen wie Elastic sind überaus leistungsstark, stellen aber überdurchschnittliche Anforderungen an das interne Sicherheitsteam der Kundschaft.

Ist ein Proof of Concept wirklich notwendig?

Pauschale Aussagen wie „Anbietende X sind besser als Anbietende Y“ einzig und allein auf der Basis von Berichten (etwa von Gartner/Forrester) sind nicht möglich. Bei jeder Lösung, die wir kennen, hängt das tatsächlich erreichte Schutzniveau viel zu sehr von der Systemlandschaft, den Anwendungen und dem Nutzendenverhalten ab. Aus diesem Grund empfehlen wir immer so genannte „Purple Team Proof of Concept Tests“, die einen aussagekräftigen Vergleich der unterschiedlichen Lösungen in der tatsächlichen Systemumgebung ermöglichen. Die Kundschaft sollte Red/Purple Team Tests durchführen – entweder in Kooperation mit effektiven Dienstleistenden oder eigenständig mit Open-Source-Tools wie Redcanary/atomic-red-team.

Bei diesen Tests kommt ein Skript zum Einsatz, das sicherzustellt, dass der Proof of Concept über unterschiedliche Standorte hinweg vergleichbar ist, und beispielsweise überprüft, wie die Supportfunktionen der Herstellenden oder Anbietenden auf Funktionsstörungen und Alarmmeldungen reagieren. Solche Tests haben z.B. gezeigt, dass bei einer Lösung die „Tamper Protection“ nicht funktionierte (hier war es auch ohne Admin-Rechte/-Ausweis möglich, den Agenten auszuschalten) – trotz anders lautender Aussagen im Datenblatt von Herstellenden.

Zumindest sollten vor dem Treffen einer Entscheidung ausführliche Demos mit einer Überprüfung vergleichbarer Testfälle durchgeführt werden. Bei diesen Testfällen können bestimmte Angriffsvektoren, die Kompatibilität mit anderen Softwareprodukten oder das Erstellen individueller Erkennungs- und Reaktions-Runbooks geprüft werden. Palo Alto Networks bietet eine gute Sammlung möglicher Alarm-Testfälle samt den erforderlichen Logquellen und empfohlenen Untersuchungsmaßnahmen, die ebenfalls getestet werden können.

2. Welche Dinge sind wichtig zu wissen?

Funktionieren Lösungen von US-Herstellern auch in China?

Ja. Wir kennen bislang keine Fälle, in denen nicht problemlos chinesische Standorte eingebunden werden konnten. Cloud-Lösungen laufen bislang reibungslos. Natürlich ist es notwendig, dass sich Kunden bei Datenübertragungen aus China mit den zuständigen staatlichen Stellen abstimmen (in der Regel müssen unverschlüsselte Daten übertragen oder die Schlüssel offengelegt werden).

Gibt es Anbieter mit Hauptsitz in der EU?

Ja. Unternehmen wie Bitdefender, ESET, SEKOIA.IO oder TEHTRIS haben alle ihren Hauptsitz in der EU. Unter dem Strich sind sie aber vielleicht nicht die beste Wahl für Ihre Anforderungen. Alle führenden Anbieter gewährleisten die Einhaltung der DSGVO (mit in der EU betriebenen Rechenzentren und in manchen Fällen auch einem Analystenteam in Europa) und haben bereits Kunden im staatlichen Sektor oder im Bereich der kritischen Infrastruktur.

Was ist mit garantierter Breach Protection?

Als Teil der Falcon Complete Services garantiert CrowdStrike, dass Endpunkte mit seinen Agenten nicht gehackt werden können. Hinter dieser Garantie steht eine US-Versicherungsgesellschaft. SentinelOne bietet bei Nutzung ihrer Singularity-Plattform auf Wunsch eine ähnliche Garantie, ebenso wie seit Kurzem Sophos.

Dieser Ansatz ist grundsätzlich begrüßenswert und, soweit wir es beurteilen können, ein innovatives Verkaufsargument. Ein genauerer Blick auf die Ausschlusskriterien (Länder, Systeme) zeigt jedoch, dass diese „Garantie“ selbst bei IT-Infrastrukturen mit moderater Komplexität nicht mehr umfassend ist. So gelten die Garantieansprüche i.A. nur für unterstützte Windows-Betriebssysteme. Nur Endpunkte mit Cloud-Anbindung werden abgedeckt, was zeigt, dass diese Systeme nur mit Internetanbindung wirksam sind. Die maximale Zahlung (z.B. begrenzt auf 100.000 USD bei weniger als 5.000 Endpunkten oder auf 1 Mio. USD für jedes Lizenzjahr) deckt meist nur einen Bruchteil der Lizenzkosten ab und reicht nicht aus, um den durch Cyberkriminalität entstandenen tatsächlichen Schaden auszugleichen.

Ist Microsoft Defender als Teil von Microsoft 365 eine sinnvolle Option?

Defender für Endpunkt Plan 1 beinhaltet die klassischen AV-Funktionen und ist aktuell z.B. in E3-Lizenzen enthalten. Beim angebotenen Erkennungs- und Schutzniveau ist Defender Plan 2 eine der führenden EDR-Lösungen, die über weitere Pakete wie Defender for Office, Defender for Cloud Apps ein sehr umfangreiches Schutzniveau bietet. Der Preis hängt maßgeblich von den bestehenden Microsoft-Lizenzen des Kunden ab. Auch im Bereich Operational Technology Security (OT-Sicherheit) hat Microsoft seit der Übernahme von CyberX (jetzt Defender for IoT) große Fortschritte gemacht, ist allerdings immer noch ein Nischenprodukt im Vergleich zu Claroty, Nozomi o.ä..

Zu den Nachteilen gehört, dass die User Experience auf Grund einer komplizierteren Konfiguration in der Regel schlechter ist als bei anderen Tools. Linux Clients und Server verfügen Kundentests zufolge nur über einen eingeschränkten Funktionsumfang oder beschränkte Erkennungsfähigkeiten. Der rollenbasierte Zugang beschränkt sich auf wenige vordefinierte Rollen, was bei Multi-Tenant-Unternehmen und Managed Security Service Providers (MSSPs) weitere Komplikationen verursacht. Das Betriebssystem von der Sicherheitsüberwachung zu trennen, kann Vorteile haben (hat aber auch Nachteile).

Aktuell gehen wir davon aus, dass Microsoft allmählich de facto zum Standardanbieter für Endpunktsicherheit wird, insbesondere bei homogenen IT-Umgebungen und mittelständischen Unternehmen. Viele Kunden steigen ohnehin auf Microsoft 365 um, und die darin enthaltenen Sicherheitsfunktionen werden mit der Zeit immer besser werden. Unternehmen mit begrenzten IT-Ressourcen können sich das Leben erleichtern, wenn sie sich auf möglichst wenige unterschiedliche Anbieter und Schnittstellen beschränken. Kein anderer Lösungsanbieter kann auf mehr Daten oder finanzielle Ressourcen zurückgreifen, um sein System zu optimieren und bei neuen Bedrohungen schnell zu aktualisieren. Das Kosten-Nutzen-Verhältnis fällt jedoch je nach Kunde noch unterschiedlich aus. Im Allgemeinen werden Betrieb und Überwachung durch einen der zahlreichen MDR-Dienstleister übernommen, die sich auf MS Defender spezialisiert haben.

Mit welchen Kosten ist zu rechnen?

Listenpreise sind nur Schall und Rauch – was die Kundschaft tatsächlich bezahlt, hängt maßgeblich vom Kanal (Distributor, Channel Partner, MSSP) und von der Wettbewerbssituation ab. Wir empfehlen, mit den Resellern, die die Angebote erstellen, über Rabatte zu verhandeln, und für alle Herstellenden mit einem anderen Resellenden zusammenzuarbeiten, um bessere Preise zu bekommen. Als Faustregel lassen sich pro Endpunkt 20 bis 70 EUR jährlich veranschlagen.

Verständlicherweise konzentrieren alle Herstellende ihre Vertriebsaktivitäten auf Unternehmen mit mehr als 2.000 Beschäftigten. Wir haben sogar erlebt, dass manche Herstellende oder Systemhäuser zögern, kleinerer Kundschaft überhaupt ein Angebot zu unterbreiten. Gerne unterstützen wir Sie dabei, ein faires Preis-/Leistungsverhältnis zu erzielen.

Brauche ich im Rahmen von XDR ein Identity-Protection-Modul?

Es gibt unterschiedliche Arten, Identitäten zu schützen und verdächtiges Verhalten aufzudecken, etwa anonyme IP-Adressen, Atypical/Impossible Travel, unbekannte Geolocation, viele fehlgeschlagene Anmeldeversuche oder die unbefugte Nutzung von Ressourcen unter Umgehung von Kerberos (womöglich ein Golden-Ticket-Angriff). Die Reaktionen auf solche Fälle können vom Anfordern eines zweiten Authentifizierungsfaktors (im Rahmen der Multifaktorauthentifizierung) über das Sperren des Zugangs oder Beschränken der Admin-Rechte/privilegierten Zugangsrechte bis hin zum Sperren oder sogar Löschen von Nutzern führen.

Hinweise auf Identity Compromise

- Anonyme IP-Adresse
- Atypical/Impossible Travel
- unbekannte Geolocation
- viele fehlgeschlagene Anmeldeversuche
- unbefugte Nutzung von Ressourcen unter Umgehung von Kerberos (womöglich ein Golden-Ticket-Angriff)

Reaktionsmöglichkeiten

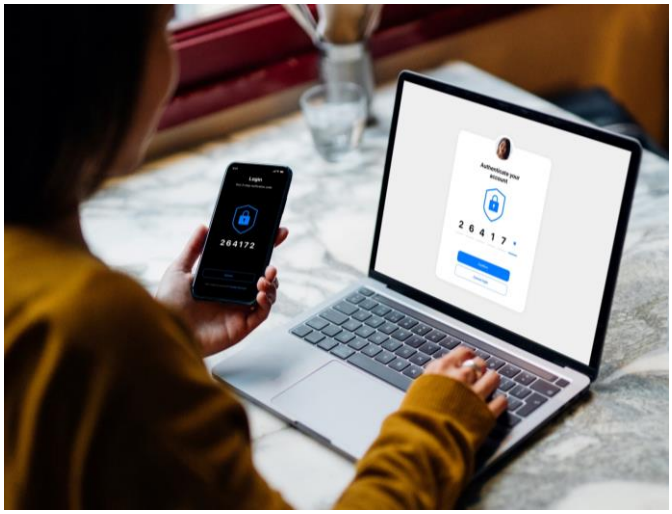
- Anfordern eines zweiten Authentifizierungsfaktors
- Sperren des Zugangs
- Beschränken der Admin-Rechte/privilegierten Zugangsrechte
- Sperren oder Löschen von Nutzern

Um solche Fälle zu erkennen und entsprechend reagieren zu können, bietet sich z.B. der Kauf eines Identity-Protection-Moduls bei einem XDR-Anbietenden an (das in der Regel von einem Softwareagenten auf dem Domain Controller installiert und für die Genehmigung aller Authentifizierungen verwendet wird). Als Alternative lassen sich die Logs und Events der Identitätsdienste (inbs. AD / Azure AD) überwachen. Bei manchen XDR-Lösungen sind einige Anwendungsfälle bereits standardmäßig implementiert, andere lassen sich über benutzerdefinierte Regeln und Skripte abdecken, die mit der Identity- und Access-Management-Lösung kommunizieren. Eine andere Möglichkeit, solche Fälle zu erkennen und darauf zu reagieren, sind „Privileged Access Management“-Systeme oder die Implementierung der Anwendungsfälle mit einem „Security Information and Event Management“(SIEM)-System oder einem „Security Orchestration, Automation, and Response“ (SOAR)-System. Wichtig ist, diese Angriffstaktiken bei der Risikoanalyse zu berücksichtigen.

Manche Dienstleistende bieten an, Passwort-Hashes mit Darkweb-Informationen abzugleichen, um zu überprüfen, ob die Zugangsdaten gestohlen und zum Verkauf angeboten wurden – diese Dienstleistung lässt sich bei externen IT-Sicherheitsberatungen natürlich auch separat kaufen.

USB Device Control

Viele der EPP/EDR Lösungen bieten entweder aufpreispflichtig oder standardmäßig die Funktion an, USB Ports zu sperren. Allerdings kann die Steuerung i.A. nicht ähnlich granular wie bei dedizierten Device Control Lösungen (z.B. DriveLock, EgoSecure o.ä.) erfolgen. Auch eine Verschlüsselung der Daten kann im Normalfall nicht erzwungen werden.



Funktionsumfang auf Linux Systemen

Die Erkennung von Angriffen auf Linux-Clients und -Server mittels EDR funktioniert oft eingeschränkt. Viele Anbieter (z.B. Deep Instinct, ESET, Qualys, Sophos, oder Fortinet) hatten für die MITRE Enterprise ATT&CK Auswertung 2022 noch keinen Linux-Agenten, der für Tests zur Verfügung stand. Auch die Antivirus-Funktionalität ist oft eingeschränkt – so wird Malware für Windows-Rechner oft nicht erkannt, wenn sie auf Linux-Systemen gespeichert wird. Red Canary hingegen bietet z.B. ein EDR System speziell für Linux an. Gerne unterstützen wir Sie bei der Auswahl einer Endpunktlösung, die für die bei Ihnen eingesetzten Distributionen den besten Schutz darstellt.

Was ist mit Mobilfunkgeräten wie Smartphones und Tablets?

Das hängt von den kundenspezifischen Risiken ab. Bei der meisten Kundschaft, abgesehen vom Bankwesen, ist es nach wie vor am wichtigsten, auf allen Geräten, die auf Ressourcen des Unternehmens zugreifen können, ein Mobile Device Management (MDM) wie Microsoft Intune oder MobileIron einzurichten. Zu den wichtigsten Einstellungen gehören unter anderem automatische Sicherheitsupdates, das Erkennen und Quarantänisieren nicht konformer, gejailbreakter oder gerooteter Geräte sowie das Sandboxing von App-Daten. Die Betriebssysteme Android und iOS erlauben keine Erkennungs- und Reaktionsfähigkeiten, die mit EDR auf einer Workstation oder einem Server vergleichbar sind.

Einige Lösungen ermöglichen die Installation einer „Mobile Threat Prevention“-App auf Smartphones und Tablets, um Missbrauch oder Angriffe wie sicherheitsgefährdendes Browsing-Verhalten oder Phishing über SMS/Messenger-Apps zu erkennen und zu verhindern. Wichtig ist aber, dass dies „auch nur eine weitere App“ ist, die in ihrem Funktionsumfang nicht mit einem EDR-Agenten vergleichbar ist. Die Lösungen unterscheiden sich außerdem in ihrer Nutzung von MDM-Protokollen, um Alarmmeldungen zu erzeugen und Korrelationen zwischen Alarmmeldungen zu analysieren.

3. Verschiedene Optionen und Wege kennen

Was sind Managed Detection und Response (MDR) Services?

Die Kunschaft möchte oft die 24/7-Überwachung und den Betrieb eines XDR-Tools auslagern, um Ressourcen zu sparen. Das ist sinnvoll, denn wenn MDR-Anbietende ihre Analysierenden und Infrastruktur für Hunderte oder Tausende von Kaufenden nutzen, profitieren sie von Größeneffekten. Manchmal gibt es auch Hybridansätze mit einem externen MDR-Anbietenden, der ein internes SOC-Team bei Threat Intelligence, Threat Hunting, Triage oder Incident Response unterstützt.

Immer mehr Anbietende verkaufen MDR-Services als Add-on zu ihrer Software (z.B. Cynet, Cybereason, Fortinet, SentinelOne, CrowdStrike, Rapid7, Sophos, Secureworks' Taegis, Trend Micro, Palo Alto Networks), selbst Microsoft bietet inzwischen eigene Überwachungs-Services wie „Defender Experts for Hunting“ an. Daneben gibt es insbesondere für die weitverbreiteten Anbietenden MSSPs, die Managed SOC/MDR/“SecOps“ anbieten. Beide Ansätze funktionieren in der Praxis gut. Dienstleistungsverträge mit großen XDR-Anbietenden sind natürlich meist stark standardisiert, während kleinere MSSPs unter Umständen eine individuelle Gestaltung der Konditionen anbieten. In beiden Fällen ist aber das Kleingedruckte in den Verträgen entscheidend, einschließlich Antworten auf die folgenden Fragen:

Was sind Managed Detection und Response (MDR) Services? *(fort.)*

Wer ist dafür verantwortlich, die Agenten einzusetzen (etwa bei neuen Geräten), die zentrale Konsole zu konfigurieren, Schwierigkeiten beim Betrieb der Agenten zu lösen und sie später wieder zu deinstallieren?

Wer kümmert sich gegebenenfalls um das Einrichten und Aktualisieren von Decoys?

Wer ist dafür verantwortlich, Logquellen zu integrieren und benutzerdefinierte Erkennungsregeln zu schreiben?

Wie häufig wird nach Bedrohungen gesucht, welche Daten kommen zum Einsatz und auf der Basis welcher Hypothesen wird dabei vorgegangen?

Wie lang sind die Reaktionszeiten bei schwerwiegenden und kritischen Vorfällen?

Brauchen Kunden eine Kontaktperson vor Ort, die bei einem Alarm rund um die Uhr, sieben Tage die Woche erreichbar ist?

Eindämmung: Welche Assets kann der MDR-Anbieter sofort isolieren, welche erst nach Zustimmung der Kunden? Wie sehen die Entscheidungsprozesse auf Kundenseite aus? So dürften z.B. für einen ERP-Server und Single Clients unterschiedliche Regeln gelten.

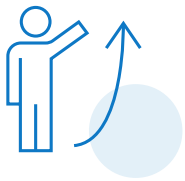
Gibt es einen Incident-Response-Service vor Ort oder nur remote?

Wer ist für Wiederherstellung und Forensik verantwortlich?

Haben die Kunden Zugang zu allen Daten, und können die Kunden die Daten separat speichern?

Erfahrene MDR-/Managed-SOC-Anbietende haben für solche Fragen bereits vorbereitete Playbooks und RACI-Charts. Abgesehen von solchen Aspekten lässt sich die Erfahrung von Anbietenden auch daran ablesen, wie viele Endpunkte sie bereits mit einer spezifischen Lösung schützen, wie lange Analysierende im Durchschnitt beim Unternehmen bleiben und welche Zertifizierungen einzelne Teammitglieder und die Organisation als Ganzes haben.

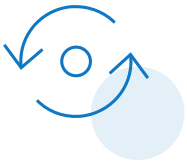
Sollten Kunden direkt mit der Einführung eines Managed SIEM/SOCs beginnen oder lieber mit MDR auf Basis von EDR/XDR/NDR?



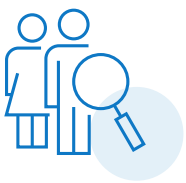
Wir empfehlen in fast allen Fällen, mit einem korrekt aufgesetzten und konfigurierten EDR / XDR-System zu beginnen und erst im zweiten Schritt auf SIEM/SOAR aufzustocken. Dazu gehört auch ein gründliches Baselining (in der Regel mehrere Monate lang), um falsch positive Ergebnisse herauszufiltern und die Playbooks anzupassen.

Das „Schutzniveau pro ausgegebenen Euro“ erscheint uns bei hostbasierten Endpunktsicherungen höher als bei SIEM; außerdem ist der interne Implementierungsaufwand geringer. Darüber hinaus bieten eine Reihe von XDR-Anbietern bereits SIEM-ähnliche Möglichkeiten für Protokollierung und Logkorrelation in Data Lakes. Für Kunden, die nicht aus Compliance-Gründen ein SIEM benötigen, ist ein gut konfiguriertes XDR wahrscheinlich die effektivere Alternative.

Dieser Trend spiegelt sich auch in den M&A-Aktivitäten: SentinelOne kaufte 2021 den Logging-Spezialisten Scalyr. Dies dürfte dazu führen, dass es in Zukunft bei den unterschiedlichen Produkten mehr Überschneidungen gibt.



Das Gleiche gilt für Identity- und Access-Management . Auch hier bieten viele Hersteller bereits Module an oder übernehmen entsprechend spezialisierte Anbieter.



Ob NDR-Funktionen (etwa Lösungen von Vectra, Darktrace oder ExtraHop) wichtiger sind als EDR, ist Ansichtssache. In unseren Augen bringen EDR-Hersteller und Lösungen in Bereichen wie Kundenbetreuung oder Support für Altsysteme mehr Erfahrung mit und bieten insgesamt ein besseres Kosten-Nutzen-Verhältnis (u.a. auf Grund des höheren Wettbewerbsdrucks in diesem Bereich, aber auch aufgrund der weiten Verbreitung von verschlüsseltem Netzverkehr und mobilem Arbeiten in Verbindung mit SaaS/IaaS – eine Kombination, bei der NDR-Lösungen kaum Chancen auf Bedrohungserkennung haben).

Manche Hersteller bieten inzwischen zwar ebenfalls ausgereifte Lösungen und globale Größeneffekte (vor allem bei Threat Intelligence), aber sie kosten nicht unbedingt weniger als die SOC-Services eines unabhängigen MSSP. Die entscheidenden Kriterien sind Erfahrung mit dem System und eine klare Aufteilung der Zuständigkeiten (Verantwortung für Alarmmeldungen und Reaktion, auch für Entscheidungen über das Isolieren von Geräten oder Netzwerkabschnitten).

Überblick der Anbieter und Aufführung in Analystenberichten

Vendor / Analyst reports	MITRE 2022 ATT&CK evaluation Managed Services (OilRig)	MITRE 2022 ATT&CK evaluation, Wizard Spider and Sandworm	MITRE ATT&CK evaluation 2021, Carbanak and FIN7	Gartner MQ Endpoint Protection (2022)	Gartner MQ Endpoint Protection (2021)	Endpoint Security Solutions Review (2022)	SE Labs Endpoint Security Enterprise Q1.2023	Kuppinger-Cole EPDR (2022)	Forrester: Enterprise Detection and Response, Q2 2022	Forrester: Managed Detection and Response, Q2 2023	IDC MarketScape: Worldwide Modern Endpoint Security for Enterprises 2021 Vendor Assessment
Ahnlab		✓	✓								
Binary Defense						✓					
Bitdefender	✓	✓	✓	✓	✓				✓		
Blackberry Cylance	✓	✓	✓	✓		✓			✓		
Checkpoint		✓	✓	✓	✓				✓		✓
Cisco		✓	✓	✓	✓						✓
Crowdstrike	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Cybereason		✓	✓	✓	✓	✓		✓	✓		✓
Cycraft		✓	✓								
Cynet		✓	✓			✓					
Deep Instinct		✓		✓							
Elastic		✓	✓						✓		
ESET		✓	✓	✓	✓		✓	✓			✓
Fidelis		✓	✓			✓					
Fortinet		✓	✓	✓	✓		✓		✓		
GoSecure			✓			✓					
IBM Security Qradar/Reaqta		✓	✓			✓					
Malwarebytes		✓	✓			✓					
McAfee / Trellix / FireEye Helix		✓	✓	✓	✓		✓		✓		✓
Microsoft	✓	✓	✓	✓	✓		✓	✓	✓		✓
NetWitness						✓					
Opentext EnCase / ArcSight	✓		✓								
Palo Alto Networks	✓	✓	✓	✓		✓			✓		✓
Qualys		✓									
Rapid7	✓	✓								✓	
Red Canary	✓									✓	
Secpod						✓					
SecureWorks Taegis										✓	
Sekoia.io											
SentinelOne	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓
Sophos	✓	✓	✓	✓	✓		✓	✓	✓		✓
Symantec / Broadcom		✓	✓	✓	✓		✓	✓			✓
Tanium						✓					
Tehtris											
Trend Micro	✓	✓	✓	✓	✓				✓		✓
Uptycs		✓	✓								
VMWare CarbonBlack		✓	✓	✓	✓	✓			✓		✓
Watchguard Panda							✓				✓
WithSecure	✓	✓	✓	✓	✓						

4. Was man noch wissen sollte

Schutz vor Ransomware

Als letzte Verteidigungslinie gibt es am Markt spezielle Tools zum Schutz vor Ransomware oder zur Eindämmung des Schadens, wenn doch ein Angriff gelingt. Der Hauptzweck besteht darin, Schadsoftware (die womöglich vom EDR-System nicht erkannt wurde) daran zu hindern, große Datenmengen zu verschlüsseln oder zu beschädigen.

Da diese Lösungen nicht dazu beitragen, Angreifende im Netzwerk zu erkennen oder die Exfiltration von Daten (auf deren Basis dann Lösegeld erpresst werden kann) zu verhindern, setzen die meisten kaufenden Personen solche Programme als Ergänzung („EDR+1“) zu ihren EDR- oder XDR-Systemen ein, nicht als Ersatz. Ein Vorteil dieses Ansatzes ist ein geringerer Anteil an falschpositiven XDR-Ergebnissen. Zu den typischen Kundschaftsgruppen zählen bisher Finanzinstitute und kritische Infrastrukturorganisationen, während andere Segmente die zusätzlichen Kosten scheuen (die Preise pro Nutzende bewegen sich in einem ähnlichen Rahmen wie bei EDR-Lösungen).

Deep Instinct arbeitet z.B. mit einem Deep-Learning-Algorithmus statt mit Signatur- oder Reputationsdatenbanken. Der Vorteil besteht darin, dass Agenten auf Systemen ohne Internetverbindung deutlich länger effektiv bleiben (auch gegen Zero-Day-Bedrohungen) als klassische AV-/NGAV-Lösungen. Sowohl während der Übertragung als auch im Speicher lassen sich Dateien scannen und an der Ausführung hindern. Die Lösung ist typischerweise vom ersten Tag an wirksam und erfordert keine Baselining-Phase. Bei größeren Einsatzbereichen bieten die Hersteller häufig Schadenersatzzahlungen für den Fall, dass trotz installierter Software ein Ransomware-Angriff Erfolg hat.

Der dänische Herstellende BullWall schützt File Shares, Anwendungsserver und Cloud-Datenbanken (aber nicht einzelne Clients) mit einem agentenlosen System vor Verschlüsselung. Das entsprechende Produkt RansomCare überwacht Benachrichtigungen über Dateiereignisse, die versandt werden, wenn Dateien umbenannt, geändert oder gelöscht werden. Daher ist eine Baselining-Phase zum Kennenlernen und Erfassen des normalen Verhaltens erforderlich, bevor das System seine volle Wirksamkeit erreicht. Die Software reagiert, indem sie betroffene Nutzende oder Geräte schnell isoliert (was in der Regel bedeutet, dass nicht mehr als 10 bis 50 Dateien beschädigt werden).

Beide Anbietende testen auf Wunsch auch bestehende EDR-/XDR-Systeme der Kunden in einem direkten Vergleich.

Bedrohungsbasierte Erkennung

Insbesondere für Security-Analysierende (Inhouse oder bei MSSPs) werden Threat Intelligence Feeds (auch branchenspezifisch) und weitere Tools angeboten, um das Schutzniveau zu erhöhen und die SecOps-Arbeit effizienter zu gestalten. Dazu gehören neben SOAR-Lösungen auch einzelne Bausteine wie Regelsätze (z.B. von oder Konfigurationen, die in einer modellierten Umgebung auf die Erkennung von Angriffsketten getestet werden können (z.B. von AttackIQ oder Tidal Cyber).

5. Fazit

Kunden sollten die Breite des Angebots am Markt ausnutzen und sich den Anbieter aussuchen, der wirklich am besten zu den individuellen Anforderungen passt. Ein reiner Abgleich der technischen Features auf Basis von Marktstudien und Marketingunterlagen bildet in der Regel keine gute Basis für eine fundierte Entscheidung.

Kontaktieren Sie uns!

Mehr Security für Ihr Budget:
Pragmatisch. Unabhängig. Zusammen.

cybercompare@bosch.com

Verbände/Industriekooperationen von **Bosch CyberCompare**

Besuchen Sie unsere Website:
www.cybercompare.com