
STORMSHIELD
XDR
Warum wird eXtended Detection & Response das neue Paradigma der Cybersicherheit sein?

Inhalt

Executive Summary

Über dieses E-Book

Wir beschreiben die verschiedenen Aspekte, die eine Organisation bei der Einführung eines sicheren und vertrauenswürdigen XDR-Ansatzes oder einer XDR-Lösung berücksichtigen muss.

Dieses Dokument richtet sich an Berater und Verantwortliche für die Sicherheit von Informationssystemen, um die Ziele zu verstehen, die XDR-Lösungen für einen optimalen Schutz von Unternehmen erreichen müssen.

Heutzutage stellen Cyberangriffe eine nahezu alltägliche Realität dar. Sie werden immer raffinierter und hartnäckiger, wodurch sie herkömmliche Cyberschutzlösungen aushebeln. Um ihnen entgegenzuwirken, erscheinen neue Werkzeuge und Techniken auf dem Markt für Cybersicherheit.

EXtended Detection and Response oder XDR ist die Weiterentwicklung von Detection and Response-Lösungen wie EDR. Dieser neue Ansatz stellt einen Vorwärtsschritt bei der Behandlung verschiedener Bedrohungen dar, indem andere Datenquellen (Netzwerke, Dateien, Cyber Threat Intelligence usw.) zur Erkennung von Indikatoren hinzugefügt werden. Diese Häufung von Informationen in einem Datensammlungstool erfordert die Implementierung von Orchestrierungsfunktionen, um Ereignisse zu korrelieren, Warnungen zu generieren und Zwischenfälle durch Reaktions- und Abhilfeszenarien zu verwalten. Das Ganze fügt sich zu **einer umfassenden Lösung zusammen, die einen Gesamtüberblick über die Infrastruktur bietet, um die Entscheidungsfindung erheblich zu verbessern** und ein optimales Sicherheitsniveau aufrechtzuerhalten.

Angesichts der Menge an Warnmeldungen und Falschmeldungen, mit denen die Teams des Security Operations Center (SOC) häufig konfrontiert sind, ist es entscheidend, die wichtigsten Vorfälle zu identifizieren und die Teammitglieder bei der Entscheidungsfindung zu unterstützen, um Vorfälle besser zu bewältigen und Bedrohungen mit hohem Gefährdungsgrad zu priorisieren.

Um die Sicherheit von Unternehmen zu optimieren, **muss die XDR** daher nicht nur **Daten sammeln und korrelieren**, um **einen Gesamtüberblick zu erhalten, sondern auch passende Antworten auf verschiedene potenzielle Bedrohungen anbieten**.

So sind Cyber-Analysten in der Lage, Angriffe, die die Organisation bedrohen, zu **identifizieren**, konkrete Maßnahmen zu **ergreifen** und letztendlich zu **neutralisieren**.

Beim Aufbau einer XDR-Lösung sind verschiedene Richtungen möglich, und jeder Herausgeber wird bestimmte Elemente besonders hervorheben. Eine XDR-Lösung muss jedoch mindestens 4 wesentliche Aspekte abdecken:

- Die Erkennung von Ereignissen
- Die Pluralität der Ereignisquellen
- Die Korrelation von Daten
- Die Automatisierung geeigneter Antworten je nach Art des Zwischenfalles

Zusammenfassend lässt sich sagen, dass XDR mit einer umfassenden und integrierten Lösung gewährleistet, dass Unternehmen aller Größenordnungen auf die raffiniertesten Bedrohungen reagieren können, indem sie ihre betriebliche Effizienz steigern.

Was ist XDR?

Bei jedem neuen Ansatz zur Internetsicherheit sind die Antworten und Lösungen von Hersteller zu Hersteller unterschiedlich.

Wussten Sie das schon?

Gartner definiert eXtended Detection and Response oder XDR als: „Eine einheitliche Plattform zur Erkennung und Reaktion auf verschiedene Vorfälle, die automatisch verschiedene Daten aus mehreren proprietären Sicherheitselementen sammelt und miteinander in Beziehung setzt. “

Quelle: https://ebooks.cisco.com/story/10-ways-cisco-delivers-xdr-capabilities-today-ebook/page/1/7

Heute erfordert die Komplexität von Cyberangriffen einen neuen Ansatz, um Verhaltensweisen zu identifizieren, die darauf ausgelegt sind, innerhalb einer Organisation so lange wie möglich unentdeckt zu bleiben.

XDR ist eine Cybersicherheitslösung mit dem Ziel, Aufgaben zur **Erkennung von Vorfällen und tiefgehende Analysen** durchzuführen, **um** auf die Bedrohung **abgestimmte Reaktionen anzuwenden** . Auch wenn die Hersteller unterschiedliche Ansätze anbieten, können wir dennoch Ähnlichkeiten hinsichtlich der funktionalen Abdeckung feststellen, die ihre jeweilige Lösung bietet.

Diese Lösungen zeichnen sich daher zunächst durch die Vielzahl der Erkennungsquellen (Netzwerke, Arbeitsstationen, Server, die Benutzer, ...) aus, um anormale Verhaltensweisen zu identifizieren. Diese umfassende Sicht auf das System sorgt für eine leichtere Einsicht in das gesamte Ausmaß der Sicherheitsprobleme. Sie werden dann ihre verschiedenen Datensätze normalisieren, um die Informationen zu korrelieren und wichtige Zwischenfälle zurückzumelden.

Schließlich erleichtern die XDR-Lösungen die Verwaltung dieser Vorfälle, indem sie die Maßnahmen orchestrieren, die zur wirksamen Reaktion auf die Bedrohung ergriffen werden müssen. Diese Aktionen sind in Form von Reaktionsszenarien oder Playbooks zusammengefasst und sorgen dafür, dass die Sicherheitsteams in Echtzeit alarmiert werden, infizierte Computer isoliert werden oder die zur Wiederherstellung des Arbeitsplatzes erforderlichen Sanierungsmaßnahmen durchgeführt werden.

> *Die Vielzahl an zu schützenden Netzwerkpunkten und Endgeräten sowie eine uneinheitliche Sicherheitspolitik führen dazu, dass Unternehmen schlechter auf Angriffe reagieren können. Aus diesem Grund* ***bietet XDR eine zusätzliche Sicherheitsebene*** *als Ergänzung zu herkömmlichen Schutzlösungen"*
>
> - **SÉBASTIEN VIOU,**
> Direktor Product Management,
> Stormshield

Die Versprechungen von XDR *versus* Realität vor Ort

Eine Mehrheit der Hersteller von Cybersicherheitslösungen bietet heute XDR-Lösungen mit einer Philosophie an, die sich hauptsächlich auf die Erkennung und Reaktion auf Vorfälle stützt. Dieser Ansatz, der eine reaktive Haltung erfordert, muss die Schutzlösungen ergänzen, die das richtige Maß an Sicherheit bieten werden. Man wird also die Angriffsfläche präventiv begrenzen, um proaktiv auf die Bedrohung zu reagieren.

Die Integration dieser Schutzelemente in die Architektur der XDR-Lösung gewährleistet eine echte Synergie zwischen Proaktivität und Reaktivität. Neben dem Konzept der Prävention bieten Schutzlösungen auch die Möglichkeit, optimale und nachhaltige Antworten zu finden, indem sie das Sicherheitsniveau bei Bedarf erhöhen.

Damit die XDR -Lösung ihre Aufgabe erfüllen kann, muss sie außerdem so eng wie möglich in Ihre Systeme integriert werden, um Ihnen eine automatisierte Korrelation der Daten und eine angemessene Reaktion innerhalb Ihrer Infrastruktur bieten zu können.

Notwendiger Schutz

XDR richtet sich an alle Arten von Unternehmen.

Außer bei besonders gezielten Angriffen unterscheiden moderne Bedrohungen nicht spezifisch zwischen ihren Zielen. Jede Organisation, unabhängig von ihrer Größe und ihrer Branche, ist gefährdet.

Für Unternehmen mit Cyber-Teams

Da die XDR-Technologie die operativen Sicherheitsteams bei der Erkennung und Reaktion auf Bedrohungen unterstützt, kann sie keinen Wert schaffen, wenn kein SOC[2]-Team vorhanden ist, das sie einsetzt. Aus diesem Grund wurden die XDR-Lösungen historisch gesehen zuerst von großen Unternehmen eingeführt, die über die Mittel und die internen Fähigkeiten verfügten, ein SOC-Team zu unterhalten.

Durch die Weiterentwicklung der XDR-Lösungen konnten sie die Qualität der Erkennung und die Klarheit der gemeldeten Warnungen sowie die Anzahl und die Relevanz der vorgeschlagenen Abhilfemaßnahmen stetig verbessern.

Dadurch können die erforderlichen Personalinvestitionen und das Cyber-Know-how weiter reduziert werden.

Heutzutage kann eine XDR-Lösung die Sicherheit kleiner und mittlerer Unternehmen optimieren; allerdings immer nur unter der Voraussetzung, dass diese Unternehmen trotzdem über einige interne Fähigkeiten verfügen, um die Lösung zu betreiben. Da diese Unternehmen über weniger Mittel und Kompetenzen verfügen, können sie keine allzu hohen Integrationskosten tragen. Sie bevorzugen dann sogenannte „native" XDR-Lösungen, die ein komplettes, vorintegriertes und vom Anbieter kontrolliertes Paket liefern, das sowohl die für die Informationssammlung erforderlichen Agenten und Geräte als auch vorkonfigurierte Korrelations- und automatisierte Reaktionsmaschinen umfasst. Ein All-in-One-Ansatz für eine schnellere und einfachere operative Umsetzung.

Verwaltung über MSSP[1] sichert Unternehmen ohne interne SOC-Teams ab

Viele Unternehmen sind jedoch nicht in der Lage, ein internes SOC einzurichten und zu unterhalten und somit selbst eine XDR-Lösung einzusetzen.

In diesem Fall können sie sich an einen MSSP-Anbieter wenden, der über ein eigenes SOC verfügt, um die von der Infrastruktur seines Kunden gemeldeten Ereignisse zu verarbeiten und an seiner Stelle zu reagieren.

Man spricht dann von „Managed Detection and Response" (MDR).

Die SOCs dieser MSSP-Anbieter stehen vor denselben Problemen und verlassen sich selbst auf XDR-Lösungen, um ihnen zu helfen, effektiv auf ihre Kunden zu reagieren und gleichzeitig ihre Kosten im Griff zu behalten.

[1] **MSSP**: Akronym für Managed Security Service Provider auf Englisch.
[2] **SOC**: Akronym für Security Operations Center auf Englisch.

Ein SOC, was ist das?

Das SOC oder Security Operation Center bezeichnet die Umgebung, in der die für die Sicherheit einer Organisation zuständigen Teams arbeiten.

Zu den Hauptaufgaben der SOC-Teams zählen:

- Die Analyse von Ereignissen, die von Systemen und Infrastrukturen gemeldet werden, um Sicherheitszwischenfälle zu erkennen,
- und dann die Reaktion auf diese Vorfälle, um ihre Auswirkungen zu begrenzen oder sogar zu vermeiden.

Diese Aufgaben der Erkennung und Reaktion **erfordern eine ständige Wachsamkeit** der SOC-Teams, die angesichts der Masse an Informationen, die ständig verarbeitet werden müssen, der Gefahr ausgesetzt sind zu ermüden. Mit dem Ergebnis **einer geringeren Effizienz, aber auch einem hohen Risiko der Fluktuation**.

Ein Konzentrat aus mehreren Technologien

Das Akronym XDR steht für eXtended Detection and Response (erweiterte Erkennung und Reaktion) und bedeutet, dass die Erkennung und Reaktion die gesamte Bandbreite der zu schützenden Systeme und Infrastruktur abdeckt.

Lösungen wie EDR (Endpoint), NDR (Network) oder auch FDR (File) konzentrieren sich nur auf einen Teil der Umgebung. Diese verschiedenen Konzepte müssen jedoch in ihrer Gesamtheit betrachtet werden.

Dies liegt daran, dass eine XDR-Lösung Ereignisse aus einer Vielzahl von Quellen benötigt, um eine globale Abdeckung zu gewährleisten.

XDR stützt sich daher zwangsläufig auf diese verschiedenen Technologien.

Daher ist es wichtig, dass jedes dieser Elemente eine qualitativ hochwertige Rückmeldung von Ereignissen bietet. Um auch sehr schwache Signale zu erkennen, benötigt die XDR-Lösung sehr präzise Informationen von der Quelle über den gesamten Umkreis.

Dazu müssen die Technologien, die den XDR speisen, jeweils feine Analysen in ihrem eigenen Bereich durchführen. Beispiel:

- **Der EDR-Agent** muss das Verhalten der auf **dem Endpoint** ausgeführten Prozesse genau analysieren,
- **Die NDR-Ausrüstung** soll eine gründliche Tiefeninspektion (DPI-Deep Packet Inspection) der **Kommunikation** verschiedener **Netzwerke** wie IT-Informationssysteme, aber auch operativer OT-Netzwerke durchführen,
- **Und die FDR** muss detailliert analysieren, wie sich **eine Datei** in der Umgebung verhält, in der sie geöffnet wird.

Die Zusammenstellung eines qualitativ hochwertigen XDR muss daher die Leistung und Abdeckung aller Lösungen berücksichtigen, die dazu beitragen, und nicht nur das zentrale Gehirn des Geräts.

Bei der Zusammenstellung eines qualitativ hochwertigen XDR muss die Leistung und Abdeckung aller Lösungen berücksichtigt werden, die dazu beitragen, und nicht nur das zentrale Gehirn des Geräts.

Die wichtigsten Phasen des XDR-Ansatzes

1. Erkennung, Korrelation & Warnung

Schutzlösungen, egal ob sie auf das Netzwerk oder die Desktops abzielen, agieren oft in Silos, ohne ihr jeweiliges Wissen wirklich auszutauschen. Dies führt zu Problemen für Unternehmen und die Teams, die sie betreiben: Komplexe Angriffe passieren die Schutzfilter unerkannt und die Menge an Ereignissen, die manuell korreliert werden müssen, ist gigantisch.

Die Erwartungen an XDR-Lösungen decken genau diese Herausforderungen ab: Die Analyse und Korrelation der von den verschiedenen Lösungen ausgegebenen Logs zu automatisieren und die operativen Teams im Falle eines Sicherheitszwischenfalles zu alarmieren. Diese aus der Welt des SIEM[1] stammenden Funktionen ermöglichen es, anormale Situationen zu identifizieren, indem sie andere Faktoren berücksichtigen als die, die traditionell von Schutzlösungen verwendet werden.

Darüber hinaus gewinnen die Erkennung und Korrelation von Ereignissen an Bedeutung, wenn sie mit Funktionen für das Alarmmanagement kombiniert werden. Denn bei immer mehr Angriffen, die von Cybersicherheitslösungen besser erkannt werden, führt dies zu einer großen Anzahl von Situationen, die von den oft überforderten operativen Teams bewältigt werden müssen. Letztere äußern daher einen sehr operativen Bedarf: über Lösungen zu verfügen, die es ermöglichen, Warnungen zu erheben, indem sie ihnen eine Größenordnung des Zwischenfalles zuordnen. So können sie sich auf die kritischsten Warnungen konzentrieren, die eine sofortige Reaktion erfordern.

> So kann man z. B. durch die Betrachtung der Häufigkeit des Auftretens eines Ereignisses oder durch die Korrelation eines Verhaltens auf einer Arbeitsstation mit Netzwerkereignissen eine sehr unauffällige Datenexfiltration charakterisieren, die eine manuelle Analyse vielleicht nicht hätte erkennen können.

2. Reaktion und Wiederherstellung

Wo historische SIEM-Lösungen aufhören und nur Korrelation und Warnung abdecken, übernehmen XDR-Lösungen die Aufgabe, indem sie mehr Wert liefern.

Denn es reicht nicht aus, nur zu erkennen und zu warnen, sondern es muss auch eine angemessene Reaktion erfolgen. Die Herausforderung für Unternehmen besteht darin, Zwischenfälle so schnell wie möglich angemessen zu behandeln, um den Schaden zu begrenzen.

Die Erwartung der Sicherheitsteams besteht vor allem darin, die kritischsten Angriffe einzudämmen, um ihre Auswirkungen so gering wie möglich zu halten. Egal, ob es sich um eine lateralisierende Ransomware oder einen Datendiebstahl handelt, die Antwort muss so schnell wie möglich kommen.

Wenn also der Grad des Zwischenfalles sehr hoch ist, ist es operativ vertretbar, eine automatische Antwort in Betracht zu ziehen. Diese ermöglicht die Anwendung von angemessenen Reaktionsmaßnahmen auf die XDR-Warnungen, die den Sicherheitszwischenfall ausmachen.

Wenn das Ausmaß des Zwischenfalles jedoch geringer ist und das Risiko, die Infrastruktur zu blockieren, nicht neutral ist, bevorzugen die Unternehmen eine teilweise automatisierte Reaktion mit einer menschlichen Entscheidung.

Die Funktionen zur Reaktionsplanung stammen diesmal aus der Welt von SOAR[2] und ermöglichen es, Szenarien oder Playbooks im Voraus zu entwerfen und so viele Aufgaben wie möglich zu automatisieren, um die Entscheidungsfindung so einfach wie möglich zu machen und die Reaktion, obwohl technisch komplex, schnell umzusetzen.

Danach kommen wir zur Wiederherstellung. Ein notwendiger Schritt, dessen Ziele zum einen die Wiederherstellung einer gesunden Situation und zum anderen die Sicherstellung sind, dass die verwendeten Angriffsvektoren nun geschützt sind.

Die XDR-Lösung muss daher kompromittierte Assets identifizieren, sie in einen normalen Betriebszustand zurückversetzen, z. B. durch Wiederherstellung von Dateien, die bei einem Ransomware-Angriff verschlüsselt wurden, und schließlich den gesamten Kontext erfassen und wiedergeben, um ein mehrstufiges Eingreifen zu ermöglichen, um die Sicherheit zu erhöhen und künftige Angriffe zu verhindern.

[1] **SIEM**: Akronym für Security Information and Event Management auf Englisch.

[2] **SOAR**: Akronym für Security Orchestration, Automation and Response auf Englisch.

Operative Vorteile der XDR-Lösungen

Der XDR-Ansatz ermöglicht den verschiedenen Unternehmen einen umfassenden und orchestrierten Schutz vor den verschiedenen Bedrohungen.

Um diese Aufgabe erfolgreich zu bewältigen, ist es wichtig, die 4 wichtigsten betrieblichen Vorteile zu verstehen, die jede XDR-Technologie den für die Sicherheit zuständigen Teams bieten muss:

- 360°-Sichtbarkeit der Infrastruktur
- Schnelle Identifizierung der Bedrohung
- Zentrale Verwaltung von Vorfällen
- Automatisierung von Antworten

360°-Sichtbarkeit der Infrastruktur

Die XDR-Technologie soll einen umfassenden Einblick in die Sicherheit der Organisation verschaffen. Die Integration von Daten aus verschiedenen Quellen sorgt dafür, dass die Bedrohung überall von einer einzigen Konsole aus sichtbar ist, was die betriebliche Effizienz steigert.

Identifikation der Bedrohung

XDR-Lösungen müssen eine optimale Erkennung von abnormalem Verhalten für die verschiedenen Quellen gewährleisten. Sie müssen auch in der Lage sein, diese untereinander und mit dem CTI zu verbinden, um größere Zuverlässigkeit zu erreichen. Dadurch werden die Informationen für die Analysten rationalisiert, um ihnen ein besseres Verständnis des zu behandelnden Zwischenfalles zu ermöglichen.

Zentrale Verwaltung von Vorfällen

Angesichts der Vielzahl von Alarmen, mit denen die für das Security Operations Center oder SOC zuständigen Teams konfrontiert sind, müssen XDR-Lösungen die wichtigsten Vorfälle identifizieren und priorisieren, um die Entscheidungsfindung zu erleichtern. Die zentrale Verwaltung gewährleistet die Zusammenarbeit und den Informationsaustausch zwischen den Teammitgliedern, um die Effektivität des Bedrohungsmanagements zu erhöhen.

Automatisierung von Antworten

Indem sie je nach Zwischenfall passende Antworten anbieten, gewinnen die Analysten Zeit, um sich auf wertschöpfende Aufgaben zu konzentrieren. Ebenso müssen diese Antworten auf den am besten geeigneten Sicherheitsprodukten eingesetzt werden, um je nach Sicherheitszwischenfall die beste aller Lösungen anzuwenden.

Ansätze der verschiedenen Hersteller

Die Akteure auf dem XDR-Markt zeichnen sich vor allem durch ihren Heimatmarkt aus.

Hersteller von Arbeitsplatzschutzlösungen, wobei die Hersteller ihre Erkennungslösungen weiterentwickelt haben, indem sie andere Informationsquellen wie Netzwerkdaten einbezogen haben.

Hersteller, die vor allem in den Bereichen Netzwerksicherheit und Arbeitsplatzschutz tätig sind und die alle Ereignisse in einer speziellen Lösung korrelieren.

Hersteller, die Lösungen für das Zwischenfallmanagement (SIEM/SOAR) anbieten, die herstellerübergreifende Datenquellen aus dem Netzwerk, den Arbeitsstationen oder sogar dem Unternehmensverzeichnis integrieren.

Hersteller von Endpoint-Lösungen

EDR, EPP, AV

EDR ist ein ABLEGER von Endpoint Protection (EPP) und führt das Konzept der Reaktion auf den Arbeitsplatz ein, wobei es sich auf den historischen Markt der Windows-Computer konzentriert.

So setzen sich die Akteure aus dem Bereich des Endpunktschutzes für einen XDR-Ansatz ein, der sich auf Endgeräte (Tablets, PCs, Server oder auch Mobiltelefone) und seit kurzem auch auf Mobile EDR konzentriert. Auch wenn dieser Ansatz eine gute Kontrolle über mobile und nicht-mobile Arbeitsplätze gewährleistet, stellen wir dennoch fest, dass das „X" von XDR nur selten die Analyse von Netzwerkflüssen beinhaltet.

Andere Anbieter haben jedoch erkannt, dass es sinnvoll ist, sich an beiden Fronten zu positionieren: auf den Endgeräten und im Netzwerk. Um den Wert des Netzwerks zu steigern, erwerben einige die IPS-Technologie, die sich zu NDR[1] weiterentwickelt, um den Datenverkehr in Echtzeit zu analysieren und die ersten schwachen Anzeichen eines Angriffs zu erkennen. So kaufte Trend Micro beispielsweise 2016[2] TippingPoint, um seine Netzwerkstrategie zu stärken. Sie wurden dann zu gemischten Akteuren mit Fachwissen über die gesamte Kette.

Außerdem werden EDR-Spezialisten von Netzwerkspezialisten übernommen, wie wir weiter unten sehen werden.

Vorteile

- Starke geräteübergreifende Abdeckung (Handy, Tablet, PC, etc.)
- Sehr gute Erkennungsleistung für Windows
- Begriff der kontrollierten Mobilität (Cloud-Sammlung etc.)

Nachteile

- Keine Netzwerklösung verfügbar
- Mangelnde Sichtbarkeit eines Teils der Infrastruktur
- Wenig oder keine Netzwerkwiederherstellung
- Auf den Terminalbestand beschränkte Aktionen

[1] **NDR**: Akronym für Network Detection and Response auf Englisch.

Hersteller aus dem Bereich der Netzwerksicherheit

NDR, NGF//UTM

Diese Kategorie von Akteuren umfasst hauptsächlich Hersteller, die sich auf den Schutz von Netzwerken (Firewall, NG-Firewall) spezialisiert haben und Netzwerksondierungsfunktionen (NDR), Intrusion Prevention Systems (IPS/IDS) und Netzwerkfilter (Firewall) anbieten. Es gibt jedoch eine Einschränkung bei der Netzwerkerkennung, da es schwierig, wenn nicht gar unmöglich ist, verschlüsselte Datenströme zu analysieren.

Diese Hersteller bieten auch Lösungen zum Schutz von Desktops an, entweder nativ oder durch Übernahmen wie die von Palo Alto mit der Übernahme von Cyvera im Jahr 2014[2]. Dieser Ansatz erweitert die Erkennungsmöglichkeiten und sorgt so für einen umfassenden Überblick über die Infrastruktur.

Ihre Endpoint-Erkennungsfunktionen in Kombination mit Netzwerklösungen sorgen für bessere Abhilfefähigkeiten, indem sie sowohl auf die Kommunikationsströme als auch auf die Endgeräte einwirken. Außerdem bieten diese Hersteller in der Regel FDR[1]-Möglichkeiten über Sandboxing-Lösungen als Ergänzung bei der Suche nach Malware an, um die Analysepunkte zu vervielfachen.

Vorteile

- Erleichterte Bereitstellung
- Fähigkeiten zur Analyse von Netzwerkflüssen zu Cloud-Infrastrukturen
- Größere Handlungsfähigkeit (Flussunterbrechung)

Nachteile

- Im Sondenmodus, manchmal schwerfälliger Einsatz (Notwendigkeit, TAP-Modus hinzuzufügen)
- Problematik der TLS 1.3-Verschlüsselung
- Notwendigkeit der Entschlüsselung, um effektiv zu sein

[1] **FDR**: Akronym für File Detection and Response auf Englisch.

[2] **Quelle**: https://www.paloaltonetworks.com/blog/2014/03/palo-alto-networks-acquire-cyvera/

Hersteller aus dem Zwischenfallmanagement

SIEM/SOAR

In dieser Kategorie finden wir SIEM-Anbieter, die sich auf die Erkennung und Korrelation von Warnmeldungen spezialisiert haben.

Durch die Integration der Sammlung von Protokollen verschiedener Lösungen, die einen sehr großen Teil des Informationssystems abdecken, verfügen diese Plattformen über große Datenmengen aus den verschiedenen Systemen, die in der Infrastruktur vorhanden sind. Diese Herausgeber haben Werkzeuge entwickelt, um sie so zu verarbeiten, dass daraus abweichendes oder riskantes Verhalten hervorgehoben wird. Dadurch wird die Untersuchung von Vorfällen in den SOCs durch das von solchen Lösungen angebotene Zwischenfallmanagement erleichtert.

So sind SIEM-Anbieter von Haus aus Lösungen für die „Erkennung“ oder zumindest für die Verarbeitung bereits erkannter Daten. Es bleibt jedoch die Fähigkeit, Reaktionen hervorzubringen, was durch die Steuerung von Dritten über APIs ermöglicht wird. Die SOAR-Technologien wurden geboren. Daher sind die Erkennung, Reaktion und Interoperabilität mit allen Sicherheitsakteuren oder Anwendungen des Informationssystems ein zentraler Punkt einer XDR-Lösung, und es ist für die SIEM/SOAR-Hersteller selbstverständlich, ihre Produkte auf diesem Markt zu positionieren.

Es gibt jedoch einen Schatten auf diesem Bild: Die Fähigkeit, Sicherheitslösungen oder Informationssystem-Anwendungen zu verwalten. Neben der Integration von Protokollen, die ihr Hauptaufgabengebiet darstellt, erfordert die Einrichtung von Abhilfe-Regelsätzen (Playbook) ein umfassendes Wissen über Sicherheitslösungen. In diesem Bereich ist man weiterhin auf das Wissen der Anbieter angewiesen, die nach wie vor der Maßstab für das Fachwissen über Ihre Lösungen sind.

Außerdem sind solche Lösungen auf Erkennungsquellen von Drittanbietern angewiesen. Daher stellen SIEM/SOAR-Tools allein keine vollwertige XDR-Lösung dar.

Vorteile

- Abdeckung eines sehr großen Teils des IS
- Schließt Warnungen von Anwendungen ein
- Verwaltung von Zwischenfällen
- Häufig bereits auf IS für Sammelzwecke installiert

Nachteile

- Muss für Quellen auf Dritte zurückgreifen (Terminals, Netzwerke ...)
- Erforderliche Kenntnisse über mehrere Hersteller (SIEM/SOAR und Sonden)
- Begrenzte Kenntnisse über Sicherheitsprodukte

Welchem Ansatz sollte der Vorzug gegeben werden?

Der XDR-Markt ist in den letzten Jahren stark gewachsen und wir finden dort manchmal Akteure, die sich als **Pure Player** bezeichnen**.** In der Praxis haben wir beobachtet, dass XDR-Ansätze aus einer Reihe von Lösungen (Netzwerk, Endgeräte, Cloud usw.) bestehen, mit denen sich die Sichtbarkeit des gesamten Informationssystems erreichen lässt.

Denn im Gegensatz zu anderen aufstrebenden Märkten, die von neuen innovativen Technologien angetrieben werden, ist es für einen effektiven XDR-Ansatz schwierig, in mehreren Märkten gleichzeitig gut positioniert zu sein. Um als „Pure Player" bezeichnet zu werden, müsste ein Akteur ausgereifte Produkte sowohl für die Erkennung, für Endgeräte und Netzwerke, als auch im Bereich der Korrelation von Ereignissen, der Verwaltung von Zwischenfällen und der Abhilfe anbieten. Es ist also durchaus logisch, davon auszugehen, dass es keine XDR-Akteure im eigentlichen Sinne gibt und dass es angesichts der unterschiedlichen Philosophien und technischen Anwendungen der verschiedenen Akteure kompliziert ist, eine Technologie als „DAS ECHTE XDR" zu fördern.

Zusammenfassend lässt sich sagen, dass nur Akteure mit einem umfassenden gemischten Angebot sowie Pure Player im Bereich Zwischenfallmanagement den Anspruch erheben können, eine echte XDR-Lösung anzubieten. SIEM/SOAR-Lösungen bieten den Vorteil, dass sie einen sehr großen Teil des Informationssystems abdecken, wo Native Mixed Players mit dem tiefen Wissen ihrer Lösungen, die sowohl Endgeräte als auch Netzwerke abdecken, die Wirksamkeit von Korrelationsregeln und Szenarien für Abhilfemaßnahmen gewährleisten.

	Vorteile	Nachteile
ENDPOINT	**Starke Multi-Device-Abdeckung (Handy, Tablet, PC...)**	Keine Netzwerklösung verfügbar
	Sehr gute Erkennungsleistung für Windows	Mangelnde Sichtbarkeit eines Teils der Infrastruktur
	Konzept der kontrollierten Mobilität (Cloud-Sammlung, etc.)	Steuert keine Netzwerksonden
		Auf den Terminalbestand beschränkte Aktionen

	Vorteile	Nachteile
NETZWERK	**Wenn aus der Firewall kommend, einfacher Einsatz**	Im Sondenmodus, manchmal schwerfälliger Einsatz (Notwendigkeit, TAP-Modus hinzuzufügen)
	Fähigkeit, den Netzwerkfluss zu Cloud-Infrastrukturen zu analysieren	Problematik der TLS 1.3-Verschlüsselung
	Größere Handlungsfähigkeit (Flussunterbrechung)	Notwendigkeit der Entschlüsselung, um effektiv zu sein

	Vorteile	Nachteile
VERWALTUNG VON ZWISCHENFÄLLEN	**Sehr breite Abdeckung des Informationssystems**	Notwendigkeit, sich für Sonden an Dritte zu wenden (Terminals, Netzwerke ...)
	Verwaltung von Vorfällen	Begrenzte Kenntnisse über Sicherheitsprodukte

	Vorteile	Nachteile
GEMISCHT	**Umfassende Beherrschung von Sicherheitsprodukten zur Erkennung, Korrelation und Behebung von Missständen**	

Stormshield XDR für den optimalen Schutz

MAÎTRISE • PRODUCTIVITÉ • COHÉRENCE

Die Stormshield XDR-Lösung sichert Ihr gesamtes Informationssystem.

Stormshield XDR reduziert Cyberrisiken und erhöht gleichzeitig die Produktivität der Sicherheitsanalysten. Es ergänzt den proaktiven Schutz und sorgt so für eine optimale Sicherung Ihrer Vermögenswerte.

Profitieren Sie außerdem von einem zentralen Punkt, von dem aus Sie Ihre gesamte Sicherheit überwachen können: Auf der Grundlage der Erkennung und Korrelation von Daten aus verschiedenen Quellen (Endgeräte, Netzwerke und Dateien) können Sie je nach Kontext des Zwischenfalles schnell die am besten geeigneten Reaktionselemente anwenden, um eine schnelle und wirksame Abhilfe zu schaffen.

Ebenso schließt die native XDR-Lösung von Stormshield die Lücken, die bei der Integration heterogener Sicherheitslösungen entstehen. Dies ermöglicht eine umfassende All-in-One-Lösung für Ihre Infrastruktur.

So begleitet Sie Stormshield, um eine kontrollierte Integration Ihrer XDR-Lösung so nah wie möglich an Ihrer Infrastruktur durchzuführen, um mehr Sicherheit und Leistung zu erreichen.

Steigern Sie die Cyber-Betriebseffizienz Ihrer Infrastruktur mit einer vertrauenswürdigen europäischen Lösung.

Mit Stormshield XDR sind Sie jederzeit geschützt

Kontrollieren Sie alle Elemente Ihrer Infrastruktur

Zentrale Verwaltung von Sicherheitszwischenfällen

Reagieren Sie effektiv auf Sicherheitszwischenfälle

Die 100% vertrauenswürdige europäische Lösung

Die Stormshield XDR-Lösung

ERKENNT
ORCHESTRIERT
REAGIERT

Stormshield
Endpoint Security

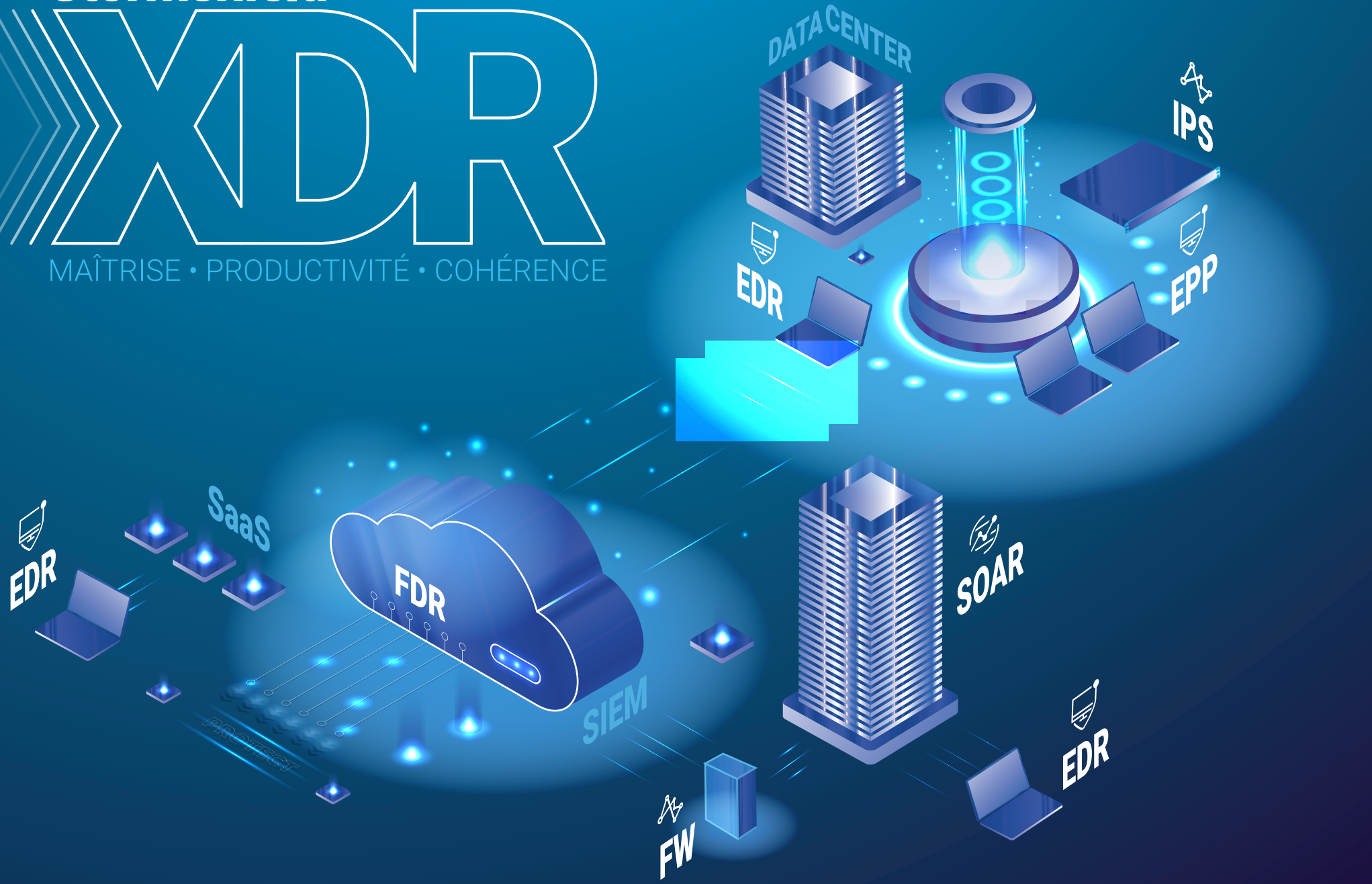
Stormshield
Network Security

Stormshield
Cyber Threat Intelligence

Stormshield

XDR

MAÎTRISE • PRODUCTIVITÉ • COHÉRENCE



DIE **EUROPÄISCHE WAHL** FÜR **CYBERSICHERHEIT**

www.stormshield.com