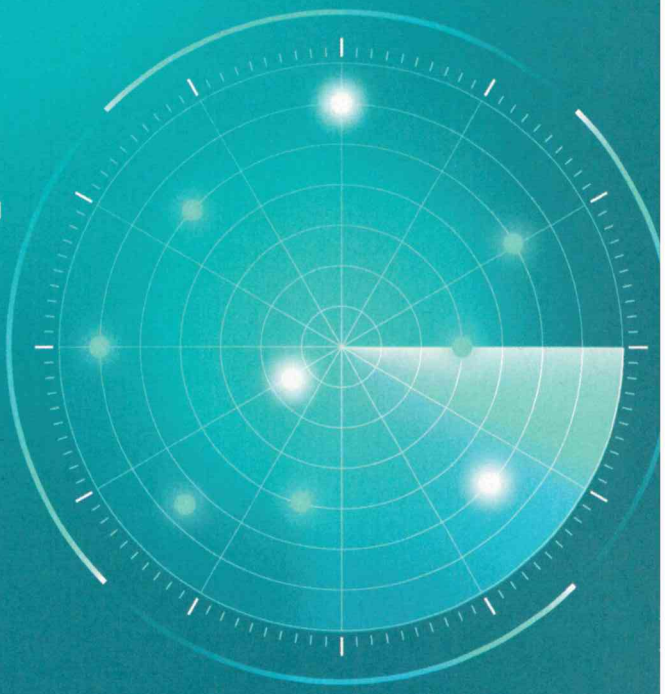
Endpoint Detection and Response:
Gefahren schnell erkennen und reagieren

Auf dem Radar

Konstantin Bücheler, Martin Hartmann, Alain Rödel, Stefan Strobel



Aus den einst simplen Virenscannern, die heutigen Sicherheitsanforderungen nicht mehr genügen, sind komplexe Produkte zum Schutz der Endgeräte im Netz entstanden. *iX* hat sich den üppigen Markt der EDR-Produkte angeschaut.

Sicherheitsvorfälle wie der Angriff auf den IT-Dienstleister Kaseya oder der Hackerangriff Sunburst auf die IT-Überwachungs- und Managementsoftware SolarWinds Orion, der auch zahlreiche US-Ministerien und-Institutionen zum Ziel hatte, verdeutlichen die Grenzen heutiger IT-Sicherheitsmaßnahmen eindrucksvoll. In beiden Fällen handelte es sich um einen Supply-Chain-Angriff, bei dem der eigentliche Schadcode über den Updateprozess des angegriffenen IT-Dienstleisters weiterverteilt wird.

Rein präventive Sicherheitsmaßnahmen allein können Unternehmen also nicht ausreichend vor gezielten Angriffen schützen. Einem professionellen Angreifer mit genügend Ressourcen fällt es nicht schwer, solche Maßnahmen zu umgehen oder zu deaktivieren. Das frühzeitige Erkennen einer Kompromittierung der eigenen Infrastruktur und das Reagieren darauf wird daher immer wichtiger.

Prävention als Voraussetzung

Natürlich bedeutet das nicht, dass Produkte zur Prävention von Angriffen überflüssig sind. Während Maßnahmen zum Verhindern von Malware- und Hackerangriffen rein automatisiert ablaufen, müssen Alarme von Erkennungsprodukten manuell analysiert und verifiziert werden. Filtert die präventive Maßnahme nicht bereits einen großen Teil heraus, übersteigt die Anzahl der Alarme schnell die personellen Kapazitäten, die sich eine Organisation leisten kann.

Früher setzte man zur Erkennung von Angriffen auf Intrusion-Detection-Systeme (IDS), was sich in den meisten Fällen aber als nicht sehr effizient herausstellte. Ähnlich wie bei herkömmlichen AV-Produkten basierten diese Systeme auf Angriffssignaturen, die professionelle Angreifer leicht umgehen konnten. Außerdem führten viele Fehlalarme zu einem enormen Betriebsaufwand.

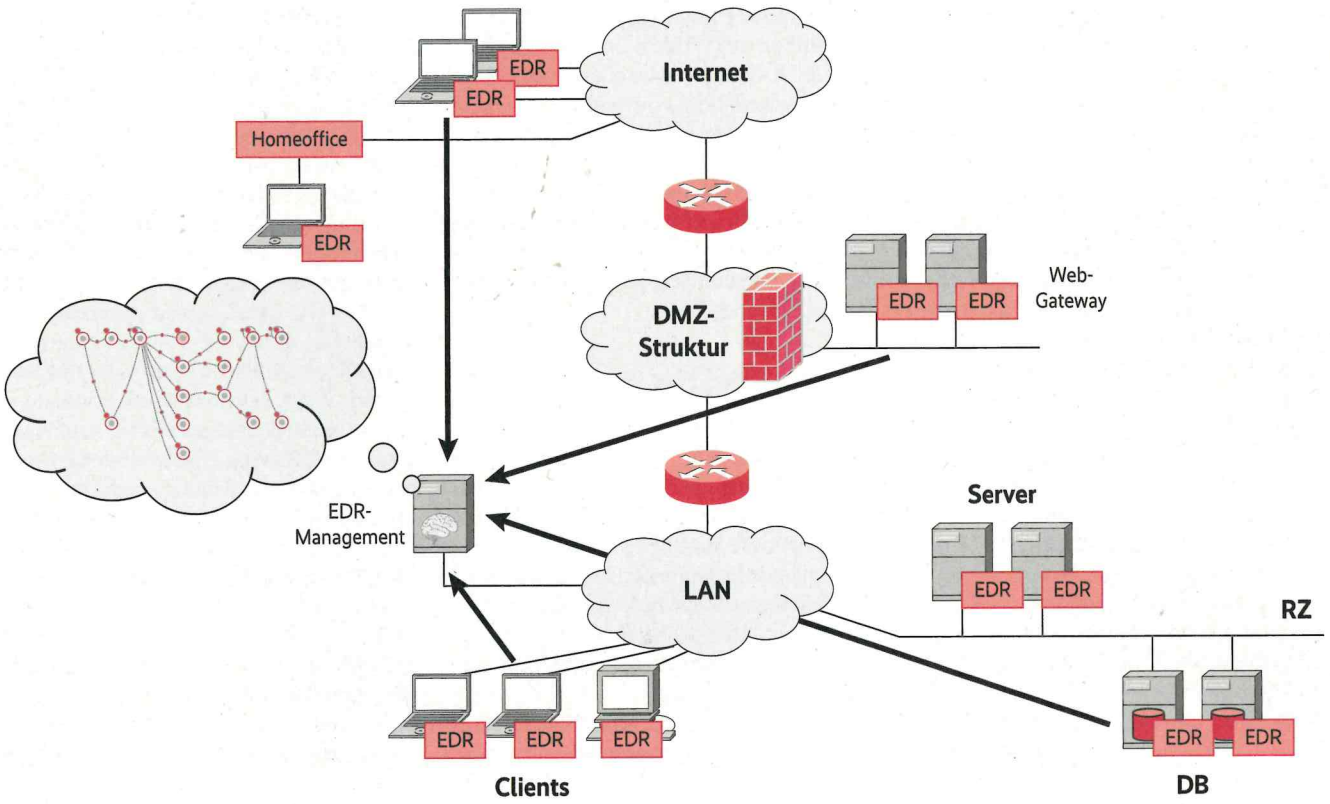
Danach kamen vermehrt Security-Information-and-Event-Management-Systeme (SIEM) zum Einsatz, die Events aus verschiedenen Quellen korrelieren, um eine bessere Erkennung zu erreichen. Aber auch hier schreckte das Verhältnis zwischen Aufwand und Nutzen vor allem kleinere Unternehmen ab. Viele entschieden sich deshalb dafür, ein SIEM als Service einzukaufen, das von Externen verwaltet wird. Andere Unternehmen, die selbst ein SIEM betreiben wollen, stehen nun vor der großen Herausforderung, all die Alarme zu analysieren und zu bearbeiten, was viel Zeit beansprucht. Ein wichtiger Teil dabei besteht in der meist sehr aufwendigen Rekonstruktion von Kontextdaten, die aufklären sollen, was auf einem kompromittierten Endgerät wirklich geschehen ist.

EDR und XDR

Derzeit kommen immer mehr Produkte mit der Bezeichnung Endpoint Detection and Response (EDR) oder Extended De-

iX-TRACT

- Gegen heutige gezielte und komplexe Angriffe reichen präventive Sicherheitsmaßnahmen nicht mehr aus. Je früher ein Unternehmen einen Angriff auf die eigene IT erkennt, desto besser lässt sich der Schaden begrenzen.
- Ältere Systeme wie IDS oder Virenschutz können leicht umgangen werden und produzieren zu viele Fehlalarme. Außerdem benötigen viele Sicherheitssysteme einen hohen Aufwand für manuelle Analysen.
- Neuere Ansätze wie EDR und XDR sammeln und interpretieren zahlreiche Daten, um teils automatisiert auf Unregelmäßigkeiten zu reagieren, Fehlalarme zu minimieren und den Betriebsaufwand möglichst gering zu halten.



Bei EDR sammeln die auf den Endgeräten installierten Agenten Informationen zu allen Prozessen und reagieren anhand der mitgelieferten vordefinierten Regeln sowie mit KI-Mechanismen auf außergewöhnliche Ereignisse (Abb. 1).

tection and Response (XDR) auf den Markt. EDR verfügt meist über einen Agenten, der direkt auf den Endgeräten installiert wird und dort das Verhalten sämtlicher Prozesse beobachtet (Abbildung 1). Dabei geht es nicht um das Verhalten der Anwender, sondern um technische Vorgänge wie den Zugriff auf Dateien und die Registry, die Netzwerkkommunikation, das Starten und Stoppen von Prozessen, die Manipulation von Arbeitsspeicher und vieles mehr.

Bei XDR werden zusätzliche Sensoren im Netzwerk platziert, um noch mehr Telemetriedaten zu erfassen (Abbildung 2). Sämtliche Informationen werden zentral gesammelt und im Gesamtbild betrachtet, meist unter Einsatz moderner KI-Methoden. Sofern solche Produkte ein Verhaltensmuster entdecken, das auf das Vorhandensein von Malware oder auf Angriffe hindeutet, lösen sie Alarm aus. Im Gegensatz zu einem SIEM-Produkt, dem meist sehr viel weniger Details zu Verfügung stehen, hat ein EDR-Werkzeug die Detailinformationen des Endgeräts und kann sie im Gesamtkontext bewerten.

Dem EDR-Werkzeug stehen damit Informationen über komplette Angriffsketten zur Verfügung. Beispielsweise lässt sich mit ihm nachvollziehen, woher ein ausführbares bösartiges Programm kam, wer es gestartet hat, auf welche anderen Systeme es zugegriffen und mit welchen anderen Prozessen oder Dateien es interagiert hat. Der Knackpunkt dabei ist, dass diese Daten nicht manuell von einem Sicherheitsexperten ausgewertet und keine eigenen Regeln definiert werden müssen. Die EDR-Software wird bereits mit einem Regelsatz ausgeliefert, den die Hersteller regelmäßig mit Updates versorgen. Andere Zusammenhänge stellt das Produkt mithilfe von maschinellem Lernen automatisch her.

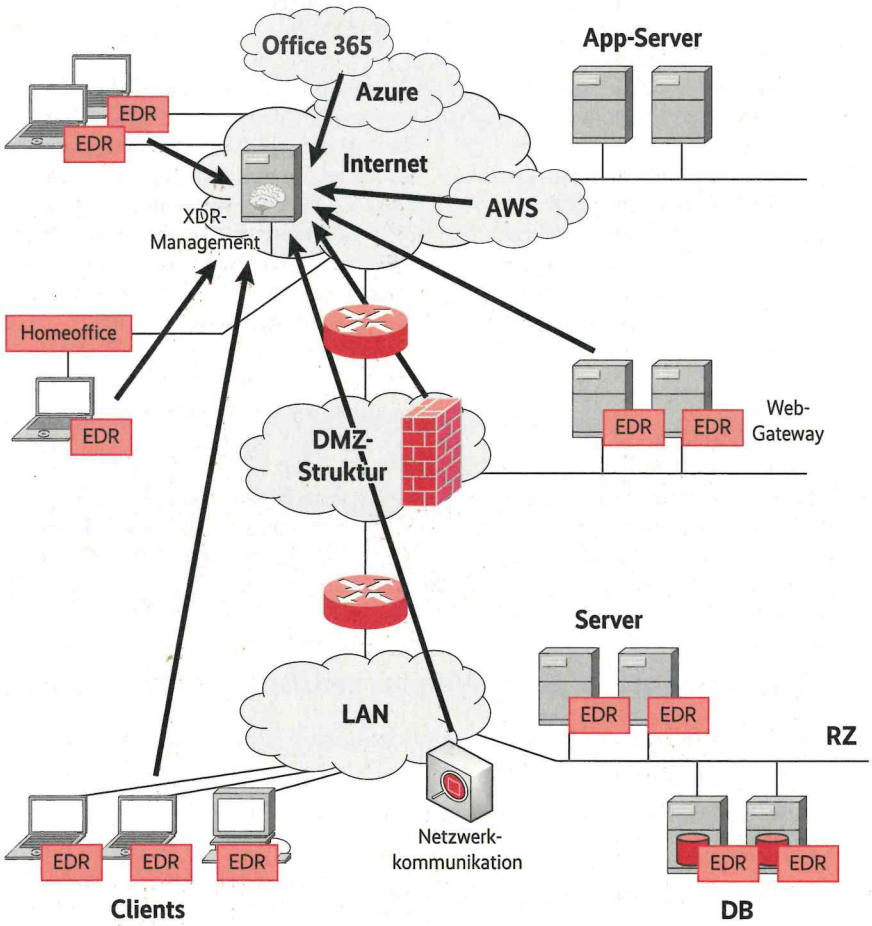
Ein EDR-Produkt kann damit Kompromittierungen auf Endgeräten genauer und zuverlässiger erkennen als klassische Ansätze. Organisationen, die EDR bereits eingeführt haben, um damit SIEM-Alarme zu verifizieren, stellen fest, dass das Produkt nicht nur zur Verifikation hilfreich ist, sondern sogar eine primäre Quelle für die Erkennung wird. Die erkannten Verhaltensmuster können auf verschiedene Techniken und Taktiken der MITRE-ATT&CK-Matrix (siehe ix.de/zmtg), einer Wissenssammlung von Angriffsinformationen, abgebildet werden und ermöglichen so eine standardisierte Einordnung (Abbildung 3). Die Non-Profit-Organisation MITRE evaluiert zudem regelmäßig und auf transparente Weise die Erkennungsleistung verschiedenster EDR-Produkte auf technischer Ebene.

Verzahnung mit dem Betriebssystem

Um verdächtiges Prozessverhalten frühzeitig und zuverlässig zu erkennen, muss ein EDR tiefe Einblicke in das Betriebssystem und alle laufenden Prozesse haben. Bei Windows-Systemen wird das im Allgemeinen durch das Laden einer DLL in jeden laufenden Prozess erreicht. Dadurch können Prozessaktivitäten überwacht und analysiert werden. Zusätzlich werden Zugriffe und Änderungen der Windows-Registry überwacht, da bestimmte Einträge darin auch für Angriffe verwendet werden. Beispielsweise kann mithilfe des Eintrags „Image File Execution Options“ (IFEO) ein bösartiger an einen gutartigen Prozess angehängt werden. Das ist ein bekanntes Vorgehen, Persistenz auf einem System zu erreichen oder die Privilegien zu erhöhen.

Mithilfe der Überwachung von Dateizugriffen lässt sich typisches Verhalten von Ransomware erkennen. Ein möglicher Auslöser für einen Alarm könnte beispielsweise sein, dass viele Dateien innerhalb kurzer Zeit gelöscht oder verschlüsselt werden. Auch das Löschen von Schattenkopien ist ein deutlicher Hinweis auf Ransomware-Aktivität. Ein weiterer Ansatz bei der Erkennung sind Deception-Techniken: Einige Produkte platzieren sogenannte Canary-Dateien an unterschiedlichen Stellen auf dem Endgerät und stellen einer potenziellen Schadsoftware dadurch Fallen. Sobald eine Malware oder Ransomware darauf zugreift, diese Dateien löscht oder verschlüsselt, löst das Produkt Alarm aus. Besonders interessant an dieser Technik ist, dass sie in der Praxis so gut wie keine Fehlalarme erzeugt und damit der Betriebsaufwand minimal ist. Bei den Canary-Dateien handelt es sich meist um versteckte Dateien mit kryptischem Namen. Andere Produkte verstecken diese Dateien bewusst nicht, da gewisse Ransomware-Software versteckte Dateien absichtlich überspringt.

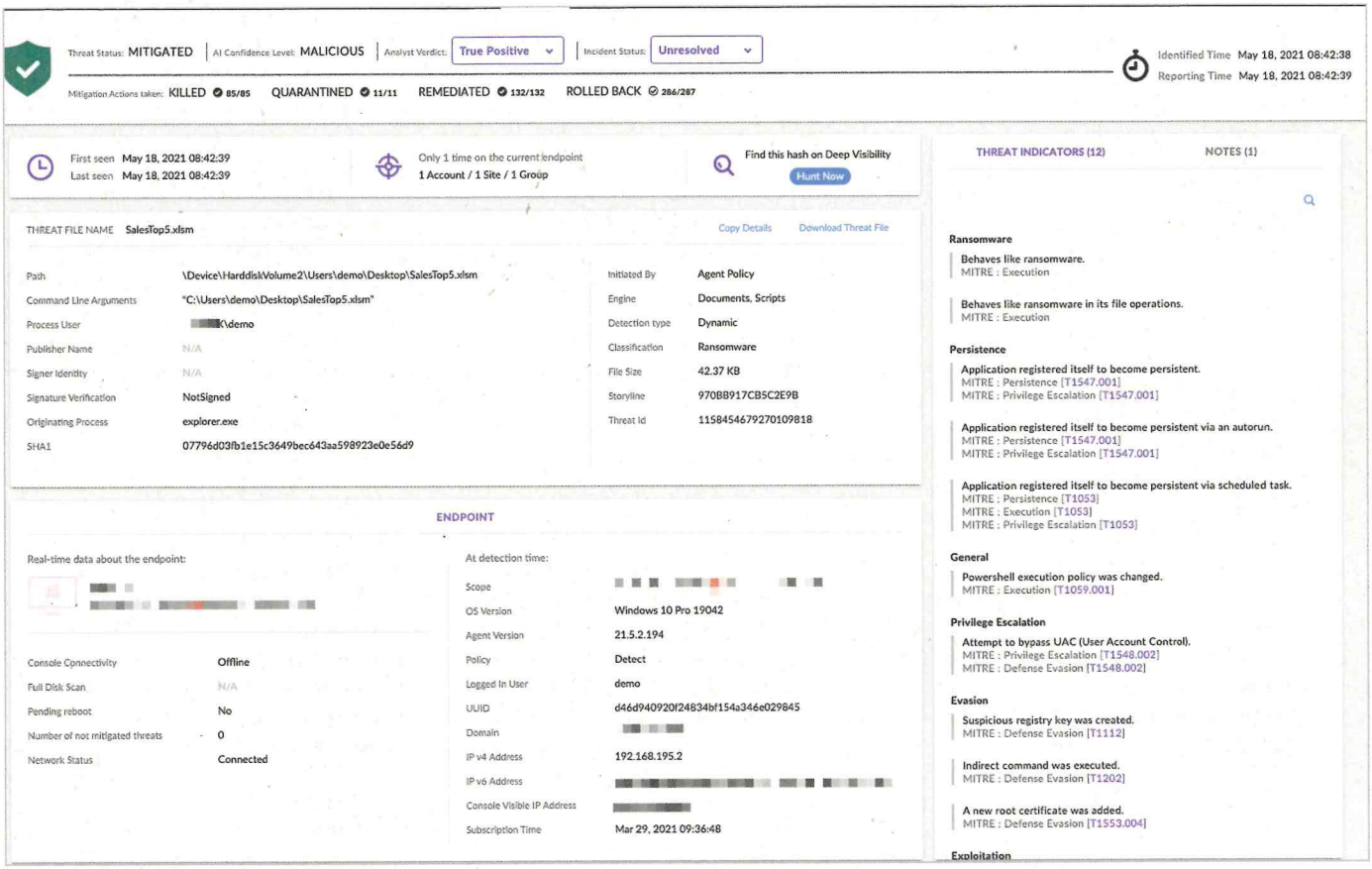
Beim Überwachen der Netzwerkkommunikation unterscheiden sich die Produkte stark. Einige Hersteller setzen hierbei auf eine protokollspezifische Deep Packet Inspection (DPI). Dabei wird sowohl der Inhalt als auch der Header von Netzwerkpaketen analysiert. Andere Hersteller hingegen überwachen die Netzwerkkommunikation ausschließlich auf Grundlage der Metainformationen von Verbindungen.



Zusätzliche Telemetriedaten liefern die bei XDR im Netzwerk platzierten Sensoren. Aus der Gesamtheit der Informationen lassen sich Angriffsmuster erkennen, auf die das Werkzeug reagieren kann (Abb. 2).

Nächster Schritt: Incident Response

Wie der Name EDR bereits suggeriert, beobachten und korrelieren die Produkte nicht nur das Verhalten der Prozesse, sondern bieten auch Funktionen zur Reaktion auf Vorfälle. Zu den Standardreaktionen vieler Produkte gehört das Beenden des schadhaften Prozesses und aller von ihm erzeugten Unterprozesse. Falls sich der Angreifer aber bereits durch eine Persistenztechnik auf dem System eingenistet hat, ist die Gefahr durch das alleinige Beenden von Prozessen nicht abgewendet. Einige Produkte bieten deshalb Funktionen zur netzwerkseitigen Isolation des in-



Bei SentinelOne sind rechts die Referenzen zur MITRE-ATT&CK-Matrix dargestellt. Im Beispiel ist der Alarm eines Ransomware-Vorfalls zu sehen, der durch die im Produkt enthaltene Rollback-Funktion bereits behoben ist (Abb. 3).

fizierten Geräts an, um zu verhindern, dass sich das Programm im Netzwerk weiterverbreitet. Im isolierten Zustand ist lediglich die Kommunikation zur Managementkonsole möglich.

Nun können Sicherheitsfachleute das Prozessverhalten nachvollziehen und die nächsten Schritte einleiten. Die meisten EDR-Produkte sind an dieser Stelle im Funktionsumfang erschöpft. Einige Anbieter erlauben allerdings das Zurückrollen von Änderungen auf dem Dateisystem und der Registry, das Erstellen von Speicherabbildern zur forensischen Untersuchung oder den Zugriff auf eine Remote-Konsole, die die Investigation auf dem potenziell infizierten System ermöglicht. Die Grenze zwischen einem Werkzeug für die Erkennung und einem für Incident Response und Live-Forensik verschwimmen dabei.

Neben den Reaktionsfähigkeiten bieten viele Produkte auch eine aktive und automatisierte Suche nach Anzeichen einer Kompromittierung (Indicators of Compromise; IoC) oder eines Angriffs (IoA), was oft als Hunting bezeichnet wird. Die Hersteller bieten dazu entweder eigene Threat-Intelligence-Feeds an, über die Hashwerte bekannter Malware-Dateien, IP-Adressen von Command-and-Control-Servern (C&C) oder Registry-Einträge von Malware geliefert werden, oder das Produkt verfügt über Schnittstellen, über die sich eigene und öffentliche Threat-Intelligence-Quellen einbinden lassen. Auch an diesem Punkt beginnen EDR-Werkzeuge, sich mit einem SIEM zu überschneiden.

Die zentralen EDR-Konsolen zum Verwalten der Events und Reagieren auf Alarme bieten meist aufwendig gestaltete Dashboards, die eine große Fülle an Informationen darstellen. In Form von Prozessaufrufbäumen und Zeitachsen werden Vorfälle detailliert visualisiert, sodass die Experten die Aktionen potenzieller Malware genau nachvollziehen und darauf reagieren können (Abbildung 4). Viele der Dashboards bieten zudem die Möglichkeit, automatisch generierte Reports zu Incidents und Statistiken zu erstellen. Das Dashboard ist also, ergänzend zu den APIs, die zentrale Möglichkeit, die Vorfälle zu überwachen und zu bewerten.

Ist ein Dashboard jedoch nicht übersichtlich und intuitiv zu bedienen, kann ein EDR-Produkt eine noch so gute Erkennungsrate haben: Wenn die Auswertung der Alarme zu kompliziert ist, bringt das Produkt keinen entscheidenden Mehrwert. Die Hersteller müssen also einen Kompromiss zwischen Übersichtlichkeit, Detaillierungsgrad und Zusatzinformationen finden, um die Arbeit der Sicherheitsexperten zu erleichtern.

Zur Marktübersicht

Um die Informationsgrundlagen für einen Überblick der am Markt befindlichen Produkte zu erhalten, wurde den Herstellern ein Fragebogen zugesendet. Die Tabelle in diesem Artikel wurde auf Basis der Angaben der Hersteller sowie nach Recherchen der Autoren erstellt. Es fand kein praktischer Test der einzelnen Produkte statt. Eine qualitative Bewertung der Produkte und Funktionen lässt sich aus dem Überblick daher nicht ableiten. Nicht alle kontaktierten Hersteller haben den Fragebogen beantwortet, zum Beispiel FireEye, Check Point, VMware, Fidelis und Elastic. Außerdem konnten in einzelnen Fällen bestimmte Informationen aufgrund missverständlicher oder unvollständiger Antworten nicht in die Tabelle aufgenommen werden. Die vollständige Tabelle ist über ix.de/zmtg zugänglich.

Zusammenspiel mit Endgeräteschutz

Obwohl sich viele der im Artikel beschriebenen Techniken bei den meisten Anbietern am Markt wiederfinden, interpretiert jeder Hersteller EDR anders. Während manche Produkte nur in Kombination mit der klassischen End-

Überblick über die Hersteller und ihre Entwicklung

Bitdefender: Das erste AV-Produkt von Bitdefender wurde bereits im Jahr 1996 unter dem Namen AVX von der rumänischen Firma Softwin auf den Markt gebracht. 2001 entstand der Markenname Bitdefender, unter dem 2007 eine eigene Firma ausgegründet wurde. Das heutige Produkt wird unter dem Namen GravityZone vermarktet und bietet diverse Funktionen wie Antivirus, Endgerätehärtung, Device-Kontrolle, Anwendungskontrolle und EDR.

BlackBerry ist hauptsächlich als Telefon- und MDM-Anbieter bekannt. Durch die Akquise von Cylance – einem Spezialisten für Malwareschutz auf Basis künstlicher Intelligenz – erweiterte der Hersteller im Jahr 2019 sein Produktportfolio und fokussiert sich seitdem verstärkt auf IT-Security-Produkte. Das bekannteste Malwareschutz-Produkt des Herstellers konzentriert sich auf die Klassifikation von Dateien mit KI-Methoden, es gibt jedoch auch ein Zusatzprodukt für EDR namens Optics.

Check Point wurde 1993 in Israel gegründet und ist insbesondere für den Bereich Netzwerksicherheit bekannt. Neben Firewall- und VPN-Produkten bietet der Hersteller auch einen Agenten für Endgeräte an. Harmony Endpoint (ehemals SandBlast Agent) wird als umfassendes Next-Gen-Antivirus-Programm beworben, das auch EDR-Funktionen enthält.

CrowdStrike wurde 2011 unter anderem von George Kurtz und Dmitri Alperowitsch (ehemals McAfee) gegründet. Die ersten Produkte von CrowdStrike waren einerseits Threat-Intelligence-Services mit Hintergrundinformationen zu Angreifern, ihren Werkzeugen und Techniken, und andererseits ein Produkt für Endpoint-Security, das schon damals seinen Fokus auf die Überwachung von Prozessen auf dem Endgerät richtete und dabei alle Informationen in der Cloud von CrowdStrike verarbeitete. Es wurde unter anderem um proaktive Schutzfunktionen und Offlineschutz erweitert, legt seinen Schwerpunkt aber weiterhin auf Erkennung und Reaktion zusammen mit diversen Managed Services.

Cisco Systems wurde bereits 1984 gegründet und ist vor allem als Hersteller von Netzwerkgeräten bekannt. Das Unternehmen bietet seit der Akquisition von Sourcefire im Jahr 2013 auch Produkte für die Endgerätesicherheit an. EDR-Funktionen stecken dabei in AMP for Endpoints. Durch die Integration in die SecureX-Plattform lassen sich Informationen aus den unterschiedlichen Produkten korrelieren und gemeinsam verwalten.

Cybereason ist ein Anbieter, der sich seit seiner Gründung 2012 in Israel auf die Prozessverhaltensanalyse beziehungsweise EDR konzentriert. Heute hat das Unternehmen seinen Sitz in Boston.

Cynet wurde 2015 in Tel Aviv gegründet. Das Portfolio umfasst neben der XDR-Lösung auch Next-Gen-Antivirus-Produkte sowie Programme zur Überwachung von Nutzerverhalten und Netzwerkkommunikation.

Elastic wurde 2012 in den Niederlanden unter dem Namen Elasticsearch gegründet und ist hauptsächlich bekannt für die Entwicklung des ELK-Stacks (Elasticsearch, Kibana, Beats und Logstash), der als Open-Source-Plattform von diversen Logging- und Visualisierungs- sowie in SIEM-Produkten genutzt wird. 2019 hat das Unternehmen Endgame aufgekauft und dessen Endpunkt-Security, die auf dem ELK-Stack basiert, in das eigene Produktportfolio integriert.

ESET: Die Geschichte dieses Unternehmens geht zurück auf Einzelpersonen, die schon Ende der 80er-Jahre Virenschutzsoftware in der ehemaligen Tschechoslowakei entwickelt haben. 1992 gründeten sie die Firma ESET und 1998 kam mit NOD32 ihr erster Virenschutz für PCs auf den Markt. Die Firma ist nach wie vor in Privatbesitz und in Bratislava ansässig.

Fidelis Cybersecurity: Fidelis wurde 2002 gegründet und konzentrierte sich zunächst auf Netzwerk-Appliances mit Deep-Packet-Inspection-Features zur Erkennung von Datenabflüssen und Kompromittierung im Netzwerk. 2012 wurde das Unternehmen an General Dynamics verkauft und 2015 von einer Investmentfirma wieder herausgekauft. Das Endpunkt-Produkt basiert ursprünglich auf einer Software von Access Data. Dieser Geschäftsbereich wurde 2014 von Access Data als eigenständige Firma mit dem Namen Resolution1 herausgelöst und 2015 von Fidelis aufgekauft.

FireEye: Bereits 2004 gegründet, entwickelte FireEye zunächst ein Produkt zur Sandbox-Analyse. Es kam 2010 auf den Markt und erlaubte es, Dateien in einer gesicherten Umgebung zu öffnen, um ihr Verhalten zu beobachten. 2014 übernahm FireEye die Firma Mandiant, die zuvor vor allem als Anbieter für Incident Response und Forensik bekannt war und zu diesem Zweck auch eine Software entwickelt hatte. FireEye bietet mittlerweile ein umfangreiches Produktportfolio einschließlich XDR-Funktionen an.

Fortinet ist ein Anbieter verschiedenartiger Produkte im Kontext der IT-Sicherheit. Sein Portfolio umfasst diverse Firewall- und Netzwerkkomponenten sowie Software für Identity- und Access-Management. Im Jahr 2019 kaufte Fortinet die Firma Ensilo auf, von der das heutige EDR-Produkt stammt.

F-Secure: Die finnische Firma wurde 1988 unter dem Namen Data Fellows gegründet und brachte 1994 ihr erstes Virenschutzprodukt auf den Markt. 1999 änderte das Unternehmen seinen Namen in F-Secure und gehört bis heute zu den etablierten Herstellern von Antivirensoftware. Seit 2018 bietet das Unternehmen auch ein EDR-Produkt an.

Kaspersky: Die Wurzeln des Virenschutzes von Kaspersky reichen zurück ins Jahr 1989, als Eugene Kaspersky als Hobby begann, sich mit Virenschutz zu beschäftigen und eine erste Software zu entwickeln. 1992 wurde sein Produkt unter dem Namen Antiviral Toolkit Pro von der Firma

point-Protection-Plattform (EPP) desselben Herstellers sinnvoll funktionieren, stellen andere die Analysefunktionen weitgehend autark bereit. Die enge Verzahnung zwischen EPP und EDR ermöglicht es, schädliches Verhalten schon früher zu erkennen und automatisch zu verhindern – beispielsweise, wenn das mit einem Prozess berechnete Sicherheitsrisiko einen bestimmten Schwellenwert erreicht. Das kann in der Praxis zu einem erhöhten präventiven Schutz, aber auch zu einer erhöhten an Anzahl False Positives führen.

Hersteller, die ihr EDR-Produkt losgelöst von präventiven Maßnahmen anbieten, setzen den Fokus meist stärker auf die individuelle Reaktion auf Vorfälle. Hier liegt die Annahme zugrunde, dass bereits vorhandene Schutzmaßnahmen umgangen wurden und somit vermutlich eine professionelle Malware aktiv ist. In diesem Fall sind automatisierte Blockaden weniger zweckdienlich. Stattdessen erhält der Analyst einen umfassenden Werkzeug-

KAMI vermarktet. Die Firma Kaspersky Lab wurde im Jahr 1996 in Russland gegründet. Heute gehört Kaspersky zu den weltweit größten Anbietern im Virenschutzmarkt.

Malwarebytes wurde 2008 gegründet und hat den Firmenhauptsitz in Santa Clara, Kalifornien. Laut eigenen Angaben entstand Malwarebytes aus einem Hobbyprojekt von Marcin Kleczynski, der sich selbst das Programmieren beibrachte, nachdem sein Computer von Schadsoftware befallen wurde.

McAfee wurde 1987 von John McAfee gegründet und vermarktete sein Virenschutzprogramm ursprünglich als Shareware. Der Gründer zog sich nach dem Börsengang im Jahr 1994 aus dem Unternehmen zurück. 1997 schloss sich McAfee mit Network General als Network Associates (NAI) zusammen, trennte sich aber später wieder von deren Geschäftsbereich und änderte den Namen zurück auf McAfee. 2011 kaufte Intel die Firma McAfee, verkaufte jedoch 2017 wieder die Mehrheit an die Investoren. Seit März 2021 ist bekannt, dass McAfee seine Geschäftskundensparte an die Symphony Technology Group verkaufen wird.

Microsoft: Als Hersteller von Windows spielt Microsoft eine besondere Rolle. Vor dem Erscheinen von Windows 10 wurde der Virenschutz von Microsoft oft belächelt. Das Unternehmen kaufte diverse Konkurrenzprodukte auf, um sie zunächst auf Eis zu legen (2003 GeCAD, 2005 Sybari). Seit 2017 erweiterte Microsoft seinen Virenschutz jedoch massiv. Seitdem findet man den kostenlosen Defender AV auch immer häufiger in Tests und Vergleichen von Virenschutzprogrammen auf einem der vorderen Plätze. Dazu kommt, dass Windows 10 neben dem Defender AV viele weitere kostenlose Sicherheitsfunktionen wie AppLocker oder Exploit Guard enthält. Der Defender für Endpunkt (früher Defender ATP) als EDR und zentrales Management für AV ist beispielsweise in der E5-Lizenz enthalten.

Palo Alto Networks hatte zunächst wenig mit Endgerätesicherheit zu tun. Die Firma wurde im Jahr 2005 von Nir Zuk gegründet, der einer der ersten Firewall-Entwickler bei Check Point war, und konzentrierte sich ausschließlich auf Firewalls. Das Endpoint-Security-Produkt von Palo Alto wurde ursprünglich von der Firma Cyvera entwickelt und hatte seinen Schwerpunkt im Bereich Exploit Mitigation. Cyvera wurde 2014 von Palo Alto übernommen und seither stark erweitert. Das Produkt Cortex-XDR von Palo Alto basiert auf einer Zusammenfassung von EDR-Features im Endgeräteprodukt Traps und Netzwerkinformationen der Firewalls in einer zentralen cloudbasierten Analyse und Konsole.

RSA Security: Der Firmenname bildet sich aus den Initialen der Erfinder des RSA-Algorithmus Rivest, Shamir und Adleman, die im Jahr 1982 die Firma RSA Data Security gründeten. Diese wurde im Jahr 1996 von Security Dynamics aufgekauft, die vor allem für ihre SecurID-Token bekannt geworden war. 1999 änderte Security Dynamics seinen Namen in RSA Security und wurde 2006 von dem heute zu Dell gehörenden Unternehmen EMC übernommen. Seit 2012 bietet RSA auch ein Produkt für die Endpoint-Security, das heute unter dem Namen NetWitness Endpoint verkauft wird und EDR-Funktionen bietet.

SentinelOne: Die 2013 gegründete Firma SentinelOne hat wie viele Hersteller von Sicherheitsprodukten ihre Wurzeln in Israel und ihr Hauptquartier in den USA. Der Anbieter hat sich zunächst auf die Überwachung des Prozessverhaltens spezialisiert und später präventive Malwareschutzfunktionen hinzugefügt. 2021 ging das Unternehmen an die Börse.

Sequretec wurde 2013 in Indien gegründet. 2018 brachten sie ihr EDPR als Kombination aus EDR und Advanced Threat Protection auf den Markt.

Sophos: Das britische Unternehmen wurde 1985 von zwei Entwicklern gegründet und brachte im Jahr 1988 das erste Virenschutzprodukt auf den Markt. Neben dem ursprünglichen AV-Bereich hat Sophos sein Portfolio durch einige Firmenzukäufe erweitert, unter anderem erwarb es 2011 die deutsche Firma Astaro und 2017 Invincea, die Produkte im Bereich der Prozessverhaltensanalyse und der Isolation entwickelt haben.

Trend Micro wurde 1988 in Los Angeles als IT-Sicherheitsfirma gegründet und das Hauptquartier kurz darauf nach Taiwan verlegt. Nach der Übernahme durch eine japanische Firma wurde der Hauptsitz erneut verlegt, dieses Mal nach Tokio. Bereits 1990 erschien PC-Cillin als Virenschutz für den Endverbrauchermarkt und kurz darauf auch für Unternehmen.

Uptycs: Als relativ junges Unternehmen, das 2016 gegründet wurde, möchte Uptycs einen Open-Source-Agent zur Verfügung stellen, der eine möglichst breite Palette an Systemdaten liefert, die man analysieren kann.

VMware (CarbonBlack): CarbonBlack geht ursprünglich auf zwei Firmen zurück. Die 2002 gegründete Bit9 konzentrierte sich vor allem auf Application Whitelisting. Im Jahr 2014 kaufte Bit9 die 2010 gegründete Firma CarbonBlack, die sich auf Prozessverhaltensanalyse spezialisierte hatte. Das Unternehmen nannte sich bis 2016 Bit9 + CarbonBlack. Im Jahr 2016 wurde mit Confer ein Hersteller einer Next-Generation-AV-Lösung dazugekauft und 2019 wurde CarbonBlack selbst von VMware übernommen.

WatchGuard Technologies: Das 1996 in Seattle gegründete Unternehmen wurde bekannt für seine Firewalls auf Linux-Basis. Im Juli 2020 übernahm WatchGuard das europäische Unternehmen Panda Security, das sich vor allem auf Sicherheitsprodukte für Endpunkte konzentriert.

Wazuh entstand 2015 in Silicon Valley, Kalifornien, als Open-Source-Projekt. Es liefert eine freie und quelloffene Alternative zu anderen EDR-Produkten. Als Unternehmen bietet Wazuh Dienstleistungen wie Schulungen oder technischen Support an.

kasten, um auf einzelne Vorfälle gezielt zu reagieren.

Automatisierung per API

Auffällig ist, dass fast alle Anbieter Schnittstellen anbieten, mit denen die Produkte durch den Kunden angepasst oder in bestehende Infrastrukturen integriert werden können. Nicht selten verfolgen die Hersteller eine „API first"-Strategie, die es ermöglicht, sämtliche Programmfunktionen zur Erkennung und Reaktion zu automatisieren. Für tiefergehende Analysen erlauben diese Schnittstellen den direkten Zugriff auf das Datenmodell, um detaillierte Abfragen durchzuführen, die so über das zentrale Management nicht möglich sind.

Das Anbieterfeld von EDR ist mittlerweile sehr vielfältig. Die frühen Anbieter waren wie so oft in der Securitybranche zunächst kleine Start-ups, die dynamisch

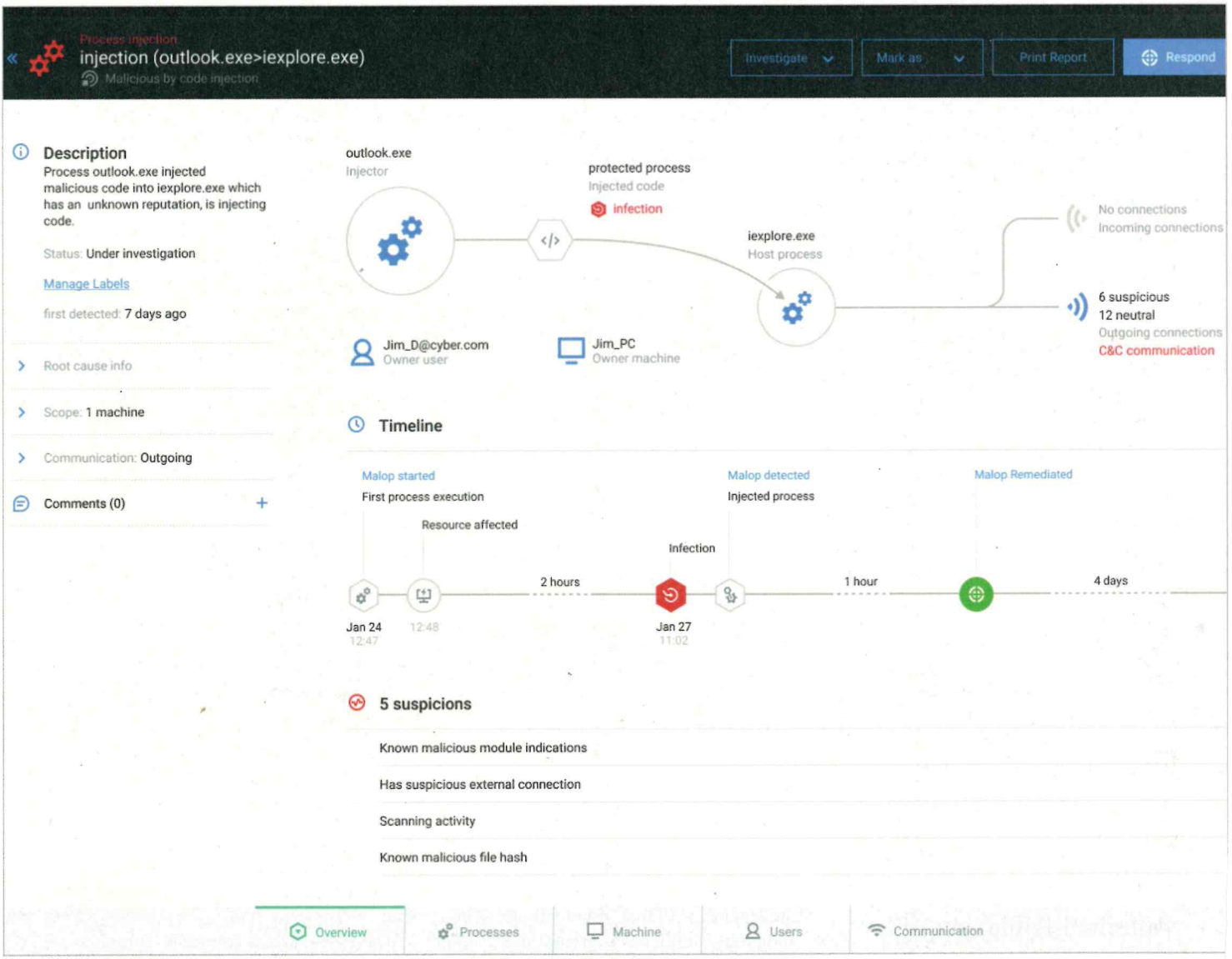
und innovativ neue technische Ideen implementierten. Die großen, etablierten Hersteller von Endpoint-Security-Produkten sind meist etwas schwerfälliger oder sie kaufen Start-ups auf und erweitern so ihre Produktsuiten. Es ist naheliegend, dass ein großer Anbieter im nächsten Schritt versucht, die zugekaufte EDR-Software in seine Produkte zu integrieren, sodass beispielsweise ein aus einer Netzwerkanomalieerkennung resultierender Alarm automatisch vom EDR-Produkt verifiziert wird.

Um die eigenen integrierten Produkte von denen der Konkurrenz abzugrenzen, entstand dabei die Bezeichnung Extended Detection and Response (XDR). XDR ist damit die naheliegende Weiterentwicklung von EDR. Hersteller, die neben einem EDR-Produkt auch Erkennungstechniken im Netzwerk oder sogar in weiteren Bereichen im Portfolio haben, tendieren fast alle dazu, dies als XDR zu bewerben. In einzelnen Fällen wird XDR dabei anders ausgelegt und das „X" steht für Cross-Layer (schichtenübergreifend) statt für Extended. Das soll verdeutlichen, dass Erkennung und Reaktion gleichzeitig auf verschiedenen Ebenen stattfinden.

Alternative zu klassischem SIEM

Die Hersteller von XDR konzipieren ihr Produkt meist so, dass es möglichst viele Datenquellen aus den anderen eigenen Produkten integriert. Eine native Integration von Produkten anderer Hersteller ist selten möglich. Das ist auch nachvollziehbar, da eine vollständige Integration weitaus komplexer ist als nur das Zusammenfassen einzelner Events. Um wirklichen Mehrwert zu erzeugen, müssen die Einzelteile eines XDR eng verzahnt sein, Informationen mit Kontext austauschen und aktiv zusammenarbeiten.

Durch das Zusammenspiel verschiedenartiger Sensoren und Agenten wird XDR noch viel deutlicher eine Alternative zum klassischen SIEM-Ansatz, der Events ohne Kontext korreliert, um daraus den Kontext zu rekonstruieren. Bei der Automatisierung sind die Gemeinsamkeiten und Gegensätze der beiden Produktfamilien ebenfalls zu erkennen. SIEM-Produkte erzeugen nicht mehr nur Alarme, sondern werden oft mit Funktionen für Security Orchestration Automation and Response (SOAR) ergänzt. Diese Tools können automatische Aktionen für das Anreichern mit Zusatzinformationen, das Verifizieren oder das Reagieren auslösen.



Das Dashboard, hier von Cybereason, macht die Malops (Malicious Operations) anhand der visualisierten Timeline und der aufgerufenen Prozesse nachvollziehbar (Abb. 4).

Klassisches SOAR muss dies, ähnlich wie beim SIEM, für zahlreiche Produkte unterschiedlicher Hersteller leisten und dabei die Schnittstellen bei jeder Änderung eines Drittprodukts anpassen. Beim XDR-Ansatz kommen die Komponenten eines einzelnen Herstellers zusammen, der die Schnittstellen selbst definiert und kontrolliert. Der Integrationsaufwand fällt daher beim Hersteller und Entwickler der XDR-Lösung selbst an und nicht beim Kunden, der seine SIEM- und SOAR-Produkte selbst konfigurieren muss.

Die zentrale Intelligenz und Verwaltung eines EDR ist sehr häufig in der Cloud des Herstellers angesiedelt. Dies passt zur Intention, den Aufwand weitgehend beim Hersteller zu belassen und den Betrieb für den Kunden so einfach wie möglich zu gestalten. Die meisten Hersteller geben an, lediglich Metadaten in die Cloud zu übertragen. Wer dabei trotzdem noch datenschutztechnische Bedenken hat, kann in der Regel das EDR-Produkt auch on Premises hosten. Dabei fallen allerdings höhere Kosten für Infrastruktur, Konfiguration und Wartung an.

Neben der Software bieten einige Hersteller auch gleich den Betrieb von EDR- oder XDR-Produkten zusammen mit Dienstleistungen für die Reaktion auf Vorfälle an und nennen es dann Managed Detection and Response (MDR), wobei dieser Begriff je nach Anbieter unterschiedlich interpretiert wird. Man findet Anbieter, die ein EDR- oder XDR-Produkt als MDR betreiben, sowie solche, die nur Logdaten mit einem klassischen SIEM auswerten und darauf reagieren.

Gefahr von Monokulturen

XDR als Out-of-the-box-Produkt aus der Hand eines einzelnen Herstellers zu beziehen, bei dem die verschiedenen Sensoren aufeinander abgestimmt sind und automatisch zusammenarbeiten, ist potenziell ein vielversprechender Ansatz. Einige Hersteller gehen sogar noch weiter und integrieren nicht nur Techniken zum Erkennen von Kompromittierungen, sondern auch Schwachstellenmanagement, um unsichere Fehlkonfigurationen oder fehlende Patches zu erfassen und in das Gesamtbild einfließen zu lassen. Manche integrieren eine zusätzliche Device-Control-Komponente als Data-Loss-Prävention, um den Abfluss von Daten über USB-Sticks zu verhindern.

Optionale zusätzliche Sandboxen können das EDR mit weiteren Informationen anreichern. Der Funktionsumfang dieser Zusatzkomponenten kommt zwar oft nicht an den der darauf spezialisierten Produkte heran, kann aber durchaus eine sinnvolle Erweiterung sein. Durch die tiefe und automatische Integration, die deutlich weniger Fehlalarme zur Folge hat, sowie die Bereitstellung der zentralen Komponente in der Cloud des Herstellers wird bei solchen Lösungen ein Eigenbetrieb für viele auch kleinere Organisationen attraktiv. Allerdings macht sich ein Unternehmen mit der Einführung eines XDR-Produkts noch stärker von einem einzelnen Anbieter abhängig.

Sofern das XDR nur aus einem Endpunktagenten und zusätzlicher Netzwerksensorik besteht, hat dies noch keine gravierenden Konsequenzen. Wenn das XDR aber nur im Zusammenspiel mit der Firewall und den Web- und Mail-Gateways desselben Herstellers richtig funktioniert, entsteht eine hohe Abhängigkeit. Sicherheitsexperten erachten solche Monokulturen oft als problematisch.

Marktübersicht Endpoint Detection and Response (EDR), Teil 1

Hersteller	Bitdefender	BlackBerry	Cisco	CrowdStrike
Produktname	Bitdefender GravityZone Ultra	BlackBerry Optics / BlackBerry Guard	Cisco Secure Endpoint	CrowdStrike Falcon
allgemein				
Architektur (Endpunktagent / zentrale Konsole / Netzwerksensoren)	✓ / ✓ / ✓	✓ / ✓ / –	✓ / ✓ / –	✓ / ✓ / –
Betriebsmodelle (on Premises / Cloud / Hybrid)	✓ / ✓ / –	✓ / ✓ / ✓	✓ / ✓ / –	– / ✓ / –
unterstützte Betriebssysteme (Windows / Linux / macOS / Android / iOS)	✓ / ✓ / ✓ / – / –	✓ / ✓ / ✓ / (✓) / (✓)	✓ / ✓ / ✓ / (✓) / (✓)	✓ / ✓ / ✓ / (✓) / (✓)
klassische AV-Funktionen				
statische Analyse (Signaturen / Heuristiken / Hash-Lookups / Code-Analyse / KI-Engine)	✓ / ✓ / ✓ / ✓ / ✓	– / ✓ / – / ✓ / ✓	✓ / ✓ / ✓ / ✓ / ✓	– / ✓ / ✓ / ✓ / ✓
dynamische Analyse der zentralen Konsole (Sandbox-Analyse / Code-Emulierung)	✓ / ✓	– / –	– / –	✓ / –
Logging/Weiterleitung von Events an das zentrale Management				
Dateioperationen (lesen / schreiben / erstellen / löschen)	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓
Registry-Zugriff (lesen / schreiben / erstellen / löschen)	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	– / ✓ / ✓ / ✓
Netzwerkkommunikation (TCP / UDP / DNS / andere)	✓ / ✓ / ✓ / –	✓ / – / ✓ / –	✓ / – / ✓ / die ersten 25 Netzwerk-Flows jedes Prozesses	✓ / ✓ / ✓ / Verletzungen der lokalen Firewall-Regeln
Hardwareschnittstellen (USB / Thunderbold / andere)	✓ / – / –	✓ / – / –	– / – / Gerätetreiberdaten	✓ / – / Bluetooth, WLAN
Windows-interne Kommunikation (IPC / RPC / COM / andere)	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / –	k. A.	✓ / ✓ / – / –
Arbeitsspeicherzugriff (Reservierung von Speicher / Schreiben in Speicher fremder Prozesse / Lesen von Speicher fremder Prozesse / andere)	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / –	k. A.	✓ / ✓ / ✓ / –
Interaktion mit anderen Prozessen (Starten von Prozessen / Stoppen von Prozessen / Anlegen von Aufgaben / Anlegen von Diensten)	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	✓ / – / ✓ / ✓	✓ / ✓ / ✓ / ✓
zusätzliche Überwachung	k. A.	k. A.	Manipulation der lokalen Firewall und Benutzerkontensteuerung, Deaktivierung von Diensten, Änderungen an Schattenkopien, Verwendung von WMI	Laden von Bibliotheken, Starten von Skripten
enthaltene Eventinformationen (gesamte Datei / Metadaten / Dateiheader / Arbeitsspeicherinhalte / andere)	✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / – / konfigurierbar	✓ / ✓ / ✓ / – / –	✓ / ✓ / ✓ / ✓ / –
Erkennung/Alarmierung				
Erkennung von schadhaftem Verhalten (statisches Regelwerk / musterbasierte IoCs / Punkte-System / andere)	✓ / ✓ / ✓ / –	✓ / ✓ / – / KI-Modell	✓ / ✓ / – / –	✓ / ✓ / ✓ / –
Parameter zur manuellen Definition von Ausnahmen aufgrund der Prozessumgebung (Datei-Hash / Dateispeicherort / Benutzerkontext / Elternprozess / Dateiherkunft / andere)	✓ / ✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / – / ✓ / – / –	✓ / ✓ / ✓ / ✓ / ✓ / Versionsinformationen von Programmen	✓ / ✓ / – / – / – / –
Referenzen zum MITRE-ATT&CK-Framework (Taktik / Technik / Empfehlung)	✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / ✓ / ✓
Beispielkriterien für die Erkennung einer Rechteerweiterung	LSASS-Prozessüberwachung, Verwendung von Mimikatz, unregelmäßige Interprozess-kommunikation	LSASS-Prozessüberwachung, Überwachung der Benutzer-kontensteuerung	LSASS-Prozessüber-wachung, abnormale Benutzung von Named Pipes, Überwachung der Benutzerkontensteuerung	LSASS-Prozessüberwachung, SAM, NTDS.dit, Registry-Operationen, Benutzerkontensteuerung
Beispielkriterien für die Erkennung eines Netzwerkscans	Log-in-Versuche	k. A.	k. A.	hohe Anzahl von Verbindungsversuchen
Beispielkriterien zur Erkennung von Lateral Movement	Unregelmäßigkeiten im SMB-Verkehr, Verwendung von PSEXEC und DCOM, Verwen-dung bekannter Exploits	k. A.	Verwendung von PSEXEC und WMI, Auslesen von Anmeldedaten	z. B. Verwendung von WMI oder RDP
Beispielkriterien zur Erkennung von C&C-Kommunikation	IP-Reputationen, Blocklisten, Anomalieerkennung	k. A.	Domain-Reputationen, Verwendung von Net use, WebDav, MSBuild, Installation lokaler Proxydienste	auffällige Verwendung spezieller Netzwerkprotokolle (z. B. DNS), Verwendung von Proxys, Änderungen an der lokalen Firewall, Starten von Netzwerk-Listenern

✓: ja / vorhanden / trifft zu; (✓): trifft eingeschränkt zu; –: nein / nicht vorhanden / trifft nicht zu; n. a: nicht anwendbar; k. A.: keine Angabe

Cybereason	Cynet	Eset	F-Secure	Fortinet	Kaspersky	Malwarebytes
The Cybereason Defense Platform	Cynet 360	ESET Enterprise Inspector	F-Secure Elements Endpoint Detection and Response	FortiEDR	Kaspersky Endpoint Detection and Response	Malwarebytes Endpoint Detection and Response
✓ / ✓ / –	✓ / ✓ / –	✓ / ✓ / –	✓ / ✓ / –	✓ / ✓ / ✓	✓ / ✓ / –	✓ / ✓ / –
✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / – / –	– / ✓ / –	✓ / ✓ / ✓	✓ / – / ✓	– / ✓ / –
✓ / ✓ / ✓ / ✓ / (✓) / (✓)	✓ / ✓ / ✓ / – / –	✓ / – / ✓ / – / –	✓ / ✓ / ✓ / – / –	✓ / ✓ / ✓ / – / –	✓ / ✓ / – / – / –	✓ / – / ✓ / – / –
✓ / ✓ / – / – / ✓	✓ / ✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / – / –	✓ / ✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓ / ✓	– / ✓ / – / – / ✓
– / –	✓ / ✓	✓ / ✓	k. A.	✓ / –	✓ / ✓	✓ / –
– / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	(✓) / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	– / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓
– / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	– / ✓ / ✓ / ✓	– / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	– / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓
✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / ICMP	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / IP	– / – / – / –
✓ / ✓ / –	✓ / – / CD-ROM	✓ / ✓ / –	k. A.	✓ / – / –	✓ / – / –	– / – / –
✓ / ✓ / ✓ / Erstellen von Named Pipes	✓ / ✓ / ✓ / –	– / – / – / Erstellen von Named Pipes	✓ / ✓ / – / API-Aufrufe	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / –
✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / –	– / ✓ / (✓) / –	– / ✓ / – / –	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / –
✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	✓ / ✓ / (✓) / –	✓ / – / ✓ / ✓	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓
k. A.	Laden von Bibliotheken	Laden von Bibliotheken, Erstellen/Verändern von Benutzerkonten, Verwendung von WMI, AMSI-Informationen	k. A.	Laden von Bibliotheken	k. A.	k. A.
k. A.	– / ✓ / ✓ / – / –	✓ / ✓ / ✓ / – / Datei-Hashes, Dateisignaturen	– / ✓ / – / – / –	– / ✓ / – / – / z. B. Benutzernamen, digitale Zertifikate, Prozessdaten, Produktbeschreibung	✓ / ✓ / ✓ / ✓ / –	– / ✓ / ✓ / – / –
✓ / ✓ / ✓ / KI-Modell	✓ / ✓ / ✓ / Anomalieerkennung	✓ / – / ✓ / –	✓ / ✓ / ✓ / –	✓ / – / – / –	✓ / ✓ / ✓ / –	✓ / ✓ / – / –
✓ / ✓ / k. A. / k. A. / ✓ / –	✓ / ✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / ✓ / ✓ / Dateisignatur, Dateireputationen	k. A.	✓ / ✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / – / ✓ / – / –	✓ / ✓ / – / ✓ / – / –
✓ / ✓ / ✓	✓ / ✓ / –	✓ / ✓ / –	✓ / ✓ / –	✓ / ✓ / –	✓ / ✓ / ✓	✓ / ✓ / –
LSASS-Prozessüberwachung, Überwachung der Benutzerkontensteuerung, Anlegen von Benutzern	LSASS-Prozessüberwachung, Überwachung der Benutzerkontensteuerung, Registry-Operationen, Verwendung von Mimikatz	LSASS-Prozessüberwachung, Überwachung der Benutzerkontensteuerung, Anlegen von Benutzern	k. A.	k. A.	LSASS-Prozessüberwachung, Verwendung von Mimikatz	k. A.
Verwendung verdächtiger Netzwerktools	Deep Packet Inspection, Anomalieerkennung	Deep Packet Inspection	k. A.	k. A.	Suricata-Regeln (mit Netzwerksensor)	k. A.
Verwendung von WMI, PSEXEC, RunAs, Auslesen von Anmeldedaten	Verwendung von WMI, PSEXEC, DCOM, RunAs, Auslesen von Anmeldedaten, Zugriff auf administrative Freigaben	Verwendung von WMI, PSEXEC, PowerShell Remoting, Auslesen von Anmeldedaten, Log-in-Versuche, Schreiben in SMB-Shares	k. A.	k. A.	k. A.	k. A.
auffällige Verwendung spezieller Netzwerkprotokolle, Kommunikation mit verdächtigen Adressen	Domain-/IP-Reputationen, auffällige Verwendung spezieller Netzwerkprotokolle (z. B. ICMP, DNS)	Kommunikation mit verdächtigen Adressen	k. A.	k. A.	Suricata-Regeln (mit Netzwerksensor)	IP-Reputationen, Blocklisten

Die vollständige Tabelle ist über ix.de/zmtg zugänglich.

Marktübersicht Endpoint Detection and Response (EDR), Teil 1

Hersteller	Bitdefender	BlackBerry	Cisco	CrowdStrike
Beispielkriterien zur Erkennung von Datendiebstahl	Deep Packet Inspection: Alarmierung bei Abfluss von Benutzernamen und Passwörtern, Kreditkartendaten, Dokumenten und ZIP-Archiven	Überwachung von Screenshot- und Keylogging-Funktionen	k. A.	k. A.
Beispielkriterien zur Erkennung von Ransomware	hohe Anzahl an Verschlüsselungsoperationen, Verwendung bekannter Dateiendungen	k. A.	hohe Anzahl an Dateioperationen (Verschieben, Verschlüsseln, Löschen)	Zugriff auf Schattenkopien, Verwendung von Verschlüsselungsoperationen
Beispielkriterien zur Erkennung schadhafter Office-Makros	Überwachung von API-Aufrufen	k. A.	z. B. Aufruf von PowerShell	z. B. Ausführung von Skripten oder codierten Befehlen
Beispielkriterien zur Erkennung von DLL-Hijacking	k. A.	k. A.	k. A.	k. A.
Erkennung von Persistenztechniken (Manipulation der Registry / Aufgabenplanung / Anlegen von Benutzerkonten / andere)	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / Erstellung von Diensten, WMI-Persistenz
Exploit-Schutz (Bufferoverflow-Schutz, ROP-Schutz, andere)	✓ / ✓ / –	✓ / ✓ / –	– / ✓ / Heap-Spray-Schutz	✓ / ✓ / Heap-Spray-Schutz, Erzwingen von DEP und ASLR, Null Page Allocation, SEHOP
Analyse des Netzwerkverhaltens des Endgeräts	Deep Packet Inspection mit Heuristiken, Regelwerken und Anomalieerkennung	k. A.	Die ersten 25 Netzwerk-Flows jedes Prozesses werden gespeichert.	Überwachung sämtlicher IP-Kommunikation
Überwachung bestimmter Netzwerkprotokolle (DNS / HTTP(S) / FTP / SSH / andere)	✓ / ✓ / ✓ / ✓ / ICMP, SSL, RDP, SMTP, POP3, IMAP, MS-Exchange, TelNet, KERBEROS, LDAP, DHCP, VNC, NFS, QUICK, SOCKS, RPC	k. A.	✓ / ✓ / – / – / –	✓ / ✓ / ✓ / ✓ / –
Deception-Techniken	–	–	–	–
zentrale Sandbox-Analyse				
unterstützte Dateitypen (ausführbare Dateien / Office-Dokumente / PDFs / Skripte / andere)	✓ / ✓ / ✓ / ✓ / –	✓ / – / – / – / –	✓ / ✓ / ✓ / ✓ / beliebige Dateitypen	✓ / ✓ / ✓ / ✓ / E-Mails, Java-Anwendungen, Linux ELF, SVG
unterstützte Betriebssysteme (Windows / Linux / macOS / iOS / Android)	✓ / – / – / – / –	k. A.	✓ / – / – / – / –	✓ / ✓ / – / – / ✓
Response-Workflow				
Aufzeichnung administrativer Tätigkeiten (auf den Endgeräten ausgeführte Kommandos / Suchanfragen / Response-Schritte / Zugriff auf Logs / vollständiges Audit-Trail / andere)	✓ / ✓ / ✓ / – / – / –	✓ / ✓ / ✓ / ✓ / ✓ / ✓ / –	– / ✓ / ✓ / – / – / Anpassen von Richtlinien und Gruppenzugehörigkeiten, Anfertigung eines forensischen Abbilds	✓ / ✓ / ✓ / ✓ / ✓ / –
Alarmierung (E-Mail / SMS / Telefonanruf / andere)	✓ / – / – / –	✓ / – / – / SIEM-Integration	✓ / – / – / API	✓ / – / ✓ / Slack-Benachrichtigung
aktive Response-Möglichkeiten (Stoppen von Prozessen / Dateiwiederherstellung / Fernzugriff per Konsole / Client-Isolation / Löschen von Dateien / andere)	✓ / ✓ / ✓ / ✓ / ✓ / Schwachstellenscan, Sandbox-Analyse	✓ / – / ✓ / ✓ / ✓ / –	– / – / – / ✓ / – / Dateiquarantäne	✓ / ✓ / ✓ / ✓ / ✓ / –
automatische Response-Schritte (Stoppen von Prozessen / Unterbrechen von Prozessen / Client-Isolation / Löschen von Dateien / Dateiwiederherstellung / andere)	✓ / – / – / ✓ / ✓ / –	✓ / ✓ / ✓ / ✓ / – / –	– / – / ✓ / – / – / Anfertigung eines forensischen Abbilds, Dateianalyse	✓ / ✓ / ✓ / ✓ / (✓) / Bereinigung der Registry, Ausführung beliebiger Kommandos und Skripte
manuelle Abfrage von Information vom Endgerät (Dateien / Prozess-Dumps / Prozessliste / forensisch verwertbare Speicherabbilder / andere)	✓ / – / ✓ / – / –	k. A. / k. A. / k. A. / ✓ / –	✓ / – / ✓ / – / –	✓ / ✓ / ✓ / ✓ / Registry-Keys, Datei-Hashes, Forensikdaten über ein spezielles Auswertungstool
Kollaboration zwischen Analysten (integriertes Ticket-Tool / Kommentarfunktion / Jira-Integration / andere)	– / ✓ / – / –	– / – / – / Integration in ServiceDesk und Splunk	✓ / ✓ / – / Integration in Cisco SecureX	✓ / ✓ / – / –
Threat Hunting				
Suchkriterien für IoCs (Dateinamen / Datei-Hashes / Registry-Keys / IP-Adressen / Domainnamen / Netzwerkartefakte / andere)	✓ / ✓ / ✓ / ✓ / ✓ / – / Taktiken und Techniken	✓ / ✓ / ✓ / ✓ / ✓ / ✓ / – / Prozessparameter	✓ / ✓ / – / ✓ / ✓ / – / TTPs	✓ / ✓ / ✓ / ✓ / ✓ / ✓ / Prozessnamen
eingebundene Threat-Intelligence-Datenbanken	z. B. Honeypots, VirusTotal, Google, RecordedFuture, TTPs, Telemetriedaten von anderen Kunden	VirusTotal, eigene Threat-Intelligence-Quellen	Cisco Talos, Cisco AMP Dateireputationen, Cisco Umbrella, VirusTotal, und diverse Drittanbieter für Threat Intelligence	eigene Threat Intelligence, VirusTotal, diverse zusätzliche Quellen

✓: ja / vorhanden / trifft zu; (✓): trifft eingeschränkt zu; –: nein / nicht vorhanden / trifft nicht zu; n. a: nicht anwendbar; k. A.: keine Angabe

Cybereason	Cynet	Eset	F-Secure	Fortinet	Kaspersky	Malwarebytes
unregelmäßig hohes Kommunikationsaufkommen, unregelmäßige Dateioperationen	Überwachung von Screenshot- und Keylogging-Funktionen	Überwachung von Screenshot- und Keylogging-Funktionen	k. A.	k. A.	Überwachung von Screenshot- und Keylogging-Funktionen	–
Zugriff auf Schattenkopien oder Canary-Dateien	Zugriff auf Canary-Dateien	hohe Anzahl an Dateioperationen (Verschieben, Verschlüsseln, Löschen), Verhaltensanalyse	hohe Anzahl an Dateioperationen	k. A.	Löschen von Schattenkopien, Verschlüsseln oder Löschen wichtiger Dateien	Verschlüsselungsoperationen
z. B. Aufruf verdächtiger Unterprozesse, WMI, Verhaltensanalyse	Aufruf verdächtiger Unterprozesse wie z. B. WinAPI-Aufrufe	Office-Anwendung, die Prozesse startet	k. A.	z. B. Ausführung von Skripten	k. A.	k. A.
Laden aus unsicheren Quellen, Reputationen, Speicherort und Dateisignatur	Reputationen, Speicherort und Dateisignatur	Speicherort und Dateisignatur	k. A.	k. A.	k. A.	k. A.
✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / Manipulation des PowerShell-Profils, WMI-Persistenz, Autostart-Manipulation	k. A.	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / –	✓ / ✓ / – / –
– / – / Limitierung bei der Erstellung von Kindprozessen, Speichermanipulation	k. A.	✓ / ✓ / –	– / – / –	✓ / ✓ / –	✓ / ✓ / –	✓ / ✓ / –
DNS-/IP-Reputationen, abnormale Verwendung bestimmter Ports und Protokolle, Deep Packet Inspection	Deep Packet Inspection	Deep Packet Inspection	k. A.	k. A.	Überwachung von Netzwerkverkehr und Anomalieerkennung	Überwachung auf Basis von Protokollen und Port
✓ / ✓ / – / – / –	✓ / ✓ / ✓ / ✓ / ICMP	✓ / ✓ / ✓ / ✓ / BitTorrent, DCERCP, IMAP, IRC, POP3, RDP, SIP, SMB, SMB2, SMTP, TOR, VNC, XMPP, RDP	k. A.	✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / ✓ / z. B. MSSQL, RDP, SNMP	k. A.
Platzierung und Überwachung von Canary-Dateien	Platzierung und Überwachung von Canary-Dateien	–	–	–	Platzierung und Überwachung von Canary-Dateien	–
n. a.	✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / ✓ / –	k. A.	✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / ✓ / –	✓ / – / – / – / –
n. a.	✓ / – / – / – / –	✓ / ✓ / – / – / –	k. A.	✓ / (✓) / – / – / –	✓ / – / – / – / –	✓ / – / – / – / –
✓ / ✓ / ✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / ✓ / ✓ / –	– / – / ✓ / – / – / –	✓ / ✓ / ✓ / ✓ / ✓ / –	✓ / – / ✓ / – / – / –	– / – / ✓ / ✓ / – / –
✓ / ✓ / – / Syslog	✓ / – / ✓ / Mobile App	✓ / – / – / –	✓ / – / – / API	✓ / – / – / –	✓ / – / – / –	✓ / – / – / API
✓ / ✓ / ✓ / ✓ / ✓ / ✓ / –	✓ / – / ✓ / ✓ / ✓ / Benutzer sperren, Dateiquarantäne	✓ / – / ✓ / ✓ / – / –	– / – / – / ✓ / – / –	✓ / ✓ / – / ✓ / ✓ / –	✓ / ✓ / – / ✓ / ✓ / Starten von Programmen	✓ / ✓ / – / ✓ / – / –
✓ / – / ✓ / ✓ / – / –	✓ / ✓ / ✓ / ✓ / ✓ / Benutzer sperren, Dateiquarantäne	✓ / – / ✓ / ✓ / – / –	– / – / ✓ / – / – / –	✓ / – / ✓ / ✓ / ✓ / –	✓ / – / – / ✓ / ✓ / –	n. a.
✓ / ✓ / ✓ / ✓ / ✓ / Forensikdaten über ein spezielles Auswertungstool	✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / – / diverse Logs	– / – / – / – / Logs, Registry, Netzwerkdiagnosedaten, installierte Software, Interface-Status, bestimmte Systemdateien	✓ / ✓ / – / ✓ / –	✓ / – / ✓ / – / Liste von Dateien	n. a.
– / ✓ / – / –	– / ✓ / – / –	– / ✓ / – / Incident Management System geplant	– / ✓ / – / –	– / ✓ / ✓ / –	✓ / ✓ / – / –	✓ / – / – / –
✓ / ✓ / ✓ / ✓ / ✓ / ✓ / ✓ / TTPs, WMI-Aktivitäten, bestimmte Verhaltensmuster, ausgeführte Befehle, Log-in-Versuche	✓ / ✓ / – / ✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / ✓ / ✓ / – / –	k. A.	✓ / ✓ / ✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / – / ✓ / ✓ / – / Prozess-Hashes
eigene Threat Intelligence, VirusTotal	VirusTotal, MalwareBazaar, Cisco Talos, VirusShare, ANY.RUN, Ministerium für Innere Sicherheit der Vereinigten Staaten	VirusTotal, diverse OSINT-Quellen	VirusTotal	FortiGuard Labs, MITRE CVE Datenbank, VirusTotal	Kaspersky Threat Intelligence, VirusTotal	VirusTotal

Die vollständige Tabelle ist über ix.de/zmtg zugänglich.

Marktübersicht Endpoint Detection and Response (EDR), Teil 2

Hersteller	McAfee	Microsoft	Palo Alto	SentinelOne
Produktname	McAfee MVISION EDR	Microsoft Defender for Endpoint	Cortex XDR	SentinelOne ActiveEDR
allgemein				
Architektur (Endpunktagent / zentrale Konsole / Netzwerksensoren)	✓ / ✓ / ✓	✓ / ✓ / –	✓ / ✓ / ✓	✓ / ✓ / –
Betriebsmodelle (on Premises / Cloud / Hybrid)	✓ / ✓ / ✓	– / ✓ / –	– / ✓ / –	✓ / ✓ / –
unterstützte Betriebssysteme (Windows / Linux / macOS / Android / iOS)	✓ / ✓ / ✓ / (✓) / (✓)	✓ / ✓ / ✓ / (✓) / (✓)	✓ / ✓ / ✓ / (✓) / –	✓ / ✓ / ✓ / – / –
klassische AV-Funktionen				
statische Analyse (Signaturen / Heuristiken / Hash-Lookups / Codeanalyse / KI-Engine)	✓ / ✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / – / ✓	✓ / – / ✓ / ✓ / ✓
dynamische Analyse der zentralen Konsole (Sandbox-Analyse / Code-Emulierung)	✓ / ✓	✓ / ✓	✓ / –	– / –
Logging/Weiterleitung von Events an das zentrale Management				
Dateioperationen (lesen / schreiben / erstellen / löschen)	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	– / ✓ / ✓ / ✓	– / ✓ / ✓ / ✓
Registry-Zugriff (lesen / schreiben / erstellen / löschen)	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	– / ✓ / ✓ / ✓	– / ✓ / ✓ / ✓
Netzwerkkommunikation (TCP / UDP / DNS / andere)	✓ / ✓ / ✓ / HTTP, HTTPS	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / Socket-Events, HTTP	✓ / ✓ / ✓ / –
Hardwareschnittstellen (USB / Thunderbold / andere)	✓ / ✓ / z. B. Bluetooth, PCI	✓ / ✓ / –	–	✓ / – / Bluetooth, Bluetooth LE
Windows-interne Kommunikation (IPC / RPC / COM / andere)	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / k. A.	– / ✓ / – / Systemaufrufe	n. a.
Arbeitsspeicherzugriff (Reservierung von Speicher / Schreiben in Speicher fremder Prozesse / Lesen von Speicher fremder Prozesse / andere)	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / –
Interaktion mit anderen Prozessen (Starten von Prozessen / Stoppen von Prozessen / Anlegen von Aufgaben / Anlegen von Diensten)	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / ✓	✓ / – / ✓ / ✓
zusätzliche Überwachung	z. B. API-Calls, Laden von Bibliotheken	Image Load Events, Änderungen an der Firmware	Windows-Event-Log, Benutzer-Sessions, Gerätestatus	Benutzer-Sessions, Gerätestatus, Netzwerkstatus, Firewallstatus
enthaltene Eventinformationen (gesamte Datei / Metadaten / Dateiheader / Arbeitsspeicherinhalte / andere)	– / ✓ / – / – / –	– / ✓ / ✓ / – / –	– / ✓ / – / – / –	– / ✓ / – / – / –
Erkennung/Alarmierung				
Erkennung von schadhaftem Verhalten (statisches Regelwerk / musterbasierte IoCs / Punktesystem / andere)	✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / IoA, verdächtiges Verhalten	✓ / ✓ / k. A. / Anomalieerkennung	✓ / ✓ / ✓ / ✓ / Anomalieerkennung
Parameter zur manuellen Definition von Ausnahmen aufgrund der Prozessumgebung (Datei-Hash / Dateispeicherort / Benutzerkontext / Elternprozess / Dateiherkunft / andere)	✓ / ✓ / ✓ / ✓ / ✓ / – / –	✓ / ✓ / ✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / ✓ / ✓ / ✓ / –
Referenzen zum MITRE-ATT&CK-Framework (Taktik / Technik / Empfehlung)	✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / ✓ / ✓
Beispielkriterien für die Erkennung einer Rechteerweiterung	LSASS-Prozessüberwachung, Benutzererstellung, UAC-Bypass	k. A.	LSASS-Prozessüberwachung, UAC-Bypass, Named Pipe Impersonation	z. B. LSASS Prozessüberwachung, UAC-Bypass
Beispielkriterien für die Erkennung eines Netzwerkscans	k. A.	k. A.	Verwendung verdächtiger Netzwerk-Tools	n. a.
Beispielkriterien zur Erkennung von Lateral Movement	Unregelmäßigkeiten im SMB-Verkehr, Verwendung von PSEXEC, Verwendung verdächtiger Werkzeuge	k. A.	z. B. unübliche Verwendung von WinRM/WinRS	Verwendung von PSEXEC, WMI, Net use, DCOM, RPC
Beispielkriterien zur Erkennung von C&C-Kommunikation	auffällige Verwendung spezieller Netzwerkprotokolle, IP-/DNS-Reputation	auffällige Verwendung spezieller Netzwerkprotokolle, Kommunikation mit verdächtigen Adressen	Verwendung des Tor-Netzwerks, Aufbau eines SSH-Tunnels, auffällige Verwendung spezieller Netzwerkprotokolle	Erkennung verbreiteter C2-Werkzeuge
Beispielkriterien zur Erkennung von Datendiebstahl	Überwachung von Screenshot- und Keylogging-Funktionen	k. A.	Nutzung von Werkzeugen wie curl, wget oder BitTorrent, unüblich große Uploadrate zu unbekannten Zielen	Überwachung von Screenshot- und Keylogging-Funktionen
Beispielkriterien zur Erkennung von Ransomware	Verhaltensanalyse	Zugriff auf geschützte Ordner, Office-Anwendung, die Prozesse startet	Zugriff auf Canary-Dateien	Ändern/Löschen von Dateie die nicht in Verbindung mit dem Quellprozess stehen
Beispielkriterien zur Erkennung schadhafter Office-Makros	Office-Anwendung, die Prozesse startet	Office-Anwendung, die Prozesse startet	Verhaltensanalyse, Office-Anwendung, die Prozesse startet	spezifische Verhaltensanalyse für Makros

✓: ja / vorhanden / trifft zu; (✓): trifft eingeschränkt zu; –: nein / nicht vorhanden / trifft nicht zu; n. a: nicht anwendbar; k. A.: keine Angabe

Sequretek	Sophos	Trend Micro	Uptycs	WatchGuard	Wazuh
Sequretek EDPR	Intercept X Advanced with EDR	Trend Micro XDR for Users	Endpoint Secure	Panda Adaptive Defense 360	Wazuh
✓/✓/–	✓/✓/✓	✓/✓/✓	✓/✓/–	✓/✓/–	✓/✓/✓
✓/✓/–	–/✓/–	✓/✓/✓	✓/✓/–	–/✓/–	✓/✓/–
✓/✓/✓/–/–	✓/✓/✓/–/–	✓/✓/✓/–/–	✓/✓/✓/–/–	✓/✓/✓/✓/–	✓/✓/✓/–/–
✓/✓/✓/✓/✓	✓/✓/✓/✓/✓	✓/✓/✓/✓/✓	–/–/✓/–/–	✓/✓/✓/✓/✓	✓/✓/✓/✓/–
✓/–	–/–	✓/–	–	✓/✓	–
✓/✓/✓/–	✓/✓/✓/✓	✓/✓/✓/✓	–/–/✓/–	✓/✓/✓/✓	prüft, ob ausgewählte Dateien verändert wurden
–/✓/✓/–	✓/✓/✓/✓	✓/✓/✓/✓	–/✓/✓/✓	✓/✓/✓/✓	prüft, ob ausgewählte Einträge verändert wurden
✓/–/✓/–	✓/✓/✓/–	✓/✓/✓/–	–/–/✓/ HTTP, Socket-Kommunikation	✓/✓/✓/–	–/–/–/–/ Interfaces und offene Ports
✓/–/–	k. A.	✓/✓/ Bluetooth	k. A.	✓/✓/–	–
✓/✓/✓/–	k. A.	✓/✓/✓/ WMI	✓/–/–/–	✓/✓/✓/–	–/–/–/ Systemaufrufe
✓/✓/✓/–	k. A.	–/✓/✓/–	–/–/–/ Zugriff auf geteilten Speicher	✓/✓/✓/–	–
✓/✓/✓/✓	✓/–/✓/✓	✓/✓/✓/–	✓/–/–/–	✓/✓/✓/✓	Linux-Logs
k. A.	k. A.	k. A.	Benutzer-Sessions, Benutzeraktivitäten, Zugriffe auf Peripheriegeräte	k. A.	Systemaufrufe
k. A.	–/–/–/–/ Datei-Hashes, URLs	–/✓/–/–/–	–/✓/–/–/ Compliancestatus	–/✓/–/–/–	k. A.
✓/✓/✓/–	✓/✓/✓/–	–	✓/–/✓/–	✓/✓/✓/–	✓/✓/–/–
✓/✓/✓/✓/✓/–	✓/✓/–/–/–/–	✓/✓/–/✓/–/–	✓/–/–/✓/–/–	✓/✓/–/–/✓/ Signaturen	✓/✓/–/✓/–/–
✓/✓/✓	✓/✓/–	✓/✓/–	✓/✓/✓	✓/✓/✓	✓/✓/✓
k. A.	z. B. Zugriff auf die SAM Datenbank, UAC-Bypass	z. B. LSASS-Prozessüberwachung, Prozessintegrität, UAC-Bypass	LSASS-Prozessüberwachung, Prozessintegrität, UAC-Bypass, Verwendung von Mimikatz	Allowlist von Prozessketten, basierend auf Machine Learning und Threat-Intelligence-Daten	Modifizierungen von Nutzern und Gruppen, verdächtige Befehlsausführungen
k. A.	k. A.	k. A.	Verwendung verdächtiger Netzwerktools, YARA-Regeln	Allowlist von Prozessketten, basierend auf Machine Learning und Threat-Intelligence-Daten	k. A.
k. A.	z. B. Verwendung von SMB, DCI oder wmci	z. B. Unregelmäßigkeiten im SMB-Verkehr, Verwendung von PSEXEC	Verwendung von PSEXEC, WMI oder PowerShell	Allowlist von Prozessketten, basierend auf Machine Learning und Threat-Intelligence-Daten	Verwendung verdächtiger Prozesse
k. A.	IP-Reputationen	auffällige Verwendung spezieller Netzwerkprotokolle, IP-/DNS-Reputation	verdächtige Verwendung von Werkzeugen wie PowerShell, wscript, cscript, wget, curl und rsync	Allowlist von Prozessketten, basierend auf Machine Learning und Threat-Intelligence-Daten	verdächtige Portfreigaben
k. A.	k. A.	Überwachung bekannter Übertragungswege wie USB, SMB oder FTP	Überwachung von Screenshot- und Keylogging-Funktionen	Allowlist von Prozessketten, basierend auf Machine Learning und Threat-Intelligence-Daten	Verbindungen zu bekannten Datenübertragungsports
k. A.	hohe Anzahl veränderter Dateien in einer bestimmten Zeit	Dateioperationen	Löschen von Schattenkopien mithilfe von vssadmin	Allowlist von Prozessketten, basierend auf Machine Learning und Threat-Intelligence-Daten	Dateiintegritätsüberwachung
Erkennung bestimmter Schlüsselwörter in Makros	Verhaltensanalyse, Office-Anwendung, die eine PowerShell startet	Verhaltensanalyse	Office-Anwendung, die Prozesse startet	Allowlist von Prozessketten, basierend auf Machine Learning und Threat-Intelligence-Daten	Verhaltensanalyse, verdächtige Dateioperationen

Die vollständige Tabelle ist über ix.de/zmtg zugänglich.

Marktübersicht Endpoint Detection and Response (EDR), Teil 2

Hersteller	McAfee	Microsoft	Palo Alto	SentinelOne
Beispielkriterien zur Erkennung von DLL-Hijacking	k. A.	k. A.	Laden einer DLLs von unsicheren Orten	Überwachung von DLL-Load Events, Laden unsignierter Bibliotheken
Erkennung von Persistenztechniken (Manipulation der Registry / Aufgabenplanung / Anlegen von Benutzerkonten / andere)	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / Laden von Kernelmodulen	✓ / ✓ / ✓ / –
Exploit-Schutz (Bufferoverflow-Schutz, ROP-Schutz, andere)	✓ / – / –	✓ / ✓ / –	✓ / ✓ / Heap-Spray-Schutz, Schutz des Elternprozesses	k. A.
Analyse des Netzwerkverhaltens des Endgeräts	Anomalieerkennung, Deep Packet Inspection möglich mit zusätzlichem Modul	Anomalieerkennung	Überwachung von Netzwerkverkehr	n. a.
Überwachung bestimmter Netzwerkprotokolle (DNS / HTTP(S) / FTP / SSH / andere)	✓ / ✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / – / –	✓ / ✓ / – / – / –	– / – / – / – / –
Deception-Techniken	n. a.	k. A.	Platzierung und Überwachung von Canary-Dateien	Platzierung und Überwachung von Canary-Dateien
zentrale Sandbox-Analyse				
unterstützte Dateitypen (ausführbare Dateien / Office-Dokumente / PDFs / Skripte / andere)	✓ / ✓ / ✓ / ✓ / ✓ / APK	✓ / – / – / ✓ / –	✓ / ✓ / ✓ / ✓ / APK, Linux ELF	n. a.
unterstützte Betriebssysteme (Windows / Linux / macOS / iOS / Android)	✓ / – / – / – / ✓	k. A.	✓ / ✓ / ✓ / – / ✓	n. a.
Response-Workflow				
Aufzeichnung administrativer Tätigkeiten (auf den Endgeräten ausgeführte Kommandos / Suchanfragen / Response-Schritte / Zugriff auf Logs / vollständiges Audit-Trail / andere)	✓ / – / ✓ / – / – / –	✓ / ✓ / ✓ / – / – / –	✓ / ✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / ✓ / ✓ / –
Alarmierung (E-Mail / SMS / Telefonanruf / andere)	✓ / ✓ / ✓ / Syslog, API, SIEM	✓ / ✓ / – / PowerAutomate, Teams	✓ / – / – / Slack, Syslog	✓ / – / – / Syslog, API, Slack
aktive Response-Möglichkeiten (Stoppen von Prozessen / Dateiwiederherstellung / Fernzugriff per Konsole / Client-Isolation / Löschen von Dateien / andere)	✓ / ✓ / – / ✓ / ✓ / Reboot, Herunterfahren, Log-out, Dumpen eines Prozessspeichers, Löschen von Registry-Werten	✓ / ✓ / ✓ / ✓ / – / –	✓ / ✓ / ✓ / ✓ / ✓ / Schwachstellenscan	✓ / ✓ / ✓ / ✓ / ✓ / –
automatische Response-Schritte (Stoppen von Prozessen / Unterbrechen von Prozessen / Client-Isolation / Löschen von Dateien / Dateiwiederherstellung / andere)	✓ / – / ✓ / ✓ / ✓ / weitere über Custom-Reactions	k. A.	– / – / – / – / – / Quarantäne für Dateien	✓ / ✓ / ✓ / ✓ / ✓ / Quarantäne für Dateien, Hochladen von Dateien
manuelle Abfrage von Information vom Endgerät (Dateien / Prozess-Dumps / Prozessliste / forensisch verwertbare Speicherabbilder / andere)	✓ / ✓ / ✓ / – / –	✓ / ✓ / ✓ / ✓ / –	✓ / – / – / – / Ausführen von Skripten	✓ / ✓ / ✓ / ✓ / Ausführen von Skripten
Kollaboration zwischen Analysten (integriertes Ticket-Tool / Kommentarfunktion / Jira-Integration / andere)	✓ / ✓ / – / –	✓ / – / – / –	– / ✓ / – / –	– / ✓ / – / –
Threat Hunting				
Suchkriterien für IoCs (Dateinamen / Datei-Hashes / Registry-Keys / IP-Adressen / Domainnamen / Netzwerkartefakte / andere)	✓ / ✓ / ✓ / ✓ / ✓ / ✓ / z. B. Umgebungsvariablen, installierte Treiber, USB-Geräte	✓ / ✓ / – / ✓ / – / ✓ / –	✓ / ✓ / ✓ / ✓ / ✓ / – / –	✓ / ✓ / ✓ / ✓ / ✓ / – / alle übermittelten Daten
eingebundene Threat-Intelligence-Datenbanken	McAfee GTI, VirusTotal, Phishtank, MVISION Insights	Microsoft Global Threat Optics, diverse Drittanbieter, z. B. Anomali, RiskIQ	VirusTotal, Palo Alto Networks AutoFocus Threat Intelligence Service	VirusTotal, Recorded Future, eigene Threat Intelligence, weitere über API

✓: ja / vorhanden / trifft zu; (✓): trifft eingeschränkt zu; –: nein / nicht vorhanden / trifft nicht zu; n. a: nicht anwendbar; k. A.: keine Angabe

Die Gefahr einer Monokultur besteht auch beim Einsatz der Securityprodukte von Microsoft. Auch das Unternehmen aus Redmond bietet mit seinem Defender for Endpoint ein EDR-Produkt an, das in Windows 10 bereits integriert ist und nur lizenziert werden muss. Das zusätzliche Ausrollen von Agenten kann damit entfallen. Die Lizenz ist beispielsweise im Microsoft-365-E5-Paket enthalten, das auch viele weitere Sicherheitsfeatures enthält. Organisationen, die eine solche Lizenz einsetzen, verwenden dann typischerweise auch den Defender AV und den Defender für Office 365 von Microsoft als Virenschutz. Das führt zu einer starken Abhängigkeit von einem einzelnen Hersteller, wenn vom Betriebssystem über die präventiven Sicherheitsfunktionen bis zur Erkennung und Reaktion alles aus einer Hand stammt.

Hindernisse bei der Erkennung

Schädliches von harmlosem Prozessverhalten zu unterscheiden, ist eine komplexe Aufgabe, die die verschiedenen Hersteller durch unterschiedlichste Ansätze anstreben. Die klassische, reputationsbasierte Verhaltenskontrolle beobachtet einen Prozess und bewertet jedes potenziell schädliche Verhalten. Wenn die Summe aus verdächtigen Einzelaktionen den gesetzten Schwellenwert überschreitet, wird ein Alarm und eine Reaktion wie das Beenden des Prozesses ausgelöst. Dieser Ansatz funktioniert beispielsweise dann gut, wenn ein aus einer E-Mail stammendes Office-Makro ausgeführt wird, das ein Programm aus dem Internet nachlädt und in den

Sequretek	Sophos	Trend Micro	Uptycs	WatchGuard	Wazuh
k. A.	k. A.	Reputationen und Dateisignatur	Überwachung von DLL-Load Events	Allowlist von Prozessketten, basierend auf Machine Learning und Threat-Intelligence-Daten	k. A.
✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / Erstellen von Systemprozessen, Autostart-Manipulation, Browser-Erweiterung	✓ / ✓ / ✓ / Manipulation des PowerShell-Profils, WMI-Persistenz, Autostart-Manipulation	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / –
✓ / ✓ / –	✓ / ✓ / Heap-Spray-Schutz, Erkennen von Reflective DLL Injection	✓ / ✓ / –	–	✓ / ✓ / –	– / – / Integration von Windows Defender Exploit Guard
k. A.	k. A.	Deep Packet Inspection	Socket-Events, DNS-Lookups, HTTP-Kommunikation	Deep Packet Inspection, Anomalieerkennung	n. a.
– / ✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / – / – / –	✓ / ✓ / ✓ / ✓ / –	n. a.
Platzierung und Überwachung von Canary-Dateien	k. A.	–	–	–	Honeypot-Ordner
✓ / ✓ / ✓ / – / –	✓ / ✓ / ✓ / – / –	✓ / ✓ / ✓ / ✓ / –	n. a.	✓ / – / – / – / –	n. a.
✓ / ✓ / – / – / –	✓ / – / – / – / –	✓ / – / ✓ / – / –	n. a.	✓ / – / – / – / –	n. a.
✓ / ✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / – / ✓ / –	✓ / – / ✓ / – / – / –	✓ / ✓ / ✓ / ✓ / ✓ / –	✓ / – / – / – / – / –	– / ✓ / ✓ / ✓ / ✓ / –
k. A.	✓ / – / – / API	✓ / – / ✓ / –	✓ / – / – / Slack, PagerDuty	✓ / – / – / –	✓ / – / – / Slack, API
k. A. / k. A. / ✓ / k. A. / k. A. / k. A.	✓ / ✓ / ✓ / ✓ / ✓ / ✓ / –	✓ / – / – / ✓ / ✓ / Blockade von IPs, Domains, URLs oder E-Mails	✓ / – / – / ✓ / ✓ / DNS-Blockaden	– / ✓ / – / ✓ / ✓ / Schwachstellenscan	– / – / – / ✓ / ✓ / Schwachstellenscan, Deaktivierung von Benutzerkonten, Blockieren von IPs oder Ports
k. A.	✓ / – / ✓ / ✓ / ✓ / –	✓ / – / ✓ / ✓ / – / –	n. a.	✓ / ✓ / ✓ / ✓ / ✓ / –	– / – / ✓ / ✓ / – / AV-Scan, Blockade von IPs und Ports
✓ / – / ✓ / ✓ / –	✓ / – / ✓ / – / Windows-Logs	k. A.	✓ / ✓ / ✓ / ✓ / –	✓ / – / ✓ / – / –	–
✓ / – / ✓ / –	– / ✓ / ✓ / –	✓ / ✓ / – / –	✓ / ✓ / – / –	✓ / – / – / –	– / – / ✓ / –
✓ / ✓ / k. A. / ✓ / ✓ / – / –	✓ / ✓ / ✓ / ✓ / ✓ / ✓ / – / –	✓ / ✓ / ✓ / ✓ / ✓ / ✓ / ✓ / Taktiken und Techniken	– / ✓ / ✓ / ✓ / ✓ / ✓ / – / –	✓ / ✓ / ✓ / ✓ / ✓ / ✓ / ✓ / Hashes von Prozessketten, Prozessaktivitäten	✓ / ✓ / ✓ / ✓ / ✓ / ✓ / – / –
VirusTotal	–	Trend Micro Smart Protection Network	VirusTotal	–	VirusTotal, AlienVault OTX

Die vollständige Tabelle ist über ix.de/zmtg zugänglich.

Autostart-Eintrag der Registry schreibt. Solche Indikatoren sind klare Anzeichen für Angriffe und erreichen schnell den Schwellenwert.

Schwieriger wird es, wenn ein Angreifer einen legitimen und von Windows signierten Prozess missbraucht, um in diesem Kontext den schadhaften Code auszuführen. An dieser Stelle muss der EDR-Agent eine Baseline an normalem Verhalten für diesen Prozess gelernt haben, um bei Abweichungen Alarm zu schlagen. Wenn beispielsweise der explorer.exe-Prozess seit Jahren keine Konnektivität ins Internet hatte, kann eine nun auftretende Kommunikation als Indikator für eine Infektion gewertet werden.

Die Rolle von KI

Bei allen Feinheiten der Unterscheidung bleibt allerdings ein Aspekt immer konstant: Der Prozess und alle dazugehörigen Operationen müssen vom Agenten in seinem gesamten Kontext betrachtet werden. Einen vom Anwender über den Desktop gestarteten PowerShell-Prozess sollte der Agent anders bewerten als einen PowerShell-Prozess, der aus einem Office-Makro gestartet wurde. Diese in Zukunft noch weiter wachsende Komplexität in Regeln abzubilden, ist nicht zielführend. Daher versuchen immer mehr Hersteller, wie auch in anderen Bereichen der IT, künstliche Intelligenz und maschinelles Lernen zum Schutz vor Angriffen und zur Erkennung von Malware zu verwenden.

Die KI-Komponente kann dabei entweder in der Cloud des Herstellers oder auf dem Endgerät selbst liegen. Bei herkömmlichen AV-Produkten beschränkt sich die

Aufgabe der KI darauf, Dateien als harmlos oder schädlich zu klassifizieren. Damit werden keine Signaturen mehr benötigt und das ständige Aktualisieren von Signaturlisten kann entfallen. Dadurch, dass neuronale Netze potenziell auch unbekannte Bedrohungen erkennen können, für die es noch keine Regeln gibt, kommt ein solches System in Summe auf beeindruckende Ergebnisse.

Im Fall von EDR beschränkt sich die Verwendung von KI nicht nur auf das Klassifizieren unbekannter Dateien, sondern dient auch der Einordnung von Prozessverhalten und dem Erkennen verdächtigen Verhaltens durch die Analyse korrelierender Events. Damit sollen auch raffiniertere Angriffstechniken wie dateilose oder speicherbasierte Malware erkannt werden. Bei beiden Verfahren wird der eigentliche Schadcode zur Laufzeit direkt in den Arbeitsspeicher geladen, ohne dass er zuvor in lesbarer Form auf der Festplatte abgelegt wird.

Einige Hersteller benutzen KI auch auf anderen Ebenen. McAfee beispielsweise setzt KI zusätzlich für eine sogenannte AI-Guided Threat Investigation ein, um Sicherheitsexperten bei der Auswertung von Alarmen zu unterstützen. Insbesondere geht es darum, Schlüsselereignisse zu einem bestimmten Incident zu identifizieren, was den erforderlichen manuellen Arbeitsaufwand reduziert.

Nicht alles Gold

Auch KI-Techniken haben ihre Schattenseiten. Bei der Klassifikation von Dateien verwenden beispielsweise die meisten Hersteller ihre KI-Komponente bisher überwiegend nur zum Klassifizieren ausführbarer Programme. Für Office-Dokumente, Bilddateien oder PowerShell-Skripte sind solche Modelle meist nicht anwendbar. Bei anderem verdächtigen Verhalten ist die KI überwiegend auf die Erkennung üblicher Angriffstechniken beschränkt. Ein professioneller Täter kann, wenn er das eingesetzte Produkt kennt, mit vertretbarem Aufwand einen Angriff so gestalten, dass er keinem bekannten Profil mehr folgt. Hierbei wird ein weiteres Grundkonzept klar: Bisher nicht klassifiziertes Verhalten wird oft nicht zuverlässig erkannt. Die meisten Hersteller verwenden die KI deshalb nur als Ergänzung zu herkömmlichen Erkennungsmethoden.

In Bezug auf die Marktübersicht ist KI auch ein schwieriges Thema, da viele der Hersteller bei Fragen zu Erkennungsmethoden und -kriterien ausschließlich auf ihre KI-Methoden verweisen. Für Experten ist daher manchmal unklar, welche Faktoren die KI tatsächlich berücksichtigt und mit welchen Daten sie trainiert wurde. Oft findet die finale Bewertung der Kritikalität der generierten Alarme in einer undurchsichtigen Blackbox statt und ist nicht eindeutig nachvollziehbar.

Alles beim Alten: Katz und Maus

Die Idee von EDR klingt sehr attraktiv, ist allerdings relativ jung und die Produkte entwickeln sich noch stark weiter. Gemeinsamer Nenner bei allen EDR-Produkten ist das Überwachen und Bewerten von Aktionen auf dem Betriebssystem. Windows bietet den EDR-Treibern dazu Schnittstellen, um verschiedene Informationen über das Starten von Prozessen oder Öffnen von Dateien abzugreifen. Professionelle Angreifer kennen diese Mechanismen allerdings und schaffen es immer wieder, sie auszutricksen. Dabei wird der Agent vom Angreifer in der Regel nicht gestoppt, was meist weitere Alarme nach sich ziehen würde, sondern vielmehr blind geschaltet.

Dazu muss der Angreifer seinen eigenen Treiber in das Betriebssystem laden und so die Schnittstellen zum EDR-Agenten kappen. Sobald ein Angreifer also hohe Privilegien auf einem System erreicht hat, kann man den Informationen und Alarmen dieses Systems nicht mehr vertrauen. Ein Analyst muss in der Lage sein, die bis dahin gesammelten Telemetriedaten auszuwerten und die richtigen Schlüsse zu ziehen.

An dieser Stelle beginnt das altbekannte Katz-und-Maus-Spiel zwischen dem Angreifer und dem EDR. Hier kann wiederum ein XDR-Produkt zu mehr Visibilität beitragen, um beispielsweise die Ausbreitung von Angriffen auch auf Netzwerkebene zu korrelieren und aufzudecken.

Viele der Hersteller bieten neben EDR-Agenten für Windows-Systeme auch solche für Linux und macOS an. Andere haben sogar Agenten für Android und iOS im Portfolio. Dabei ist allerdings zu beachten, dass viele der beschriebenen Funktionen nur für Windows im vollen Umfang anwendbar sind. Andere Betriebssysteme bieten gar nicht erst die nötigen Schnittstellen, um Telemetrie in dem Maße zu erfassen, mit dem ein EDR sinnvolle Rückschlüsse ziehen kann. Bei iOS beispielsweise beschränken sich die Funktionen meist auf den Schutz vor Malware und Phishing.

Fazit

EDR-Produkte schaffen eine deutlich höhere Transparenz auf dem Endpunkt und gewährleisten in Kombination mit den zumeist mitgelieferten Endpoint-Protection-Plattformen einen soliden Grundschutz. Die automatisierte Auswertung der Telemetriedaten zieht aber noch nicht immer die richtigen Schlüsse. Und selbst wenn der Agent technisch überzeugt, kann eine wirre und unübersichtliche Managementoberfläche bewirken, dass man nicht damit arbeiten möchte oder dass Alarme untergehen, die eigentlich eine höhere Aufmerksamkeit erfordern.

Bei dem eingangs erwähnten Angriff über SolarWinds Orion wären Kunden einiger EDR-Werkzeuge schon deshalb nicht betroffen gewesen, weil die dort verwendete Malware zunächst anhand einer langen Liste geprüft hätte, ob EDR- oder Forensikwerkzeuge auf dem Zielsystem installiert sind, und es gegebenenfalls nicht infiziert hätte. Das zeigt, dass auch aus Sicht der Malware-Autoren EDR- und XDR-Werkzeuge geeignet sind, irreguläre Aktivitäten frühzeitig aufzudecken.

Trotz aller konzeptionellen Vorzüge der Idee hinter EDR kommt es deshalb auf die tatsächliche Produktqualität im Einzelfall an. Die Produkte unterscheiden sich in der Konzeption meist nur wenig voneinander, in der Praxis jedoch erheblich. Um sie zu testen, benötigt eine Organisation jedoch meist die Unterstützung von Experten, die während der Testphase realistische Angriffe simulieren. Das einfache Starten von ein paar Malware-Samples oder Exploits in einer Testumgebung sagt wenig aus. Zudem ist der Markt jung und in Bewegung, sodass zu erwarten ist, dass kleinere Anbieter von größeren Herstellern aufgekauft und integriert werden und sich dabei die Produktstrategie ändert. (ur@ix.de)

Quellen

Das Angriffs-Framework MITRE ATT&CK und die ungekürzte Tabelle sind über ix.de/zmtg zu finden.

Konstantin Bücheler, Martin Hartmann und Alain Rödel

sind IT-Sicherheitsberater beim Heilbronner Beratungsunternehmen cirosec.

Stefan Strobel

ist Buchautor sowie Gründer und Geschäftsführer des IT-Sicherheitshauses cirosec.