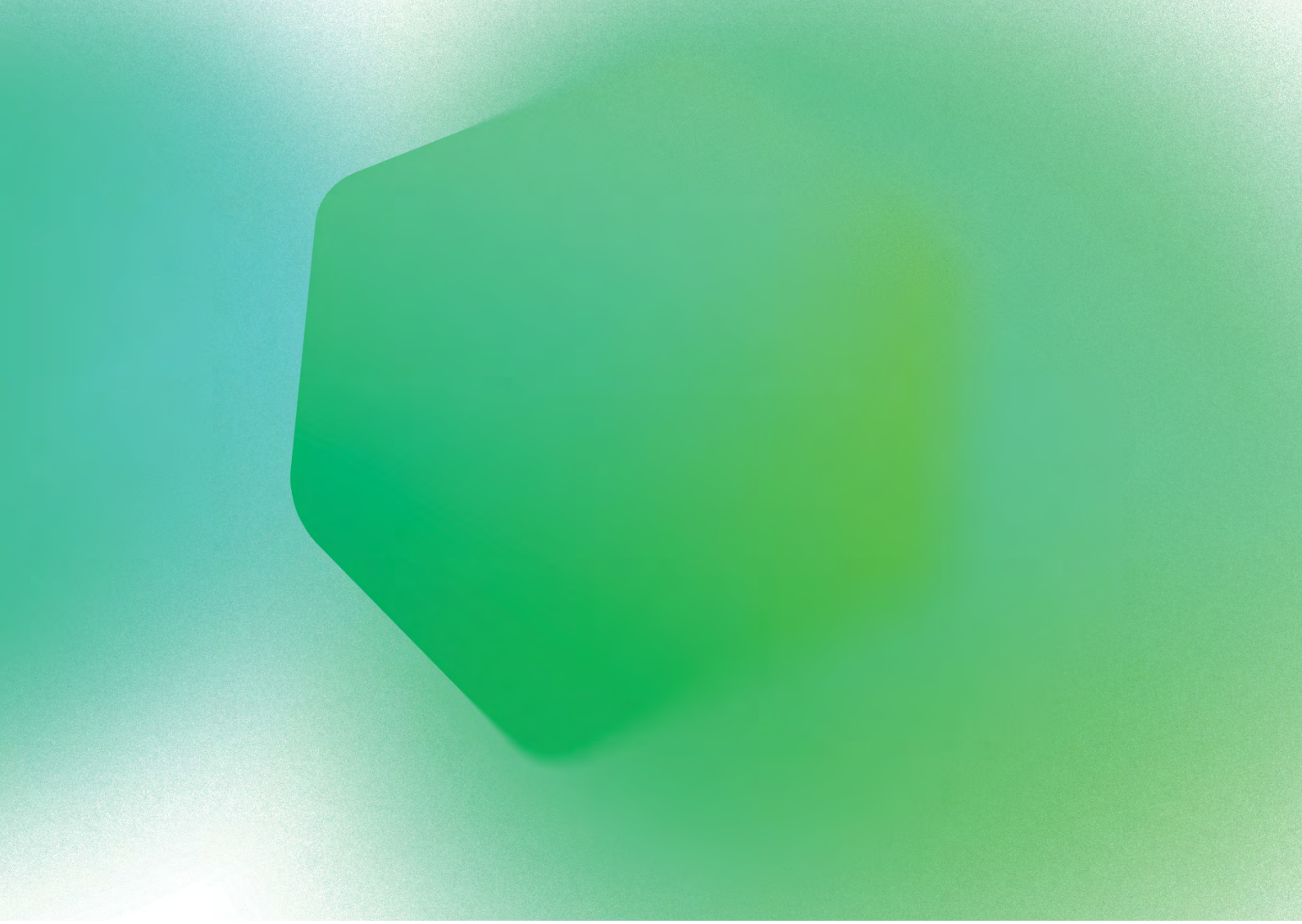


EDR – ein Fall für Automatisierung und Vereinfachung

kaspersky

Weitere Informationen finden Sie unter kaspersky.de
#bringonthefuture

Einleitung

Wenn Sie die Ereignisse der vergangenen Jahre verfolgt haben, ist Ihnen sicherlich nicht die große Panikmache angesichts der eskalierenden Zunahme und Komplexität von Cyberbedrohungen entgangen.

Das ist alles richtig. Aber es ist auch wieder nicht so neu. Cyberkriminelle entwickeln Angriffsmechanismen, Anbieter entwickeln Gegenmaßnahmen, woraufhin Cyberkriminelle Umgehungsmaßnahmen entwickeln, die wir wiederum mit weiteren Technologien kontern und so weiter. So läuft das Spiel seit Jahren.

Wahrscheinlich haben Sie auch schon von mehreren Seiten gehört, dass Endpoint Detection and Response (EDR) mehr eine Notwendigkeit denn ein Luxus ist.

Auch das ist richtig. Aber wie bei allen Aspekten der Cybersicherheit ist auch hier Ausgewogenheit gefragt. Mit welcher Wahrscheinlichkeit sind Sie welchen Formen von Bedrohungen ausgesetzt und wie viel Zeit, Geld und Ressourcen sollten Sie für welche Maßnahmen aufwenden? Die Antworten fallen je nach Art Ihres Unternehmens, der Größe und der geographischen Streuung sowie der zur Verfügung stehenden Mittel unterschiedlich aus.

Ist also jetzt die Zeit gekommen, um in EDR zu investieren? Die vergangenen Wochen und Monate, in denen so viele Unternehmen darauf angewiesen waren, dass ihre Mitarbeiter außerhalb der IT-Umgebung und des Gateway-Schutzes des Unternehmens arbeiteten, haben uns die Wichtigkeit unterbrechungsfreier und sicherer Zusammenarbeit und geschützter Kommunikationskanäle sowie unsere Abhängigkeit von effektiver Endpoint-Sicherheit dramatisch vor Augen geführt. Unternehmen gleich welcher Art und Größe und ungeachtet ihrer Kenntnisse im Bereich Cybersicherheit sollten jetzt in Erwägung ziehen, wie sie höhere Transparenz und verbesserte Erkennung komplexer Bedrohungen und sofortige Reaktionen auf diese erreichen können.

Dabei müssen Sie jedoch auch darauf achten, was Sie für Ihr Geld bekommen und wie Sie dieses einsetzen.

Was ist EDR?

Endpoint Detection and Response (Endpoint-Erkennung und -Reaktion, EDR) ist ein Element des Endpoint-Schutzes, das unterbrechungsfreie Überwachung von Endpoints bietet und moderne Bedrohungen an Endpoints erkennt und auf diese reagiert, während Antiviren- (AV) und Malware-Schutz primär in der Phase vor der Ausführung ansetzt. Obgleich EDR die Reichweite „herkömmlicher" Endpoint-Protection-Plattformen (EPP) erweitert, ist EDR nicht als Ersatz zu verstehen: Ihre Investition in EDR ist nur dann sinnvoll, wenn Sie bereits über ein solides Fundament von Schutzfunktionen verfügen. Wenn Sie lediglich planen, eine minderwertige Endpoint-Protection-Plattform durch Hinzufügen von EDR zu verbessern, sollten Sie sich zunächst auf eine Modernisierung Ihrer EPP konzentrieren.

Alle EDR-Produkte haben das gleiche Ziel: Moderne und komplexe Malware-Bedrohungen sollen schnell identifiziert, untersucht und gehandhabt werden. Das hierfür erforderliche Toolset umfasst die meisten, wenn nicht gar alle der folgenden Elemente:

- Eine Detection Engine mit Technologien wie Strukturanalyse auf Grundlage maschinellen Lernens und Sandbox-Emulation zur Erkennung und Abwehr von Malware-Mustern.
- Echtzeitanalyse zur Speicherüberwachung und zur Suche nach Verhaltensmustern, mit der Exploits erkannt und komplexe, zuvor unbekannte Bedrohungen schnell diagnostiziert werden können.
- Angewandte Threat Intelligence, die aus einer ganzen Reihe separater Quellen bezogen werden kann.
- Umfassende Endpoint-Transparenz – diese ist besonders wichtig zur Erkennung schädlicher Aktivitäten.
- Überwachung und Aufzeichnung von Ereignisdaten in Echtzeit sowie deren Weiterleitung zur Analyse.
- Forensik-Tools zur Vorfallsuntersuchung und zum Aufspüren von Bedrohungen, die unerkannt an einem Endpoint versteckt sind.
- Reaktion auf Vorfälle – Generierung automatischer Warnmeldungen und Antworten.
- Vorfallsfilterung zur Vermeidung von Fehlalarmen, damit keine Überlastung durch unnötige Warnmeldungen entsteht.

Nicht alle EDR-Tools arbeiten auf die gleiche Art und Weise. Bei manchen werden mehr Analysen am Agent ausgeführt, während der Schwerpunkt bei anderen über eine Verwaltungskonsole auf dem Backend liegt. Zeit und Umfang der Datenerfassung können variieren, ebenso wie Qualität und Quellen der Threat Intelligence. Und nicht jedes angebotene Tool passt zu Ihren bestehenden Cybersicherheits-Maßnahmen. So erfordert beispielsweise Threat Hunting Ressourcen und spezifische Fachkenntnisse, die in den meisten IT-Abteilungen nicht vorhanden sind.

Der Begriff „Endpoint Threat Detection and Response" (ETDR) wurde 2013 bei Gartner von Anton Chuvakin geprägt. Dieser definierte den Begriff als „Tools, die primär dazu dienen, verdächtige Aktivitäten und andere Probleme (und deren Spuren) auf Hosts/Endpoints zu erkennen und zu untersuchen". Der Begriff „Threat" fiel später weg und aus ETDR wurde EDR.

„Eine schwache Endpoint Protection Platform-Lösung [1] macht den Wert eines EDR-Tools zunichte"

2IDC, Endpoint Security 2020: The Resurgence of EPP and the Manifest Destiny of EDR, Dok.-Nr. US45794219, 2020

1 EPP – Endpoint Protection Platform

Statt also alle EDR-Lösung mit all ihren Funktionen zu bewerten, sollten Sie Ihr Augenmerk eher darauf richten, was Sie wirklich benötigen, um die bei Ihnen anstehenden Aufgaben zu erfüllen. Zahlen Sie also nicht für Funktionen, die Sie nie verwenden werden und die das System nur unnötig verkomplizieren. Wählen Sie ein Produkt, das in Ihr bestehendes EPP-System integrierbar ist und auf das Sie sich verlassen können, ohne Ihren Aufwand und Ihre Arbeitslast zu erhöhen.

Gegen welche Bedrohungen wird EDR eingesetztund wie arbeitet EDR?

Gefährdungsindikatoren
Bei IoCs handelt es sich um forensische Daten, mit denen potentiell schädliche Aktivitäten in einem System oder Netzwerk identifiziert werden und die bereits in den Anfangsphasen des Angriffs zur Erkennung schädlicher Aktivitäten führen können.

Für Cyberbedrohungen ist im Allgemeinen ein mehrschichtiger Ansatz am besten, bei dem mit einer Reihe von Filtern immer schwerer auffindbare Bedrohungen erkannt und bekämpft werden.

Sobald der Host angegriffen wird, wendet die Endpoint Protection Engine unterschiedliche Schutzmaßnahmen an, beispielsweise strukturelle ML-Modelle, Verhaltensanalysen und andere komplexe Erkennungstechnologien, mit denen die große Mehrheit der verbleibenden Bedrohungen identifiziert und neutralisiert werden kann.

Nachdem der Großteil der Malware durch diese direkten und hochautomatisierten Prozesse ausgesiebt wurde, können die Ressourcen auf den verbleibenden kleinen Rest fokussiert werden. Diese noch unerkannten Bedrohungen umfassen komplexe, schwer auffindbare und zielgerichtete Angriffe, die natürlich besonders gefährlich sind und schweren Schaden anrichten können.

Und hier kommt EDR zum Einsatz.

Eine der Hauptaufgaben von EDR ist es, für **Transparenz** zu sorgen, damit Ihr Team sehen kann, was an Ihren Endpoints tatsächlich vor sich geht. Schneller Zugriff auf Vorfallsdaten, Bereitstellung detaillierter Informationen und gezielte Scans auf Gefährdungsindikatoren (Indicator of Compromise, IoC) sind wesentliche Merkmale des Endpoint-Schutzes.

Eine weitere Schlüsselfunktion von EDR ist **Untersuchung.** Auch wenn mithilfe von EPP eine Reaktion beispielsweise auf das Ablegen einer Datei oder auf eine Prozessinjektion in einen regulären Prozess (Malware-freier Angriff) erfolgt ist, bedeutet dies nicht immer, dass die Bedrohung wirklich behoben wurde, insbesondere nicht bei komplexeren Angriffen. Ein eingehendes Verständnis der Bedrohungsursache sorgt dafür, dass etwaige noch vorhandene Komponenten einer Bedrohung nicht unbeachtet bleiben. So kann es beim einfachen Löschen einer schädlichen Datei vorkommen, dass der Hacker auf andere Art und Weise immer noch mit dem Host verbunden ist. Ebenso verhindert die Beendigung eines einzelnen Prozesses keine Neuinfektion, wenn die eigentliche Ursache nicht erkannt und behandelt wurde.

Darüber hinaus entwickeln sich viele moderne Bedrohungen sehr schnell und wenn die Komponenten einer Bedrohung nicht schnell erkannt werden, können die Folgen vernichtend sein (beispielsweise bei Ransomware). Daher ist eine **schnelle und möglichst automatisierte Reaktion** entscheidend, bei der eine Bedrohung nicht nur erkannt und analysiert, sondern auch neutralisiert wird.

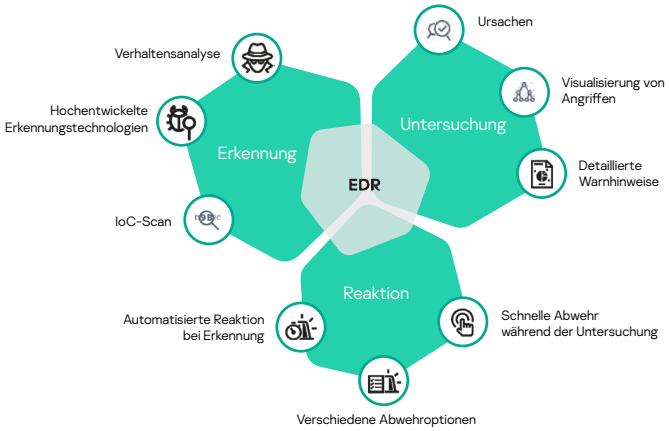


Abbildung 3 Die wichtigsten EDR-Funktionen

Anmerkung zu Ressourcen

Laut (ISC) liegt der globale Fachkräftemangel im Bereich IT-Sicherheit bei über 4 Millionen unbesetzter Stellen[2].

Cybersecurity Workforce Study, 2019, (ISC)[2]

Jede EDR-Lösung muss zu den Ressourcen passen, die Sie für die Einführung und Wartung bereitstellen können. Das Budget für Hardware und Software ist die eine Frage, die andere Frage ist: Wie finde ich entsprechend ausgebildete Mitarbeiter?

Der Fachkräftemangel im Bereich IT-Sicherheit hat mittlerweile krisenhafte Züge angenommen. Zum aktuellen Stand beträgt die Anzahl unbesetzter Stellen weltweit 4,07 Millionen, im selben Zeitraum waren es im Vorjahr noch 2,93 Millionen. Wenn also derzeit Ihr Personalstand an Fachkräften für IT-Sicherheit nicht voll belegt ist, sollten Sie nicht darauf bauen, dass sie neue Mitarbeiter finden werden. Sie werden wahrscheinlich eine andere Lösung finden müssen.

Wie weit lässt sich EDR automatisieren und vereinfachen?

Bei begrenzten Ressourcen besteht eine der effektivsten Möglichkeiten zur EDR-Bereitstellung darin, Prozesse dort, wo es möglich und sicher ist, zu automatisieren und jene Prozesse, bei denen eine Automatisierung nicht ratsam oder nicht praktikabel ist, zu vereinfachen. Automatisierung spart Zeit, Ressourcen und Geld und weil Maschinen weniger fehleranfällig sind als Menschen, steigert sie sogar die Wirksamkeit Ihrer Sicherheitsmaßnahmen. Je einfacher Ihre EDR-Lösung für Ihr Team zu handhaben ist, umso schneller und präziser werden ihre Mitarbeiter. Wenn Sie das Glück haben, über gut ausgebildete Fachkräfte im Bereich IT-Sicherheit zu verfügen, werden diese durch Automatisierung und Vereinfachung von mühsamen manuellen Aufgaben entlastet und können ihre kostbare Zeit echten Herausforderungen und interessanten Aufgaben widmen.

Welche EDR-Prozesse lassen sich effektiv automatisieren und wie können manuelle Prozesse vereinfacht werden?

Vorfiltern

Zu allererst muss Ihr Endpoint-Schutz in der Lage sein, Vorfälle effizient vorzufiltern, bevor EDR zum Einsatz kommt. Je früher in der Ereigniskette die große Mehrheit von Bedrohungen automatisch erkannt und behandelt wird, desto geringer sind die Gesamtauswirkungen auf Ihre Ressourcen. Die meisten Sicherheitsvorfälle können mithilfe einer guten EPP-Lösung direkt behoben werden, so dass die Kapazitäten Ihrer EDR-Lösung und Ihrer Mitarbeiter frei sind für die Abwehr komplexerer und damit auch gefährlicherer Bedrohungen. Wir können immer nur wiederholen: Achten Sie darauf, dass Ihre EPP-Lösung an der richtigen Stelle eingesetzt wird.

Vereinfachung der Vorfallsanalyse

Eine Analyse der Ursachen besteht, einfach gesagt, darin herauszufinden, was passiert ist und die Ursache dafür zu identifizieren und dafür zu sorgen, dass der Vorfall umfassend behandelt wurde und nicht wieder vorkommen kann.

Ein weiterer Schlüssel ist die Transparenz der Abläufe. Eine automatisch generierte und übersichtliche visuelle Darstellung der einzelnen Phasen des Ereignisses (das selbst mehr Elemente enthalten kann, einschließlich von bereits in ihrem System eingebetteten Komponenten, als im EPP zu diesem Zeitpunkt erkannt wurden) bietet alle für die Untersuchung erforderlichen Daten.

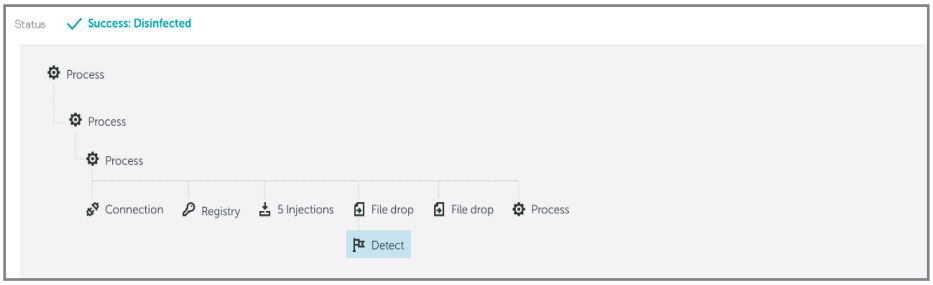


Abbildung 2: Visualisierung des Bedrohungspfades und der vorliegenden Verbindungen

Der zweite Schritt besteht in der automatischen Erstellung einer Warnhinweiskarte, auf der alle erforderlichen Daten an einer Stelle gesammelt werden, um so den Untersuchungsvorgang zu vereinfachen und zu beschleunigen. Diese Daten sollten die vollständigen Einzelheiten und den Kontext des Vorfalls umfassen: Wann genau und auf welchem Host das Ereignis auftrat, welche Nutzerkonten verwendet wurden, Detailinformationen zu Dateien, Prozessen, Änderungen an Registrierungsschlüsseln oder damit zusammenhängende Verbindungen.

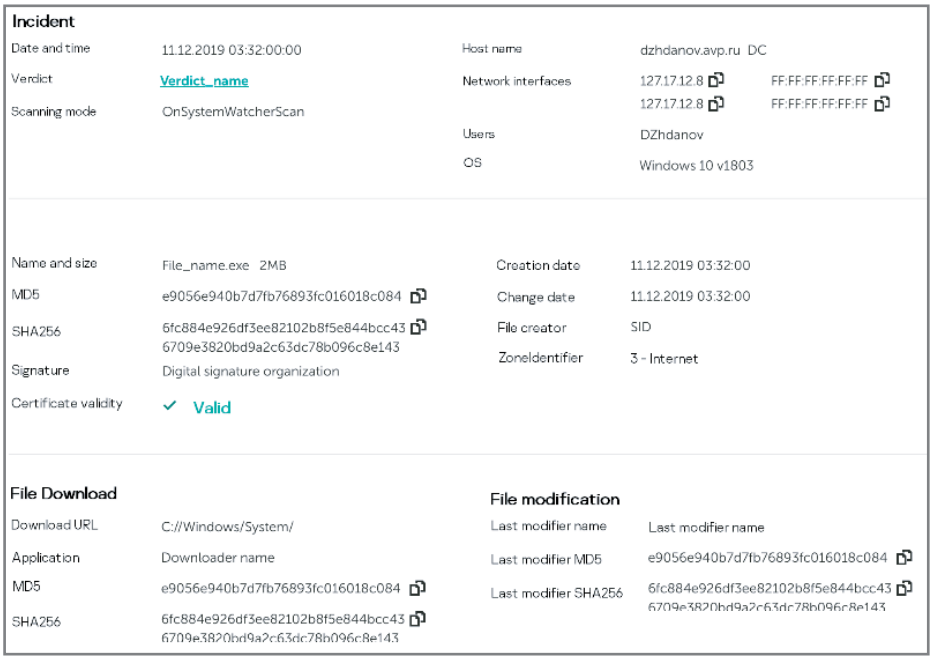
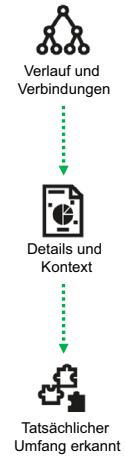


Abbildung 3. Beispiel einer Warnhinweiskarte mit den erforderlichen Informationen



Anwendungsfall

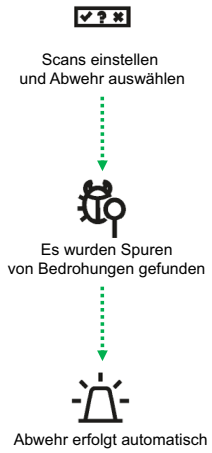
Per Mausklick öffnet der Sicherheitsbeauftragte die Warnhinweiskarte und sieht dort alle erforderlichen Informationen, beginnend mit den Daten zu Dateien und Hosts, den Erkennungsergebnissen und auf den einzelnen Erkennungsebenen erfolgten Reaktionen, bis hin zu detaillierter Visualisierung der Verbindungen zwischen den verschiedenen Ereignissen auf dem Host. Die übersichtliche Darstellung der Daten an einer Stelle vereinfacht die Untersuchung des Vorfalls. Gleichfalls kann herausgefunden werden, ob im System noch aktive oder inaktive Bedrohungskomponenten vorliegen oder ob der Umfang der Bedrohung größer ist, als es zunächst erschien. Der Sicherheitsbeauftragte kann dadurch sicherstellen, dass keine Überreste des Angriffs im System verbleiben.

Meldung von Gefährdungsindikatoren und automatische Scans

Die Ursachenanalyse eines Vorfalls kann dazu führen, dass aufgrund der mit der erkannten Bedrohung verbundenen Aktivitäten Gefährdungsindikatoren (IoCs) generiert werden. Scans auf IoCs sind, wie bereits gesagt, eine wichtige Abwehrmaßnahme in EDR, mit der Sie ermitteln können, welche anderen Hosts möglicherweise angegriffen wurden oder wo Anzeichen von Bedrohungen vorliegen. Bekannte IoCs (die Sie beispielsweise von einer Aufsichtsbehörde oder durch einen Newsletter oder eine Mailing-Liste erhalten haben) können als automatisierter Prozess importiert werden. Regelmäßige automatische Scans auf neue und importierte IoCs sind ein wichtiger Bestandteil der Systempflege. Da eine große Wahrscheinlichkeit besteht, dass eine einmal erkannte und analysierte Bedrohung erneut auftaucht, sind regelmäßige Scans auf IoCs, die durch analysierte Bedrohungen generiert wurden, von großem Vorteil. Und wenn Sie wissen, dass ein bestimmter Angriff für Ihre Branche typisch ist und entsprechende IoCs verfügbar sind, helfen Ihnen regelmäßige Scans auf diese importierten IoCs dabei, den Angriff in möglichst kurzer Zeit zu erkennen und abzuwehren.

Anwendungsfall

Sie erhalten Informationen über einen spezifischen Angriff, der Ihre Branche betrifft, so dass Sie nach bestimmten IoCs suchen müssen. Statt einer manuellen Suche können Sie diese IoCs einfach importieren und einen geplanten Scan einrichten.



Automatisierte Reaktion

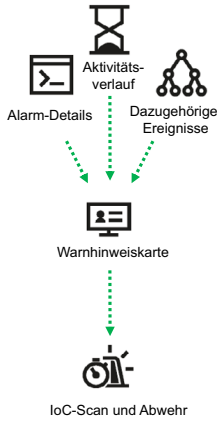
EDR-Lösungen müssen schnelle und automatisierte Reaktionen bieten, wozu es zwei effektive Möglichkeiten gibt: Automatisierung (wenn beispielsweise ein IoC-Scan ausgeführt wird und Bedrohungen gefunden wurden, auf die eine sofortige Reaktion erforderlich ist) oder direkt von der Warnhinweiskarte, wenn der Sicherheitsbeauftragte beispielsweise einen Host während der Analyse isolieren muss.

Mögliche Optionen bei der Reaktion auf Bedrohungen sind das Verhindern der Ausführung einer Datei (z. B. durch Erstellen einer Regel, mit der eine Datei mit einem bestimmten Hash für die Ausführung auf Hosts blockiert wird), das Isolieren eines befallenen Hosts, das Löschen einer Datei und das automatische Scannen anderer Hosts mithilfe von EPP.

Anwendungsfall

Während der Untersuchung stellt der Sicherheitsbeauftragte fest, dass eine bestimmte Datei oder Anwendung (z. B. ein legitimes RAT, Remote Administration Tool, von unklarer Herkunft) eine Komponente eines Cyberangriffs ist, die das Potential hat, zahlreiche schädliche Aktivitäten zu entfalten. Die Umstände (das Tool wurde auf einem Computer erkannt, auf dem vertrauliche Daten verarbeitet werden) machen es erforderlich, dass der Host als Vorsichtsmaßnahme unverzüglich isoliert wird, bis der Vorfall umfassend analysiert ist und der Angriff vollständig abgewehrt wurde.

Nachdem der Sicherheitsbeauftragte den Host isoliert hat, kann er einen IoC-Scan starten, um ähnliche Dateien auf allen Endpoints zu finden, wobei er eine automatisierte Reaktion einrichtet (z. B. Löschen der Datei oder gar Isolieren des Hosts vom Netzwerk zwecks weiterer Untersuchung) und damit sicherstellt, dass die Bedrohung unmittelbar nach Erkennung behandelt wird.



Alles beisammen halten

Das Wechseln zwischen mehreren Tools ist zeitaufwendig und aufgrund eingeschränkter Transparenz fehleranfällig. Ihre Mitarbeiter sollten über eine gemeinsame Konsole in der Lage sein, Untersuchungen und Ursachenanalysen durchzuführen, auf Bedrohungen zu reagieren und alle Prozesse zu verfolgen. Wenn Sie für Ihre EPP-Lösung die gleiche Konsole und den gleichen Agent verwenden können – umso besser.

Anwendungsfall

Wenn Sie eine verdächtige oder schädliche Aktivität aufdecken, müssen Sie nicht mehrere Tools öffnen oder gar den Endpoint selbst, um Protokolle, zugehörige Ereignisse sowie den EPP- und EDR-Aktivitätsverlauf zu analysieren oder IoC-Scans auszuführen, um dann womöglich mit noch einem anderen Tool auf die Bedrohung zu reagieren. Dies alles können Sie innerhalb einer einzigen Konsole erledigen.

Ergebnisse effektiver EDR-Implementierung unter Einbeziehung von Automatisierung

Automatisierung und Vereinfachung von Prozessen spart Zeit und Ressourcen – und erhöht die Sicherheit. Dies können Sie erwarten:

- Keine gefährlichen „Überbleibsel" von Angriffen – eindeutige Klärung, ob eine Bedrohung noch in Ihrem Netzwerk vorhanden ist oder nicht.
- Schnellere mittlere Zeit bis zur Abwehr (Mean Time to Respond, MTTR) von Vorfällen – für Ransomware eine entscheidende Metrik
- Vorfälle werden in jedem Einzelfall unverzüglich behandelt – ein hoher Automatisierungsgrad bedeutet, dass nichts vernachlässigt oder übergangen wird, weil sich vielleicht eine gewisse „Alarmmüdigkeit" breit gemacht hat.
- Mehr Aufmerksamkeit steht damit für Ereignisse zur Verfügung, für die wirklich ein Einsatz von Fachkräften erforderlich ist, der wiederum durch erhöhte Transparenz und detaillierte Vorfallsdaten unterstützt wird.
- Es sind keine Investitionen in zusätzliche Schulungen oder in die Einstellung weiterer Fachkräfte erforderlich, um Ihre EDR-Lösung im Tagesgeschäft zu verwalten – diese werden nur dort wo nötig eingesetzt.
- Ihr Team muss nicht mehr so viele Routineaufgaben erledigen und arbeitet mit einem einfachen EDR-Toolkit, was die Produktivität und die Zufriedenheit Ihrer Mitarbeiter steigert, die dadurch weniger anfällig für Abwerbeversuche werden.

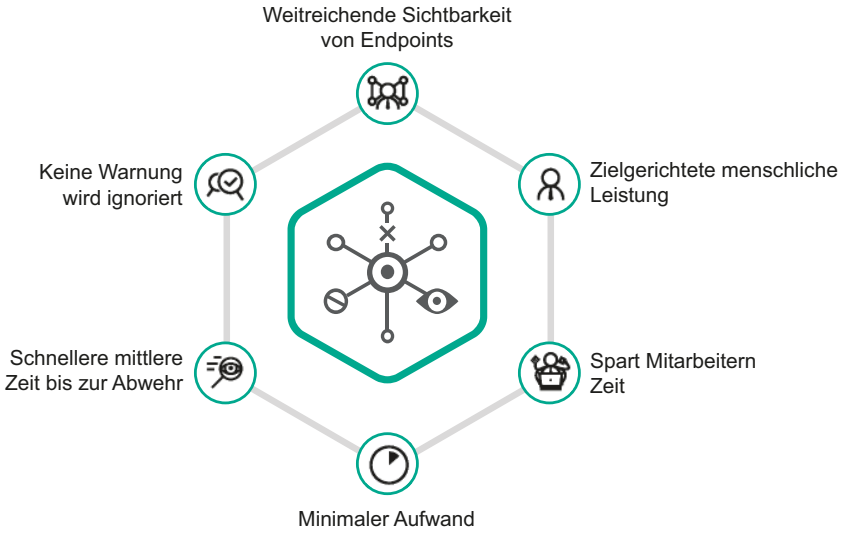


Abbildung 4: Die wichtigsten Ergebnisse einer effektiven EDR-Implementierung

Einführung in Kaspersky Endpoint Detection and Response Optimum

Auf Grundlage dieser Konzepte haben wir bei Kaspersky unser neues EDR-Produkt entwickelt – Kaspersky Endpoint Detection and Response (EDR) Optimum.

Mit Kaspersky EDR Optimum können Sie ohne zusätzlichen Aufwand eine zuverlässige weitreichende Abwehr gegen moderne komplexe Bedrohungen aufbauen.

Durch die Kombination eines benutzerfreundlichen hochautomatisierten Toolkits für Erkennung und Reaktion mit dem leistungsstarken Endpoint-Schutz und den hochentwickelten Erkennungsfunktionen von Kaspersky Endpoint Security for Business in einem einzigen Angebotspaket erhalten Sie effektive und effiziente Sicherheit für Ihre Endpoints.

Ein schlanker Workflow, kein zusätzlicher Aufwand und Automatisierung: Vorfälle werden schnell und effizient gehandhabt und entlasten dadurch Ihre Mitarbeiter in der Cybersicherheit.

Was kommt als Nächstes?

Jedes Unternehmen ist individuell. Deshalb appellieren wir an Sie, sich eingehend damit zu beschäftigen, welche EDR-Funktionen Sie für Ihr Unternehmen wirklich benötigen.

Benötigen Sie bessere Bedrohungserkennung und Abwehrfunktionen und möchten gleichzeitig Ihre Mitarbeiter durch ein einfaches und automatisiertes Tool entlasten? In diesem Fall könnte **Kaspersky Endpoint Detection and Response Optimum** das Richtige für Sie sein.

Oder benötigen Sie verbesserte Bedrohungserkennung, proaktives Threat Hunting und zentralisierte Möglichkeiten zur Reaktion auf Vorfälle, um Ihr Fachteam mit Tools zur Bekämpfung komplexer und gefährlicher zielgerichteter Angriffe auszustatten? Vielleicht finden Sie dann in **Kaspersky Endpoint Detection and Response** als Bestandteil von **Kaspersky Anti-Targeted Attack Platform** das, was Sie suchen.

Oder Sie benötigen vielleicht einen Rundum-Schutz für Ihre Unternehmen, damit Ihre Mitarbeiter und Ressourcen frei sind für andere Aufgaben? **Kaspersky Managed Detection and Response** erfüllt auch diese Bedürfnisse.

Wenn Sie Fragen dazu haben, wie Kaspersky Ihnen bei der Sicherheit Ihres Unternehmens helfen kann, besuchen Sie **https://kaspersky.de/enterprise-security/**.

Cyber Threat News:
https://de.securelist.com/
IT-Sicherheitsnachrichten:
business.kaspersky.de/

www.kaspersky.de

kaspersky BRING ON THE FUTURE