SOPHOS

5 Gründe für EDR

Tools im Bereich Endpoint Detection and Response (EDR) ergänzen Ihre Endpoint Security um leistungsstarke Funktionen zur Erkennung, Analyse und Reaktion. Im aktuellen Hype um EDR-Tools ist es allerdings oft gar nicht so einfach zu verstehen, wofür genau EDR eigentlich genutzt werden sollte und warum. Darüber hinaus sind die meisten EDR-Lösungen vielen Unternehmen heutzutage kaum von Nutzen, da sie ressourcenintensiv sind und in Bezug auf Bedienerfreundlichkeit und Schutzfunktionen zu wünschen übrig lassen.

Sophos Intercept X with EDR kombiniert intelligente EDR mit branchenweit erstklassiger Endpoint und Server Protection in einer Lösung. Damit erhalten Unternehmen detaillierte Informationen und können kritische Fragen zu Sicherheitsvorfällen beantworten. Im Folgenden zeigen wir Ihnen die 5 wichtigsten Gründe, warum Sie eine EDR-Lösung einführen sollten:

Sorgen Sie für die Einhaltung von Sicherheitsvorgaben und finden Sie verborgene Bedrohungen

Je nach Unternehmen können IT Operations und IT Security entweder zur selben Abteilung gehören, unabhängig agieren oder sogar in den Aufgabenbereich von ein und derselben Person fallen. Unabhängig davon erfordern beide Bereiche unterschiedliche Anwendungsfälle von einem EDR-Tool. Ein EDR-Tool sollte also in der Lage sein, beide Aufgabenbereiche abzudecken und ohne Leistungseinbußen zugänglich bleiben.

Für Administratoren im Bereich IT Operations hat die Einhaltung von Sicherheitsvorgaben in der IT-Umgebung ihres Unternehmens oberste Priorität. Sie müssen beispielsweise in der Lage sein, Systeme mit Leistungsproblemen wie geringem Festplattenspeicher oder hoher Speicherauslastung ausfindig zu machen. Sie müssen erkennen können, auf welchen Geräten Programme mit Schwachstellen vorhanden sind, die gepatcht werden müssen. Und sie müssen Endpoints und Server ausfindig machen können, auf denen unnötigerweise RDP oder noch Gastkonten aktiviert sind. Sophos EDR bietet Administratoren die Tools, um all diese Aufgaben zu erledigen. Außerdem können sie remote auf betroffene Geräte zugreifen, um Sicherheitslücken zu beheben, indem sie Leistungsprobleme untersuchen, Patches installieren und RDP und Gastkonten deaktivieren.

Cybersecurity-Spezialisten müssen in der Lage sein, subtile, evasive Bedrohungen aufzuspüren, die nicht automatisch von ihrem Endpoint-Schutz erkannt werden. Ihr EDR-Tool muss Indikatoren für eine Kompromittierung (Indicators of Compromise – IOCs) zuverlässig aufspüren können, z. B. Prozesse, die versuchen, eine Verbindung über Nicht-Standardports herzustellen, Prozesse, die Dateien oder Registry-Schlüssel bearbeitet haben oder Prozesse, die ihre wahre Identität verbergen. Zudem muss sich mit dem Tool ermitteln lassen, welche Mitarbeiter in einer Phishing-E-Mail auf einen Link geklickt haben. Mit Sophos EDR können solche Analysen für die gesamte IT-Umgebung eines Unternehmens schnell und einfach durchgeführt werden. Anschließend kann remote einfach auf betroffene Geräte zugegriffen werden, um weitere Analysen vorzunehmen, forensiche Tools bereitzustellen und verdächtige Prozesse zu beenden.

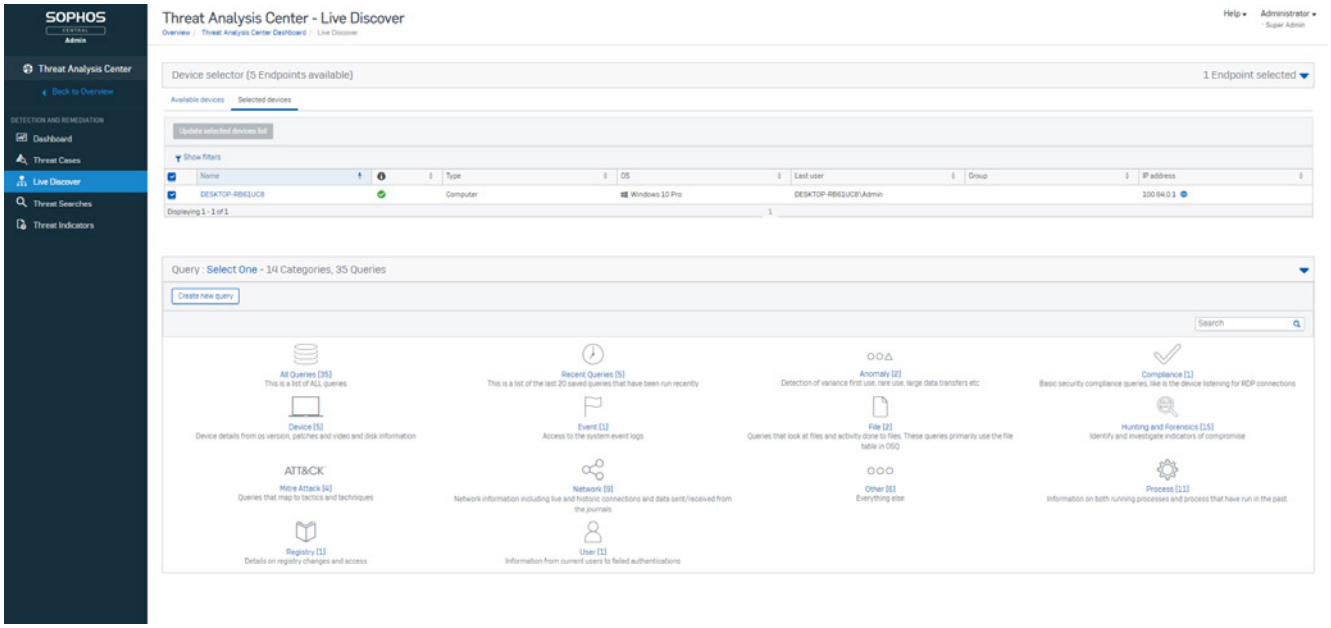

Abbildung 1: Mit Sophos Intercept X with EDR können Benutzer detaillierte Abfragen für ihre gesamte Umgebung durchführen

Erkennen Sie Angriffe, die bislang nicht bemerkt wurden

Bei entsprechendem Zeit- und Ressourceneinsatz auf Seiten der Angreifer sind auch die fortschrittlichsten Security Tools manchmal nicht in der Lage, Cyberangriffe abzuwehren. Häufig verlassen sich Unternehmen auf Präventionsmaßnahmen als einzigen Schutz. Dies ist ein großes Problem, denn Prävention ist zwar wichtig, aber nicht ausreichend. Genau hier kommt EDR ins Spiel.

Mit EDR können Unternehmen nach Indikatoren für eine Kompromittierung (Indicators of Compromise – IOCs) suchen. und damit schnell und einfach Angriffe aufspüren, die sonst unbemerkt blieben. Die Suche nach Bedrohungen wird häufig gestartet, nachdem ein Unternehmen von einer externen Stelle einen Hinweis erhalten hat. Beispielsweise könnte eine Regierungsbehörde ein Unternehmen über verdächtige Netzwerkaktivitäten informieren. Möglicherweise erhält das Unternehmen zusätzlich eine Liste mit Kompromittierungs-Indikatoren als Ausgangspunkt für die weitere Suche.

Die Funktion „Bedrohungsindikatoren" in Intercept X informiert über verdächtige Ereignisse. So wissen Analysten genau, was sie prüfen müssen. Mithilfe leistungsstarker Machine-Learning-Funktionen aus den SophosLabs wird eine Liste mit den verdächtigsten Ereignissen generiert, die nach ihrem Bedrohungswert absteigend sortiert angezeigt werden. So können Ihre Analysten wichtige Aufgaben mit Vorrang bearbeiten und sich auf das Wesentliche konzentrieren.

Wenn die Analysten wissen, wo sie ansetzen müssen, können sie alle Instanzen eines verdächtigen Elements in der gesamten IT-Umgebung aufspüren und schnell Maßnahmen zur Bereinigung ergreifen. Darüber hinaus können sie über leistungsstarke SQL-Abfragen weitere Indikatoren für eine Kompromittierung (Indicators of Compromise – IOCs) aufspüren, z. B. Prozesse, die Registry-Schlüssel bearbeiten, und Prozesse, die versuchen, eine Verbindung über Nicht-Standardports herzustellen.

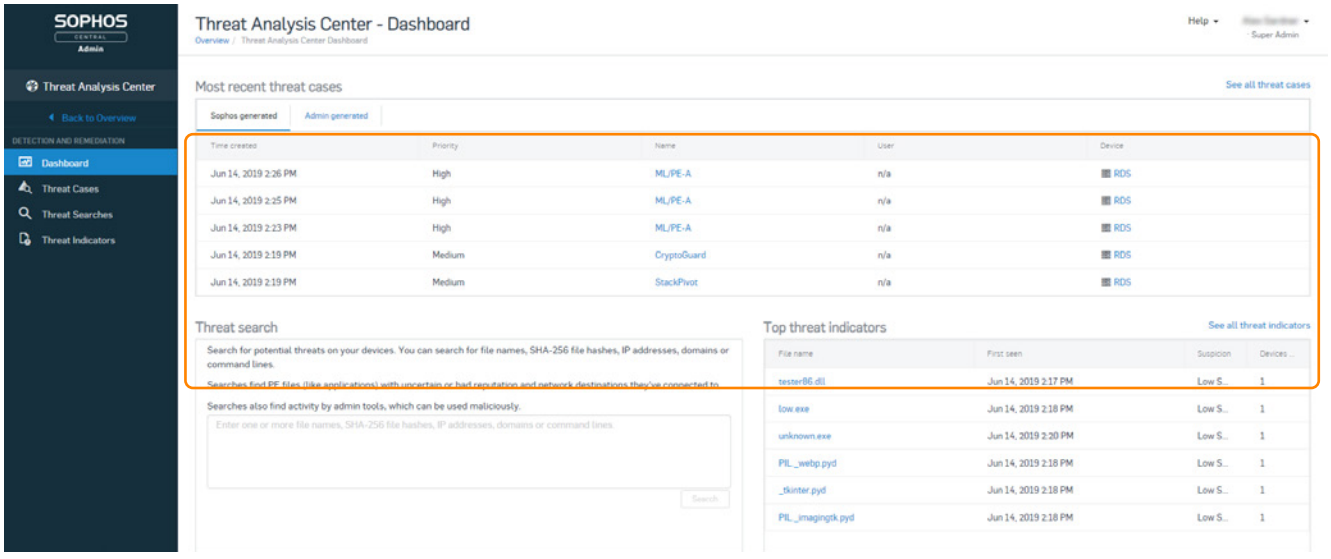

Abbildung 2: Sophos Intercept X with EDR ermöglicht die netzwerkweite Suche nach Indikatoren für eine Kompromittierung. Außerdem ermittelt die Lösung mit Hilfe von Machine Learning die verdächtigsten Ereignisse, die näher untersucht werden sollten.

Administratoren erhalten eine einzigartige Kombination an Funktionen: Sie können detaillierte Fragen stellen, erhalten Hilfestellung, wo sie mit ihrer Überprüfung starten sollten, und können auf minutiös gepflegte Bedrohungsdaten zurückgreifen. Dadurch ist Sophos EDR einfach zu bedienen und gleichzeitig hocheffektiv.

Reagieren Sie schneller auf potenzielle Vorfälle

Sobald ein Vorfall entdeckt wird, setzen IT-Abteilungen alle Hebel in Bewegung, um diesen schnellstmöglich zu beheben, denn das Ausbreitungsrisiko und der potenzielle Schaden sollen begrenzt werden. Die entscheidende Frage lautet: Wie kann jede mit dem Vorfall verbundene Bedrohung beseitigt werden? Im Durchschnitt ist eine IT-Abteilung über drei Stunden damit beschäftigt, einen Vorfall zu beheben. Mit EDR kann diese Zeit deutlich verringert werden.

In einem ersten Schritt würde ein Analyst zunächst die Ausbreitung des Angriffs verhindern. Intercept X with EDR isoliert Endpoints und Server bei Bedarf – ein wichtiger Schritt, um die Ausbreitung des Angriffs im Netzwerk zu verhindern. Analysten greifen oft direkt zu dieser Maßnahme, bevor sie eine weitere Überprüfung vornehmen, um Zeit zu gewinnen, während sie die optimale Vorgehensweise abstimmen.

Die genaue Überprüfung ist dann oft ein komplexer und mühsamer Prozess. Vorausgesetzt, sie wird überhaupt durchgeführt. Wenn auf einen Vorfall reagiert werden muss, kommt es vor allem auf hochqualifiziertes Fachpersonal an. Der Erfolg der meisten EDR-Tools hängt in erster Linie davon ab, ob Ihre IT-Mitarbeiter die richtigen Fragen stellen und Antworten auswerten können. Mit Intercept X with EDR können auch weniger spezialisierte IT-Abteilungen schnell auf Sicherheitsvorfälle reagieren, denn geführte Analysen enthalten Empfehlungen für nächste Schritte, eine verständliche visuelle Darstellung des Angriffs sowie integriertes Know-how.

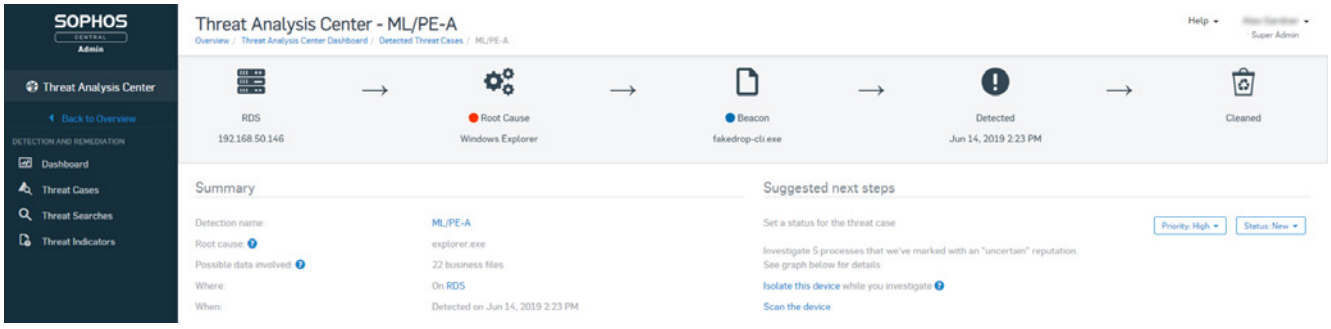

Abbildung 3: Die Funktion „Geführte Reaktion auf Vorfälle" empfiehlt nächste Schritte und isoliert Endpoints bei Bedarf zur schnellen und sicheren Behebung von Vorfällen.

Sophos EDR bietet außerdem die Möglichkeit, über eine Befehlszeilenschnittstelle remote auf Geräte zuzugreifen. So wird immer eine schnelle Reaktion ermöglicht – selbst wenn der betroffene Mitarbeiter nicht im Büro ist. Nach dem Zugriff auf das Gerät können Administratoren weitere Analysen vornehmen, indem sie forensische Tools bereitstellen, Software installieren/deinstallieren, Prozesse beenden und das Gerät neu starten.

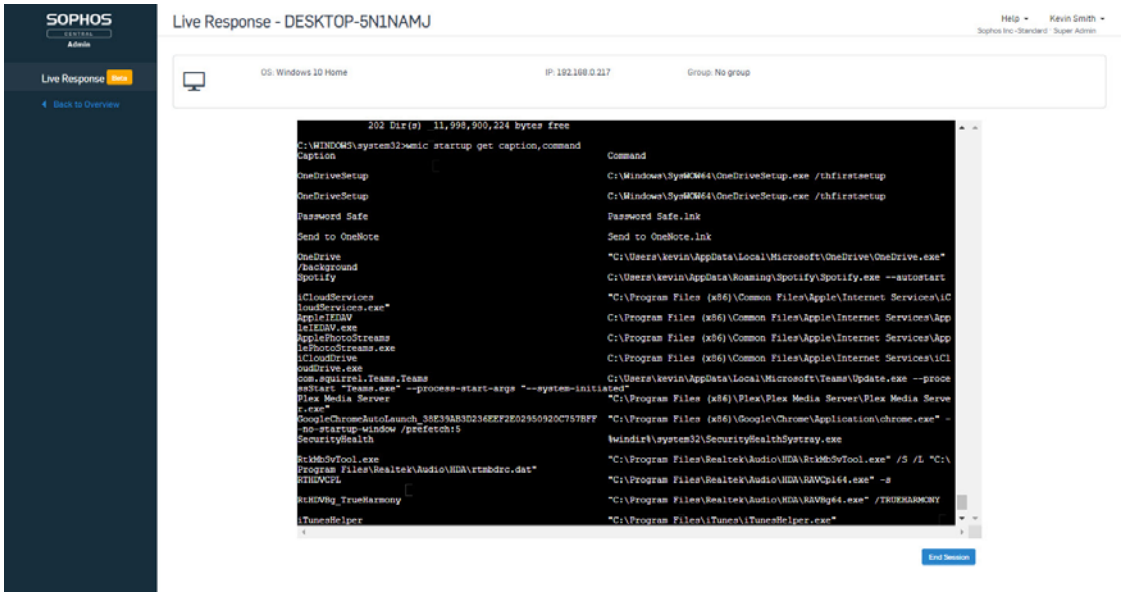

Abbildung 4: Intercept X with EDR bietet Schaltflächen mit zahlreichen Optionen zur Behebung von Vorfällen, u. a. die Option „Entfernen und blockieren".

Erhalten Sie fundiertes Expertenwissen – ohne zusätzliches Personal

Die meisten Unternehmen geben unzureichende Fachkenntnisse ihrer Mitarbeiter als Hauptgrund dafür an, keine EDR-Lösung einzuführen. Dies ist wenig verwunderlich, da der Fachkräftemangel im Bereich Cybersecurity schon seit Jahren intensiv diskutiert wird. Hiervon sind kleinere Unternehmen in besonderem Maße betroffen.

Die Hauptgründe, warum Unternehmen keine EDR-Lösung einführen:

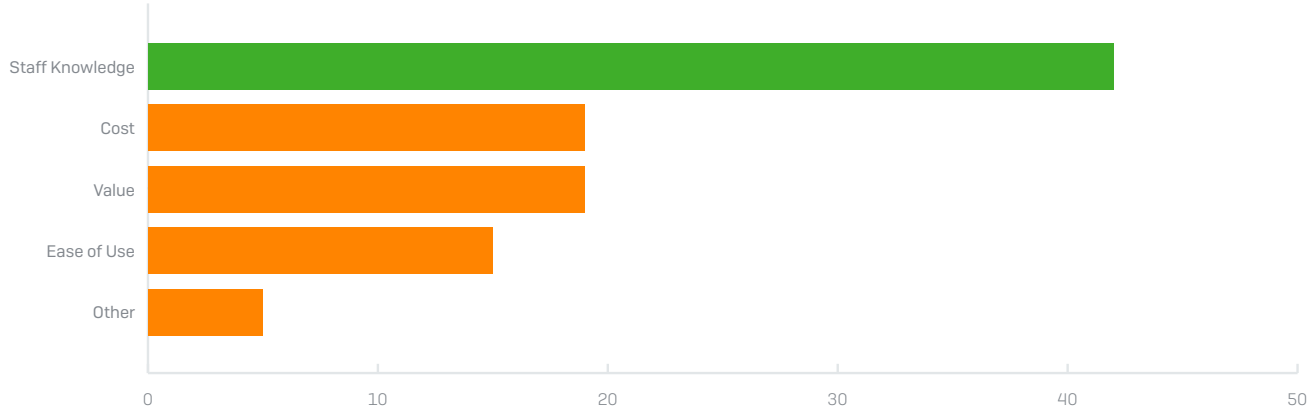

Abbildung 5: Mangelnde Fachkenntnisse der Mitarbeiter werden als Hauptgrund dafür angegeben, warum Unternehmen keine EDR-Lösung einführen (Quelle: Studie von Sapio Research in Zusammenarbeit mit Sophos, Oktober 2018)

Um dem Fachkräftemangel zu begegnen, übernimmt Intercept X with EDR die Aufgaben von schwer zu findenden Analysten. Mit Hilfe von Machine Learning liefert Intercept X Advanced with EDR detaillierten Einblick in Ihre IT-Sicherheit und nutzt außerdem aktuelle Bedrohungsdaten aus den SophosLabs. So erhalten Sie fundiertes Expertenwissen, ohne zusätzliche Mitarbeiter einstellen zu müssen. Intelligente EDR-Funktionen ergänzen die fehlenden Fachkenntnisse Ihrer Mitarbeiter und übernehmen die folgenden Aufgaben:

- Sicherheitsanalyse: Sicherheitsanalysten bilden die erste Verteidigungslinie. Sie erkennen Vorfälle und entscheiden, bei welchen Alarmmeldungen sofortiger Handlungsbedarf besteht. Im Idealfall gehen sie proaktiv vor, um Angriffe aufzuspüren, die eventuell noch nicht bemerkt wurden. Intercept X with EDR erkennt und priorisiert potenzielle Bedrohungen automatisch. Dank Machine Learning werden verdächtige Ereignisse erkannt und zur Priorisierung ihrer Dringlichkeit mit einem Bedrohungswert gekennzeichnet. Die Ereignisse mit den höchsten Bedrohungswerten erfordern sofortigen Handlungsbedarf. So können Analysten schnell feststellen, worauf sie sich konzentrieren sollten, und eine Sicherheitsüberprüfung starten.
- Malware-Analyse: Unternehmen verlassen sich häufig auf Malware-Experten, die verdächtige Dateien per Reverse Engineering analysieren. Diese Vorgehensweise ist zeitraubend und kompliziert, und viele Unternehmen verfügen auch nicht über das notwendige Fachpersonal. Hier ist die Expertise von Malwareanalysten gefragt, um zu beurteilen, ob es sich bei der blockierten Datei tatsächlich um Malware handelt. Möglicherweise untersucht der Analyst erkannte Dateien zudem mit besonderem Augenmerk auf False Positives. Die bessere Alternative: Intercept X with EDR mit Machine-Learning-Malware-Analyse. Unsere branchenführende Malware-Erkennungsengine analysiert mit extremer Genauigkeit automatisch Malware, indem sie Dateiattribute und Code aufschlüsselt und mit Millionen anderer Dateien vergleicht. So können Analysten schnell feststellen, welche Attribute und Code-Segmente als „als unschädlich bekannt“ und „als schädlich bekannt“ eingestuft werden und bestimmen, ob eine Datei blockiert oder erlaubt werden soll.
- Bedrohungsdatenanalyse: Zu Analysezwecken können von dritter Seite erhobene (und daher meist kostenpflichtige) Bedrohungsdaten herangezogen werden, um einen besseren Einblick in die Bedrohungen zu erhalten. Hier ist die Expertise von Analysten zur Interpretation und Integration dieser Daten gefragt, um einen Nutzen gewährleisten zu können. Bedrohungsdaten können als Ausgangspunkt für weitere Analysen verwendet oder hinzugezogen werden, um mit der Security Community verdächtige Dateien zu diskutieren. So können Sie schnell erkennen, ob Ihr Unternehmen gefährdet ist. Dank Intercept X with

EDR können Ihre IT-Sicherheitsadministratoren mehr Einblick erhalten und jederzeit Bedrohungsdaten aus den SophosLabs abrufen. Um volle Transparenz über die aktuelle Bedrohungslandschaft zu gewährleisten, untersuchen die SophosLabs täglich 400.000 einzigartige, bislang unbekannte Malware-Samples. Diese Bedrohungsdaten werden gesammelt und kategorisiert, um die Analyse so einfach wie möglich zu gestalten. Auf diese Weise können auch Sicherheitsteams, die nicht durch hochqualifiziertes Fachpersonal unterstützt werden oder kostspieligen Zugang zu komplizierten Bedrohungsdaten haben, von weltweit führender Spitzenforschung in der Cybersecurity profitieren.

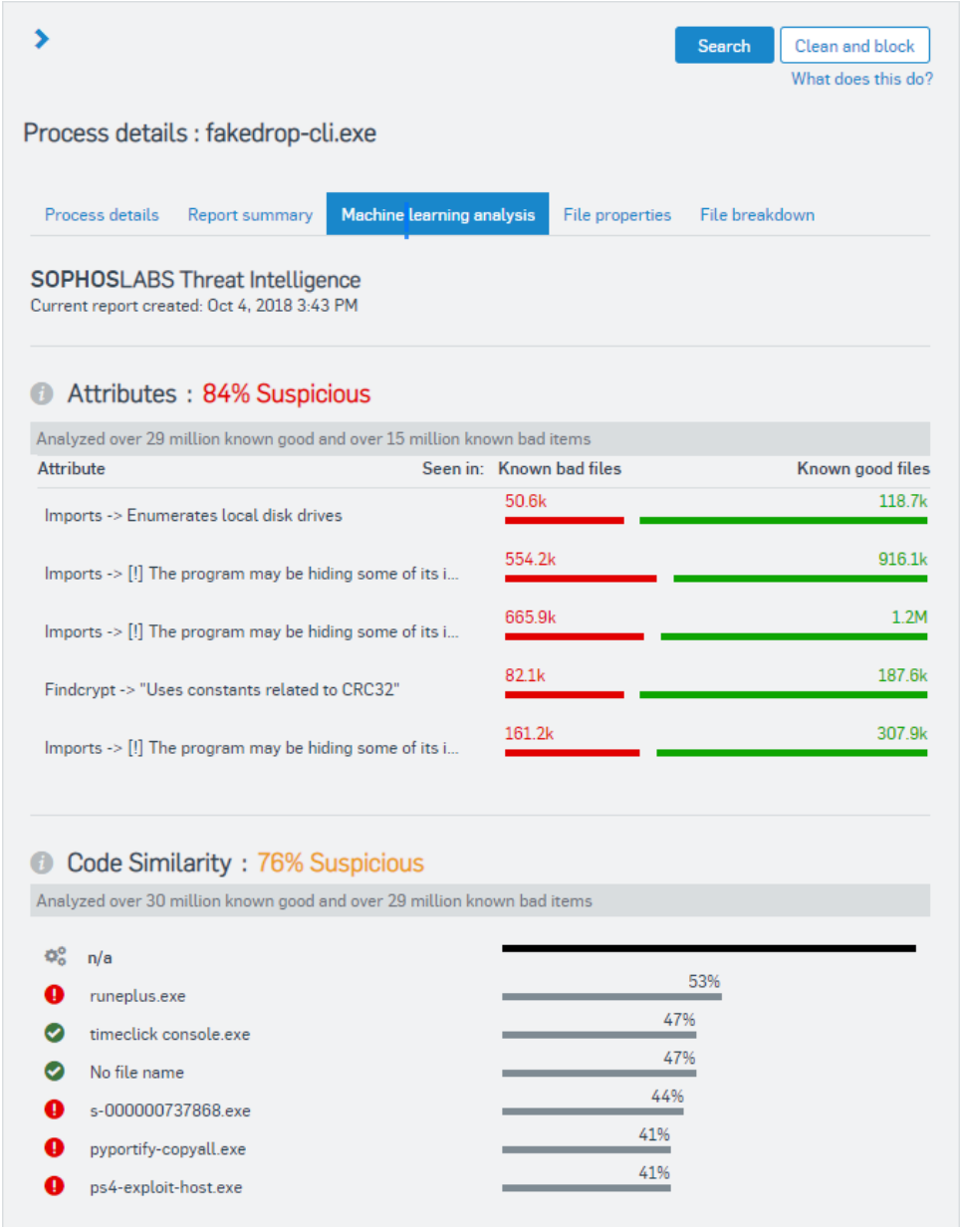

Abbildung 6: Die Machine-Learning-Analyse zeigt Attribute, Code-Ähnlichkeit und eine Dateipfad-Analyse für eine detaillierte und gleichzeitig einfache Analyse.

Managed Threat Response (MTR)

Benötigen Sie Hilfe bei der EDR-Verwaltung? Durch Kombination von modernsten Technologien und Expertenanalysen ermöglicht der Sophos MTR-Service eine bessere Bedrohungssuche und -erkennung, eine genauere Analyse von Warnmeldungen und gezielte Maßnahmen zur Beseitigung hochkomplexer Bedrohungen.

Verstehen Sie vergangene Angriffe und verhindern Sie diese in der Zukunft

Wurde ein Unternehmen Opfer eines Angriffs, werden Sicherheitsanalysten meist mit der Frage konfrontiert: „Wie konnte das passieren?“ Oft können sie diese Frage nicht beantworten. Durch das Erkennen und Entfernen der schädlichen Dateien wird zwar das unmittelbare Problem beseitigt, doch es wird nicht geklärt, wie die Malware in das System gelangt ist oder was die Angreifer getan haben, bevor der Angriff gestoppt wurde.

Intercept X with EDR bietet eine Übersicht über Bedrohungsfälle und zeigt alle Ereignisse, die zur Erkennung geführt haben. So lässt sich leicht sehen, welche Dateien, Prozesse und Registry-Schlüssel mit der Malware in Kontakt gekommen und welche Bereiche betroffen sind. Eine visuelle Darstellung der gesamten Angriffskette macht es ganz einfach möglich, zuverlässig Auskunft darüber zu geben, wie der Angriff begann und welchen Lauf er genommen hat. Ein weiterer wichtiger Vorteil dabei: Wurde die Ursache eines Angriffs gefunden, ist es sehr viel wahrscheinlicher, dass Ihre IT-Abteilung einen solchen Angriff künftig abwehren kann.

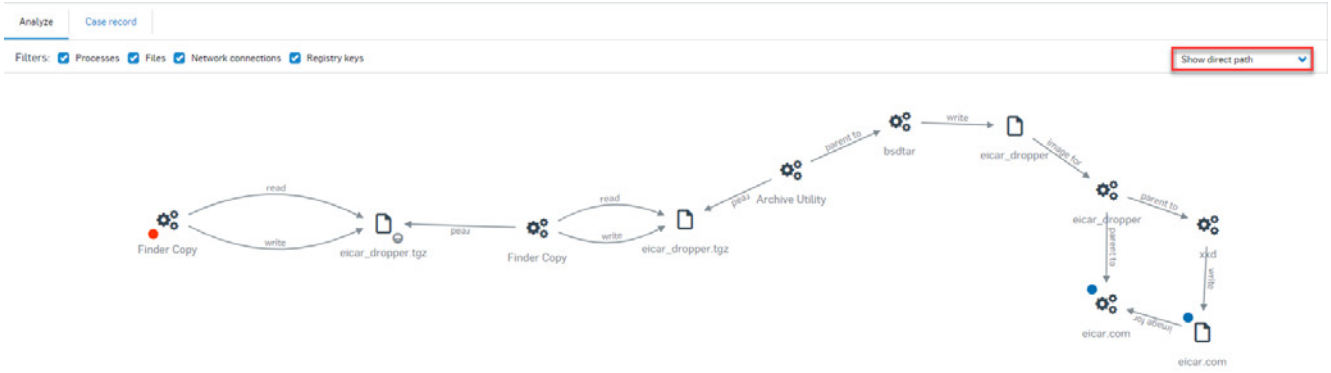

Abbildung 7: Bedrohungsfälle bieten eine visuelle und interaktive Darstellung der Angriffskette.

Transparenz über Ihre gesamte Cybersecurity-Umgebung

Sophos hat sowohl EDR als auch XDR (Extended Detection and Response) im Angebot. Damit erhalten Sie maximale Transparenz über Ihre Endpoints und Server und darüber hinaus auch Netzwerk- und E-Mail-Daten. Bei Bedarf können Sie von der ganzheitlichen Übersicht direkt zu spezifischen Detailinformationen wechseln. Kombiniert in einer einzigen Lösung erhalten Sie damit leistungsstarke EDR/XDR und branchenführenden Schutz, der neueste Bedrohungen wie Ransomware stoppt, Exploit-Techniken blockiert und Hacker-Aktivitäten unterbindet.

Weitere Informationen und eine Testversion finden Sie unter www.sophos.de/intercept-x.

Jetzt kostenfrei testen

Kostenlose 30-Tage-Testversion unter
www.sophos.de/intercept-x

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0 | +49 721 255 16 0
E-Mail: sales@sophos.de

2021-04-19 (MP)

SOPHOS