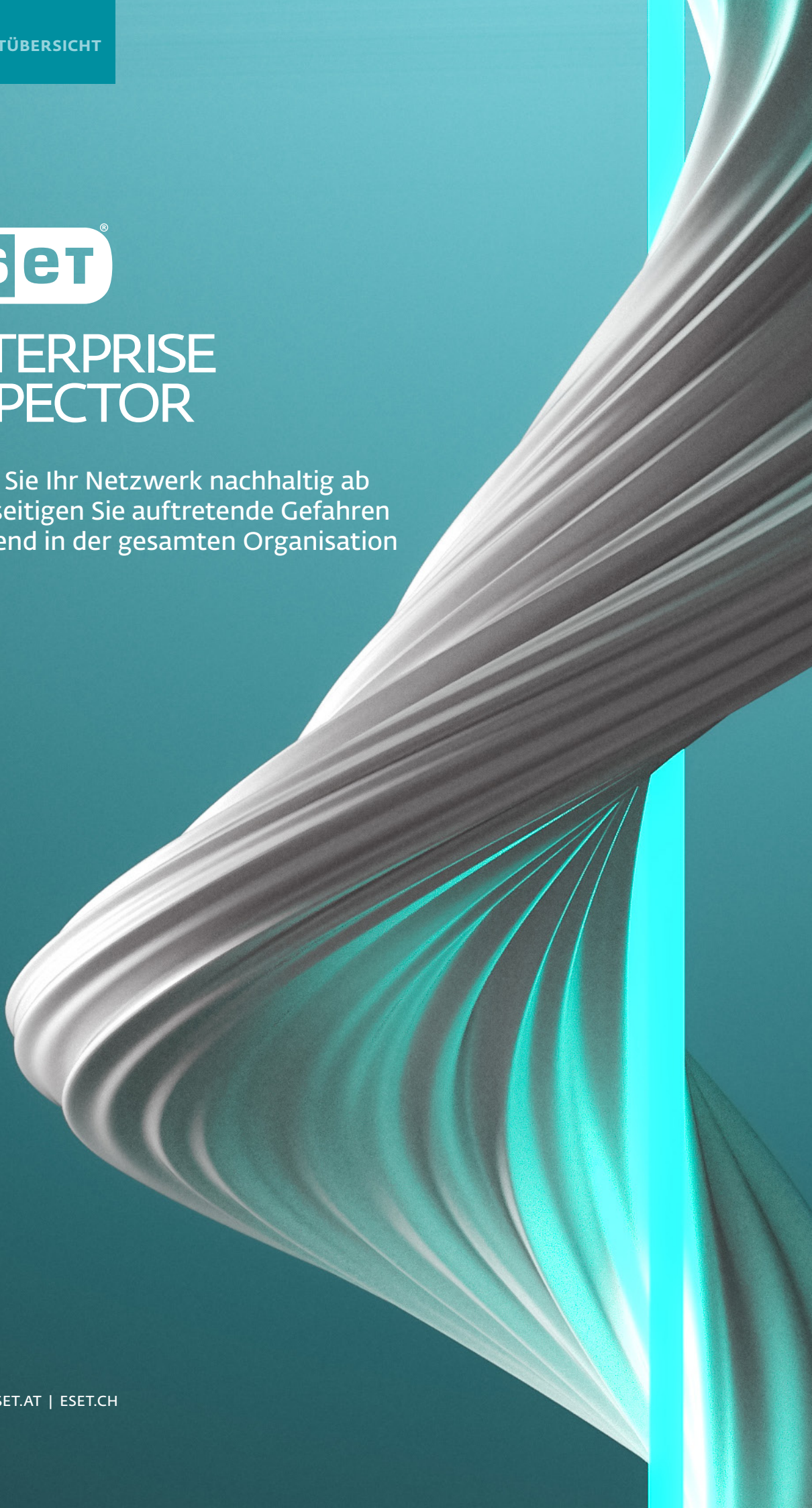
PRODUKTÜBERSICHT

ENTERPRISE INSPECTOR

Sichern Sie Ihr Netzwerk nachhaltig ab und beseitigen Sie auftretende Gefahren umgehend in der gesamten Organisation



VERFÜGBAR ALS MANAGED SERVICE

ESET.DE | ESET.AT | ESET.CH

Was ist eine **Endpoint Detection and Response (EDR) Lösung?**

Mit einem EDR-Tool decken Sie verdächtiges Verhalten sowie Sicherheitslücken auf und können Risiken besser abschätzen. Zudem ermöglicht es eine schnelle Reaktion auf Vorfälle sowie umfangreiche Analysen, wie es dazu kommen konnte.

Der ESET Enterprise Inspector (EEI) überwacht und bewertet alle Aktivitäten innerhalb des Netzwerks (Nutzer-, Datei-, Prozess-, Registry-, Speicher- und Netzwerkvorgänge) in Echtzeit, sodass Sie bei Bedarf schnell handeln können. Über die Management-Konsole ESET PROTECT (On-Premises) kann der ESET Enterprise Inspector gemeinsam mit anderen ESET Sicherheitslösungen zentral verwaltet werden.

Drei **gute Gründe**

DATENLECKS

Unternehmen sind heute mehr denn je in der Pflicht, Datenschutzvorfälle zu erkennen und Schäden so gering wie möglich zu halten. Dieser Prozess muss mit höchster Sorgfalt und ohne Unterbrechung des laufenden Geschäfts erfolgen. Allerdings fehlt es vielfach an unternehmensinternen Ressourcen, entsprechend umfassende Analysen durchzuführen. Viele Unternehmen verlassen sich daher auf externe Dienstleister. Zusätzlich müssen Unternehmen heutzutage über alle Vorgänge in ihrem Netzwerk informiert sein, um Angriffe von außen, Fehlverhalten von Mitarbeitern und unerwünschte Anwendungen umgehend entdecken zu können.

Besonders Branchen, die mit hochsensiblen und wertvollen Informationen arbeiten, sind für Angreifer interessant. Dazu gehören unter anderem die Finanzbranche, der Einzelhandel, das Gesundheitswesen und der öffentliche Sektor. Das heißt jedoch keineswegs, dass andere Branchen sicher sind. Wie jeder andere „Unternehmer" auch wägen professionelle Hacker Kosten und Nutzen einer Unternehmung sorgfältig ab. Entsprechend sollte man es Ihnen so schwer wie möglich machen.

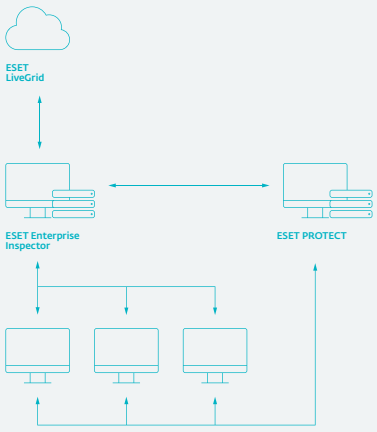
APTs UND GEZIELTE ANGRIFFE

Eines der wichtigsten Einsatzgebiete für EDR-Systeme ist die Identifikation von sogenannten Advanced Persistent Threats (APTs) und gezielten Angriffen. Außerdem helfen sie, die Reaktionszeit auf solche Angriffe zu verringern und zukünftige Vorfälle zu verhindern. Insbesondere APTs, vor allem solche, die sich teilweise monatelang im Netzwerk verborgen halten, sind für viele Unternehmen eine Bedrohung, der sie sich allein kaum gewachsen fühlen.

BESSERE TRANSPARENZ

Phishing-Angriffe und Social Engineering stellen ein großes Problem für Unternehmen dar, machen sie sich doch einen der verwundbarsten Angriffsvektoren zunutze: die Mitarbeiter des Unternehmens. Die Anzahl von Personen, die im Unternehmensnetzwerk arbeiten, ist teilweise unüberschaubar groß. Unternehmen bieten so eine große und potenziell sehr lukrative Angriffsfläche für Hacker. Schon ein einziger unaufmerksamer Mitarbeiter genügt, um die komplette Unternehmens-IT in Mitleidenschaft zu ziehen. Mit zunehmender Anzahl an Personen, die im Netzwerk arbeiten, steigt auch die Wahrscheinlichkeit, dass mindestens ein Mitarbeiter nicht im Interesse des Unternehmens handelt und sogenannte Insider-Attacken fährt.

EDR-Systeme helfen Unternehmen, alle verbundenen Geräte im Blick zu behalten und im Gefahrenfall Anwendungen oder ganze Geräte zu blockieren. Mit dem ESET Enterprise Inspector können Sie z.B. gefährliche Inhalte, die sich als Bestandteil von intakten Dateien wie Word-Dokumenten tarnen, schnell identifizieren und löschen.



Bietet Security-Teams einen umfassenden **Einblick in den verhaltens- und reputationsbasierten Erkennungsprozess**. Über LiveGrid erhalten Sie Feedback von mehr als 110 Millionen Endpoints in Echtzeit.

ESET Endpoint Sicherheitslösungen
Jede einzelne Schicht unserer Endpoint Lösung liefert Daten an den ESET Enterprise Inspector.

+

ESET Enterprise Inspector
Hochentwickeltes EDR-Tool, mit dem Sie in Echtzeit große Datenmengen analysieren und so jede Gefahr frühzeitig erkennen.

=

Eine umfassende Sicherheitslösungen zur Abwehr von Gefahren für Ihr Netzwerk, inklusive Maßnahmen zur Vorbeugung, Erkennung und Beseitigung.

Unternehmen müssen heute umfassend über die Vorgänge in ihrem Netzwerk informiert sein, um **Angriffe von außen, Fehlverhalten von Mitarbeitern** und **unerwünschte Anwendungen** umgehend zu identifizieren.

ESET **bietet einfach mehr**

SYNCHRONISIERTE REAKTION

Der ESET Enterprise Inspector basiert auf den bestehenden ESET Endpoint Sicherheitslösungen. Er agiert somit in einem kompletten Ökosystem und ermöglicht durch die Verknüpfung aller relevanten Objekte die synchronisierte Bekämpfung von Gefahren. Sicherheitsteams können Prozesse abbrechen, die Alarm verursachende Datei herunterladen oder das Herunterfahren bzw. einen Neustart oder Scan des betroffenen Rechners erzwingen sowie umgehend vom Netzwerk isolieren.

OFFENE ARCHITEKTUR

Bietet Security-Teams vollen Einblick in den verhaltens- und reputationsbasierten Erkennungsprozess. Alle Regeln sind in einem gängigen XML-Format definiert und lassen sich entsprechend der Gegebenheiten von Unternehmensumgebungen (z.B. SIEM) einfach anpassen oder neu erstellen.

REMOTE-ZUGRIFF

Der ESET Enterprise Inspector stellt PowerShell-Funktionen bereit, mit denen Security-Teams die Unternehmensgeräte aus der Ferne überprüfen und konfigurieren können. Das ermöglicht umgehende Reaktionen, ohne den Nutzer in seiner täglichen Arbeit zu stören.

ANPASSBARE SENSITIVITÄT

Verringern Sie die Wahrscheinlichkeit von Fehlalarmen, indem Sie die Erkennungsregeln je nach Computer- oder Nutzergruppe festlegen. Kombinieren Sie z.B. Dateiname, Pfad, Hash, Kommandozeile oder Bezeichner zur Anpassung der Trigger-Bedingungen.

MULTIPLATTFORM

Der ESET Enterprise Inspector unterstützt neben Windows auch macOS und ist damit die ideale Wahl für heterogene Netzwerk-Umgebungen.

ÖFFENTLICHE API

Die REST-API ermöglicht eine effektive Integration in Tools wie zum Beispiel SIEM, SOAR oder Ticketing-Tools.

ROLLENBASIERTE INSTALLATIONS-PROFILE

Wählen Sie bei der Installation Ihr bevorzugtes Profil - egal ob als Security Operations Center (SOC), sicherheitsorientiertes IT-Team oder allgemeiner IT-Admin. Entsprechend Ihrer Auswahl stehen Ihnen somit optimierte Ansichten zur Verfügung.

REPUTATIONSSYSTEM

Mithilfe von ESETs Reputationssystem lassen sich bekannte saubere Anwendungen herausfiltern. Das System nutzt dafür eine Datenbank aus mehreren Millionen gutartiger Dateien und verringert so die Wahrscheinlichkeit von Fehlalarmen. Dadurch bleibt dem IT-Team mehr Zeit für die Bearbeitung von potenziell gefährlichen Vorfällen.

MITRE ATT&CK™

Der ESET Enterprise Inspector verweist bei den Informationen über erkannte Schädlinge auf das MITRE ATT&CK™ Framework. Hier haben Sie mit nur einem Klick einen umfangreichen Überblick, selbst über komplexe Bedrohungen.

So **funktioniert's**

Umfassende Gefahrenanalyse – Ransomware

Ransomware ist mittlerweile zur akuten Bedrohung für Unternehmensnetzwerke geworden. Dabei verbleibt sie oft über Monate hinweg unbemerkt im Netzwerk und greift teilweise sogar Backup-Systeme an.

Der ESET Enterprise Inspector ergänzt die ESET Endpoint Sicherheitslösungen um die Möglichkeit, bereits im Netzwerk vorhandene Ransomware zu identifizieren. Typische Ransomware-Angriffe beginnen häufig ganz unauffällig damit, dass ein Nutzer eine E-Mail mit einem Anhang erhält, meist ein Word-Dokument. Der Nutzer öffnet dieses Dokument und wird aufgefordert, enthaltene Makros auszuführen. Tut er dies, verschlüsselt eine ausführbare Datei alle Daten, auf die sie zugreifen kann, Lösegeldforderungen folgen.

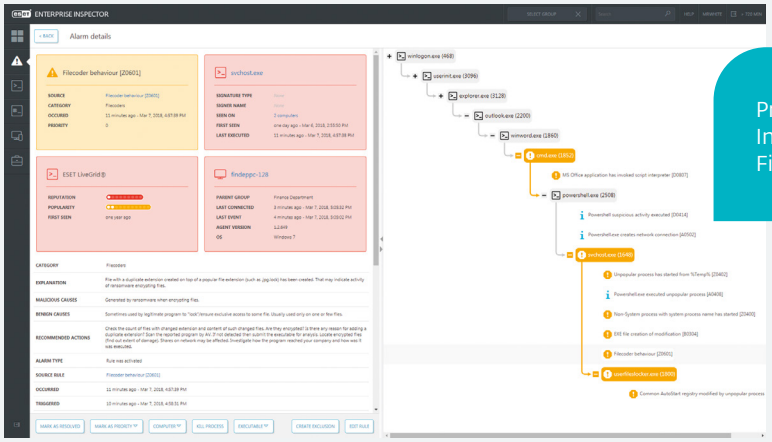
Der ESET Enterprise Inspector macht Verantwortliche hierauf aufmerksam. Mit nur wenigen Klicks können diese dann in Erfahrung bringen, welche Rechner und Laufwerke vom Angriff betroffen sind und wann und wo eine bestimmte Datei ausgeführt wurde. Die Infektion lässt sich so bis zu ihrem Ursprung zurückverfolgen.

PROBLEM

Unternehmen müssen in der Lage sein, Ransomware bereits vor einer tatsächlichen Infektion zu erkennen. Hat eine Infektion stattgefunden, müssen die Verantwortlichen umgehend informiert werden.

LÖSUNG

- ✓ Mithilfe umfassend konfigurierbarer Regeln werden Anwendungen erkannt, die aus temporären Ordnern ausgeführt werden.
- ✓ Ebenso lassen sich für Office-Dateien (Word, Excel, PowerPoint) Regeln festlegen, sobald diese versuchen, zusätzliche Skripte oder ausführbare Dateien zu starten.
- ✓ Werden Dateinamen, die für Ransomware typisch sind, auf einem Gerät erkannt, wird ebenfalls Alarm ausgelöst.
- ✓ Alle Benachrichtigungen des Ransomware Shields von ESET Endpoint Sicherheitslösungen werden übersichtlich in einer Konsole dargestellt.



Prozessablauf und detaillierte Information zum Verhalten eines Filecoders.

Verhaltenserkennung und „Wiederholungstäter“

Oft sitzt die größte Gefahr in Sachen IT-Security vor dem Rechner – unwissend und ohne böse Absichten.

Mithilfe des ESET Enterprise Inspectors lassen sich diejenigen Rechner identifizieren, die besonders viele Alarme ausgelöst haben. Hat ein Nutzer bereits mehrfach Alarm ausgelöst, können entsprechende Gegenmaßnahmen eingeleitet werden.

PROBLEM

In fast jedem Unternehmen gibt es Mitarbeiter, deren Rechner immer wieder mit Malware infiziert sind. Liegt es an unsicherem Verhalten auf Seiten des Mitarbeiters? Oder steht er, z.B. aufgrund seiner Position im Unternehmen, schlicht öfter im Fadenkreuz von Angreifern?

LÖSUNG

- ✓ Behalten Sie den Überblick über häufig infizierte Nutzer und Geräte.
- ✓ Identifizieren Sie den Grund für die Infektionen mithilfe einer detaillierten Ursachenanalyse.
- ✓ Ergreifen Sie Maßnahmen, um typische Angriffsvektoren wie E-Mail, Internet oder USB-Geräte abzusichern.

Mit dem ESET Enterprise Inspector kann jede Art von bösartigem Verhalten erkannt und genauer untersucht werden.

Gefahrensuche und -abwehr

Die besondere Stärke des ESET Enterprise Inspectors liegt in seinem Ansatz, den sprichwörtlichen Heuhaufen nach der Nadel zu durchsuchen.

Verschiedenste Filter helfen dabei, verdächtige Aktivitäten frühzeitig zu erkennen. Sie ermöglichen eine Sortierung nach Beliebtheit/Reputation, Signatur, Verhalten sowie Kontext-Informationen. Durch Anpassung und Kombination von Filtern lässt sich die Abwehr genau an die Bedürfnisse des Unternehmens anpassen und Erkennungs- bzw. Abwehrprozesse automatisieren.

PROBLEM

Ihr Frühwarnsystem oder SOC (Security Operations Center) gibt eine Warnung vor einer aktuellen Bedrohung heraus. Was ist nun zu tun?

LÖSUNG

- ✓ Nutzen Sie die Funktionalitäten des Frühwarnsystems, um detailliertere Informationen zu erhalten.
- ✓ Überprüfen Sie, ob sich der neue Malware-Typ bereits auf einem Rechner Ihres Netzwerk eingenistet hat.
- ✓ Prüfen Sie, ob IoCs anzeigen, dass die Malware schon vor dem Zeitpunkt der Warnung irgendwo innerhalb Ihres Netzwerks vorhanden war.
- ✓ Verhindern Sie, dass potenziell gefährliche Anwendungen ausgeführt werden.

Netzwerk-Transparenz

Die Architektur des ESET Enterprise Inspectors ist bewusst offen gehalten, sodass Sicherheitsteams je nach den Bedürfnissen des Unternehmens Modifikationen vornehmen können.

Zugleich ist es möglich, mithilfe des ESET Enterprise Inspectors Verstöße gegen Unternehmensrichtlinien zu identifizieren, z.B. die Nutzung von Torrents, Tor-Browsern und Cloud-Systemen sowie das Aufsetzen eigener Server und anderer unerwünschter Anwendungen.

PROBLEM

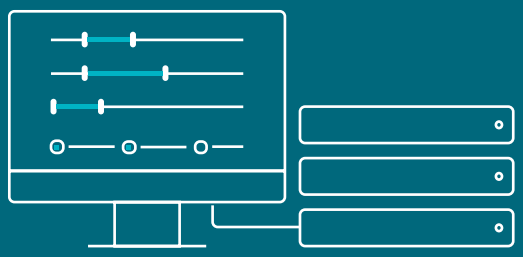
Viele Unternehmen wollen sicherstellen, dass Mitarbeiter keine unerwünschten Applikationen auf Unternehmensrechnern ausführen. Dabei geht es nicht nur um traditionelle Software, sondern auch um portable Anwendungen, die von einem mobilen Datenträger aus gestartet werden. Wie können sie dies gewährleisten?

LÖSUNG

- ✓ Behalten Sie den Überblick über alle Geräte und die darauf installierten Anwendungen.
- ✓ Überwachen Sie die Skripte, die auf den Geräten ausgeführt werden.
- ✓ Blockieren Sie unautorisierte Skripte oder Anwendungen.
- ✓ Informieren Sie Nutzer über unerwünschte Anwendungen und deinstallieren Sie diese automatisch.

Viele Unternehmen wollen sicherstellen, dass Mitarbeiter keine unerwünschten Applikationen auf Unternehmensrechnern ausführen. Wie können sie dies gewährleisten?

Sicherheitsteams können **Erkennungsregeln** den Bedürfnissen des Unternehmens anpassen.



Kontextbasierte Untersuchung und Gegenmaßnahmen

Wie gefährlich eine Datei tatsächlich ist, hängt auch stark vom Kontext ab, in dem sie ausgeführt wird.

So führt zum Beispiel ein Netzwerkadministrator gänzlich andere Anwendungen auf seinem Rechner aus als ein Mitarbeiter der Buchhaltung. Mithilfe vom EEI können Sicherheitsverantwortliche Rechner einzelnen Gruppen zuordnen und überprüfen, ob der Nutzer eine Aktion entsprechend seiner Rolle überhaupt durchführen durfte. Durch Synchronisation der Endpoint-Gruppen aus der Management-Konsole ESET PROTECT (On-Premises) mit den Regeln vom EEI lässt sich umfassender Kontext für die Untersuchung generieren.

PROBLEM

Ohne Kontext sind Informationen mehr oder weniger wertlos. Sinnvolle Entscheidungen lassen sich nur treffen, wenn folgende Informationen bekannt sind: Bedrohungsart, betroffenes Gerät und alarmierender Nutzer.

LÖSUNG

- ✓ Sortieren Sie Rechner entsprechend der Active Directory oder anhand automatisch/manuell festgelegter Gruppen.
- ✓ Erlauben oder blockieren Sie die Ausführung von Programmen oder Skripten für ganze Gruppen mit nur einem Klick.
- ✓ Erlauben oder verbieten Sie bestimmten Nutzern die Ausführung von Programmen oder Skripten.
- ✓ Legen Sie fest, dass Sie nur für bestimmte Gruppen Benachrichtigungen erhalten.

Einfaches Setup und Reaktion auf Vorfälle

Selbst wenn ein Unternehmen über ein eigenes Security-Team verfügt, muss dieses eine Vielzahl von Alarmen bearbeiten und priorisieren.

Der EEI schlägt daher für jeden Sicherheitsvorfall mögliche nächste Schritte vor. Wird eine Bedrohung erkannt, wird sogleich eine mögliche Gegenmaßnahme vorgeschlagen und auf Wunsch durchgeführt, z.B. Blockierung von Dateien, Abbruch/Quarantäne von Prozessen, Isolation einzelner Rechner und Abschaltung per Fernzugriff.

PROBLEM

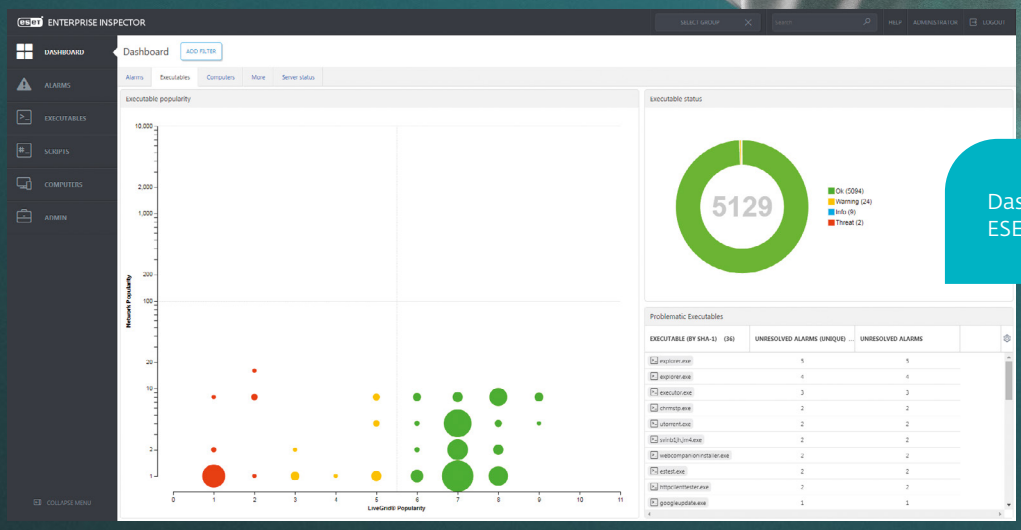
Nicht jedes Unternehmen hat eigene Security-Teams. Umfangreiche Erkennungsregeln zu erstellen und zu implementieren ist aufwendig und zeitraubend.

LÖSUNG

- ✓ Mehrere hundert vorkonfigurierte Erkennungsregeln
- ✓ Mit nur einem Klick lassen sich Geräte blockieren, herunterfahren oder in Quarantäne verschieben.
- ✓ Jede Benachrichtigung über einen Sicherheitsvorfall enthält zugleich mögliche nächste Schritte zur Wiederherstellung des Status quo.
- ✓ Die Regeln lassen sich ganz einfach per XML-Format modifizieren oder neu erstellen.

Wie gefährlich eine Datei wirklich ist, hängt stark vom Kontext ab, in dem sie ausgeführt wird.

Zu jedem Alarm werden Empfehlungen für Gegenmaßnahmen geliefert.



Dashboard des
ESET Enterprise Inspectors

Einsatzbereiche

THREAT HUNTING

Filtern und sortieren Sie Daten nach Beliebtheit, Reputation, Signatur, Verhalten oder Kontext-Informationen. Die Verwendung mehrerer Filter ermöglicht die automatische Suche nach Bedrohungen. Werden im EEI die Verhaltensregeln individuell angepasst, kann die gesamte Datenbank erneut auf nicht entdeckte Bedrohungen überprüft werden.

URSACHENSUCHE

Das Dashboard bietet einen Überblick über alle Sicherheitsvorfälle. Sicherheitsteams haben zudem die Möglichkeit, sich eine detaillierte Ursachenanalyse anzeigen zu lassen: Was war betroffen? Wo und wann wurden welche fraglichen Skripte oder Aktionen ausgeführt?

GEGENMASSNAHMEN

Nutzen Sie vorgegebene Regeln oder erstellen Sie eigene, um auf Vorfälle zu reagieren. Zu jedem Alarm werden Empfehlungen für Gegenmaßnahmen geliefert, z.B. Blockierung bestimmter Dateien per Hash, Beendigung oder Quarantäne von Prozessen sowie Isolation oder Abschaltung bestimmter Rechner. Dank dieser sogenannten Quick-Response-Lösungen kann kein Einzelvorfall das gesamte System kompromittieren.

GERÄTETRENNUNG MIT EINEM KLICK

Definieren Sie Regeln für den Netzwerkzugang, um die Ausbreitung von Malware zu stoppen. Isolieren Sie ein gefährdetes Gerät mit nur einem Klick in der EEI-Oberfläche vom Netzwerk.

PRIORISIERUNG VON MELDUNGEN

Stufen Sie die Relevanz von Warnungen über die Bewertungsfunktion ein, die bestimmten Ereignissen einen Schweregrad zuweist. So kann der Admin potenzielle Gefahren effizienter identifizieren.

TAGGING

Markieren Sie EEI-Objekte wie Computer, Alarme, Ausschlüsse, Aufgaben, auszuführende Dateien, Prozesse sowie Skripte, um sie schnell zu filtern und anschließend Nutzern/Gruppen zuzuordnen.

DATENSAMMLUNG

Erhalten Sie umfassende Informationen zu neu ausgeführten Elementen, z.B. über den Ausführungszeitpunkt, den ausführenden Nutzer, Verweildauer und betroffene Geräte.

SICHERE ANMELDUNG

Mit der Aktivierung der 2FA schützen Sie Ihr Admin-Konto zudem vor unerlaubten Zugriffen durch andere, selbst wenn diese Ihr Passwort kennen.

IDENTIFIKATION VON IOCS

Module lassen sich anhand von 30 Indikatoren einsehen und blockieren. Dazu gehören Hashes, Registry-Änderungen, Änderungen von Dateien oder Netzwerkverbindungen, usw.

ERKENNUNG VON VERDÄCHTIGEM VERHALTEN

Überprüfen Sie Aktivitäten von ausführbaren Dateien und nutzen Sie ESET LiveGrid®, um verdächtige Prozesse umgehend zu erkennen. Mittels individueller Regeln, die durch das Nutzerverhalten getriggert werden, können neben Schadsoftware auch verdächtige nutzerbezogene Ereignisse identifiziert werden. Durch die Zuweisung von Rechnern zu Nutzer- oder Abteilungsgruppen können Sicherheitsteams zudem unzulässige Aktionen schnell erkennen.

VERLETZUNG VON UNTERNEHMENSRICHTLINIEN

Verhindern Sie, dass schädliche Module in Ihrem Netzwerk ausgeführt werden. Mit dem EEI sind Sie in der Lage, Policy-Verletzungen bzgl. der Nutzung bestimmter Software zu identifizieren.

Über ESET

Als europäischer Hersteller mit mehr als 30 Jahren Erfahrung bietet ESET ein breites Portfolio an Sicherheitslösungen für jede Unternehmensgröße. Wir schützen betriebssystemübergreifend sämtliche Endpoints und Server mit einer vielfach ausgezeichneten mehrschichtigen Technologie, unterstützen Ihren Datenschutz mit Hilfe von Multi-Faktor-Authentifizierung und zertifizierten Verschlüsselungsprodukten oder halten Ihr Netzwerk mit Hilfe von Cloud-Sandboxing frei von Zero-Day-Bedrohungen. Unsere Endpoint Detection and Response Lösungen und Frühwarnsysteme wie Threat Intelligence Services ergänzen das Angebot im Hinblick auf Forensik sowie gezieltem Schutz vor Cyberkriminalität und APTs. Dabei setzt ESET nicht nur allein auf Next-Gen-Technologien, sondern kombiniert Erkenntnisse aus der cloudbasierten Repudationsdatenbank ESET LiveGrid® mit Machine Learning und menschlicher Expertise, um Ihnen den besten Schutz zu gewährleisten.

ZUFRIEDENE KUNDEN

BVB 09 Champion Partner

Seit 2019 ein starkes Team
auf dem Feld und digital

Allianz Suisse

Seit 2016 durch ESET geschützt
Mehr als 4.000 Postfächer

T

ISP Security Partner seit 2008
2 Millionen Kunden

BEWÄHRT

Security made in EU
Trust Seal www.teletrust.de/itsmie

ESET wurde das Vertrauenssiegel
„IT Security made in EU" verliehen

CERTIFIED ISO 9001:2015 COMPANY
CERTIFIED ISO 27001:2013 COMPANY

Unsere Lösungen sind nach
Qualitätsstandards zertifiziert

ESET IN ZAHLEN

110+ Mio.
Nutzer weltweit

400k+
Business-Kunden

200+
Länder & Regionen

13
Forschungs- und Entwicklungs-zentren weltweit

welivesecurity by eset

ESET Deutschland GmbH | Spitzweidenweg 32 | 07743 Jena | Tel.:+49 3641 3114 200

ESET.DE | ESET.AT | ESET.CH