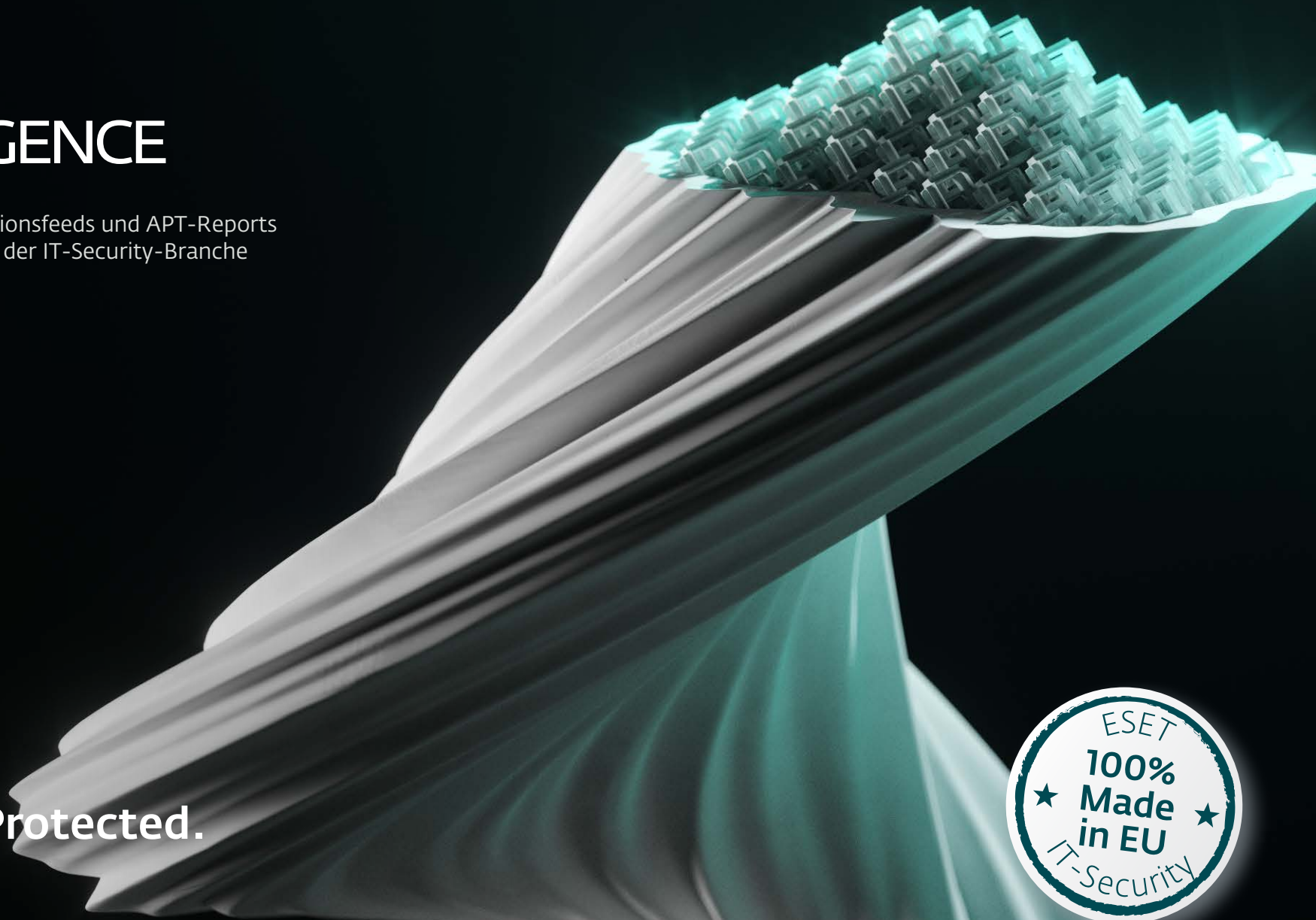
THREAT INTELLIGENCE

Hochwertige Informationsfeeds und APT-Reports
von den Top-Experten der IT-Security-Branche

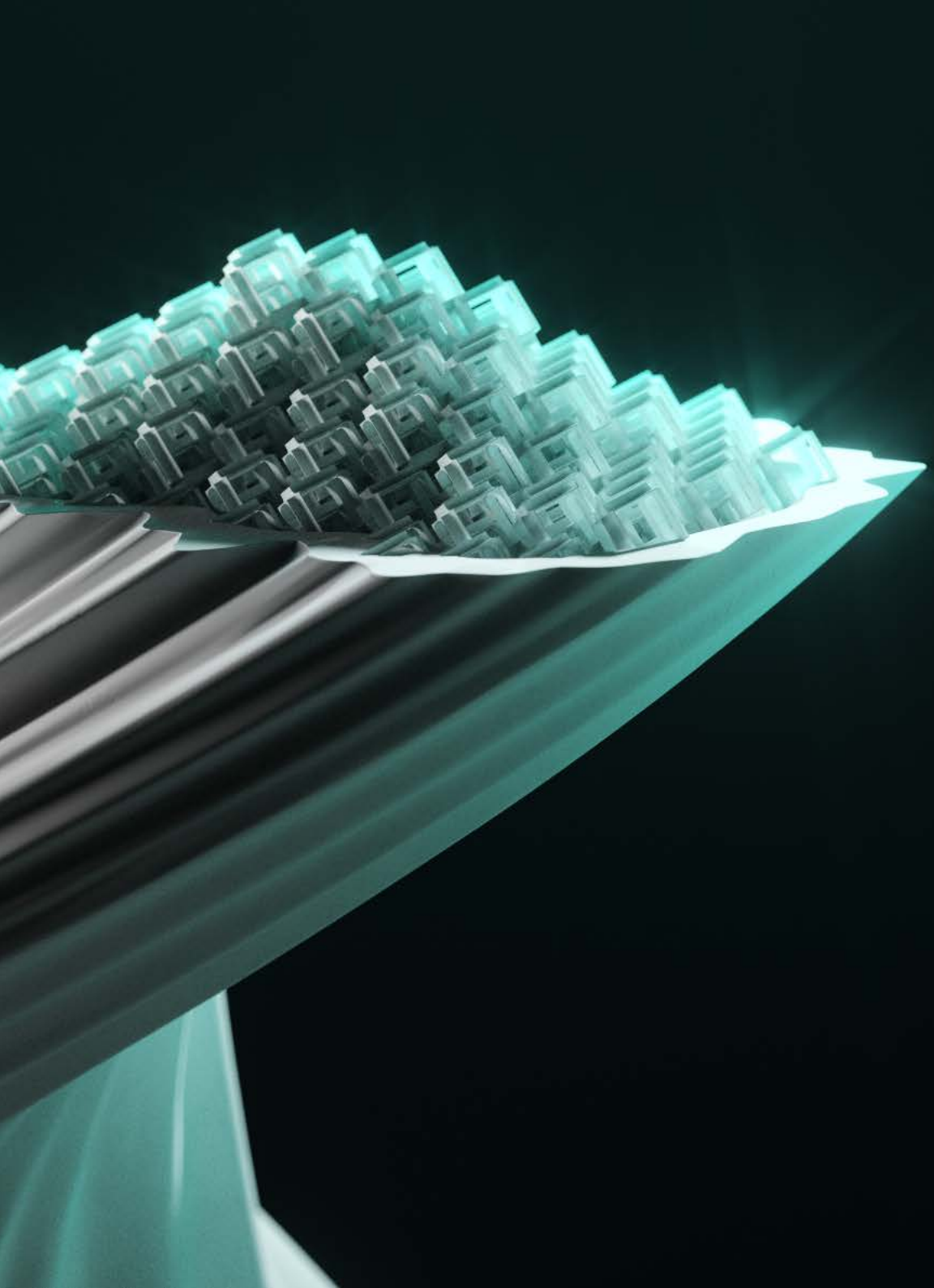
TEIL DER ZERO-TRUST-SECURITY-STRATEGIE



ESET 100% Made in EU IT-Security

Progress. Protected.

ESET.DE | ESET.AT | ESET.CH



Was ist Threat Intelligence?

Der Threat Intelligence Service von ESET bietet globales Wissen über gezielte Angriffe, Advanced Persistent Threats (APTs), Zero-Days und Botnet-Aktivitäten, das von den ESET Experten gesammelt wird. Damit unterstützt ESET IT-Verantwortliche dabei, Gefahren für das Unternehmensnetzwerk frühzeitig zu erkennen.

Gute Gründe für Threat Intelligence

BEZWINGEN SIE DIE INFORMATIONSFLUT

Ransomware, Zero-Days, Advanced Persistent Threats (APTs), gezielte Angriffe und Botnets stellen für Organisationen weltweit Probleme dar. Die Herausforderung besteht darin, dass Unternehmen aufgrund der Vielzahl an verschiedenen Bedrohungen nicht ohne Weiteres erkennen können, welche proaktiven Schutz- und Abhilfemaßnahmen am wichtigsten sind.

Das führt letztendlich dazu, dass Unternehmen versuchen, in verschiedenen Datensätzen aus externen Quellen aussagekräftige Informationen u.a. zu IoCs (Indicators of Compromise), den Angreifern, den Angriffsvektoren und zur Vorgehensweise/Verhaltensweise der Malware zu finden. Threat Intelligence Services helfen dabei, die hierdurch entstehende Datenflut zu bewältigen und die wesentlichen Informationen für spezifische Unternehmen zu extrahieren.

Mit Threat Intelligence Services können Organisationen Bedrohungen schnell und einfach priorisieren, sodass Ihnen mehr Zeit bleibt, um proaktiv neue Schutzmaßnahmen zu implementieren.

BEKÄMPFEN SIE BEDROHUNGEN PROAKTIV

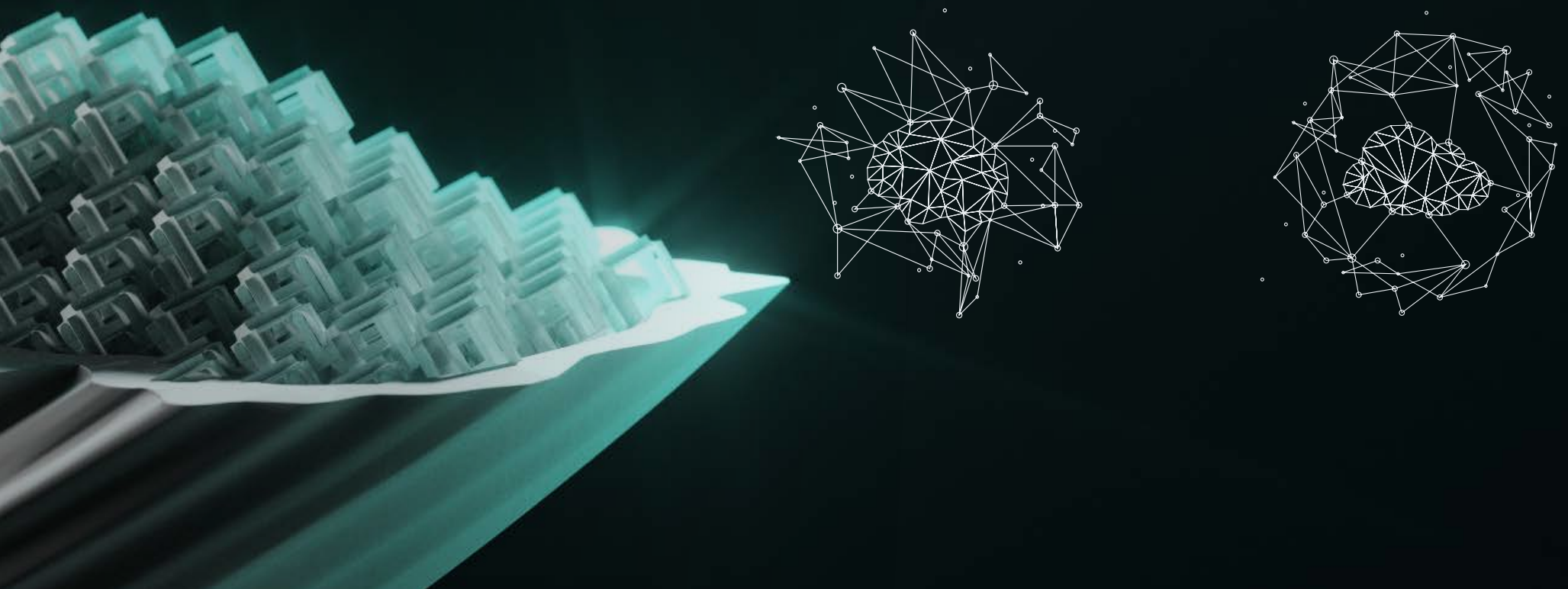
Die moderne Bedrohungslandschaft entwickelt sich rasant mit ständig neuen Angriffsmethoden und bis dahin unbekannten Gefahren.

Wenn es zu einem Angriff oder Datenschutzvorfall kommt, sind Organisationen in der Regel überrascht, dass ihre Abwehrmechanismen überwunden wurden, oder sie haben den Vorfall erst gar nicht bemerkt. Nachdem der Angriff schließlich entdeckt wurde, implementieren Unternehmen reaktiv Schutzmaßnahmen, um eine Wiederholung solcher Vorfälle in Zukunft zu verhindern. Das schützt Sie jedoch nicht vor Angriffen, die einen anderen Vektor nutzen.

Threat Intelligence Services bieten Einblicke in die aktuelle Bedrohungslage sowie potenzielle künftige Geschäftsrisiken. Hierdurch können Unternehmen proaktiv agieren und die Wirksamkeit ihrer Abwehrmaßnahmen verbessern.

ESET bietet einfach mehr

Menschliches Know-how gestärkt durch Machine Learning. Unser Reputationssystem ESET LiveGrid® nutzt über 110 Millionen Sensoren weltweit und wird angereichert durch Wissen unserer hauseigenen IS-Teams.



ESET bietet einfach mehr

1

MENSCHLICHES KNOW-HOW GESTÄRKT DURCH MACHINE LEARNING

Die Nutzung von Machine Learning zur Automatisierung von Entscheidungen und der Bewertung möglicher Bedrohungen ist ein Grundpfeiler unseres Ansatzes. Doch das System ist nur so stark wie die Personen, die dahinter stehen. Menschliches Know-how ist bei der Bereitstellung von Threat Intelligence Services entscheidend, um Fehlarme im System zu vermeiden.

2

STARKES REPUTATIONSSYSTEM – ESET LIVEGRID®

Die ESET Endpoint-Lösungen nutzen ein cloudbasiertes Reputationssystem, das Informationen über aktuelle Bedrohungen und saubere Dateien bereitstellt.
ESET LiveGrid® nutzt 110 Millionen Sensoren weltweit und wird in unseren Forschungs- und Entwicklungszentren geprüft. Dadurch können Kunden stets auf die Zuverlässigkeit der Informationen und Berichte in ihrer Konsole vertrauen.

3

IT-SICHERHEIT MADE IN EU

Seit 1987 ist ESET Teil der IT-Security-Branche mit Hauptsitz im Herzen Europas. Darüber hinaus verfügt ESET weltweit über 13 Forschungs- und Entwicklungszentren. ESET Lösungen sind zudem in mehr als 200 Ländern und Regionen erhältlich. So können wir frühzeitig auf Bedrohungen reagieren und Abwehrmechanismen gegen neuartige Malware-Trends entwickeln.

ESET bietet einfach mehr

EINZIGARTIGE EINBLICKE

ESET sammelt Daten zur aktuellen Bedrohungslage aus einer Vielzahl von Quellen weltweit und verfügt über herausragende Praxiserfahrungen. Vorallem geopolitische Einblicke auf aktuelle Ereignisse staatlicher Akteure machen unsere Daten so wertvoll.

SCHNELL UND RICHTIG HANDELN

Dank unserer umfassenden Berichte und vereinheitlichten Feeds erkennen Sie mögliche Bedrohungen umgehend und sind so in der Lage, schnellere und bessere Entscheidungen zu treffen. Mit diesem Frühwarnsystem minimieren Sie das Risiko eines erfolgreichen Angriffs.

AUTOMATISIERTE BEDROHUNGSANALYSE

Die ESET Technologien halten über verschiedene Ebenen hinweg permanent Ausschau nach Bedrohungen auf einem Gerät – von Pre-Boot bis Ruhemodus. Profitieren Sie von Telemetriedaten aus allen Ländern, in denen ESET aufkommende Bedrohungen aufspürt.

BEDROHUNGEN STETS EIN SCHRITT VORAUS

ESET folgt den Spuren des Geldes und überwacht insbesondere Orte, wo APT-Gruppen entdeckt wurden, die westliche Organisationen ins Visier nehmen: Russland, China, Nordkorea und Iran. So erfahren Sie zuerst von unbekannten, neuartigen Bedrohungen.

UPGRADE FÜR IHR SCHUTZLEVEL

Die ESET Datafeeds helfen Ihnen, Ihre Möglichkeiten zur Erkennung und Behebung von Bedrohungen zu stärken, APTs und Ransomware zu blockieren und Ihre IT-Infrastruktur insgesamt nachhaltig abzusichern.

Advanced Persistent Threat (APT) Reports

PROFITIEREN SIE VON UNSERER FORSCHUNG

Unser Forschungsteam ist in der digitalen Sicherheitswelt bereits bekannt, unter anderem dank unseres mehrfach ausgezeichneten Blogs WeLiveSecurity. Die exzellenten Forschungsergebnisse und Zusammenfassungen zu APT-Aktivitäten sowie viele weitere detaillierte Informationen werden regelmäßig veröffentlicht und stehen ESET Kunden exklusiv schon vorab bereit.

TREFFEN SIE PROAKTIVE VORKEHRUNGEN SCHNELLER

Die wertvollen Informationen aus dem Report verschaffen Ihnen einen strategischen Vorteil im Kampf gegen Cyberkriminelle. Sie erfahren zuerst, was auf der „dunklen Seite des Internets" vor sich geht und haben einen Einblick in den Kontext. Damit können Sie umgehend interne Vorkehrungen treffen, noch bevor die Bedrohungen Sie erreichen.

HOHE DATENQUALITÄT ALS HANDLUNGSBASIS

Die Berichte liefern umfangreiche Kontextinformationen darüber, was vor sich geht und warum. Dank dieser Informationen können sich Organisationen proaktiv auf potenzielle Gefahren vorbereiten. Dabei stellen unsere Experten sicher, dass die Inhalte leicht zu verstehen sind.

ZUGANG ZU ESET EXPERTEN

Alle Kunden der APT-Reports können sich bis zu 4 Stunden pro Monat mit einem ESET Analysten austauschen. Das bietet Ihnen die Möglichkeit, Themen im Detail zu besprechen und offene Fragen zu klären.

MIT DEN APT-REPORTS ERHALTEN SIE:

- ✓ Zugang zu exklusiven, detaillierten technischen Analysen
- ✓ APT Activity Summary Reports
- ✓ Monatliche Zusammenfassungen für Ihre Führungskräfte
- ✓ Direkter Zugang zu ESET Cybersicherheitsexperten
- ✓ Zugriff auf unseren MISP-Server

TIEFGEHENDE ANALYSE

Der Report beinhaltet monatliche ausführliche technische Analyseberichte zu aktuellen Angriffen, Toolsets und verwandten Themen. Außerdem erhalten Sie alle zwei Wochen eine Zusammenfassung über die aktuellen APT-Kampagnen verschiedener Akteure, die die ESET-Forscher verfolgt haben sowie deren Ziele und natürlich die dazugehörigen IoCs (Indicators of Compromise). Eine monatliche Übersicht stellt die Informationen aus den technischen Analysen und den Zusammenfassungen des Vormonat in einer kürzeren und leicht verständlichen Form bereit.

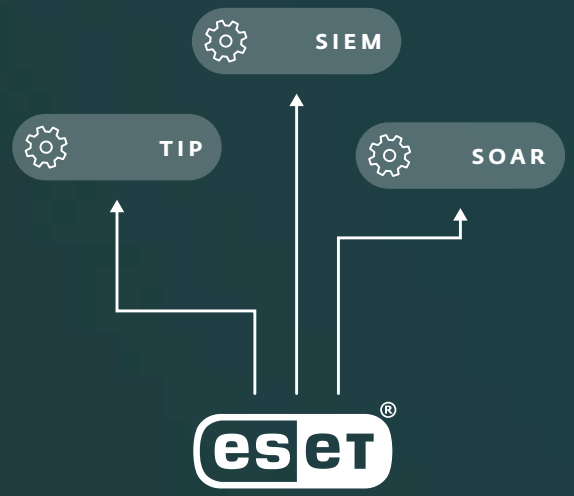
So funktioniert die Integration in Ihr System

Die Integration der ESET Telemetrie ist einfach und wird die Qualität Ihres **TIP, SIEM** oder **SOAR** bereichern.

Wir verfügen über eine **umfangreiche API mit ausführlicher Dokumentation**.

Wir liefern Daten in **standardisierten Formaten** wie JSON und STIX-Feeds via TAXII und ermöglichen so eine Integration in andere Tools.

Mithilfe von **Schritt-für-Schritt-Anleitungen** – u.a. für IBM QRadar, Anomali und Logpoint – gewährleisten wir eine reibungslose Implementierung.



Bereitgestellte Datafeeds von ESET

Verschaffen Sie sich einen Überblick über die weltweite Bedrohungslandschaft. Die ESET Datafeeds liefern ein ganzheitliches Lagebild und ermöglichen dadurch eine schnelle Blockierung von IoCs in Ihrer Umgebung. Die Feeds werden in den Formaten JSON und STIX 2.0 bereitgestellt.

Ideal geeignet für SOC, SIEM, MSSP und CERT.

MALICIOUS FILES FEED

Erfahren Sie, welche schädlichen Dateien aktuell in Umlauf sind. Der Feed enthält Domains, die als bösartig gelten, einschließlich Domainname, IP-Adresse, Erkennung der von einer URL heruntergeladenen Datei sowie der Datei, die versucht hat, auf die URL zuzugreifen. Zudem werden gemeinsame Hashes von schädlichen ausführbaren Dateien und den dazugehörigen Daten bereitgestellt.

DOMAIN FEED

Blockieren Sie dank diesem Feed als schädlich eingestufte Domains. Der Feed enthält Domainnamen, IP-Adressen und dazugehörige Datumsangaben/Zeitstempel. Die Domains werden nach ihrem Schweregrad eingestuft, sodass Sie Ihre Maßnahmen entsprechend anpassen und z.B. nur besonders gefährliche Domains blockieren können.

IP-FEED

Dieser Feed enthält als schädlich eingestufte IP-Adressen und die damit verbundenen Daten. Die Struktur der Informationen ist ähnlich wie bei den URL- und Domain Feeds. Der Hauptnutzen besteht darin, die jeweils aktuell verbreiteten schädlichen IP-Adressen zu kennen, die besonders gefährlichen zu blockieren und zu prüfen, ob sie bereits Schaden angerichtet haben.

URL-FEED

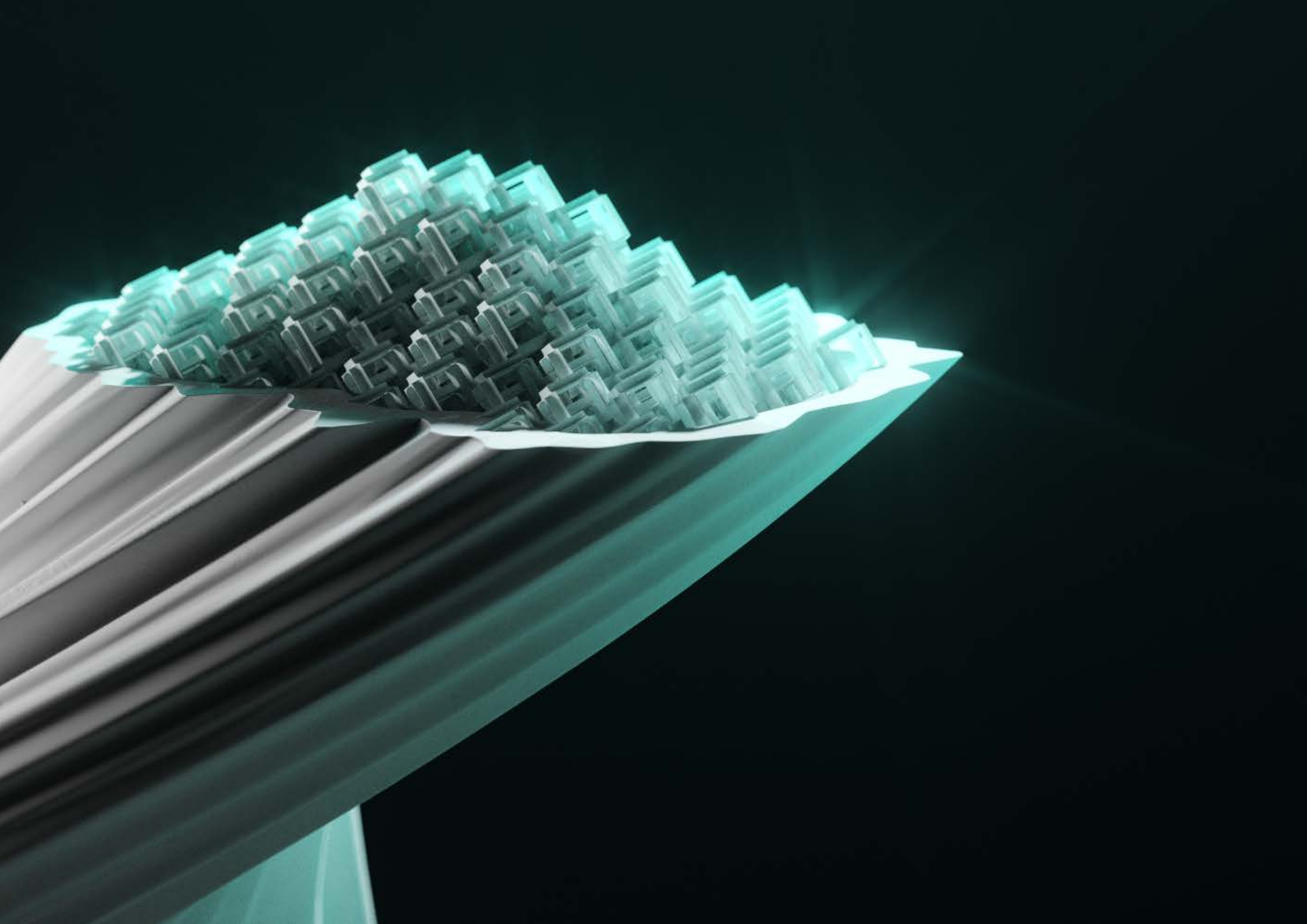
Ähnlich wie der Domain Feed stellt der URL-Feed Informationen über bestimmte Adressen bereit. Hierzu gehören Daten, die sich auf die URL beziehen, sowie Informationen über die Domains, die sie hosten. Alle Informationen werden gefiltert, sodass nur Ergebnisse mit hoher Zuverlässigkeit angezeigt werden. Zudem enthalten sie leicht verständliche Erklärungen, warum eine URL markiert wurde.

BOTNET FEED

Basierend auf dem ESET-eigenen Botnet-Tracker-Netzwerk bietet der Botnet Feed drei Arten von Unterkategorien – Botnet, Command & Control (C&C) und Ziele. Zu den bereitgestellten Daten gehören Erkennung (IoCs), Hash, letzte erkannte Aktivität, heruntergeladene Dateien, IP-Adressen, Protokolle, Ziele und andere Informationen.

APT-FEED

Dieser Feed besteht aus Informationen zu APTs. Grundlegend handelt es sich um einen Export aus dem internen ESET Malware Information Sharing Platform (MISP) Server. Alle geteilten Daten werden in den APT-Reports ausführlicher erläutert. Der APT-Feed ist Teil dieses Reports, kann aber auch separat erworben werden.



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 und halten Ihr Netzwerk mit Hilfe von Cloud-Sandboxing frei von Zero-Day-Bedrohungen. Mittels Multi-Faktor-Authentifizierung und zertifizierter Verschlüsselungsprodukte unterstützen wir Sie bei der Umsetzung von Datenschutzbestimmungen.

Unsere XDR-Basis mit Endpoint Detection and Response Lösung, Frühwarnsysteme (bspw. Threat Intelligence) und dedizierte Services ergänzen das Angebot im Hinblick auf Forensik sowie den gezielten Schutz vor Cyberkriminalität und APTs. Dabei setzt ESET nicht nur allein auf Next-Gen-Technologien, sondern kombiniert Erkenntnisse aus der cloudbasierten Reputationsdatenbank 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

ISP Security Partner seit 2008
2 Millionen Kunden

Allianz Suisse

Seit 2016 durch ESET geschützt
Mehr als 4.000 Postfächer

BEWÄHRT

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

Unsere Lösungen sind nach den Qualitäts- und Informationssicherheitsstandards ISO 9001:2015 und ISO/IEC 27001:2013 zertifiziert

ESET IN ZAHLEN

110+ Mio.
Geschützte Nutzer weltweit

400 k+
Geschützte Unternehmen

200+
Länder & Regionen

13
Forschungs- und Entwicklungs-zentren weltweit

BEWERTUNGEN VON ANALYSTEN

ESET wurde zum dritten Mal in Folge als ‚Top-Player' in Radicati's APT Protection Marktquadranten-Report ausgezeichnet.

ESET wurde im LEADERSHIP COMPASS 2022 Report als „Overall Leader" ausgezeichnet.

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

ESET.DE | ESET.AT | ESET.CH

ESET.DE | ESET.AT | ESET.CH

Stand: 02/2023