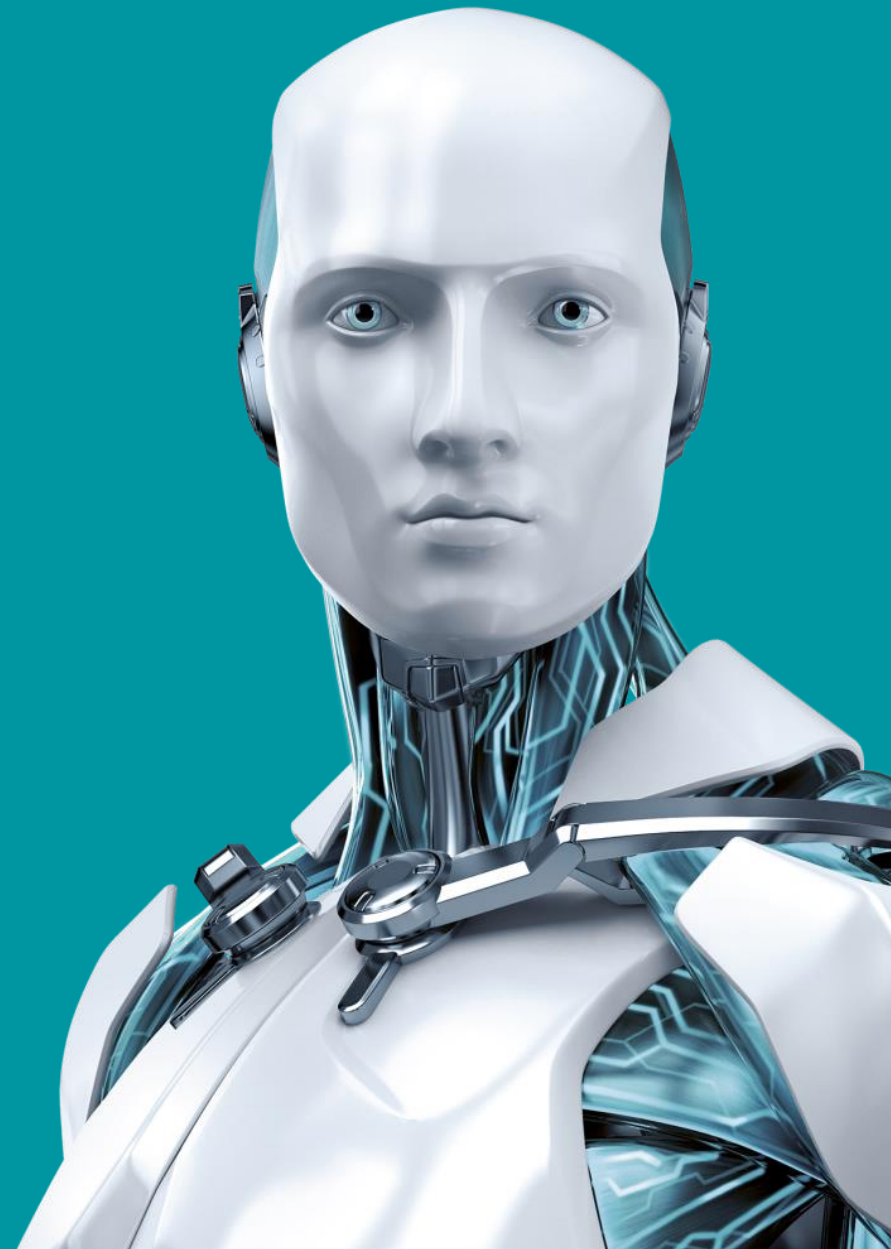
ESET Produkt Portfolio

Patrik Werren
Presales Engineer

30 YEARS OF CONTINUOUS IT SECURITY INNOVATION

ENJOY SAFER TECHNOLOGY™



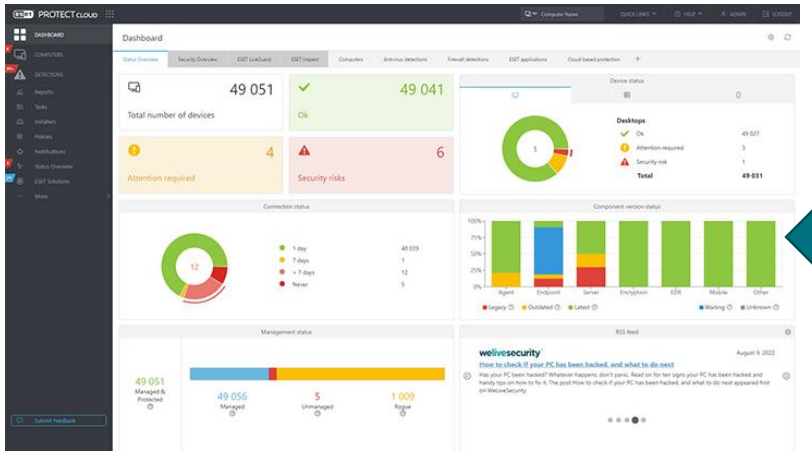
ESET-Schutztechnologien
ESET PROTECT Management

ESET PROTECT

Die ESET-Schutztechnologien

ESET PROTECT

Zentrales Management
für Malwareschutz



Endpoint
Detection & Response

ESET INSPECT

ESET Threat Intelligence
Globales Frühwarnsystem

ESET Management Systeme

ESET PROTECT

On Premise

Windows Server Installation - **PROTECT & INSPECT**

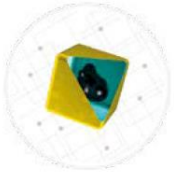
Rocky Linux Appliance - **PROTECT**

Cloud

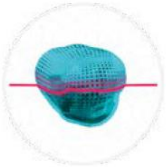
ESET - Rechenzentrum

EU / USA / Kanada

UNSERE EINGESETZTEN **SCHUTZMODULE**



INTEGRIERTE SANDBOX

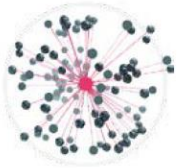


ERWEITERTE SPEICHERPRÜFUNG

SCHUTZ VOR BRUTE-FORCE-ANGRIFFEN

RANSOMWARE SHIELD

Neu: Ransomware Remediation



BOTNET-ERKENNUNG

VERHALTENSBASIERTE ERKENNUNG – HIPS

EXPLOIT-BLOCKER

SCHUTZ VOR NETZ-WERKANGRIFFEN

UEFI-SCANNER

ESET PROTECT Management onPrem / Cloud

Nur Cloud

Windows

Endpoint

- Endpoint Antivirus
- Endpoint Security
- Server Security
- SharePoint Security
- Exchange Security

Patch- & Schwachstellen Management

Nur Cloud

Personal Firewall

Web Kontrolle

Device Kontrolle

Server

macOS

- Endpoint Antivirus
- Endpoint Security

Linux

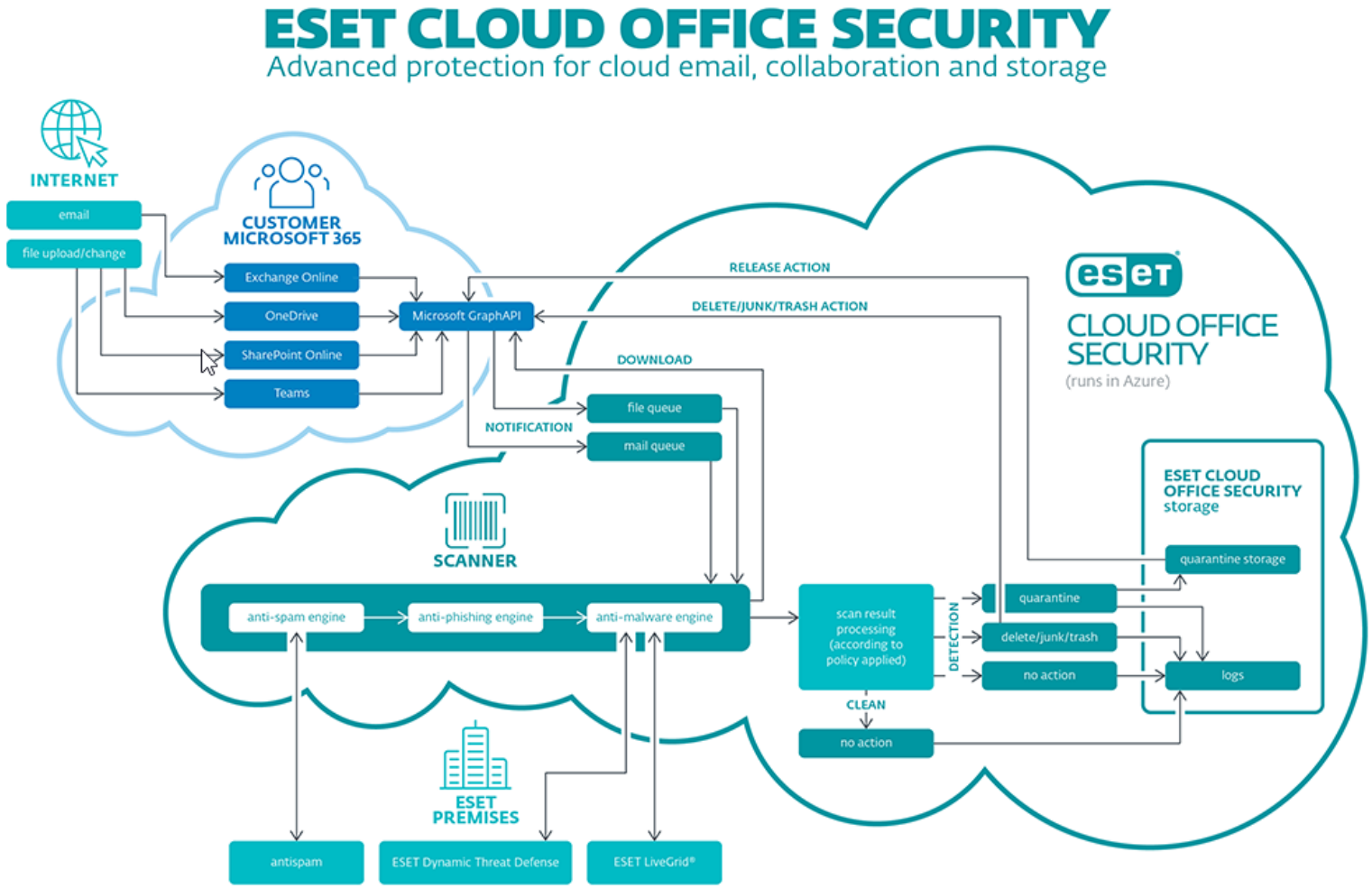
- Endpoint
- Server

CentOS
Red Hat
SUSE
Ubuntu
Debian
Mandriva
Fedora

Mobil

- Android
- iOS

ECOS-Integration in Microsoft 365



ESET PROTECT Bundles

Modul	MDR Ultimate	MDR	Elite	Enterprise	Complete	Advanced	Lösung	Kompatibilität
Zentrale Management-Konsole	●	●	●	●	●	●	ESET PROTECT	Konsole:
	●	●	●	●	●	●	ESET PROTECT On-Prem	Server:
Schutz von Clients, Mobilgeräten und Fileservern	●	●	●	●	●	●	ESET Endpoint Security* | Antivirus	
	●	●	●	●	●	●	Feature: Ransomware Remediation	
	●	●	●	●	●	●	ESET Server Security	
	●	●	●	●	●	●	Mobile Device Management* (nur mit Cloud-Version von ESET PROTECT verfügbar)	iOS
Cloud Sandboxing	●	●	●	●	●	●	ESET LiveGuard® Advanced	
Verschlüsselung	●	●	●	●	●	●	ESET Full Disk Encryption	
Schutz von Mailservern	●	●	●		●		ESET Mail Security (inkl. ESET LiveGuard® Advanced für Exchange)	Exchange
Schutz von Cloud-Anwendungen	●	●	●		●		ESET Cloud Office Security (inkl. ESET LiveGuard® Advanced)	
Schwachstellen- & Patch-Management	●	●	●		●		ESET Vulnerability & Patch Management (nur mit Cloud-Version von ESET PROTECT verfügbar)	
Multi-Faktor-Authentifizierung	●	●	●				ESET Secure Authentication	Konsole: Server: Apps: iOS
Endpoint Detection and Response	●	●	●	●			ESET Inspect**	Konsole:
	●						Feature: ESET AI Advisor	Server:
	●	●	●	●			ESET Inspect On-Prem**	Clients:
Premium Support Service	● Ultimate	●					ESET Premium Support	
MDR-Service	● Ultimate	●					ESET MDR	

* ab ESET PROTECT Advanced kann pro Seat ein weiteres Mobilgerät (Mobile Threat Defense) geschützt werden

** ESET Inspect nur mit ESET PROTECT, ESET Inspect On-Prem nur mit ESET PROTECT On-Prem

Weitere ESET PROTECT Bundles

ESET PROTECT Entry
- Zentrale Management Konsole (ESET PROTECT | ESET PROTECT On-Prem)
- Schutz von Endpoints (ESET Endpoint Security | ESET Endpoint Antivirus | ESET Server Security | Mobile Device Management)

ESET PROTECT Mail Plus
- Zentrale Management Konsole (ESET PROTECT | ESET PROTECT On-Prem)
- Schutz von Mailservern (ESET Mail Security inkl. ESET LiveGuard® Advanced für Exchange)

Weitere ESET Lösungen

ESET Threat Intelligence

ESET Endpoint Encryption
- Verschlüsselung für Windows- und macOS-Clients

ESET Security for Microsoft SharePoint Server

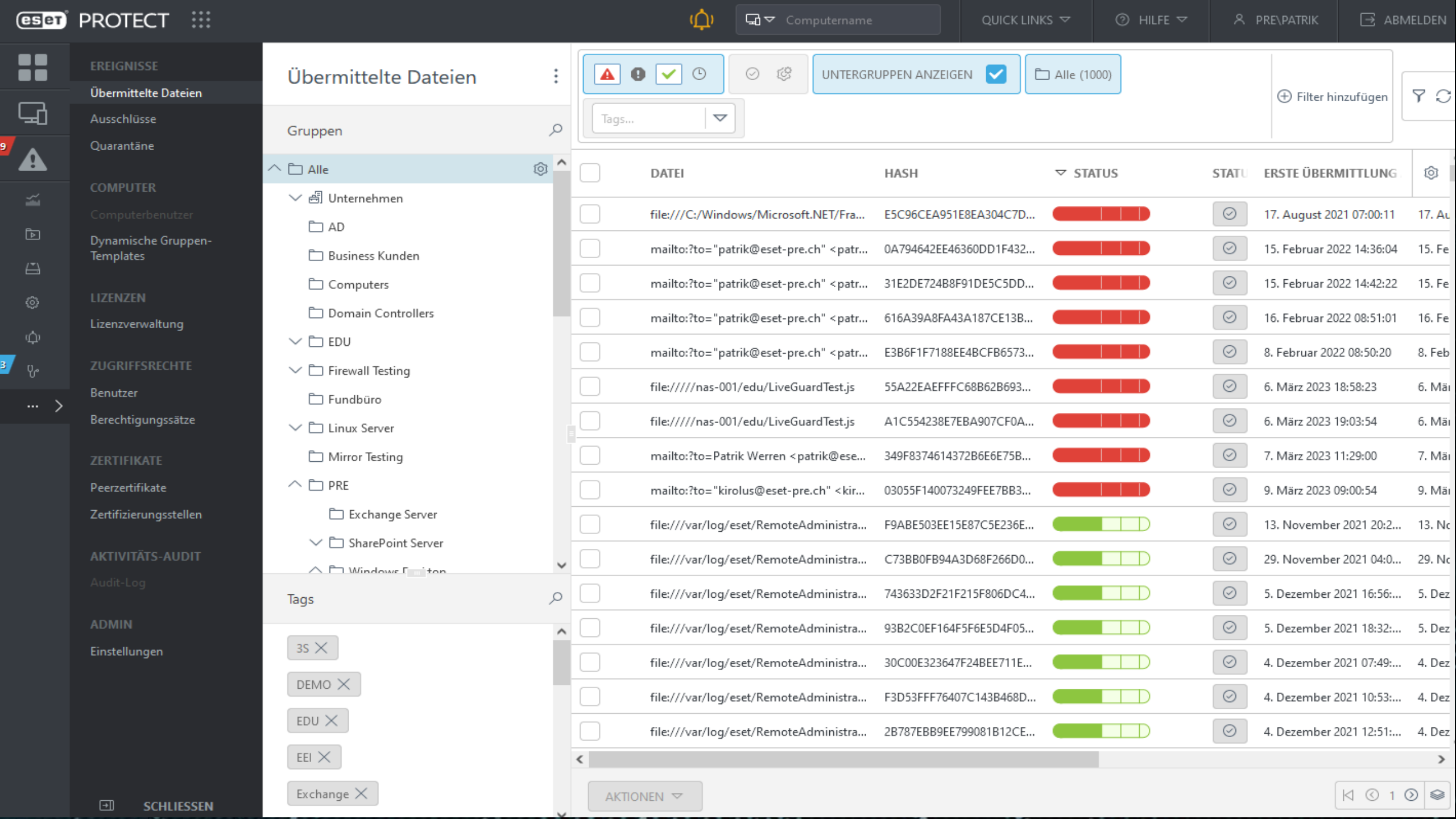
ESET AntiVirus Lösungen
ESET Cloud Sandboxing

ESET LiveGuard – Cloud Sandboxing

EDTD – Datei Analyse in der Sandbox

Der Benutzer erhält folgende Nachrichten auf dem Desktop

Die Analyse in der LIVEGUARD Sandbox dauert ca. 1-2 Minuten


PROTECT
Computername
QUICK LINKS
HILFE
PRE\PATRIK
ABMELDEN
EREIGNISSE
Übermittelte Dateien
Ausschlüsse
Quarantäne
COMPUTER
Computerbenutzer
Dynamische Gruppen-Templates
LIZENZEN
Lizenzverwaltung
ZUGRIFFSRECHTE
Benutzer
Berechtigungssätze
ZERTIFIKATE
Peerzertifikate
Zertifizierungsstellen
AKTIVITÄTS-AUDIT
Audit-Log
ADMIN
Einstellungen
SCHLIESSEN
Übermittelte Dateien
Gruppen
Alle
Unternehmen
AD
Business Kunden
Computers
Domain Controllers
EDU
Firewall Testing
Fundbüro
Linux Server
Mirror Testing
PRE
Exchange Server
SharePoint Server
Tags
3S
DEMO
EDU
EEI
Exchange
UNTERGRUPPEN ANZEIGEN
Alle (1000)
Tags...
Filter hinzufügen
DATEI
HASH
STATUS
ERSTE ÜBERMITTLUNG
file:///C:/Windows/Microsoft.NET/Fra...
E5C96CEA951E8EA304C7D...
17. August 2021 07:00:11
mailto:?to="patrik@eset-pre.ch" <patr...
0A794642EE46360DD1F432...
15. Februar 2022 14:36:04
mailto:?to="patrik@eset-pre.ch" <patr...
31E2DE724B8F91DE5C5DD...
15. Februar 2022 14:42:22
mailto:?to="patrik@eset-pre.ch" <patr...
616A39A8FA43A187CE13B...
16. Februar 2022 08:51:01
mailto:?to="patrik@eset-pre.ch" <patr...
E3B6F1F7188EE4BCFB6573...
8. Februar 2022 08:50:20
file://///nas-001/edu/LiveGuardTest.js
55A22EAEFFFC68B62B693...
6. März 2023 18:58:23
file://///nas-001/edu/LiveGuardTest.js
A1C554238E7EBA907CF0A...
6. März 2023 19:03:54
mailto:?to=Patrik Werren <patrik@ese...
349F8374614372B6E6E75B...
7. März 2023 11:29:00
mailto:?to="kirolus@eset-pre.ch" <kir...
03055F140073249FEE7BB3...
9. März 2023 09:00:54
file:///var/log/eset/RemoteAdministra...
F9ABE503EE15E87C5E236E...
13. November 2021 20:2...
file:///var/log/eset/RemoteAdministra...
C73BB0FB94A3D68F266D0...
29. November 2021 04:0...
file:///var/log/eset/RemoteAdministra...
743633D2F21F215F806DC4...
5. Dezember 2021 16:56:...
file:///var/log/eset/RemoteAdministra...
93B2C0EF164F5F6E5D4F05...
5. Dezember 2021 18:32:...
file:///var/log/eset/RemoteAdministra...
30C00E323647F24BEE711E...
4. Dezember 2021 07:49:...
file:///var/log/eset/RemoteAdministra...
F3D53FFF76407C143B468D...
4. Dezember 2021 10:53:...
file:///var/log/eset/RemoteAdministra...
2B787EBB9EE799081B12CE...
4. Dezember 2021 12:51:...
AKTIONEN
1

ESET LIVEGUARD

BÖSARTIG

SHA-1 A1C554238E7EBA907CF0A09B6D2105EC46F3E8B7

Kategorie Skript

ERWEITERTE SCAN-MODULE

Erweitertes Entpacken Und Scannen

Das Sample wird statisch analysiert, mit modernsten Methoden entpackt und anschließend mit einer umfassenden Bedrohungsdatenbank abgeglichen.

Sample ist sauber

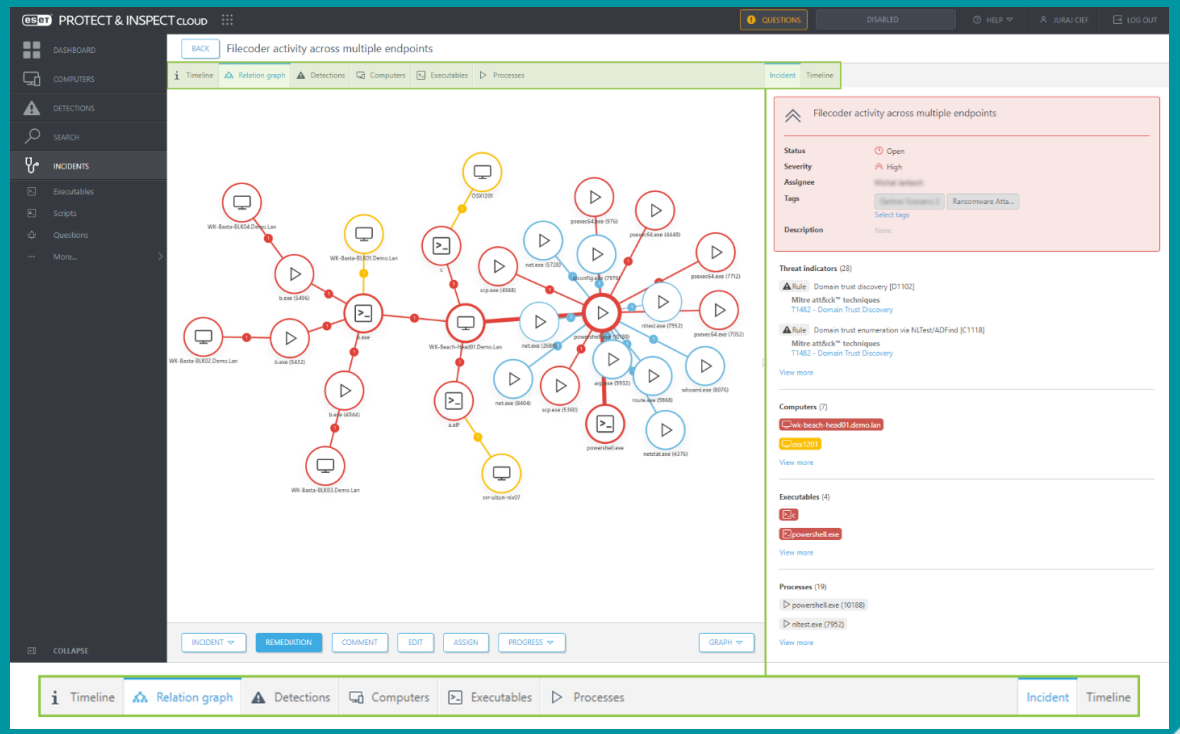
Erkennung Durch Erweitertes Machine Learning

Für die statische und dynamische Analyse wird eine Vielzahl von Machine-Learning-Algorithmen verwendet, inklusive Deep Learning.

Nicht erforderlich für dieses Sample

Ausführbarer Stack Erstellt	Verhalten nicht erkannt
Erkennung Durch Machine Learning	Verhalten nicht erkannt
Verzögerte Ausführung.	Verhalten nicht erkannt
Virenschutzinteraktion	Verhalten nicht erkannt
Verdächtige Namensänderung.	Verhalten nicht erkannt
Ausgeführte Datei Von Sample Gelöscht	Verhalten nicht erkannt
Eingabegeräte Abgefangen	Verhalten nicht erkannt
Link In Verknüpfung Geändert	Verhalten nicht erkannt
Browser Gestartet	Verhalten nicht erkannt
Sample Hat Laufenden Prozess Modifiziert	Verhalten nicht erkannt
Unerwünschtes Objekt Gefunden	Verhalten nicht erkannt
Injektion In Ausgeführte Prozesse	Verhalten nicht erkannt
Ausgeführte Datei Von Sample Verschoben	Verhalten nicht erkannt
Dienstzugriff	Verhalten nicht erkannt
Umgebungserkennung	Verhalten nicht erkannt
Netzwerkkommunikation Erkannt	Verhalten nicht erkannt
Autorun Erstellt	Verhalten nicht erkannt
Erkennung Durch Machine Learning	Verhalten nicht erkannt
Zugriff Auf Private Daten	Verhalten nicht erkannt
Skriptausführung	Verhalten nicht erkannt
Verdächtige DLL Geladen	Verhalten nicht erkannt
Botnet-Datenverkehr Erkannt	Verhalten nicht erkannt
Dateien Im Windows-Ordner Erstellt	Verhalten nicht erkannt
Neuer Desktop Erstellt	Verhalten nicht erkannt
Kritischer Prozess Erstellt	Verhalten nicht erkannt
Dateilose Bedrohung	Verhalten nicht erkannt

ESET INSPECT



30 YEARS OF CONTINUOUS IT SECURITY INNOVATION

ENJOY SAFER TECHNOLOGY™

ESET Inspect

- Ein umfassendes Erkennungs- und Reaktionssystem für Endpoints mit den folgenden Funktionen:

- Erkennung von Vorfällen, gezielten Angriffen APT

- Verwaltung und Auflösung von Vorfällen

- Datensammlung und Indikatoren für die Erkennung von Angriffen, Anomalien, Verhaltensweisen und Policy Verletzungen

Gezielte Angriffe auf Unternehmen

Der Unterschied zu einem herkömmlichen Hackerangriff

Ein Angreifer unternimmt einen grossen Aufwand in Kauf und sucht sich einen oder mehrere Nutzer eines Unternehmens aus

Das Ziel ist es, nach dem Eindringen, in kleinen und unauffälligen Schritten weiter in das lokale Netzwerk vorzustossen

Der Angreifer will so lange wie möglich unentdeckt bleiben, um grosse Menge an Daten auszuspähen, zu kopieren und danach einen grösstmöglichen Schaden anzurichten

Wie geht ein Angreifer typischerweise vor?

Der Angreifer sammelt schon im Vorfeld gezielt Informationen über seine Opfer, meistens Unternehmen

Dabei werden über soziale Medien Information über einen kleinen Personenkreis gesammelt, Mitarbeiter und deren Aufgabengebiete bzw. Funktionen

Der Schadcode wird typischerweise über „Spear Phishing-E-Mail“ verbreitet, oder über einen Internetlink zu einer präparierten Webseite, auf welcher der Schadcode automatisiert, installiert wird

Ist der Schritt erfolgreich, versucht der Angreifer weiter in das Netzwerk vorzudringen, bemächtigt sich an Benutzeraccounts mit hoher Berechtigung

Wie geht ein Angreifer typischerweise vor?

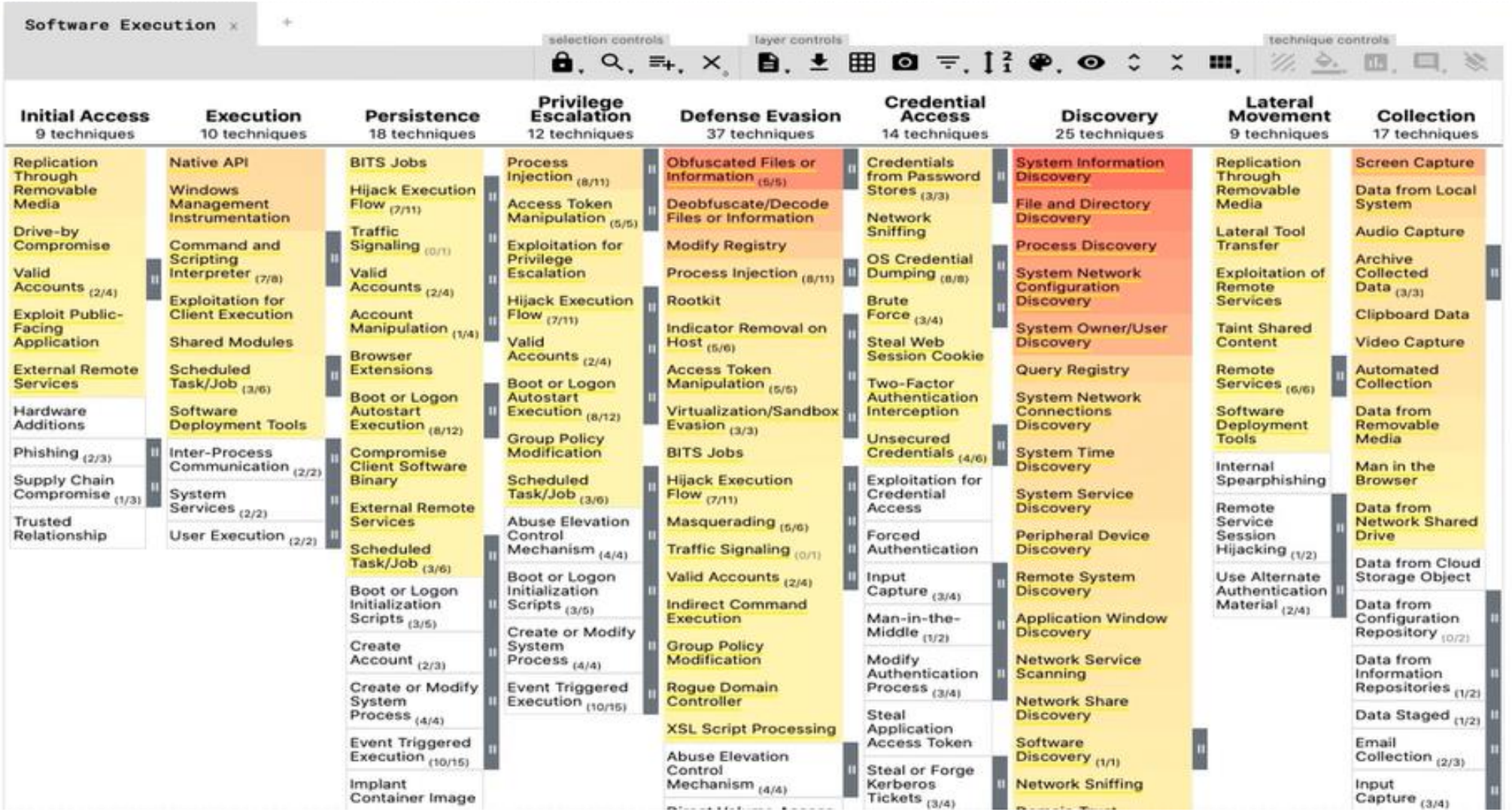
Durch die erlangten Admin Berechtigungen werden nun Daten abgegriffen und nach extern übertragen

Der Angreifer transferiert dabei immer kleinere Datenmengen, um nicht durch untypische erhöhte Datenübertragungen aufzufallen

Ist der Angreifer im Besitz der gewünschten Daten, wird er über dem bestehenden Backdoor nun die massgeschneiderte Schadsoftware übertragen und gezielt die firmenrelevanten Systeme verschlüsseln

Nun wird das Unternehmen mit einer horrenden Lösegeldforderung konfrontiert

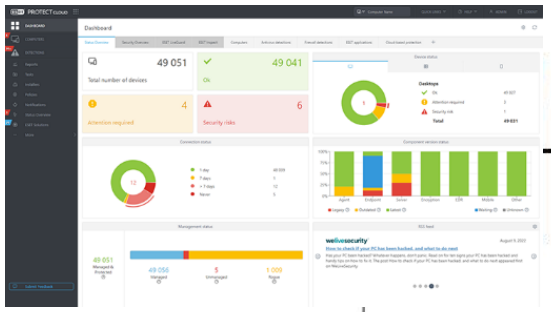
Wie geht ein Angreifer typischerweise vor?

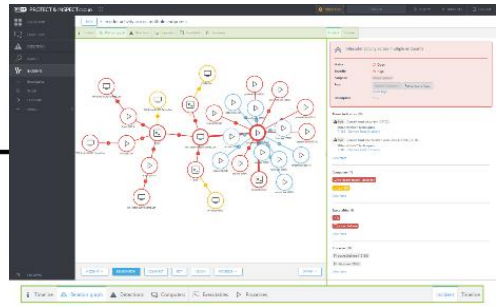


ESET-Integration in ein Security Operation Center

30 YEARS OF CONTINUOUS IT SECURITY INNOVATION

ENJOY SAFER TECHNOLOGY™





ESET Threat Intelligence

TAXII Feeds

ESET PROTECT

ESET INSPECT

Syslog / API

API

SIEM

SOC - Security Operation Center

PROTECT & INSPECT Agent

PROTECT & INSPECT Agent

PROTECT & INSPECT Agent

Digital Security
Progress. Protected.

ESET MANAGED DETECTION AND RESPONSE SERVICE

ESET - MDR Services

Service-Übersicht für die Verwaltung von ESET Inspect je nach erworbenem ESET PROTECT BUNDLE

	PROTECT MDR ULTIMATE	PROTECT MDR	PROTECT ELITE
Konfiguration	●	◐	○
Threat Hunting 24/7	●	●	○
Optimierung & Automatisierung	●	◐	○
Reaktion auf Sicherheitsereignisse	●	●	○
Angriffsanalyse	●	○	○
Präventive Maßnahmen	●	◐	○
Kundenkommunikation	●	◐	○
Meetings	●	○	○
Reports	●	●	○

Legende:
Service Leistung durch ESET:

- ● inbegriffen
- ◐ teilweise inbegriffen
- ○ nicht inbegriffen

SLAs für ESET Security Services: https://help.eset.com/enterprise_services/de-DE/spec_ess.html
SLAs für ESET Professional Services: https://help.eset.com/enterprise_services/de-DE/spec_eps.html

ESET - MDR Ultimate Service

Konfiguration

- ESET (SOC-Team in Jena) übernimmt das Roll-out von ESET Inspect auf bis zu 100 Geräten und nimmt initiale Einstellungen und Optimierungen vor (ESET Deployment & Upgrade Service).
- Kunden übernehmen eigenständig das Rollout von ESET Inspect, die MDR-Umgebung wird automatisch nach Freischaltung aktiviert.

Reaktion auf Sicherheitsereignisse

- Aufkommende Gefahren werden umgehend beseitigt (entweder mit proaktiver Unterstützung in Abstimmung durch den Kunden bzw. das SOC-Team in Jena inkl. Threat Hunting Reports bei ESET PROTECT MDR Ultimate oder automatisiert innerhalb von 6 Minuten mit Dokumentation der eingeleiteten Schritte bei ESET PROTECT MDR).

Kundenkommunikation

- Proaktive Kommunikation mit direktem Kontakt zum SOC-Team in Jena, inklusive Hinterlegung von Notfallkontakten aufseiten des Kunden.
- Reaktive Kommunikation über Ticketsystem im ESET Service Hub.

Threat Hunting 24/7

- Proaktives Monitoring und Threat Hunting rund um die Uhr inklusive Reaktionen auf Sicherheitsvorfälle (entweder kundespezifisch durch das SOC-Team in Jena bei ESET PROTECT MDR Ultimate oder automatisiert mithilfe von KI und HQ-Experten bei ESET PROTECT MDR).

Angriffsanalyse

- Bereitstellung umfassender Analysen von Angriffsvektoren, inklusive Beratung sowie detaillierte forensische Einblicke (nur ESET PROTECT MDR Ultimate).

Meetings

- Regelmäßige Meetings mit dem SOC-Team in Jena zur Besprechung von Sicherheitslücken oder Security-Aktivitäten (nur ESET PROTECT MDR Ultimate).

Optimierung & Automatisierung

- Kunden erhalten auf ihre Umgebung zugeschnittene Empfehlungen zur Optimierung von Regeln und Ausschlüssen durch das SOC-Team in Jena und profitieren von einer kontinuierlichen Stärkung ihrer Sicherheitsmaßnahmen.
- Kunden erhalten allgemeine Empfehlungen und Vorschläge zur Optimierung von Regeln und Ausschlüssen für eine eigenständige Umsetzung.

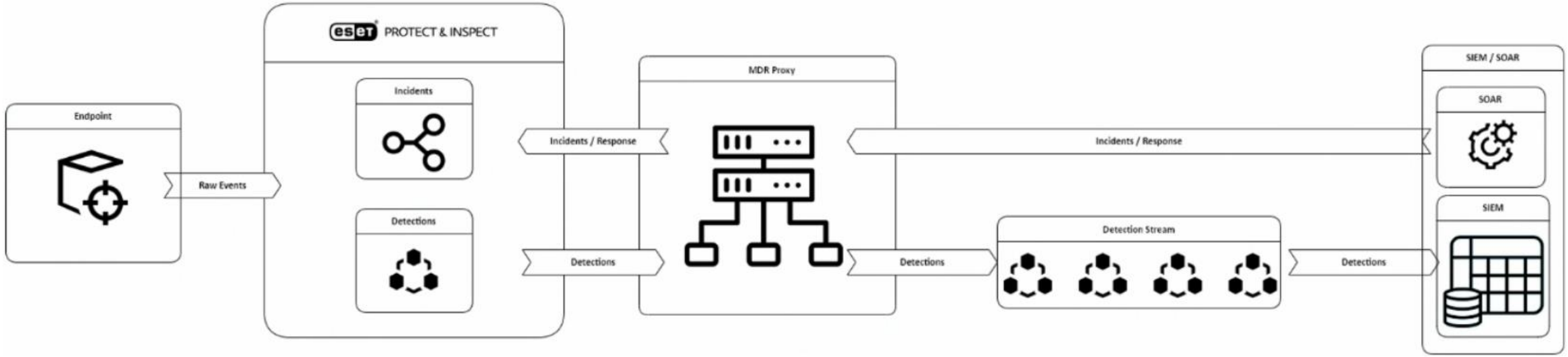
Präventive Maßnahmen

- Sofern möglich, erhalten Kunden auf ihre Umgebung zugeschnittene Handlungsempfehlungen zur Verbesserung der grundlegenden Sicherheit.
- Kunden erhalten allgemeine Handlungsempfehlun-gen, die eigenständig umgesetzt werden können, um die grundlegende Sicherheit zu verbessern.

Reports

- Bereitstellung von automatisch erstellten Reports (entweder monatlich bei ESET PROTECT MDR Ultimate oder wöchentlich und/oder monatlich bei ESET PROTECT MDR).

ESET - MDR KI Service – Workflow



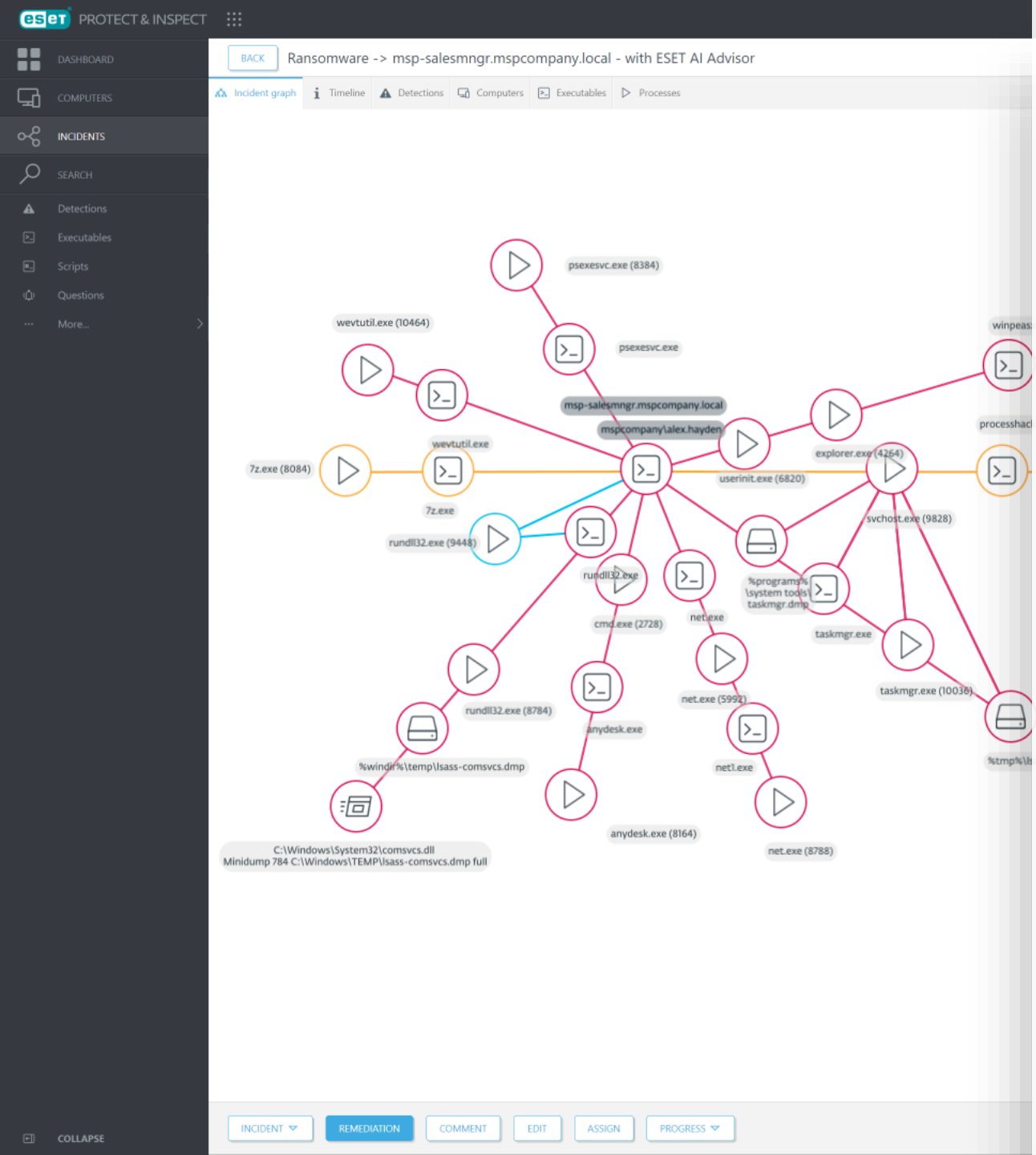

eset
AI ADVISOR

Wobei unterstützt mich der AI Advisor

- **Detaillierte IT-Forensik**
- **Untersuchung eines Incidents / Threat Hunting**
- **Handlungsempfehlungen mit schnellen Eingriffen**
- **Erhältlich als Add-On für folgende Bundes:**

  ESET PROTECT Enterprise
  ESET PROTECT Elite
  ESET PROTECT MDR

- **AI Advisor ist im Ultimate MDR Service inbegriffen**



Hello! How can I help you with this incident?

Provide summary of incident, focus on attack chain steps and provide result in bullet points.

The incident involves the execution of trusted utilities and access of malicious files by user **alex.hayden** on the computer **msp-salesmngr.mspcompany.local**. The attack chain steps are as follows:

- Execution of trusted utilities (**whoami.exe, net.exe, net1.exe**) from PowerShell to gather information about system users and domain-level groups.
- Access of multiple malicious files (**winpeasx64.exe, winpeasany.exe, winpeasany_ofs.exe, gmer.exe, winpeasx86_ofs.exe, winpeasx64_ofs.exe**) by Windows File Explorer, leading to detection of **MSIL/HackTool.Agent.OS** threat.
- Execution of processhacker.exe, loading of **kprocesshacker.sys** and access of LSASS process, indicating potential credential dumping.
- Use of PsExec tool and PowerShell for remote program execution.
- Creation of a minidump of LSASS process memory and attempts to add and hide user accounts.
- Installation of **AnyDesk** with settings associated with **Conti ransomware gang**.
- Use of 7zip utility to create a password-protected archive file and clearing of the Application event log.

The result of the incident includes the detection of **MSIL/HackTool.Agent.OS** threat and potential post-compromise communication using **AnyDesk ID.**

ESET Threat Intelligence
Globales Frühwarnsystem

ESET Threat Intelligence – Globales Frühwarnsystem

ESET Threat Intelligence – 10 Data Feeds

Feed-Name	Beschreibung	Anwendungsfall / Zweck
Botnet Feed	Enthält IPs und Domains, die mit bekannten Botnet Command-and-Control (C&C) Servern in Verbindung stehen.	Erkennung kompromittierter Systeme, Netzwerkanalyse, Blockierung bösartiger Kommunikation.
Malicious URL Feed	Liste verdächtiger oder bestätigter bösartiger URLs (Phishing, Malware, Exploits).	Webfilterung, URL-Blocking, Schutz vor Phishing/Malvertising.
APT Feed	Indikatoren (IPs, Domains, Hashes) über Aktivitäten fortgeschrittener, zielgerichteter Angreifergruppen (z. B. Sednit, Lazarus).	Threat Hunting, Frühwarnung bei staatlich motivierten Angriffen.
Malware Hash Feed	Hash-Werte (z. B. SHA-1/SHA-256) bekannter Schadsoftware-Dateien.	Datei-basierte Erkennung in SIEMs, Endpunktschutz, forensische Analyse.
Spam Domain/IP Feed	Domains und IP-Adressen, die beim Versenden von Spam, Phishing oder schadhaften Inhalten verwendet wurden.	E-Mail-Filterung, Anti-Spam-Massnahmen, Netzwerküberwachung.
DDoS Indicator Feed	Frühindikatoren für DDoS-Angriffe wie erkannte Botnet-Aktivitäten oder Angriffsmuster.	Präventiver Schutz gegen volumetrische und anwendungsbezogene Angriffe.
Mobile Threat Feed	Bedrohungen und schadhafte Apps im mobilen Bereich, insbesondere Android.	Schutz von MDM-/Mobile-Lösungen, App-Whitelisting.
Tor Exit Node Feed	Liste aktueller Tor-Exit-Knoten – kann genutzt werden, um potenziell anonymisierten Traffic zu erkennen oder zu blockieren.	Kontrolle über Anonymität im Netzwerk, forensische Netzwerk-Analysen.
Brute Force IP Feed	IP-Adressen, die bei Brute-Force-Angriffen auf E-Mail-, Web- oder SSH-Dienste aufgefallen sind.	Schutz durch Firewall-Blocking, Login-Monitoring, Rate Limiting.
Fresh Registered Domains Feed	Domains, die kürzlich registriert wurden – oft verwendet für Phishing oder Betrugsversuche kurz nach Erstellung.	Früherkennung von Fraud-Domains, Web-Traffic-Analyse.

ETI – Data Feeds (TAXII)

- ETI Data Feeds erfolgen in Echtzeit

- IoCs enthalten Hashes, Signaturen, IP-Adressen, Domänen Namen (z.B. von CnC - Command-and-Control Servern), sowie URLs

- Die Feeds werden über **TAXII Server** bereit gestellt
- Die Feeds erfolgen in den Formaten: **JSON** ans **STIX v2.0**
- Feeds sind gefiltert, nach neusten und weit verbreiteten Daten

- Out-of-the-box Integration in Threat Intelligence Plattformen:

  ThreatQuotien, Anomali für Feeds …


```
"cncs": [
    {
        "last_alive": "2016-10-12 12:06:09 UTC",
        "url": "http://api.ipify.org/"
    },
    {
        "last_alive": "2019-08-26 09:03:51 UTC",
        "url": "http://wysq6o3r64d46bnn.onion/"
    }
],
"file": {
    "count": 1,
    "file_name": "file",
    "file_type": "text/x-Algol68",
    "first_seen": "2019-08-26 10:07:34 UTC",
    "md5": "bcce66e4bdab44418b6ce54b2637e1a1",
    "sha1": "d433942895aec4e4f51c89430a5eb643225a25c5",
    "sha256": "f6d2a1ea50cd2f744af08b7754014acf342cced5ee82b193b227143e52e87649",
    "size": 92877,
    "ssdeep": "1536:Rb8rg8jqc3g2ETqyTP6VO3MCf13O4hjhKOePeJSXed714:WATBTCVUhpLCISI4"
},
"files": [],
"targets": [],
"threat": "JS/Retefe.I trojan",
"valid_to": "2020-05-29 10:21:04 UTC"
```


CnC server URL and last communication heartbeat timestamp

Information related to file which was able to communicate with CnC server (filename, mime categorization, main IoCs hashes, fuzzy hash)

Simple deduplication – findings are shared immediately, but sharing will be repeated after 24 hours


```
"files": [
    {
        "count": 1,
        "file_name": "11aee18d1f525f3f04d2a4fb8bf50fb6b3187903",
        "file_type": "application/x-dosexec",
        "first_seen": "2020-05-22 07:07:03 UTC",
        "md5": "de9fccaadd67587ad131278aa1d6739b",
        "origin": "downloaded",
        "sha1": "11aee18d1f525f3f04d2a4fb8bf50fb6b3187903",
        "sha256": "964dfce1006bd7c3239a37d92c88e73469546b59c1f6d992655fabea2a8849db
        "size": 643072,
        "ssdeep": "12288:75a9486snGXQkED80kqVMDgQX9SwAZcaNntriOw+VJ:1M3Qt0CDgK9EpRn
```


Information related to files that were either dropped, downloaded or unpacket (filename, mime categorization, main IoCs hashes, fuzzy hash)


```
"targets": [
    "*[redacted].*/webscr?cmd=_login-submit*",
    "*[redacted].*/*ServiceLoginAuth*",
    "*[redacted].*/*login.psp*",
    "*[redacted].*/login.psp*",
    "*[redacted].*/*index.php*",
    "*[redacted].*/mail/*",
    "*[redacted].*/*FormLogin*",
    "*[redacted]*/*post.srf*",
```

```
"targets": [
    "Banco [redacted]",
    "Banco [redacted]",
    "Banco [redacted]",
    "Banco [redacted]",
    "Banco [redacted]",
[redacted],
```


Targets of the malware obtained from CnC configuration

ESET Threat Intelligence – Globales Frühwarnsystem

Report zu zielgerichteten Angriffen

Informiert Nutzer über mögliche aufkommende oder gezielte andauernde Angriffe gegen das Unternehmen. Der Bericht enthält YARA Regelsätze, Informationen zur Reputation, ähnliche Binärprogramme, Details über die Datei, Sandbox-Output und mehr.

Report zu Botnet-Aktivitäten

Liefert quantitative Daten über bekannte Malware-Familien und Botnet-Varianten. Zudem erhalten Sie Informationen über bekannte, in Botnet-Kampagnen eingesetzte Command and Control (C&C) Server, Samples von Botnets, wöchentliche globale Statistiken und eine Liste an Zielen der Malware.

Report zur automatischen Sample-Analyse

Erstellt einen individuellen Bericht anhand der eingereichten Dateien oder Hashes und liefert so wertvolle Informationen für Entscheidungsfindungen und Vorfallsanalysen.

Report zu gefälschten SSL-Zertifikaten

Wird generiert, wenn ESET ein neues SSL-Zertifikat erkennt, das Ähnlichkeiten zu einem Zertifikat aufweist, das der Kunde beim ursprünglichen Setup bereitgestellt hat. Zu den enthaltenen Informationen gehören gegebenenfalls auch Details über aufkommende Phishing-Kampagnen, die das Zertifikat einsetzen, YARA Übereinstimmungen und Zertifikatsdaten.

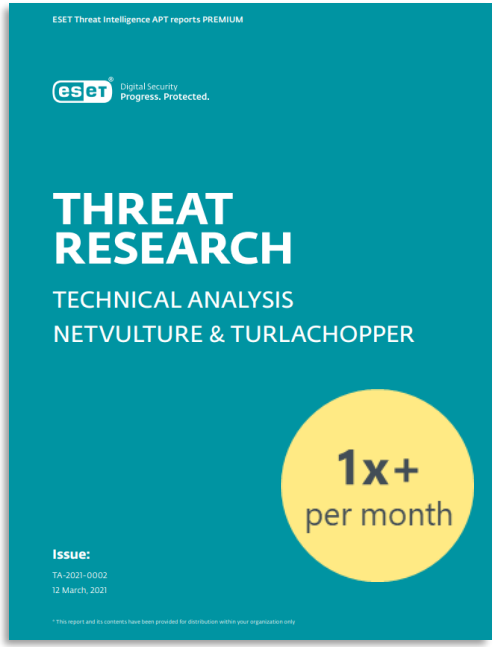
Report zu zielgerichteten Phishing-Angriffen

Stellt Daten über Phishing-Aktivitäten gegen das jeweils ausgewählte Unternehmen an. Der Bericht umfasst Informationen über Phishing-Attacken, einschließlich Ausmaß, Anzahl an betroffenen Clients, URL Screenshots, Vorschau der Phishing-Mail, Standort des Servers und vieles mehr.

APT Premium Reports

Activity Summary reports

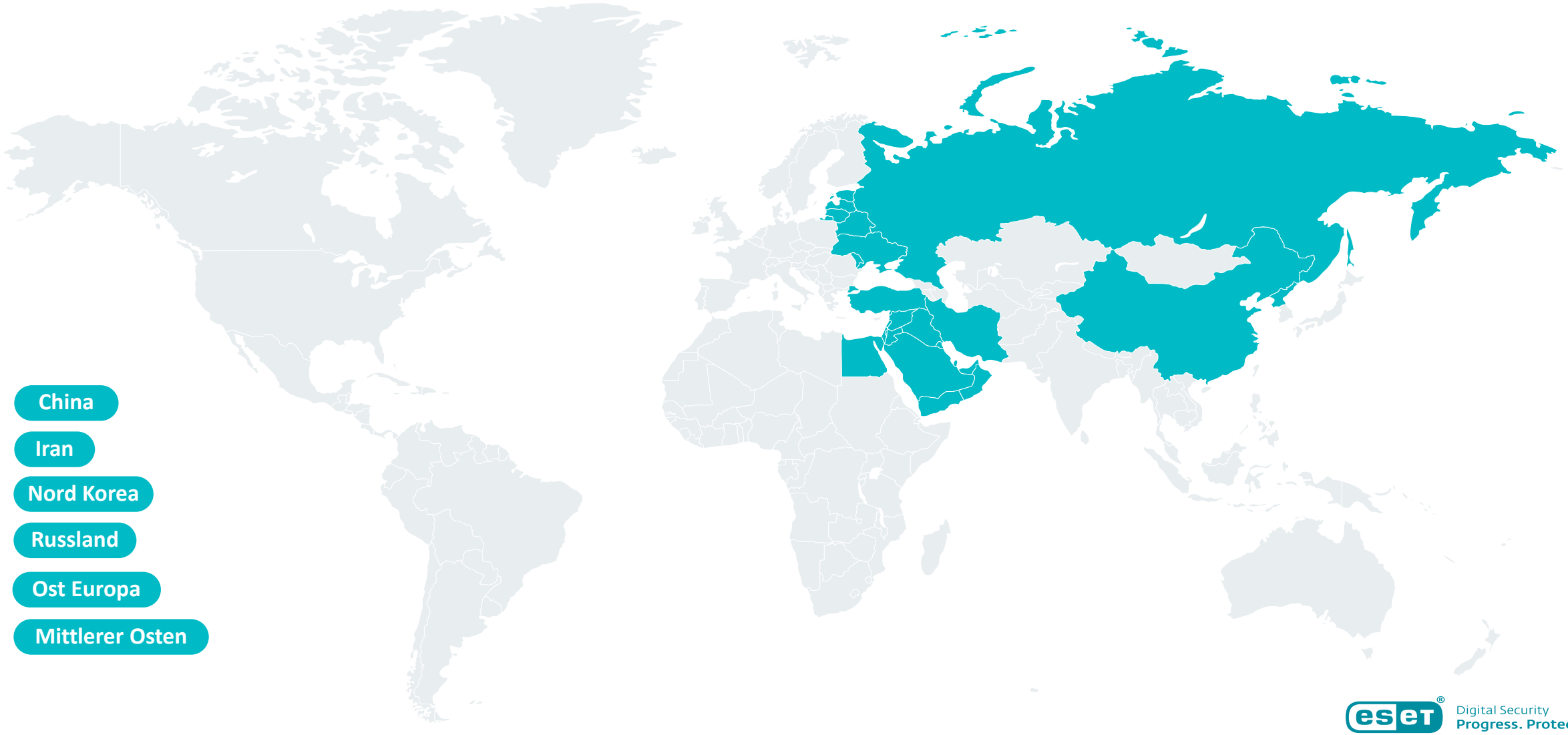
Technical Analysis reports



Monthly Overview Reports

IOCs (MISP)	IOCs (STIX/TAXII)	Snort rules	YARA rules	MITRE ATT&CK mapping
APT Feed	Access to APT MISP	Retrospective Intelligence	Pre-publication access to welive security	Access to analysts

ESET - APT GROUPS REPORTS



- China
- Iran
- Nord Korea
- Russland
- Ost Europa
- Mittlerer Osten

ESET AntiVirus Lösungen
Full Disk Encryption

Anforderung an eine Verschlüsselung

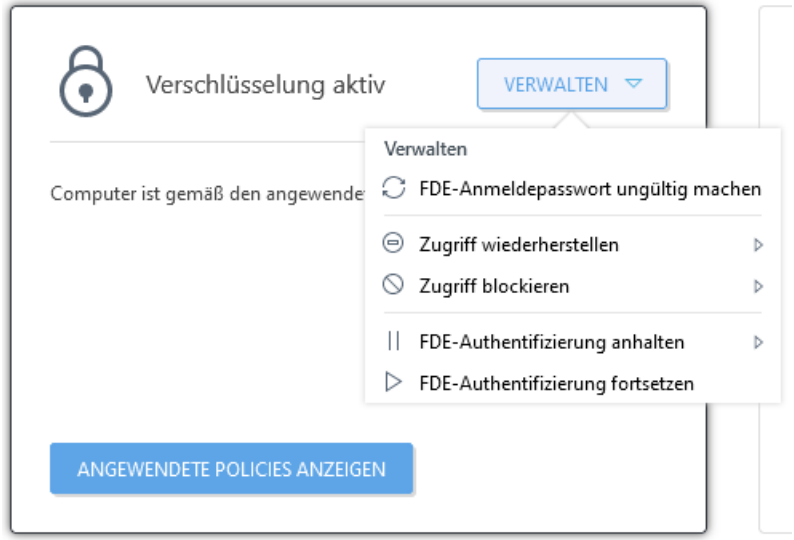
- Schutz der lokalen Daten bei Diebstahl des Endpunktes

- Zentrale Verwaltung im ESET PROTECT Management
- Einfache Verteilung auf die Endpunkte durch den Administrator im ESET PROTECT
- Self Enrollment durch den Benutzer

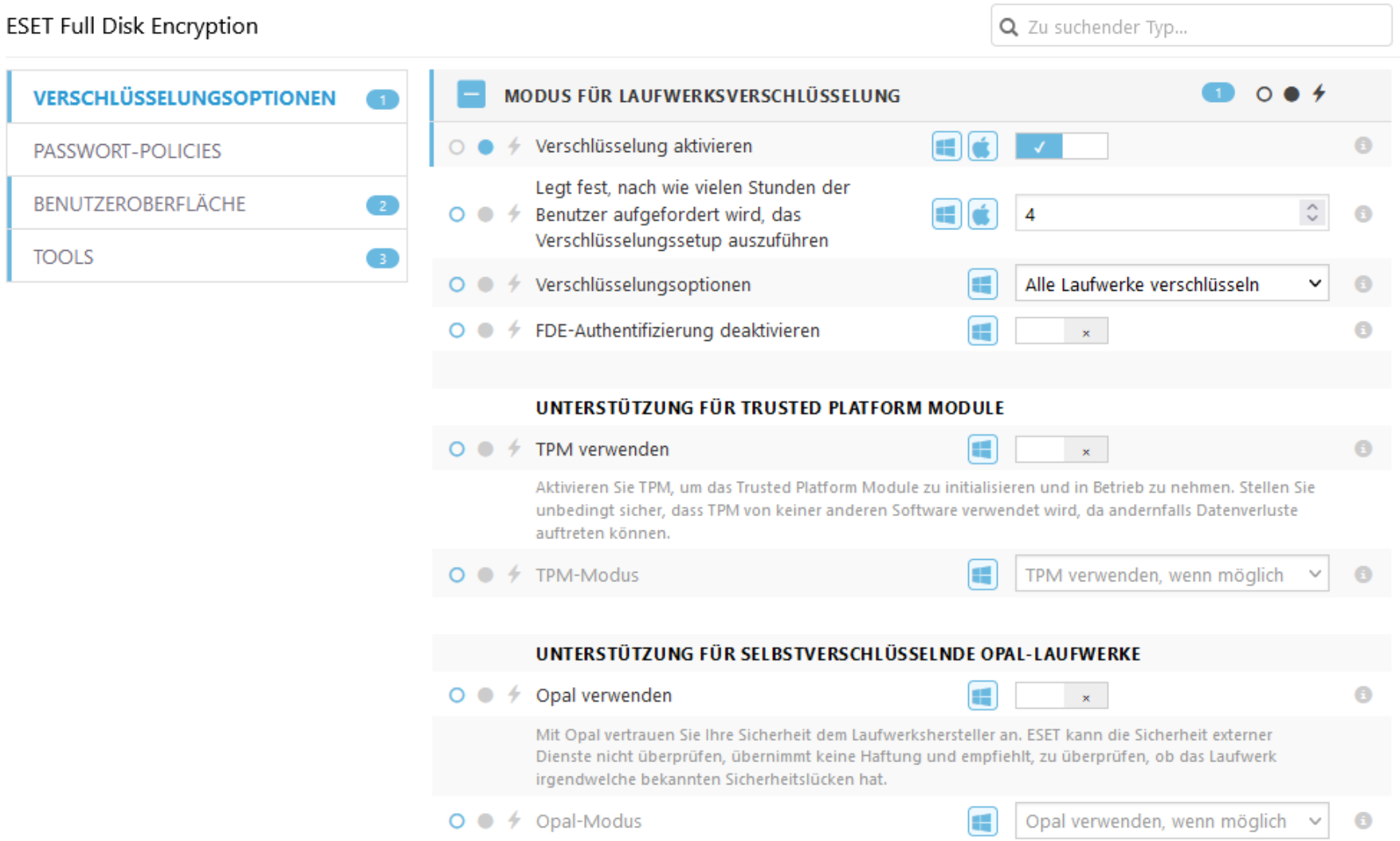
- Erfüllung der DSGVO Datenschutzes

EFDE – Management Funktionen im ESET PROTECT

- Der Administrator aktiviert die Verschlüsselung über das ESET PROTECT Management
- Verschlüsselungs-Software Rollout auf die Endpoints
- Verschlüsselung zentral starten
- Endpoint zentral entschlüsseln, falls Mitarbeiter das Unternehmen verlässt
- Passwort zentral zurücksetzen, blockieren, löschen

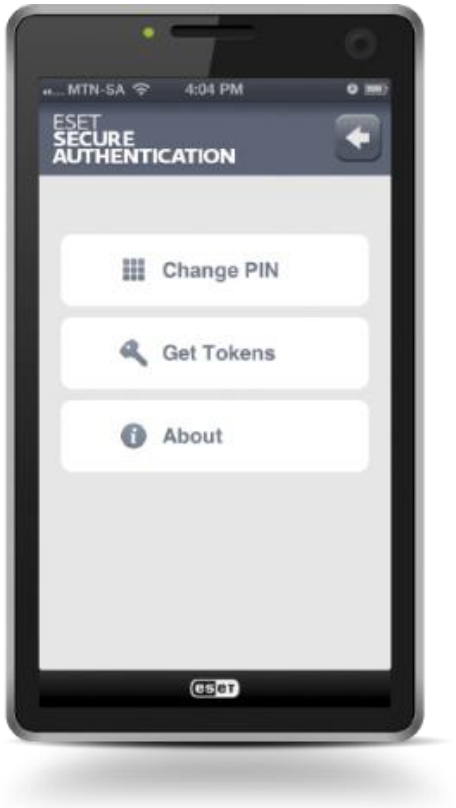


EFDE – Zentrale Verschlüsselungs Policy



ESET Secure Authentication
2-Faktor Absicherung

ESET – ESA - 2 Faktor Möglichkeiten



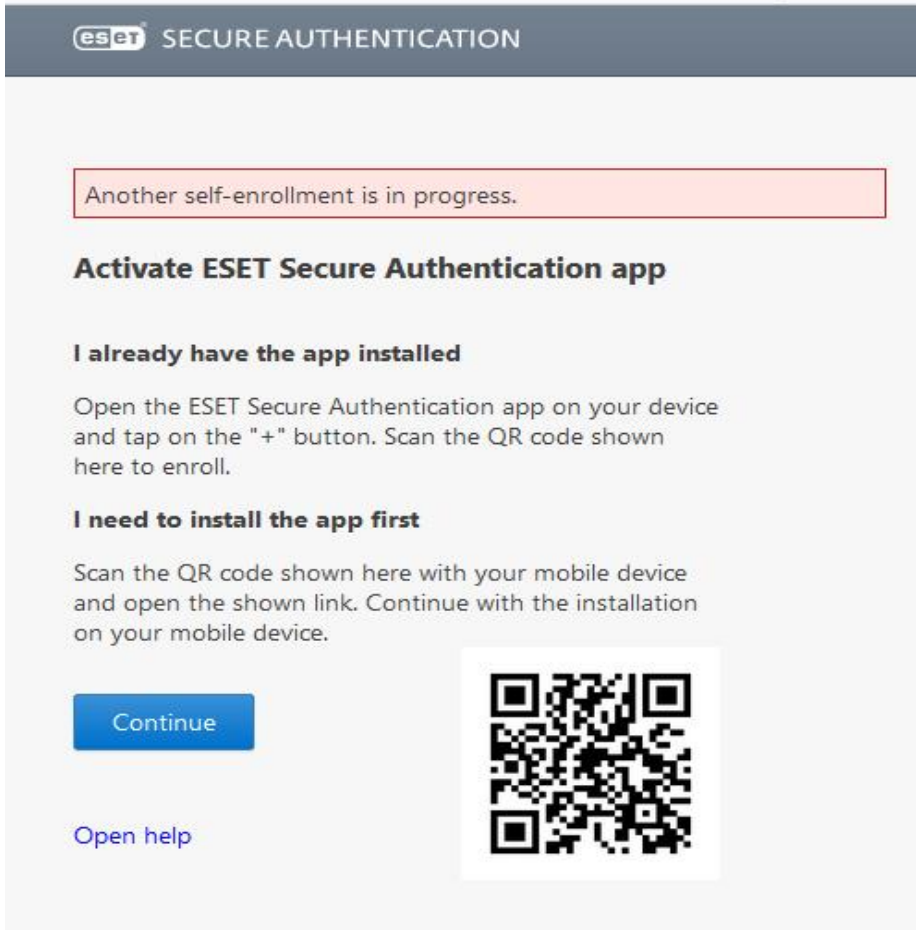
Software Token

Hardware Token

SMS-Token

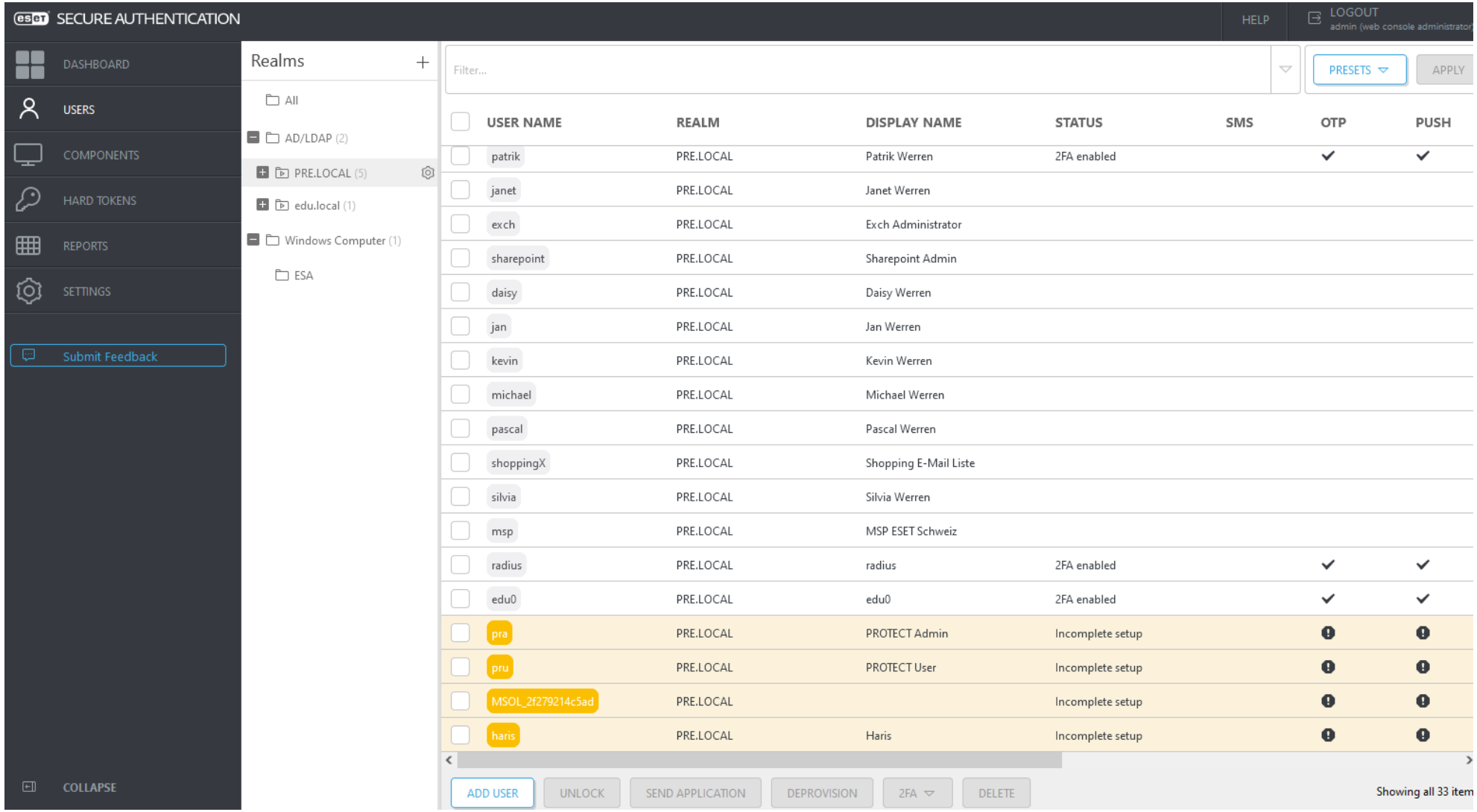
ESET Secure Authentication – Einsatz Möglichkeiten

- Windows Login
- Remote Desktop
- Microsoft Exchange Server
- Microsoft SharePoint Server

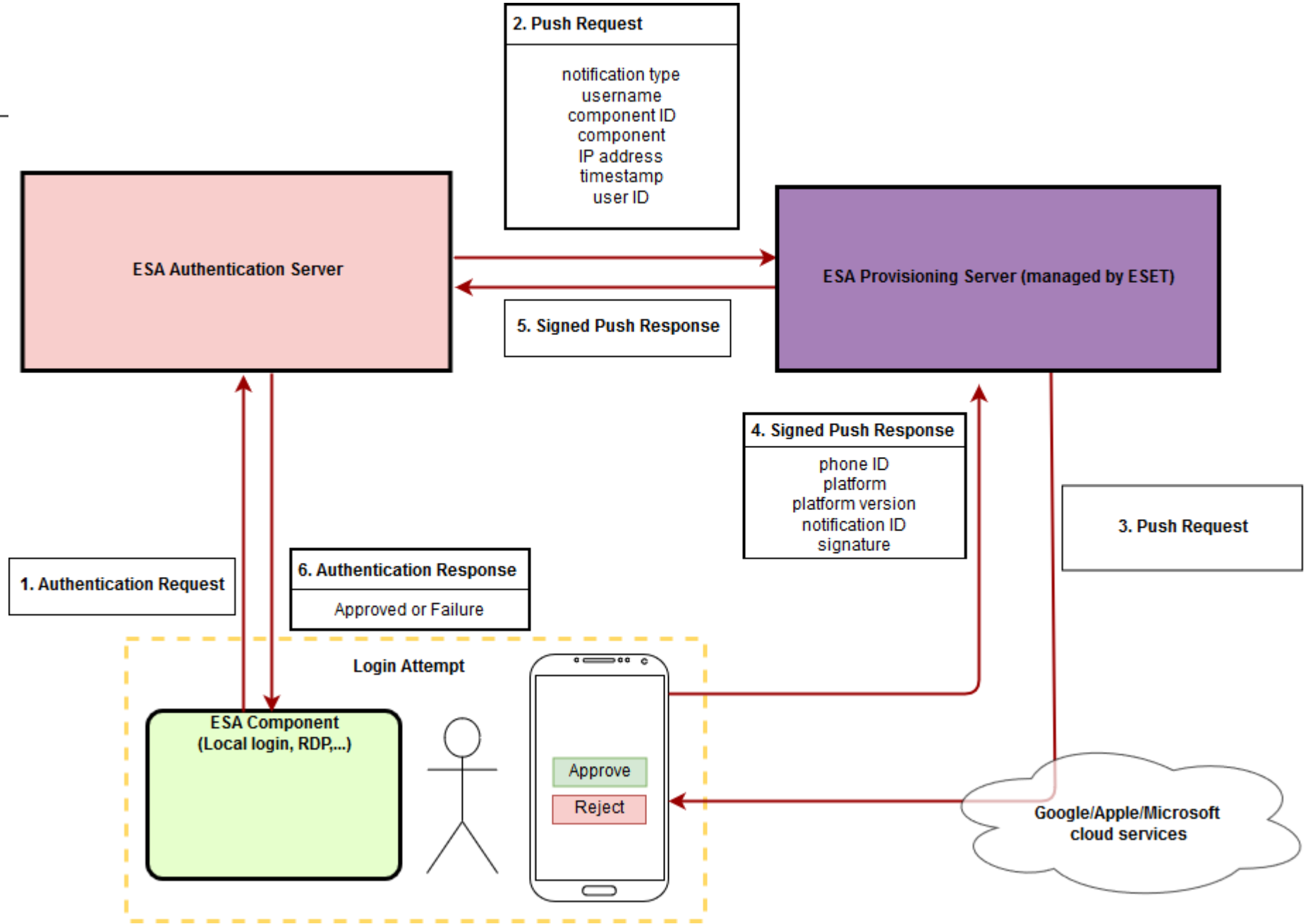


- RADIUS Server für VPN Firewall Verbindungen

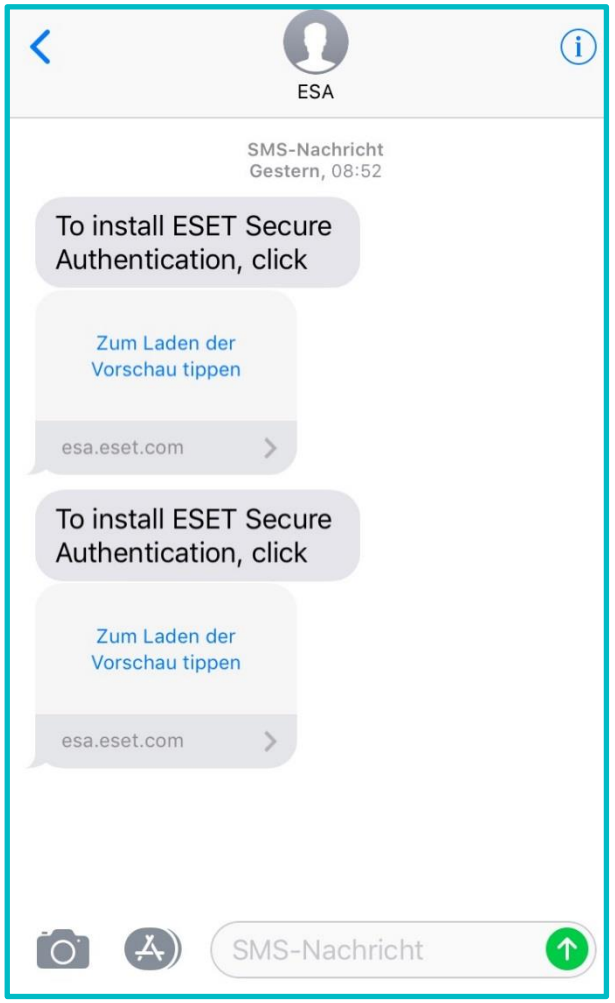
ESET Secure Authentication – Zentrales Management

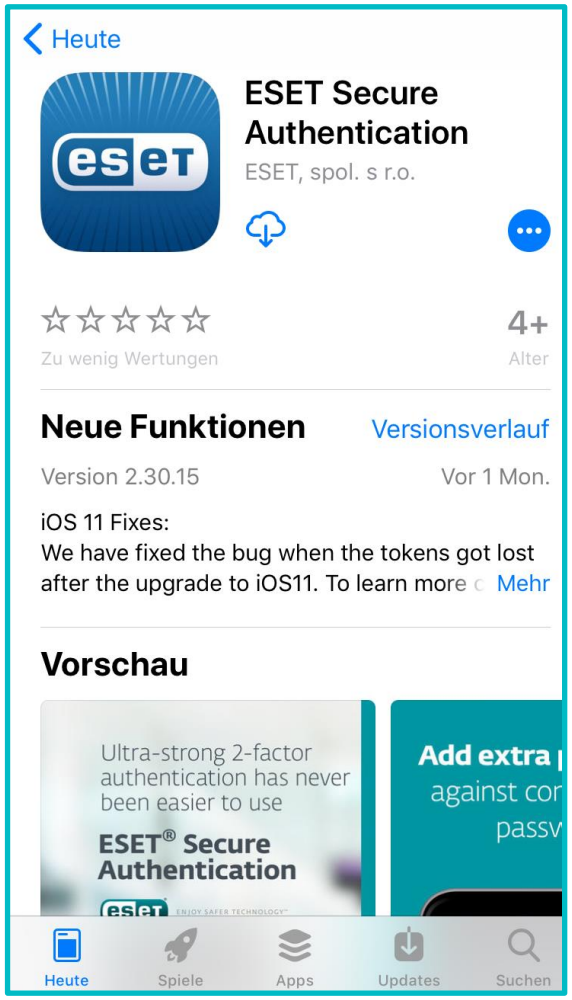


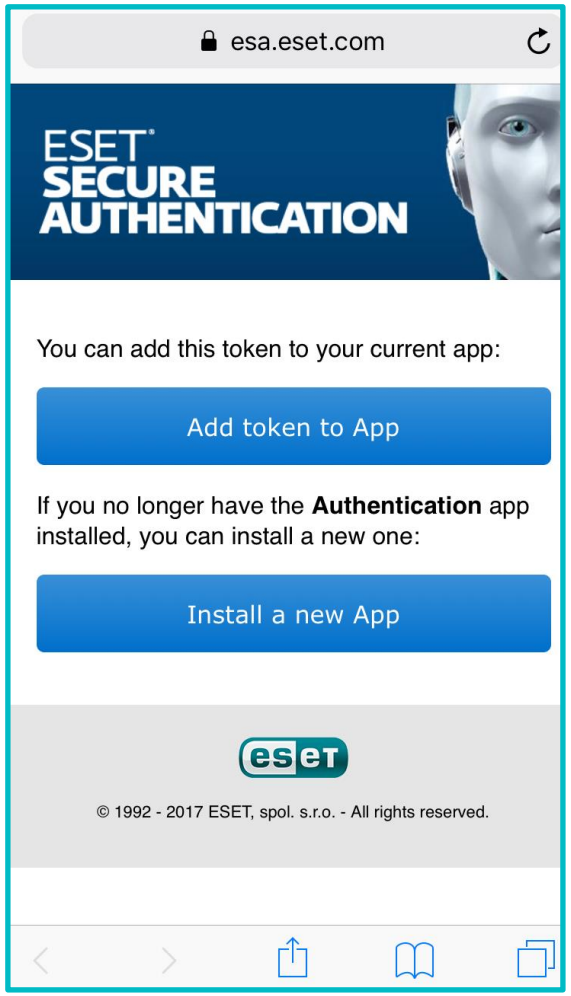
Kommunikation

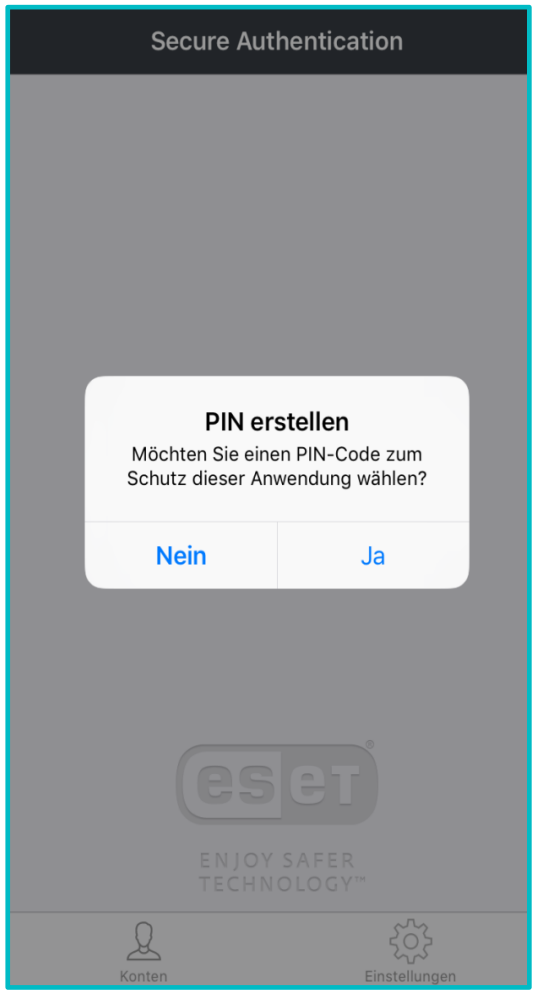


ESET Secure Authentication – Installation auf iPhone - Android

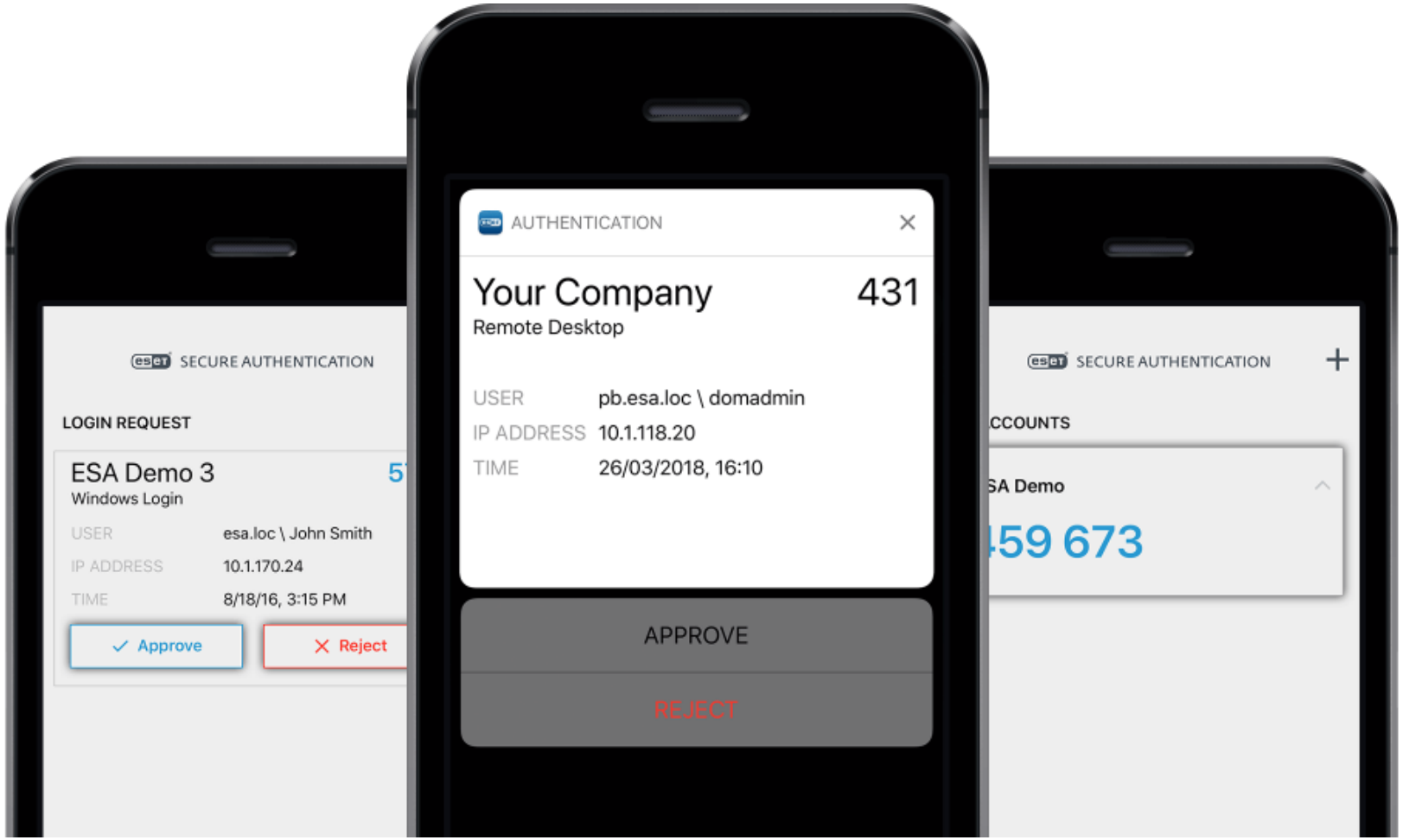








ESET Secure Authentication – OTP-Token & Push Token



Vielen Dank für die Aufmerksamkeit

30 YEARS OF CONTINUOUS IT SECURITY INNOVATION

ENJOY SAFER TECHNOLOGY™