Digital Security
Progress. Protected.

Anleitung:

# ESET SHAREPOINT POC


ESET.DE | ESET.AT | ESET.CH

# Inhaltsverzeichnis

# Beschreibung **des SharePoint PoC**

Der SharePoint PoC umfasst eine komplette Installation mit einem potentiellen Neukunden, welcher seinen SharePoint damit absichern möchte. Dabei zeigen wir auf, welche Möglichkeiten unsere Lösung beinhaltet und richten das Produkt entweder in einer Stand Alone Umgebung (ohne ESET PROTECT), oder in einer verwalteten Umgebung mit dem ESET PROTECT ein.

Zu der Grundkonfiguration gehört es auch, ein Regelwerk mit dem Kunden zu definieren, welche Dateien in die SharePoint Datenbank hochgeladen werden dürfen und welche blockiert werden. Die blockierten Objekte landen in der Quarantäne und wie diese im täglichen Umfeld bedient wird, zeigen wir ebenfalls in diesem Dokument.

# Installation der Sicherheitslösung für **die SharePoint Datenbank**

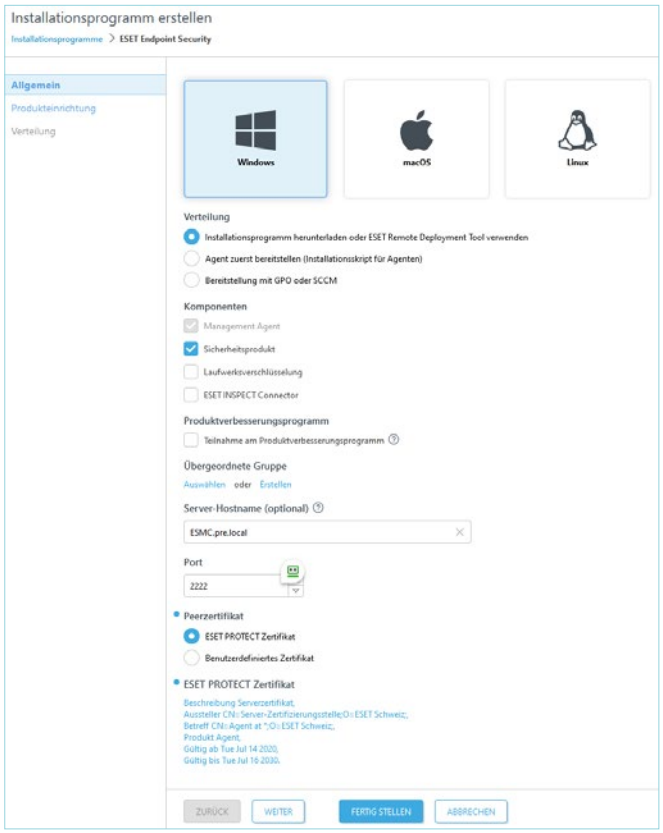
Die Installation kann auf diesen drei möglichen Wegen erfolgen:

1. Erstellen eines Installer in ESET PROTECT
2. Direkter Download und Installation des MSI
3. Installation durch die Aktivierung des Cluster-Modus

### Erstellen eines Installer in ESET PROTECT

Kunden, die ihre SharePoint Server über den ESET PROTECT verwalten, können den SharePoint Schutz direkt als Installer oder einen Task auf die Server verteilen.

Gehen Sie hierzu auf *Installationsprogramme* und klicken Sie auf *Installationsprogramm erstellen*. Danach öffnet sich folgende Maske:

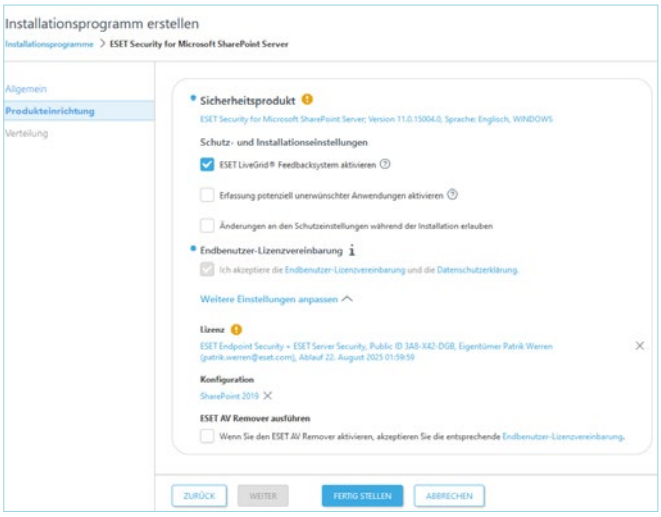



Konfigurieren Sie den Installer anhand dieser Maske mit ihren vorgegebenen Einstellungen. Klicken Sie danach auf *Weiter*.

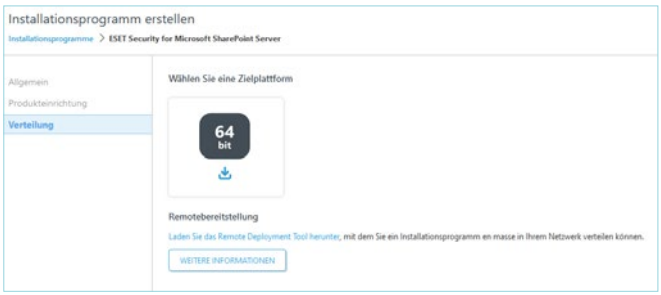
In der nächsten Maske wählen Sie bei Sicherheitsprodukt den aktuellen SharePoint Schutz und die gewünschte Sprache aus.

Die Lizenz wird automatisch von ESET PROTECT ausgewählt.

Wenn Sie bereits eine SharePoint Konfiguration haben, kann diese hier hinterlegt werden.

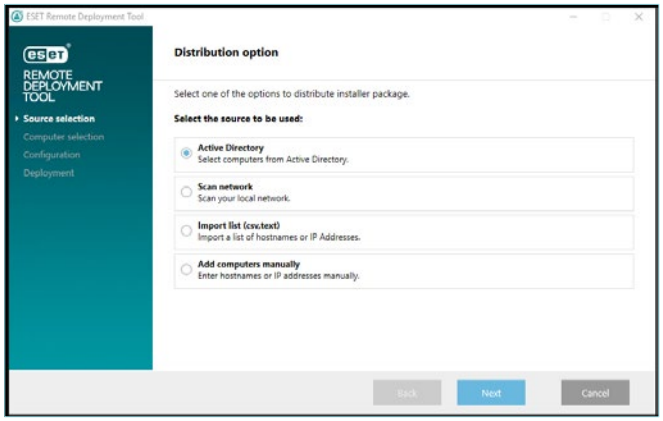



Klicken Sie auf *Fertig stellen*. Anschließend wird der Installer als 64-bit Version heruntergeladen.




Sie können den Installer direkt auf die Server verteilen und mit einem Doppelklick ausführen. Das ist der schnellste Weg, wenn Sie nur wenige SharePoint Server damit ausrollen möchten.

Bei einer größeren Anzahl SharePoint Server können Sie den Installer auch über das ESET Remote Deployment Tool verteilen.

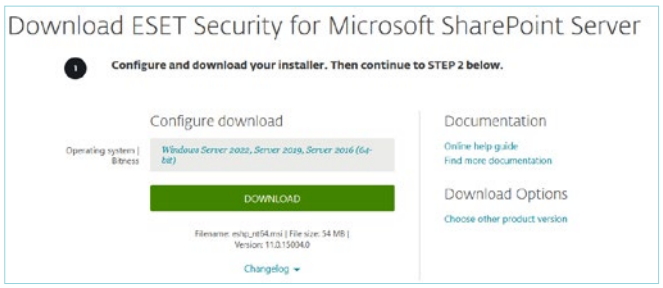



Das Tool bietet die Möglichkeit, die SharePoint Server über das Active Directory auszuwählen, was wir auch empfehlen. Alternativ können Sie die SharePoint Server über eine csv-Liste oder von Hand erstellen, was allerdings einen erheblichen Mehraufwand für Sie bedeutet.

## MSI direkt herunterladen und installieren

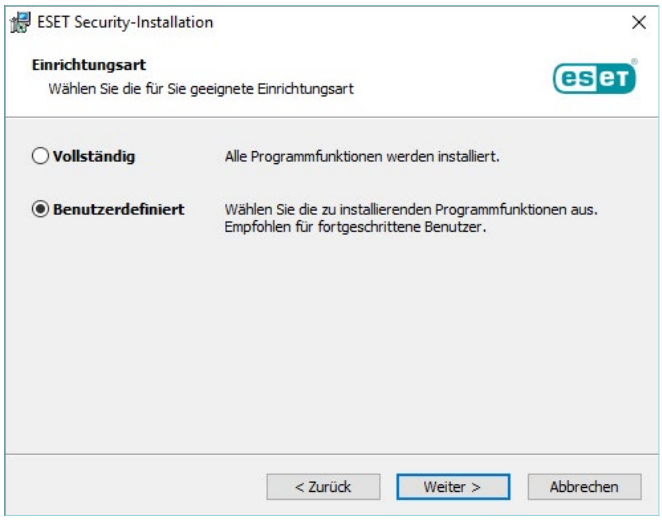
Über den nachfolgenden Link ist es möglich, den ESET SharePoint Installer direkt von unserer Webseite runterzuladen:

↗www.eset.com/int/business/download/microsoft-sharepoint-security/




Mittels der MSI-Datei können Sie die Installation anpassen, sowohl die Komponenten, die Sie installieren möchten als auch die Installationspfade.

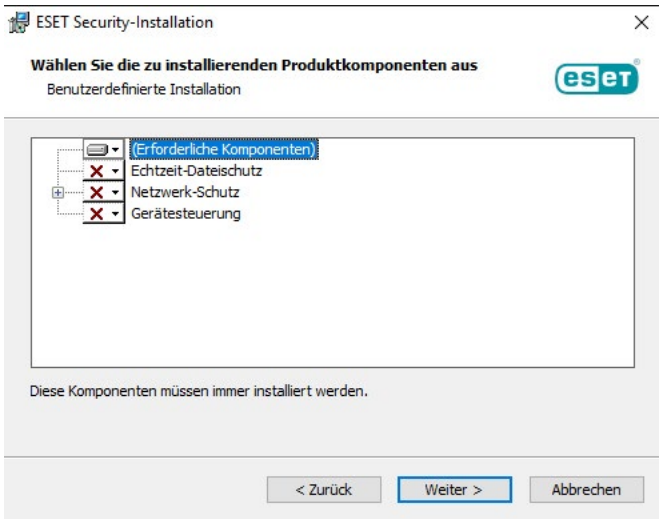

Sobald der Installer startet, können Sie die Installationssprache auswählen. Klicken Sie danach auf *Weiter*.



Im zweiten Schritt, geben Sie an, ob die Installation *Vollständig*, oder *Benutzerdefiniert* erfolgen soll.

Falls Sie die bestehende Sicherheitslösung für den SharePoint Host beibehalten und von ESET nur die SharePoint Datenbank absichern wollen, ist eine benutzerdefinierte Installation erforderlich.

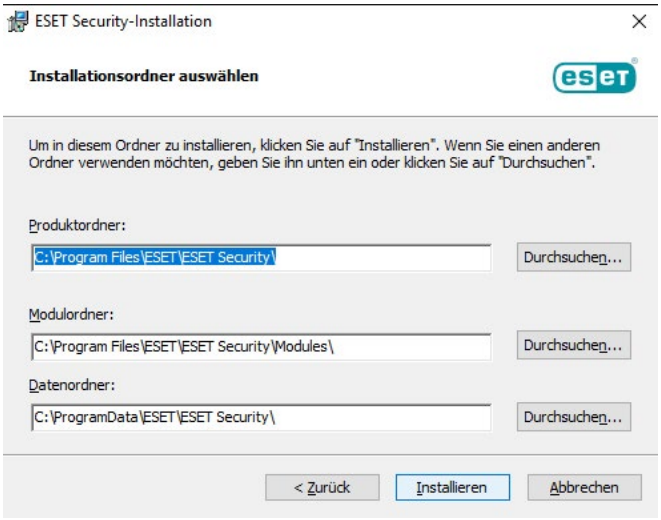
In diesem Fall wählen Sie *Benutzerdefiniert* und klicken auf *Weiter.*




Deaktivieren Sie folgende Komponenten:

1. Echtzeit-Dateischutz
2. Netzwerk-Schutz
3. Gerätesteuerung

Danach klicken Sie auf *Weiter*




Im letzten Schritt besteht die Möglichkeit, ESET for SharePoint auf einem anderen Laufwerk als dem C:\-Laufwerk zu installieren, z.B. auf einem lokalen D:\-Laufwerk. Beachten Sie, dass Netzlaufwerke werden NICHT unterstützt werden.

## Installation durch die Aktivierung des Cluster-Modus

Mit der Aktivierung des Cluster-Modus, wird auf sämtlichen ausgewählten SharePoint Servern der ESET Schutz ausgerollt, falls er noch nicht installiert ist. Bei dieser Form der Einrichtung ist es erforderlich, die ESET Software auf dem primären SharePoint zu installieren und anschließend den Cluster-Modus zu aktivieren. Auf der nachfolgenden Seite finden Sie alle Informationen zum Cluster-Modus.

# Konfiguration in ESET PROTECT oder **im lokalen ESET SharePoint GUI**

Die ESET SharePoint Konfiguration kann entweder über das ESET PROTECT Management, oder lokal im GUI erfolgen.

### ESET PROTECT:

Das Management repliziert regelmässig die SharePoint Policy auf sämtliche SharePoint Server.

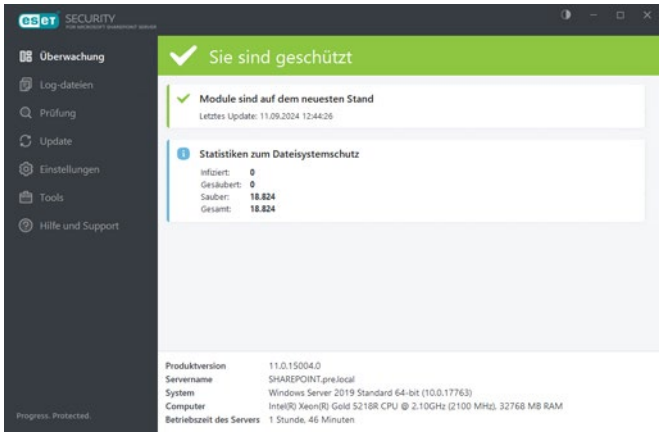
### Lokales ESET-SharePoint GUI:

Möchte der Kunde kein zentrales Management einsetzen, kann die Policy auch lokal im ESET SharePoint GUI konfiguriert werden. Die Replikation der Policy auf sämtliche SharePoint Server übernimmt der ESET Cluster-Modus.

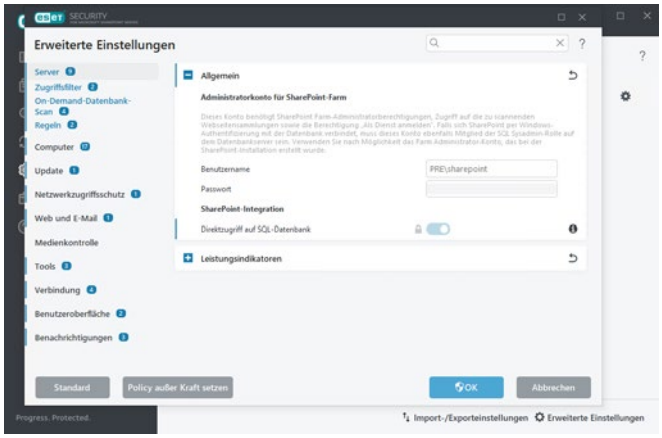
Es spielt dabei keine Rolle, auf welchem Server die Policy angepasst wird. Sobald auf einem SharePoint Server eine Änderung an der Policy vorgenommen wird, ändert sich die Policy automatisch auf sämtlichen SharePoint Servern.

# Erklärung der wichtigsten Einstellungen **im ESET SharePoint GUI**

Ohne das zentrale Management ESET PROTECT lassen sich die meisten Einstellungen direkt auf den SharePoint Servern einstellen. Wir zeigen diese Themen kurz in der Demo.




In der ESET Security for SharePoint sehen Sie beim Reiter *Überwachung* den aktuellen Stand der Module und die Statistiken zum Dateisystemschutz.

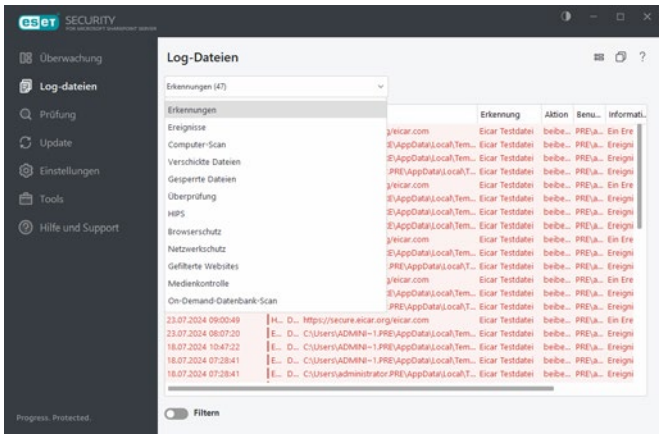



Die wichtigste Einstellung für den PoC ist die Integration des SharePoint-Farm Konto. Damit ist die ESET Sicherheitslösung in der Lage, Dateien in der SharePoint Datenbank zu scannen.

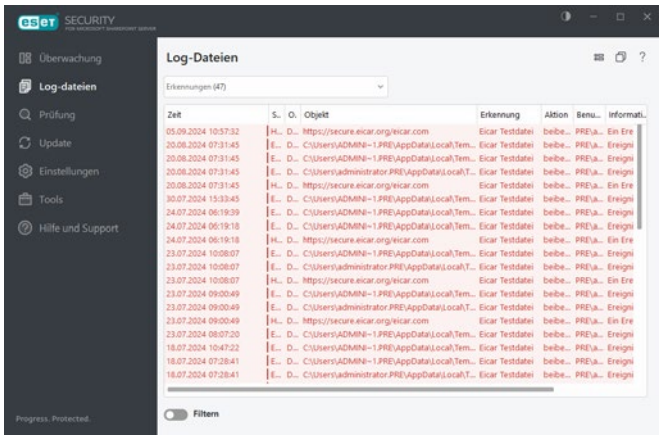
Dies umfasst die SharePoint Datenbanken, wie auch den Up- und Download auf den einzelnen SharePoint Sites.

Die Integration des SharePoint-Farm Admins kann lokal auf dem SharePoint Server oder auch direkt in der Policy in ESET PROTECT erfolgen.

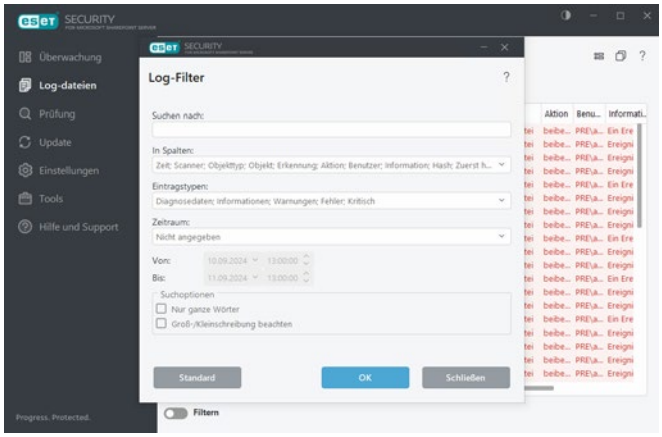
Bei größeren Umgebungen ist es auch möglich bei einer großen Anzahl an SharePoint Servern, dies direkt über eshell und einen Task in ESET PROTECT auf Hunderten von SharePoint Servern einzutragen.



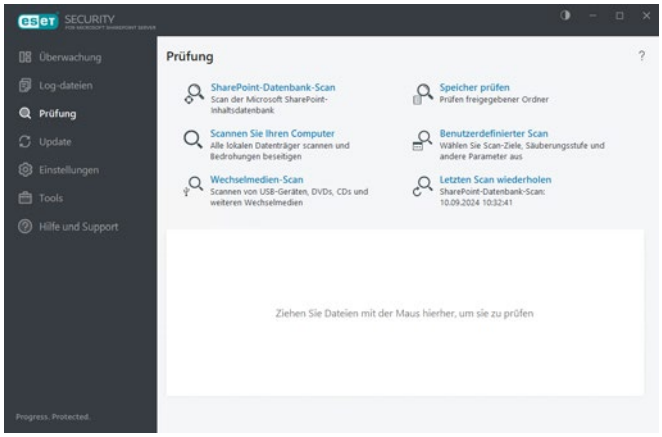

Die wichtigsten Logs im Bereich SharePoint sehen Sie in den Registern *Erkennungen* und *On-Demand-Datenbank-Scan*.



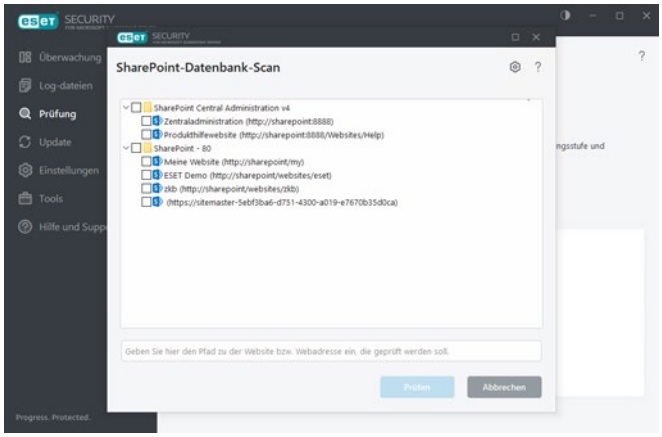

Suchen Sie gezielt nach einem Event, ist es ratsam, den Filter zu nutzen.



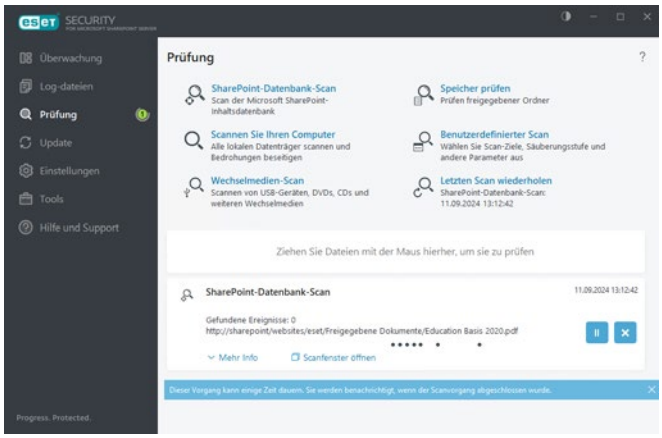

Der Log-Filter ermöglicht es, nach einem Event-Namen, nach Spalten, Eintragstypen und über einen speziellen Zeitraum zu suchen.



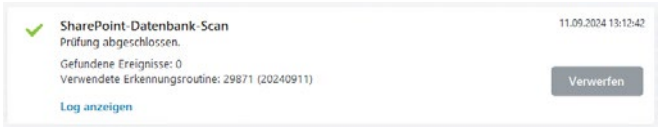

Die SharePoint Datenbanken können direkt über das GUI auf Malware geprüft werden. Wir empfehlen den zeitgesteuerten Scan über einen Task.



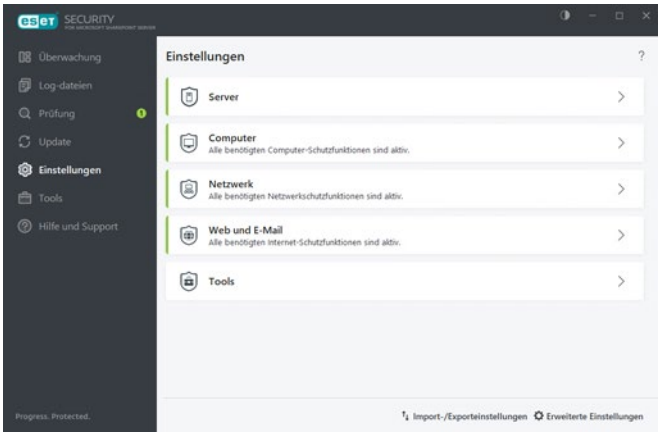

Beim manuellen Scan wählen Sie einfach die gewünschte/n SharePoint Datenbank/en aus und klicken auf *Prüfen*.




Danach läuft der Malware-Scan. Die Prüfzeit variiert je nach Größe der Datenbank. Bei einer großen Datenbank kann es auch bis zu mehreren Stunden dauern.

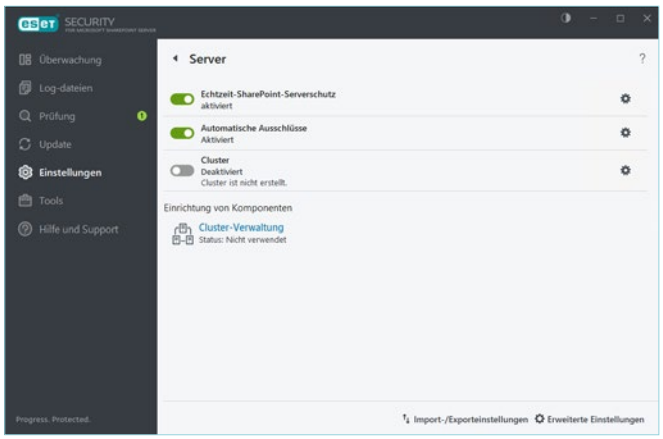



Ist der Scan komplett abgeschlossen, erhalten Sie eine Meldung. Möchten Sie den Inhalt des Scans sehen, klicken Sie auf *Log anzeigen.*




Wichtige Einstellungen zu SharePoint finden Sie im Register Server.

# Clustermodus – **für die Policy Synchronisation**




Im Enterprise PoC empfiehlt es sich immer, den Cluster-Modus zu aktivieren.

Der ESET Cluster ist eine P2P-Kommunikationsinfrastruktur aus der ESET Produktlinie für Microsoft Windows Server.

Diese Infrastruktur ermöglicht, dass ESET Serverlösungen miteinander kommunizieren, Daten wie z. B. Konfigurationen und Benachrichtigungen austauschen und die für den ordnungsgemäßen Betrieb einer Gruppe von Produktinstanzen erforderlichen Daten synchronisieren können.

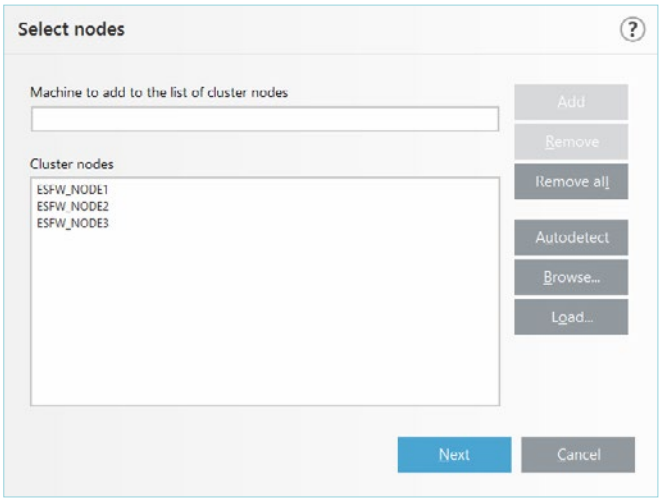
Ein Beispiel einer solchen Gruppe ist eine Knotengruppe in einem Windows-Failover-Cluster oder einem Network Load Balancing (NLB)-Cluster mit installierter ESET Lösung, bei der das Produkt im gesamten Cluster gleich konfiguriert sein muss. ESET Cluster garantiert diese Einheitlichkeit zwischen den Instanzen.

Der Cluster-Modus ist nur sinnvoll, wenn Sie explizit keine zentrale Verwaltung wie ESET PROTECT verwenden möchten. In diesem Fall können Sie die SharePoint Policy auf einem x-beliebigen SharePoint Knotenpunkt anpassen. Die vorgenommene Änderung wird anschließend automatisch auf sämtliche SharePoint Server synchronisiert.

## Cluster aktivieren und konfigurieren

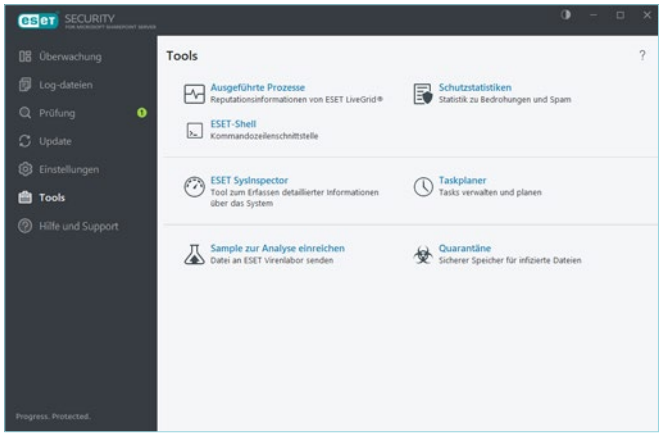
1. Den Schieberegler Cluster einschalten
2. Die Cluster-Member von Hand eintragen oder über die automatische Erkennung suchen.

   **Wichtig:** Der Standardport ist 9777. Sollte dieser Port bereits belegt sein, verwenden Sie eine andere Portnummer.

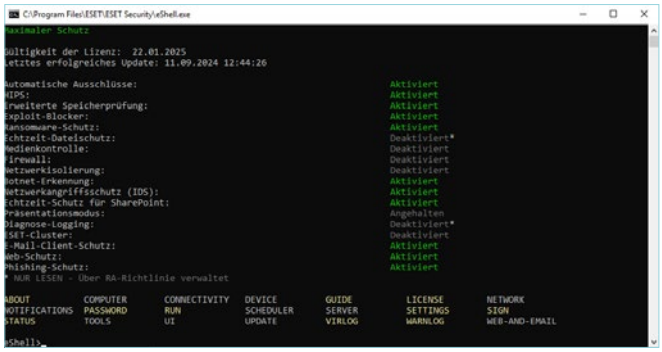



3. Klicken Sie auf *Next* und das Cluster wird automatisch gebaut. Sollte auf einem der Cluster Nodes noch keine ESET SharePoint Software installiert sein, wird sie automatisch über den Cluster Wizzard ausgerollt und installiert.

# ESET **Shell**



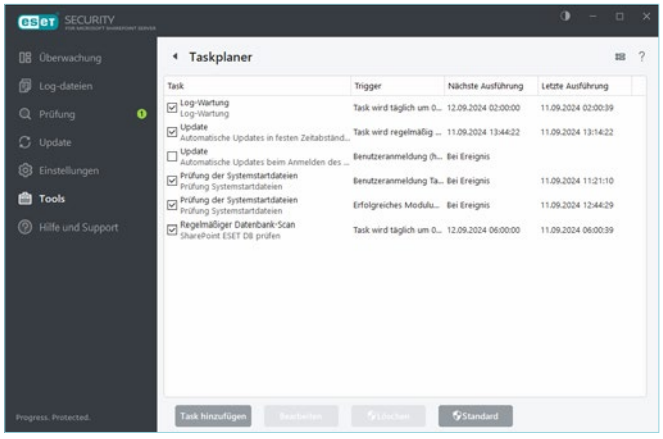

Unter *Tools*, finden Sie den Taskplaner für zeitgesteuerte SharePoint Datenbank Scans, sowie den Aufruf der ESET Shell Kommandos:



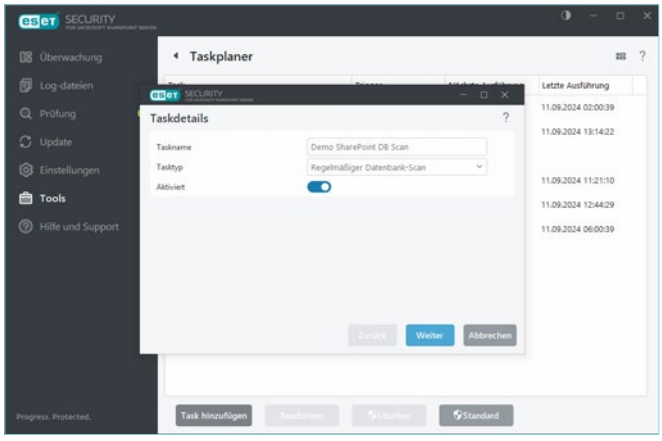

Die ESET Shells können remote per PowerShell über einen Server Task im ESET PROTECT Management aufgerufen werden.

Hier finden Sie den Link zur Beschreibung:
↗help.eset.com/eshp/11.0/de-DE/work_eshell.html

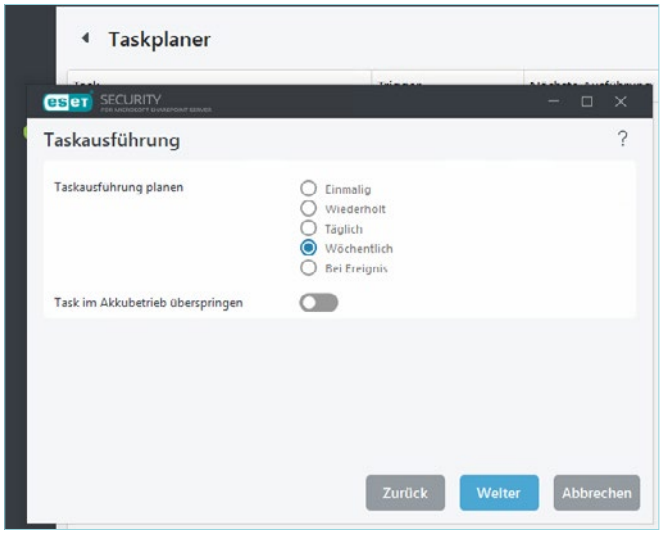
# ESET SharePoint **Taskplaner**



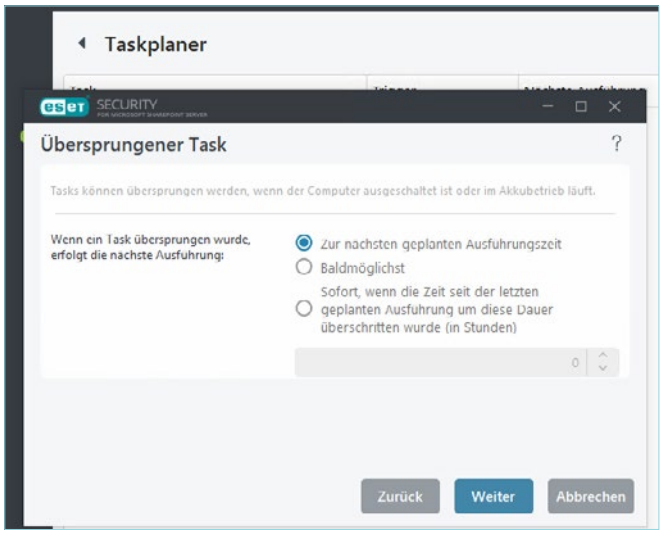

Im Taskplaner sind schon einige voreingestellte Tasks hinterlegt, wie zum Beispiel die Log-Wartung, Updates und die Prüfung der Systemstartdateien.



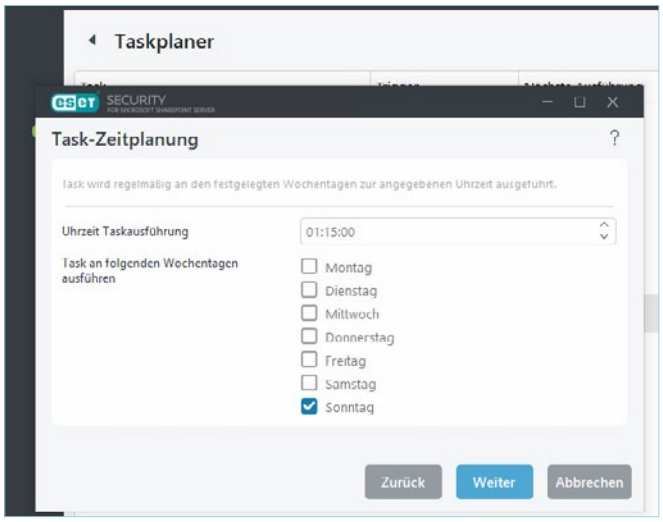

Als Beispiel erstellen wir im PoC eine Demo zum Thema SharePoint Datenbank-Scan. Hierzu klicken wir auf *Task hinzufügen* und vergeben in den Taskdetails einen *Tasknamen*. Beim *Tasktyp* wählen wir *Regelmäßiger Datenbank-Scan* aus.



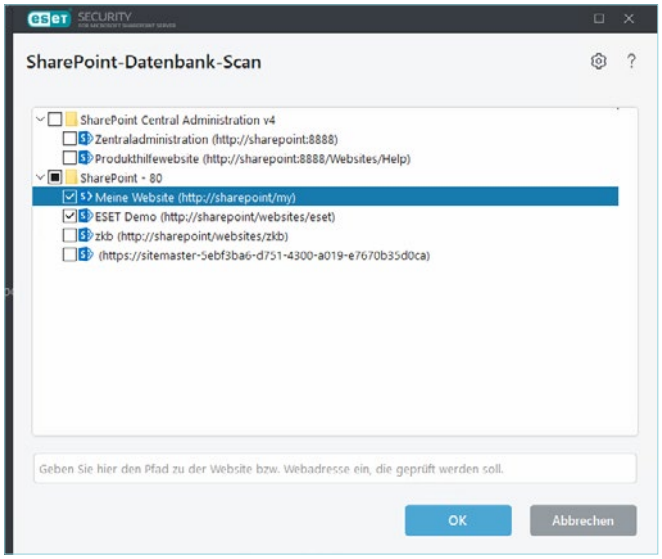

Den SharePoint Datenbank-Scan planen wir mit einer wöchentlichen Ausführung.




Der Task soll zur nächsten geplanten Ausführungszeit ausgeführt werden.

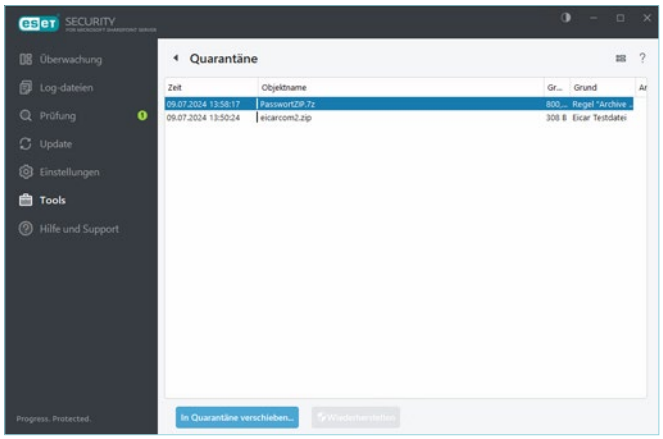



Damit der SharePoint Server in der Leistung nicht beeinträchtigt wird, legen wir die Taskausführung auf Sonntag 01:15 Uhr.




Wir wählen die SharePoint Datenbanken aus, die auf Malware geprüft werden sollen. Im Anschluss wird der Task angelegt und am definierten Zeitpunkt ausgeführt.

# ESET SharePoint **Quarantäne**




Jeder SharePoint Server besitzt eine lokale Quarantäne seiner SharePoint Datenbanken.

Es ist möglich, an dieser Stelle Objekte wieder freizugeben. Verwalten Sie den SharePoint Server über ESET PROTECT, finden Sie die Quarantäne-Objekte direkt im Management. Dort müssen sie auch freigegeben werden.

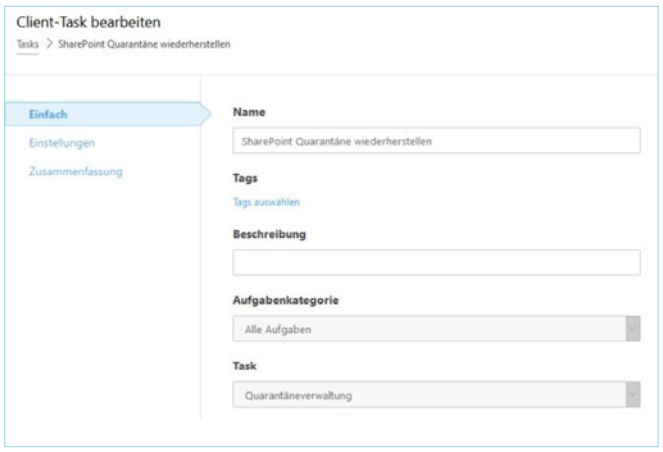
Muss eine große Anzahl an Objekten aus der Quarantäne freigegeben werden, empfiehlt es sich, dies per ESET Shell über einen Server-Task zu tun.

**Nachfolgendes Beispiel**

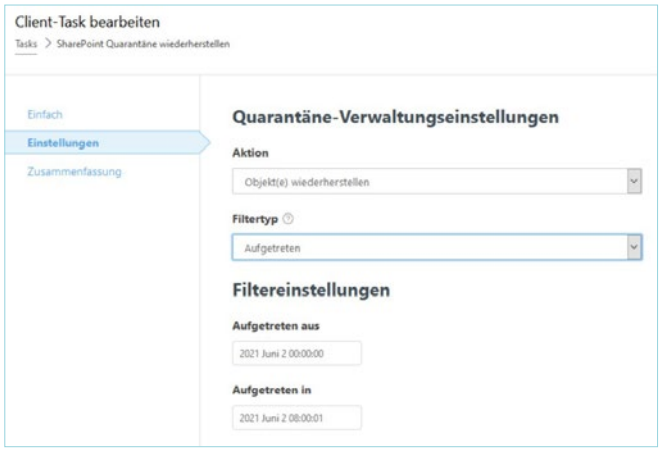
### Passwortgeschützte Archive aus der ESET SharePoint Quarantäne wiederherstellen

Datenbankobjekte, die von ESET in die Quarantäne verschoben werden, können nicht mittels GUI auf dem SharePoint Server wiederhergestellt werden. Dies wird über einen Task in ESET PROTECT vorgenommen.

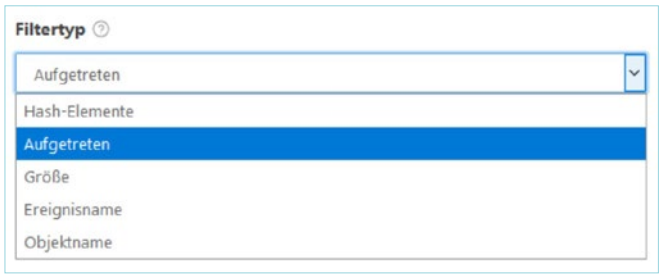
## 1. Erstellen eines Quarantäne Wiederherstellungstasks



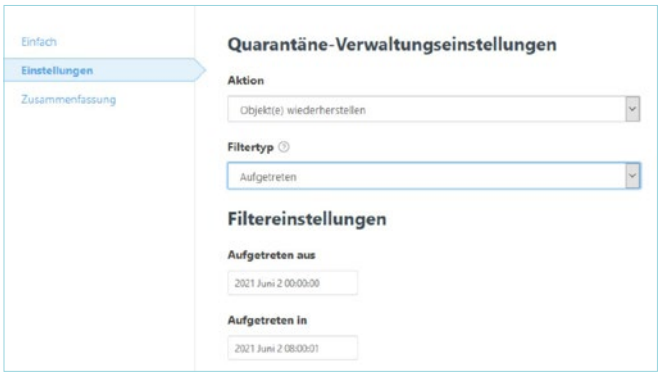

Wählen Sie beim Client-Task unter Task *Quarantäneverwaltung* aus




Es gibt unterschiedliche Filtertypen, die je nach Fall gezielt eine Wiederherstellung einleiten können. Wurden durch einen Datenbank-Scan sehr viele ZIP-Dateien mit Passwortschutz gelöscht, ist die einzige effektive Möglichkeit, die Dateien zwischen zwei Zeitstempeln wiederherzustellen.

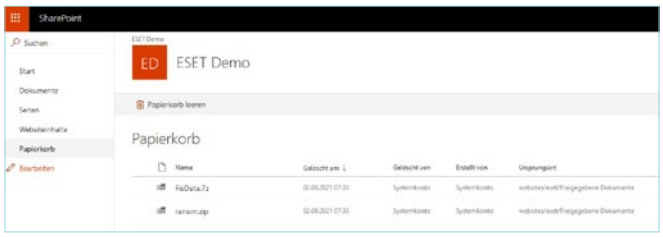



Dazu schauen Sie am besten in der Log-Datei nach, von wann bis wann der Datenbank Scan gelaufen ist. Tragen Sie anschließend den Anfangs- und Endwert ein.

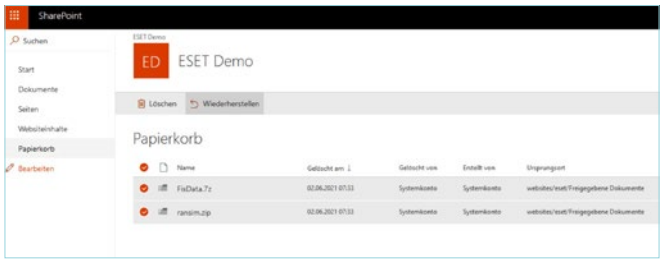



**2. Sobald die Erstellung des Tasks erfolgt, werden Sie aufgefordert, einen Trigger einzustellen. Hier kann der Admin im Anschluss definieren, wann der Wiederherstellungstask aufgeführt werden soll.**

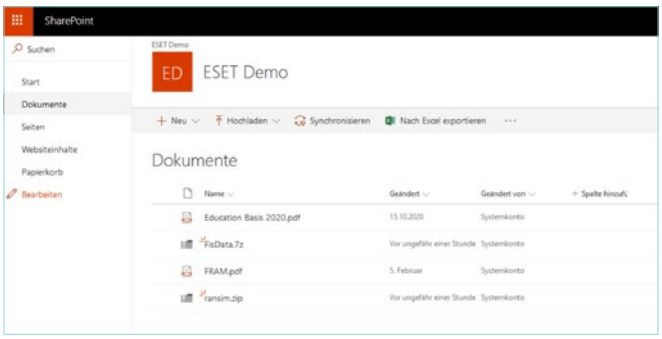
**3. Sobald der Task vollständig durchgelaufen ist, sind sämtliche t Archive im SharePoint wieder verfügbar und verschwinden aus der Quarantäne.**




Wichtiger Hinweis an alle Nutzer: Die Archive werden im Papierkorb wiederhergestellt und benötigen eine Nacharbeit auf dem SharePoint Server.



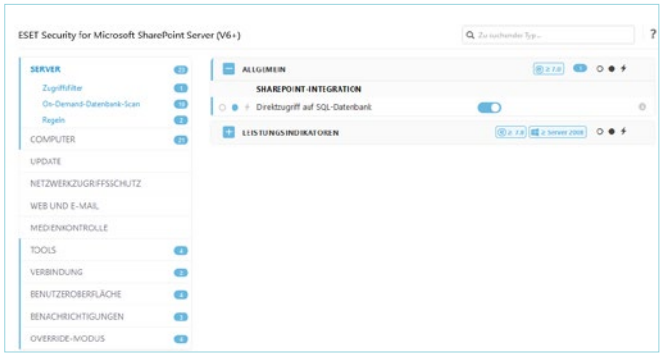

Die Dokumente müssen alle selektiert werden. Anschließend gelangen Sie über den Button *Wiederherstellen* zurück an den Ursprungsort.



# Konfiguration der SharePoint **Policy im ESET PROTECT**

In diesem Abschnitt stellen wir die Einstellungen direkt in der SharePoint Policy im ESET PROTECT vor. Im Wesentlichen sind sie gleich aufgebaut wie direkt im GUI auf dem SharePoint Server.

Es gibt aber ein paar Details, welche nur über den ESET PROTECT gesteuert werden können.



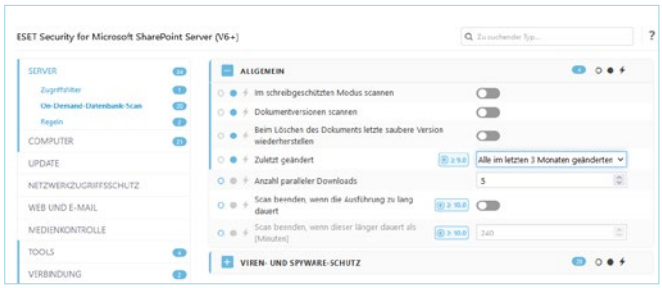

Der Direktzugriff auf die SharePoint SQL-Datenbank wird in der Policy eingeschaltet.


Die SharePoint Schutzeinstellungen umfassen:

*Einschalten:* Dokumente beim Hoch- und Runterladen scannen

*Fragen an Kunden:* Sollen infizierte Dokumente heruntergeladen werden können?

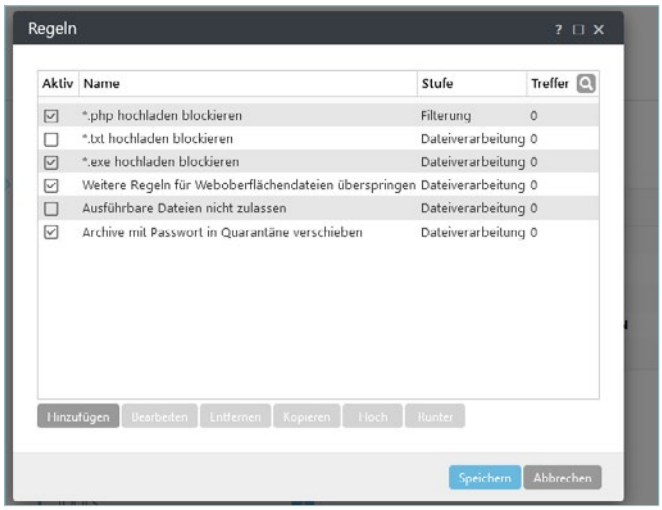
*Einschalten:* Versuchen, infizierte Dokument zu säubern



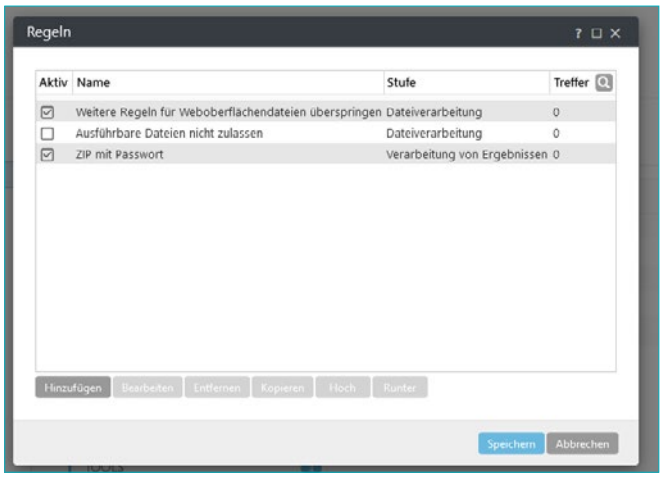

*Im schreibgeschützten Modus scannen* wird empfohlen, falls Sie externe SharePoint Datenbanken ins Unternehmen migrieren und in einem ersten Schritt feststellen möchten, ob sich Malware darin befindet, ohne sie zu löschen. Bitte bachten Sie, das dies nur eine Auswertung darstellt.


Die Regeln umfassen:

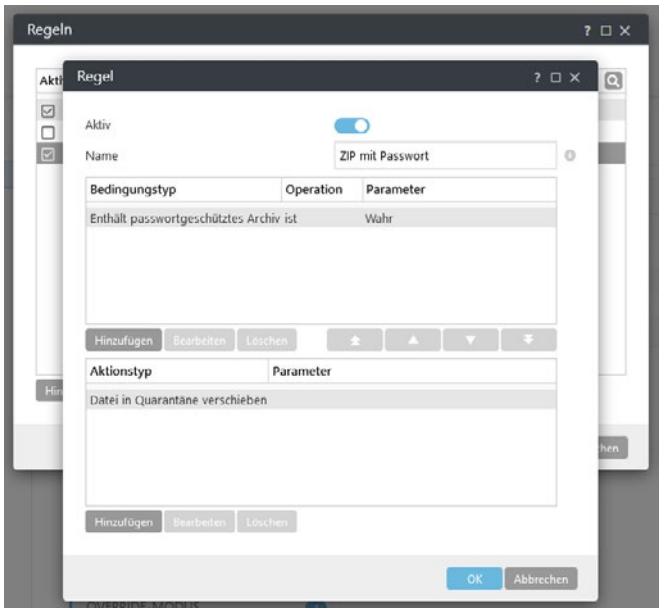
1. Zugriffsfilter auf die SharePoint Datenbank
2. Filterregeln für den On-Demand-Datenbank-Scan




Im PoC sind folgende Erweiterungen zur Demo vorhanden: .php, .txt, .exe.




Die Regel ZIP Passwort kann aktiviert und deaktiviert werden.

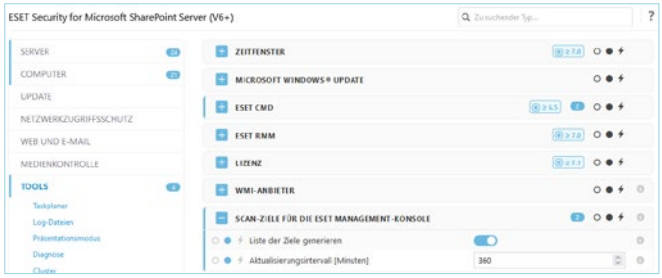



Eine Regel umfasst immer einen Bedingungstypen und einen Aktionstypen:

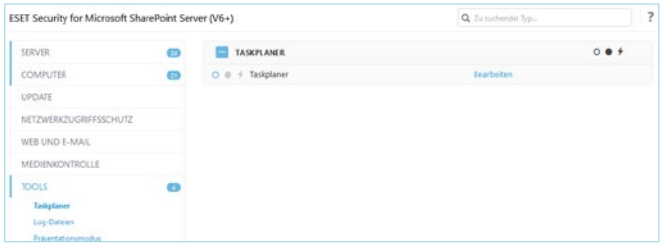
*Bedingungstyp:* Worauf sich die Regel bezieht

*Aktionstyp:* Was soll geschehen, falls der Parameter *Wahr* zutrifft

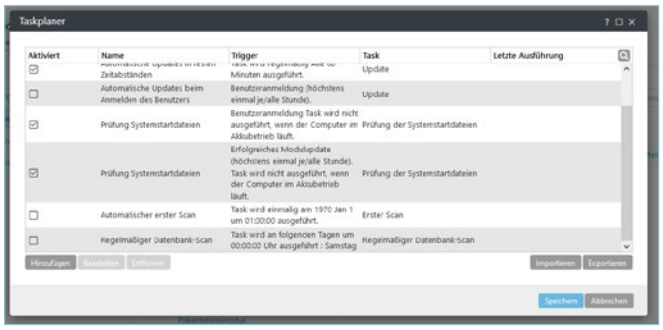

Die erweiterten ECMD-Befehle erlauben dem Administrator, mittels PowerShell mögliche Kommandos der ESET SharePoint Security über die Shell auszuführen. Es wird empfohlen, dafür immer ein Passwort zu setzen.



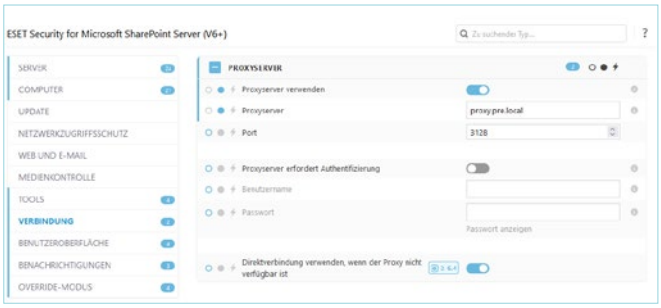

Die Scan-Ziele umfassen SharePoint Datenbanken. Damit sie für einen zeitlich gesteuerten Scan-Task verwendet werden können, ist es erforderlich, sie vorgängig auszulesen und an ESET PROTECT zu übermitteln.




Die Tasks können entweder direkt im GUI auf dem SharePoint Server oder zentral in der ESET PROTECT Management-Konsole angelegt und geändert werden.




Sämtliche Tasks werden in der Übersicht angezeigt und können jederzeit bearbeitet werden.

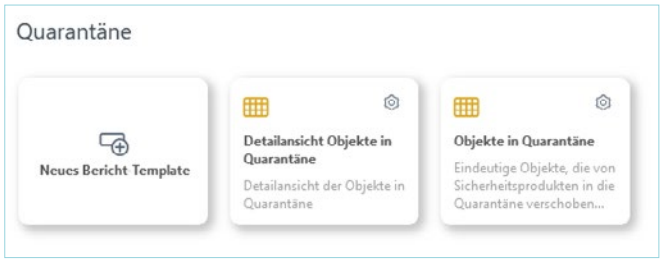



In dem meisten Fällen haben die SharePoint Server bei den Kunden keinen direkten Zugriff auf die Cloud. Damit sich das ESET SharePoint Produkt aktiveren sowie Modul- und Signaturupdates empfangen kann, ist ein Proxy Server einzutragen - entweder der Proxy Server vom Kunden oder alternativ auch eine ESET Bridge.

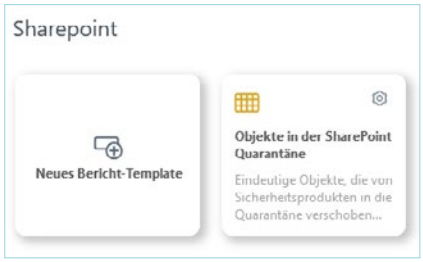
# SharePoint **Quarantäne Bericht**

ESET bietet standardmäßig keinen Quarantäne-bericht an. Es ist allerdings kein Problem, ihn selbst zu erstellen. So geht's:

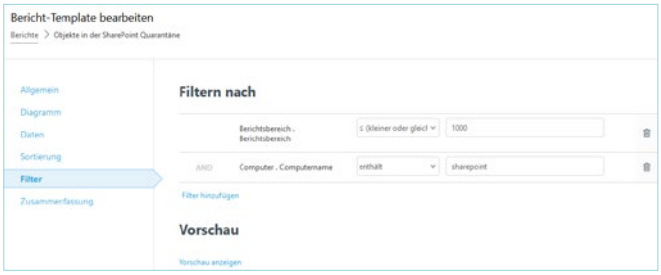
1. Erstellen Sie bei den Berichten eine neue Kategorie namens *SharePoint*.
2. Kopieren Sie den bestehenden Bericht *Objekte in Quarantäne* und weisen Sie sie der Kategorie *SharePoint* zu.



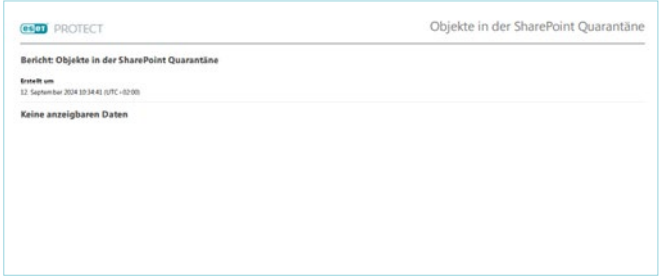

3. Benennen Sie den kopierten Bericht um in *Objekte in der SharePoint Quarantäne*




4. Erweitern Sie den Bericht unter *Filter* mit einer AND-Bedingung «Computer, Computername» > enthält > sharepoint.
   Beachten Sie, dass der Servername *sharepoint* dem Server des Kunden entsprechen muss!



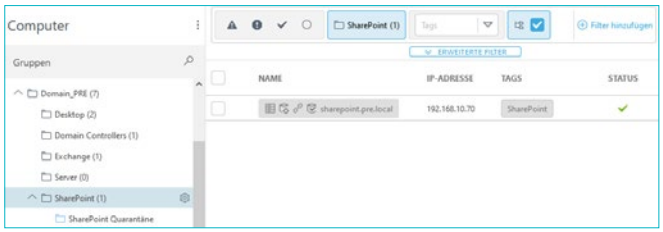

5. Erstellen Sie einen Testbericht als PDF zur Kontrolle. Er enthält beim ersten Aufruf noch keine Daten.



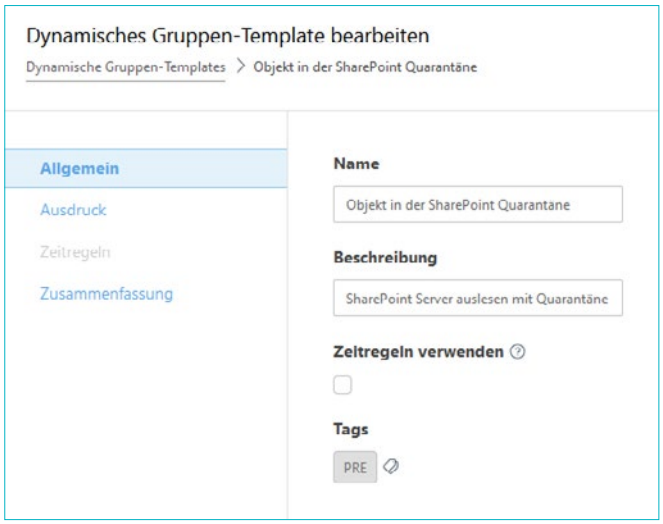
Digital Security
Progress. Protected.

# SharePoint Quarantäne
# **Benachrichtigung per E-Mail einrichten**

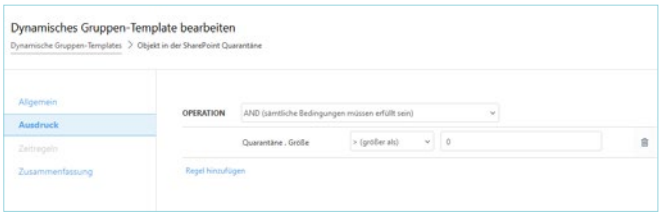
Sobald Malware in die SharePoint Quarantäne verschoben wird, gibt es eine aktive Benachrichtigung. Sie wird unmittelbar per E-Mail ausgelöst. Die Benachrichtigung wird über eine dynamische Gruppe realisiert.




1. Im Beispiel erstellen wir eine statische Gruppe für sämtliche SharePoint Server.
2. Unter der statischen Gruppe erstellen wir anschließend eine dynamische Quarantäne Gruppe.

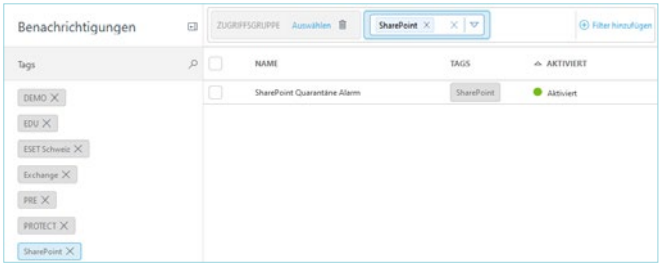



Wir fügen dann der dynamischen Quarantäne-Gruppe ein Gruppen-Template hinzu. In unserem Beispiel benennen wir dieses *Objekt in der SharePoint Quarantäne*.

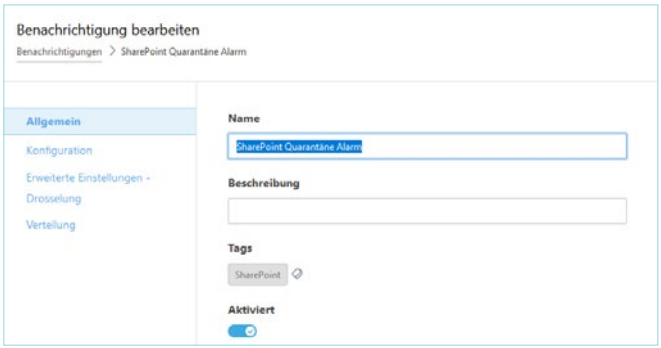


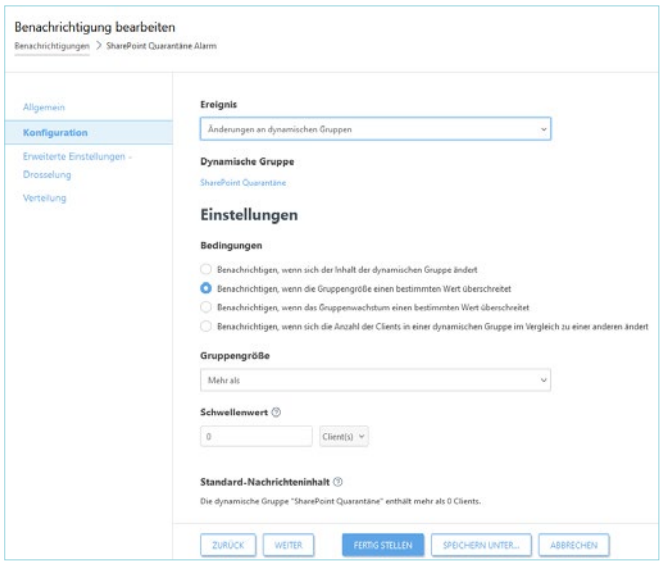

Unter *Ausdruck* fügen wir anschließend eine Regel hinzu. Als Operation wählen wir eine AND-Regel und die Filterung *Quarantäne*, *Größe* wird als *größer 0* definiert.

## Quarantäne Benachrichtigung per E-Mail



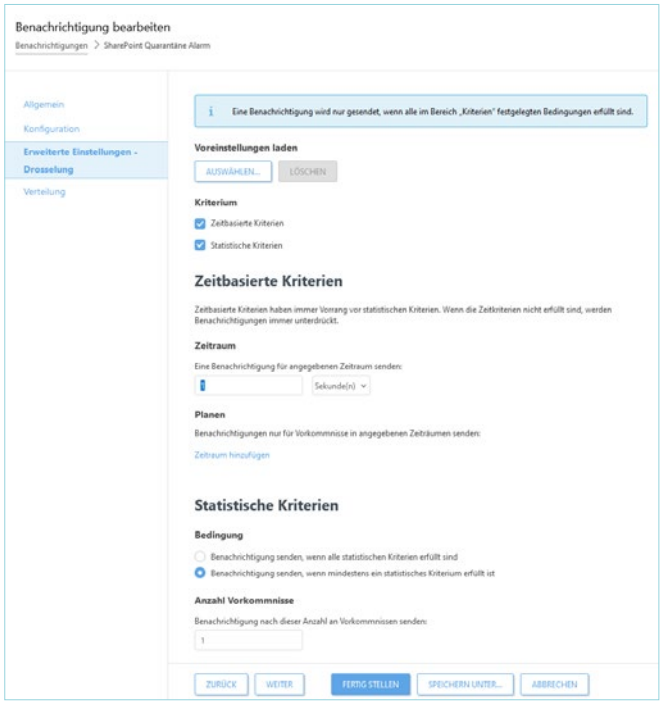

Im Anschluss erstellen wir eine neue Benachrichtigung namens *SharePoint Quarantäne Alarm*.



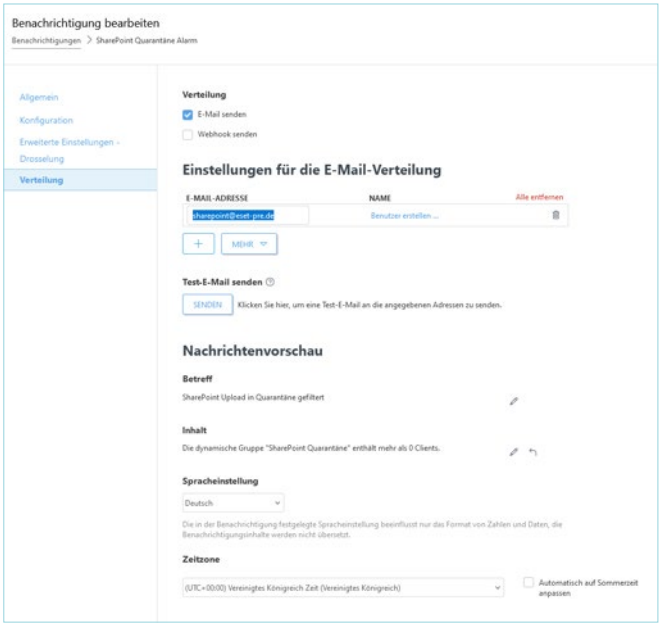



Das Ereignis wird bei Änderung der dynamischen Gruppe ausgelöst. In diesem Fall wählen wir die dynamische Gruppe *SharePoint Quarantäne* aus.

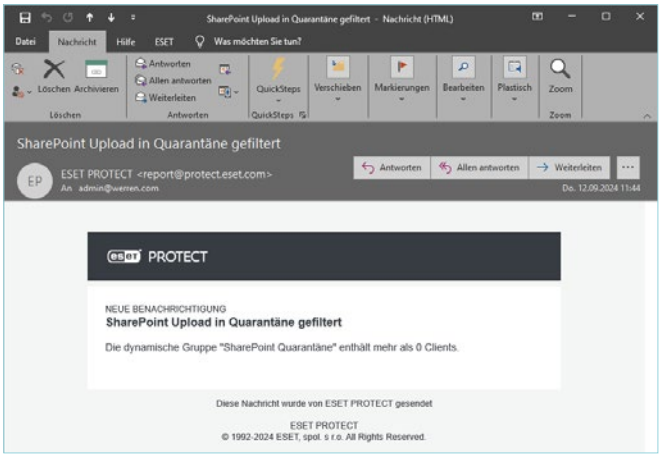
Bei den Bedingungen ist der Wert 0 als Gruppengröße maßgebend.




Damit die Quarantäne-E-Mail sofort verschickt wird, definieren wir beim zeitbasierten Kriterium den Wert von 1 Sekunde. Als statistisches Kriterium wird für die Anzahl Vorkommnisse der Wert 1 definiert. Dadurch wird nach einer Sekunde bei jedem Hochladen eines Objektes in die Quarantäne direkt eine E-Mail verschickt. Diese Parameter können an den Kundenbedarf jederzeit angepasst werden.

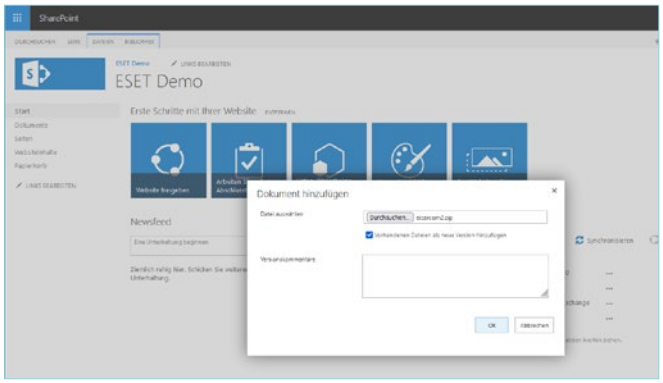



Im letzten Schritt geben wir noch die Empfänger E-Mail-Adresse an. Hier können einzelne Adressen oder auch Gruppenadressen hinzugefügt werden. Damit der Empfänger sofort weiß, worum es in der E-Mail geht, legen wir den Betreff auf *SharePoint Upload in Quarantäne gefiltert* fest. Die Sprache der E-Mail kann ebenfalls an den Kunden angepasst werden z. B. Englisch.

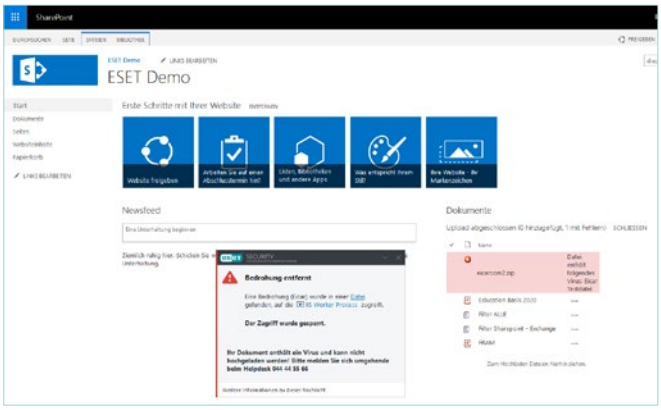


# ESET SharePoint Demo –
# **Hochladen von nicht erlaubtem Inhalt**

In der Demo versuchen wir, den Test-Virus Eicar auf den SharePoint hochzuladen.




Dazu wählen wir die Datei mit Malware-Inhalt aus.




Der SharePoint Server fängt die Datei ab und schiebt sie direkt in die Quarantäne. Gleichzeitig wird eine Warnung angezeigt und im Hintergrund eine E-Mail verschickt.

Digital Security
Progress. Protected.

# Über **ESET**

Als europäischer Hersteller mit mehr als 30 Jahren Erfahrung bietet ESET ein breites Portfolio an Sicherheitslösungen für jede Organisationsgröße. Wir schützen betriebssystemübergreifend sämtliche Endpoints und Server mit einer vielfach ausgezeichneten mehrschichtigen Technologie und halten Ihre Infrastruktur mithilfe von Cloud Sandboxing frei von Zero-Day-Bedrohungen. Mittels Multi-Faktor-Authentifizierung und zertifizierter Verschlüsselungslösungen unterstützen wir Sie bei der Umsetzung von Datenschutzbestimmungen sowie Compliance-Maßnahmen.

Unsere Endpoint Detection and Response-Lösung, dedizierte Services wie z.B. Managed Detection and Response und Frühwarnsysteme in Form von Threat Intelligence ergänzen das Angebot im Hinblick auf Incident Management sowie den Schutz vor gezielter Cyberkriminalität und APTs. Dabei setzt ESET nicht allein auf modernste KI-Technologie, sondern kombiniert Erkenntnisse aus der cloudbasierten Reputationsdatenbank ESET LiveGrid® mit Machine Learning und menschlicher Expertise, um Ihnen den besten Schutz zu gewährleisten

## 3 VON ÜBER 400.000 ZUFRIEDENEN KUNDEN

BVB 09 CHAMPION PARTNER

Seit 2019 ein starkes Team
auf dem Platz und digital

Allianz Suisse

Seit 2016 durch ESET geschützt
Mehr als 4.000 Postfächer

ISP Security Partner seit 2008
2 Millionen Kunden

## BEWÄHRT

Secur|Ty made in EU
Trust Seal www.teletrust.de/itsmie

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

ISO 9001 SGS · ISO/IEC 27001 SGS

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

## KONTAKT

Bei Rückfragen können sich ESET Partner
an die Partnerbetreuung wenden.

Tel: +49 (0) 3641 / 31 14 - 170 (Mo - Fr 8 - 17 Uhr)
E-Mail: partner@eset.de

welivesecurity by ESET

Digital Security Guide

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