

1 Phil

Anleitung: ESET SHAREPOINT POC



ESET.DE | ESET.AT | ESET.CH



ESET.DE | ESET.AT | ESET.CH

Inhaltsverzeichnis

Beschreibung des SharePoint PoC2
Installation der Sicherheitslösung für die SharePoint Datenbank 2
Konfiguration in ESET PROTECT oder im lokalen ESET SharePoint GUI
Erklärung der wichtigsten Einstellungenim ESET SharePoint GUI6
Clustermodus – für die Policy Synchronisation9
ESET Shell10
ESET SharePoint Taskplaner10
ESET SharePoint Quarantäne12
Konfiguration der SharePoint Policy im ESET PROTECT14
SharePoint Quarantäne Bericht16
SharePoint QuarantäneBenachrichtigung per E-Mail einrichten
ESET SharePoint Demo – Hochladen von nicht erlaubtem Inhalt

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:



Allgemein	
Produkteinrichtung	
ferteilung	Windows macOS Linux
	Verteilung
	Installationsprogramm herunterladen oder ESET Remote Deployment Tool verwenden
	Agent zuerst bereitstellen (Installationsskrict für Agenten)
	Bereitstellung mit GPO oder SCCM
	Komponenten
	Management Agent
	Sicherheitsprodukt
	Laufwerksverschlüsselung
	ESET INSPECT Connector
	Produktverbesserungsprogramm
	Teilnahme am Produktverbesserungsprogramm ③
	Übergeordnete Gruppe
	Auswählen oder Erstellen
	Server-Hostname (optional) ③
	ESMC.pre.local
	Port
	2222
	Peerzertifikat
	Eser PROTECT Zentrifikat
	Benutzerdelmiertes Zertifikat
	 ESET PROTECT Zertifikat
	Beschreibung Serversentifikät, Aussteller (No. Server-Settatraungsstelle, On ISET Schweiz, Betreff, CNA Agent 4: "On ISET Schweiz, Produkt Agent, Golding ab Tare Jul 14 2003, Gulfag ab Tare Jul 14 2003,



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

Installationsprogramm erstellen Installationsprograme > ISIT Security for Microsoft SkerePoint Server					
Allgemein Produkteinrichtung	Wilklen Sie eine Zielplattform				
Verteilung	64 bit				
	Remotebereitstellung Laden Sie das Remote Deployment Soch heurter; mit dem Sie ein Installationsprogramm en masse in ihrem Netwerk verteilen können. Visittige processioneen				

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.

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

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

ESET Remote Deployment Tool	Distribution option	×
REMOTE DEPLOYMENT TOOL • Source selection Computer selection Configuration	Select one of the options to distribute installer package. Select the source to be used: Active Directory	
Deployment	Sener: Computers non-Active Lineculty. Scan network Scan your local network. Import list (crx.text) Import list the hostnames or IP Addresses.	
	Add computers manually Enter hostnames or IP addresses manually.	
	lack Net Cancel	

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.

ESET Security-Installation	×	
CESET SECURITY FOR MICROSOFT SHAREPOINT SERVER	Willkommen beim Setup-Assistent von ESET Security Der Setup-Assistent wird ESET Security auf Ihrem Computer	
	installieren. Klicken Sie auf "Weiter", um fortzufahren, oder auf "Abbrechen", um den Setup-Assistent zu beenden.	
	Sie müssen andere residente Sicherheitsanwendungen wie Viren- und Spyware-Schutzprogramme und Firewalls unbedingt deinstallieren, bevor Sie die Installation fortsetzen. Anderenfalls können schwerwiegende Probleme auftreten.	
Progress. Protected.	Sprache:	
	English V	
11.0.15004.0	< Zurück Weiter > Abbrechen	

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

ESET Security-Installatio	n	×
Einrichtungsart Wählen Sie die für Sie ge	eignete Einrichtungsart	езет
○ Vollständig	Alle Programmfunktionen werden installiert.	
Benutzerdefiniert	Wählen Sie die zu installierenden Programmfunktioner Empfohlen für fortgeschrittene Benutzer.	1 aus.



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.

Wählen Sie die zu installierenden Produktkomponenten aus			GELOT
Benutzerdefinierte Installatio	n		Gene
(Erforderliche Ko	omponenten)		
X - Echtzeit-Dateisc	hutz		
Netzwerk-Schut	z		
Geralestederun	а		
)iese Komponenten müssen imm	ner installiert werden.		
Diese Komponenten müssen imm	ner installiert werden.		
Diese Komponenten müssen imm	ner installiert werden.		

Deaktivieren Sie folgende Komponenten:

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

Danach klicken Sie auf Weiter

eser
en". Wenn Sie einen anderen dran Sie auf "Durchauchen"
Durchsuchen
Durchsuchen
Durchsuchen
Durchsuche <u>n</u> Durchsuche <u>n</u>

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 Share-Point Policy auf sämtliche SharePoint Server.

Lokales ESET-SharePoint GUI:

Möchte der Kunde kein zentrales Management einsetzen, kann die Policy auch lokal im ESET Share-Point 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.

CELT SECURITY					
08 Überwachung	🗸 Sie sind				
	Laure et				
	Module sind au Letztes Update: 11.	1 dem neuesten Stand .09.2024 12:44:26			
	Infiziert: 0	Dateisystemschutz			
	Gesäubert: 0 Sauber: 18.82	84			
Hilfe und Support	Gesamt: 18.82	54			
	Produktversion	11.0.15004.0			
	System	SHAREPOINT.preJocal Windows Server 2019 Standard 64-bit (10.0.17763)			
	Computer Batrichtzeit der Senerr	Intel(R) Xeon(R) Gold 5218R CPU @ 2.10GHz (2100 MHz), 32768 MB RA	м		

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 Share-Point 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.

	Log-Dateien				18	٥
Log-dateien	Erkennungen (47)	v				
	Erkennungen		Erkennung	Aktion	Senu	Inform
	Ereignisse	y/eicar.com	Eicar Testdatei	beibe	PRELA	Ein Er
	Computer-Scan	st\AppData\Local\Tem.	Eicar Testdatei	bebe	PRE\A_	Ereig
	Verschickte Dateien	:E\AppData\Local\Tem.	Eicar Testdatei	beibe	PRE\a	Ereigr
	Gesperrte Dateien	PRE\AppData\Local\T.	. Eicar Testdatei	beibe	PREVA	Ereign
	Obamohan	3/eicar.com	Eicar Testdatei	bebe	PRE\a_	Ein Er
	oberprotong	E\AppOata\Local\Tem.	Excar Testdater	bebe	PREAL	Ereig
	HPS	ExppData(Local)Tem.	Eicar Testdatei	beibe	PREVA.	Ereig
	Browserschutz	Meicar com	Eicar Testidatei	helte	PREVA	Ein Fr
	Netzwerkschutz	E\AppData\Local\Tem.	Eicar Testdatei	bebe	PREVA	Ereig
	Gefilterte Websites	PRE\AppData\Local\T.	Eicar Testdatei	beibe	PRELA	Ereig
	Medienkontrolle	g/eicar.com	Eicar Testdatei	beibe	PRE\a.	Ein Er
	On Demand Dateshark Scan	#\AppData\Local\Tem.	Eicar Testdatei	beibe	PREVA	Ereig
	CIPOEnano-Davendaric scari	PRE\AppData\Local\T.	Eicar Testdatei	bebe	PRE\a_	Ereig
	23.07.2024 09:00:49 H., D., https://	secure.eicar.org/eicar.com	Eicar Testdatei	bebe	PREVA	En Er
	23.07.2024 08:07:20 E. D. ChUsen	s/ADMINI-1.PRE\AppData\Local\Tem.	Eicar Testdatei	bebe	PRE\a_	Ereig
	18.07.2024 07:28:41 E. D. Californi	chDhilble 1 PPE (appliately ocal Tem.	Eicar Testdatei	bebe.	PRE A	Ereig
	16.07.2024 07:28:41	sadministrator PRE\appData\Local\T	Eicar Testdatei	bebe	PREVA	Ereice

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

	Log-Dateien				18	0
Log-dateien	Erkennungen (47)	Ŷ				
	Zeit	S., O. Objekt	Erkennung	Aktion	Benu	Inform
	05.09.2024 10:57:32	H., D., https://secure.eicar.org/eicar.com	Eicar Testdatei	bebe	PRE\a_	Ein Ere
	20.08.2024 07:31:45	E., D., C:\Users\ADMINI=1.PRE\AppData\Local\Tem	Eicar Testdatei	bebe	PRE\A_	Ereign
	20.08.2024 07:31:45	E., D., C\Users\ADMINI~1.PRE\AppData\Local\Tem	Eicar Testdatei	beibe	PRE\a_	Ereign
Einstellungen	20.08.2024 07:31:45	E., D., C:\Users\administrator.PRE\AppData\Local\T.,	Eicar Testdatei	bebe	PRE\a_	Ereigr
	20.08.2024 07:31:45	H., D., https://secure.eicar.org/eicar.com	Eicar Testdatei	bebe	PRE\a_	Ein Er
	30.07.2024 15:33:45	E., D., C:\Users\ADMINI-1.PRE\AppData\Local\Tem	Eicar Testdatei	bebe	PRE\A_	Ereigr
	24.07.2024 06:19:39	E., D., C:\Users\ADMINI=1.PRE\AppData\Local\Tem	Eicar Testdatei	bebe	PRE\a_	Ereign
	24.07.2024 06:19:18	E., D., C\Users\ADMINI~1.PRE\AppData\Local\Tem	Eicar Testdatei	beibe	PREVA	Ereign
	24.07.2024 06:19:18	H., D., https://secure.eicar.org/eicar.com	Eicar Testdatei	bebe	PRELA	Ein Er
	23.07.2024 10:08:07	E., D., C:\Users\ADMINI=1.PRE\AppData\Local\Tem	Eicar Testdatei	bebe	PRE\a_	Ereign
	23.07.2024 10:08:07	E., D., C:\Users\administrator.PRE\AppData\Local\T.,	Eicar Testdatei	bebe	PRE\a_	Ereigr
	23.07.2024 10:08:07	H., D., https://secure.eicar.org/eicar.com	Eicar Testdatei	bebe	PRE\a.	Ein Er
	23.07.2024 09:00:49	E., D., C:\Users\ADMINI=1.PRE\AppData\Local\Tem	Eicar Testdatei	beibe	PRE\A_	Ereigr
	23.07.2024 09:00:49	E., D., C:\Users\administrator.PRE\AppData\Local\T.,	Eicar Testdatei	beibe	PRE\a.	Ereigr
	23.07.2024 09:00:49	H., D., https://secure.eicar.org/eicar.com	Eicar Testdatei	beibe	PREVAL	Ein Er
	23.07.2024 08:07:20	E., D., C:\Users\ADMINI~1.PRE\AppData\Local\Tem	Eicar Testdatei	bebe	PRE\a_	Ereign
	18.07.2024 10:47:22	E., D., C:\Users\ADMINI-1.PRE\AppData\Local\Tem	Eicar Testdatei	bebe	PRE\a_	Ereign
	18.07.2024 07:28:41	E., D., C:\Users\ADMINI~1.PRE\AppData\Local\Tem	Eicar Testdatei	bebe	PRE\a_	Ereign
	18.07.2024 07:28:41	E., D., C:\Users\administrator.PRE\AppData\Local\T.,	Eicar Testdatei	beibe	PRELA	Ereign

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

	CSCI SECURITY -	×	= O
Log-dateien	Log-Filter	?	
	Suchen nach:		Aktion Benu. Inform
	In Eastern	te te	i bebe PRE\a Ein Ere i bebe PRE\a Ereigni
Cinctellungen	Zeit: Scanner; Objekttyp; Objekt; Erkennung; Aktion: Benutzer; Information; Hash: Zuerst h	~ 10	i beibe PRE\a Ereigni
• Einsteilungen	Entraostvoen:	te	i beibe PREVA Ein Ere
	Diagnosedater; Informationer; Warnunger; Fehler; Kritisch	~ te	beibe PRE\a Ereigni
	Zeitraum:	te	i bebe PRE\a Ereigni
Fille und Support	Nicht angegeben	v te	i beibe PRE\a Ein Ere
	Mann Indonation Indonesia	te	beibe PRE\a Ereign
	Re- Discourse - Transmit	te	i beibe PRE\a Ereign
	Surhontingen	- te	i beibe PRE\a Ereign
	Nur ganze Wörter	te	beibe PRE\a Ereign
	Gro8-/Kleinschreibung beachten	te	i bebe PRE\a Ein Ere
	1	te	i beibe PRE\a Ereign
		te	beibe PRE\a Ereign
			beibe., PRE\a., Ereion
	Standard OK Schließen		

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

CSCT SECURITY	0	n x
	Prüfung	?
Log-dateien Q Prüfung	StatePoint-Datenbank-Scan Scan der Microsoft StatePoint- tinhätstatebank	
C Update	C Scannen Sie Ihren Computer Alle Islaken Dietritzger scannen auf Beruftzerfährer Scannen die Beruftzerfährer aus Wahlen Sie Scan-Zeite, Sauberungsstufe und Beruftzer Barameter aus	
 Einstellungen Tools 	Wechselmedien-Scan Scanen von USE-Geraten, DVDs, CDs und wechselmedien Construction Constructin Construction Constructin Const	
Ø Hilfe und Support		
	Ziehen Sie Dateien mit der Maus hierher, um sie zu prüfen	
Progress. Protected.		

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

8



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.

~	SharePoint-Datenbank-Scan Prüfung abgeschlossen.	11.09.2024 13:12:42
	Gefundene Ereignisse: 0 Verwendete Erkennungsroutine: 29871 (20240911)	Verwerfen
	Log anzeigen	

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

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



ESCT SECURITY		0 - ¤ ×
DB Oberwachung	Einstellungen	?
 Log-dateien Prüfung 	Server	>
C Update	Computer Alle benötigten Computer-Schutzfunktionen sind aktiv.	>
Einstellungen Tools	Netzwerk Alle benötigten Netzwerkschutzfunktionen sind aktiv.	>
Ø Hilfe und Support	Web und E-Mail Alle benötigten internet-Schutzfunktionen sind aktiv.	>
	D Tools	>
Progress. Protected.	14 Import-/Exporteinstellungen 🗘 I	irweiterte Einstellungen

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.

Select nodes		?
Machine to add to the list of cluster nodes		Add
Cluster nodes		<u>R</u> emove
ESFW_NODE1 ESFW_NODE2 ESFW_NODE3		Remove al <u>l</u> Autodetect
		<u>B</u> rowse L <u>o</u> ad
	Next	Çancel

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:

C:\Program Fil	es\ESET\ESET Secur	ity\eShell.exe					-	0	×
Haximaler Schu	utz								^
Gültigkeit der Letztes erfolg	r Lizenz: 22 greiches Upda	.01.2025 te: 11.09.2024 12							Ľ
Automatische / HTPS: Exploit-Block Lansomware-Sci Echtzeit-Date Medienkontroll Ifrewall: Netzwerkisolli Ustnet-Erkenn Netzwerkisoli Chtzeit-Schu Präsentations (SiI-Cluster: E-Mail-Cluster: Bhishing-Schutz; Phishing-Schutz;	Ausschlüsse: eicherprüfung er: hutz: ischutz: le: erung: ung: ung: ffsschutz (ID tz für ShareP modus: ing: -Schutz: tz: Über RA-Rich	: S): Sint: tlinie verwaltet			Aktiviert Aktiviert Aktiviert Aktiviert Deaktiviert Deaktiviert Deaktiviert Aktiviert Aktiviert Aktiviert Aktiviert Aktiviert Aktiviert Aktiviert Aktiviert				
ABOUT NOTIFICATIONS STATUS	COMPUTER PASSWORD TOOLS	CONNECTIVITY RUN UI	DEVICE SCHEDULER UPDATE	GUIDE SERVER VIRLOG	LICENSE SETTINGS WARNLOG	NETWORK SIGN WEB-AND-EMAIL			
Shells_									~

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

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

ESET SharePoint Taskplaner

SECURITY				0 - 0	×
08 Oberwachung	 Taskplaner 			18	?
🕼 Log-dateien	Task	Trigger	Nächste Ausführung	Letzte Ausführung	
Q Prüfung 🕦	✓ Log-Wartung Log-Wartung	Task wird täglich um 0	12.09.2024 02:00:00	11.09.2024 02:00:39	
C. Hodata	Update Automatische Updates in festen Zeitabständ	Task wird regelmäßig	11.09.2024 13:44:22	11.09.2024 13:14:22	
	Update Automatische Updates beim Anmelden des	Benutzeranmeldung (h	Bei Ereignis		
② Einstellungen	Prüfung der Systemstartdateien Prüfung Systemstartdateien	Benutzeranmeldung Ta	Bei Ereignis	11.09.2024 11:21:10	
💼 Tools	Prüfung der Systemstartdateien	Erfolgreiches Modulu	Bei Ereignis	11.09.2024 12:44:29	
⑦ Hilfe und Support	Regelmäßiger Datenbank-Scan SharePoint ESET D8 prüfen	Task wird täglich um 0	12.09.2024 06:00:00	11.09.2024 06:00:39	
Progress, Protected.	Task hinzufügen	Section	Standard		

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

	 Taskplaner 			18
	CELT SECURITY		σ×	Letzte Ausführung
	Taskdetails		?	11.09.2024 02:00:39
🕽 Update	Taskname	Demo SharePoint DB Scan		11.09.2024 13:14:22
	Tasktyp	Regelmäßiger Datenbank-Scan	5	11.02.2024 11.21.10
🗂 Tools	Aktiviert			11.09.2024 12:44:29
				11.09.2024 06:00:39
		Zarijeck Wester Ab	brechen	

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.



	Triana.	×
Taskausführung		1
Taskausfuhrung planen	 Einmalig Wiederholt Täglich Wöchentlich Bei Ereignis 	
Task im Akkubetrieb überspringen		

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



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



Der Task soll zur nächsten geplanten Ausführungszeit ausgeführt werden.



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

CESCI SECURITY) - 0	
08 Überwachung	 Quarantă 	ne		12	?
🗊 Log-dateien	Zeit	Objektname	Gr	Grund	Ar
Q Prüfung 0	09.07.2024 13:58:17 09.07.2024 13:50:24	PasswortZIP.7z eicarcom2.zip	800, 308 8	Regel "Archive . Eicar Testdatei	
🗘 Update					
Einstellungen					
🛱 Tools					
② Hilfe und Support					
Progress. Protected.	In Quarantine v	verschieben			

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

Einfach	->	Name	
Einstellungen		SharePoint Quarantäne wiederherstellen	
Zusammenfassung		Tags Tags auswählen Beschreibung	
		Aufgabenkategorie	
		Alle Aufgaben	
		Task	
		Quarantäneverwaltung	

Einfach	Quarantäne-Verwaltungseinstellung	gen
Einstellungen	Aktion	
Zusammenfassung	Objekt(e) wiederherstellen	
	Filtertyp 💿	
	Aufgetreten	
	Filtereinstellungen Aufgetreten aus	
	2021 Juni 2 00:00:00	

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.

iltertyp 💿	
Aufgetreten	~
Hash-Elemente	
Aufgetreten	
Größe	
Ereignisname	
Objektname	

Einfach	Quarantäne-Verwaltungseinstellungen	
Einstellungen	Aktion	
Zusammenfassung	Objekt(e) wiederherstellen	~
	Filtertyp ③	
	Aufgetreten	~
	Filtereinstellungen	
	Aufgetreten aus	
	2021 Juni 2 00:00:00	
	Aufgetreten in	
	2021 Juni 2 08:00:01	

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.

P Suchen	1SLT Dome					
Start	ED	ESET Demo				
Dokumente Seiten	Papieri	korb leeren				
Websiteinhalte	Papier	korb				
Papierkorb	rapier	NOT D				
Bearbeiten	D	Name	Gelöscht am 1	Gelescht von	Erstellt von	Gegenungspirt
		FisDuta71	92.06.2021 07.33	Systemikoets	Systemicanto	websites/east/Triegegebene Dokumente
		teraim.zip	02.06-2021 07.33	Symerikanta	Synemiceto	websites/koel/Finigegebene Dokumente

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

,O Suchen	15ET Demo				
Start	ED ESET Demo				
Seiten	🔋 Löschen 为 Wiederherstellen				
Websiteinhalte	Panierkorb				
Papierkorb	ropicitoro				
Ø Bearbeiten	🗢 🗋 Name	Geldscht am 1	Geldocht von	Entellt von	Unprungsont
	🗢 🗐 FisData.7z	02.06.2021 07.33	Systemicanto	Systemianta	websites/eset/Freigegebene Dokumente
	😑 💷 ransim.zip	02.06.2021 07:33	Systemiconte	Systemicanto	websites/eset/Freigegebene Dokumente

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

-	SharePoint					
,Q s	uchen	ESET Demo				
Sta	rt	ED	ESET Demo			
Do	kumente					
Sei	ten	+ Neu ~	🕆 🛉 Hochladen 🗸 🎧 Synchronisieren	Nach Excel exportien	en ···	
We Pag	ibsiteinhalte pierkorb	Dokun	nente			
Ø Bei	arbeiten	D	Name 🗸	Geindert 🗸	Geändert von 😔	+ Spalte hinzufi;
		8	Education Basis 2020.pdf	15.10.2020	Systemkonto	
		10	³⁷ FisData.7z	Vor ungefähr einer Stunde	Systemkonto	
		8	FRAM.pdf	5. Februar	Systemkonto	
		uff.	³⁰ ransim.zip	Vor ungefähr einer Stunde	Systemkonto	

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.

ET Security for Microsoft Shar	ePoint Server (V6+)	Q. Zu inchander Typ	
SERVER		ALLGIMEIN	() 27# 💷 O I	• +
Zugiffifite	O	SHAREPOINT-INTEGRATION		
On-Demand-Datenbank-Scan	0	🔾 🛢 🕂 Direktzugriff auf SQL-Datenbank		0
Regeln	0	LEISTUNGSINDIKATOREN	(0 a z a) (1 a sorrer 2008) O 4	• +
IMPUTER	6	-		
PDATE				
T2WERKZUGR/FFSSCHUTZ				
B UND E-MAIL				
DENKONTROLLE				
0015	Ø			
ERBINDUNG				
ENUTZEROBERFLÄCHE	•			
ENACHRICHTIGUNGEN	0			
OVERRIDE-MODUS	0			

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

ET Security for Microsoft Sha	rePoint Ser	ver (V6+)	🕽 Zu suchender Typ				
SERVER	Ø	ALLGEMEN		0		+	
Zugriffsfilter	•	O ⊕ ≠ Zugriffsfilter aktivieren					
On-Demand-Datenbank-Scan	O	SHAREPOINT-SCHUTZEINSTELLUNGEN				+	
Regela	Ø	Die unten angezeigten Sharefoint-Servenchutzeinstellungen könn	en auch in der SharePoint-Zi	induladmi	nistutio		
COMPUTER	ø	serwaltat werden. Die her vorgenommenen Anderungen werden u SharePoint angezeigt.	ster Umständen erst nach ei	Jügen Seks	umden im		
IPDATE		🔾 🔍 🔄 Dokumente beim Hochladen scannen					
NETZWERKZUGRIFFSSCHUTZ		🖸 🔍 🕆 Dokumente beim Herunterladen scannen					
AFR UND F-MAIL		🖸 🔍 🕈 Zulassen, dass Benutzer infizierte Dokumente herunterladen					0
and the second s		🔾 🐵 🕂 Versuchen, infizierte Dokumente zu slubern					
AEDIENKON KOLLE		O ⊕ ÷ Zeitüberschreitung (Sek.)	300			0	
DOLS	Ø	O @ + Anzahl der Scanthreads	5			6	
VERBINDUNG	Ø	_					
BENUTZEROBERFLÄCHE	0	VIREN- UND SPYWARE-SCHUTZ			0.	*	

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

T Security for Microsoft Share	ePoint Sen	er (V6+) 0.	, Zuzuchender Typ
ERVER	Ø	ALIGEMEIN	• • • • •
Zugriffshiter	0	🔿 💿 🗲 im schreibgeschützten Modus scannen	
On Demand-Datenbank Scan	0	O Ø Ø Dokumentversionen scannen	
COMPUTER	0		
PDATE		○ ● ÷ Zuletzt geändert	Alle im letzten 3 Monaten geänderten 👻
ET2WERK2UGRIFFSSCHUTZ		O @ + Anzahl paralleler Downloads	5 (0)
VEB UND E-MAIL		© ⊕ + Scan beenden, wenn die 4usfihrung zu lang (@≥ 10.0	
/EDIENKONTROLLE		O	240
0015	0	VIEN. IND SPYWARE-SCHUTZ	
ERBINDUNG		MINEN OND SPTWARE SCHOIL	

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.

ET Security for Microsoft Shar	ePoint Serve	r (V6+)	Q Zu suchender Typ		3
SERVER	0	REGELN			
Zugnitsfilter	•	ZUGRIFFSFILTER			
On-Demand-Datenbank-Scan		🔿 🖷 🖗 Regeln	Bearbeiten & Instan	• DErsetzen	
Regela	0				
COMPUTER	Ø	ON-DEMAND-DATENBANK-SCAN			
UPDATE		🖸 🗧 🕈 Regeln	Bearbeiten 🖧 Instan	• 🗆 Ernetzen	•
NETZWERKZUGRIFFSSCHUTZ					

Die Regeln umfassen:

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

Aktiv	Name	Stufe	Treffer 🧕
2	*.php hochladen blockieren	Filterung	0
	°.txt hochladen blockieren	Dateiverarbeitung	0
	*.exe hochladen blockieren	Dateiverarbeitung	0
2	Weitere Regeln für Weboberflächendateien überspringen	Dateiverarbeitung	0
	Ausführbare Dateien nicht zulassen	Dateiverarbeitung	0
Hinzu	tügen Dearbeiten Lintterner Kopieren i loch	Runter	

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

Weitere Regeln für Weboberflächendateien überspringen Dateiverarbeitung Ausführbare Dateien nicht zulassen Dateiverarbeitung ZIP mit Passwort Verarbeitung von Erg	Weitere Regeln für Weboberflächendateien überspringen		
Ausführbare Dateien nicht zulassen Dateiverarbeitung ZIP mit Passwort Verarbeitung von Erg	the second	Dateiverarbeitung	0
ZIP mit Passwort Verarbeitung von Erg	Ausführbare Dateien nicht zulassen	Dateiverarbeitung	0
	ZIP mit Passwort	Verarbeitung von Ergebnissen	0

Die Regel ZIP Passwort kann aktiviert und deaktiviert werden.

1	Aktiv		D	
	Name	ZI	P mit Passwort	0
	Bedingungstyp	Operation	Parameter	
	Enthält passwortgeschütztes	Archiv ist	Wahr	
	Hinzufügen Bearbeiten I	Loschen	È] A] V]	Ŧ
	Hinzufügen Bearbeiten Aktionstyp	Loschen Parameter	2 A [V [¥
tire	Hinzufugen Bearbeiten Aktionstyp Datei in Quarantäne verschiel	Parameter	È 🔺 🔽	÷
fin	Hinzufugen Bearbeiten Aktionstyp Datei in Quarantäne verschiel	Parameter ben	È 🔺 🛛 🔻 🗌	×
firm	Hinzufugen Bearbeiten Aktionstyp Datei in Quarantäne verschiel	Parameter ben	È [▲] ▼ [¥

Eine Regel umfasst immer einen Bedingungstypen und einen Aktionstypen:

Bedingungstyp: Worauf sich die Regel bezieht

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

SET Security for Microsoft	SharePoint Serv	ver (V6+)	Q Zu suchender lyp	
SERVER	0	E ZUTTENSTER	(€≥7.0) 0 ● \$	
COMPUTER	•	B MICROSOFT WINDOWS * UPDATE	0	
UPDATE		EST CMD	()>43 () 0 • f	
NETZWERKZUGRIFFSSCHUT	TZ	O • • Erweiterte ECMD-Befehle aktivieren		0
WEB UND E-MAIL		Autorisierungsmethode	Passwort fär erweiterte Einstellungen 🗢	
MEDIENKONTROLLE				

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.

T Security for Microsoft Shar	rePoint Sen	ver (V6+)	Q Zusuchender Typ.,		
SERVER	ø	E ZUTFENSTER	(#) 2 T.O	0.,	
OMPUTER.	ø	MICROSOFT WINDOWS # UPDATE		0	
PDATE		ESET CMD	(245) (D	0	
ETZWERKZUGRIFFSSCHUTZ		ESET RNM	(H) 2 7.0		
AEDIENKONTROLLE		1121NZ	(B + 7.1)	0	
DOLS	0	WMI-ANDIETER		0	0
Taskplaner Log-Dateien		SCAN-ZIELE FÜR DIE ESET MANAGEMENT-KONSOLE	0	0	0
Präsentationsmodus		○ ● ∮ Liste der Zele generieren			0
Diagnose		🔿 🌒 🖈 Aktualisierungsirtervall [Minuten]	360	0	0

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.

ET Security for Microsoft Sh	arePoint Ser	ver (V6+)	Q. Zu suchender Typ.,	1
SERVER	Ø	TASKPLANER		0 • +
COMPUTER	•	O 🛛 🕂 Taskplaner	Jearbeiten	
UPDATE				
NETZWERKZUGRIFFSSCHUTZ				
WEB UND E-MAIL				
MEDIENKONTROLLE				
TOOLS Taskplaner Log-Dateen	0			

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

Aktiviert	Name	Trigger	Task	Letzte Ausführung	0
	Zeitabständen	Minuten ausgeführt.	Update		1
	Automatische Updates beim Anmelden des Benutzers	Benutzeranmeldung (höchstens einmal je/alle Stunde).	Update		
Ø	Prüfung Systemstartdateien	Benutzeranmeldung Task wird nicht ausgeführt, wenn der Computer im Akkubetrieb läuft.	Prüfung der Systemstartdateien		
Ø	Prüfung Systemstartdateien	Erfolgreiches Modulupdate (höchstens einmal jejalle Stunde). Task wird nicht ausgeführt, wenn der Computer im Aksubetrieb läuft.	Prüfung der Systemstartdateien		
	Automatischer erster Scan	Task wird einmalig am 1970 Jan 1 um 01:00:00 ausgeführt.	Erster Scan		
	Regelmaßiger Datenbank-Scan	Task wird an folgenden Tagen um 00:00:00 Uhr ausgeführt : Samstag	Regeimaßiger Datenbank-Scan		
•	Automatischer erster Scan Hegelmaßiger Datenbank-Scan	Task wird einmalig am 1970 Jan 1 um 01:00:00 ausgeführt. Task wird an folgenden Tagen um 00:00:00 Uhr ausgeführt : Samstag	Erster Scan Regeimaßiger Datenbank-Scan		

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

er security for Microsoft Shar	epoint Ser	ver (vo+)	d resonance when		
SERVER	0	PROXYSERVER			
COMPUTER	0	🔾 🔹 🕴 Proxyserver verwenden			0
UPDATE		🔿 🔿 🖗 Proxyserver	proxy pre-local		0
NETZWERKZUGRIFFSSCHUTZ		O @ + Port	3128	0	
WEB UND E-MAIL					
MEDIENKONTROLLE		O			0
TOOLS		O @ + Beeutzername			0
VERBINDUNG		O @ # Passwort	Passault anteinen		0
BENUTZEROBERFLÄCHE					
BENACHRICHTIGUNGEN	0	O @ + Direktverbindung verwenden, wenn der Proxy nicht			
OVERRIDE-MODUS	0				

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 Quarantänebericht 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*



 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!

Bericht-Template bearbei Berichte > Objekte in der SharePoin	iten t Quarantäne						
Algemein	Fil	tern i	hach				
Daten			Berichtsbereich - Berichtsbereich	s @deiner ode	r gleicl v	1000	8
Sortierung		AND .	Computer - Computername	enthalt	v	sharepoint	8
Filter Zusammerfassung	Ve	rscha	u				

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

CON PROTECT	Objekte in der SharePoint Quarantäne
Bericht: Objekte in der SharePoint Quarantäne	
Bratelit um 12. September 2004 10:34:43 (UTC - 10:00)	
Keine anzeigbaren Daten	

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.

Computer	1	0	~	0	🗀 SharePoint (1)	Tagi	▼ 12 🔽	Filter hinaufügen
Gruppen	Q					V ERWEITERT	E FILTER	
	^	N	ME			IP-ADRESSE	TAGS	STATUS
→ □ Domain_PRIE (7)		19	Ere.	212	shareount one local	192 168 10 70	CharaBrint	2
Desktop (2)			80 VV	1.0	and branchester of the		(search search	10.54
Domain Controllers (1)								
🛅 Exchange (1)								
Server (0)								
SharePoint (1)	۲							
C SharePoint Quarantâne								

- 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*.

Dynamisches Gruppen-Templates >	emplate bearbeiten Objekt in der SharePoint Qua	arantáne			
Aligemein Ausdruck	OPERATION	AND (samtliche Bedingur	ngen müssen erfüllt sein)	×	
		Quarantane . Größe	> (grdßer als) v	0	8
Zusammenfassung	Regel hinzufüg)en			

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

Quarantäne Benachrichtigung per E-Mail



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

llgemein	Name	
onfiguration	SharePoint Quarantăne Alarm	
rweiterte Einstellungen -	Beschreibung	
Prosselung		
erteilung		
	Tags	



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 O als Gruppengröße maßgebend.

Aligemein	1 Eine Benachrichtigung wird nur gezendet, wenn alle im Bereich "Kriterien" festgelegten Bedingungen erfüllt sin
invelterte Einstellungen -	Voreinstellungen laden
Prosselung	AUSWÄHLEN LÖSCHEN
erteilung	
	Kriterium
	Catitiche Kitzien
	Zeitbasierte Kriterien
	Zeitbasierte Kriterien haben immer Vorrang vor statistischen Kriterien. Wenn die Zeitkriterien nicht erfüllt sind, werden Benachrichtigungen immer unterdrückt.
	Zeitraum
	Eine Benachrichtigung für angegebenen Zeitraum senden:
	Sekunde(n) ~
	Planen
	Benachrichtigungen nur für Vorkommnisse in angegebenen Zeiträumen senden:
	Zeitreum hinzufügen
	Statistische Kriterien
	Bedingung
	Benachrichtigung senden, wenn alle statistischen Kriterien erfüllt sind
	Denachrichtigung senden, wenn mindestens ein statistisches Kriterium erfüllt ist
	Anzahl Vorkommnisse
	Benachrichtigung nach dieser Anzahl an Vorkommnissen senden:

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.

Algemein Konfiguration Erweiterte Einstellungen - Drosselung Verteilung	Vertailung Constant Sandan Vertailung Vertainak sandan Vertainak sandan Einstellungen für die E-Mail-Verteilung	
	E-MAIL-ADRESSE NAME	Alle entfernen
	sharepoint@eset.pre.de Benutzer enteilen	8
	Test-E-Mail senden () SINCHT Rücken Se hier, um eine Test-E-Mail an die angegebenen Adressen z	su senden.
	Test-E-Mail senden () stroctiv stroctiv Nachrichtenvorschau Bereff Suefeist (bjeled in Question gefitter	u senden.
	Test-E-Mail senden © stroctiv stroctiv Nachrichtenvorschau Bereff Suefeint Uplead in Gueentine gefitert Inhait	u sanden.
	Test-E-Mail senden () Stricter V Machrichtenvorschau Bereff SharePoint Uplead in Quanation gefittet . Ishait Die dynamische Gruppe "SharePoint Quanations" ershält mehr als O Clerets.	n sanden.
	Test-E-Mail senden (*) structury televan Ser hier, um eine Test-E-Mail an die angegebenen Adressen z Nachrichtenvorschau Betreff Starefosie Upload in Quesatäne gefitter: Inhait Die dynamische Gruppe "ShaniPeint Quaratäne" enthält mehr als O Clients. Spracheinstellung	u xanden.
	Test-E-Mail senden (*) Strötty Otkan Sichier, um eine Test-E-Mail an die angegebenen Adressen z Nachrichtenvorschau Betreff Starefolie Upload in Quesatäne gefitter: Inhait Die dynamische Gruppe "Sharefoliet Quaratäne" enthält mehr als O Clients. Spracheinstellung Deutsch	u worden.
	Test-E-Mail sender () Strotter Machrichtenvorschau Evert SharePoint Uploed in Quasartäne gefäret : Inhalt De dynamische Gruppe "SharePoint Quasartäne" enthält mehr als O Cleres. Specheinstellung Destis. Che dis Dataschöfungen fühigteligt förschämstellung beenfungt nur des Finned Breuchlichtigungeinhalte weden mehr die Generater.	tu sanden.
	Test-E-Mail sender (*) Strottry Ottom Schne, um eine Test-E-Mail an die angegebenen Adressen z Nachrichtenvorschau Bereff Buefolst Uplead in Quaretäne griftet Ishabt Die dynamische Gruppe "SharePoint Quaretäne" ershält mehr als O Clients. Spracheinstellung Deutsch Die die Bescheidungs bespheiste Spracheinstellung beenfunst nur dan Formet Benefungspracheke werden nicht überstellt. Zeitzone	tu sandan.

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.

realidesteps for	K	Antworten	4 Allen and	worten	→ Weiterleite Do. 12.0	2024 115
tcom>	•	Antworten	S Allen and	tworten	→ Weiterleite Do. 12.0	57 1 ···· 9.2024 1154
Lcom>	ï				Do. 12.0	9.2024 11:4
uarantäne ge	filtert					
arePoint Quaran	ntäne" enthä	It mehr als 0 C	lients.			
Nachricht wurde v	von ESET PRO	DTECT gesendel				
h	harePoint Quarar	harePoint Quarantâne" enthă se Nachricht wurde von ESET PRI	harePoint Quarantäne" enthält mehr als 0 C	harePoint Quarantäne* enthält mehr als 0 Clients.	harePoint Quarantane* enthält mehr als 0 Clients.	harePoint Quarantäne* enthält mehr als 0 Clients.

ESET SharePoint Demo – Hochladen von nicht erlaubtem Inhalt

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





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.

Dazu wählen wir die Datei mit Malware-Inhalt aus.



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



Seit 2019 ein starkes Team auf dem Platz und digital



Seit 2016 durch ESET geschützt Mehr als 4.000 Postfächer

BEWÄHRT



ISP Security Partner seit 2008 2 Millionen Kunden



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

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: <u>partner@eset.de</u>





ESET Digital Security Guide

ESET.DE | ESET.AT | ESET.CH

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