

Cyberhex Anleitung

Inhalt

Installation des Cyberhex Servers	2
Vorbereitende Arbeiten	2
Starten des Docker Containers.....	2
Erstkonfiguration des Servers über das Webinterface	2
Einloggen in Cyberhex	4
Übersicht über das Interface.....	5
Konfigurieren von Einstellungen	6
Profil Einstellungen	6
Server Einstellungen	6
Client Einstellungen.....	7
Datenbank Einstellungen	9
Verwalten von Clients	10
Clients Hinzufügen	10
Clients verwalten.....	10
Verwalten der Logs	11
Log ansehen	11
Log exportieren	11
Log Backups	12
Server Log	12
Incident Response.....	13
Incident erstellen.....	13
Incident verwalten.....	13

Installation des Cyberhex Servers

Vorbereitende Arbeiten

Für eine Reibungslose Installation des Cyberhex Servers sind einige Vorbereitungsarbeiten auszuführen. Diese Arbeiten beinhalten das Erstellen von SSL-Zertifikaten sowie einigen Ordner, welche der Server benötigt, um sicher zu arbeiten.

Folgende Schritte werden benötigt:

- Installieren Sie die benötigten Linux-Tools:
 - Git: [Wie installiere ich Git?](#)
 - Docker: [Wie installiere ich Docker?](#)
 - Docker-Compose: [Wie installiere ich Docker-Compose?](#)
- Klonen Sie das Cyberhex Repository:
 - Führen Sie «`git clone https://github.com/jakani24/ma`» aus, um das Repository zu klonen
- Erstellen Sie die benötigten Ordner und setzen die Berechtigungen
 - «`mkdir -p cyberhex_code/export`»
 - «`mkdir -p cyberhex_code/import`»
 - «`mkdir -p cyberhex_code/database_srv`»
 - «`chown cyberhex_code/export www-data:www-data`»
 - «`chown cyberhex_code/import www-data:www-data`»
 - «`chown cyberhex_code/database_srv www-data:www-data`»
- Besorgen Sie Sich SSL-Zertifikate und Kopieren dies in die richtigen Ordner
 - Falls Sie noch nicht über ein Zertifikat verfügen, können Sie [hier](#) eins erstellen.
 - Kopieren Sie die Zertifikate in den «certs» Ordner.
 - Wobei das Keyfile als «`privkey.pem`», und das Zertifikatfile als «`fullchain.pem`» gespeichert sein soll.
- Die vorbereitenden Arbeiten sind nun abgeschlossen. Sollte Sie Probleme haben bei einem dieser Schritte, melden Sie sich bitte bei info.jakach@gmail.com.

Starten des Docker Containers

Nachdem Sie alle vorbereitenden Aufgaben abgeschlossen haben, ist Ihre Installation bereit das erste Mal gestartet zu werden.

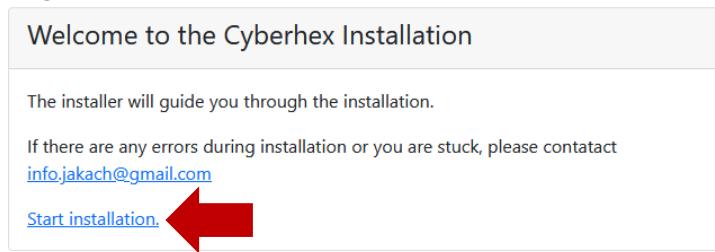
- Starten Sie den Docker Container mit folgendem Befehl: «`docker-compose up --build`».
- Dies startet den Server sowie den Datenbank Server.
- Warten Sie nun einige Minuten, während sich die Server initialisieren.

Erstkonfiguration des Servers über das Webinterface

Sie haben nun sowohl den Docker Container gestartet als auch einige Minuten gewartet, damit sich die Server initialisieren konnten. Nun können Sie damit starten, den Cyberhex Server zu konfigurieren.

- Öffnen Sie einen (modernen) Browser.
- Navigieren Sie zu «`<Server IP oder URL>/install/welcome.php`»
- Der Installer wird Sie durch das Setup führen.

- Wenn Ihre Installation bis jetzt erfolgreich verlief, werden Sie mit folgender Seite begrüßt.



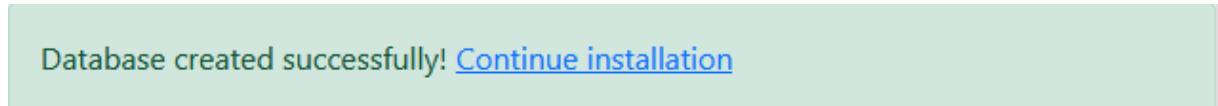
Welcome to the Cyberhex Installation

The installer will guide you through the installation.

If there are any errors during installation or you are stuck, please contact info.jakach@gmail.com

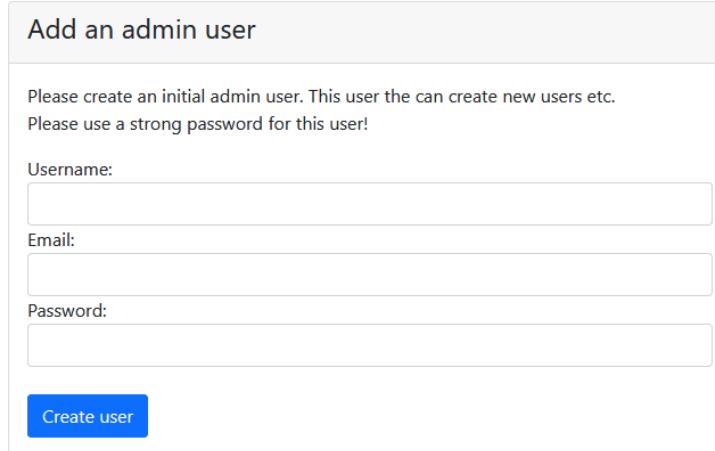
[Start installation.](#)

- Drücken Sie auf «Start installation»
- Im nächsten Fenster werden einige Grüne Meldungen angezeigt. Sollte eine dieser Meldungen Rot sein, melden Sie sich bitte bei info.jakach@gmail.com.
- Klicken Sie dann auf «Continue installation» ganz unten auf der Seite.



Database created successfully! [Continue installation](#)

- Auf der Nächsten Seite können Sie einen ersten Administrator Benutzer erstellen



Add an admin user

Please create an initial admin user. This user the can create new users etc.
Please use a strong password for this user!

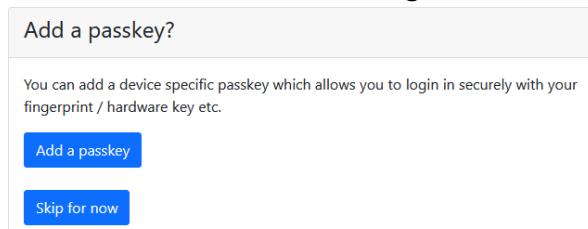
Username:

Email:

Password:

[Create user](#)

- Geben Sie hierzu unbedingt ein sehr starkes Passwort ein! Wenn ein Angreifer dieses Passwort herausfinden kann, kann er sämtlichen Schutz von Cyberhex umgehen.
- Drücken Sie anschliessend auf «Create user».
- Und dann auf «Continue installation».
- Im nächsten Fenster können Sie einen Passkey hinzufügen, mit dem Sie sich ohne Passwort verifizieren können. Dieser Passkey kann ein Hardware Passkey oder Ihre Windows Hello Authentifizierung sein.



Add a passkey?

You can add a device specific passkey which allows you to login in securely with your fingerprint / hardware key etc.

[Add a passkey](#)

[Skip for now](#)

- Sollten Sie dies nicht wollen, oder über kein Passkey fähiges Gerät verfügen, können Sie diesen Schritt auch überspringen, indem Sie auf «Skip for now» drücken.

- Sie haben die Installation nun abgeschlossen. Drücken Sie nun noch auf «Finish installation».

You have installed cyberhex! Thank you for choosing us!

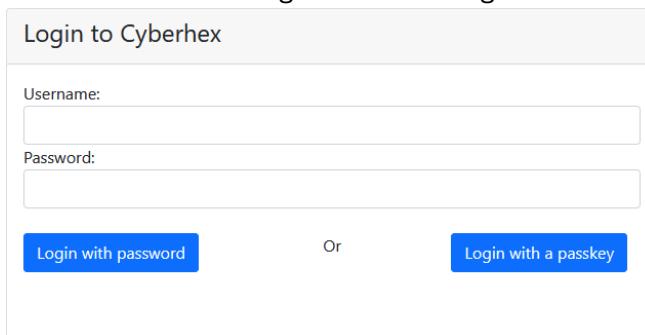
[Finish installation.](#)

- Sie werden nun auf die Anmeldemaske von Cyberhex geführt. Bitte lesen Sie nun den Abschnitt «Einloggen in Cyberhex», «Übersicht über das Interface» und «Konfigurieren von Einstellungen».

Einloggen in Cyberhex

Nachdem Sie einen (Administrator) Account erstellt haben, können Sie sich in Cyberhex einloggen. Vergewissern Sie sich, dass niemand Ihnen dabei zusehen kann, wenn Sie Ihr Passwort eingeben.

- Navigieren Sie in einem Browser zu der URL / IP-Adresse Ihres Cyberhex Servers.
- Sie werden mit der folgenden Seite begrüßt:



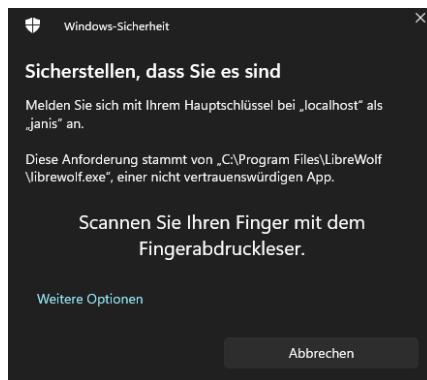
Login to Cyberhex

Username:

Password:

[Login with password](#) Or [Login with a passkey](#)

- Sollten Sie über einen Account verfügen, haben Sie nun zwei Möglichkeiten sich einzuloggen.
 - Mithilfe eines Passworts
 - Mithilfe eines Passkeys
- Sofern Sie «Login mit Passwort» nicht deaktiviert haben, können Sie Ihren Benutzernamen und Ihr Passwort eingeben und dann auf «Login with password» Drücken.
- Sollten Sie in Ihrem Account einen Passkey hinterlegt haben, und wollen sich auf diese Weise einloggen, befolge Sie bitte folgende Schritte:
 - Geben Sie Ihren Benutzernamen im Feld «Username» ein.
 - Drücken Sie auf «Login with a passkey»
 - Es wird ein Fenster ähnlich wie dieses angezeigt. Befolgen Sie die Anweisungen dieses Fensters.

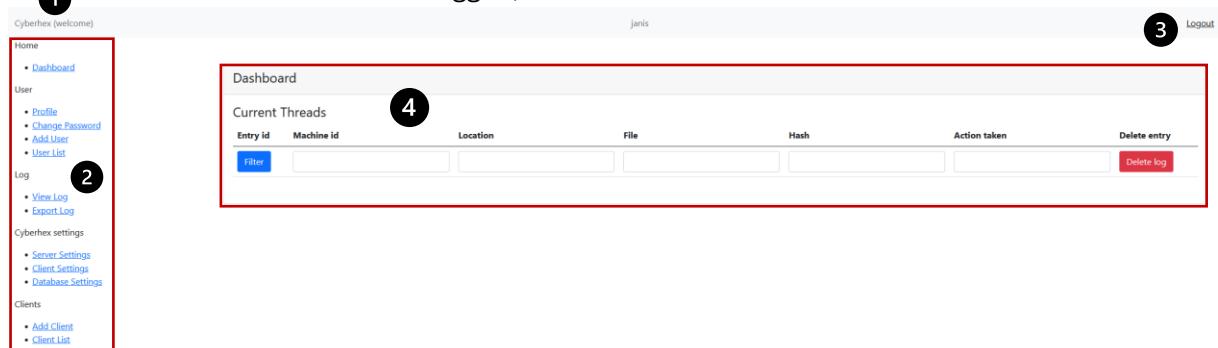


- Wenn Sie sich erfolgreich eingeloggt haben, werden Sie automatisch weitergeleitet.

Übersicht über das Interface

Das Interface des Cyberhex Servers ist so gestaltet, dass es Benutzern leicht fällt es zu bedienen. Das Design wurde bewusst minimalistisch gewählt, sodass Sie nicht überflutet werden.

- Wenn Sie sich zum ersten Mal einloggen, wird Ihr Interface etwa so aussehen.



- Dies ist die Übersichtsseite, Ihre Ansicht wird, egal wo sie sich befinden, immer ähnlich aussehen.
 - 1) Hier sehen Sie, auf welcher Seite Sie sich gerade befinden.
 - 2) Hier sehen Sie alle Seiten aufgelistet, auf welche Sie Zugriff haben, und auf denen Sie etwas einstellen können.
 - 3) Mithilfe dieses Links können Sie sich nach getaner Arbeit ausloggen.
 - 4) Sobald Sie sich einloggen, sehen Sie hier alle Bedrohungen, welche zurzeit auf den verbundenen Maschinen aktiv sind, und was Cyberhex bereits dagegen getan hat.
- Sollten bei Ihnen gewisse Links nicht angezeigt werden, haben Sie keinen Zugriff auf die dahinterliegende Seite.

Konfigurieren von Einstellungen

Cyberhex bietet die Möglichkeit gewisses Verhalten der Clients individuell zu bearbeiten. Dieser Abschnitt erklärt alle Einstellungen.

Profil Einstellungen

- Diese Einstellungenseite ist für sämtliche Benutzer zugänglich. Es werden keine Berechtigungen benötigt.

Your Profile (test)

Username: 1

Email: 2

Telegram ID: 3

Permissions: 4

Allow password logins. (Please make shure you have a passkey, if you disable this!) 5

Update 6

- Folgende Aktionen können Sie hier ausführen:

- 1) Dies ist Ihr Benutzername, mit diesem können Sie sich in Cyberhex einloggen. Sie können diesen beliebig ändern. Der Benutzername darf maximal 12 Zeichen lang sein, und nur Buchstaben, sowie «@» «.» «_» «-» beinhalten.
- 2) Dies ist Ihre E-Mail. Diese können Sie ebenfalls beliebig ändern. Ihre Mailadresse wird von Cyberhex nicht genutzt, ist aber von einem Administrator einsehbar.
- 3) Hier können Sie Ihre Telegram ID eintragen, um über Alarne von Cyberhex informiert zu werden.
- 4) Hier werden Ihre Berechtigungen angezeigt. Eine «1» steht jeweils für «Berechtigung erteilt» und eine «0» für «Berechtigung verweigert». Drücken Sie auf das «?» um die Berechtigungen anzuzeigen.
- 5) Hier können Sie Ihr Passwort deaktivieren. Dies hat den Vorteil, dass ein Hacker sowohl Ihr Gerät als auch Ihren Finger / Hardware Key etc. haben müsste, und erhöht die Sicherheit Ihres Accounts um einiges. Sollten Sie aber über ein starkes Passwort verfügen oder sich auch von anderen Computern einloggen wollen, können Sie die Passwort Authentifizierung auch eingeschalten lassen.
- 6) Sofern Sie etwas geändert haben (z.B. Ihren Benutzernamen), drücken Sie bitte auf diesen Button, um die Änderungen zu speichern.

Server Einstellungen

- Diese Einstellungen sind nur für Nutzer:innen mit der Berechtigung «Server Settings» verfügbar.

Server settings

Telegram Bot API-key 1

- 1) Hier können Sie den API Key des Telegram Bots hinterlegen, welcher genutzt wird, um Login und andere Warnungen zu verschicken. Auch Viruswarnungen werden mithilfe dieses Bots verschickt.

Client Einstellungen

- Bei den Client Einstellungen finden Sie folgendes Userinterface vor, solange Sie die Berechtigung «Client Settings» besitzen.

Client settings

General Settings RTP Settings Task Settings Application Control

1 2 3 4

- 1) Auf diesem Tab können Sie Generelle Einstellungen vornehmen.
 - 2) Der RTP-Tab gibt ihnen die Option die Echtzeit Überwachung zu konfigurieren.
 - 3) Bei den «Task Settings» können Sie automatische, geplante Aktionen koordinieren.
 - 4) Im «Application Control» Tab können Sie das Applikationskontrollsyste m konfigurieren.
- Es folgen nun genauere Beschreibungen der Einstellungen:

General

What should be done, if the scanner finds a virus?

call_srv ▾ 1

Allow communication with unsafe ssl cert? (if you are using self signed certs, activate this option)

allow ▾ 2

What is the URL of this server? (url or ip address where the clients connect to)

https://jakach.duckdns.org:8080 3

- 1) Hier können Sie definieren, wie Cyberhex mit Bedrohungen umgeht. Diese können entweder «Gelöscht», «in Quarantäne gesteckt» oder «Ignoriert» werden. In jedem Fall wird der Server benachrichtigt.
- 2) Wenn Sie den Cyberhex Server mit einem selbst signierten SSL-Zertifikat ausgestattet haben, setzen Sie diese Einstellung bitte auf «allow». Ansonsten kann keine sichere Verbindung zu den Clients aufgebaut werden.
- 3) Geben Sie hier bitte die URL, bzw. die IP Adresse des Servers an.

- Es folgt nun der RTP Tab.

RTP

RTP: on/off

- Check file modifications
- Check file modifications additionally with deepscan (Warning: this setting may use much CPU)
- Check processes
- Check processes additionally with deepscan (Warning: this setting may use much CPU)
- Kill processes which are detected to be a virus

Included folders for RTP folderscanner

#	Path	Add / Delete
000		<button>Add</button>
1	c:\	<button>Delete</button>

Excluded folders for RTP folderscanner

#	Path	Add / Delete
000		<button>Add</button>
1	c:\program files\cyberhex\	<button>Delete</button>
2	C:\Users\janis\AppData\Roaming\librewolf\Profiles	<button>Delete</button>

- 1) Hier können Sie definieren, ob die Echtzeitüberprüfung läuft, und wie diese vorgeht.
- 2) Geben Sie hier die Ordner an, welche überwacht werden sollen. Oft reicht es den Root Ordner «c:\» anzugeben. Cyberhex überwacht dann den ganzen Computer.
- 3) Gewisse Ordner sollten nicht überwacht werden. Diese können Sie hier ausschliessen.
WICHTIG: der Ordner «c:\program files\cyberhex\» sollte unbedingt ausgeschlossen werden.

- Der «Task Settings» Tab.

User Tasks

#	Time	Action	Argument	Name	Add / Delete
000	1	Choose an action	2	3	4

System Tasks (Warning: Changes may impact security)

#	Time	Action	Argument	Name	Add / Delete
000		Choose an action			<button>Add</button>
1	0 * * * 0	update database	-	update database	<button>Delete</button>
2	15 * * * *	update system (clients)	-	update system	<button>Delete</button>

- 1) In der ersten Spalte können Sie definieren, wann die Aktion ausgeführt wird. Nutzen Sie dafür die «Cron» Syntax. Eine einfache Methode diese Syntax zu erstellen, finden Sie hier: <https://crontab.guru/>.
- 2) In dieser Spalte können Sie auswählen, welche Aktion ausgeführt werden soll.
- 3) Hier können Sie ein Argument, wie ein Dateipfad etc. einfügen.
- 4) Der Name kann beliebig gesetzt werden und ist nur für administrativszwecke.

«User Tasks» und «System Tasks» unterscheiden sich im Wesentlichen nicht. Es

ist aber empfohlen Sicherheitsrelevante und nicht relevante Tasks zu trennen, um eine Verwaltung leichter zu machen.

- Der «Application Control» Tab.

Application control

AC: on/off

- 1 Activate Application control (for this to work you must activate rpt process scan too!)

Folders from where no app is allowed to start:

#	Path	Add / Delete
000	2	Add
3	c:\users*\downloads	Delete

- 1) Hier können Sie die Applikationskontrolle ein, bzw. ausschalten.
- 2) Hier definieren Sie, aus welchen Ordnern keine Apps starten dürfen. Es empfiehlt sich den «Downloads Ordner» als einen solchen nicht startbaren Ordner zu kennzeichnen.

Ein «*» steht dabei für eine «Wildcard», also für einen beliebigen Ordner/Namen.

Datenbank Einstellungen

- Die Datenbankeinstellungen können mit der Berechtigung «Database Settings» geändert werden.

Database update	Excluded signatures	Included Signatures	Yara Rules
1	2	3	4

- 1) Der erste Tab erlaubt ein Update der Datenbanken.
- 2) Hier können Sie Signaturen ausschliessen.
- 3) Oder neue Hinzufügen.
- 4) Hier können Sie gewisse Signaturen ansehen / herunterladen.

- «Database Update»

Database Update

- 1 **Update / regenerate Database (!this can take very long ~1h)**

- 1) Mithilfe dieses Buttons können Sie die Datenbank updaten und die neusten Signaturen herunterladen.

- «Excluded Signatures»

1	1	f20674a0751f58bbd67ada26a34ad922	2	false positive	3	Delete
---	---	----------------------------------	---	----------------	---	--------

- 1) Hash Werte, welche hier abgelegt sind, werden nicht mehr als Malware erkannt.
- 2) Es empfiehlt sich anzugeben, wiso dieser Hash-Wert hier ist.

- «Included Signatures»

000 **1** **2** **Add**

- 1) Auch hier können Sie einen Hash-Wert angeben. Dieser wird allerdings als Virus angesehen.
- 2) Auch ein Name kann gegeben werden.

- «Yara Rules»

Gmer.yar

[Download](#)

Hier sind sämtliche Yara Regeln und ein Downloadlink zu ihnen angegeben.

Verwalten von Clients

Sie können sowohl Clients hinzufügen als auch löschen.

Clients Hinzufügen

Wenn Sie die Berechtigung «Add Clients» besitzen, können Sie auf «Add Client» drücken.

Add a machine

Location:

Office1 - Computer of Lisa **1**

IP: (can be left blank)

2

Add Machine

- 1) Hier können Sie dem Client einen Namen geben. Z.b. der Standort des Clients.
- 2) Je nachdem können Sie hier die IP-Adresse des Clients eingeben. Dies kann die Verwaltung erleichtern, ist aber nicht notwendig.

Sobald Sie auf «Add Machine» gedrückt haben, können Sie 3 Dateien herunterladen. Laden Sie diese herunter und kopieren Sie auf dem Client Z.b. auf den Desktop. Führen Sie dann «installer.bat» aus. Dann wird Cyberhex installiert.

Clients verwalten

Hier können Sie alle Clients auflisten und Sie löschen.

b02183f64932	1	dell	2	nan	3	delete	4
def44fac9a12		vm		nan		delete	

- 1) Hier wird die ID des Clients angezeigt.
- 2) Der Name des Clients.
- 3) Falls gegeben, die IP-Adresse des Clients.
- 4) Und die Option den Client mit sofortiger Wirkung zu entfernen.

Verwalten der Logs

Log ansehen

Um das Log anzusehen, drücken Sie Links auf «view log»

[View log](#)

Log Entries

Virus	Error	Info
3.4%	32.1%	64.5%

Entry id	Loglevel	Logtext	Machine id	Location	Time & date	Delete entry
1	Filter	2				Delete log 4
2403	INFO	[update_system()]: No new version of cyberhex available.	9e867fcf9faf	janis pc	2024-10-10 13:15:00	delete 3
2402	INFO	[update_system()]: Updating system	9e867fcf9faf	janis pc	2024-10-10 13:15:00	delete

Sie werden folgende Ansicht sehen.

In **Rot**: Hier sehen Sie eine Statistik über den Log typ.

- 1) Hier sehen Sie das Filtersystem. Sie können nach gewissen Ereignissen im gesamten verfügbaren Log suchen.
- 2) Nutzen Sie dazu die Textfelder. Geben Sie einen Suchbegriff wie «update» ein und drücken Sie auf «Filter».
Es werden Ihnen nun alle Logeinträge angezeigt, welche zum Filter passen.
- 3) Wenn Sie wollen, dass ein bestimmter Eintrag nicht mehr angezeigt wird, drücken Sie auf «delete»
- 4) Wenn Sie das gesamte Log löschen wollen, drücken Sie auf «Delete log»

Log exportieren

Sie können die Logeinträge leicht exportieren. Drücken Sie auf «export log»

Export log		
Entry id	Loglevel	Logtext
2403	INFO	[update_system()]: No new version of cyberhex available.
		Machine id: 9e867fcf9faf, Location: janis pc, Time & date: 2024-10-10 13:15:00

Auch hier können Sie das Filtersystem gleich nutzen, wie in der Log anzeige.

- 1) Sobald Sie die Einträge exportieren wollen, drücken Sie auf «Export». Es wird Ihnen eine «CSV» Datei zum Download zur Verfügung gestellt.

Log Backups

Sobald ein Log Eintrag gelöscht wird, wird automatisch ein Backup des gesamten Logs erstellt. Dies verhindert den Beweisverlust, welcher sonst auftreten könnte. Drücken Sie links auf «log backups»

Log backups		
In order to ensure no attacker can delete evidence, you cannot delete these log backups unless they are older than 90 days!		
Delete old log files	3	
Log backup		Download
log_export_2024-10-01_09-19-52.csv	1	Download
log_export_2024-07-13_08-48-25.csv		Download
log_export_2024-07-13_08-48-24.csv		Download
log_export_2024-07-13_08-48-23.csv		Download
log_export_2024-07-13_08-48-20.csv		Download
server_log_export_2024-07-07_18-27-06.csv		Download

- 1) Hier sehen Sie den Dateinamen. Er beinhaltet den Log typ, sowie das Datum des Backups.
- 2) Sollten Sie ein Backup ansehen wollen, können Sie es hier herunterladen.
- 3) Diese Backups können nach 90 Tagen gelöscht werden.

Server Log

Auch der Server zeichnet Aktionen auf. Diese können Sie im Serverlog ansehen. Drücken Sie auf «server log»

View server log					
Entry id	Loglevel	Logtext	Username	Time & date	Delete entry
150	INFO	1 LOG:ENTRY=EXPORT=SUCCESS User janis exported the log.	janis	2024-10-17 10:38:17	Delete log 3 Delete 2

- 1) Auch hier steht das Filtersystem zur Verfügung.
- 2) Einzelne Einträge können Sie mit «delete» löschen.
- 3) Das ganze Log können Sie mit «delete log» löschen.

Beachten Sie, dass bei jeder Löschung ein Backup erstellt wird. Beweismittel können nicht zerstört werden.

Incident Response

Im Falle eines Angriffes sollte eine Verteidigung koordiniert werden. Das Incident Response System des Cyberhex Servers kann dabei helfen.

Incident erstellen

Drücken Sie Links auf «add incident»

Add an incident

Short description / keywords:

1

Create incident 2

- 1) Geben Sie dem Incident eine kurze Beschreibung.
- 2) Drücken Sie auf «create incident» um den Incident zu erstellen.

Incident verwalten

Drücken Sie auf «view incidents»

Incident list

Incident Id	Status	Description	Goto Incident
1	1 closed	2 high severity impactfull incident	3 Goto Incident
2	closed	aaa	Goto Incident
3	closed	sadsfd	Goto Incident
4	closed	test	Goto Incident

- 1) Hier sehen Sie den Status des Incidents.
- 2) Hier sehen Sie eine kurze beschreibung.
- 3) Drücken Sie auf «goto incident» um den Incident zu bearbeiten.

Wenn Sie einen Incident anklicken, kommen Sie in diese Ansicht.

Incident

Overview Files / Evidence Chat Todo Incident Settings 1

Incident #4

Status: closed

Description: test 2

Opened: 2024-06-25

Closed: 2024

- 1) In der Navigationsleiste können Sie die verfügbaren Funktionen für diesen Incident aufrufen.
- 2) Hier sehen Sie einige Informationen zum Incident.

- Der «Evidence» Tab

Files uploaded here can not be deleted. You can upload important files that might help authorities here.

Select file to upload: [Browse...](#) No file selected.

[Upload file](#)

[File](#)

[Download](#)

makeitmeme_NqIZs.jpeg

[Download](#)

Hier können Sie wichtige Beweisstücke hochladen. Diese können nicht gelöscht werden.

- Der «Chat» Tab

[Send message](#)

Messages

Message	From	Date
i found them	janis	2024-07-07 18-22-03
hello	janis	2024-07-07 18-21-53

Hier können Sie simple Nachrichten senden. Etwa um einen Fund zu teilen etc.

- Der «Todo» Tab

[Add a todo list](#)

baum

Done	Entry	Done By
<input checked="" type="checkbox"/>	aaa	janis
<input checked="" type="checkbox"/>	fadsfadsf	janis

aaa

Done	Entry	Done By
<input checked="" type="checkbox"/>	adfafdfasfdf	janis
<input checked="" type="checkbox"/>	adsfasdf	janis
<input checked="" type="checkbox"/>	aaaa	janis

In diesem Tab lassen sich einzelne ToDo Listen erstellen.

- Der «Settings» Tab

[Close incident](#)

Sobald der Incident vorüber ist, können Sie ihn schliessen.