Anleitung für eine Trend Micro DDAN (Deep Discovery Analyzer) ICAP Konfiguration.

Die hier aufgeführte Konfiguration erzielt eine synchrone Kommunikation ohne Verzögerung, dass heisst die Sandbox wird nicht verwendet. Weil die Sandbox-Analyse würde zirka 4 min. dauern. Anstelle dessen, wird hier ausschliesslich die PreScan Funktion verwendet.

Die PreScan Funktion bietet folgende Module:

- Advanced Threat Scan Engine (ATSE) for file scans
- YARA rules
- Suspicious objects and user-defined suspicious objects lists
- Predictive Machine Learning engine
- Web Reputation Services (WRS) for URL scans
- Deep Discovery Analyzer cache

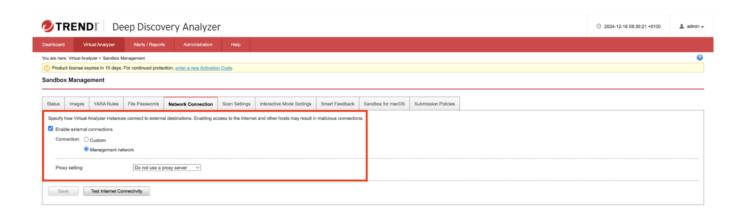
Voraussetzung für nachfolgende Anleitung ist ein minimum DDAN Software Release von 7.6.

#### **Inhalt:**

- 1. Sandbox Konfiguration
- 2. ICAP Konfiguration
- 3. Hidden ICAP Konfiguration
- 4. Allgemeine hidden PreScan Konfiguration
- 5. Testen

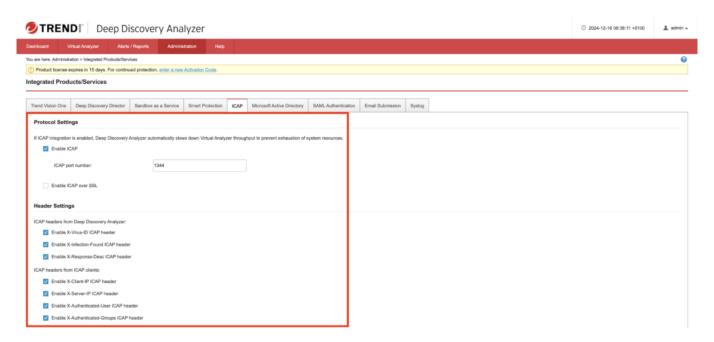
### **Sandbox Konfiguration**

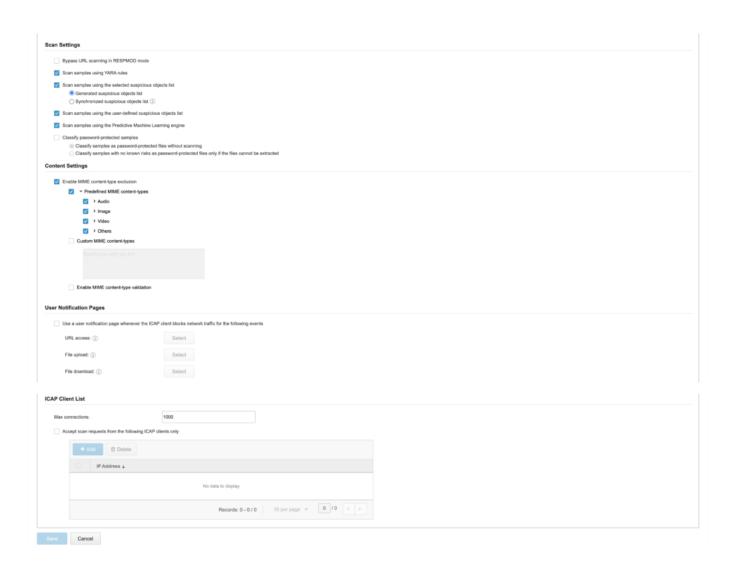
Die Sandboxen müssen Zugriff zum Internet erhalten, dass geschieht entweder über das Management Interface, wie in diesem Beispiel. Alternativ kann auch ein gesondertes Netzwerk Interface über einen Isolierten Internetzugang konfiguriert werden, die bevorzugte Variante für produktive Installationen.



# **ICAP Konfiguration**

ICAP aktivieren, mit den jeweiligen X-Headers.



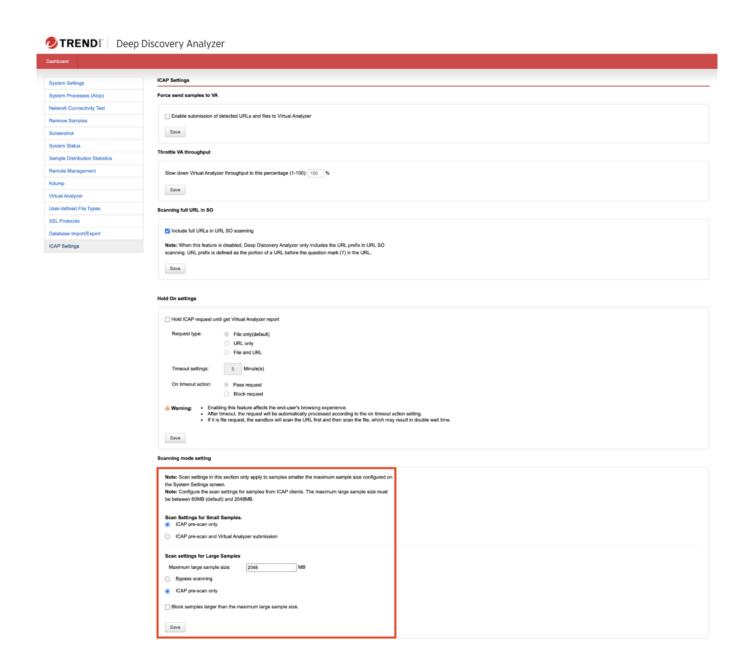


### **Hidden ICAP Konfiguration**

Erweiterte hidden ICAP Konfiguration

Hierfür muss nachfolgende URL geöffnet werden: https://192.168.x.x/pages/rdqa.php

Das Ziel ist eine synchrone Kommunikation zu erhalten. Sprich sobald das Sample hochgeladen ist, soll die Antwort zurück kommen. Alternativ wäre es möglich die Samples auch in die Sandbox hoch zuladen. Allerdings würde dass, zu einer asynchronen Kommunikation führen und die Antwort kann sich bis zu 4 min. verzögern. Die nachfolgenden Screenshots beschreiben die synchrone Kokmmunikation.



## Allgemeine hidden PreScan Konfiguration

Die PreScan Einstellungen, mit dem Fokus möglichst aggressiv und vollumfänglich zu realisieren.



System Processor (1909)  Thomas Reviews  System Processor (1909)  Thomas Reviews  System Processor (1909)  Thomas Reviews  System State  Approximation of Institute System state for Excell of Process  Approximation of Institute System state for Excell of Process  Approximation of Institute System state for Excell of Process  Approximation of Institute System System state for Excell of Process  Approximation of Institute System System state for Excell of Process  Approximation of Institute System
For the base of the second of
Note the Control of Table Showed it
Secretary   Secr
Section agreement content of factors
# Agrance
Files the Management  **Comparison  **Authorized Trained Scane Engine Mode  **Authorized Trained Scane  **Authorized Trained Scane  **On physicistic Authorized  **During Scane  **On physicistic Authorized Scane  **On physicist
**Advanced Threat Some Expire Mode **Visit of variety or 12 Topics **Sin Presents **Deletera Propriety or 12 Topics **Sin Presents **Deletera Presents **Deletera Presents **Sin Presents **Deletera Presents **Delete
**Advanced These Loss Engine Mode  **On Advanced These Loss Engine Mode  **Contribute
Clarifornia Transpare
Chick Storage
Deletes insproffcyor  CMS Settings  ** Quick Soon Mode (File)  ** Coulcins Soon Mode (File)  ** Utbrickom URL Analysis  ** Utbrickom URL Analysis  ** Utbrickom URL Analysis  ** Outch Soon Mode (File)  ** Utbrickom URL Analysis  ** Outch Soon Mode (File)  ** Outch Soon Mode (File)  ** Utbrickom URL Analysis  ** Outch Soon Mode (File)  **
Surface   Surf
Court Scan Mode (File)  Court
■ Cucks Scan Mode (File)    Finals
Note: Exists in the latest as transferred, a such action analogy Advanced Transfer Schreigh (Syring ATTSE) on the latest that her of the something of the Schreighe (Syring ATTSE) on the something of the somethi
Nets Early have not because to prefer as a cold action analogy Actions of Transit Countries (Early and TSEC) on the fact that have the conserved field as administration. If a field is desirated to be militional by ATEI, Virtual Analysis and contribution. If a field is desirated to be militional by ATEI, Virtual Analysis and prefer and the contribution of the contr
files that have not been scanner before submission. If a life is described to be melicious by ATSE, Vinsul Audiprize doors of principation update. Virtual Publipres stops temporarily and restate automatically when the update process is complete.    Constitution of the principation update. Virtual Publipres stops temporarily and restate automatically when the update process is complete.    Constitution of the principation o
During configuration, spotals, Virtual Analyses stops temporarily and restarts automatically when the update process is complete.  Brief  Cood Signer Validation  Enable  Nete: Cood signer validation is a more aggressive identicion feature that checks the digital eignatures of fine against as last of knowing good agrees in addition to conflicate validation. When disabled, city certificate validation cocous.  Sizes  1 Unknown URE, Analysis  Quick Scan Mode (URE)  Enable Quick Scan for at URE.s (fest layer URE.s only)  Disable  Nate: Enable Quick Scan for selemited URE.s (fest layer URE.s only)  Disable  Note: Enable this feature to perform a quick scan using Wich Reputation Services (WRS) on URE.s that the selement of perform a scan on the Vall.  During configuration colors.  Brief  During configuration colors.  Brief  During configuration colors.  Brief  Charles Scan for the URE.s (WRS) on URE.s that the selement of the performance of the Scan Scan using Wich Reputation Services (WRS) on URE.s that the selement of the Scan Scan using Wich Reputation Services (WRS) on URE.s that the selement of the Scan Scan Scan URE.s (WRS) on URE.s that the selement of the Scan Scan URE.s (WRS) on URE.s that the selement of the Scan Scan URE.s (WRS) on URE.s that the selement of the Scan Scan URE.s (WRS) on URE.s that the selement of the Scan Scan URE.s (WRS) on URE.s that the selement of the Scan Scan URE.s (WRS) on URE.s that the selement of the Scan URE.s (WRS) on URE.s that the selement of the Scan URE.s (WRS) on URE.s that the selement of the Scan URE.s (WRS) on URE.s that the Scan URE.s (WRS) on
Cood Signer Validation  Services  Note: Cood signer validation is a more appreasive detection feature that checks the digital signatures of file signer as all of known good signers in addition to certificate validation. When disabled, only certificate validation coors.  Size:  1 Urbinoma URE. Analysis  Quick Scan Mode (URL)  Entotic Quick Scan for all URLs  Foreite Quick Scan for all URLs  Foreite Quick Scan for undermitted URLs (first layer URLs only)  Closelate  Nest: Charles this feature to perform a quick scan using Wee Reputation Services (WHS) on URLs that have not been scanded before submissions. If a URL is detected to be malicious by WRI, Virsual Analyzer does not perform a scan on the URL.  Corner profession colonie. Virsual Analyzer stops temporarily and restarts automatically when the quick process is complete.  Size:  **Suspicious Objects List Criteria  ***Enable**  Note: Do not add ***P addresses to the Suspicious Objects list whom the IP addresses have Bills or no malicious testics or as in the Community Doman's Preputation Service approved list.
■ Cood Signer Validation ■ Enable Note: Good signer validation is a more aggressive detection feature that checks the digital signatures of fine against a list of known good signers in addition to certificate validation. When disabled, only certificate validation occurs.    Size
Note: Cood signer varidation is a more aggressive detection feature that checks the digital signatures of files against a list of honous good signers in addition to certificate varidation. When disablest, only certificate varidation occurs.    Brand   Unknown URL Analysis
Note: Cood signer varidation is a more aggressive detection feature that checks the digital signatures of files against a list of honous good signers in addition to certificate varidation. When disablest, only certificate varidation occurs.    Brand   Unknown URL Analysis
Note: Cood signer varidation is a more aggressive detection feature that checks the digital signatures of files against a list of honous good signers in addition to certificate varidation. When disablest, only certificate varidation occurs.    Brand   Unknown URL Analysis
Note: Cood signer validation is a more aggressive detection feature that checks the digital signatures of files against a last of home good signers in addition to certificate varidation. When disabled, certy certificate validation occurs.    Bave
If the against a list of known good signers in addition to certificate validation. When disabled, only certificate validation occurs.  □ Unknown URL Analysis  □ Quick Scan Mode (URL)  □ Enable Quick Scan for all URLs  □ Enable Quick Scan for submitted URLs (first layer URLs only)  □ Isable  Note: Enable this feature to perform a quick scan using Web Regulation Services (WRS) on URLs that have not been scanned before submission. If a URL is detected to be malicious by WRS, Virtual Analyzer does not perform a cacn on the URL.  During configuration update, Virtual Analyzer stops temporarily and restarts automatically when the update process is complete.  □ Enable  Note: Do not add IP addresses to the Suspicious Objects list when the IP addresses have little or no malicious traffic or are in the Community Domain*IP Reputation Service approved list.
Vinknown URL Analysis  Valick Scan Mode (URL)  Enable Quick Scan for all URLs  Enable Quick Scan for submitted URLs (first layer URLs only)  Disable  Note: Enable this feature to perform a quick scan using Web Reputation Services (WRS) on URLs that have not been scanned before submission. If a URL is desected to be malicious by WRS, Whall Analyzer does not perform a scan on the URL.  During configuration update, Vinual Analyzer stops temporarily and restarts automatically when the update process is compiles.  Service  Value (Paddessee to the Supplicious Objects List Criteria  Enable  Note: Charles on the Supplicious Objects list when the IP addressee have little or no malicious braffic or are in the Community Domain/IP Regulation Service approved isc.
Unknown URL Analysis  Quick Scan Mode (URL)  Enable Quick Scan for all URLs  Enable Quick Scan for all URLs  Enable Olick Scan for submitted URLs (first layer URLs only)  Disable  Note: Enable this feature to perform a quick scan using Web Reputation Services (WRS) on URLs that have not been scanned before submission. If a URL is detected to be malicious by WRS, Virtual Analyzer does not perform a scan on the URL.  During configuration update, Virtual Analyzer stops temporarily and restarts automatically when the update process is complete.  Save  **Suspicious Objects List Criteria  Enable  Note: On ord add IP addresses to the Suspicious Objects list when the IP addresses have little or no malicious traffic or are in the Community Domain/IP Reputation Service approved list.
■ Enable Quick Scan Mode (URL) ■ Enable Quick Scan for all URLs □ Enable Quick Scan for submitted URLs (first layer URLs only) □ Disable  Note: Enable this feature to perform a quick scan using Web Reputation Services (WRS) on URLs that have not been scanned before submission. If a URL is detected to be malicious by WRS, Virtual Analyzer does not perform a scan on the URL.  During configuration update, Virtual Analyzer stops temporarily and restarts automatically when the update process is complete.  Save  ■ Suspicious Objects List Criteria ■ Enable  Note: Do not add IP addresses to the Suspicious Objects list when the IP addresses have little or no malicious traffic or are in the Community Domain/IP Reputation Service approved list.
■ Enable Quick Scan Mode (URL) ■ Enable Quick Scan for all URLs □ Enable Quick Scan for submitted URLs (first layer URLs only) □ Disable  Note: Enable this feature to perform a quick scan using Web Reputation Services (WRS) on URLs that have not been scanned before submission. If a URL is detected to be malicious by WRS, Virtual Analyzer does not perform a scan on the URL.  During configuration update, Virtual Analyzer stops temporarily and restarts automatically when the update process is complete.  Save  ■ Suspicious Objects List Criteria ■ Enable  Note: Do not add IP addresses to the Suspicious Objects list when the IP addresses have little or no malicious traffic or are in the Community Domain/IP Reputation Service approved list.
Enable Quick Scan for all URLs  Enable Quick Scan for submitted URLs (first layer URLs only)  Disable  Note: Enable this feature to perform a quick scan using Web Reputation Services (WRS) on URLs that have not been scanned before submission. If a URL is defected to be malicious by WRS, Virtual Analyzer does not perform a scan on the URL.  During configuration update, Virtual Analyzer stops temporarily and restarts automatically when the update process is complete.  Save  ** Suspicious Objects List Criteria    Enable
Enable Quick Scan for submitted URLs (first layer URLs only)  Disable  Note: Enable this feature to perform a quick scan using Web Reputation Services (WRS) on URLs that have not been scanned before submission. If a URL is delected to be malicious by WRS, Virtual Analyzer does not perform a scan on the URL.  During configuration update, Virtual Analyzer stops temporarily and restarts automatically when the update process is complete.  Save  ** Suspicious Objects List Criteria    Enable
Disable  Note: Enable this feature to perform a quick scan using Web Reputation Services (WRS) on URLs that have not been scanned before submission. If a URL is delected to be malicious by WRS, Virtual Analyzer does not perform a scan on the URL.  During configuration update, Virtual Analyzer stops temporarily and restarts automatically when the update process is complete.  Save  ** Suspicious Objects List Criteria    Enable
Note: Enable this feature to perform a quick scan using Web Reputation Services (WRS) on URLs that have not been scanned before submission. If a URL is detected to be malicious by WRS, Virtual Analyzer does not perform a scan on the URL.  During configuration update, Virtual Analyzer stops temporarily and restarts automatically when the update process is complete.  Save  ** Suspicious Objects List Criteria
have not been scanned before submission. If a URL is delected to be malicious by WRS, Virtual Analyzer does not perform a scan on the URL.  During configuration update, Virtual Analyzer stops temporarily and restarts automatically when the update process is complete.  Save  ** Suspicious Objects List Criteria
does not perform a soon on the URL.  During configuration update, Virtual Analyzer stops temporarily and restarts automatically when the update process is complete.  Save  * Suspicious Objects List Criteria  * Enable  Note: Do not add IP addresses to the Suspicious Objects list when the IP addresses have little or no mallicious traffic or are in the Community Domain/IP Reputation Service approved list.
During configuration update, Virtual Analyzer stops temporarily and restarts automatically when the update process is complete.  Save  ** Suspicious Objects List Criteria  ** Enable  Note: Do not add IP addresses to the Suspicious Objects list when the IP addresses have little or no mallicious traffic or are in the Community Domain/IP Reputation Service approved list.
" Suspicious Objects List Criteria  © Enable  Note: Do not add IP addresses to the Suspicious Objects list when the IP addresses have little or no mallicious fraffic or are in the Community Domain/IP Reputation Service approved list.
▼ Suspicious Objects List Criteria  ☑ Enable  Note: Do not add IP addresses to the Suspicious Objects list when the IP addresses have little or no mallicious traffic or are in the Community Domain/IP Reputation Service approved list.
■ Enable Note: Do not add IP addresses to the Suspicious Objects list when the IP addresses have title or no malicious traffic or are in the Community Domain/IP Reputation Service approved list.
■ Enable Note: Do not add IP addresses to the Suspicious Objects list when the IP addresses have title or no malicious traffic or are in the Community Domain/IP Reputation Service approved list.
Note: Do not add IP addresses to the Suspicious Objects list when the IP addresses have little or no malicious traffic or are in the Community Domain/IP Reputation Service approved list.
Note: Do not add IP addresses to the Suspicious Objects list when the IP addresses have little or no malicious traffic or are in the Community Domain/IP Reputation Service approved list.
malicious traffic or are in the Community Domain/IP Reputation Service approved list.
No.
9575
* Suspicious object risk level setting for ICAP pre-scan and Virtual Analyzer analysis
Risk level:
Plisk leve:   Fligh risk only (default)
* ** *********************************
Save



#### **Testen**

Zum testen wird ein Ubuntu Linux System mit dem "c-icap-client" verwendet.

c-icap-client: https://c-icap.sourceforge.net/

eicar-Testmalware: https://www.eicar.org/download-anti-malware-testfile/

commands mit Testmalware:

"-i 192.168.x.x" entspricht der IP Adresse der DDAN.

```
/usr/local/c-icap/bin/c-icap-client -s response -i 192.168.x.x -f ./myeicar -resp ./myeicar -v
```

commands mit Clean-File:

```
/usr/local/c-icap/bin/c-icap-client -s response -i 192.168.x.x -f ./putty.exe -resp ./putty.exe -v
```