

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.

 Deep Discovery Analyzer

2024-12-16 08:30:21 +0100admin

DashboardVirtual AnalyzerAlerts / ReportsAdministrationHelp

You are here: Virtual Analyzer > Sandbox Management

Product license expires in 15 days. For continued protection, [enter a new Activation Code](#).

Sandbox Management

StatusImagesYARA RulesFile PasswordsNetwork ConnectionScan SettingsInteractive Mode SettingsSmart FeedbackSandbox for macOSSubmission Policies

Specify how Virtual Analyzer instances connect to external destinations. Enabling access to the Internet and other hosts may result in malicious connections.

☒ Enable external connections

Connection: ☐ Custom ☒ Management network

Proxy setting:

ICAP Konfiguration

ICAP aktivieren, mit den jeweiligen X-Headers.

 Deep Discovery Analyzer

2024-12-16 08:38:11 +0100admin

DashboardVirtual AnalyzerAlerts / ReportsAdministrationHelp

You are here: Administration > Integrated Products/Services

Product license expires in 15 days. For continued protection, [enter a new Activation Code](#).

Integrated Products/Services

Trend Vision OneDeep Discovery DirectorSandbox as a ServiceSmart ProtectionICAPMicrosoft Active DirectorySAML AuthenticationEmail SubmissionSyslog

Protocol Settings

If ICAP integration is enabled, Deep Discovery Analyzer automatically slows down Virtual Analyzer throughput to prevent exhaustion of system resources.

☒ Enable ICAP

ICAP port number:

☐ Enable ICAP over SSL

Header Settings

ICAP headers from Deep Discovery Analyzer:

- ☒ Enable X-Virus-ID ICAP header
- ☒ Enable X-Infection-Found ICAP header
- ☒ Enable X-Response-Desc ICAP header

ICAP headers from ICAP clients:

- ☒ Enable X-Client-IP ICAP header
- ☒ Enable X-Server-IP ICAP header
- ☒ Enable X-Authenticated-User ICAP header
- ☒ Enable X-Authenticated-Groups ICAP header

Scan Settings

☐ Bypass URL scanning in RESPMOD mode

☒ Scan samples using YARA rules

☒ Scan samples using the selected suspicious objects list

☒ Generated suspicious objects list
 ☐ Synchronized suspicious objects list ⓘ

☒ Scan samples using the user-defined suspicious objects list

☒ Scan samples using the Predictive Machine Learning engine

☐ Classify password-protected samples

☒ Classify samples as password-protected files without scanning
 ☐ Classify samples with no known risks as password-protected files only if the files cannot be extracted

Content Settings

☒ Enable MIME content-type exclusion

☒ Predefined MIME content-types

☒ Audio
 ☒ Image
 ☒ Video
 ☒ Others

☐ Custom MIME content-types

Specify new entry per line

☐ Enable MIME content-type validation

User Notification Pages

☐ Use a user notification page whenever the ICAP client blocks network traffic for the following events

URL access: ⓘ

File upload: ⓘ

File download: ⓘ

ICAP Client List

Max connections:

☐ Accept scan requests from the following ICAP clients only

☐	IP Address ↓
No data to display	

Records: 0 - 0 / 0

10 per page

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.

Dashboard

System Settings

System Processes (Atop)

Network Connectivity Test

Remove Samples

Screenshot

System Status

Sample Distribution Statistics

Remote Management

Kdump

Virtual Analyzer

User-defined File Types

SSL Protocols

Database Import/Export

ICAP Settings

ICAP Settings

Force send samples to VA

☐ Enable submission of detected URLs and files to Virtual Analyzer

Save

Throttle VA throughput

Slow down Virtual Analyzer throughput to this percentage (1-100): %

Save

Scanning full URL in SO

☒ Include full URLs in URL SO scanning

Note: When this feature is disabled, Deep Discovery Analyzer only includes the URL prefix in URL SO scanning. URL prefix is defined as the portion of a URL before the question mark (?) in the URL.

Save

Hold On settings

☐ Hold ICAP request until get Virtual Analyzer report

Request type: ☒ File only(default)
☐ URL only
☐ File and URL

Timeout settings: Minute(s)

On timeout action: ☒ Pass request
☐ Block request

Warning:

- Enabling this feature affects the end-user's browsing experience.
- After timeout, the request will be automatically processed according to the on timeout action setting.
- If it is file request, the sandbox will scan the URL first and then scan the file, which may result in double wait time.

Save

Scanning mode setting

Note: Scan settings in this section only apply to samples smaller the maximum sample size configured on the System Settings screen.
Note: Configure the scan settings for samples from ICAP clients. The maximum large sample size must be between 60MB (default) and 2048MB.

Scan Settings for Small Samples.
☒ ICAP pre-scan only
☐ ICAP pre-scan and Virtual Analyzer submission

Scan settings for Large Samples
Maximum large sample size: MB
☐ Bypass scanning
☒ ICAP pre-scan only
☐ Block samples larger than the maximum large sample size.

Save

Allgemeine hidden PreScan Konfiguration

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

System Settings
System Processes (Atop)
Network Connectivity Test
Remove Samples
Screenshot
System Status
Sample Distribution Statistics
Remote Management
Kdump
Virtual Analyzer
User-defined File Types
SSL Protocols
Database Import/Export
ICAP Settings

Virtual Analyzer

Scan Mode

- ☐ Standard
☐ Enables aggressive scan mode for Excel 4.0 macros

☒ Aggressive ⓘ

Save

Advanced Threat Scan Engine Mode

- ☒ All
☐ Only dropped files
☐ Disable

Save

Quick Scan Mode (File)

☒ Enable

Note: Enable this feature to perform a quick scan using Advanced Threat Scanning Engine (ATSE) on files that have not been scanned before submission. If a file is detected to be malicious by ATSE, Virtual Analyzer does not perform a scan on the file. During configuration update, Virtual Analyzer stops temporarily and restarts automatically when the update process is complete.

Save

Good Signer Validation

☒ Enable

Note: Good signer validation is a more aggressive detection feature that checks the digital signatures of files against a list of known good signers in addition to certificate validation. When disabled, only certificate validation occurs.

Save

Unknown URL Analysis

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.

Save

Suspicious object risk level setting for ICAP pre-scan and Virtual Analyzer analysis

- Risk level: ☐ High risk only (default)
☒ All risk levels

Save

Zip bomb detection

☒ Enable

Note: Enable this feature to detect malicious archive files. Large files extracted from archive files may contain potential threats (such as viruses and malware) or render applications or systems unresponsive due to excessive file size.

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
```