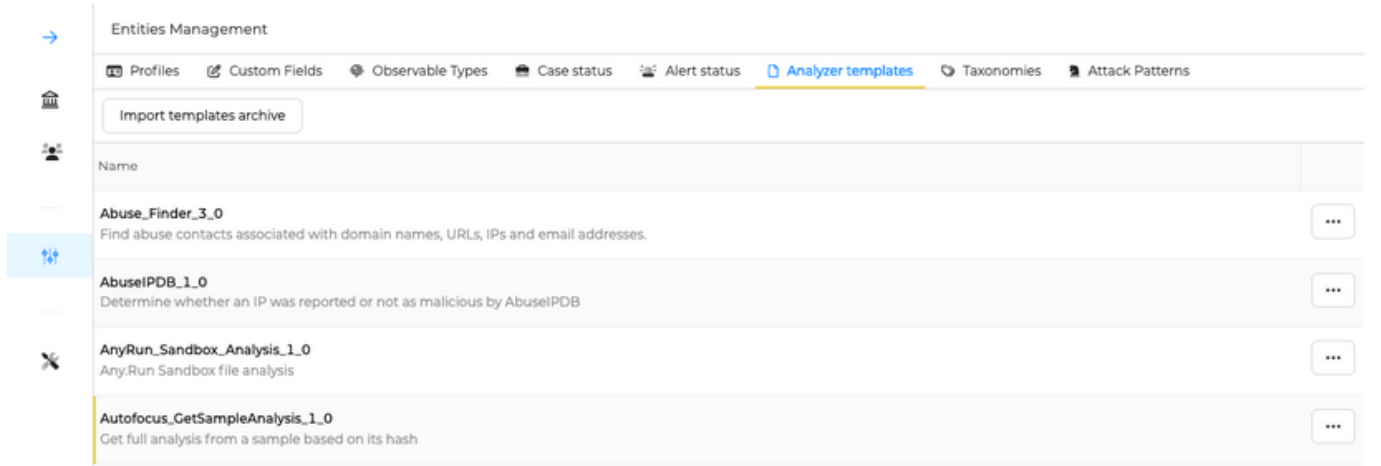


Analiz Şablonları

TheHive, analiz raporlarını görüntülemek için HTML şablonlarına ihtiyaç duyar.

Genel Analiz Şablonlarını Kurun veya Güncelleyin

- Yönetici olarak, "Varlık Yönetimi" menüsüne ve "Analiz Şablonlarına" gidin.



- ZIP arşivini indirin, ekleyin ve İçer Aktar düğmesine tıklayın.

Entities Management / Analyzer templates

→ Entities Management

Profiles Custom Fields Observable Types Case status Alert status Analyzer templates

Import templates archive

Name
Abuse_Finder_3_0 Find abuse contacts associated with domain names, URLs, IPs and email addresses.
AbuseIPDB_1_0 Determine whether an IP was reported or not as malicious by AbuseIPDB
AnyRun_Sandbox_Analysis_1_0 Any.Run Sandbox file analysis
Autofocus_GetSampleAnalysis_1_0 Get full analysis from a sample based on its hash
Autofocus_SearchIOC_1_0 Search samples in Autofocus based on a single IOC
CIRCLHashlookup_1_1 CIRCL hashlookup uses a public API to lookup hash values against databases of known good files
Crt_sh_Transparency_Logs_1_0 Query domains against the certificate transparency lists available at crt.sh.
DShield_lookup_1_0 Query the SANS ISC DShield API to check for an IP address reputation.
dshield_test_1_0 Query the SANS ISC DShield API to check for an IP address reputation.
EmlParser_2_1 Parse and visualise EML email message. Submit a .eml formatted file and extract some useful information.
FileInfo_8_0 Parse files in several formats such as OLE and OpenXML to detect VBA macros, extract their source code, generate us

Import templates archive

Download the official templates archive

You can download the latest official analyzer templates archive from here

Templates archive

Drop file or click

report-templates.zip

Import

Şablonları Düzenle

Yeni bir Analiz Cortex'te etkinleştirildiğinde ve TheHive için kullanılabilir hale geldiğinde, bu listede bir şablon satırı eklenir.

- Düzenlenecek şablonu bulun

VirusTotal_GetReport_3_1
Get the latest VirusTotal report for a file, hash, domain or an IP address.

VirusTotal_Rescan_3_1
Use VirusTotal to run new analysis on hash.

Default Template

...

Düzenleyin ve kaydedin

Entities Management / Analyzer templates

→ Entities Management

Profiles Custom Fields Observable Types Case status Alert status Analyzer templates

Import templates archive

Name

Abuse_Finder_3_0

Find abuse contacts associated with domain names, URLs, IPs and email addresses.

AbuseIPDB_1_0

Determine whether an IP was reported or not as malicious by AbuseIPDB

AnyRun_Sandbox_Analysis_1_0

Any.Run Sandbox file analysis

Autofocus_GetSampleAnalysis_1_0

Get full analysis from a sample based on its hash

Autofocus_SearchIOC_1_0

Search samples in Autofocus based on a single IOC

CIRCLHashlookup_1_1

CIRCL hashlookup uses a public API to lookup hash values against databases of known good files

Crt_sh_Transparency_Logs_1_0

Query domains against the certificate transparency lists available at crt.sh.

DShield_lookup_1_0

Query the SANS ISC DShield API to check for an IP address reputation.

dshield_test_1_0

Query the SANS ISC DShield API to check for an IP address reputation.

EmiParser_2_1

Parse and visualise EML email message. Submit a .eml formatted file and extract some useful information.

5.0.17-1 FileInfo_8_0

Parse files in several formats such as OLE and OpenXML to detect VBA macros, extract their source code, generate us

Import templates archive

Download the official templates archive

You can download the latest official analyzer templates archive [from here](#)

Templates archive

Drop file or click

report-templates.zip

Import

Bağlı analizleri çalıştırmak, yeni şablonun uygulandığı sonuçları görüntülemelidir.

Revision #2

Created 9 April 2024 10:46:10 by Güldeniz Akca

Updated 9 April 2024 10:54:03 by Güldeniz Akca