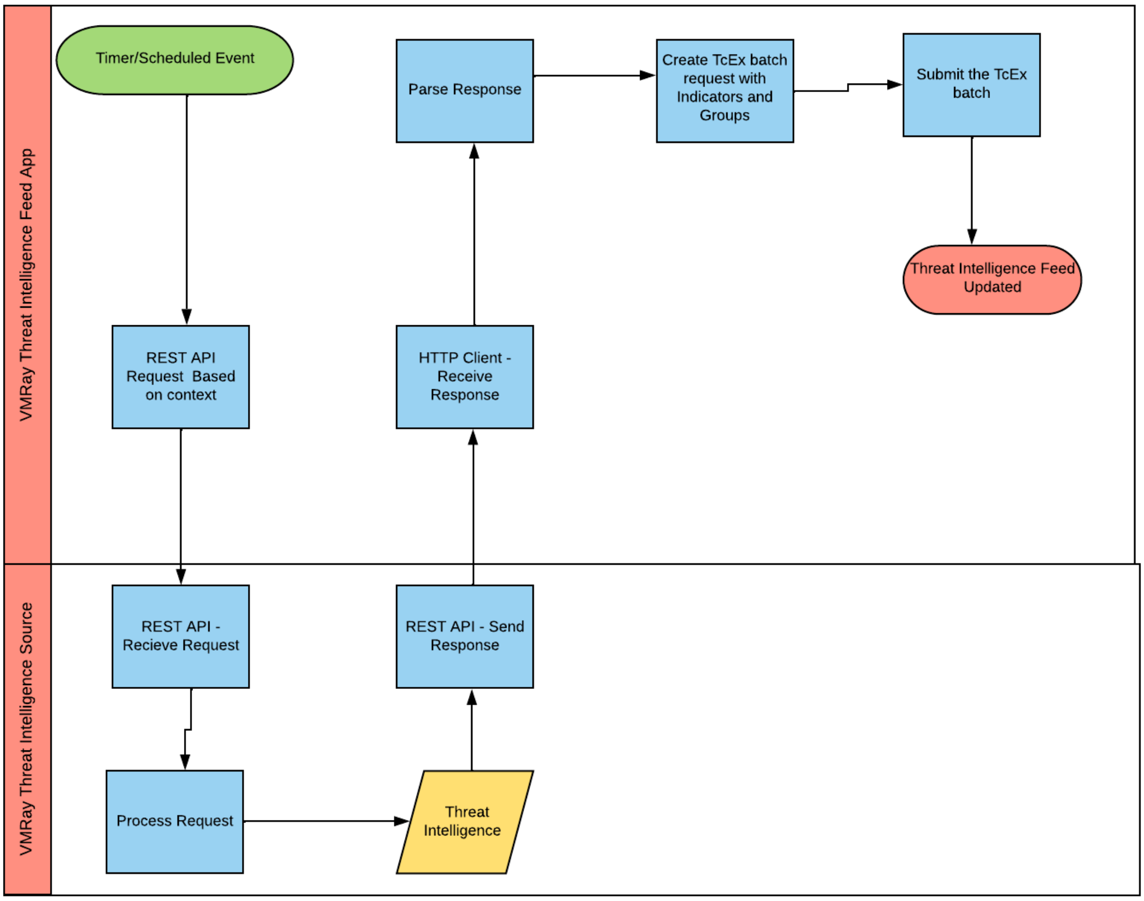
ThreatConnect – VMRay Integration User Guide

Version 1.0.0

Contents

Introduction

The ThreatConnect platform ingests and maps Threat Indicators from malware analysed by VMRay's sandbox. Indicators from VMRay are private, and are generated from SOC, CERT, and CTI teams submitting suspicious and malicious samples for analysis. VMRay conducts behavioural, static, and dynamic analysis, that produce credible IOCs. The indicators and analysis reports contain threat families, TTPs, and malware and phishing behind the threat. Security teams ingest IOCs from VMRay which include malware threat analysis from phishing emails, files, QR codes, and URLs. Credential phishing, malware, ransomware, and BEC attacks, are a few examples, provided to customers to operationalize with their SOC, CERT, and CTI teams. Each submission sample corresponds with indicator severity and that security teams can use with confidence. VMRay empowers security teams to make informed strategic decisions against today's malware and phishing attacks. This integration consists of consuming the VMRay's IOCs and reports into the ThreatConnect Platform as a Threat Intelligence feed.


VMRay Threat Intelligence Feed App
Timer/Scheduled Event
Parse Response
Create TcEx batch request with Indicators and Groups
Submit the TcEx batch
Threat Intelligence Feed Updated
REST API Request Based on context
HTTP Client - Receive Response
VMRay Threat Intelligence Source
REST API - Recieve Request
REST API - Send Response
Process Request
Threat Intelligence

Data Mapping

The table below documents the data mapping that takes place between the VMRay Threat Intelligence data and the ThreatConnect Platform.

VMRay Threat Intelligence Feed	ThreatConnect Field/Object
Sample Report general information	Group of type Report
Analysis Report	Group of type Report
Threat Names	Group of type Threat
IP	Indicator of type Address
Email Subject	Indicator of type Email Subject
URL	Indicator of type URL
Domain	Indicator of type Host
Files	Indicator of type File
Registry Key	Indicator of type Registry Key
MD5	Indicator of type File
SHA256	Indicator of type File
SHA1	Indicator of type File

Configuration Requirements

1. Access to a ThreatConnect Platform Instance
2. ThreatConnect API user

Job App Installation

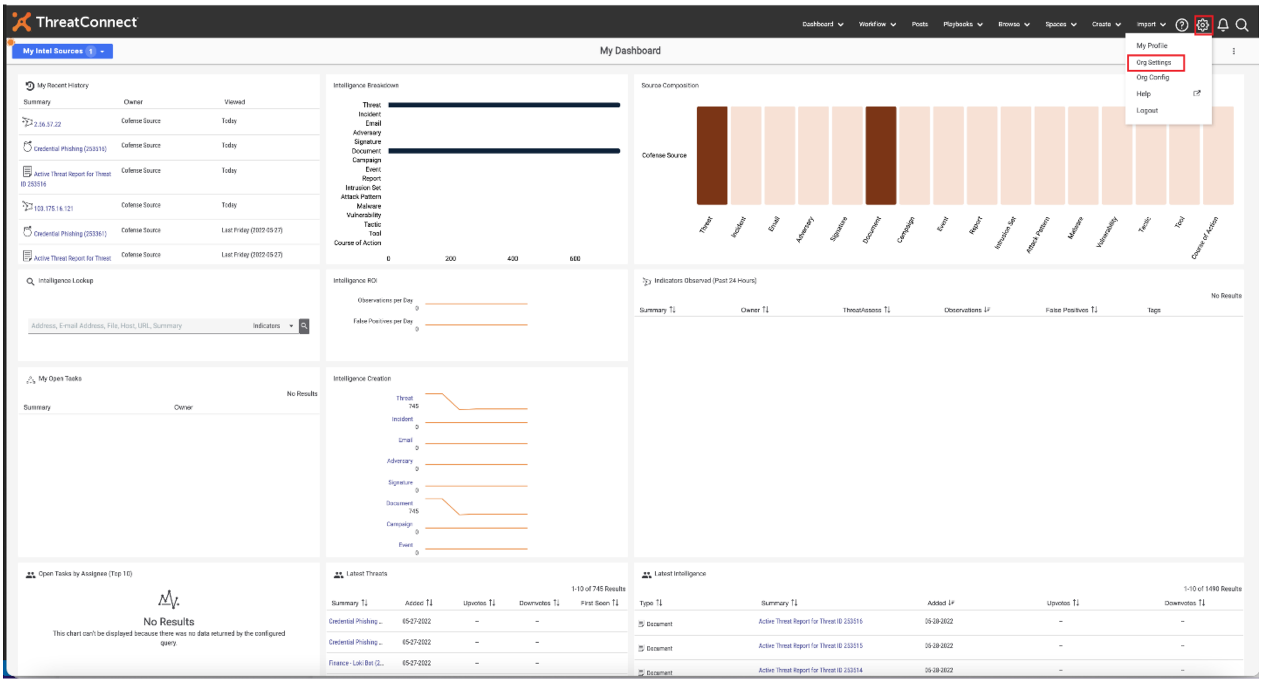
For download and installation instructions, please refer to the ThreatConnect System Administration Guide (Install an App). For more information, contact your ThreatConnect Customer Success representatives.

ThreatConnect Job Configuration

ThreatConnect Platform allows customers to run jobs on a scheduled basis. Once the package has been installed, the customer enabled to run the VMRay Threat Intelligence feed as frequently as they desire. By default, the App will run daily.

Note: These steps are not necessary if the app was deployed using Feed Deployer as the job would have already been configured.

- Go to the gear in the top right corner in the ThreatConnect platform then **Org Settings > Apps.**
- Click on the + to create a new job.



My Recent History

Summary	Owner	Viewed
2.56.57.22	Cofense Source	Today
Credential Phishing (253516)	Cofense Source	Today
Active Threat Report for Threat ID 253516	Cofense Source	Today
103.175.16.121	Cofense Source	Today
Credential Phishing (253361)	Cofense Source	Last Friday (2022-05-27)
Active Threat Report for Threat	Cofense Source	Last Friday (2022-05-27)

Indicators Observed (Past 24 Hours)

No Results

Summary	Owner	ThreatAssess	Observations	False Positives	Tags

My Open Tasks

No Results

Summary	Owner

Latest Threats

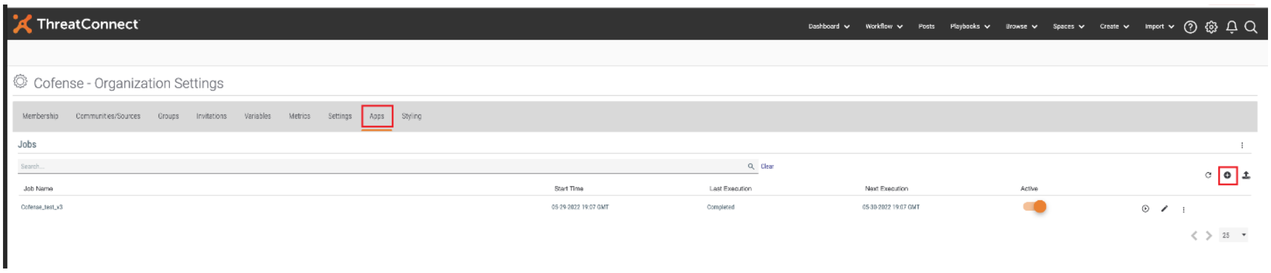
1-10 of 745 Results

Summary	Added	Upvotes	Downvotes	First Seen
Credential Phishing ...	05-27-2022	–	–	
Credential Phishing ...	05-27-2022	–	–	
Finance - Loki Bot (2...	05-27-2022	–	–	

Latest Intelligence

1-10 of 1490 Results

Type	Summary	Added	Upvotes	Downvotes
Document	Active Threat Report for Threat ID 253516	05-28-2022	–	–
Document	Active Threat Report for Threat ID 253515	05-28-2022	–	–
Document	Active Threat Report for Threat ID 253514	05-28-2022	–	–



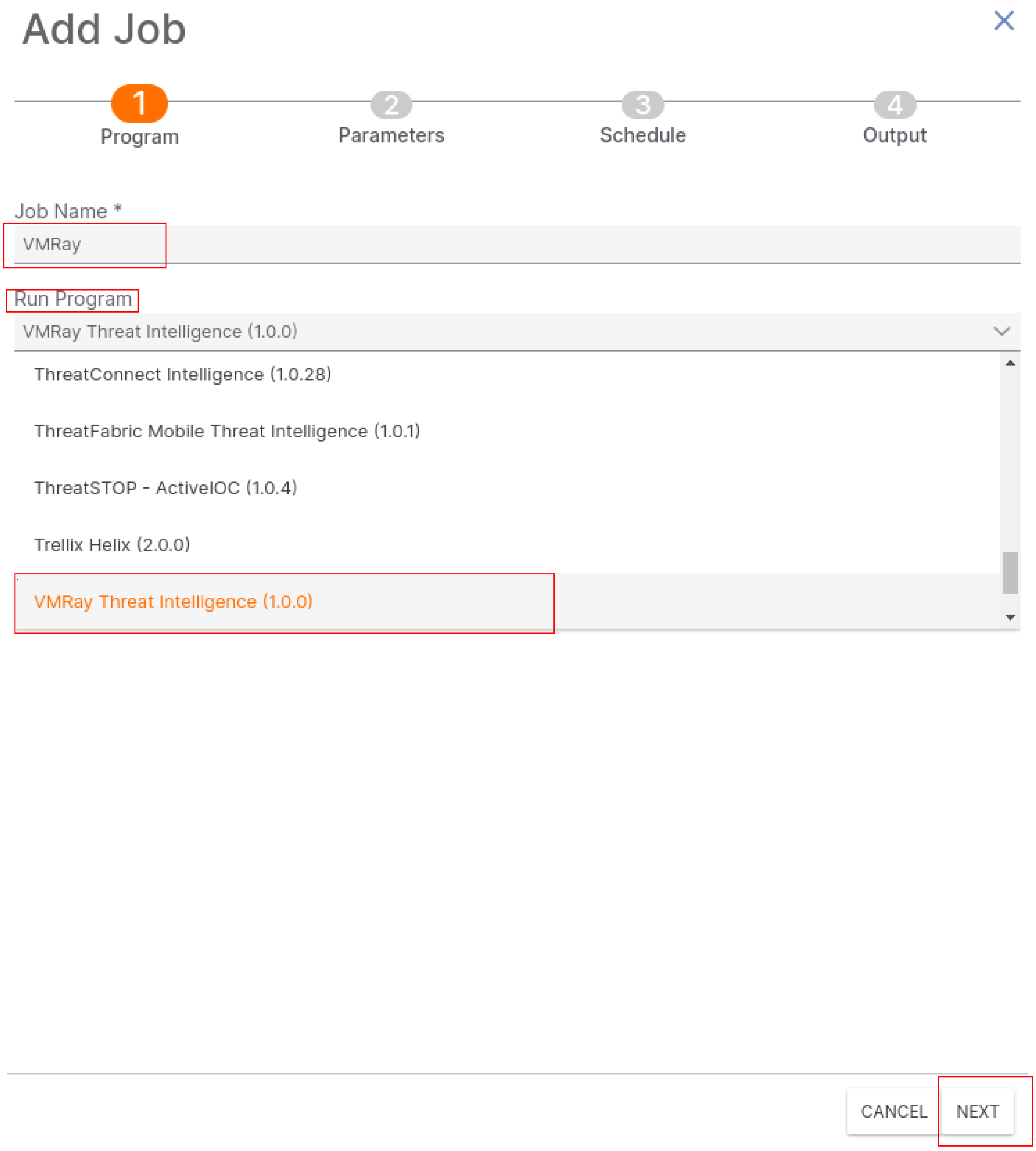
Cofense - Organization Settings

Jobs

Job Name	Start Time	Last Execution	Next Execution	Active
Cofense_test_v3	05-29-2022 19:07 GMT	Completed	05-30-2022 19:07 GMT	●

Program Screen

- Enter the Job Name (Ex: VMRay).
- Select the Run program as a “VMRay Threat Intelligence (1.0.0)” from the dropdown.
- Click NEXT.



Add Job

Job Name *
VMRay

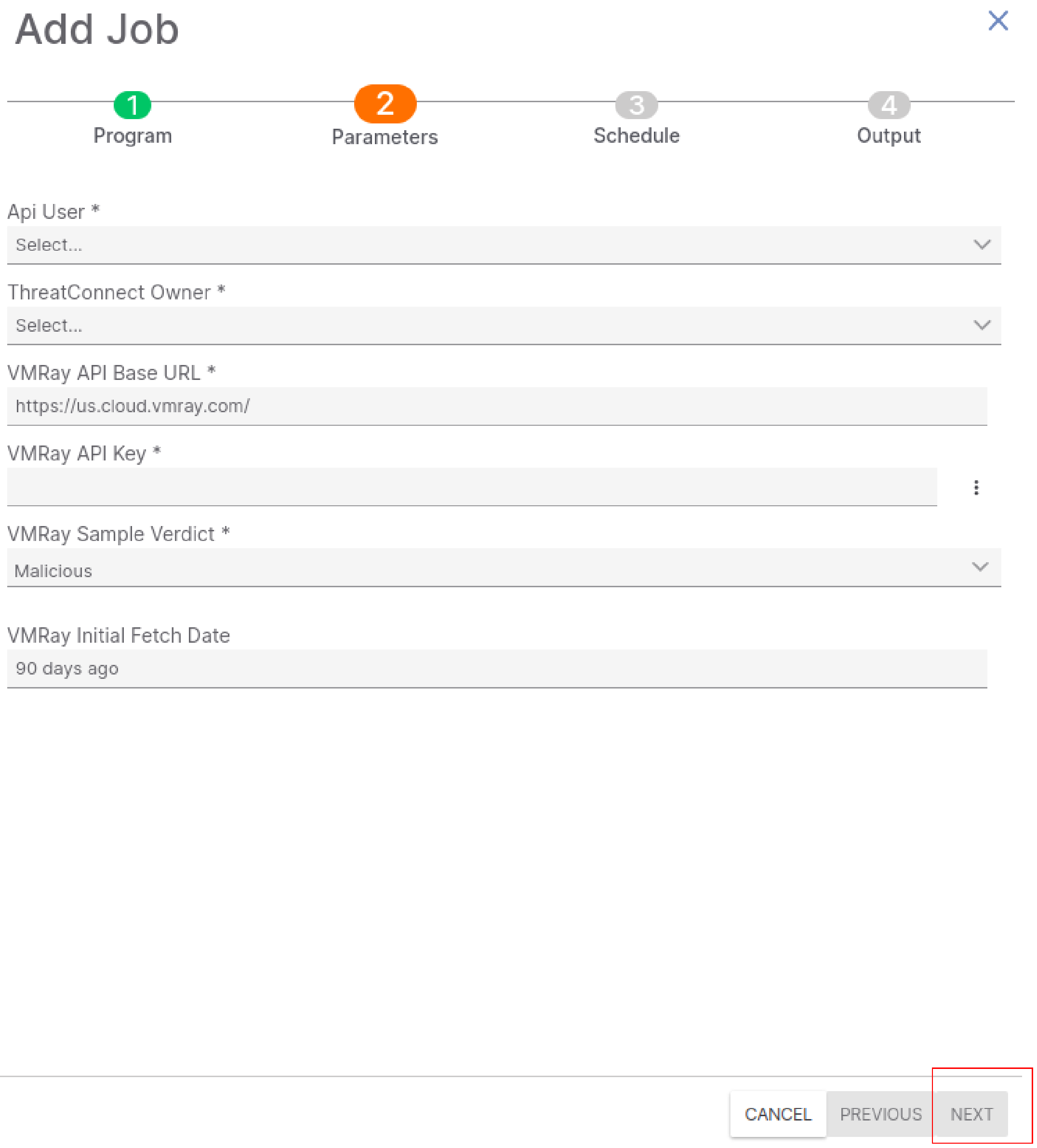
Run Program
VMRay Threat Intelligence (1.0.0)

ThreatConnect Intelligence (1.0.28)
ThreatFabric Mobile Threat Intelligence (1.0.1)
ThreatSTOP - ActiveIOC (1.0.4)
Trellix Helix (2.0.0)
VMRay Threat Intelligence (1.0.0)

Parameter Screen

- For API User, click on the down arrow and select your organization (Required – Username of VMRay API credentials that will be used)
- For ThreatConnect Default Org Name click on dropdown arrow as mentioned in the image. (Required - This parameter is the organization name with which the incoming Indicators will be associated)
- For VMRay API Base URL (Required -Ex: https://us.cloud.vmray.com/)
- VMRay API Key (Required – API Key of VMRay credentials that will be used.)

- VMRay Sample Verdict (Required – VMRay Sample verdict. By default, Malicious is selected.)
- VMRay Initial Fetch Date (Required – How far back to perform the initial ingestion of VMRay threat Intelligence. VMRay Threat Intelligence recommends 1 to 3 months.)
- Click NEXT



Add Job

Api User *
Select...

ThreatConnect Owner *
Select...

VMRay API Base URL *
https://us.cloud.vmray.com/

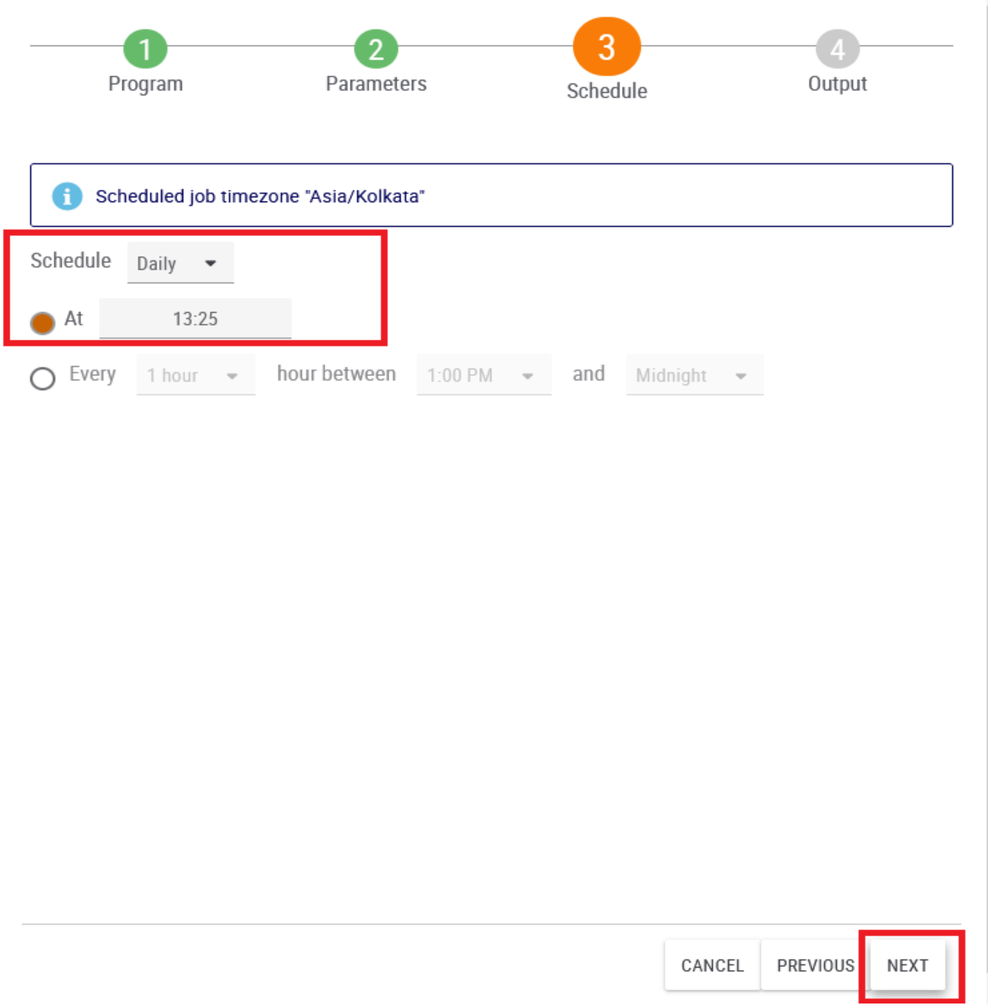
VMRay API Key *

VMRay Sample Verdict *
Malicious

VMRay Initial Fetch Date
90 days ago

Schedule Screen

- Depending on your environment, you can schedule the feed at daily hours, weekly etc., select the appropriate values from the dropdown menu.
- Click NEXT



Scheduled job timezone "Asia/Kolkata"

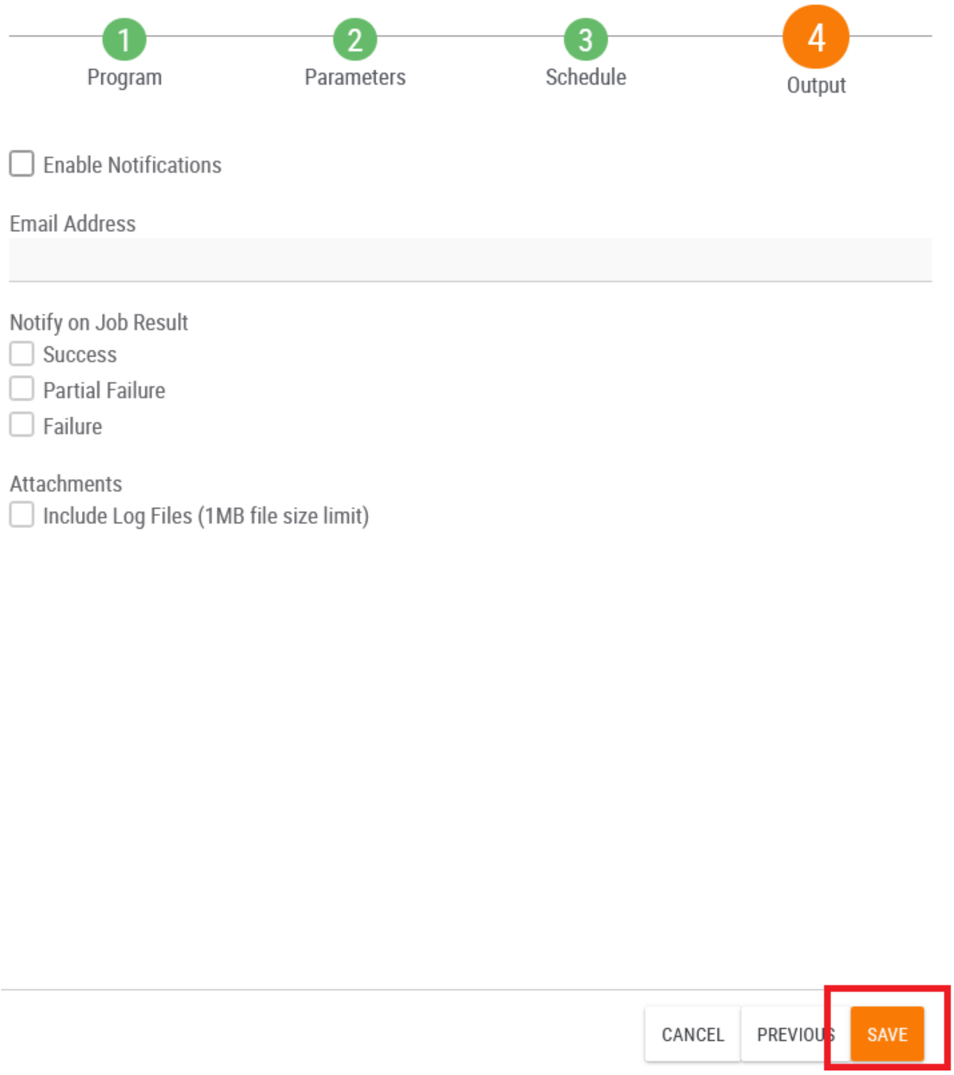
Schedule Daily

● At 13:25

○ Every 1 hour hour between 1:00 PM and Midnight

Output Screen

- If you want to be notified on job results, click the box next to Enable Notifications, enter an email address for the notifications to be sent, and which notifications that you want and if you want a log file attached.
- Click SAVE



□ Enable Notifications

Email Address

Notify on Job Result

□ Success

□ Partial Failure

□ Failure

Attachments

□ Include Log Files (1MB file size limit)

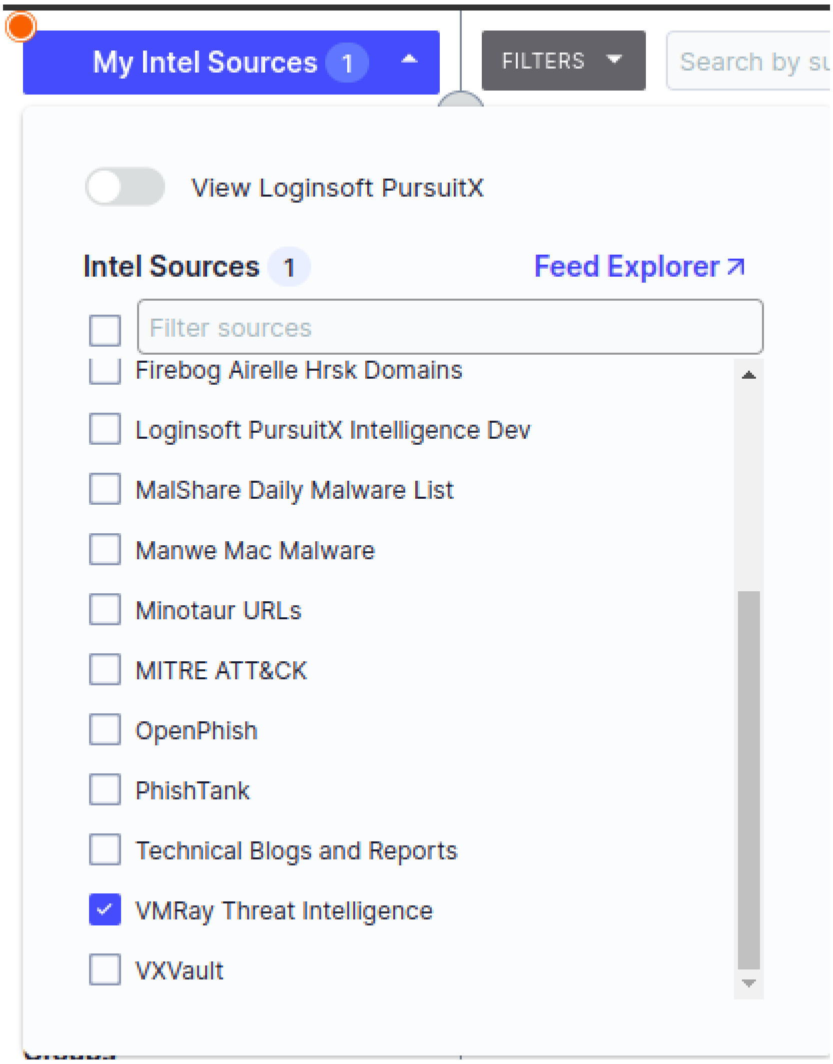
- Once the Job has been saved, we can find our job on Jobs under Apps
- Click on the slider under Active to activate the job.
- Here we can observe the Start Time and Next Execution time and Last Execution Status as well. If you want to run the job at this time, click on the play button in the options tab.

Browsing VMRay Feed

For guidance on general browsing of indicators and groups in the ThreatConnect Platform, please refer to the article below:

https://training.threatconnect.com/learn/article/browse-kb-article

Navigate to the browse page and check to make sure that the VMRay Threat Intelligence Feed is checked.



My Intel Sources 1

View Loginsoft PursuitX

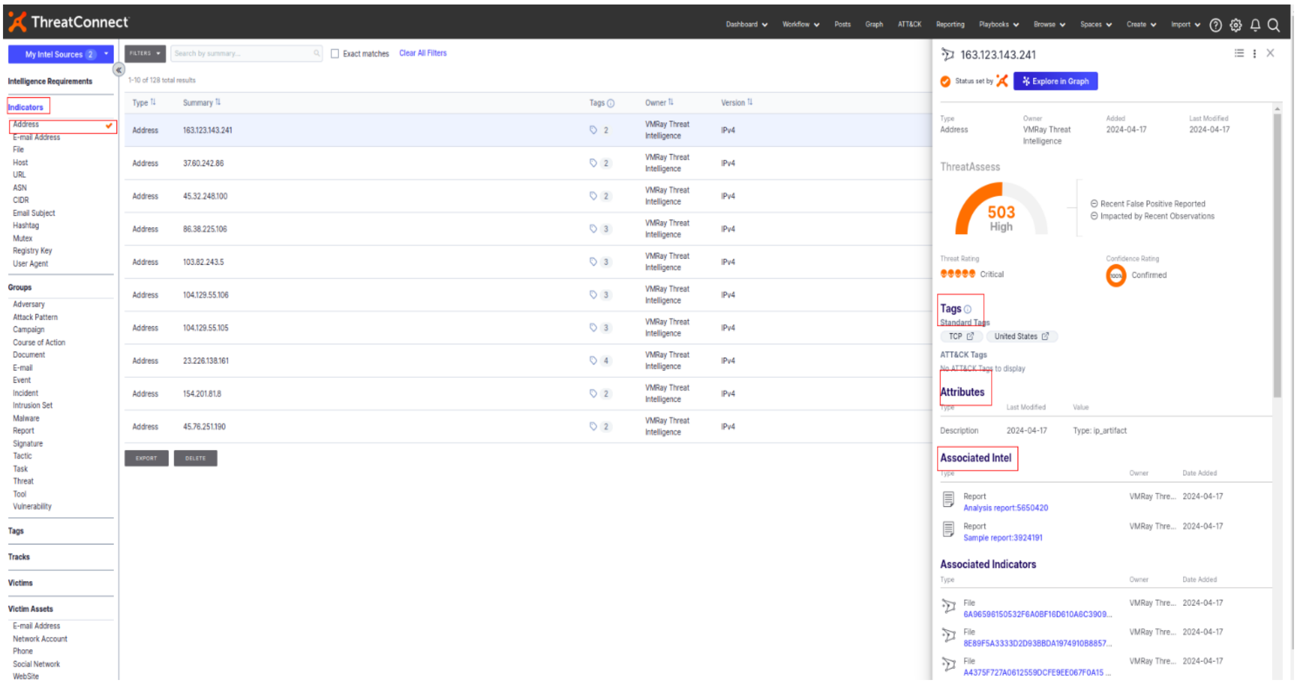
Intel Sources 1

- □ Firebog Airelle Hrsk Domains
- □ Loginsoft PursuitX Intelligence Dev
- □ MalShare Daily Malware List
- □ Manwe Mac Malware
- □ Minotaur URLs
- □ MITRE ATT&CK
- □ OpenPhish
- □ PhishTank
- □ Technical Blogs and Reports
- ☑ VMRay Threat Intelligence
- □ VXVault

Browsing Indicators

IP Address Indicators

To browse **IP Address Feed** from VMRay, select Address Indicator.



□ Exact matches Clear All Filters

1-10 of 128 total results

Type	Summary	Tags	Owner	Version
Address	163.123.143.241	2	VMRay Threat Intelligence	IPv4
Address	37.60.242.86	2	VMRay Threat Intelligence	IPv4
Address	45.32.248.100	2	VMRay Threat Intelligence	IPv4
Address	86.38.225.106	3	VMRay Threat Intelligence	IPv4
Address	103.82.243.5	3	VMRay Threat Intelligence	IPv4
Address	104.129.55.106	3	VMRay Threat Intelligence	IPv4
Address	104.129.55.105	3	VMRay Threat Intelligence	IPv4
Address	23.226.138.161	4	VMRay Threat Intelligence	IPv4
Address	154.201.81.8	2	VMRay Threat Intelligence	IPv4
Address	45.76.251.190	2	VMRay Threat Intelligence	IPv4

163.123.143.241

Status set by

Type	Owner	Added	Last Modified
Address	VMRay Threat Intelligence	2024-04-17	2024-04-17

ThreatAssess

⊖ Recent False Positive Reported
⊖ Impacted by Recent Observations

Threat Rating: Critical

Confidence Rating: 100% Confirmed

Tags

Standard Tags: TCP, United States

ATT&CK Tags

No ATT&CK Tags to display

Attributes

Type	Last Modified	Value
Description	2024-04-17	Type: ip_artifact

Associated Intel

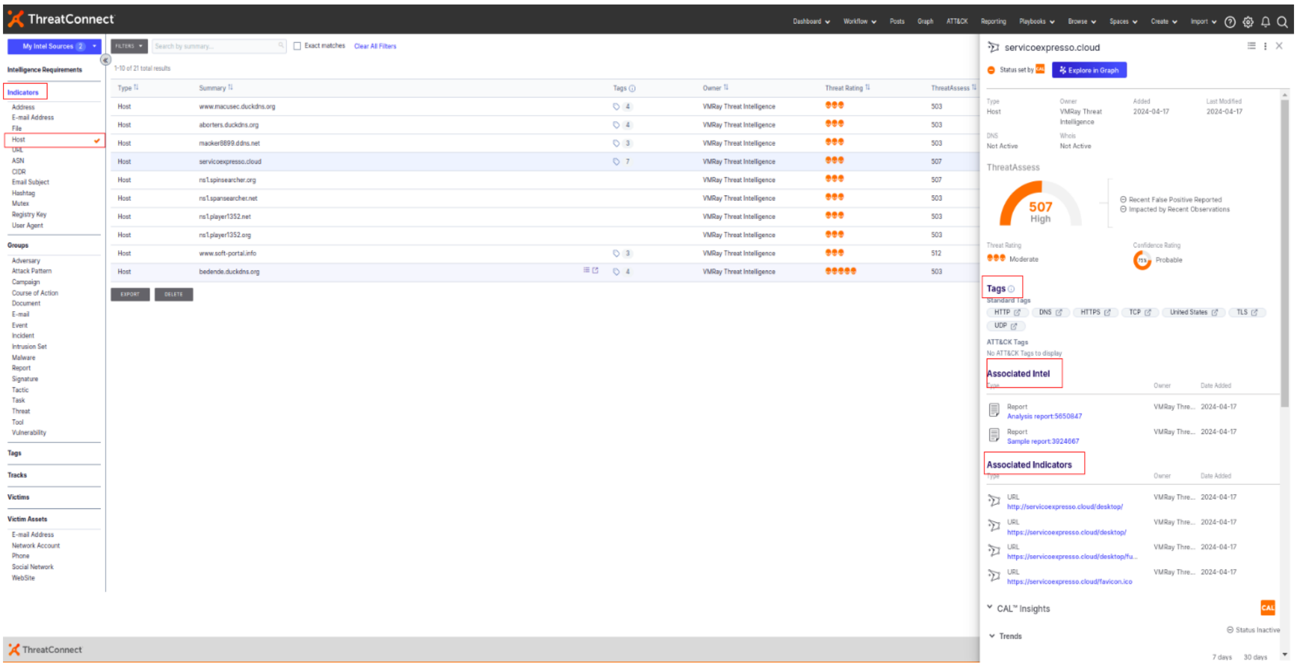
Type	Owner	Date Added
Report Analysis report:5650420	VMRay Thre...	2024-04-17
Report Sample report:3924191	VMRay Thre...	2024-04-17

Associated Indicators

Type	Owner	Date Added
File 6A96596150532F6A0BF16D610A6C3909...	VMRay Thre...	2024-04-17
File 8E89F5A3333D2D93BBDA1974910B8857...	VMRay Thre...	2024-04-17
File A4375F727A0612559DCFE9EE067F0A15 ...	VMRay Thre...	2024-04-17

Host Indicators

To browse **Hosts Feed** from VMRay, select Host Indicator.



1-10 of 21 total results

Type	Summary	Tags	Owner	Threat Rating	ThreatAssess
Host	www.macusec.duckdns.org	4	VMRay Threat Intelligence	●●●	503
Host	aborters.duckdns.org	4	VMRay Threat Intelligence	●●●	503
Host	macker8899.ddns.net	3	VMRay Threat Intelligence	●●●	503
Host	servicoexpresso.cloud	7	VMRay Threat Intelligence	●●●	507
Host	ns1.spinsearcher.org		VMRay Threat Intelligence	●●●	507
Host	ns1.spansearcher.net		VMRay Threat Intelligence	●●●	503
Host	ns1.player1352.net		VMRay Threat Intelligence	●●●	503
Host	ns1.player1352.org		VMRay Threat Intelligence	●●●	503
Host	www.soft-portal.info	3	VMRay Threat Intelligence	●●●	512
Host	bedende.duckdns.org	4	VMRay Threat Intelligence	●●●●●	503

servicoexpresso.cloud

Status set by CAL — Explore in Graph

Type	Owner	Added	Last Modified
Host	VMRay Threat Intelligence	2024-04-17	2024-04-17

DNS: Not Active
Whois: Not Active

ThreatAssess: 507 High
- Recent False Positive Reported
- Impacted by Recent Observations

Threat Rating: ●●● Moderate
Confidence Rating: 75% Probable

Tags
Standard Tags: HTTP, DNS, HTTPS, TCP, United States, TLS, UDP
ATT&CK Tags: No ATT&CK Tags to display

Associated Intel

Type	Owner	Date Added
Report Analysis report:5650847	VMRay Thre...	2024-04-17
Report Sample report:3924667	VMRay Thre...	2024-04-17

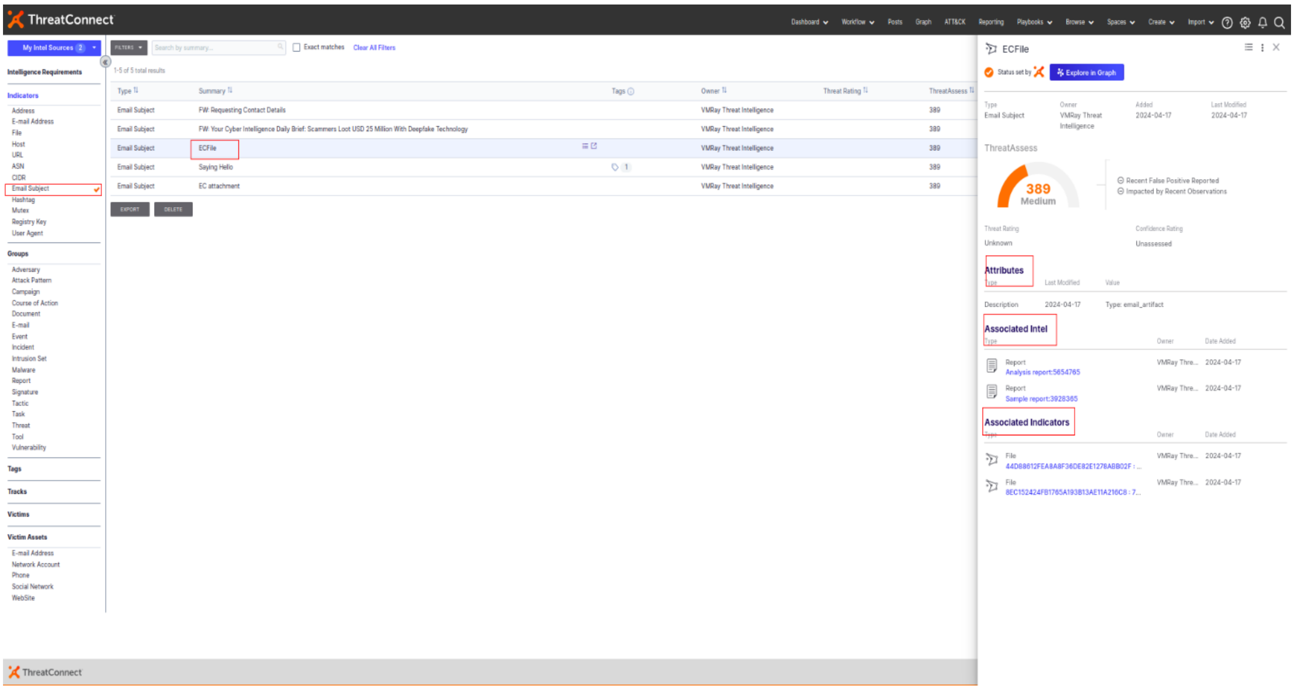
Associated Indicators

Type	Owner	Date Added
URL http://servicoexpresso.cloud/desktop/	VMRay Thre...	2024-04-17
URL https://servicoexpresso.cloud/desktop/	VMRay Thre...	2024-04-17
URL https://servicoexpresso.cloud/desktop/fu...	VMRay Thre...	2024-04-17
URL https://servicoexpresso.cloud/favicon.ico	VMRay Thre...	2024-04-17

CAL™ Insights
Trends
Status Inactive
7 days 30 days

Email Subject Indicators

To browse **Email Subject Feed** from VMRay, select Email Subject Indicator.



1-5 of 5 total results

Type	Summary	Tags	Owner	Threat Rating	ThreatAssess
Email Subject	FW: Requesting Contact Details		VMRay Threat Intelligence		389
Email Subject	FW: Your Cyber Intelligence Daily Brief: Scammers Loot USD 25 Million With Deepfake Technology		VMRay Threat Intelligence		389
Email Subject	ECFile		VMRay Threat Intelligence		389
Email Subject	Saying Hello	1	VMRay Threat Intelligence		389
Email Subject	EC attachment		VMRay Threat Intelligence		389

ECFile

Status set by — Explore in Graph

Type	Owner	Added	Last Modified
Email Subject	VMRay Threat Intelligence	2024-04-17	2024-04-17

ThreatAssess: 389 Medium
- Recent False Positive Reported
- Impacted by Recent Observations

Threat Rating: Unknown
Confidence Rating: Unassessed

Attributes

Type	Last Modified	Value
Description	2024-04-17	Type: email_artifact

Associated Intel

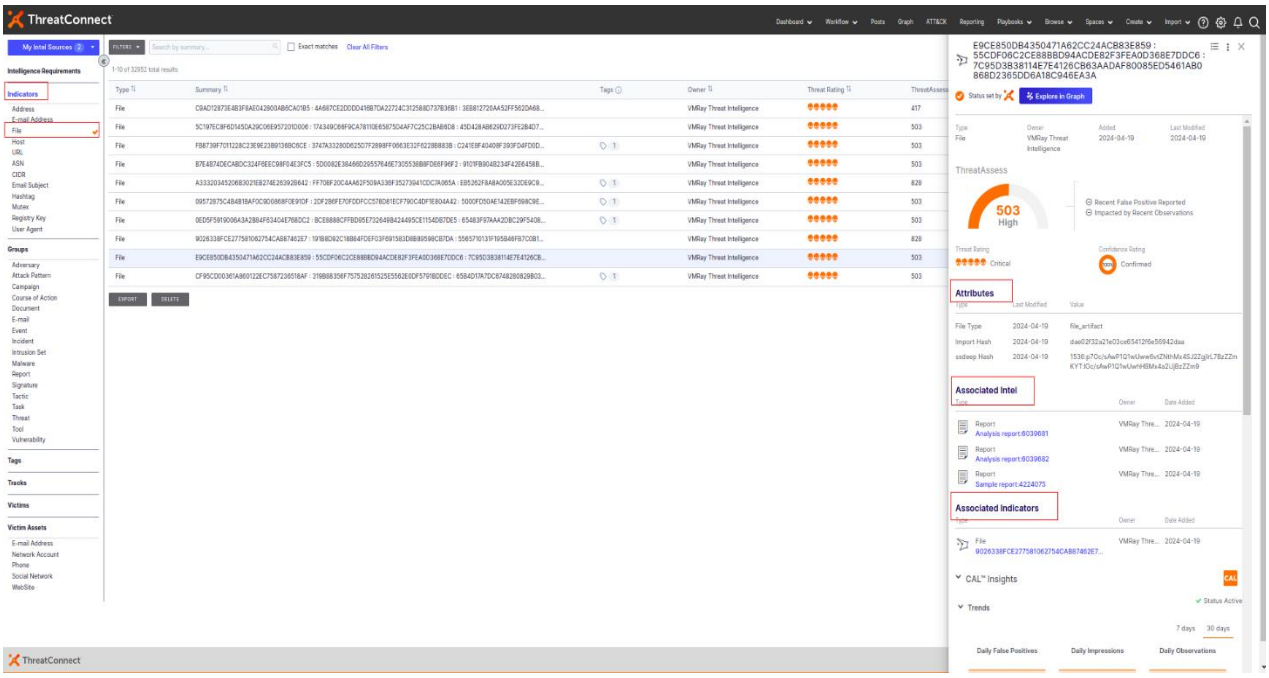
Type	Owner	Date Added
Report Analysis report:5654765	VMRay Thre...	2024-04-17
Report Sample report:3928365	VMRay Thre...	2024-04-17

Associated Indicators

Type	Owner	Date Added
File 44D88612FEA8A8F36DE82E1278ABB02F : ...	VMRay Thre...	2024-04-17
File 8EC152424FB1765A193B13AE11A216C8 : 7...	VMRay Thre...	2024-04-17

File Indicators

To browse **File Feed** from VMRay, select File Indicator.



1-10 of 32952 total results

Type	Summary	Tags	Owner	Threat Rating	ThreatAssess
File	C9AD12873E4B3F8AE042800AB6CA01B5 : 4A687CE2DDDD416B7DA22724C312588D737B36B1 : 3EB812720AA52FF562DA68...		VMRay Threat Intelligence	●●●●●	417
File	5C197EC8F6D145DA29C06E957201D006 : 174349C66F9CA78110E65875D4AF7C25C2BAB6D8 : 45D428AB629D273FE2B4D7...		VMRay Threat Intelligence	●●●●●	503
File	FB8739F7011228C23E9E23B9136BC6CE : 3747A33280D625D7F2898FF0663E32F6228B883B : C241E8F40408F393FD4FD0D...	1	VMRay Threat Intelligence	●●●●●	503
File	B7E4B74DECABDC324F6EEC98F04E3FC5 : 5D0082E38466D29557646E7305538B8FDE6F96F2 : 9101FB904B234F42E6458B...		VMRay Threat Intelligence	●●●●●	503
File	A33320345206B3021EB274E263928642 : FF70BF20C4AA62F509A336F35273941CDC7A065A : EB5262F8A8A005E320E9C9...	1	VMRay Threat Intelligence	●●●●●	828
File	09572875C4B4B1BAF0C9D0868F0E91DF : 2DF2B6FE70FDDFCC578D81ECF790C4DF1E804A42 : 5000FD50AE142EBF698C9E...	1	VMRay Threat Intelligence	●●●●●	503
File	0ED5F5919006A3A2B84F63404E768DC2 : BCE8888CFFBD95E7326498424495CE1154D87DE5 : 65483F97AAA2DBC29F5408...	1	VMRay Threat Intelligence	●●●●●	503
File	9026338FCE277581062754CAB87462E7 : 191B8D92C18884FDEF03F691583D8B89598CB7DA : 5565710131F195B46FB7C0B1...		VMRay Threat Intelligence	●●●●●	828
File	E9CE850DB4350471A62CC24ACB83E859 : 55CDF06C2CE88BBD94ACDE82F3FEA0D368E7DDC6 : 7C95D3B38114E7E4126CB...		VMRay Threat Intelligence	●●●●●	503
File	CF95CD00361A860122EC7587236516AF : 319B88356F757528261525E5562E0DF5791BDDEC : 65B4D17A7DC6748280829B03...	1	VMRay Threat Intelligence	●●●●●	503

E9CE850DB4350471A62CC24ACB83E859 : 55CDF06C2CE88BBD94ACDE82F3FEA0D368E7DDC6 : 7C95D3B38114E7E4126CB63AADAF80085ED5461AB0 868D2365DD6A18C946EA3A

Type	Owner	Added	Last Modified
File	VMRay Threat Intelligence	2024-04-19	2024-04-19

ThreatAssess

503 High

⊖ Recent False Positive Reported
⊖ Impacted by Recent Observations

Threat Rating: ●●●●● Critical

Confidence Rating: 100% Confirmed

Attributes

Type	Last Modified	Value
File Type	2024-04-19	file_artifact
Import Hash	2024-04-19	dae02f32a21e03ce65412f6e56942daa
ssdeep Hash	2024-04-19	1536:p7Oc/sAwP1Q1wUww6vtZNthMx4SJ2ZgjlrL7BzZZmKYT:lOc/sAwP1Q1wUwhHBMx4a2iJjBzZZm9

Associated Intel

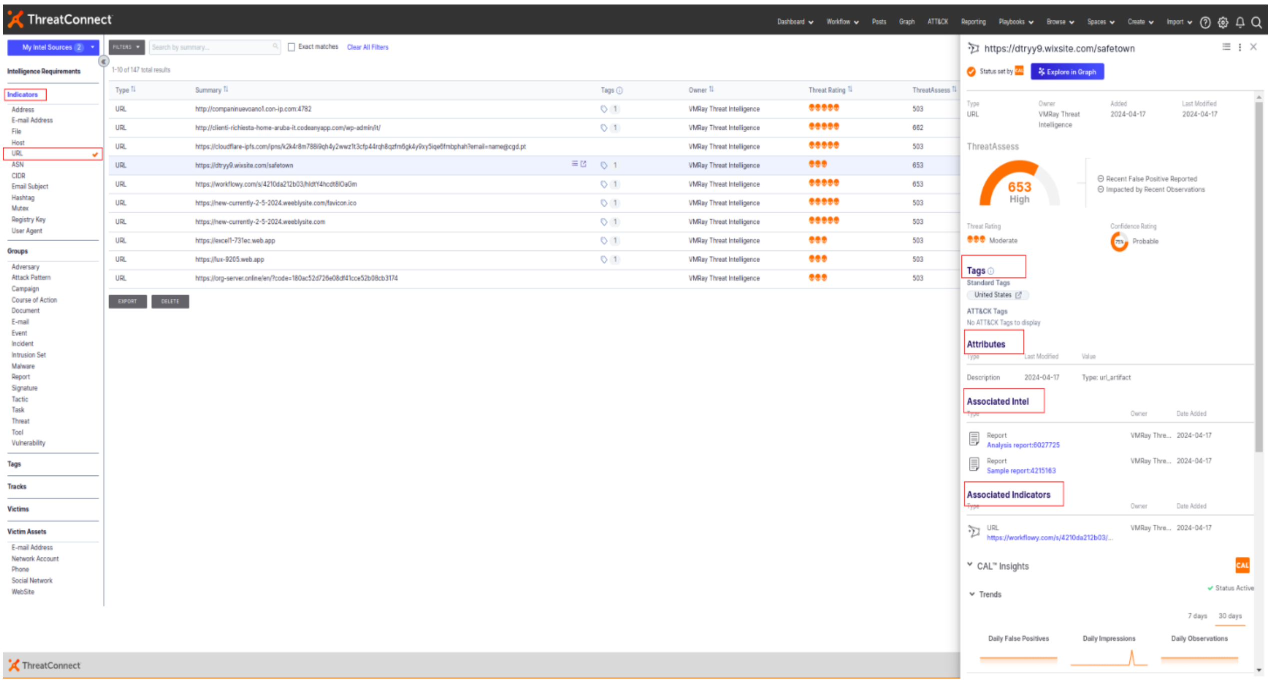
Type	Owner	Date Added
Report Analysis report:6039681	VMRay Thre...	2024-04-19
Report Analysis report:6039682	VMRay Thre...	2024-04-19
Report Sample report:4224075	VMRay Thre...	2024-04-19

Associated Indicators

Type	Owner	Date Added
File 9026338FCE277581062754CAB87462E7...	VMRay Thre...	2024-04-19

URL Indicators

To browse **URL Feed** from VMRay, select URL Indicator.



1-10 of 147 total results

Type	Summary	Tags	Owner	Threat Rating	ThreatAssess
URL	http://companinuevoano1.con-ip.com:4782	1	VMRay Threat Intelligence	●●●●●	503
URL	http://clienti-richiesta-home-aruba-it.codeanyapp.com/wp-admin/it/	1	VMRay Threat Intelligence	●●●●●	662
URL	https://cloudflare-ipfs.com/ipns/k2k4r8m788i9qh4y2wwz1t3cfp44rqh8qzfm6gk4y9xy5iqe6fmbphah?email=name@cgd.pt		VMRay Threat Intelligence	●●●●●	503
URL	https://dtryy9.wixsite.com/safetown	1	VMRay Threat Intelligence	●●●	653
URL	https://workflowy.com/s/4210da212b03/hldtY4hcdt8IOaGm	1	VMRay Threat Intelligence	●●●●●	653
URL	https://new-currently-2-5-2024.weeblysite.com/favicon.ico	1	VMRay Threat Intelligence	●●●●●	503
URL	https://new-currently-2-5-2024.weeblysite.com	1	VMRay Threat Intelligence	●●●●●	503
URL	https://excel1-731ec.web.app	1	VMRay Threat Intelligence	●●●	503
URL	https://lux-9205.web.app	1	VMRay Threat Intelligence	●●●	503
URL	https://org-server.online/en/?code=180ac52d726e08df41cce52b08cb3174		VMRay Threat Intelligence	●●●	503

https://dtryy9.wixsite.com/safetown

Status set by CAL Explore in Graph

Type	Owner	Added	Last Modified
URL	VMRay Threat Intelligence	2024-04-17	2024-04-17

ThreatAssess

653 High

⊖ Recent False Positive Reported
⊖ Impacted by Recent Observations

Threat Rating ●●● Moderate

Confidence Rating 75% Probable

Tags

Standard Tags

United States

ATT&CK Tags

No ATT&CK Tags to display

Attributes

Type	Last Modified	Value
Description	2024-04-17	Type: url_artifact

Associated Intel

Type	Owner	Date Added
Report Analysis report:6027725	VMRay Thre...	2024-04-17
Report Sample report:4215163	VMRay Thre...	2024-04-17

Associated Indicators

Type	Owner	Date Added
URL https://workflowy.com/s/4210da212b03/...	VMRay Thre...	2024-04-17

CAL™ Insights

Trends

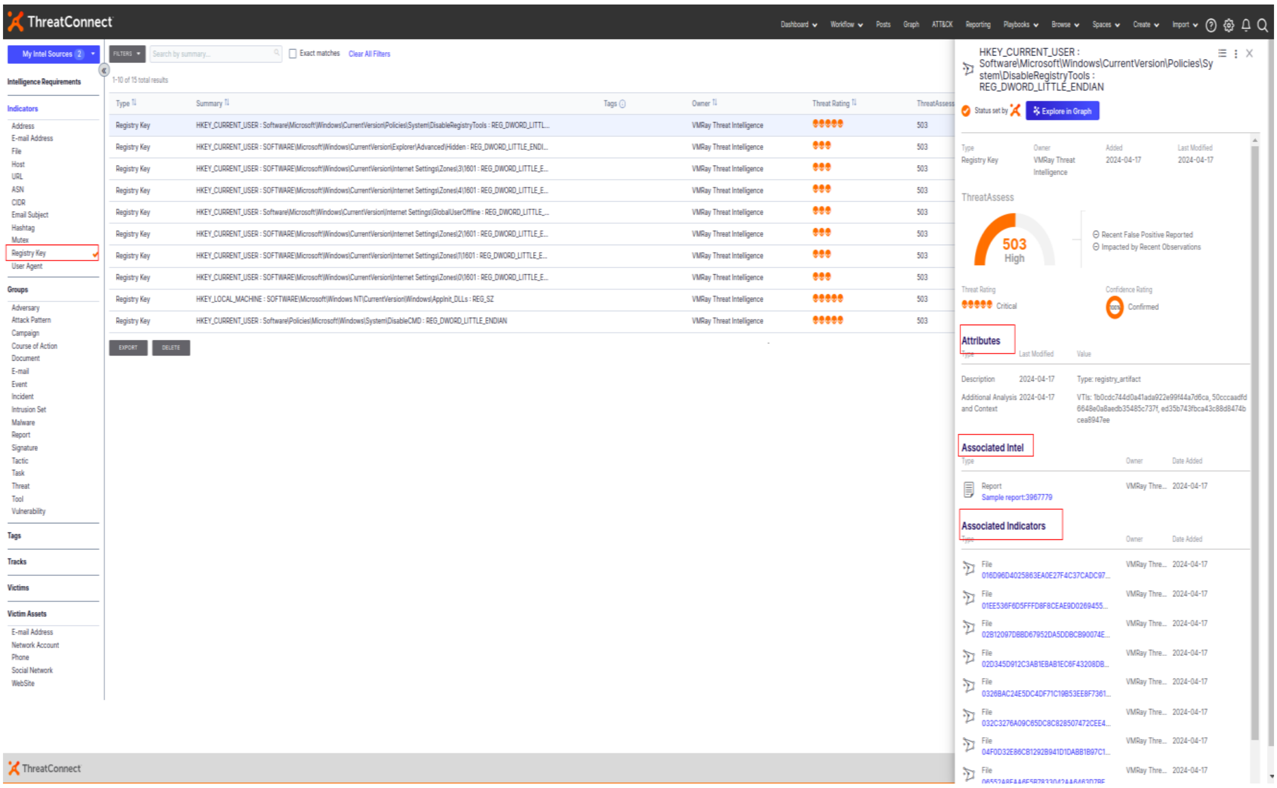
✓ Status Active

7 days 30 days

Daily False Positives Daily Impressions Daily Observations

Registry Key Indicators

To browse **Registry Key Feed** from VMRay, select Registry key Indicator.



1-10 of 15 total results

Type	Summary	Tags	Owner	Threat Rating	ThreatAssess
Registry Key	HKEY_CURRENT_USER : Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableRegistryTools : REG_DWORD_LITTL...		VMRay Threat Intelligence	●●●●●	503
Registry Key	HKEY_CURRENT_USER : SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Hidden : REG_DWORD_LITTLE_ENDI...		VMRay Threat Intelligence	●●●	503
Registry Key	HKEY_CURRENT_USER : SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\1601 : REG_DWORD_LITTLE_E...		VMRay Threat Intelligence	●●●	503
Registry Key	HKEY_CURRENT_USER : SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4\1601 : REG_DWORD_LITTLE_E...		VMRay Threat Intelligence	●●●	503
Registry Key	HKEY_CURRENT_USER : Software\Microsoft\Windows\CurrentVersion\Internet Settings\GlobalUserOffline : REG_DWORD_LITTLE_...		VMRay Threat Intelligence	●●●	503
Registry Key	HKEY_CURRENT_USER : SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2\1601 : REG_DWORD_LITTLE_E...		VMRay Threat Intelligence	●●●	503
Registry Key	HKEY_CURRENT_USER : SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1\1601 : REG_DWORD_LITTLE_E...		VMRay Threat Intelligence	●●●	503
Registry Key	HKEY_CURRENT_USER : SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0\1601 : REG_DWORD_LITTLE_E...		VMRay Threat Intelligence	●●●	503
Registry Key	HKEY_LOCAL_MACHINE : SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs : REG_SZ		VMRay Threat Intelligence	●●●●●	503
Registry Key	HKEY_CURRENT_USER : Software\Policies\Microsoft\Windows\System\DisableCMD : REG_DWORD_LITTLE_ENDIAN		VMRay Threat Intelligence	●●●●●	503

HKEY_CURRENT_USER :
Software\Microsoft\Windows\CurrentVersion\Policies\Sy
stem\DisableRegistryTools :
REG_DWORD_LITTLE_ENDIAN

Status set by Explore in Graph

Type	Owner	Added	Last Modified
Registry Key	VMRay Threat Intelligence	2024-04-17	2024-04-17

ThreatAssess

503 High

⊖ Recent False Positive Reported
⊖ Impacted by Recent Observations

Threat Rating ●●●●● Critical

Confidence Rating 100% Confirmed

Attributes

Type	Last Modified	Value
Description	2024-04-17	Type: registry_artifact
Additional Analysis and Context	2024-04-17	VTIs: 1b0cdc744d0a41ada922e99f44a7d6ca, 50cccaadfd6648e0a8aedb35485c737f, ed35b743fbca43c88d8474bcea8947ee

Associated Intel

Type	Owner	Date Added
Report Sample report:3967779	VMRay Thre...	2024-04-17

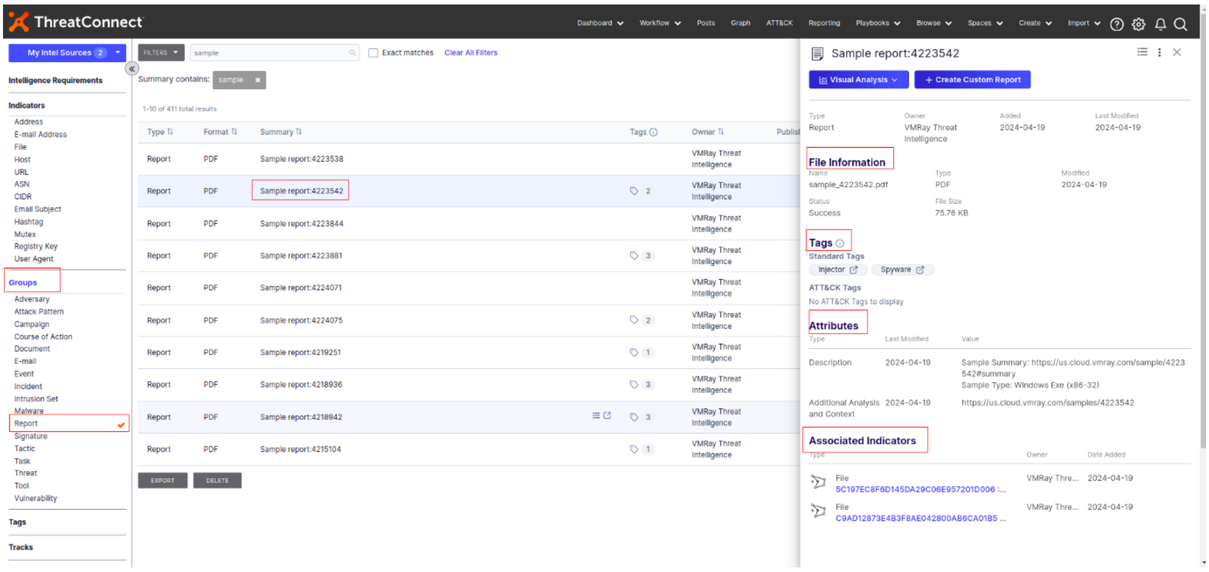
Associated Indicators

Type	Owner	Date Added
File 016D96D4025863EA0E27F4C37CADC97...	VMRay Thre...	2024-04-17
File 01EE536F6D5FFFD8F8CEAE9D0269455...	VMRay Thre...	2024-04-17
File 02B12097DBBD67952DA5DDBCB90074E...	VMRay Thre...	2024-04-17
File 02D345D912C3AB1EBAB1EC6F43208DB...	VMRay Thre...	2024-04-17
File 0326BAC24E5DC4DF71C19B53EE8F7361...	VMRay Thre...	2024-04-17
File 032C3276A09C65DC8C828507472CEE4...	VMRay Thre...	2024-04-17
File 04F0D32E86CB1292B941D1DABB1B97C1...	VMRay Thre...	2024-04-17
File 06552A8FAA6F5B7833042AA6463D7BF	VMRay Thre...	2024-04-17

Browsing Groups

Reports

To browse **Sample and Analysis Report** from VMRay, select **Report** Group.



Summary contains: sample

1-10 of 411 total results

Type	Format	Summary	Tags	Owner
Report	PDF	Sample report:4223538		VMRay Threat Intelligence
Report	PDF	Sample report:4223542	2	VMRay Threat Intelligence
Report	PDF	Sample report:4223844		VMRay Threat Intelligence
Report	PDF	Sample report:4223881	3	VMRay Threat Intelligence
Report	PDF	Sample report:4224071		VMRay Threat Intelligence
Report	PDF	Sample report:4224075	2	VMRay Threat Intelligence
Report	PDF	Sample report:4219251	1	VMRay Threat Intelligence
Report	PDF	Sample report:4218936	3	VMRay Threat Intelligence
Report	PDF	Sample report:4218942	3	VMRay Threat Intelligence
Report	PDF	Sample report:4215104	1	VMRay Threat Intelligence

Sample report:4223542

Type	Owner	Added	Last Modified
Report	VMRay Threat Intelligence	2024-04-19	2024-04-19

File Information

Name	Type	Modified
sample_4223542.pdf	PDF	2024-04-19

Status	File Size
Success	75.76 KB

Tags

Standard Tags: Injector, Spyware

ATT&CK Tags: No ATT&CK Tags to display

Attributes

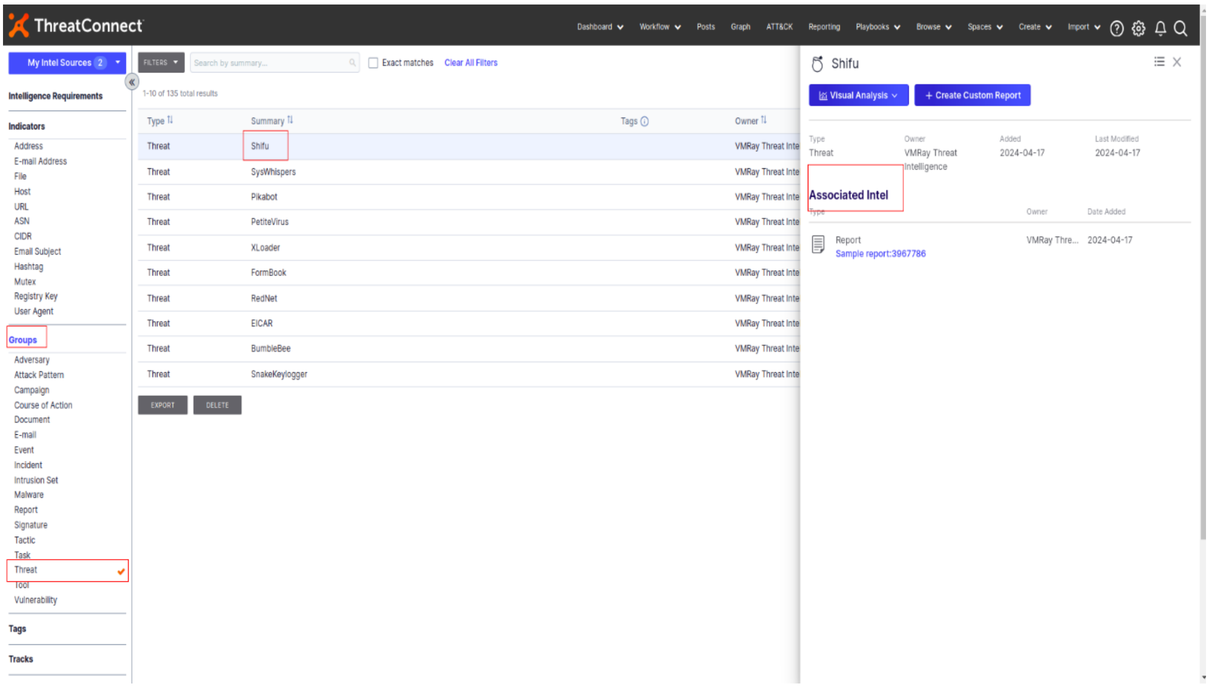
Type	Last Modified	Value
Description	2024-04-19	Sample Summary: https://us.cloud.vmray.com/sample/4223542#summary Sample Type: Windows Exe (x86-32)
Additional Analysis and Context	2024-04-19	https://us.cloud.vmray.com/samples/4223542

Associated Indicators

Type	Owner	Date Added
File 5C197EC8F6D145DA29C06E957201D006 :...	VMRay Thre...	2024-04-19
File C9AD12873E4B3F8AE042800AB6CA01B5 ...	VMRay Thre...	2024-04-19

Threats

To browse **Threat Names** from VMRay, select Threat Group.



1-10 of 135 total results

Type	Summary	Tags	Owner
Threat	Shifu		VMRay Threat Inte
Threat	SysWhispers		VMRay Threat Inte
Threat	Pikabot		VMRay Threat Inte
Threat	PetiteVirus		VMRay Threat Inte
Threat	XLoader		VMRay Threat Inte
Threat	FormBook		VMRay Threat Inte
Threat	RedNet		VMRay Threat Inte
Threat	EICAR		VMRay Threat Inte
Threat	BumbleBee		VMRay Threat Inte
Threat	SnakeKeylogger		VMRay Threat Inte

Shifu

Type	Owner	Added	Last Modified
Threat	VMRay Threat Intelligence	2024-04-17	2024-04-17

Associated Intel

Type	Owner	Date Added
Report Sample report:3967786	VMRay Thre...	2024-04-17

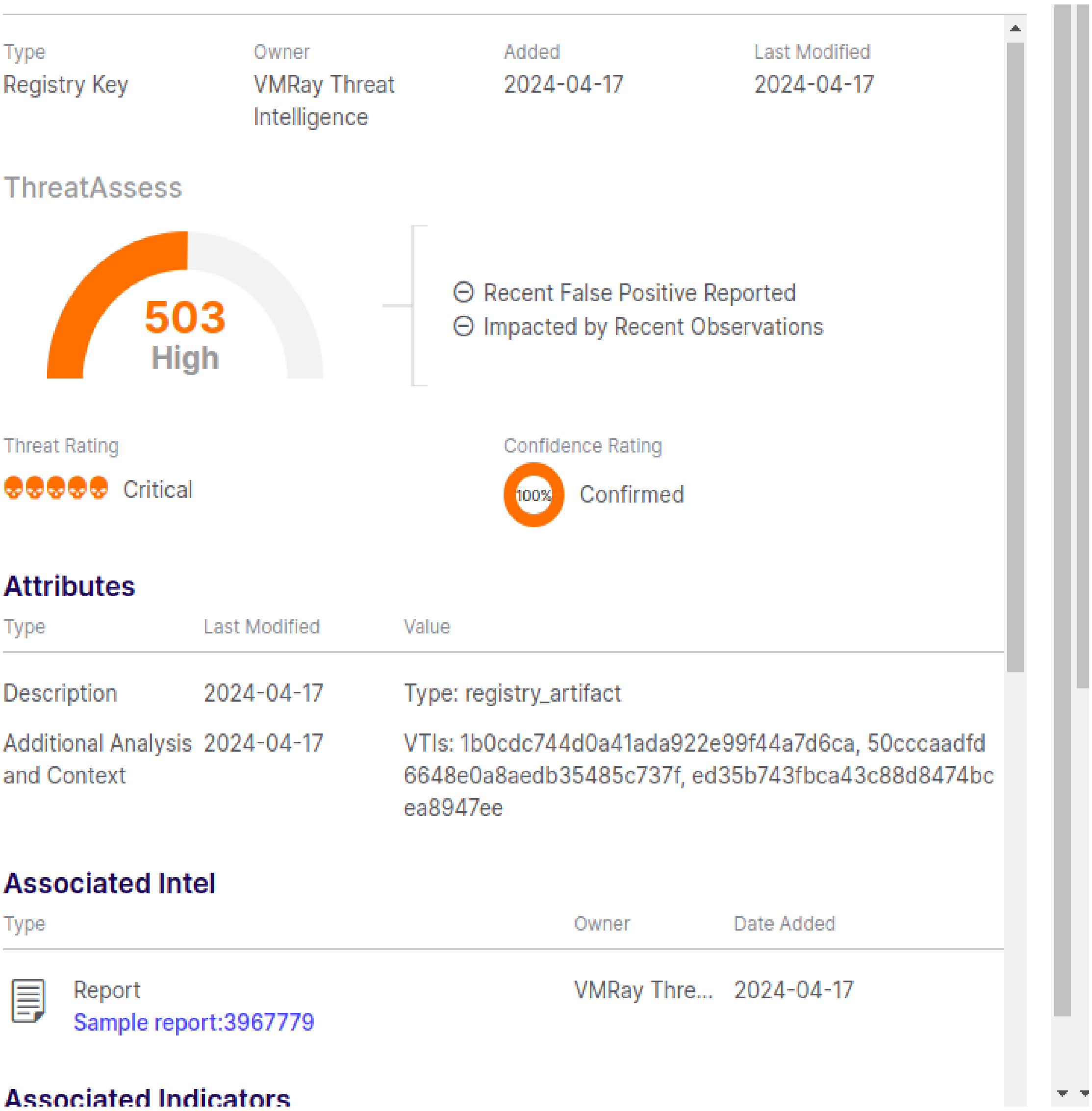
VMRay RatingsVMRay indicators use threat impacting verdict with URLs, domains, files, and IPs, Registry Key:

- Malicious
- Suspicious

Indicator Threat Rating Mapping – VMRay to ThreatConnect

- Malicious: Critical (5 skulls),
- Suspicious: Moderate (3 skulls)

The example below is a Registry key indicator, designated by VMRay with a Malicious impact verdict. In addition, VMRay will be 100% confirmed in the Confidence Rating field if indicator is malicious or 75% probable if indicator is suspicious.



Type	Owner	Added	Last Modified
Registry Key	VMRay Threat Intelligence	2024-04-17	2024-04-17

ThreatAssess

503 High

⊖ Recent False Positive Reported
⊖ Impacted by Recent Observations

Threat Rating
☠☠☠☠☠ Critical

Confidence Rating
100% Confirmed

Attributes

Type	Last Modified	Value
Description	2024-04-17	Type: registry_artifact
Additional Analysis and Context	2024-04-17	VTIs: 1b0cdc744d0a41ada922e99f44a7d6ca, 50cccaadfd6648e0a8aedb35485c737f, ed35b743fbca43c88d8474bcea8947ee

Associated Intel

Type	Owner	Date Added
Report Sample report:3967779	VMRay Thre...	2024-04-17

Associated Indicators

Release Notes

App Version	Release Date	Details

1.0.0		Initial Release.

Support

For assistance with this App, to report a bug, or feature requests please contact us via the following.

Support Portal	https://www.vmray.com/contact/support/
Email	Support@VMRay.com