

In Curation We Trust: Generating Contextual & Actionable Threat Intelligence

Michel Coene Robert Nixon

2022-09-30 TLP:White





Michel Coene

Robert Nixon

www.nviso.eu | 2

Content

What we will dive into today





www.nviso.eu | 3

Threat Intelligence Platform (TIP)

What is MISP?

MISP is an open-source threat intelligence and sharing platform.

Community project and cofinanced by the European Union

Used by many organizations across the world to share threat related data



NVISO

https://www.misp-project.org/



4

The problem

What everyone has done seen before, at least once



Threat Intelligence

Consuming & producing

NVISO MDR Managed Detect & Respond

• TI consumer

- TI producer
- SOC monitoring of our clients
- Anonymized threat data is fed back in the MDR MISP instance for future correlation
- Threat hunting

NVISO CSIRT Incident Response Team

- TI consumer
- TI producer
- Incident Response cases
- Malware Analysis
- Compromise Assessments

NVISO CTI Cyber Threat Intelligence

NVISO

- TI consumer
- TI producer
- Threat intelligence integrations
- TI Monitoring (Creds, Data Leakage)
- Threat Intel Feeds
- Tailored threat briefings
- Threat landscape reports
- Threat Intel based Red Teaming (TIBER)
- Vulnerability intelligence







digital shadows_

The architecture

The first step in an attempt to solve the problem

NVISO



Problem exemplars

Recipe for sub-optimal detection

NVISO



Lack of contextualisation or inconsistencies

tlp:white

Actionable?

Warning: Potential false positives (show)

- List of known Cloudflare IP ranges
- List of known Office 365 URLs
- Top 1,000,000 most-used sites from Tranco
- Top 10K most-used sites from Tranco
- List of RFC 1918 CIDR blocks



TLP:WHITE	Tags	#Attr. ↑
TLP: white		86089
-CERT:TLP="white" Threat tlp:White	malware	82870
marking:TLPMarking="WHITE"	 ⊘ green ⊘ malware 	76103
:traffic-light-protocol="WHITE"		757/2
100.000.00		13142

The curation procedure

In practical terms, what do we do?



Remove false positives

MISP warning lists Custom warning lists Analyst judgement

Add contextualization

Mandatory TLP tags Intel source Relations, comments and objects Target info, threat actor, sectors, MITRE ATT&CK tags, ...

Verify **relevance**, completeness and **quality** "Useful" Sanity check If this alerts, is there enough context?

An attempt to solve the problem

Curation depends on the server we're being executed

:param remove tag: Remove this tag from events

def __init__(self, logger, custom_tag, remove_tag):

self.source_tag = "nviso-cti:source=\"{}\""

self.misp = ExpandedPyMISP(misp_url, misp_key, misp_verifycert,

Class to curate NVISO events

:param logger: logger object :param custom_tag: Add this tag to events

self.custom tag = custom tag

self.remove tag = remove tag

self.logger = logger







Remove tag "complete"

if self.remove_tag:

result_tag = self.misp.untag(uuid, self.remove_tag)

self.logger.debug("Untag event {} - {} {}".format(uuid, misp_event.info, self.remove_tag))

ID 1	Name	Version	Description	Category
145	List of known Limelight CDN IPs	1	List of known Limelight CDN IPs	False positive
144	NITRO URL False Positives	39	False Positive URLs as observed by the NVISO Intelligence and Threat Response Operations.	False positive
143	NITRO Hashes False Positives	41	False Positive Hashes as observed by the NVISO Intelligence and Threat Response Operations.	False positive
142	NITRO Domain False Positives	39	False Positive Domains as observed by the NVISO Intelligence and Threat Response Operations.	False positive
140	NITRO Registry False Positive	39	False Positive Registry Keys as observed by the NVISO Intelligence and Threat Response Operations.	False positive
139	List of known Azure IPs	2	Azure data centers, edge nodes etc.	False positive
136	NVISO False Positive List	6	Indicators that are found to be false positives by the CTI team	False positive

elif tag.name.strip() == "TLP:White" or tag.name.strip() == "TLP: White" or tag.name.strip() == "TLP:WHI
self.misp.untag(uuid, tag.id)
result_tag = self.misp.tag(uuid, "tlp:white")

Add source of this event

if include_source:

servername = self.get_server(int(server))

source_tag = self.source_tag.format(servername)

www.nviso.eu | 10

Automated Curation

Automation is key!



Manual Curation

NVISO





MISP Warninglists

Shareable lists of potential false positives

		Documentation - warninglist						c	ORGP
	neurenn -	Bocumentation - warningilist				Warning: Potentia	false positives (sho	v)	
Name	Version	Description	Category Typ	be Entries		List of RFC 5735 CIDR block	5		
NITRO IP False Positives	3	False Positive IPs as observed by the NVISO Intelligence and Threat Response Operations.	False positive cid	r 3		List of RPC 1916 CIDR block	3		_
List of known Limelight CDN IPs	1	List of known Limelight CDN IPs	False positive cid	r 113					
NITRO Registry False Positive	5	False Positive Registry Keys as observed by the NVISO Intelligence and Threat Response Operations.	False positive stri	ng 11 -					
NITRO Domain False Positives	18	False Positive Domains as observed by the NVISO Intelligence and Threat Response Operations.	False positive stri	ng 135					
NITRO Hashes False Positives	34	False Positive Hashes as observed by the NVISO Intelligence and Threat Response Operations.	False positive stri	ng 294					
NITRO URL False Positives	7	False Positive URLs as observed by the NVISO Intelligence and Threat Response Operations.	False positive stri	ng 26					
List of known hashes for benign files	1	Event contains one or more benign files based on known hashes, see https://github.com/RichieB2B/nioc	False positive stri	ng 197415					
List of known Gmail sending IP ranges	20220810	List of known Gmail sending IP ranges (https://support.google.com/a/answer/27642?hl=en)	False positive cid	r 27					
CRL and OCSP domains	20220810	Domains that belongs to CRL or OCSP	False positive stri	ng 253					
List of known Wikimedia address ranges	20220810	Wikimedia address ranges (http://noc.wikimedia.org/conf/reverse-proxy.php.txt)	False positive cid	r 48					
TLDs as known by IANA	20220810	Event contains one or more TLDs as attribute with an IDS flag set	False positive stri	ng 1487					
Hashes that are often included in IOC lists but are false positives.	1	Hashes that are often included in IOC lists but are false positives.	False positive stri	ng 24644					
List of RFC 6598 CIDR blocks	5	Event contains one or more entries part of the Shared Address Space CIDR blocks (RFC 6598)	False positive cid	r 1					
List of RFC 5735 CIDR blocks	5	Event contains one or more entries part of the Special Use IPv4 Addresses CIDR blocks (RFC 5735)	False positive cid	r 15					
List of RFC 1918 CIDR blocks	5	Event contains one or more entries part of the private network CIDR blocks (RFC 1918)	False positive cid	r 3					
		<pre>c previous not s view pt + III II: x Score kogle - ● Denked II: Docy score At System(50) ● Contot ↓</pre>	Related Tags Y Filtering t	ool			En	er value to search	٩
		Date T Org Category Type Value 2001 05 09 Network article and the store of the 192.168.0.0/16: List of RFC 5	735 CIDR blocks		Correlate Related Events	Feed hits ID	S Distribution Sig	htings Activity Actions	

192,168,0,0/16: List of RFC 1918 CIDR block

Source: https://www.circl.lu/doc/misp/warninglists/

https://github.com/MISP/misp-warninglists

No need repeating

"Offender list" and blocklist



Synchronise offender lists between MISP servers

« p	revious next »			
ld	Organisation name	UUID	Created 1	Comment
•	2010	AND THE REPORT OF	2022-05-09 18:33:59	Very low quality, extremely large events with very high amount of FP's
	10.04	Which will Havinds Stationers	2022-04-05 09:54:08	Generic sandbox output, non-filtered, nonsensical
	10010-018-01	100008-008-012000-022000217	2021-10-13 08:31:00	Low quality intel, no attributes marked or markable as IDS true
10		Without and and out only wanted in	2021-09-22 08:48:29	
	0.001108	Charles of the Art Contra particular The	2021-07-29 14:39:57	Lots of low quality cuckoo analysis events.
	Charles (PTL an	The Princip Calvery Automotive Principality	2021-05-12 10:42:53	Low quality
	0547	WHEN BY NAMES AND A	2021-04-02 11:57:14	Scanner / Source IPs > 1000 hits, low value

for uuid in diff_source_blocklist_uuids:

Organisation Blocklists

payload = json.dumps({"returnFormat": "json", "uuid": uuid})

search_results = requests.request("POST", search_dest_url, headers=dest_headers, data=payload, verify=False)
if len(search_results.json()['response']) != 0:

try:

delete_response = requests.request("DELETE", delete_dest_url + uuid, headers=dest_headers, verify=False)
delete_response.raise_for_status()

deleted_count += 1

except requests.exceptions.HTTPError as err:

print(err)

Statistics

What have we seen so far?

3,492 events

1,894,155 attributes

16 blocklisted organisations

NVISO

NVISO Statistics 🗹 👕

Events: 3492 Events this month: 138 Events this month completed curation: 138 Events this month waiting curation: 0 Events this month without curation status: 0 Events this month tlp:white: 117 Events this month tlp:green: 16 Events this month tlp:amber: 5

Attributes: 1894155 Attributes this month: 9160 Attributes / event: 542 Correlations: 59835

Users: 7 Organisations: 607 Blocklisted organisations: 16 (2.64 %) Local organisations: 1 Event creator orgs: 171 Average users / org: 7

Other scripts to complement our curation

NVISO

False positives

Remove *or* tag NSRL matches – Uses Hashlookup web service hosted by CIRCL
 Sync custom warninglists with NVISO NITRO MDR service

Relevant indicators

•Deactivate indicators after a grace period - cronjob to turn off IDS flag at a certain age •Advanced decaying of indicators, can use Decaying Models in MISP

Scrape web sources

- •Collect OSINT (RSS Feeds or Manually via URL submission)
- •MISP reports generated automatically (html-to-markdown, supported via mermaid with IoC extraction and tagging!)
- •https://www.misp-project.org/2022/08/08/MISP-scraper.html/

Bulk delete events

- •Events with non-relevant information
- •You need a backup plan

Workflows in MISP

		Input Filters	Global Actions												*		Robertnixon 🖂	
View Event	test																	
View Correlation Graph																		
View Event History	Event ID	3																
Edit Event	UUID	29a6a1f9-4b55	-4ade-955e-8a404	158a01e3 🖶 🔜														
Delete Event	Creator org	Sylok Tools																
Add Attribute	Owner org	Sylok Tools																
Add Object	Creator user	robertnixon@sy	lok.tools															
Add Attachment Add Event Report	Protected Event (experimental)	Event is in ur Switch to pro	nprotected mode. stected mode															
Populate from	Tags	S tip:clear	× 🛛 + 🕹 +															
Enrich Event	Date	2022-08-22																
Merge attributes from	Threat Level	A High																
Publish Event	Analysis	Initial																
Publish (no email)	Distribution	This community	only	> <														
Contact Reporter Download as	Warnings	TLP: Unknown TL	.P tag, please ref	er to the TLP taxo	onomy as to what	is valid, othe	rwise filtering rule	s created by your	partners may miss y	our intent.			45					
List Events	Published	No																
Add Event	#Attributes	1 (0 Objects)																
	First recorded change	2022-08-22 13:	36:12															
	Last change	2022-08-22 13:	39:51															
	Modification map		^															
	Sightings	0 (0) - restricted	d to own organisat	ion only. 🔎														
	-Pivots -Galaxy -	Event graph + Eve	ent timeline 🕂 Co	rrelation graph 🚽	ATT&CK matrix	+ Event repor	rts — Attributes ·	- Discussion										
	× 3: test																	
	Galaxies																	
	⊗+ ≗+																	
	« previous next »	view all																
	+ ≣ ≞ ×	Scope toggle -	Deleted	🗠 Decay score	A Sighting DB	Context	TRelated Tags	T Filtering tool							Enter	value to s	earch	Q X
	Date 1 Org	Category	Туре	Value		Tags	Galaxies	Comment		Correlate	Related Events	Feed hits	٤	IDS Dis	stribution	Sightings	Activity Actio	ns
	C 2022 08 22	Artifacte dropp	ood md5	201242021774220	42204200146/b2o1					-	0				orit .		*	

Lessons Learned

Key components to make this work

NVISO

Tooling

- Customisation is key
- Automate as much as possible
- Extend what is available
- ZMQ and Python
 - Some conflicts here with the new Workflow functionality
- Platform features
- Taxonomies (workflow tags)
- Galaxies and clusters

Documentation

- Server architecture
- MISP synchronization data flows
- There is a limit to what you can automate
- Operating procedures for analysts
- Multiple analysts but same procedure

Communication

- Involve stakeholders at the appropriate time
- Gather and validate your Primary Intelligence Requirement (PIRs)
- Let TI consumers signal the quality of TI
- Rinse and repeat

Future State

NVISO

Roadmap

Integrate MISP workflows (New MISP feat.)

•Shareable Workflow blueprints, there is a unique Github repo to share blueprints!

•Create new modules for Workflows

•Implement the new Periodic Notifications functionality

Contribute back to community

•Event proposals

Sightings

Resources

•Mature processes

'Announcements'

•Create bot (Slack, Teams, ...) that alert when new events are in (Great place for a webhook using the new Workflows!)

Open source scripts

•Generalise code for wider use •https://github.com/NVISOsecurity/nviso-cti



THANK YOU!

Michel Coene Robert Nixon



threatintel@nviso.eu https://github.com/NVISOsecurity/nviso-cti

2022-09-30 TLP:White