

Introduction to MISP

Sam Perl,

CSIRT Development and Training Team,

CERT, SEI, Carnegie Mellon University

Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213

[Distribution Statement A] Approved for public release and unlimited distribution.

Copyright 2021 Carnegie Mellon University.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

DM21-0775

Introduction

Cybersecurity Incident Response teams want to

- Have a way to receive (trusted) data from other teams
- Ideally reduce duplication during analysis
- Move toward automated solutions where possible and appropriate
- Restrict access to certain data according to policy/practices

Information Sharing

- Can help enable private and public IT-communities to share a wide range of information.
- Sharing indicators of compromise, artifacts, <u>context</u>, TTP, and more within a community can have direct impact on reaction capability.

• Can help with prevention, detection, and response

Information Sharing Platforms

A platform may perform a variety of security tasks to help defenders such as:

- Receive data about threats from other network participants or publicly available data sources
- Help analysts perform correlation analysis between events such as 'linking' them together
- Allow analysts to add metadata to values such as URLs, Domain names, Filenames, Hash values, and much more
- Integrate with other services such as malware sandbox analysis and importing results (enrichment)
- Integrate with defensive tools including Firewalls, Intrusion Detection Systems (IDS), SIEM, or other programmable network/host event sensors such as Zeek (formerly Bro)

Sharing Platforms are only as valuable as the data they contain

- All of the platform use cases require the receipt of useful, timely, and 'actionable' security data.
- Data that is out of date or incorrect can cause unnecessary outages rather than prevent against attacks.
- Using incorrect and inaccurate cyber intelligence can lead to many other security failures.
- There are many teams that provide data for others to use (often called *Feeds*), but **careful** examination of each dataset is recommended.

Malware Information Sharing Platform



(now used for more than malware)

Key Features:

- Store, share, collaborate on cyber security indicators, malware analysis, and use to detect and prevent attacks or threats.
- Support for Events to have tags, to apply different taxonomies,
- Multi-layered Sharing groups for multiple organizations with permissions and protocols (including TLP)
- Import/Export events in various formats including indicator extraction via Regex
- Linking of attributes (observables and IOCs) between Events

Example Use

Carnegie Mellon University Software Engineering Institute

© 2021 Carnegie Mellon University

 $[\ensuremath{\mathsf{DISTRIBUTION}}\xspace$ STATEMENT A] Approved for public release and unlimited distribution.

Typical Artifact and IOC flow

- 1. Receive an alert, Create and Work a case
- 2. Ideally, "Search" on various case details such as IOCs
- 3. Track Artifacts, 'IOC', analysis, and other relevant data
 - Perform correlation on different data types
 - 'Link' values to data types such as Groups, Mitigations, Frameworks, other
 - Send data types for analysis (suspected malware) and incorporate results
- 4. Use data to respond, track, correlate and aggregate events, develop mitigations, signatures, etc.
- 5. Share <u>certain</u> results with others using rules
- 6. Store historical results for future case analysis

Sample design plan for open-src tool integration and data flow



Carnegie Mellon University Software Engineering Institute

MISP – Event List



Events from the the CIRCL MISP dataset imported into a MISP server. tlp:white

Carnegie Mellon University Software Engineering Institute

MISP – Store an Event

Home Event Actions	s ▼ Galaxies ▼ In	put Filters Global Actions		M
View Event				2
View Correlation Graph	OSINT - I	Bad Rabbit: Not-Petya is back with		
View Event History	improved	I ran	Related Events	
Propose Attribute	Event ID	1152	2017-10-25 (1000) 2017-10-25 (1000)	
Proposo Attachmont	Uuid	59f049c0-aae0-47d2-a888-4021950d210f	2017-10-25 (1023) 2017-10-24 (359)	
горозе Анаситен	Org	CIRCL		
	Contributors			
Contact Reporter	Tags	misp-galaxy:ransomware="Bad Rabbit" Type:OSINT tlp:white		
Download as		malware_classification:malware-category="Ransomware"		
		osint:source-type="blog-post"		
List Events		misp-galaxy:preventive-measure="Backup and Restore Process"		
And Frank		misp-galaxy:preventive-measure="Restrict Workstation Communication"		
Add Event	Date	2017-10-25		
	Threat Level	Low		
	Analysis	Completed		
	Distribution	All communities 0		
	Info	OSINT - Bad Rabbit: Not-Petya is back with improved ransomware		
	Published	Yes		
	#Attributes	47		
	Last change	2018-12-03 17:28:58		
	Extends			
	Extended by			
	Sightings	0 (0) - restricted to own organisation only.		
	Activity			

Events have standard fields and include Tags. *Tags* are built using *Taxonomies*

Carnegie Mellon University Software Engineering Institute

Type of Information to Be Shared

Indicators of Compromise (IOCs) – Provide warnings that a network has been compromised, enabling the parties concerned to anticipate cyber breaches and take appropriate steps. Examples of IOCs

- Unusual network activity
- Login failures
- Unusual privileged account user activity
- Change in system configuration
- Logins from non-business locations facilitate detection and response of cybercrime
- Technical aspects of attacks; Tools exist which facilitate systemic discovery of new technical aspects of attacks

Types of Information to Be Shared

Tools, techniques and procedures (TTP)

- Awareness of cyber attacker and criminal behavior is imperative to the prevention and detection misson
- Knowing what cyber criminals do and how they do it, allows for deeper understanding and recognition of source threat, suspicious patterns, malware, infrastructure launch points, and more.
- Can help organizations to plan a stronger defense against attackers and/or cybercrime.

More Information Sharing Examples

- Affected host
- Location of System
- Malware
 - Known bad
 destination
 - Threat rating based on sensors
- Check for false positives
- Triage malware samples
- Use templates

- First correlation of events
- Adding business context
- Adding tags
- Upload samples to sandbox

- Malware reverse engineering
- Manual investigation
- IOCs
- Strategic advice
- Forensic artifacts

MISP – Attributes (IOCs) attached to the Event

+			0	Filters: All File Network Financial Proposal Correlation Warnings Context	Relate
Date	Org	Category	Туре	Value Tags	Gala
2017-10-25		External analysis	link	https://www.welivesecurity.com/2017/10/24/bad-rabbit-not-petya-back/ osint:source-type="blog-post"	1
2017-10-25		External analysis	comment	A new ransomware outbreak today and has hit some major infrastructure osint:source-type="blog-post" in Ukraine including Kiev metro.	
2017-10-25		External analysis	link	https://www.virustotal.com /file/301b905eb98d8d6bb559c04bbda26628a942b2c4107c07a02e8f753b dcfe347c/analysis/1508918790/	
2017-10-25		External analysis	link	https://www.virustotal.com /file/2f8c54f9fa8e47596a3beff0031f85360e56840c77f71c6a573ace6f4641 2035/analysis/1508915760/	
2017-10-25		Network activity	url	http://www.pensionhotel.cz	
2017-10-25		Network activity	ip-dst	185.149.120.3	
2017-10-25		Network activity	url	http://osvitaportal.com.ua	
2017-10-25		Network activity	url	http://www.otbrana.com	

Attributes have different Categories and Types

Carnegie Mellon University Software Engineering Institute

Taxonomies as Tags

- Allows for a structured list of terms to select from such as:
 - Types of attacks, Specific Courses of Action COA, and much more
- Benefit: Terms can be used across organizations and teams
- Can define different types of data and types of values and can be aligned to other standards and frameworks – such as enumerations of adversary TTPs in publicly available reports
- MISP allows for both public and private taxonomies

Main Benefit

Complex data values can be semantically associated with custom lists. The lists can be set by an individual or a community.

Attempted descriptions at emerging threat behavior can be proposed and adopted and emerging data can be structured.

For example, one team built a taxonomy for Cryptocurrency threats based on CipherTrace reports to differentiate crypto related events from each other. Can be thought of as a "sub category"

- cryptocurrency-threat:Crypto Robbing Ransomware
- cryptocurrency-threat:Lightning Network Transactions (these are *off-chain* in a sense, so even harder to track)
- cryptocurrency-threat:SIM Swapping (usually specific to attacks on mobile based wallets)
- And more

MISP taxonomies - Flexible Classification for Information Sharing

MISP taxonomies is a solution to use existing taxonomies (or create your own) to classify your cybersecurity events, indicators and threats. This technique is integrated as a default mechanism for tagging in MISP (Malware Information Sharing Platform & Threat Sharing) and to support a distributed classification where organizations can share common taxonomies in a local or distributed fashion.

Classifications are distributed as simple JSON files to use with MISP but can be easily integrated into any other information sharing software.

You can also propose new taxonomies to the community.



Examples of machine tags and human readable tags :

admiralty-scale:source-reliability="c"

admiralty-scale:Source Reliability="Fairly reliable"

admiralty-scale:information-credibility="3"

admiralty-scale:Information Credibility="Possibly true"

nato:classification="NU"

nato:Classification="NATO UNCLASSIFIED"

tlp:amber

Traffic Light Protocol:(TLP:AMBER) Information exclusively given to an organization; sharing limited within the organization to be effectively acted upon.



(over 35 taxonomies)

Carnegie Mellon University Software Engineering Institute

And now Data Objects

Only available in newer versions (2.4.80 +)

Allow for template based combinations of attributes.

Groups different kind of attributes (taxonomies) together using specific templates

Among other things, used to support sharing/import in DHS CISA AIS format (sector list, source markings, etc.)

Integration with Data Services (MISP Modules)

- Can be used for data enrichment (expansion, import and export)
- Check information against outside databases in the background (expansion) and display via hover over as needed by analysts.
- Written in Python

Examples

- Hover over a CVE to display more information
- Submit files (artifact attachments) or URLs and receive a report that is imported and converted to MISP attributes such as hostname, domain, ip-src, ip-dst, various hash functions
- Also modules to export or import various formats

Sharing Communities & Data



Known Existing and Public MISP Communities

- CIRCL MISP Community
- CiviCERT MISP Community
- Fidelis malware/RAT Community
- CSSA Cyber Security Sharing & Analytics (CSSA)
- FIRST MISP Community
- NATO MISP Community
- MISP Feed Communities
- CIRCL OSINT Feed
- Botvrij.eu OSINT feed

Event Walkthrough

Carnegie Mellon University Software Engineering Institute

© 2021 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Adding Events - Menu

Home	Event Actions Galaxies	Input Filters Globel Act	ions Sync Actions Admin	istration Audit		
The even	List Events Add Event	anisations having an account o	n this platform, but not synchronise	ed to other MISP instances until it is published.		
List Events	List Attributes Search Attributes	Event				
Import from.	REST client					
REST client	View Proposals	D-15	This community only	•		
List Attribute	Events with proposals	evel O	Analysis O			
Search Attrib	new designation requests	ned ·	Initial	•		
View Proposi	List Tags	lo				
Events with p	List Tag Collections	vent Description or Trackin				
View delegat	Add lag	event				
Export	List Templates	/UID or ID. Leave blank if not applicable.				
Automation	Add Template					
	Export					
	Automation					

Set Distribution of Event

List Events Add Event	dd Event		
Add Event			
Import from Da	te	Your organisation	n only
REST client 2	019-10-15	✓ This community	only
List Attributes Th	reat Level O	All communities	munities
Search Attributes	/ledium	- Sharing group	
View Proposals Ev	ent Info		
Events with proposals	wick Event Description o	r Tracking Info	
View delegation requests Ex	tends event		
Export	vent UUID or ID. Leave b	lank if not applicable.	
Automation	Add		

Add Event

Harrie Event Actions	Gauxeen input Hitere	Labble Actions Sync Actions Administration Audit	Mittab Commis Ed	Log out
The event has been asved				×
View Event				3.7
View Correlation Graph	A BIG Event	is hitting the Communications Sector right now (TES		Comms
Vew Event History	Event ID	1458		
Edit Event	UUID	5daf1e3a-da14-4be8-b8af-7494ac110002		
Delete Event	Creator org	Communications Sector		
Add Attribute	Owner org	Communications Sector		
Add Object	Email	comme@test.test		
Add Attachment	Tags	Ø + ≜ +		
Populate from	Date	2019-10-15		
March event	Threat Level	High		
and a ministration of a second	Analysis	Ongoing		
Publish Event	Distribution	This community only 0 <		
Publish (no email)	Info	A BIG Event is hitting the Communications Sector right now (TEST DEMO). These are the details		
Download as	Published	No		
	#Attributes	0 (0 Object)		
List Events	First recorded change	1970-01-01 00:00:00		
Add Event	Last change	2019-10-15 19:30:02		
	Modification map			
Download: GhuPG Ney		Provined by MBP 2.4,118 - 2019-10-15 19:30.03		

Add Event – Populate Event Data from Other Data

Home Event Actions	Galacies Input Fibers Global Actions Sync Actions Administration Audit	Comms 🖴	Log.out
	Add Attribute		
	Choose the format that you would like to use for the import		
East Super-	Freetext Import		
Dates (1997)	Pressans using a Template		
	OpenIOC Import		
	ThreatConnect Import		
Notes ton:	(Experimental) Forensic analysis - Mactime		
	Canoal		
	Consectual Comment		
	für Infrastrum Delinicien System Batteri Import		
Add Dett			

Add Tags to Your Event – Context for Others

	And Event	G Event	is hitting the Communications Sector right now (TEST DEMO). These ar	
nt ti	List Attributes		168	Related Events
	Search Attributes		6da91463e-da114-45e90-68a1 7494ac110002	Mahuki FIN7: Responding to the Criminal Operatory New Teos and Tech
	President Science	***	Communications Renter	2019-10-10
-	View Proposale	-	Comparison Settor	
	Events with proposal		commod/level test	
ter	Vew delegation respa	ota.	00 80	
	List Tege		2019-10-15	
-	List Tag Collections	evel	Hgn	
	Adding		Orgong	
	List Taxonomies	lion	The community only 0 <	
	Add Template		A BIG Event is filling the Communications Bector right new (TEST DEMO). These are the details	
			Yee (0018-10-15 19-42:34)	
10	Export	100	3 (0 Object)	
12	Automation	proid change	2019-10-15 19 37:04	
		ast chunge	2019-10-15 19:37:04	
		Indefication map		
	5	ightings	0 (0) - instituted to own organization only. 🎤	
		6	Well-Swittes College and Well	
	5	Photo = Gelexy + F	Sent graph +Conteleton graph +ATT&CK mante =Atsituates =Discussion	
	6	HISE ADD		
		Galaxies		
		100 FB		

Add Attributes to Your Event IOCs and External Analysis

Freetox Import Result	Freetext Import Results										
View Downt View Connection Grapm View Event History	Debtw you can see the attributes that are to be created. Make save that the o Warning: You are missing worning letty that are used to recognize TLDs Proposals instead of attributes.	alagoras ar	d the types are cornect, often a syster MISP has the warnings	avans iptore vil al submodule and	bei off	end based a and updated	n en inconstantie auto or elea this tool migt	vatic nasistion. It end up mixeling valkt domaine/hostnamee/sch	. The missing lats are: TLD	e as known by	IANA
Date Event	Velue	Similar Attributes	Category	Тури	55	Dissble Correlation	Distribution	Conment	'Sept		Actio
And Obact	https://www.freeye.com/biog/treat-research/2018/10/matulo-f	1380	External analysis	e ut			Interit event				×
Adul Attautoriert.	https://www.virustotal.com/gu/file/18cc54e2fbdad5a317b6eeb5		External analysis	• m			inherit event	3			*
Populate trans Envent Swell Merge attributes from Propose Attributes Programs Attributes Doverload an Lait Events	Submit attributes							Uptime all comment fields			Change all

Download Qna70 He

Powered by MOV 0.4 111 - 2010-10-15 10:33:10

You can also import 'free' text and make use of IOC parsing tools to make initial extraction and 'type' predictions

Carnegie Mellon University Software Engineering Institute

© 2021 Carnegie Mellon University

[Distribution Statement A] Approved for public release and unlimited distribution.

After You Add an Event, MISP looks for events with the same values

Taugers websausy	and the second se		- 2/15	And Alexander And								Contra	 indett
a supervision of the second seco	Published	No											
a sector and the sector of the	skitributee	3.(0 Object)											
of Events	First recorded change	2018-10-15 18	37.04										
od Everx	Lest sharpe	2019-10-15-10	37:04										
	Modification map		^										
	Sightings	0:0) - restricted	to own s	genedia uriy. F									
	-Prom - Daiery +	Enertignich +Co	metation g	ngh +ATTECK mente -Attributes -Chargement									
	Galaxies												
	35 23												
	-person matri	nines sal											
	+previous must +	ninw al											
	+ period - nut+	nano (al Scoque loggio -	E Dela	nel id Decey score ● Contact Striketed Says - T Filtering Sco							Enter within 1	II Search	а ж
	+ E & H	now of Rogan loggin - Category	Denke Tygere	ned tit Decey score O Content Striketed Says ▼ Fitneting too Value	Togs	Galaxies	Comment	Constate	Relator	Orga Guidebol	Enter value (u search e >> >	Q. ¥
	+ previous must + + E & 24 Oute 1 Og 2019-10-15	nine sil Roque loggie - Category Payload delivery	Type sha256	nel Ef Decey score ● Context Striketed Says ▼ Fitering too Water 10cc64e2/baadsa317b6eetc6n7ds3875cc88b01ta0810886679eftcb3s102 bd8	Toga Cite	Galaxies	Constant	Correlate	Relater Events 1200	Orga: CUCESCI Date: 2010-10-10 Inte: Manas: FAI: Peop Technique:	Enter value 1	ti Saunch 	Q. X
	+ prestaut mut + + E E 24 Galler 1 Gall 2019-10-15 2019-10-15	Herry all Boogen leggle - Category Proytood delivery Enternal analysis	Type shazse un	Ef Decey score: ● Cantool St Palanol Tage: ▼ Pitering too Volue Https://www.firetes.com/blog/threat-research/0219/110/mahalo-fm? responding-to-new fixeds and -inchriques.l/##		Calacies	Comment	Correlate D	Relater Events 1390	Orga: COURSU Date: 2010-10-10 Inte: Manual: PAT Peop Technologies Constituting Velat: 19cc54x07bctactmc111fed	Enter value 1	II SHIITCH 	Q. X
	+ prestant (mut + + E 2 34 Oute 1 Org 2019-10-15 2019-10-15 2019-10-15	nian al Soqua loggio - Category Period delivey Esternal analysis Esternal analysis	Type sha256 (e) ins	Id Decky score O Climited Trace Telescol Team Telescol Climited Telescol Team Telescol Climited Telescol Telescol Telescol Team Telescol Climited Teles		Catacies Con All Con All Con All	Comment	Constate D D D	Relator Events 1390	Orge CUSEED Date: 2010-10-10 Inter Manage 74/7 Period Techniques Constating Veise: Utect/sc/facetocttc/11/tet	Enter value 1 working to the Con working to the Con where Value	ti sounch onal Operators' k shisoturenti oppar page p	QL X Here Tanks and Here Tanks and The Construction The Constr

Publish Events



Organization List



Download Doubli her

Powerki by Miler 2 4 116 - 2019-10-15 18:21:54

Create New Sharing Group

ly Profile Jashboard	New Sharing Group
ist Organisations loie Permissions	General Organisations MISP Instances Summary and Save
ist Sharing Groups dd Sharing Group	NatCritical Infrastructure Sharing Group
lser Guide erms & Conditions	Releasable to Example: Community1, Organisation1, Organisation2
erns & Conditions Statistics	Description A sharing group for the sector CSIRTs inside of the NatCSIRT constituency
	Make the sharing group selectable (active)

Add Local Organizations

Home Event Actions	Galaxies Input Filters Globel Actions Sync Actions Administr	ntion Audit	
	New Sharing Group		
List Organizations Print Processing List Descriptions Actif Shaling Group	General Competition MCP encances Enternally and Gain Add incer impactation Add encodes organisation Add encodes organisation Type Name MMD Incel OHDRAMME MMD	Select organisations to add	
time form Server & Descriptions Summer	Providuo page	Available Organisations Energy_SectorCSIRT National CSIRT 3 Transportation_SectorCSIRT	Added Organisations
		Add	Cancel

Confirm Sharing Group You Want to Add

Home Event Actions	Galaxies Input Filters Global Actions Sync Actions Administration Audit
My Profile Dashboard	New Sharing Group
List Organisations Role Permissions List Sharing Groups	General Organisations MISP Instances Summary and Save General: You are about to create the NatCritical Infrastructure Sharing Group sharing group, which
Add Sharing Group	is intended to be releasable to [Sharing group releasability not set!].
User Guide Terms & Conditions Statistics	 can extend the sharing group. Synchronisation: Furthermore, events are automatically pushed to: any interconnected instances linked by an eligible organisation. You can edit this information by going back to one of the previous pages, or if you agree with the above mentioned information, click Submit to create the Sharing group. Previous page Submit

View Sharing Group

Home Event Actions	Galaxies input Filte	rs Global Actions	Sync Actions	Administration	Audit	
My Profile						
Dashboard	Sharing Group					
List Organisations	ld	1				
Role Permissions	Uuid	5da61bb3-38a0-47f8-bc6e-7431ac110002				
Edit Sharing Group	Name	NatCritical Infrastructure Sharing Group				
Man Protocol Control	Releasability					
view snaring Group	Description	Description A sharing group for the sector CSIRTs inside of the NatCSIRT constituence				
List Sharing Groups	Selectable	*				
Add Sharing Group	Created by	ORGNAME				
Lines Chride	Organisations					
Terms & Conditions Statistics	Name		Local	Extend		
	ORGNAME		*	-		
	Energy_SectorCSIRT		*	×		
	National CSIRT 3		*	×		
	Transportation_SectorCSIRT		-	×		

Others can review your data and may add their own 'sightings' or links

Home Event Actions -	Galaxies 👻 In	put Filters - Global Actions -		M	
View Event View Correlation Graph	OSINT - E	Bad Rabbit: Not-Petya is back with		•	
View Event History	improved ran		Related Events		
	- 2017-10-25 (1100) 2017-10-25 (1				
Propose Attribute	Event ID	1152	2017-10-25 (1023) 2017-10-24 (359)		
Propose Attachment	Uuid	59f049c0-aae0-47d2-a888-4021950d210f	2011-10-20 (1020) 2011-10-24 (000)		
	Org	CIRCL			
Contact Reporter	Contributors				
	Tags	misp-galaxy:ransomware="Bad Rabbit" Type:OSINT tlp:white			
Download as		malware_classification:malware-category="Ransomware"			
		osint:source-type="blog-post"			
List Events		misp-galaxy:preventive-measure="Backup and Restore Process"			
		misp-galaxy:preventive-measure="Restrict Workstation Communication"			
Add Event	Date	2017-10-25			
	Threat Level	Low			
	Analysis	Completed			
	Distribution	All communities 0			
	Info	OSINT - Bad Rabbit: Not-Petya is back with improved ransomware			
	Published	Yes			
	#Attributes	47			
	Last change	2018-12-03 17:28:58			
	Extends				
	Extended by				
	Sightings	0 (0) - restricted to own organisation only.			
	Activity				

Events have standard fields and include Tags. Tags are built using Taxonomies

Carnegie Mellon University Software Engineering Institute

Challenges

Carnegie Mellon University Software Engineering Institute

© 2021 Carnegie Mellon University

[Distribution Statement A] Approved for public release and unlimited distribution.

Data Feeds Require Analysis

- Reports are not always entered by their original authors
- Integration with IDS requires blacklist/whitelist management
- Teams may share using different schemas (but at least they are sharing !)
- Private communities may have more context than public (not a MISP problem alone)
- Dashboard tools are add-ons
- Recommend having technical resources to help with administration and scripts (Linux, Python, SQL, PHP, etc.)

Has had some security bugs

Such as https://cve.circl.lu/cve/CVE-2019-9482

In MISP 2.4.102, an authenticated user can view sightings that they should not be eligible for. Exploiting this requires access to the event that has received the sighting. The issue affects instances with restrictive sighting settings (event only / sighting reported only).

Some are side projects to integrate other tools with MISP more natively (such as Maltego) <u>https://cve.circl.lu/cve/CVE-2020-12889</u>

But developers are responsive and provide fixes for them, updates sometimes multiple times a month.

Summary

- Sharing Platforms with quality data can help improve correlations and actionable defenses (IDS, etc.) for Cyber Protection and Incident Response Teams
- 2. Taxonomies for Term re-use and common language may improve shared understanding
- 3. MISP is an open source platform for storing and sharing events, attributes and adding meta-data for taxonomies, tags.
- 4. MISP can fit into a larger ecosystem of tools
- 5. Communities can share Events attached to IOC, TTP, and Mitigations
- 6. Has features for restricting distribution, private taxonomy, defining sharing groups, correlation.
- 7. Has integrations with other data services for enrichment

Discussions & Questions?

Carnegie Mellon University Software Engineering Institute

© 2021 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Contact Information

sjperl@cert.org

Carnegie Mellon University Software Engineering Institute

© 2021 Carnegie Mellon University

 $[\mbox{DISTRIBUTION STATEMENT A]}$ Approved for public release and unlimited distribution.