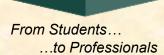
MICHIGAN STATE UNIVERSITY Alpha Presentation Enhanced MISP User Interface

The Capstone Experience

Team GM

Jordyn Rosario Alex Richards Marven Nadhum Jake Rizkallah Noah Anderson

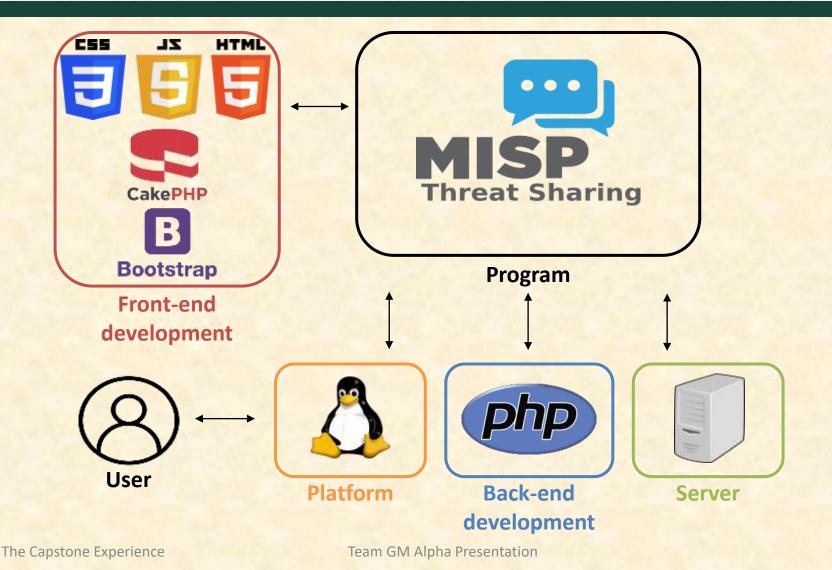
Department of Computer Science and Engineering Michigan State University Fall 2021



Project Overview

- MISP, Malware Information Sharing Platform, is an open-source software that allows for threat intelligence to be shared with security analysts
- Enhance UI to allow for customization of components and a simpler feel that provides a straightforward experience
- Improve existing functionalities to provide ease of use and increase productivity

System Architecture



Events

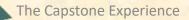
- C	OBM	tps://192.168.88	131									ŵ		8
HILF EVENT ACTORS	Dathbard	- Calabra - N	atom a	aiiliid	Actions 11/1 Syne Activ	ns - Norman	atten Ligs A	es :					B Q	•
E EXercite	Example													
II Evere	Events													
port hom	- previous	mot e												
\$T climit	93 183	eesta – Dig Keesta		WHE							Erme w	not in second		P
L Attribution		Creator ong	Owner org		Chudden	Tirgi.		WARD.	+tan	Creator user Date	(edg.)	Distrit	iotion Act	tions.
erch Attributies											DSIVE Expansion on Additional indicators relating to Sofacy.			
w Propotals	• *	Chultur\$PRL be	ORGNAME	7.20	Sofiecy G.IS	type:05INT	S tip:schite	345	•	ədminiğindirilin təsti - 2014-3	2-34 Gami Expansion in Kelenomic Interaction Instituting to Servey (APT78) phistory biog post by PWC	All 4		128 1
nts with programits					Threat Actor 9.	a ilparent a	tipositite							
e delegation requests	• ~		ORGNAME		of Axion Q ⊞	esint:saurce	-types "blog-past"	20870	x	atminipatirin fest. 2014-1	6-28 - OSINT - Operation SMN Dowettal	AII.4		CET 1
ert		ChulhuSPRLike	ORINAME		Tuol Q	8 type OSINT	a muner	35		adminiadminitest 2014-1	2.nd Resin France	AI 4		08 [°] 1
priation.	-	Condition PHL Se			Ø kogin Q ⊞	e type chiller		340			1-310 Import of CrownLab public DH of makkane indicators	414		121
						type:05INT	and the second second	and and				7125		
	•*	Chulled PRL be	ORGNAME			2 Uprovisito	and an openand	3067		atminipatiminitest 2014-1	0-02 OSINT ShellShock scanning its from Open(INS	M14		187.1
	∎Ÿ	COMPAGEMENT.	ORGNME	- 24	ibol Q @ Turia Q III	8 Type OSINT	d thronon	н.		adminikadmin.test 2014 (1-dt - Turla digging using Tataimash	All 4		R.
	•*	OnutraiPHL be	ORGNAME		Tool Q. @ Regin Q.12	d type:coliny	o taranen			admin@admin.hest 2014-1	1-26 CGINT Regin samples shared by WisaShare	A1 4		e i
	• *	CitudesSPRLine	ORDNAME		Timent Actor Q. & Sofacy Q.IE	e upgreen e) _{Туре:} озикт	114.cs		aimin@admin.taut. 2014-1	OSINT APTZE: A Window into Russiade "'s Cybor Espirituge 0-27 Operatoris? blog past by Freilyn	All 4		ur e
	• *	COMMANSPREAM	ORGNAME		Threat Actor Q Turia Group Q III	@ type crimt	a Margement			adminijadmin test. 2014-1	1-13 CSINT Expansion on Walke	A/14		187 I
	• *	COLUMN FR. Dr	ORGNARE			🛃 type cosiner	Ø tterurren			amingamintest 2014-1	0-20 CRINT OccaRd7 - A whole of a tale blog post by PWC	4114		127 1
	•*	ChubuSPRL be	ORGNAME	- 10		a negerie a	тури:озит	103e	i -	admin@admin.test 2014-1	2-13 6. Sylaistan blog post from ESET by using whele registrant	nistari Ali 4		œ 1
	• *	CTURING PRE No	ORONAME			a type osint	a thursen			adminijiadmin test 2014.1	0.50 OSAVT Black Energy 2 material analysis blog post by peoph Mathematiki	A!! K		or 1



Team GM Alpha Presentation

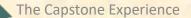
Event Attributes

# Event#26-MISP	· +													- 0 0
← → C	O & https://19	92.168.88.131/inv	nta/view/24								1	1 🕆		⊚ =
HILEP Event Actions	Destroyers Gates	ine injus Real	Gibbel Actions	Sync Atliene	Administration Loga	AR.								
Proposel Altribute	Published	12021-10-13	20:13:080											
Propose Attachment	eAttributes	86.03 O8(ects)												
Publish Sightings	First recorded change	2014-11-20-00-4	154											
Download as	Last change	2057-00-22 3.3.3	194											
List Events	Modification map													
Add Event	Sightings	OI - restricted	to own orgenisation	ordy A										
	- Posta - Malaxy - P	and graph + parts	andre ensklub	n gilast (+ATTAGE)	matus: #10end squatts: - Al	otonia - Dissi								
	824: Tirle Hyperia													
	Galaxies													
	Toni Q Si Turla Q 🖽 🗑													
	• provencia 📃 2	must - View												
		Side have *	Denter Tarberty	ala Aligned	a Occured Valented	lags T hinks	12341				Titlet Male	a dia nanarah		9.1
	Date 1 Org (Category 1	ype Value			Ъgs	Onlandes	Comment	Conclut	Related Feed	IDS Ostributio	Santingi	Activity.	Actions
	a 2016-02-18	Paytood delivery (TutbeDalicht Fw2t0 2feo4o8907a		21678663899324041396526		-	Automatically added livia chills6849971c2353c2d6a8119c4985	. 🛎		🧑 inheilt	0.9.2		•• = = •
	0018-02-10	Paytoust dativary - 1	4c49c94601x 8a256 8ba7405720		cates 11 in a feet 3982 758676cM	0% A%	-	Automatically added lvia Rhec941bec02c7flad037x07d58c9091			a minere	007		•= 8 =
	3 2914-02-18	rayload delivery i			1x3r5#674527c5%8xb#86%	-	-	Automatically added live N40c0316616d1ade66122284899d314			innent:	002		•• **
	- 2026-02-28 #	Naytood delivery	2006662673 2006662673 20077629268		c60x 83x9x895779x5x53579751			Automatically added two 3665688667ac168579215a08629ef5e	. •		🙆 minerit	1100		•• 21
Dominanti PCP public key				is is an initial insta	Prevent by HISP 2 4 190 I	Name configure	e and hanten	accordingly - 2021-10-17 20-18:52						



Save Search Query

- saveSearch - MISP	x +										- (8)	
← → Ø	O & https://192.168.	88.131/SeveSearch							ŵ		0	=
terne Konst Artista	Dashboard Galaxies	lique Filiers Global Actions	Syre Arthree	Administration	Loga -	AP1				•	۹. ۵	
Search Duory ARMI											- 8	
Vew Seved Searchers	Saved Searches											
Add Search Query	• graviting read +											
	nd. To: Merci	THE	Wite						Created at		Action	
	7 anderwn92@gmail.com	Windows Threats	145ps://102.168	i Bil 131/evento	hales hearth	all Windows			2023-10-11 20:29:01		1	i.
	6 jake20222@gmail.com	Linux Threats	141pe.0143.564	1 80 1 21, events	Index/vearch	ull Linux			2021-10-1 20:27:59			
	5 andeson02@gmail.com	High Threak Botnets	tatps://190.168	i 68 111/eventu	index/search	threathered late	ewithell Botnet		2023-10-1 20:25:44		3	•
	4 anderson92@gmail.com	High Threat APTs	https://192.164	. 60 131 Sevents	in des insertit	tag 395earcht	tveatievel 1		2023-10-17 20:28:29			
	3 andersond2sjägmail.com	September 2021 High Lavel Threats	https://192.364 /www.chDateurit	1 88 1 51/eventu 18:2021-09-30	index/second	threatinged Lin	eer:"Datefran	2021-09-01	2023-10-17 29:25:44		ä	
	Page 1 of 1, showing 5 records	out of 5 total, stanting on record 1	L entirg on S									
Operational PGP public key		This is an initial install Powe	ered by WISP 2.4.5	50 Planse config	uie and hard	ten accordingly	- 2021-10-17 :	0.24.02				



Add Search Query

SaveSearch - MISP											
e → C	○ & https://192.168.88.131/SaveSearch/add ☆	⊚ ≡									
HTTP Event Actions	Dashboard Galaxies Input Filters Global Actions Sync Actions Administration Logs API	• • •									
View Saved Searches	Add Search Query										
	Title September 2021 Hgin Level Threats Value										
	https://192.168.88.131/events/index/searchthreatlevel/1/searchDatefrom:2)										
Download: PGP public key	This is an initial install Powerod by MISP 2.4.150 Please configure and harden accordingly - 2021-10-17 20:23:08										

Team GM Alpha Presentation

What's left to do?

- Continue enhancing the MISP user interface
- Further refine search functionality
- Improve saving and sharing search query functionalities

Questions?

