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

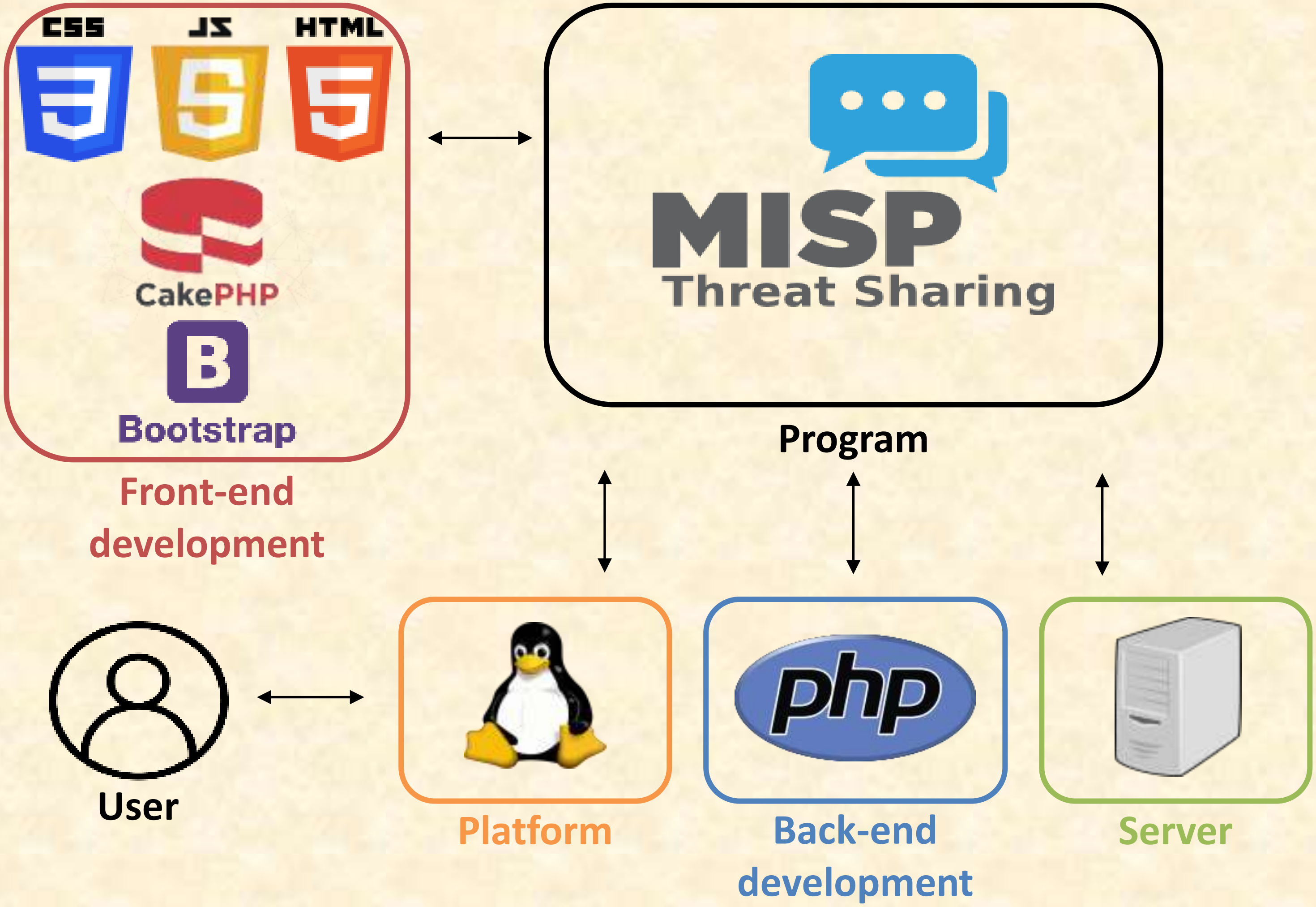
Fall 2021

From Students…
…to Professionals

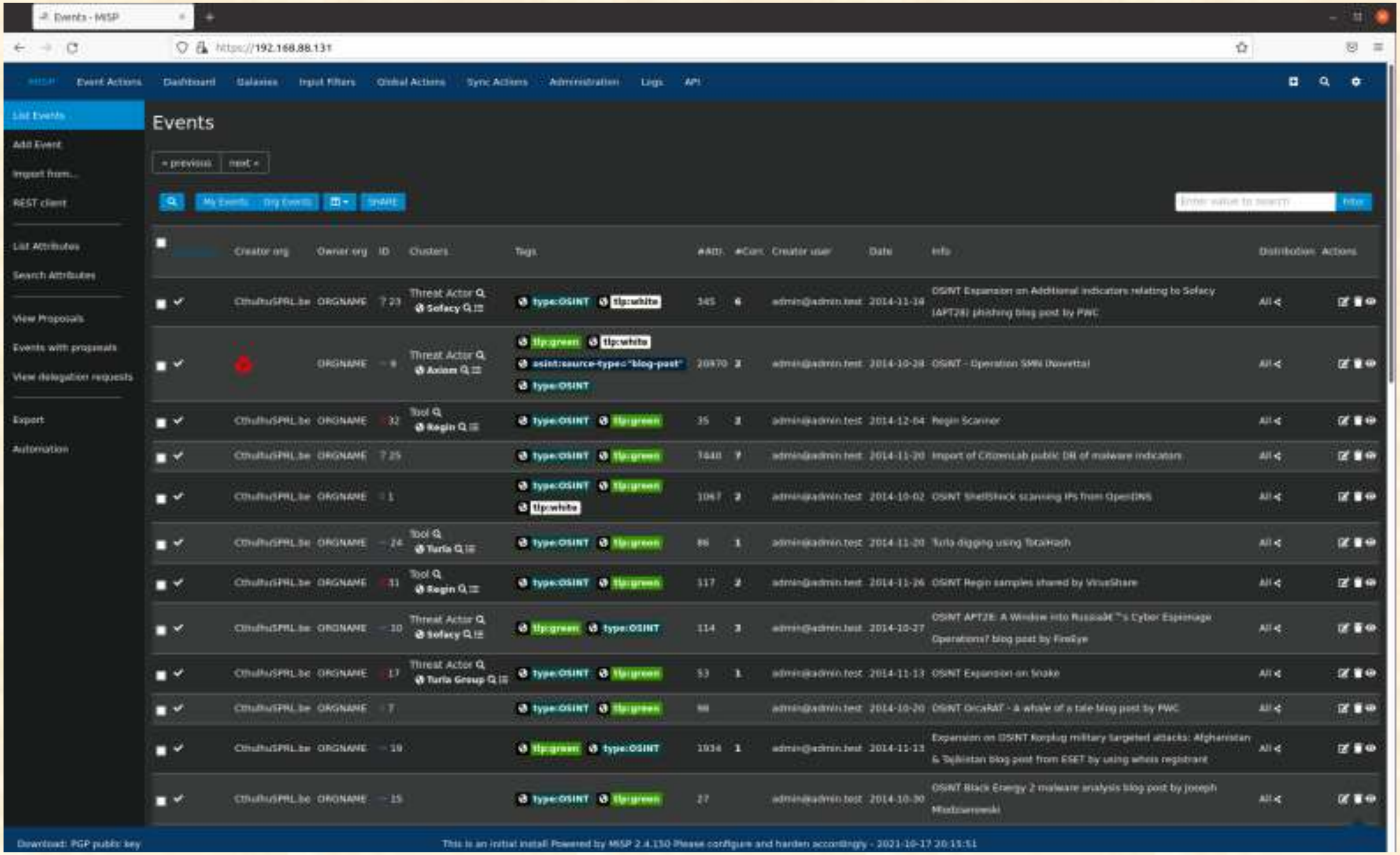
Project Overview

- 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



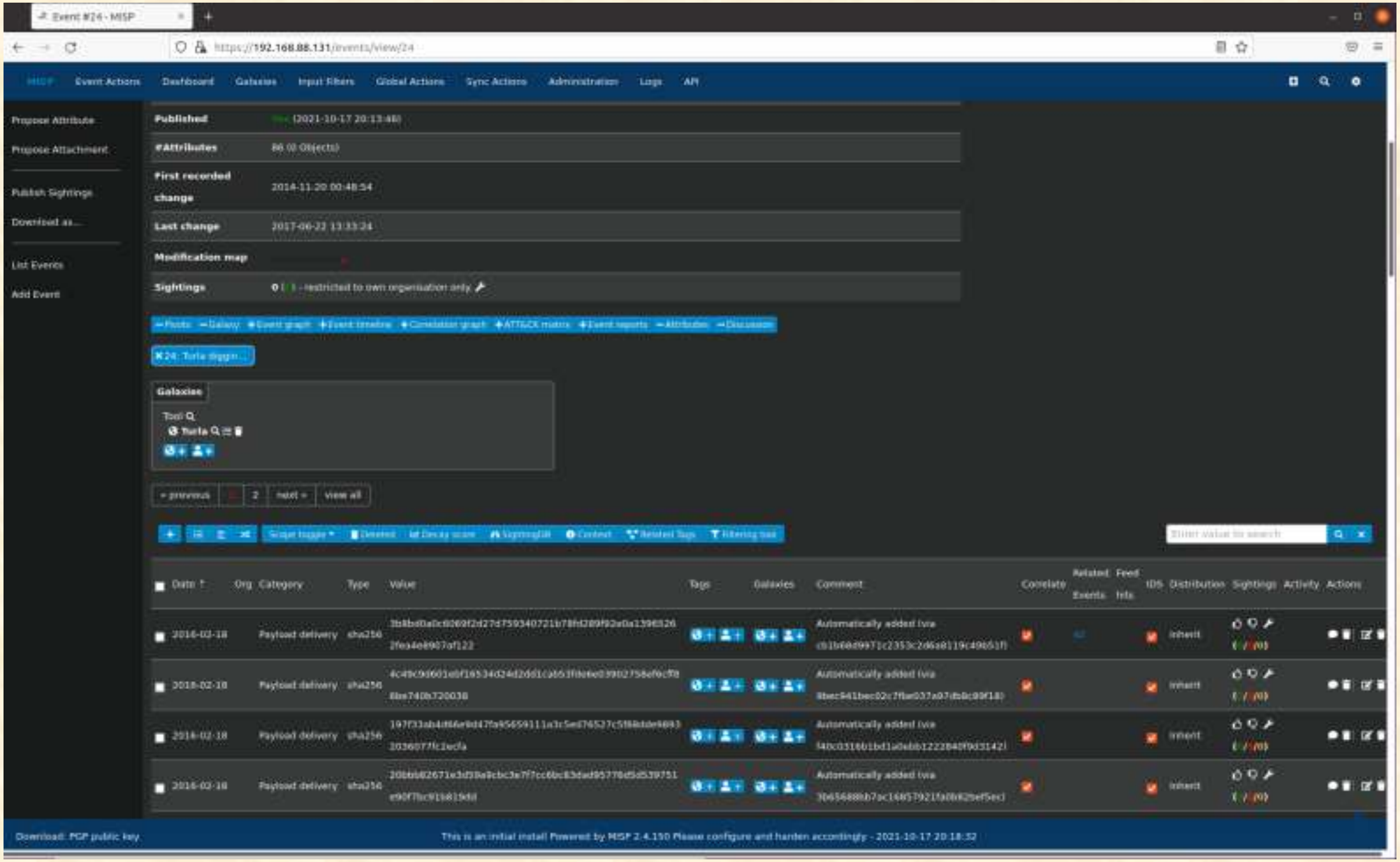
Events

☐		Creator org	Owner org	ID	Clusters	Tags	#Attr.	#Corr.	Creator user	Date	Info	Distribution	Actions
■	✓	CthulhuSPRL.be	ORGNAME	23	Threat Actor Sofacy	type:OSINT tlp:white	345	6	admin@admin.test	2014-11-18	OSINT Expansion on Additional indicators relating to Sofacy (APT28) phishing blog post by PWC	All	
■	✓		ORGNAME	9	Threat Actor Axiom	tlp:green tlp:white osint:source-type="blog-post" type:OSINT	20970	2	admin@admin.test	2014-10-28	OSINT - Operation SMN (Novetta)	All	
■	✓	CthulhuSPRL.be	ORGNAME	32	Tool Regin	type:OSINT tlp:green	35	2	admin@admin.test	2014-12-04	Regin Scanner	All	
■	✓	CthulhuSPRL.be	ORGNAME	25		type:OSINT tlp:green	7440	7	admin@admin.test	2014-11-20	Import of CitizenLab public DB of malware indicators	All	
■	✓	CthulhuSPRL.be	ORGNAME	1		type:OSINT tlp:green tlp:white	1067	2	admin@admin.test	2014-10-02	OSINT ShellShock scanning IPs from OpenDNS	All	
■	✓	CthulhuSPRL.be	ORGNAME	24	Tool Turla	type:OSINT tlp:green	86	1	admin@admin.test	2014-11-20	Turla digging using TotalHash	All	
■	✓	CthulhuSPRL.be	ORGNAME	31	Tool Regin	type:OSINT tlp:green	117	2	admin@admin.test	2014-11-26	OSINT Regin samples shared by VirusShare	All	
■	✓	CthulhuSPRL.be	ORGNAME	10	Threat Actor Sofacy	tlp:green type:OSINT	114	3	admin@admin.test	2014-10-27	OSINT APT28: A Window into Russiaâ€™s Cyber Espionage Operations? blog post by FireEye	All	
■	✓	CthulhuSPRL.be	ORGNAME	17	Threat Actor Turla Group	type:OSINT tlp:green	53	1	admin@admin.test	2014-11-13	OSINT Expansion on Snake	All	
■	✓	CthulhuSPRL.be	ORGNAME	7		type:OSINT tlp:green	98		admin@admin.test	2014-10-20	OSINT OrcaRAT - A whale of a tale blog post by PWC	All	
■	✓	CthulhuSPRL.be	ORGNAME	19		tlp:green type:OSINT	1934	1	admin@admin.test	2014-11-13	Expansion on OSINT Korplug military targeted attacks: Afghanistan & Tajikistan blog post from ESET by using whois registrant	All	
■	✓	CthulhuSPRL.be	ORGNAME	15		type:OSINT tlp:green	27		admin@admin.test	2014-10-30	OSINT Black Energy 2 malware analysis blog post by Joseph Mlodzianowski	All	

Download: PGP public key

This is an initial install Powered by MISP 2.4.150 Please configure and harden accordingly - 2021-10-17 20:15:51

Event Attributes



Event #24 - MISP

https://192.168.88.131/events/view/24

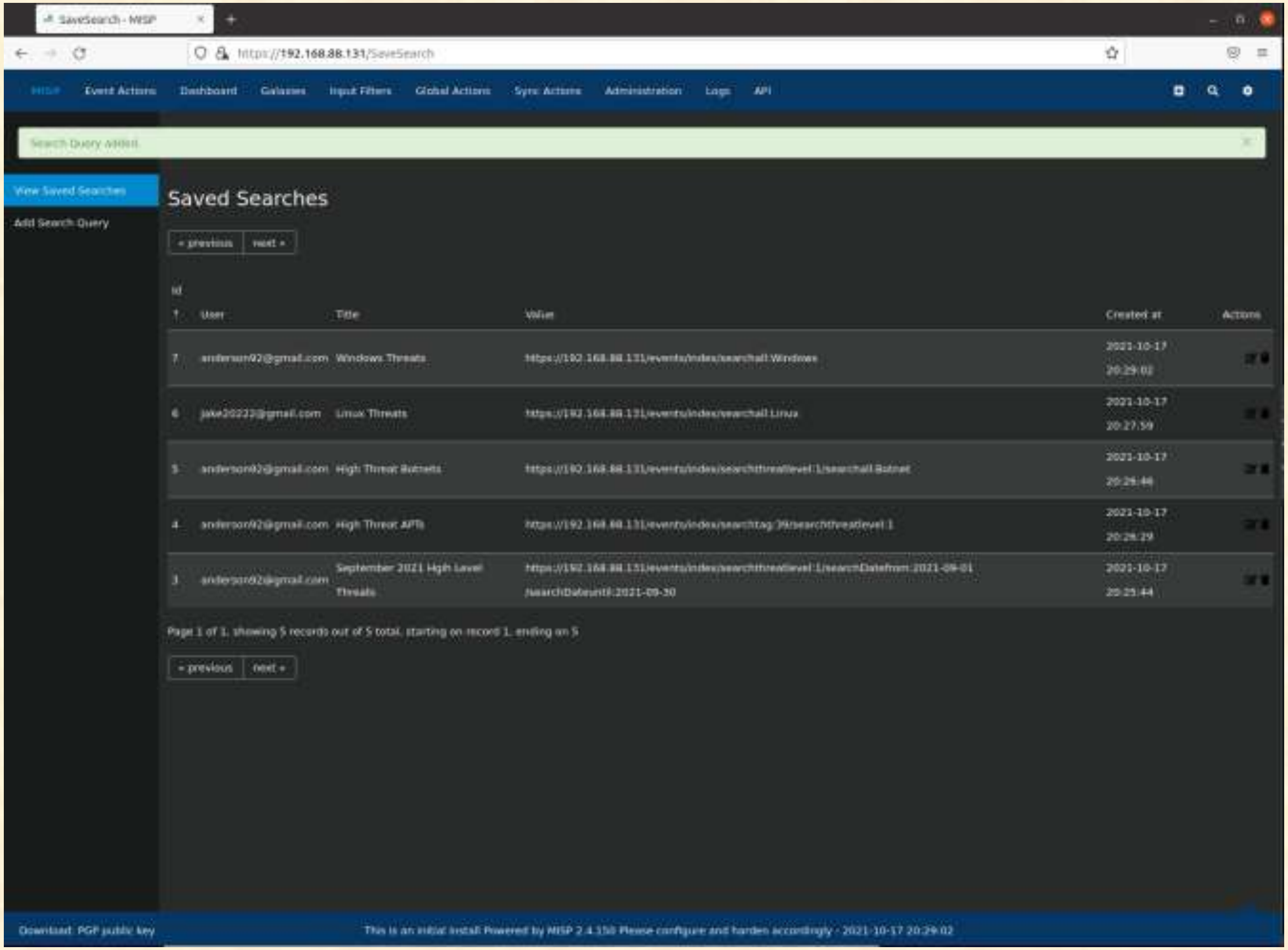
Published	Yes (2021-10-17 20:13:48)
#Attributes	86 (0 Objects)
First recorded change	2014-11-20 00:48:54
Last change	2017-06-22 13:33:24
Modification map	
Sightings	0 (/) - restricted to own organisation only.

☐ Date ↑	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings	Activity	Actions
☐ 2016-02-18		Payload delivery	sha256	3b8bd0a0c6069f2d27d759340721b78fd289f92e0a1396526 2fea4e8907af122			Automatically added (via c61b68d9971c2353c2d6a8119c49b51f)	☑	42		☑	Inherit	(/ /0)		
☐ 2016-02-18		Payload delivery	sha256	4c49c9d601ebf16534d24d2dd1cab53fdebe03902758efecff8 8be740b720038			Automatically added (via 8bec941bec02c7fba037a07db8c99f18)	☑			☑	Inherit	(/ /0)		
☐ 2016-02-18		Payload delivery	sha256	197f33ab4d66e9d47fa95659111a3c5ed76527c5f8bdde6893 2036077fc1ecfa			Automatically added (via f40c0316b1bd1a0ebb1222840f9d3142)	☑			☑	Inherit	(/ /0)		
☐ 2016-02-18		Payload delivery	sha256	20bbb82671e3d59a9cbc3e7f7cc6bc83dad95778d5d539751 e90f7bc91b819dd			Automatically added (via 3b65688bb7ac16f57921fa0b82ef5ec)	☑			☑	Inherit	(/ /0)		

Download: PGP public key

This is an initial install Powered by MISP 2.4.150 Please configure and harden accordingly - 2021-10-17 20:18:32

Save Search Query



Search Query added

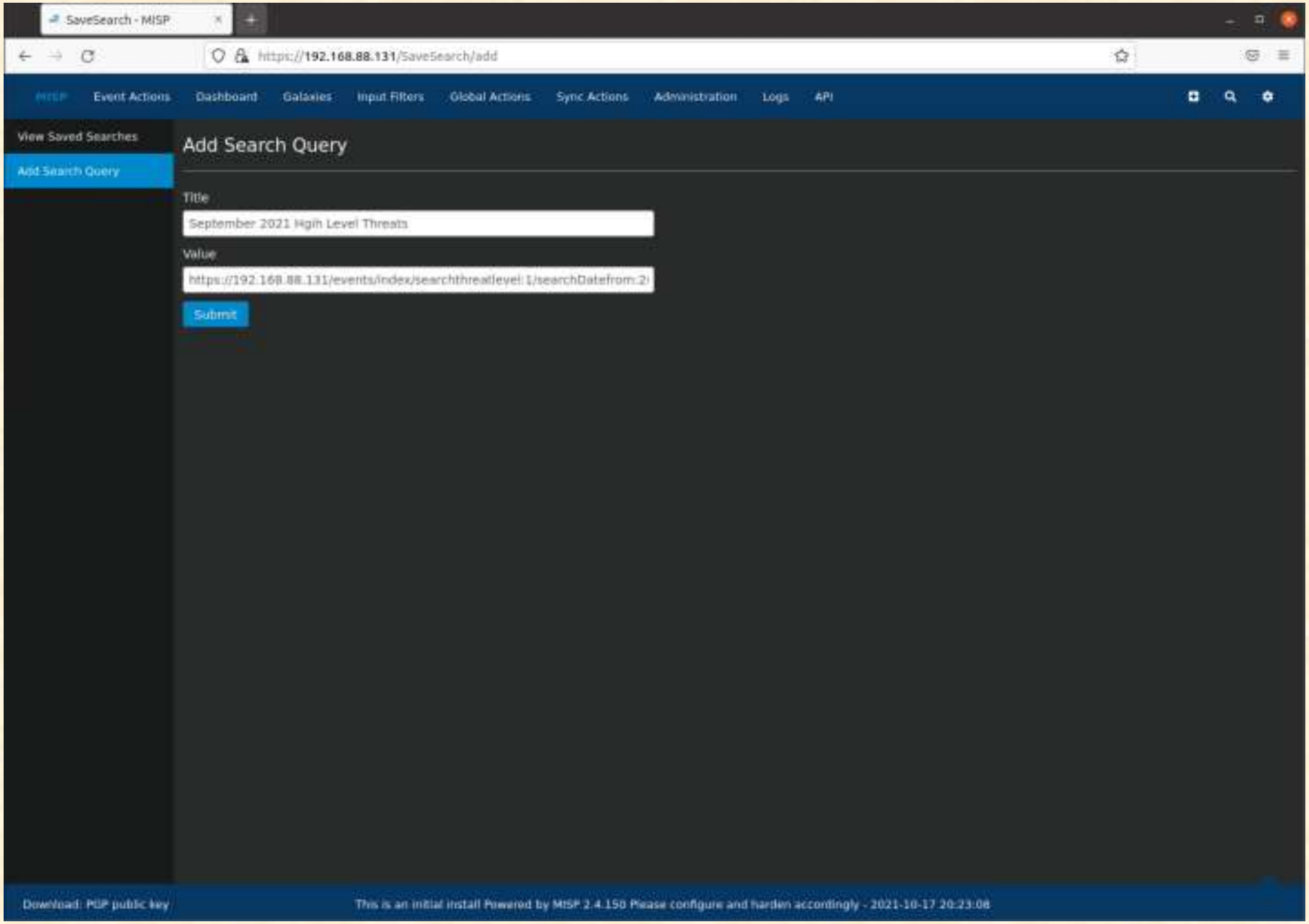
Saved Searches

Id ↑	User	Title	Value	Created at	Actions
7	anderson92@gmail.com	Windows Threats	https://192.168.88.131/events/index/searchall:Windows	2021-10-17 20:29:02	
6	jake20222@gmail.com	Linux Threats	https://192.168.88.131/events/index/searchall:Linux	2021-10-17 20:27:59	
5	anderson92@gmail.com	High Threat Botnets	https://192.168.88.131/events/index/searchthreatlevel:1/searchall:Botnet	2021-10-17 20:26:46	
4	anderson92@gmail.com	High Threat APTs	https://192.168.88.131/events/index/searchtag:39/searchthreatlevel:1	2021-10-17 20:26:29	
3	anderson92@gmail.com	September 2021 High Level Threats	https://192.168.88.131/events/index/searchthreatlevel:1/searchDatefrom:2021-09-01 /searchDateuntil:2021-09-30	2021-10-17 20:25:44	

Page 1 of 1, showing 5 records out of 5 total, starting on record 1, ending on 5

This is an initial install. Powered by MISP 2.4.150 Please configure and harden accordingly - 2021-10-17 20:29:02

Add Search Query



Add Search Query

Title

September 2021 Hgih Level Threats

Value

https://192.168.88.131/events/index/searchthreatlevel:1/searchDatefrom:2

Submit

This is an initial install Powered by MISP 2.4.150 Please configure and harden accordingly - 2021-10-17 20:23:08

What’s left to do?

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

Questions?

? ? ? ?

? ?

? ? ?