The starting point to protect agaist cyber attacks with threat intelligence

26/07/2024

About us

T-NET IT Solution Company Limited was established in Thailand and registered in Thailand on October 3, 2019 by a team of researchers and practitioners specializing in computer security in Thailand (Thai Computer Emergency Response Team, ThaiCERT).

“We are proud to provide All-encompassing cybersecurity services which complies with information security management standards”

Location

T-NET IT SOLUTION Co., Ltd.

131 Moo 9, Thailand Science Park,

Phaholyothin Road, Khlong Nueng Subdistrict,

Khlong Luang District, Pathum Thani Province

Zip code 12120 Thailand

Our Business

“Provide All-encompassing Cybersecurity” services

- **IT Security Consultant**
- **Designed** IT Architecture. **Development** software
- **Implementation** Cybersecurity **Standard** and Cybersecurity **Act.**

Company Services

Consultants

All of IT cycle.

Act., Practice, ISMS, SMS, BCMS

SOC and Log

Security Operation Center

Log compile Act.

SIEM

Software & Hardware

Develop software

IT Device Shop

Secure design

Network & Infrastructure

Data Center, System Integrator

Cloud solution

Training

Hacking [VA, Pentest] Network, SOC

ISMS, PDPA…. Cyber security, CompTIA

Audit

Act., Practice,ISMS, SMS, BCMS

Vulnerability assessment &

Penetration test

OS, Network, Website, Application

White box, Gray box, Black box

Security baseline

OS [Windows, Linux]

Network, Application, Virtual Machine

Code review

Statics Application Security Testing

Dynamic application security testing

Digital forensics

Chain of Custody

[Acquisition, Analysis, Reporting]

Our Certification

T-NET IT SOLUTION

CQI | IRCA CERTIFIED COURSE
ISO 22301 ISO/IEC 20000-1 ISO/IEC 27001

CISSP® · CSSLP® ISC2 · CCSP® ISC2 · CC℠ ISC2 · EC-Council C|CISO CERTIFIED · EC-Council ECSA CERTIFIED · EC-Council C|EH CERTIFIED · EC-Council C|HFI CERTIFIED

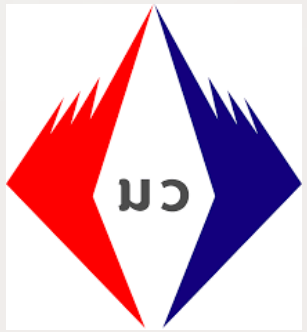
ICDL Cyber Security ICDL Workforce Certified by ICDL · ICDL Data Protection ICDL Workforce Certified by ICDL · PMI PROJECT MANAGEMENT READY℠ · Microsoft Certified Trainer MCT Trainer 2023 - 2024 · Google Cybersecurity Certificate Certificate of Completion · Microsoft Certified DEVOPS ENGINEER EXPERT · Microsoft Certified POWER PLATFORM FUNDAMENTALS · Microsoft Certified AZURE DATA FUNDAMENTALS · Microsoft Certified AZURE AI FUNDAMENTALS · CISCO CERTIFIED CCST CYBERSECURITY · CISCO CERTIFIED CCNA · Cisco Networking Academy Verified Python Essentials 2

CompTIA CSAP Security Analytics Professional · CCAP Cloud Admin Professional · CSSS Systems Support Specialist · CSAE Security Analytics Expert · CSCP Secure Cloud Professional · CNSP Network Security Professional · CIOS IT Operations Specialist · CLNP Linux Network Professional · CNVP Network Vulnerability Assessment Professional · PenTest+ Certified·CE · CySA+ Certified·CE · Security+ Certified·CE · Cloud+ Certified·CE · Project+ Certified · Data+ Certified·CE

CertiProf Certification ETHICAL HACKING CEHPC™ · CertiProf Professional Certificate CYBER SECURITY FOUNDATION CSFPC™ · CertiProf Certification SCRUM FOUNDATION SFPC™ · CCSK v4 Certificate of Cloud Security Knowledge Cloud Security Alliance · IT Specialist NETWORK SECURITY Pearson · IT Specialist CYBERSECURITY Pearson · IT Specialist CLOUD COMPUTING Pearson · IT Specialist SOFTWARE DEVELOPMENT Pearson · CompTIA ITF+ CERTIFIED · CompTIA Network+ CERTIFIED·CE · CompTIA CTT+ CERTIFIED

F5 ASEAN NGINX Super User · vmware CERTIFIED ASSOCIATE DATA CENTER VIRTUALIZATION · FORTINET CERTIFIED FUNDAMENTALS Cybersecurity · FORTINET NSE EXAM FortiGate Operator v7.4 · FORTINET CERTIFIED ASSOCIATE Cybersecurity · FORTINET NSE EXAM Introduction to the Threat Landscape v2.0 · peplink CERTIFIED SALES SPECIALIST · peplink CERTIFIED ENGINEER · peplink CERTIFIED ASSOCIATE · ace accredited configuration engineer

Company portfolio



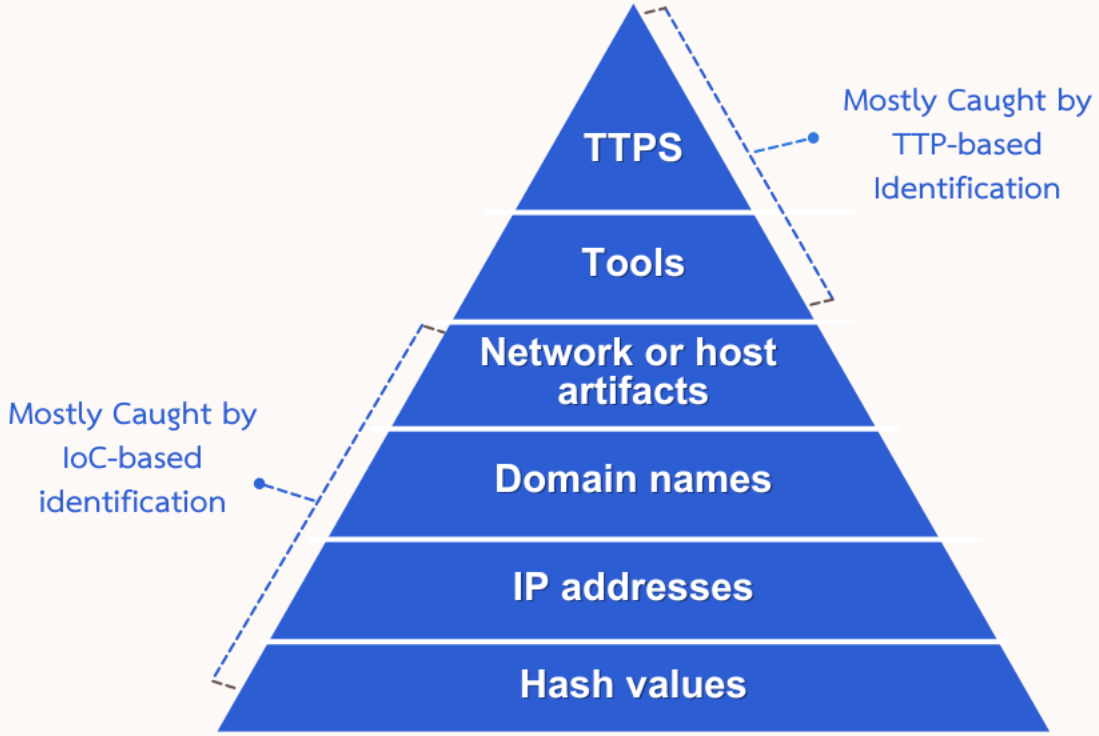
Speaker

- นาย เจษฎา ทองก้านเหลือง (ต้อม)
- กรรมการผู้จัดการ (Managing Director)
- บริษัท ที-เน็ต ไอที โซลูชัน จำกัด
- Certificate: CCNA, CEH, CHFI ,ECSA, CISO
- CompTIA Security+, CompTIA Project+, CompTIA Network+
- CompTIA CySA+, CompTIA Cloud+, Peplink Certified Engineer (PCE),
- Peplink Sales Specialist (PSS), Fortinet NSE1, Fortinet NSE2
- IT Specialist Certification (ITS): Cyber Security
- IT Specialist Certification (ITS): Network Security
- E-Mail : Jedsada@tnetitsolution.co.th
- Facebook: ผู้ดูแลกลุ่มสอนแฮกแบบหมู ๆ
- Website : www.tnetitsolution.co.th

Cyber Threat Intelligence

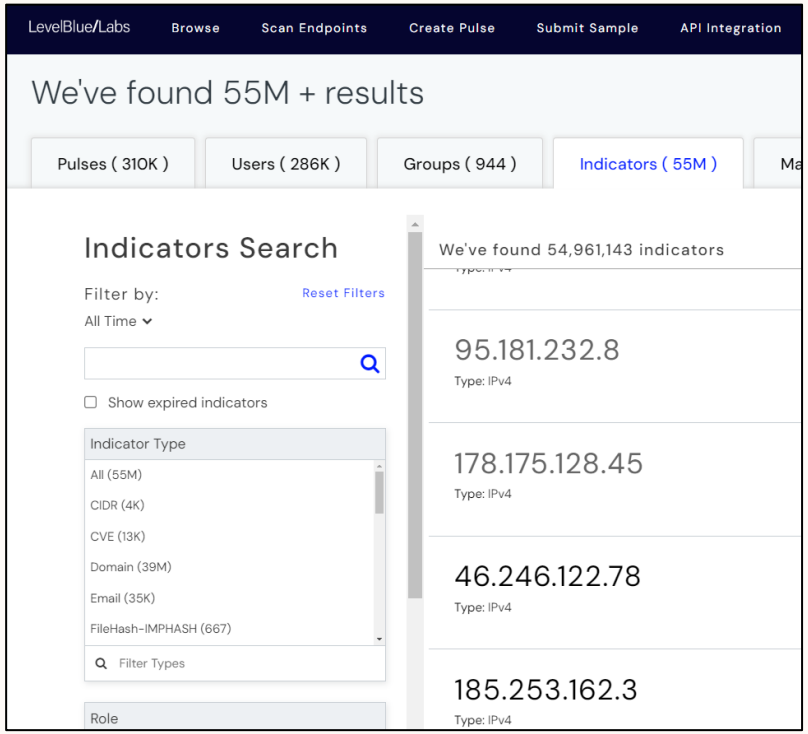
What is cyber threat intelligence?

- Threat intelligence involves gathering, analyzing, and sharing information about potential or current attacks on an organization's assets. Key aspects include:
  - **Indicators of Compromise (IOCs):** Signs of a breach, like unusual network traffic or malicious IP addresses.
  - **Tactics, Techniques, and Procedures (TTPs):** Methods used by attackers, including their strategies and tools.
  - **Threat Actors:** Details about the individuals or groups behind the threats, including their motives and activities.
  - **Vulnerabilities:** Weaknesses in systems that attackers can exploit.

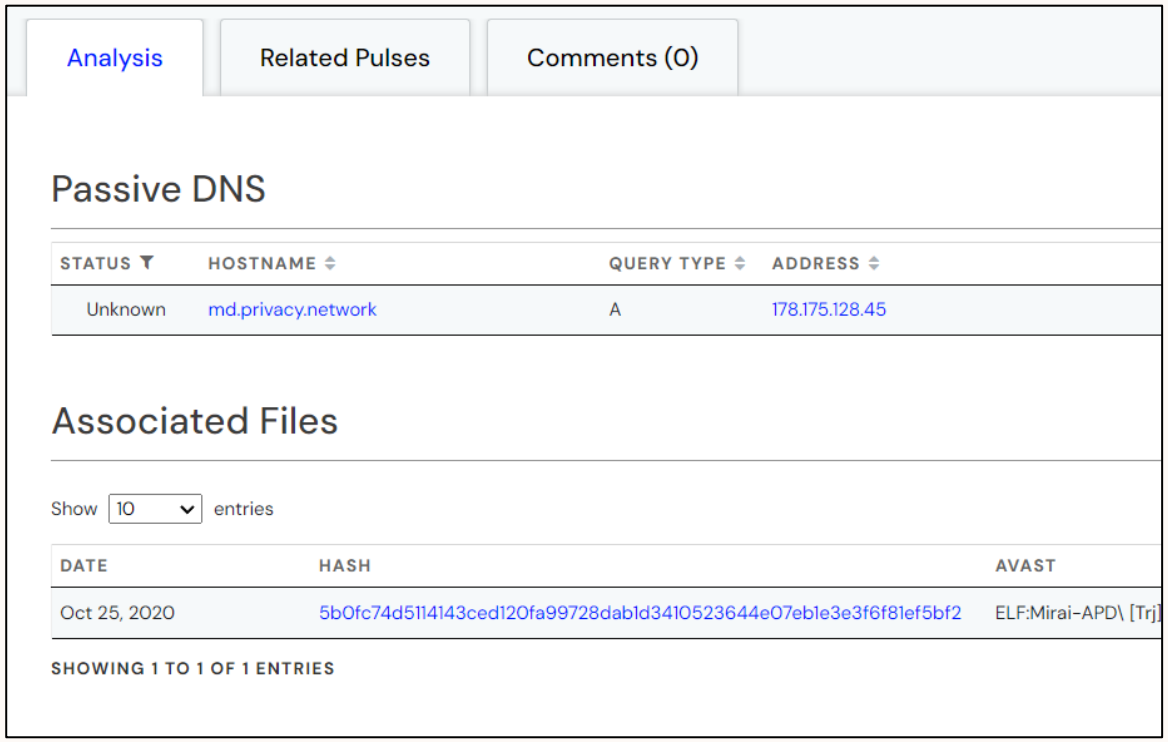


Example Indicators of Compromise

- https://otx.alienvault.com



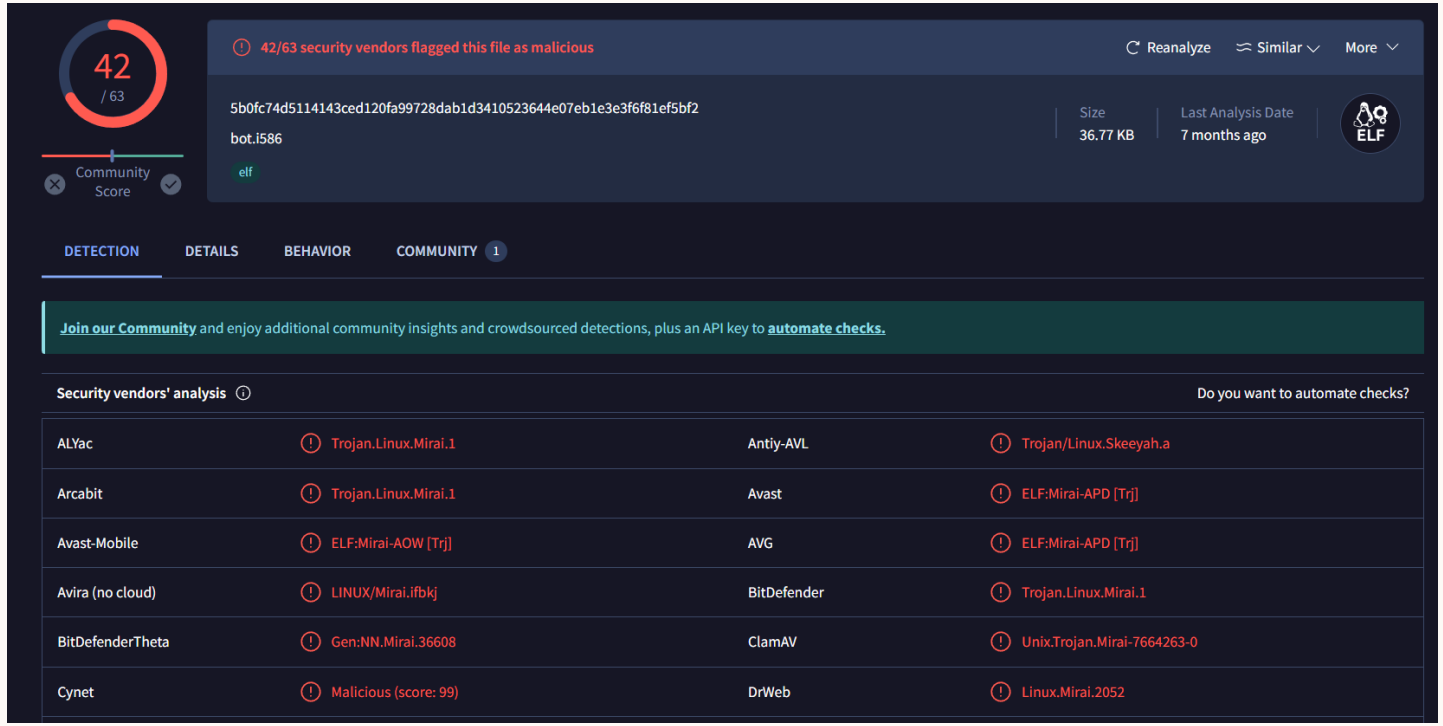
IP addresses Indicators



Hash Values

Example Indicators of Compromise

- https://www.virustotal.com



Acquire Infrastructure: Botnet

Other sub-techniques of Acquire Infrastructure (8)

Adversaries may buy, lease, or rent a network of compromised systems that can be used during targeting. A botnet is a network of compromised systems that can be instructed to perform coordinated tasks.[1] Adversaries may purchase a subscription to use an existing botnet from a booter/stresser service. With a botnet at their disposal, adversaries may perform follow-on activity such as large-scale Phishing or Distributed Denial of Service (DDoS).[2][3][4][5]

ID: T1583.005
Sub-technique of: T1583
Tactic: Resource Development
Platforms: PRE
Version: 1.0
Created: 01 October 2020
Last Modified: 15 April 2021

Version Permalink

Mirai is one of the first significant botnets targeting exposed networking devices running Linux. Found in August 2016 by MalwareMustDie, its name means "future" in Japanese. Nowadays it targets a wide range of networked embedded devices such as IP cameras, home routers (many vendors involved), and other IoT devices. Since the source code was published on "Hack Forums" many variants of the Mirai family appeared, infecting mostly home networks all around the world.

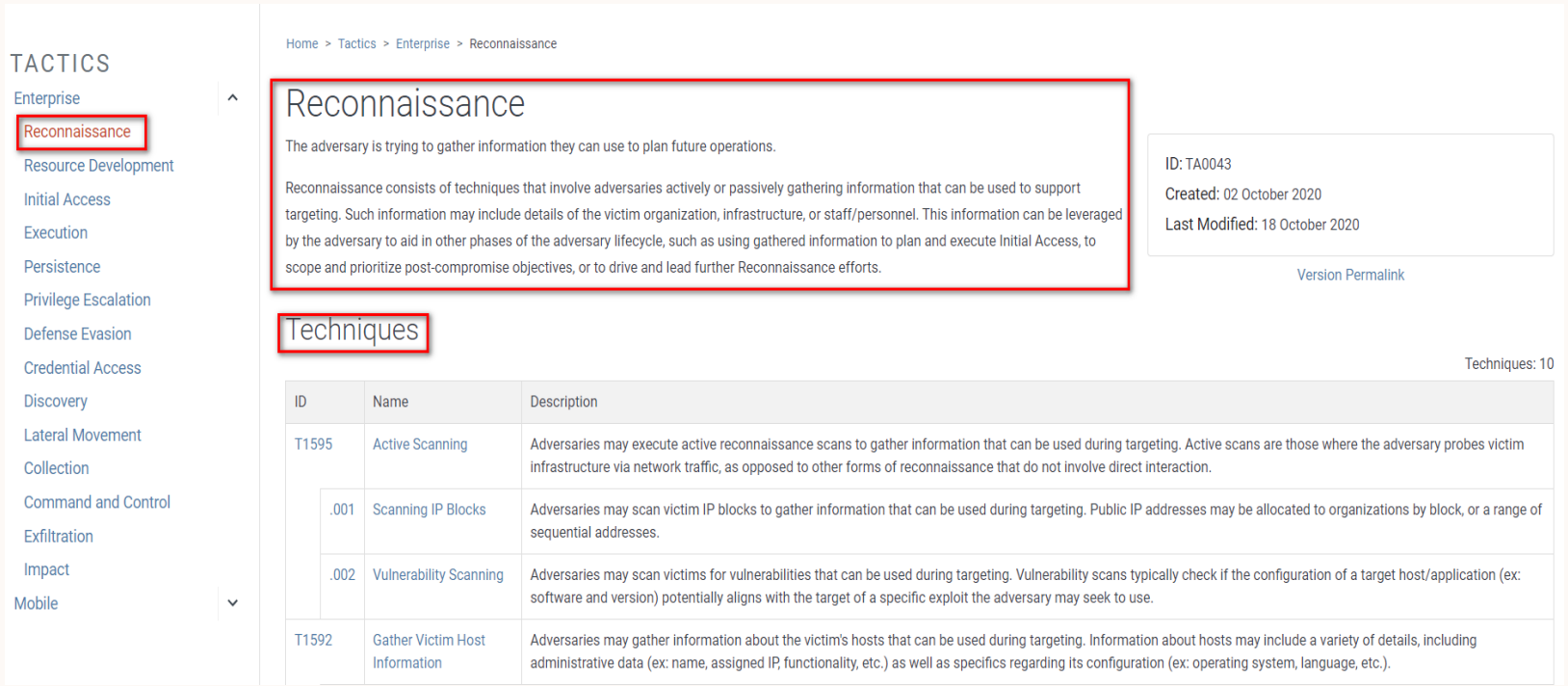
MITRE ATT&CK

- MITRE ATT&CK is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community
- **Website:** https://attack.mitre.org

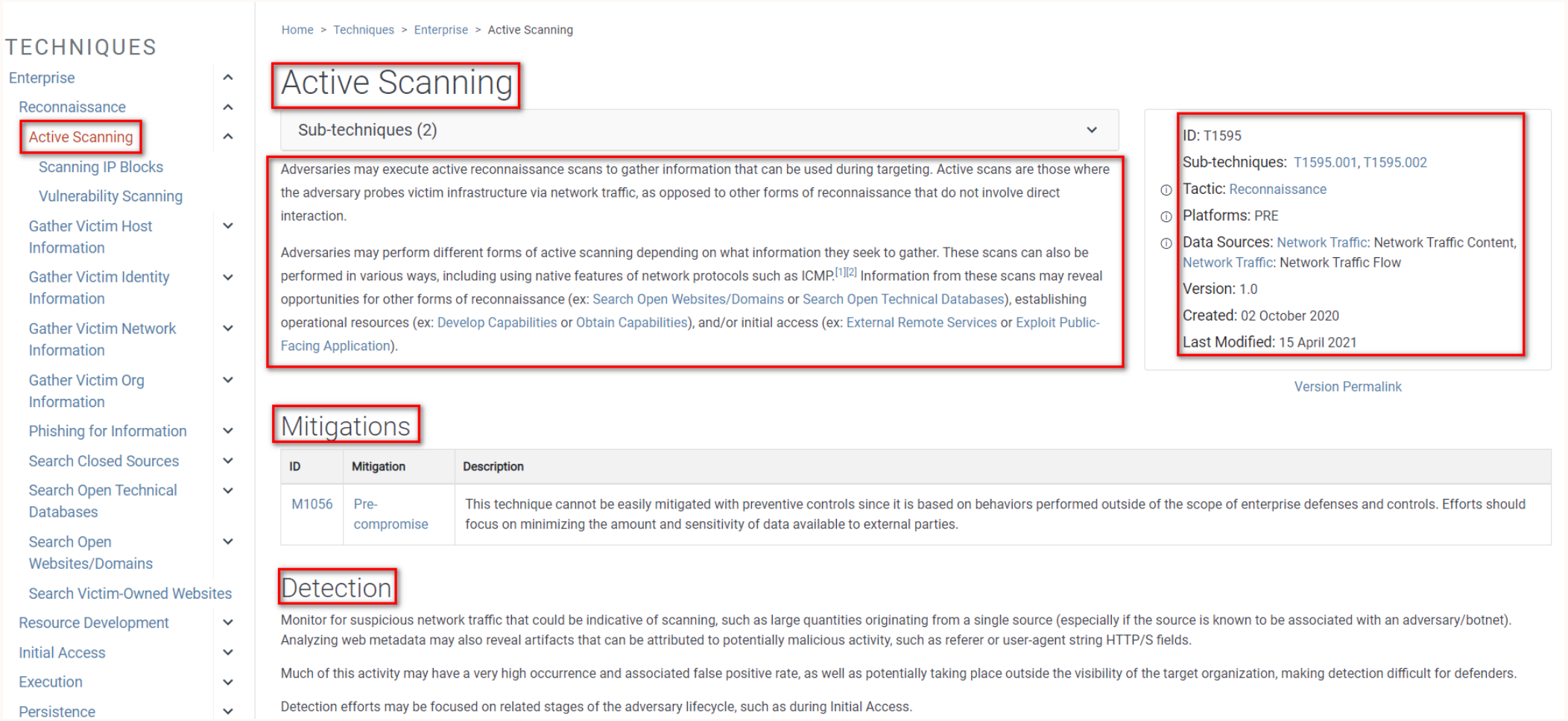
ATT&CK Matrix for Enterprise

ATT&CK Enterprise Tactics

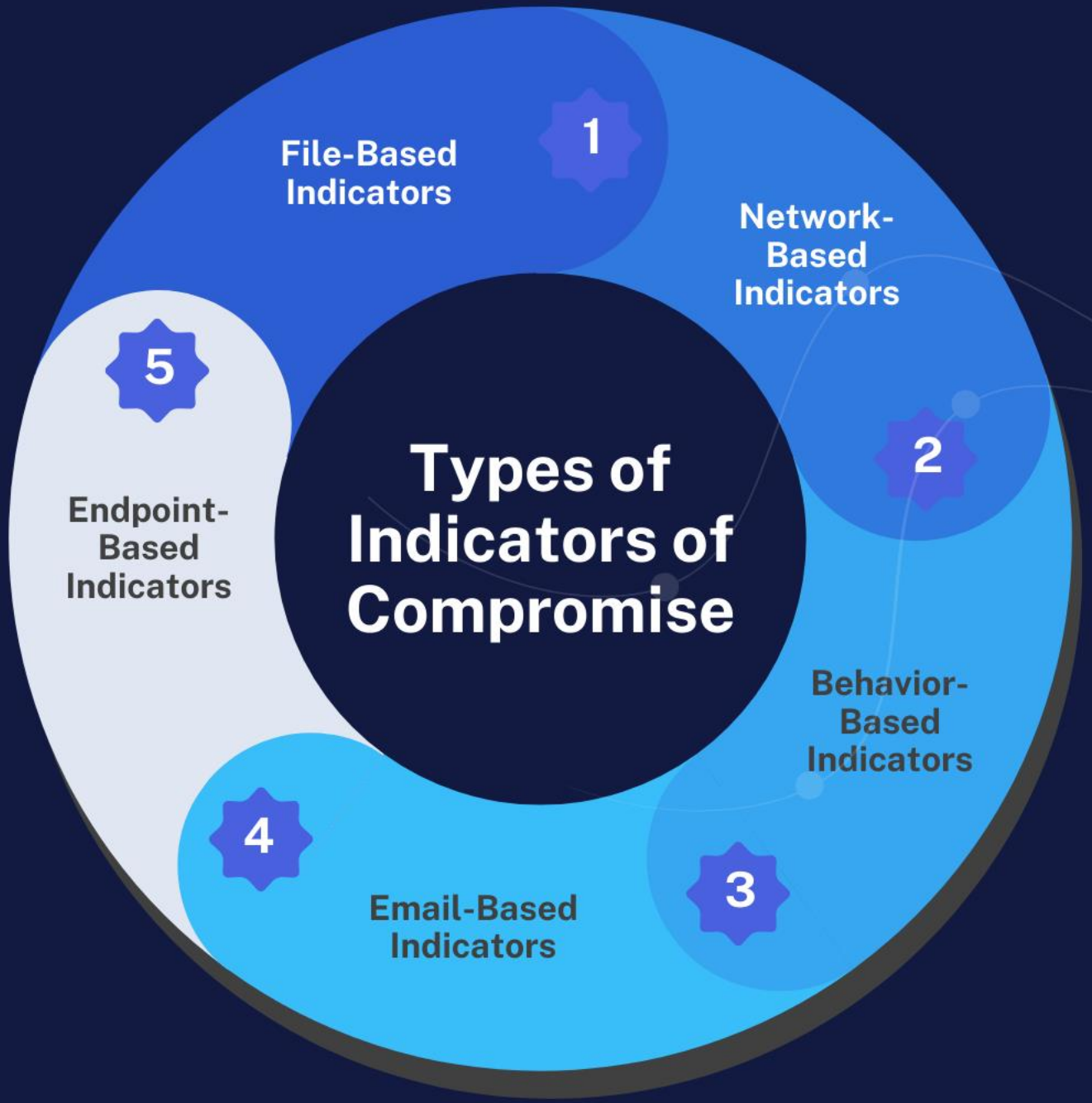
ID	NAME	DESCRIPTION
TA0043	Reconnaissance	รวบรวมข้อมูลก่อนการโจมตี หาข้อมูลของเป้าหมายให้ได้มากที่สุด
TA0042	Resource Development	เตรียมเครื่องมือเพื่อโจมตีเป้าหมาย ทั้งเขียนเอง ซื้อ หรือ ขโมยมา
TA0001	Initial Access	การโจมตีเป้าหมาย หรือ เชื่อมต่อไปยังระบบเครื่องที่ต้องการโจมตี
TA0002	Execution	สั่งการโปรแกรมที่เตรียมไว้ หรือ Code ที่อันตรายที่เป้าหมาย
TA0003	Persistence	สร้างรากฐานว่าการสั่งการไม่ถูกขัดขวางคงอยู่ได้ตลอด
TA0004	Privilege Escalation	ยกสิทธิการเข้าถึงระบบ ให้สามารถเข้าถึงได้ทุกระบบ
TA0005	Defense Evasion	หลบเลี่ยงโปรแกรมตรวจจับหรือโปรแกรมสังเกตความผิดปกติ
TA0006	Credential Access	ขโมยรหัสและบัญชีผู้ใช้ และทำการเข้าสู่ระบบ
TA0007	Discovery	ตรวจสอบขีดความสามารถในการเชื่อมต่อและระบบที่มีการใช้งาน เพื่อขโมยเครื่องอื่นๆต่อ
TA0008	Lateral Movement	เคลื่อนย้ายไปตำแหน่ง , เครื่อง หรือเป้าหมายที่มีข้อมูลที่ต้องการ
TA0009	Collection	ทำการเตรียมดึงข้อมูลออกจากระบบ หรือ เป้าหมาย
TA0011	Command and Control	ทำการเชื่อมต่อเครื่องเป้าหมายไปสู่เครื่องเก็บข้อมูลหลักของผู้โจมตี
TA0010	Exfiltration	ทำการส่งข้อมูล นำข้อมูลออก
TA0040	Impact	ทำลายหลักฐานการมีอยู่ หรือ การเรียกค่าไถ่ หรือทำลายระบบทิ้ง



ATT&CK Matrix for Enterprise



Ref: https://attack.mitre.org


Types of Indicators of Compromise
1
File-Based Indicators
2
Network-Based Indicators
3
Behavior-Based Indicators
4
Email-Based Indicators
5
Endpoint-Based Indicators

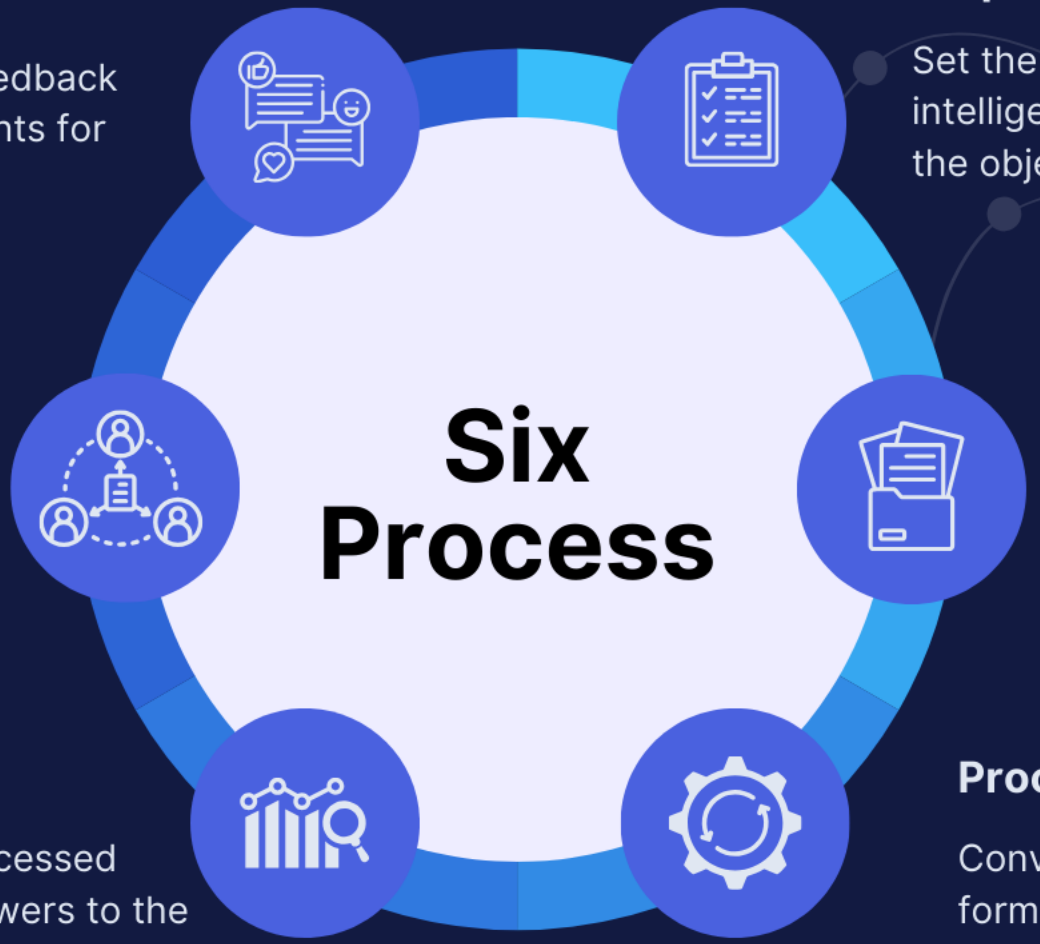
Why is Threat Intelligence Important?

- In cybersecurity, advanced persistent threats (APTs) and defenders are constantly outmaneuvering each other. Threat intelligence is crucial for:
  - Illuminating the unknown, allowing security teams to make better decisions.
  - Empowering cybersecurity stakeholders by revealing adversarial motives and TTPs.
  - Helping security professionals understand threat actors' decision-making processes.
  - Enabling business stakeholders (executive boards, CISOs, CIOs, CTOs) to invest wisely, mitigate risk, increase efficiency, and make faster decisions.

Who Benefits from Threat Intelligence?

Function	Benefits
Sec/IT Analyst	Optimize prevention and detection capabilities and strengthen defenses
SOC	Prioritize incidents based on risk and impact to the organization
CSIRT	Accelerate incident investigations, management, and prioritization
Intel Analyst	Uncover and track threat actors targeting the organization
Executive Management	Understand the risks the organization faces and what the options are to address their impact

The Threat Intelligence Lifecycle



Feedback

Receive stakeholder feedback and establish adjustments for future

Requirements

Set the roadmap for the threat intelligence operation, defining the objectives and goals.

Dissemination

Translating analysis into digestible format for stakeholders

Collection

Gather information from various sources to satisfy the defined objectives.

Analysis

Analyze the processed data to find answers to the questions posed during the requirements phase.

Processing

Convert raw data into a format suitable for analysis, ensuring it is organized and structured.

use cases by function

Function	Use Cases
Sec/IT Analyst	▪ Integrate TI feeds with other security products ▪ Block bad IPs, URLS, domains, files etc
SOC	▪ Use TI to enrich alerts ▪ Link alerts together into incidents ▪ Tune newly deployed security controls
CSIRT	▪ Look for information on the who/what/why/when/how of an incident ▪ Analyze root cause to determine scope of the incident
Intel Analyst	▪ Look wider and deeper for intrusion evidence ▪ Review reports on threat actors to better detect them
Executive Management	▪ Assess overall threat level for the organization ▪ Develop security roadmap

Types Intelligence

TACTICAL

Focused on performing malware analysis & enrichment, as well as ingesting atomic, static, and behavioral threat indicators into defensive cyber security systems.

STAKEHOLDERS:

- SOC Analyst
- SIEM
- Firewall
- Endpoints
- IDS/IPS

OPERATIONAL

Focused on understanding adversarial capabilities, infrastructure, & TTPs, and then leveraging that understanding to conduct more targeted and prioritized cybersecurity operations.

STAKEHOLDERS:

- Threat Hunter
- SOC Analyst
- Vulnerability Mgmt.
- Incident Response
- Insider Threat

STRATEGIC

Focused on understanding high level trends and adversarial motives, and then leveraging that understanding to engage in strategic security and business decision-making

STAKEHOLDERS:

- CISO
- CIO
- CTO
- Executive Board
- Strategic Intel

Top 10 Cyber Threat Intelligence

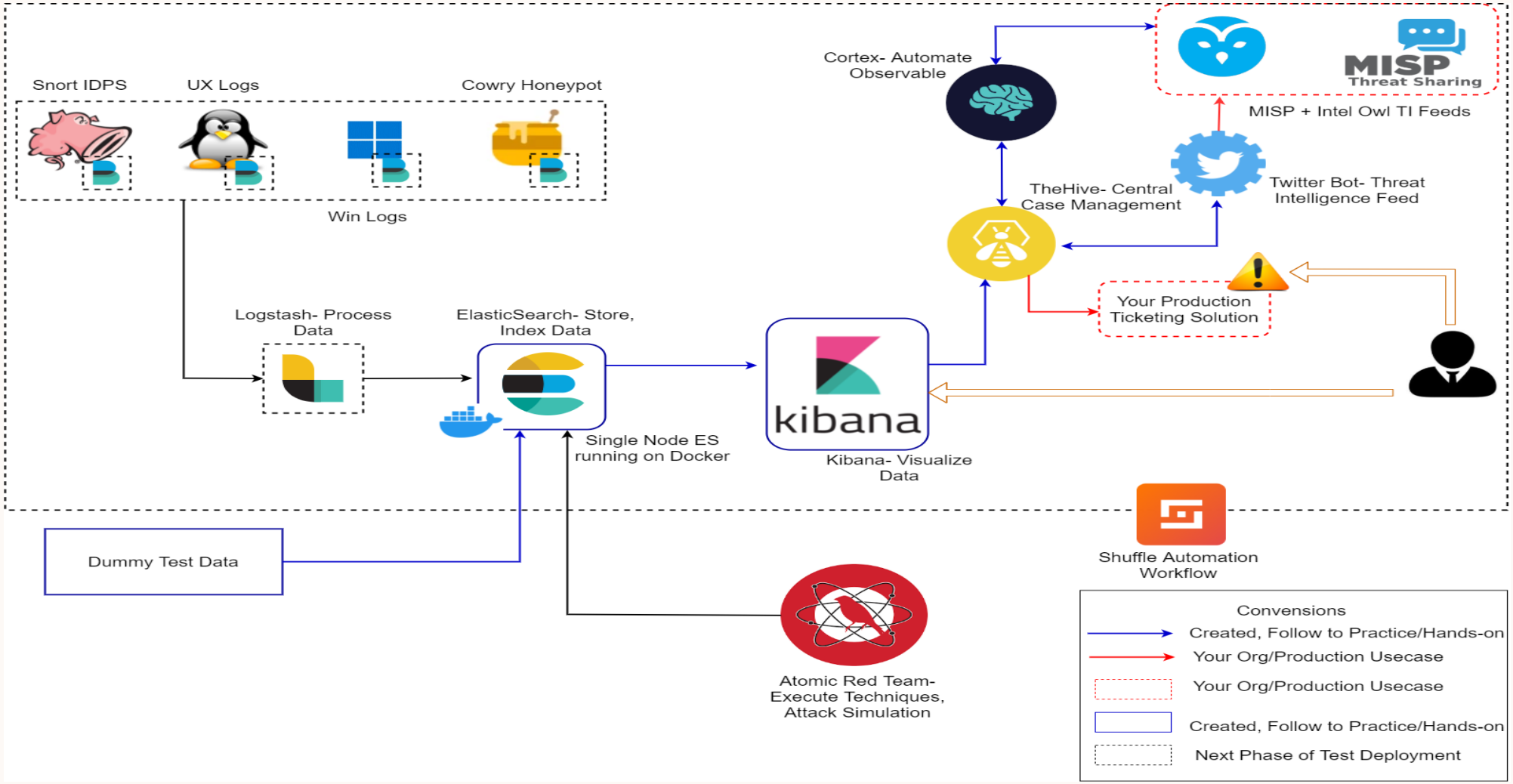
- AlienVault Open Threat Exchange (OTX)
- CTI4SOC
- DOCGuard
- GreyNoise
- Intezer
- MISP Threat Sharing
- OpenCTI - Open Cyber Threat Intelligence Platform
- PhishTank
- Pulsedive
- VirusTotal

Malware Information Sharing Platform: MISP

Malware Information Sharing Platform

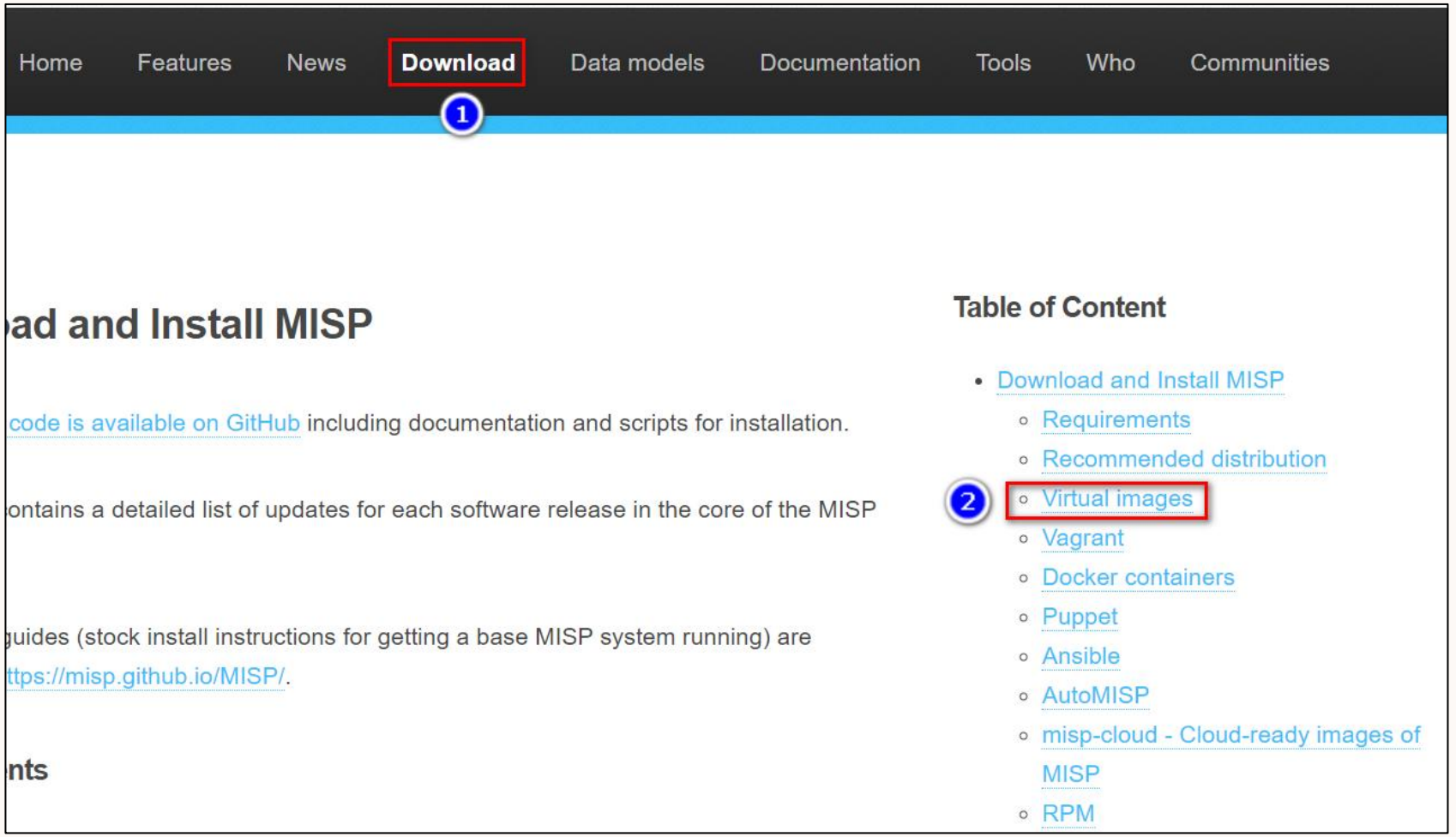
- MISP (Malware Information Sharing Platform & Threat Sharing) is an **open-source threat intelligence platform**. It enables the sharing, storing, and correlation of **threat intelligence** data among multiple organizations. The platform helps improve the **detection**, **prevention**, and **mitigation** of **cybersecurity threats** by allowing organizations to share threat data in a structured format.
- **Website:** https://www.misp-project.org
- **Download:** https://www.misp-project.org/download
- **Documentation:** https://www.misp-project.org/documentation

Architecture-Diagram



MISP: Download and Install

MISP: Download



- ❑ Click Download
- ❑ Click Virtual Images

MISP: Download Vmware images

Virtual images

If you would like to test MISP and don't want to do an installation, CIRCL generates automatically VMware images and VirtualBox at each MISP core commit. Available at https://vm.misp-project.org/. The image is to be used for testing purposes only, production-use is considered to be dangerous as is, it contains much more than MISP alone but also misp-dashboard and viper which requires additional security review before being in production.

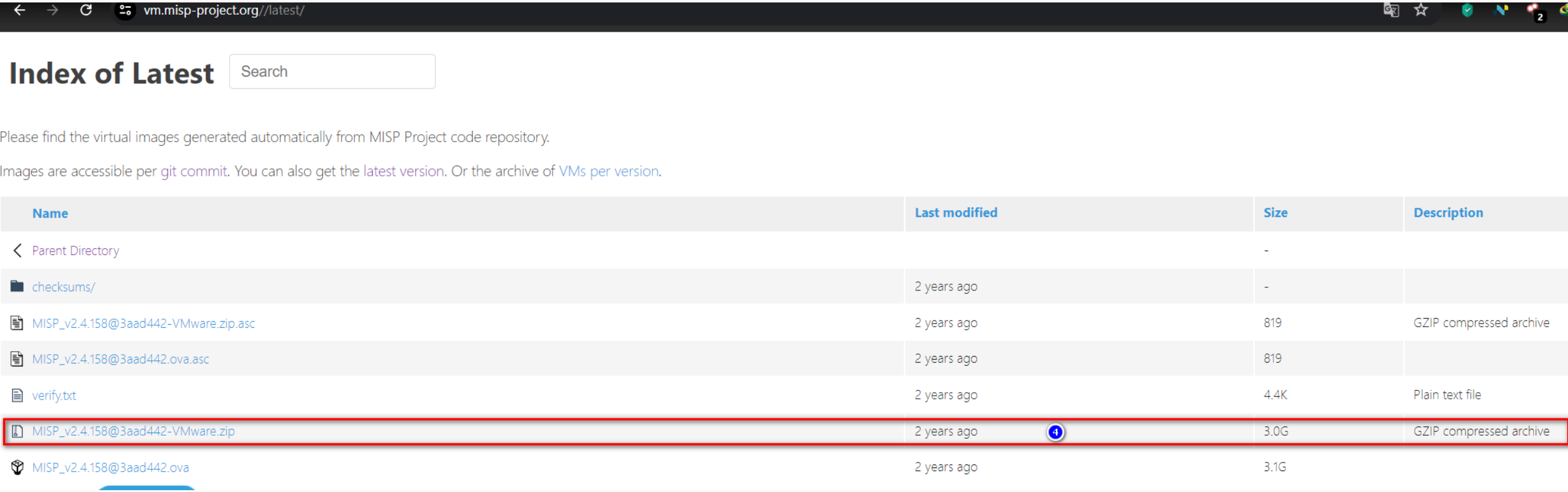
The default credentials for the automatically generated virtual machines are the following:

```
For the MISP web interface -> admin@admin.test:admin
For the system -> misp:Password1234
Please add the following forwards on your VM Host:

VBoxManage controlvm MISP_VM_NAME natpf1 www,tcp,,8080,,80
VBoxManage controlvm MISP_VM_NAME natpf1 ssh,tcp,,2222,,22
VBoxManage controlvm MISP_VM_NAME natpf1 dashboard,tcp,,8001,,8001
```

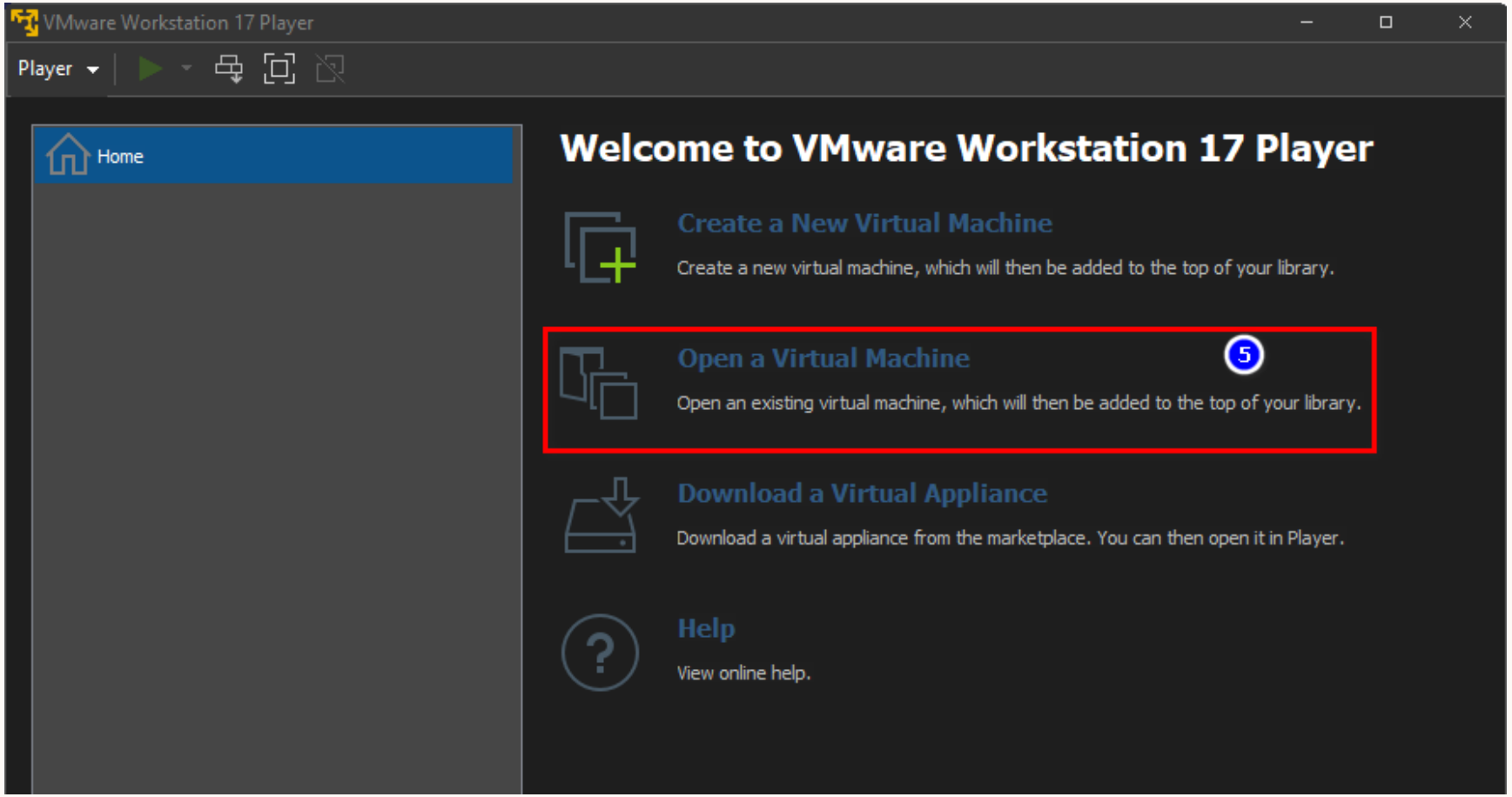
MISP: Download Vmware images

- https://vm.misp-project.org//latest



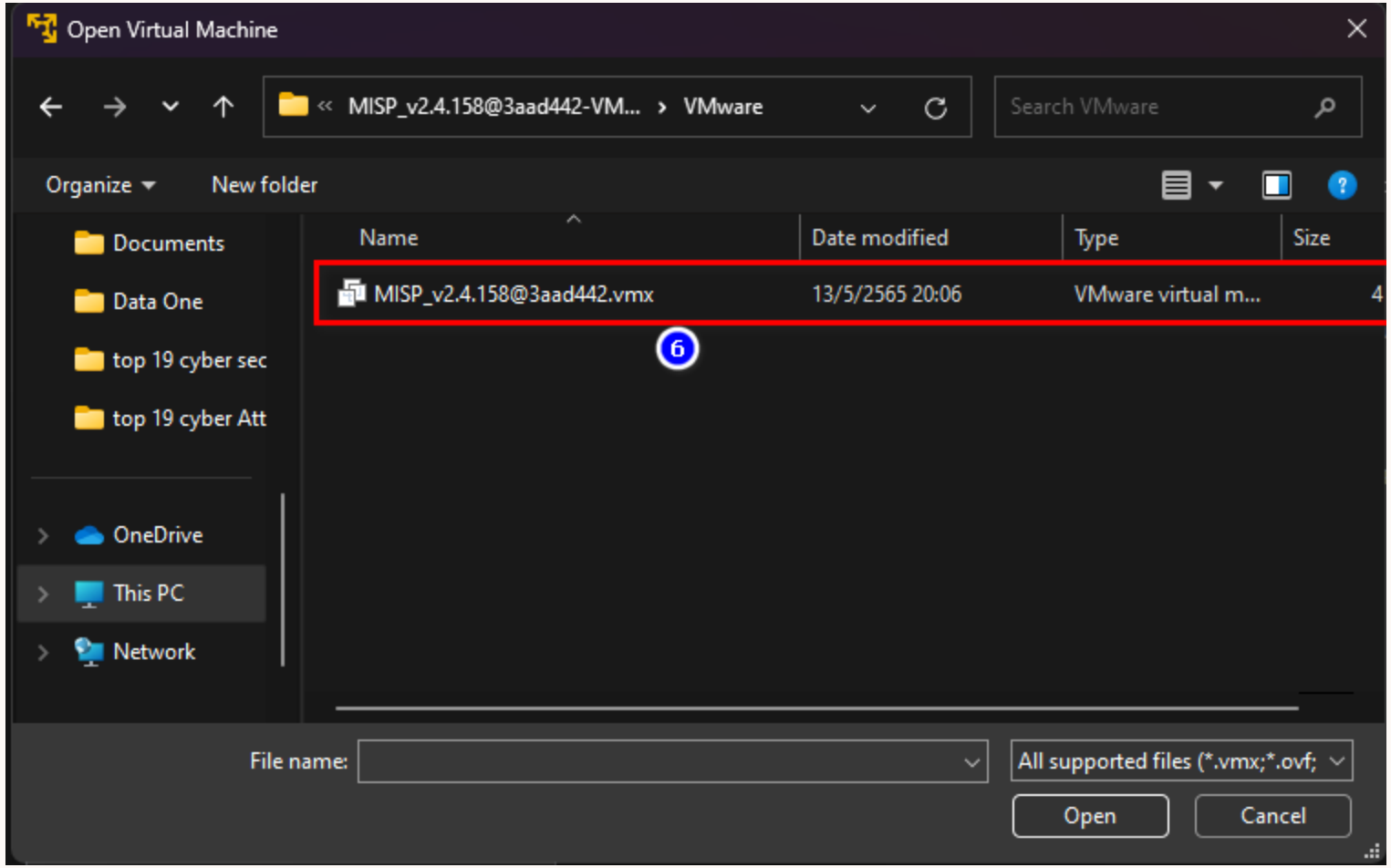
MISP: Open File

- Click Open a Virtual Machine



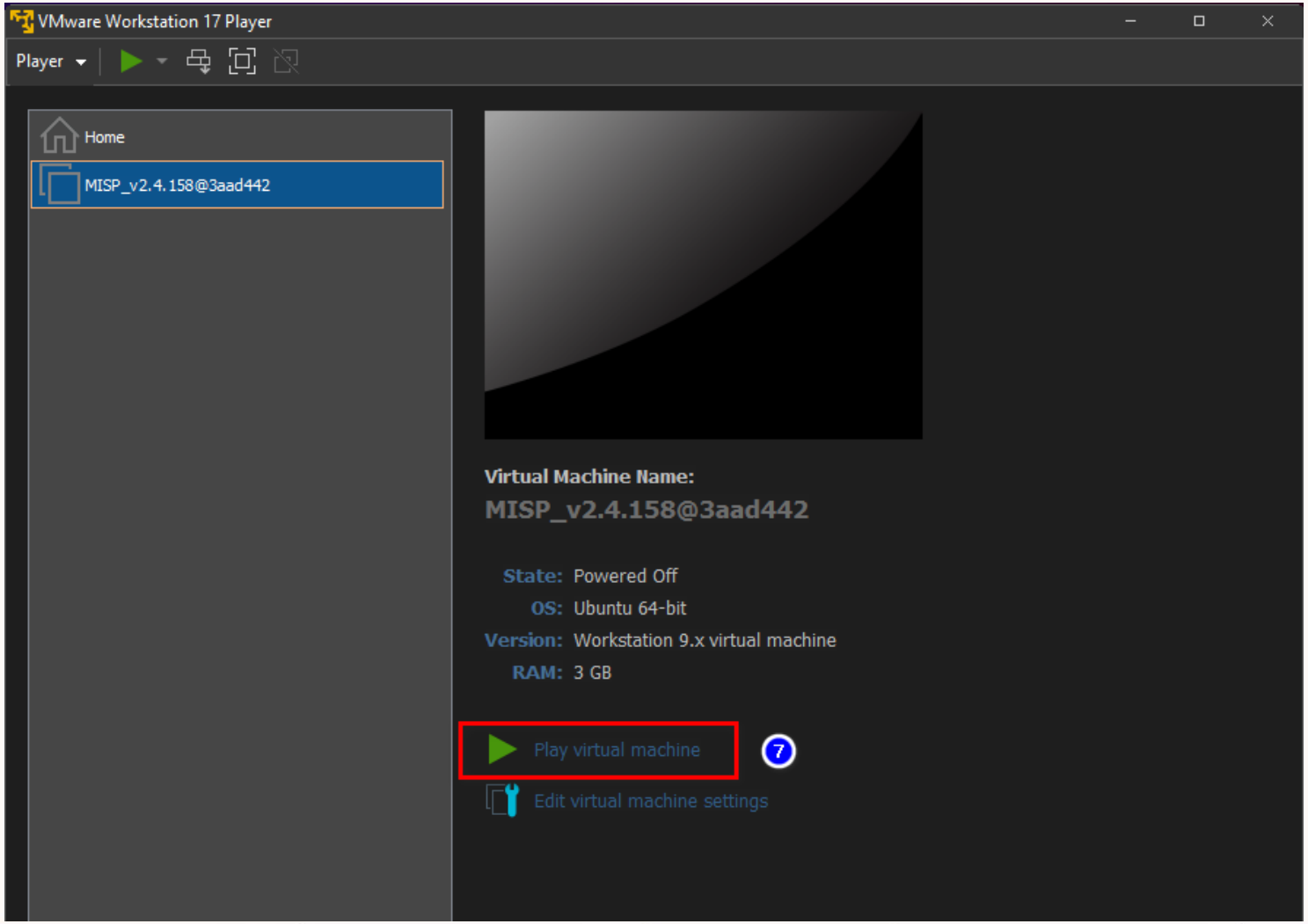
MISP: Open File on Vmware

- Select file :
  MISP_v2.4.158@3aad442.vmx
- Click Open

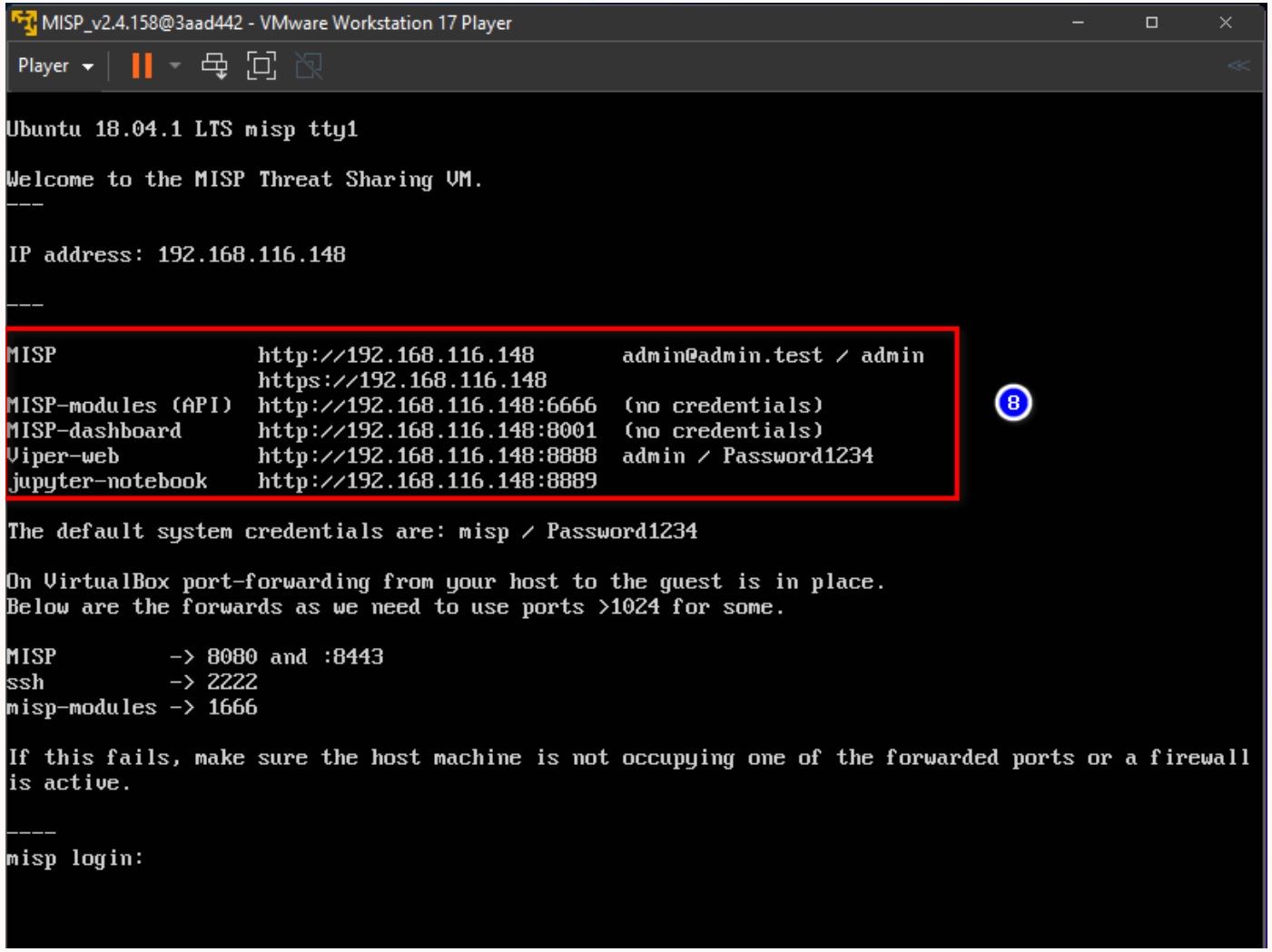


MISP: Open File on Vmware

- Click Play virtual machine



MISP: Open File on Vmware



System

User: misp

Pass: Password1234

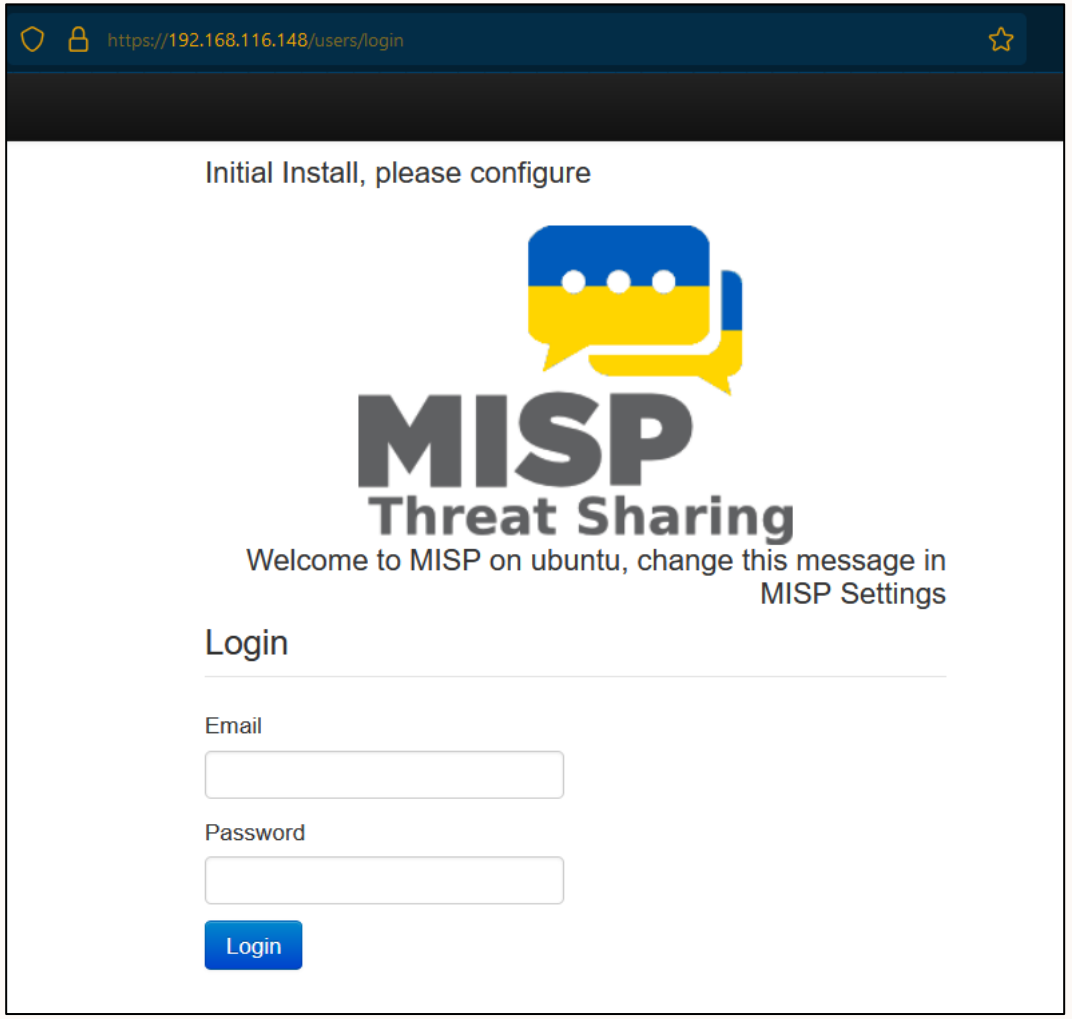
MISP: Web Interface

- https://192.168.116.148

Web interface

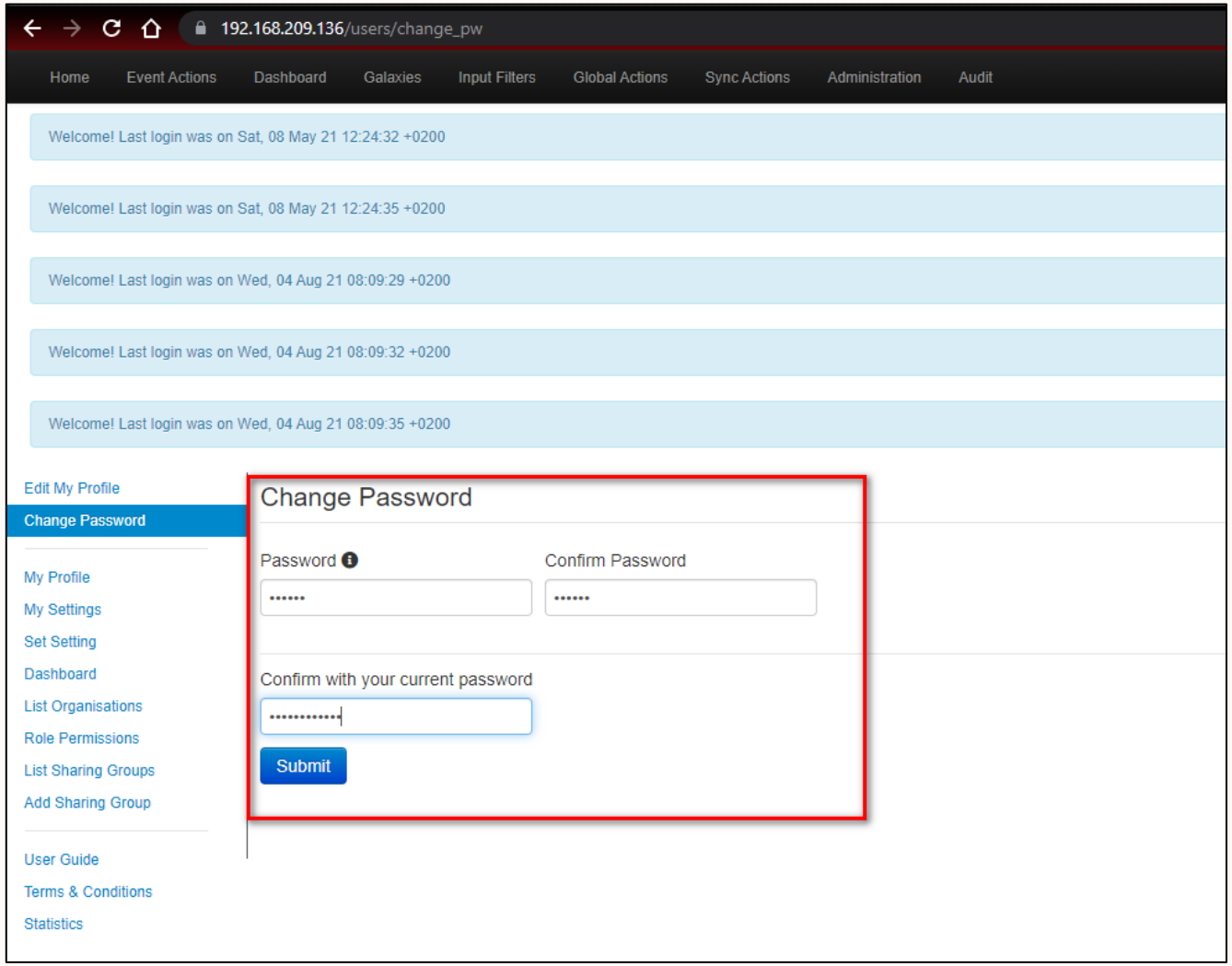
User: admin@admin.test

Pass: admin



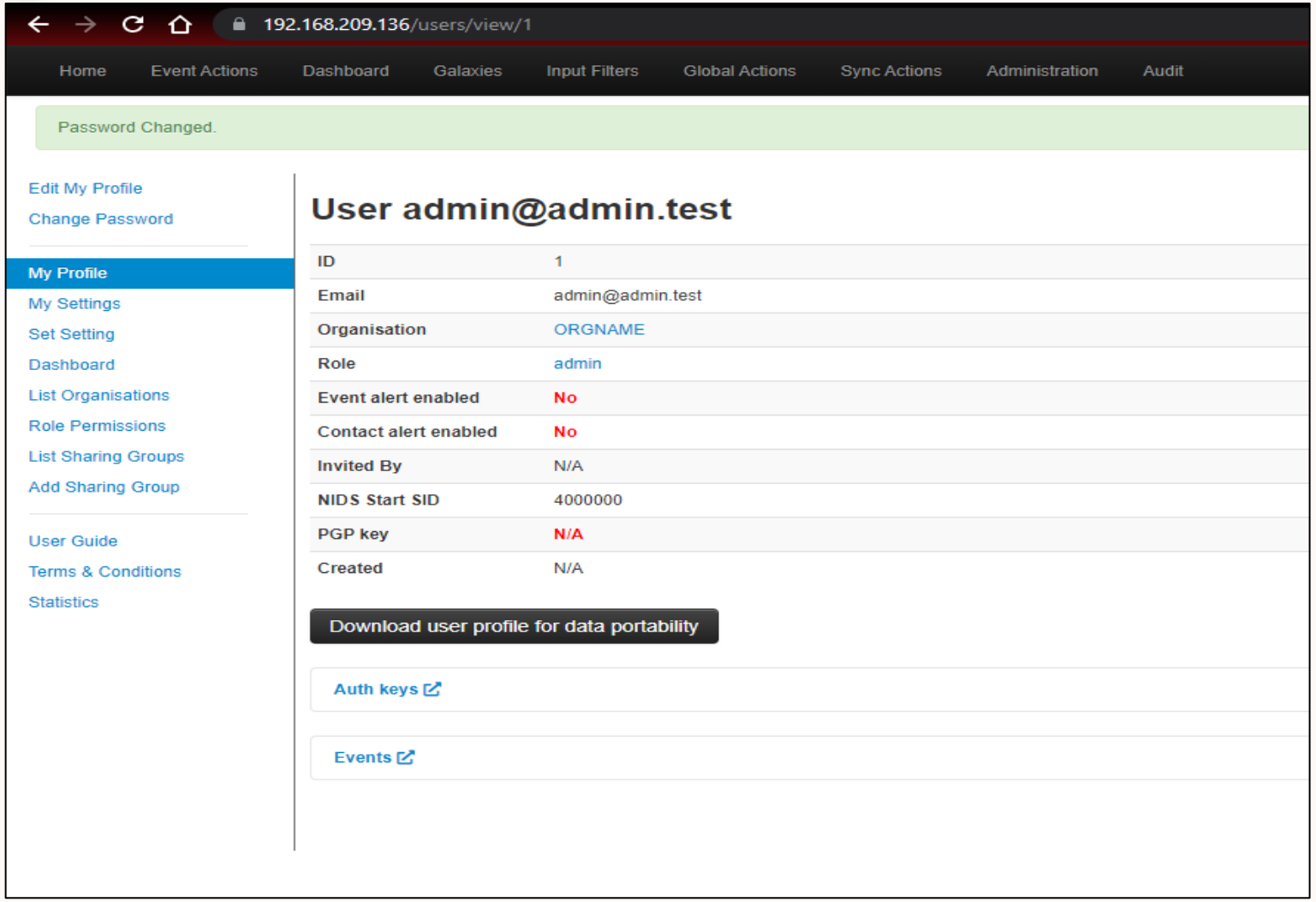
MISP: Change Password

- Change Password
- Click Submit



MISP: My Profile

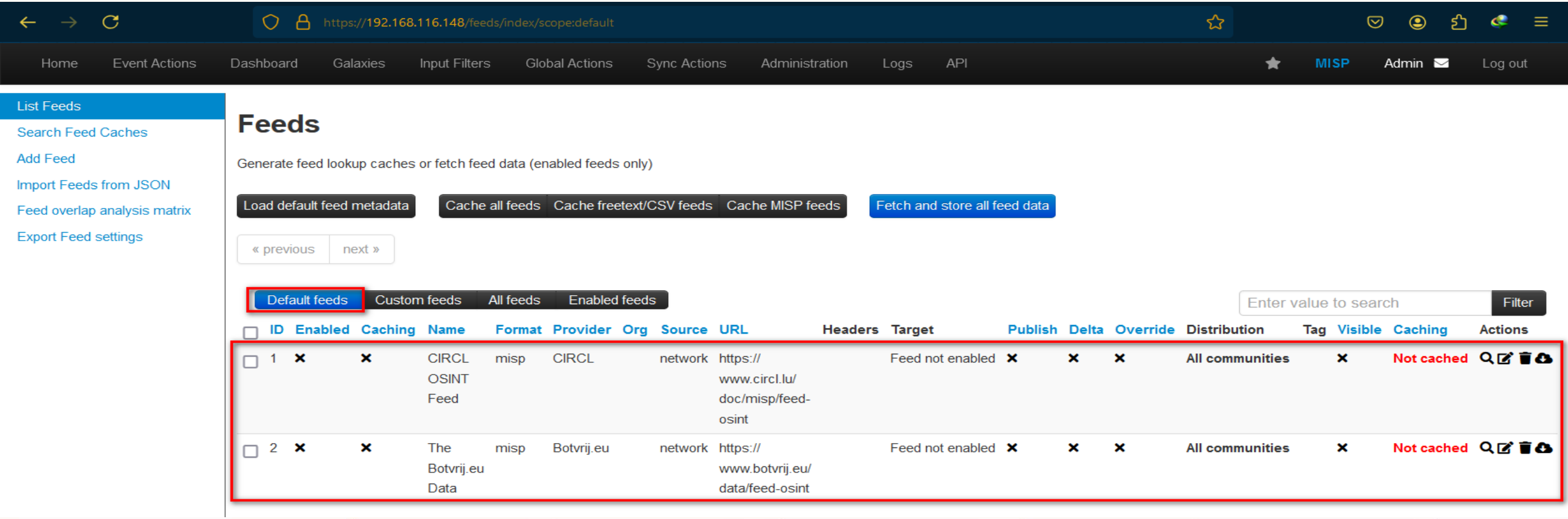
- Click My Profile



Threat Intelligence Feeds

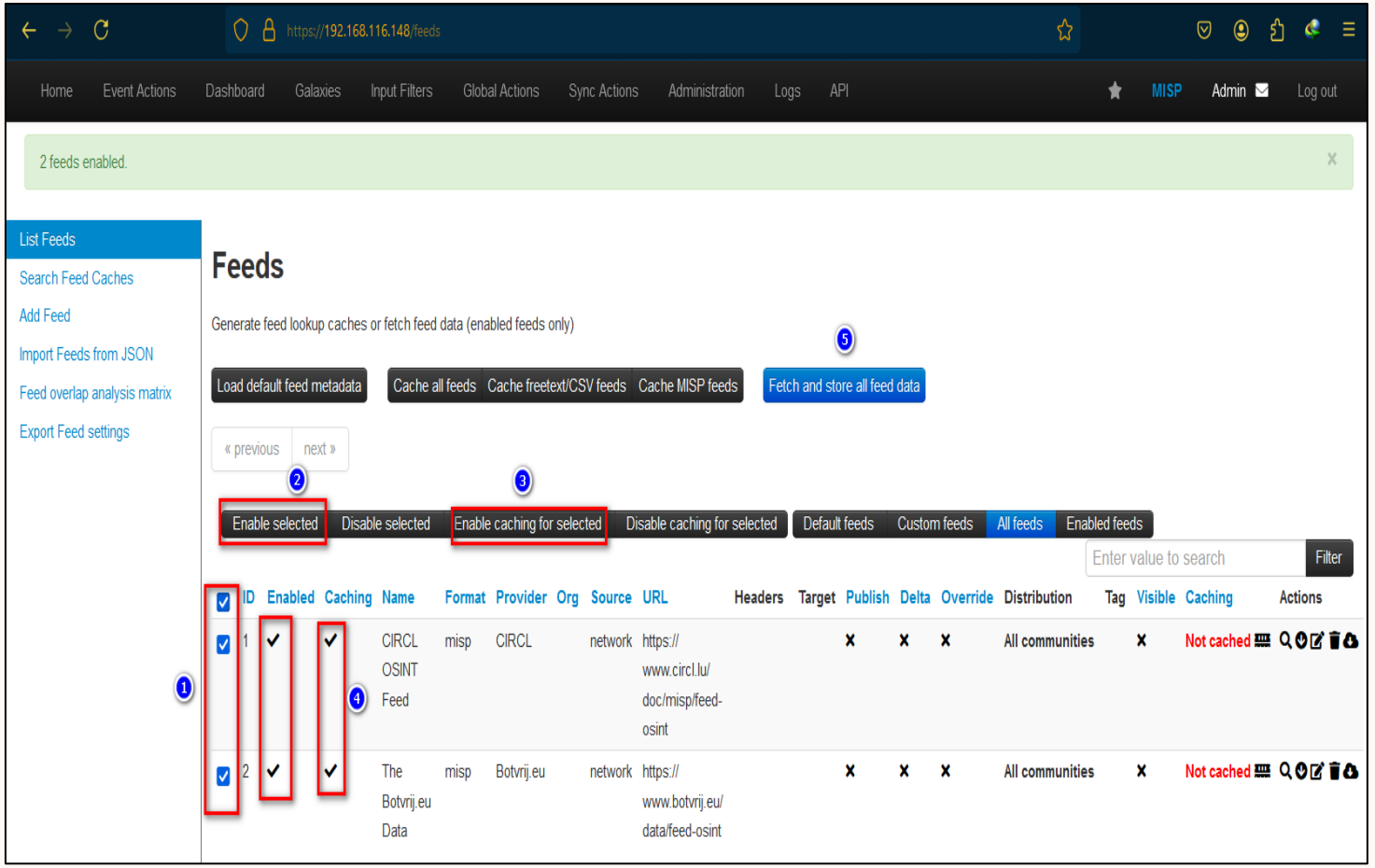
MISP: List Feeds

❑Sync Actions ➔ List Feeds



MISP: Enable Feeds

- ❑ Select Feeds
- ❑ Click Enable selected
- ❑ Click Enable caching for selected
- ❑ Click Fetch and store all feed data



Threat intelligence platform

AlienVault

https://otx.alienvault.com

VirusTotal

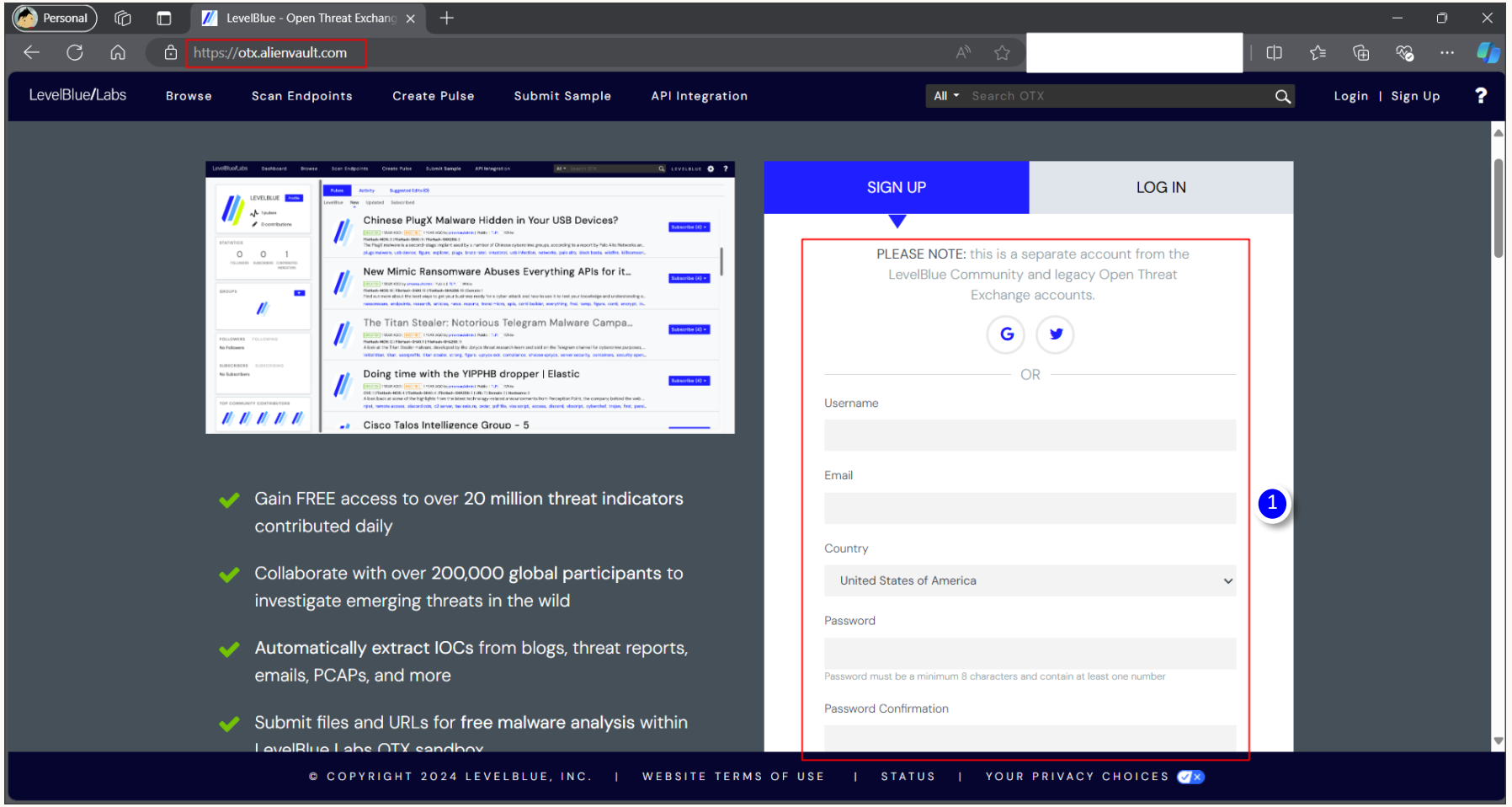
https://www.virustotal.com

PhishTank

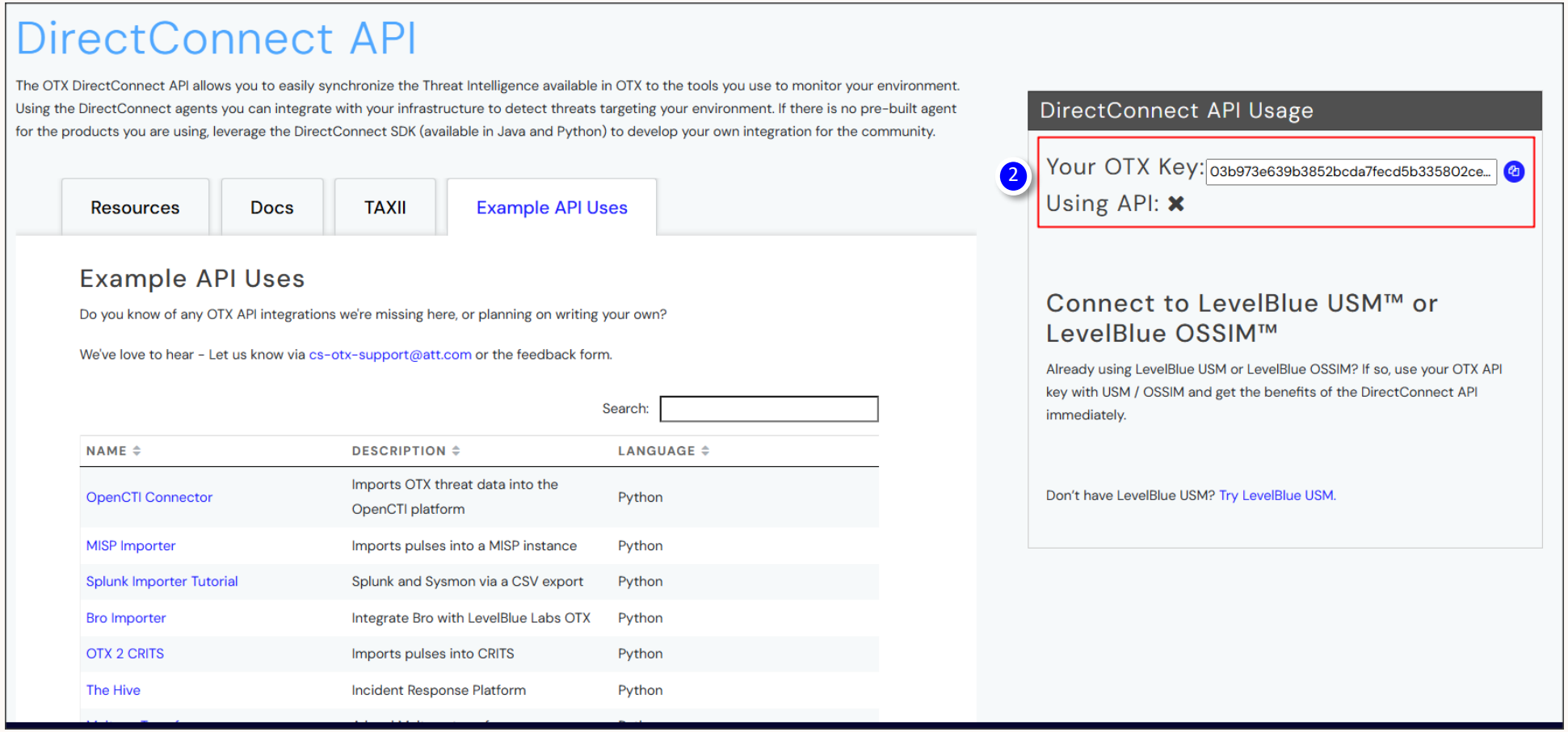
https://www.phishtank.com

Threat Intelligence Feeds: API

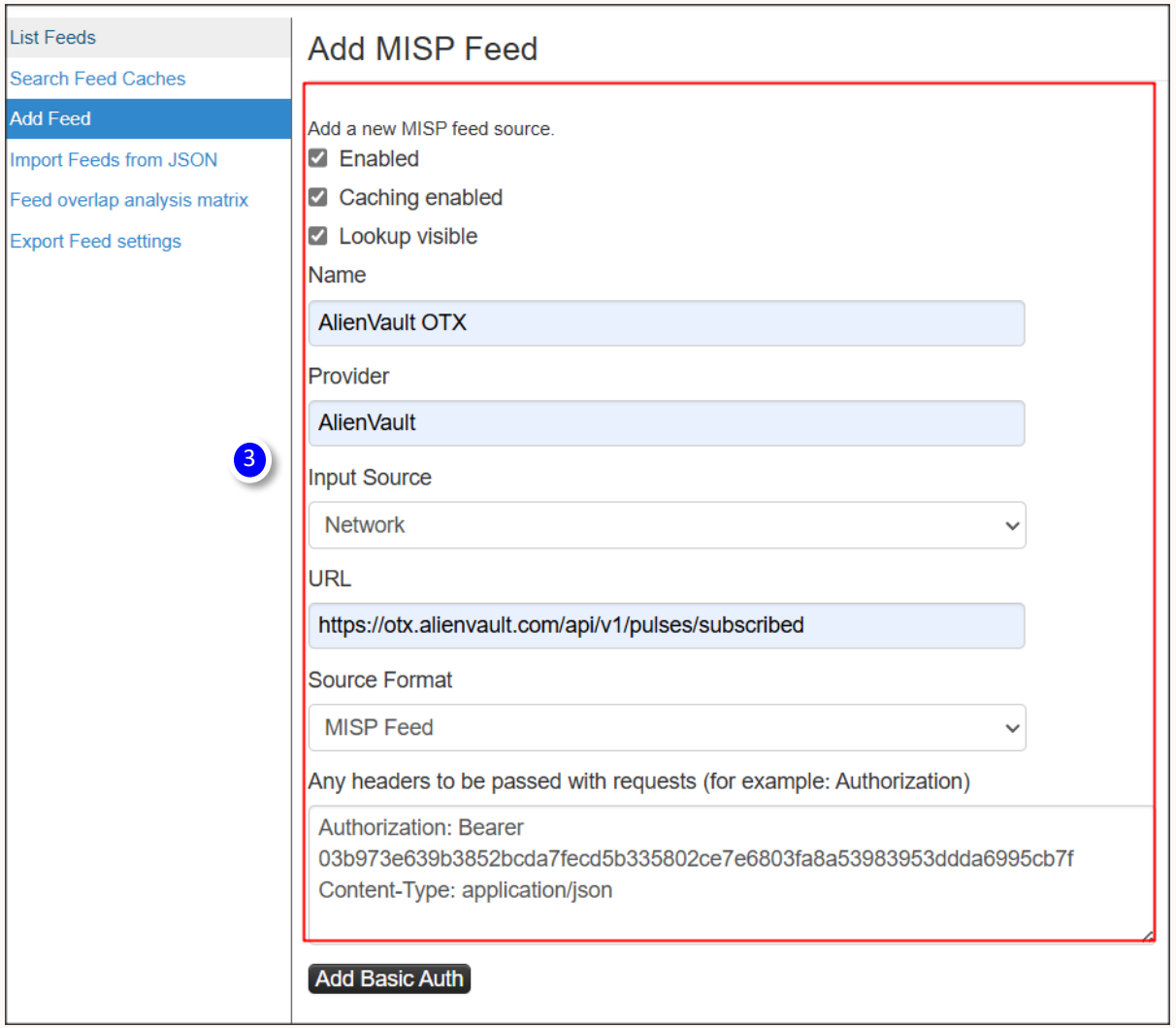
MISP: Add API Feeds



MISP: Add API Feeds

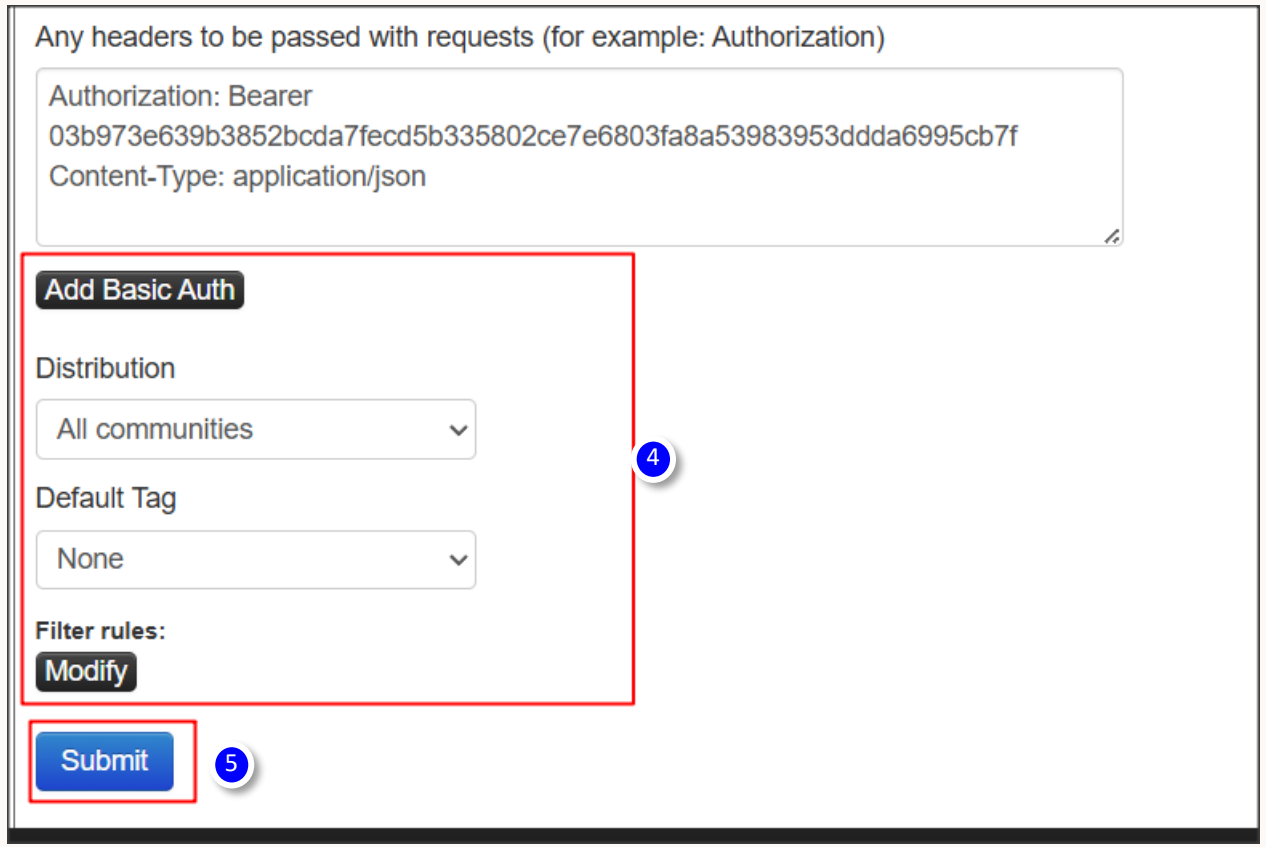


MISP: Add API Feeds



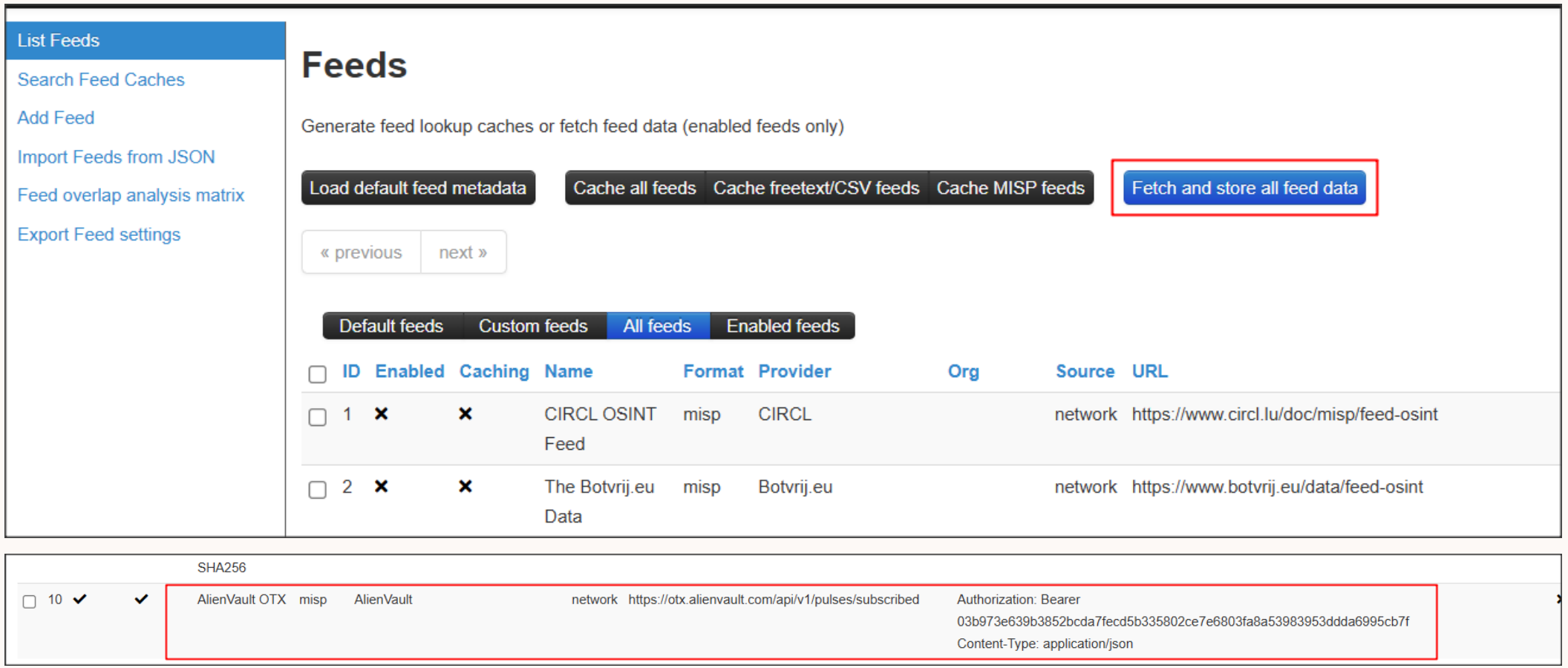
- Name: AlienVault OTX
- Provider: AlienVault
- Input Source: Network
- URL: https://otx.alienvault.com/api/v1/pulses/subscribed
- Source Format: MISP Feed
- Headers:
- Authorization: Bearer 848249a584bdabb281287fd9d9297da25e26d2b392c925109e156b48f20fa115
  Content-Type: application/json

MISP: Add API Feeds



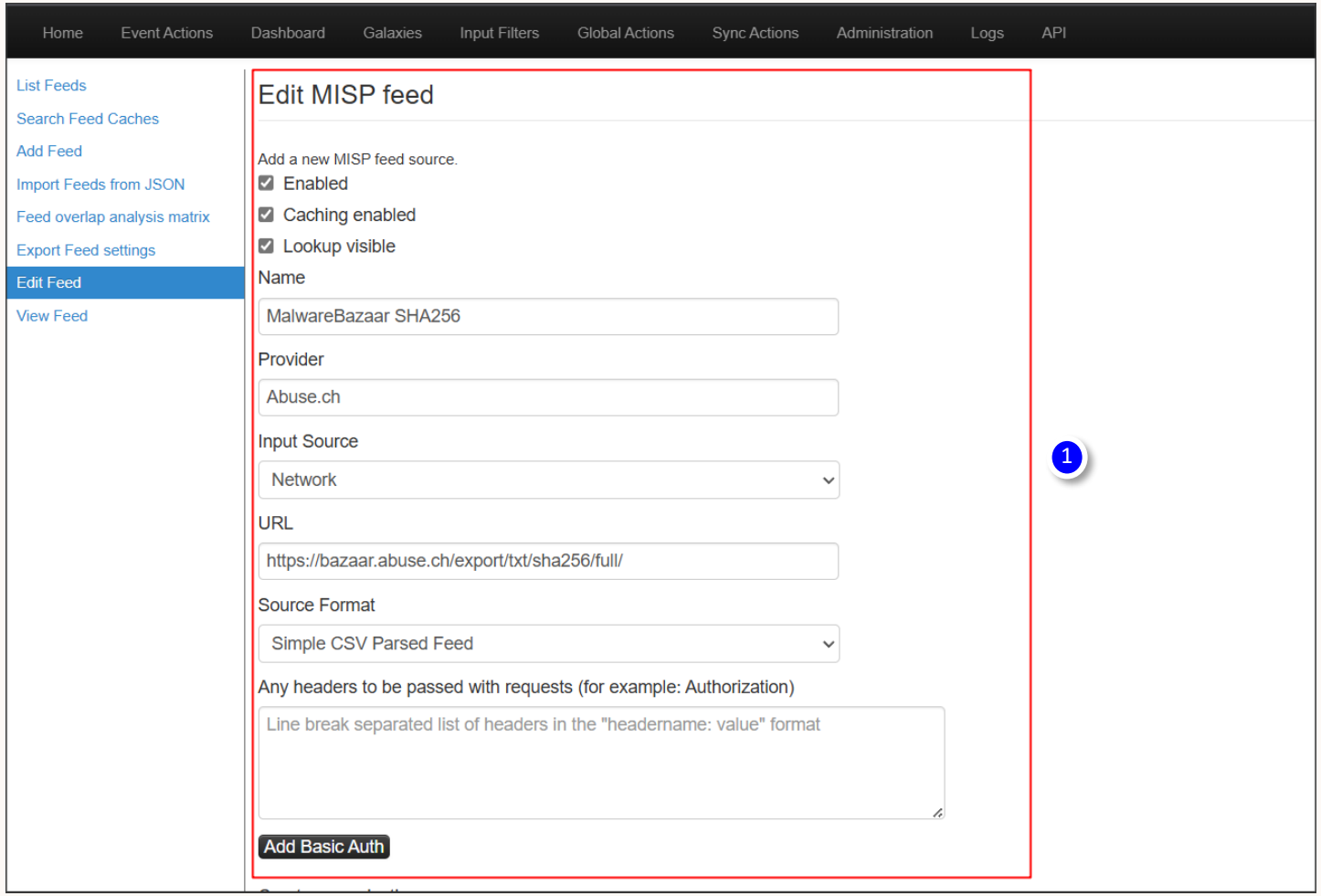
- ❑ Add Basic Auth: (leave blank)
- ❑ Distribution: All communities
- ❑ Default Tag: None
- ❑ Filter rules: (modify as needed)
- ❑ Submit

MISP: Add API Feeds



Threat Intelligence Feeds: CSV

MISP: Add CSV Feeds

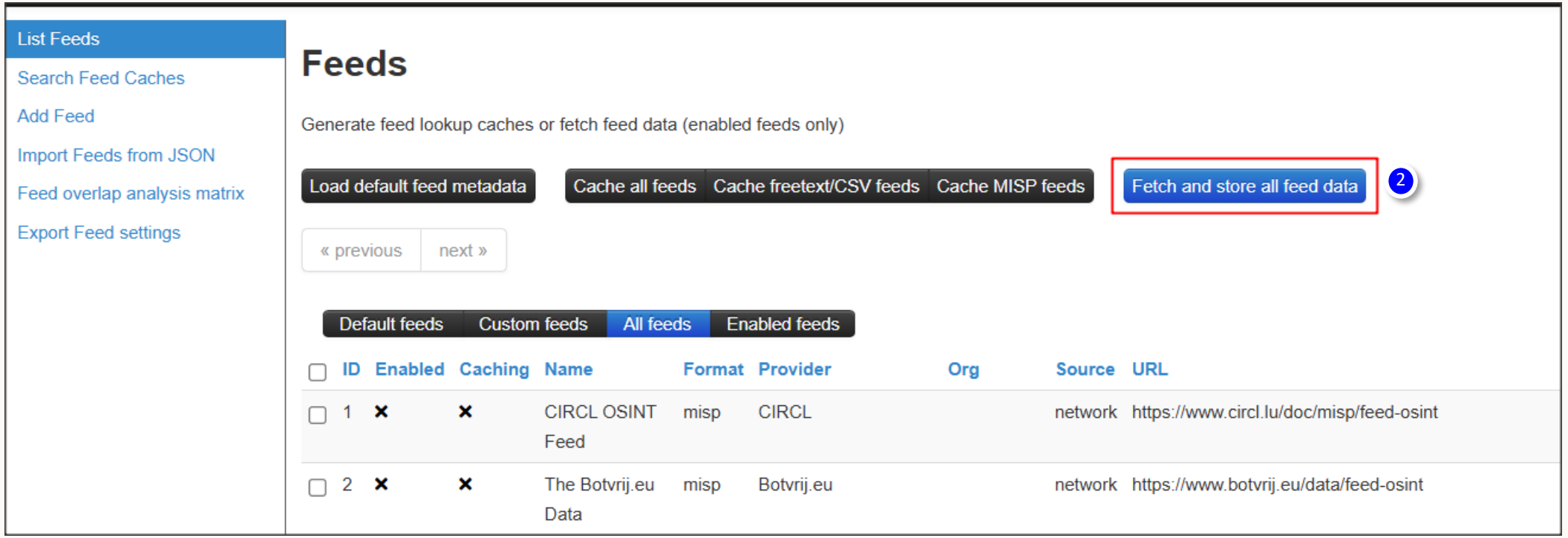


- ❑ Name: MalwareBazaar SHA256
- ❑ Provider: Abuse.ch
- ❑ Input Source: Network
- ❑ URL: https://bazaar.abuse.ch/export/txt/sha256/full/
- ❑ Source Format: CSV
- ❑ Headers: Leave blank if not needed
- ❑ Add Basic Auth: Leave blank

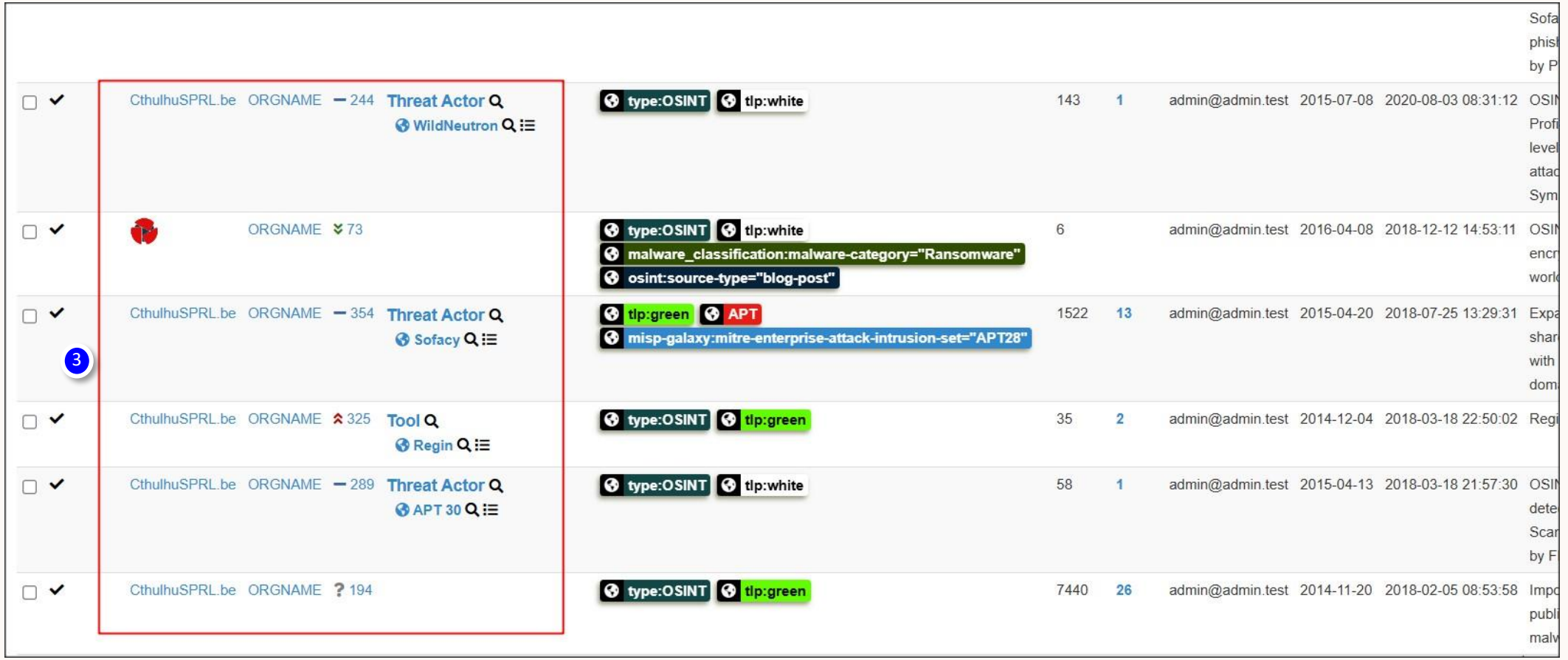
Submit

MISP: Add CSV Feeds

☐	8	✔	✔	MalwareBazaar SHA256	csv	Abuse.ch	ORGNAME	network	https://bazaar.abuse.ch/export/txt/sha256/full/	New event each pull	✖ ✖
☐	10	✔	✔	AlienVault OTX	misp	AlienVault		network	https://otx.alienvault.com/api/v1/pulses/subscribed	Authorization: Bearer 03b973e639b3852bcda7fecd5b335802ce7e6803fa8a53983953ddda6995cb7f Content-Type: application/json	✖ ✖

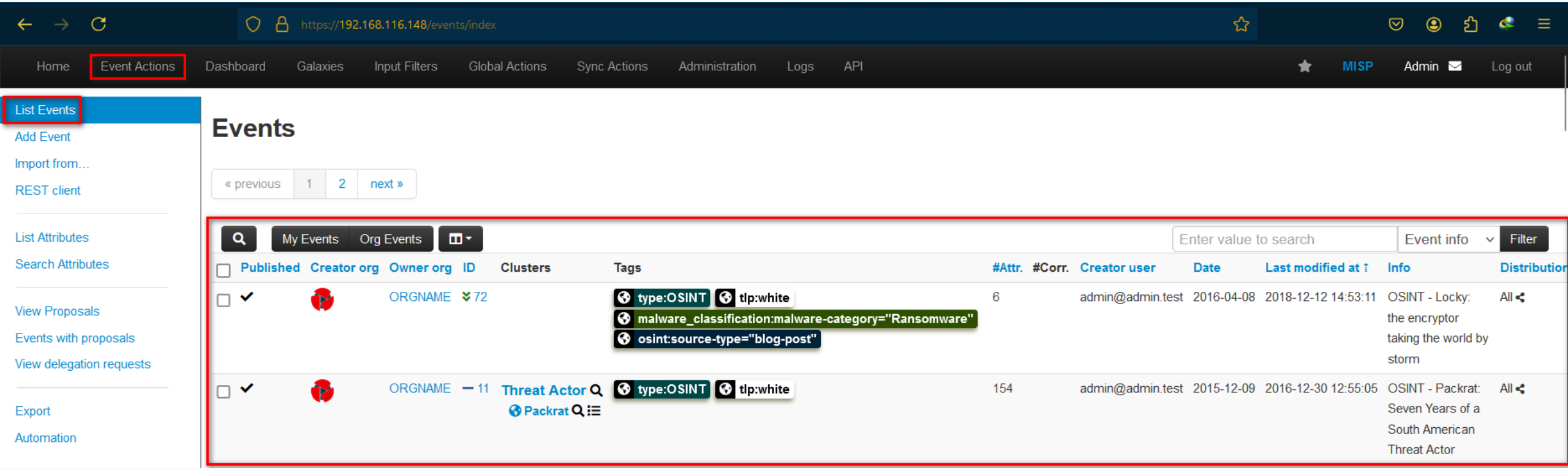


MISP: Add CSV Feeds

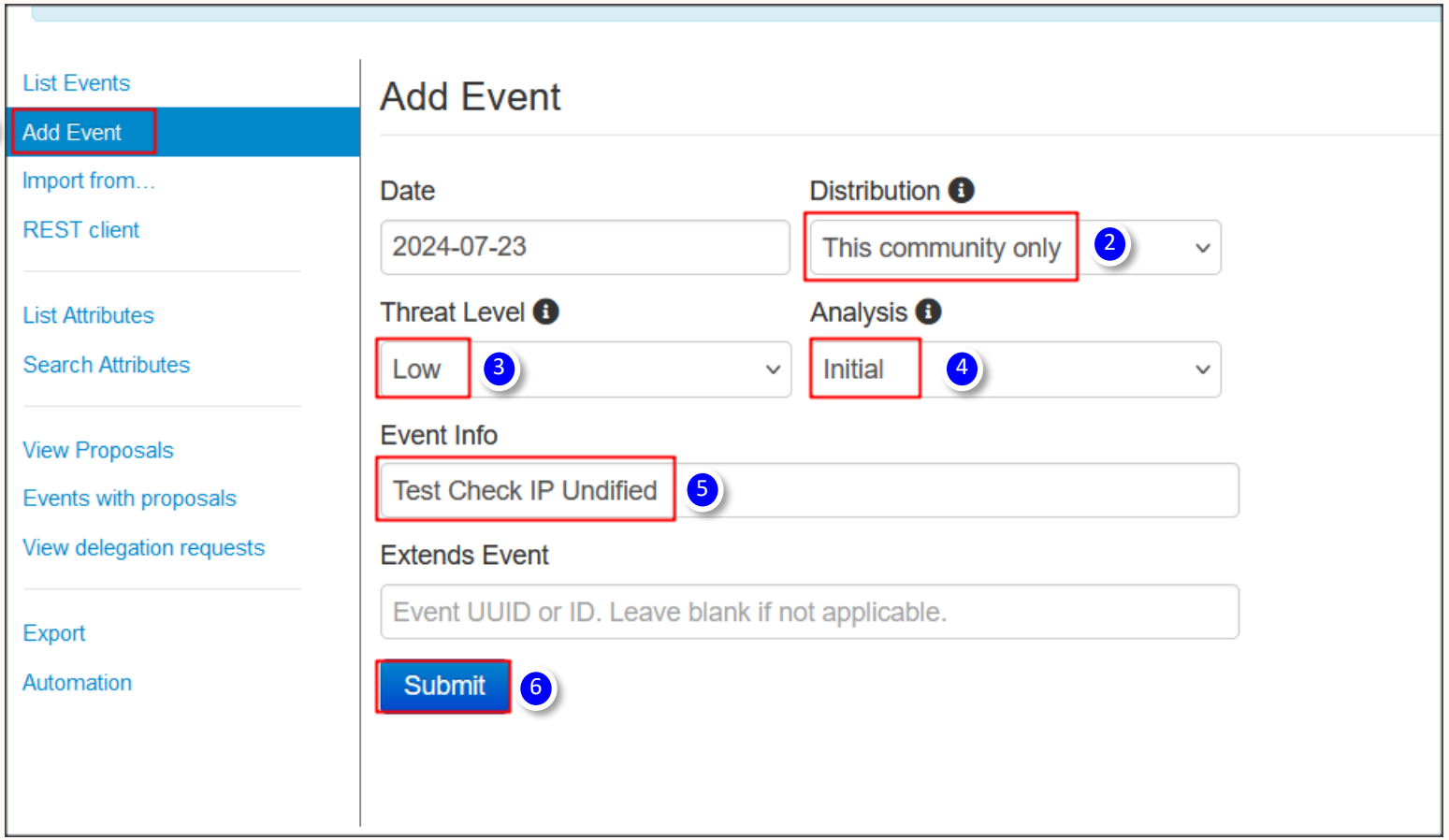


MISP: Events

❑Event Actions ➔ List Events



MISP: Events

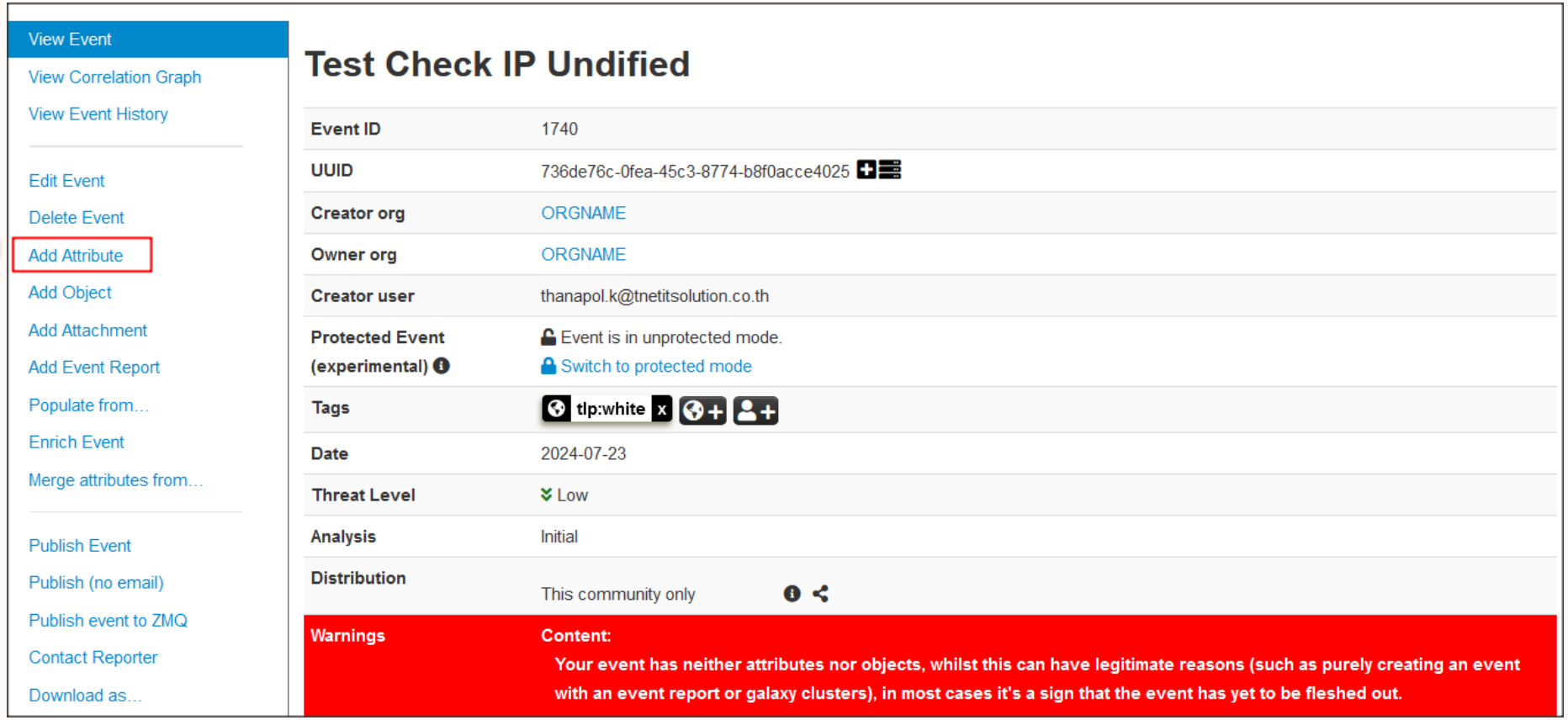


- ❑ Click Add Event
- ❑ Distribution : This community only
- ❑ Threat Level : Low
- ❑ Analysis : Initial
- ❑ Event Info : Test Check IP Unidified
- ❑ Click Submit

MISP: Events

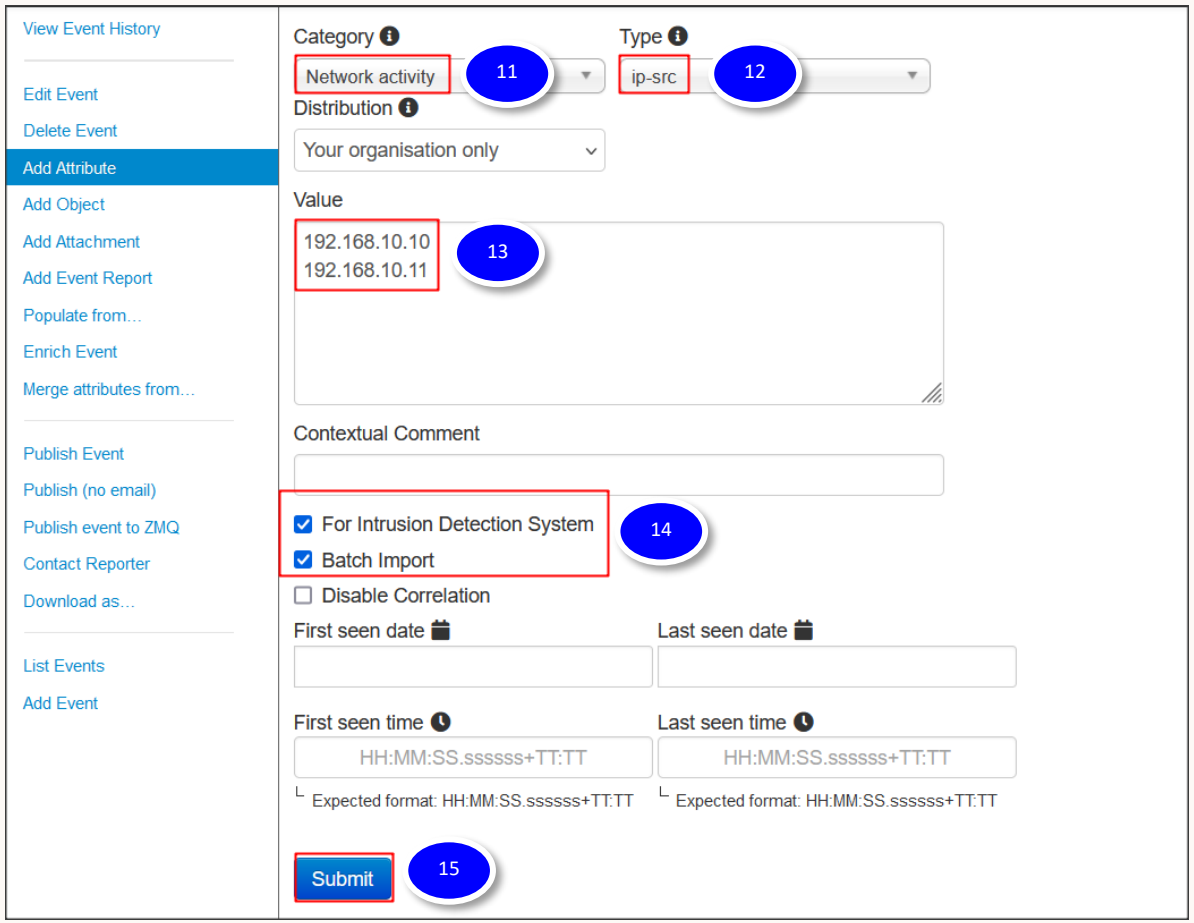
- ❑ Click Add Tag
- ❑ Search Tags : tlp:white
- ❑ Click submit

MISP: Events



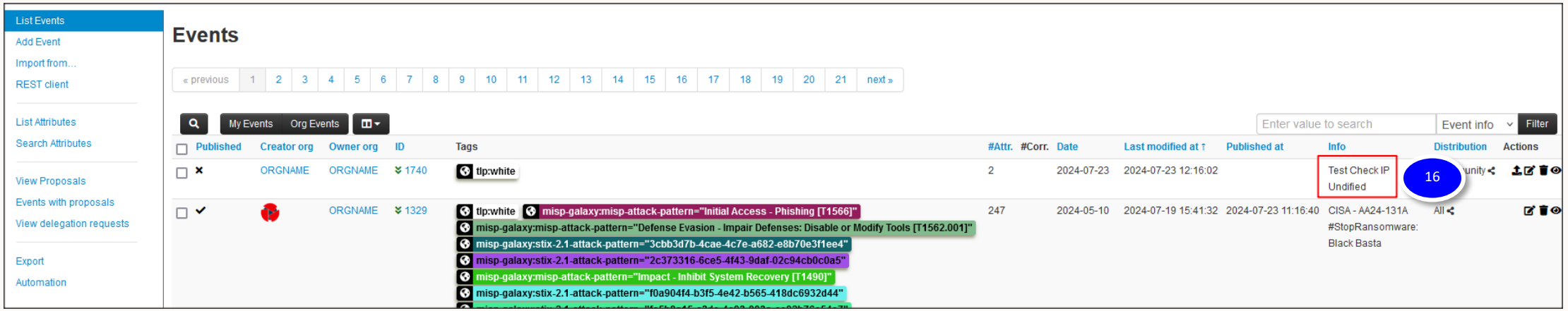
❑Click Add Attribute

MISP: Events



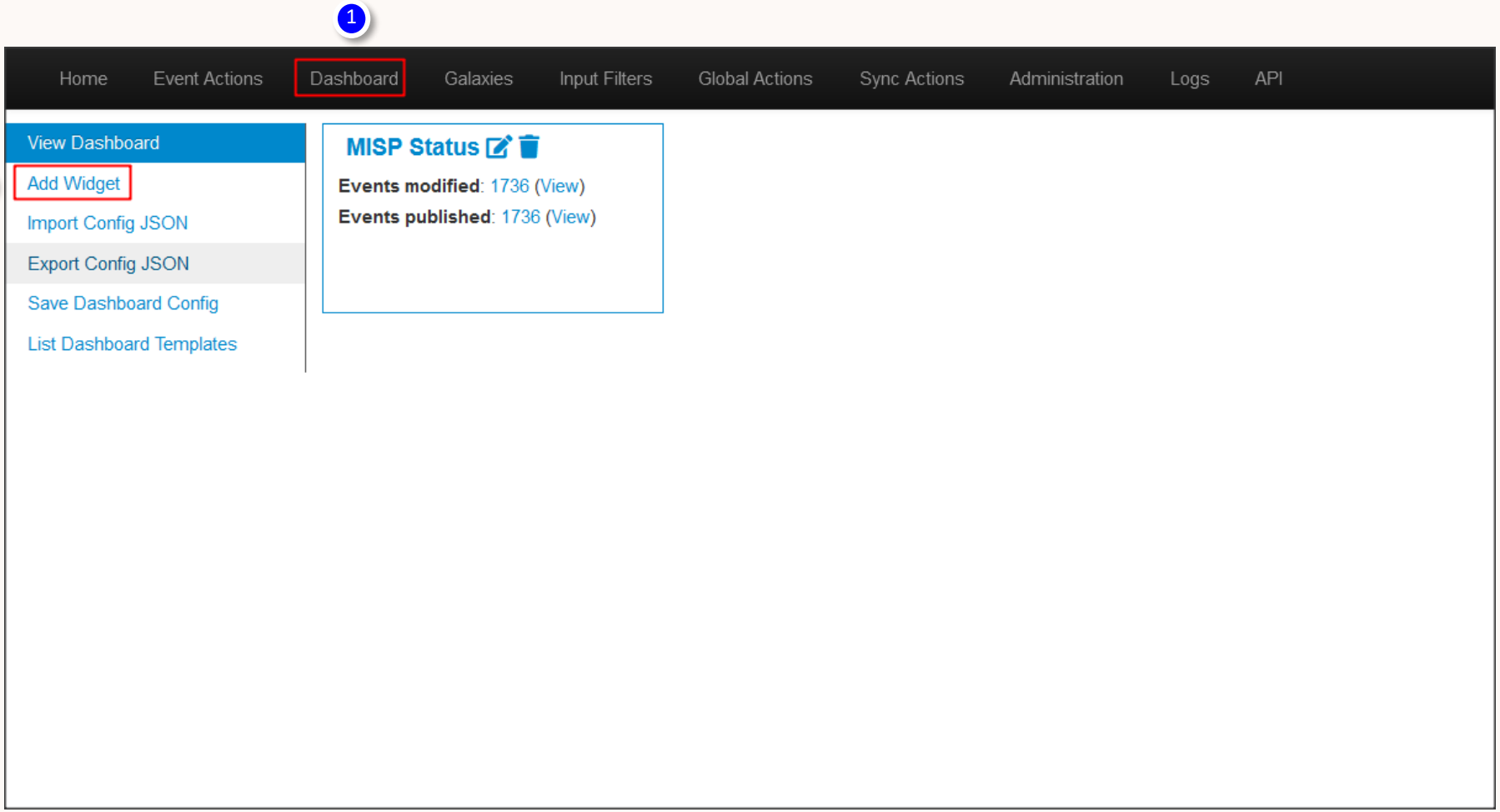
- ❑ Category : Network activity
- ❑ Type : ip-src
- ❑ Value : 192.168.10.10
- ❑ 192.168.10.11
- ❑ Check For Intrusion Detection Systemc
- ❑ Check Batch Import
- ❑ Click Submit

MISP: Events



Event Add Success

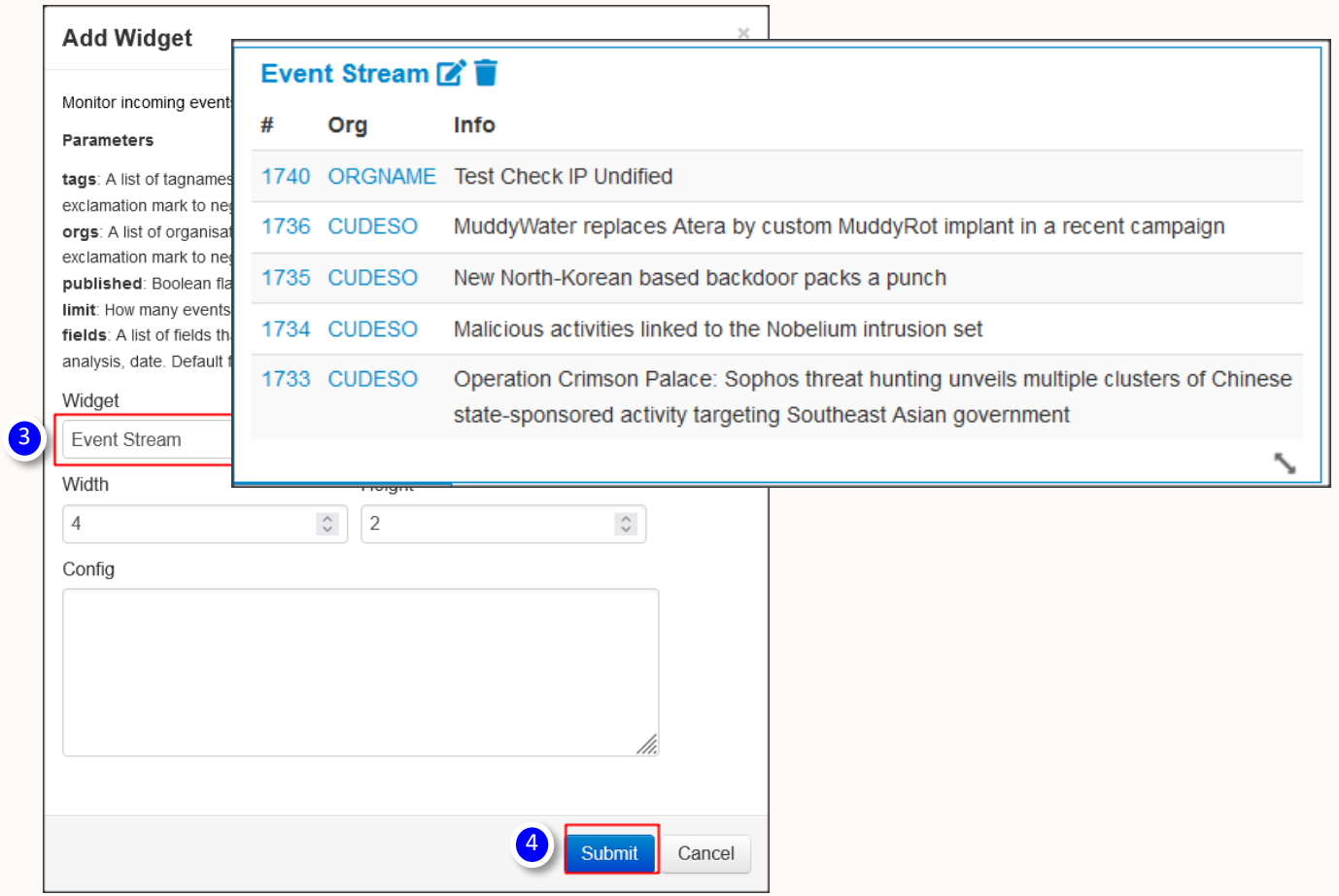
MISP: Alert Events



- ❑ Click Dashboard
- ❑ Click Add Widget

MISP: Alert Events

- ❑ Select : Event Stream
- ❑ Click Submit



MISP: Alert Email

```
root@misp:/home/misp# nano /etc/postfix/main.cf
```

```
  GNU nano 2.9.3                        /etc/postfix/main.cf

# Set your domain and hostname
myhostname = mailserver.home
mydomain = mailserver.home
myorigin = $mydomain
mydestination = $myhostname, localhost.$mydomain, $mydomain
sender_canonical_maps = hash:/etc/postfix/sender_canonical

# Gmail SMTP server
relayhost = [smtp.gmail.com]:587

# Enable SASL authentication
smtp_sasl_auth_enable = yes
smtp_sasl_security_options = noanonymous
smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd
smtp_sasl_tls_security_options = noanonymous

# Enable TLS encryption
smtp_use_tls = yes
smtp_tls_security_level = encrypt
smtp_tls_CAfile = /etc/ssl/certs/ca-certificates.crt

# Network settings
inet_interfaces = all
mynetworks = 127.0.0.0/8
```


# Set your domain and hostname
myhostname = mailserver.home
mydomain = mailserver.home
myorigin = $mydomain
mydestination = $myhostname, localhost.$mydomain, $mydomain
sender_canonical_maps = hash:/etc/postfix/sender_canonical

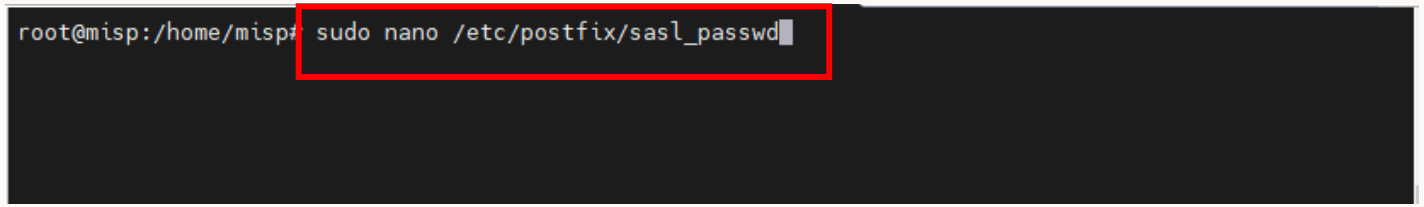
# Gmail SMTP server
relayhost = [smtp.gmail.com]:587

# Enable SASL authentication
smtp_sasl_auth_enable = yes
smtp_sasl_security_options = noanonymous
smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd
smtp_sasl_tls_security_options = noanonymous

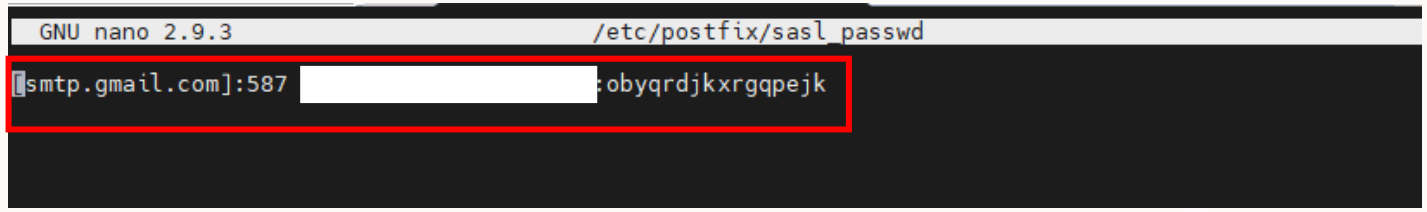
# Enable TLS encryption
smtp_use_tls = yes
smtp_tls_security_level = encrypt
smtp_tls_CAfile = /etc/ssl/certs/ca-certificates.crt

# Network settings
inet_interfaces = all
mynetworks = 127.0.0.0/8

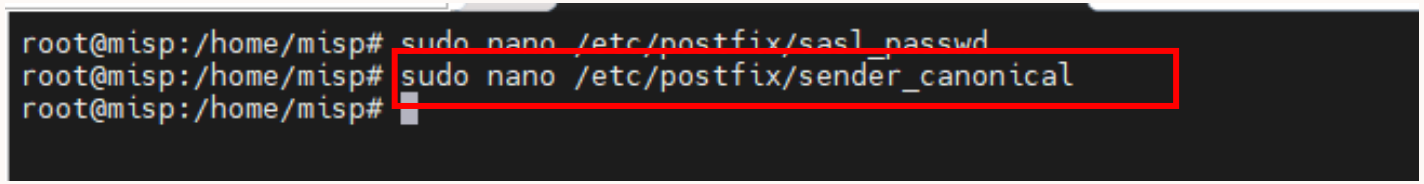
MISP: Alert Email



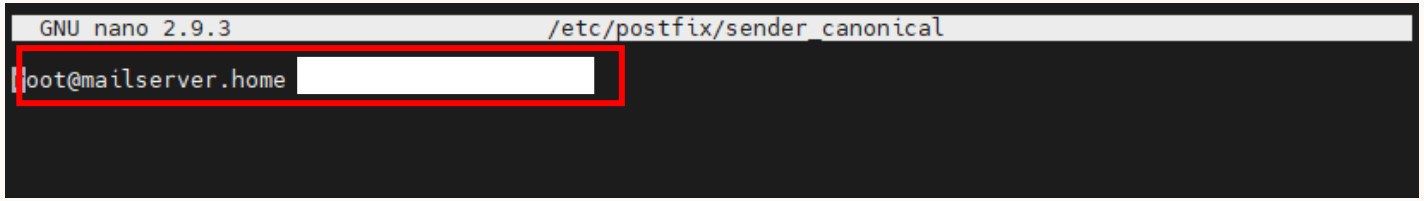
sudo nano /etc/postfix/sasl_passwd



[smtp.gmail.com]:587 {Your Gmail}:{Password}



sudo nano /etc/postfix/sender_canonical



root@mailserver.home {Your Gmail}

MISP: Alert Email

```
root@misp:/home/misp# sudo chmod 600 /etc/postfix/sasl_passwd
root@misp:/home/misp# sudo postmap /etc/postfix/sasl_passwd
root@misp:/home/misp# sudo postmap /etc/postfix/sender_canonical
root@misp:/home/misp# sudo systemctl reload postfix
root@misp:/home/misp#
```

sudo chmod 600 /etc/postfix/sasl_passwd

sudo postmap /etc/postfix/sasl_passwd

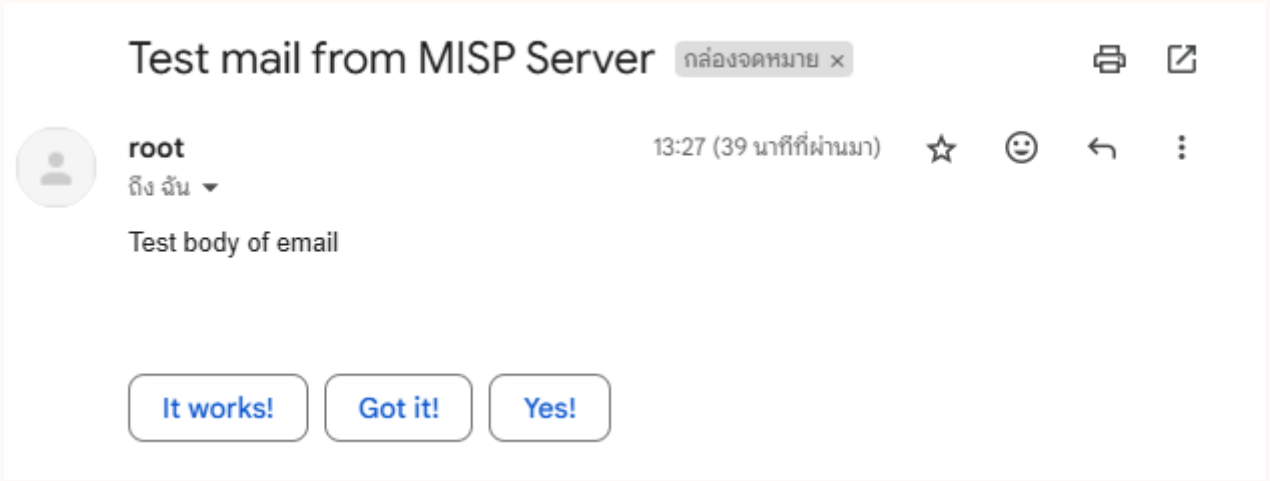
sudo postmap /etc/postfix/sender_canonical

sudo systemctl reload postfix

MISP: Alert Email

```
root@misp:/home/misp# echo "Test body of email" | mail -s "Test mail from MISP Server"
```

echo "Test body of email" | mail -s "Test mail from MISP Server" {GmailTarget}



MISP: Alert Email

```
root@misp:/home/misp# sudo nano /var/www/MISP/app/Config/email.php
root@misp:/home/misp#
```

nano /var/www/MISP/app/Config/email.php

```
class EmailConfig {
    public $default = array(
        'transport' => 'Smtp',
        'from' => array('morfeenslak@gmail.com' => 'MISP Server'), // Replace with your from address and name
        'host' => 'smtp.gmail.com',
        'port' => 587,
        'timeout' => 30,
        'username' => [redacted],
        'password' => [redacted],
        'client' => null,
        'log' => false,
        'tls' => true,
        'charset' => 'utf-8',
        'headers' => array('Precedence' => 'bulk')
    );

    // Fast email configuration
    public $fast = array(
        'from' => 'morfeenslak@gmail.com',
        'transport' => 'Smtp',
        'host' => 'smtp.gmail.com',
        'port' => 587,
        'timeout' => 30,
        'username' => [redacted],
        'password' => [redacted],
        'client' => null,
        'log' => false,
        'tls' => true
    );
}
```

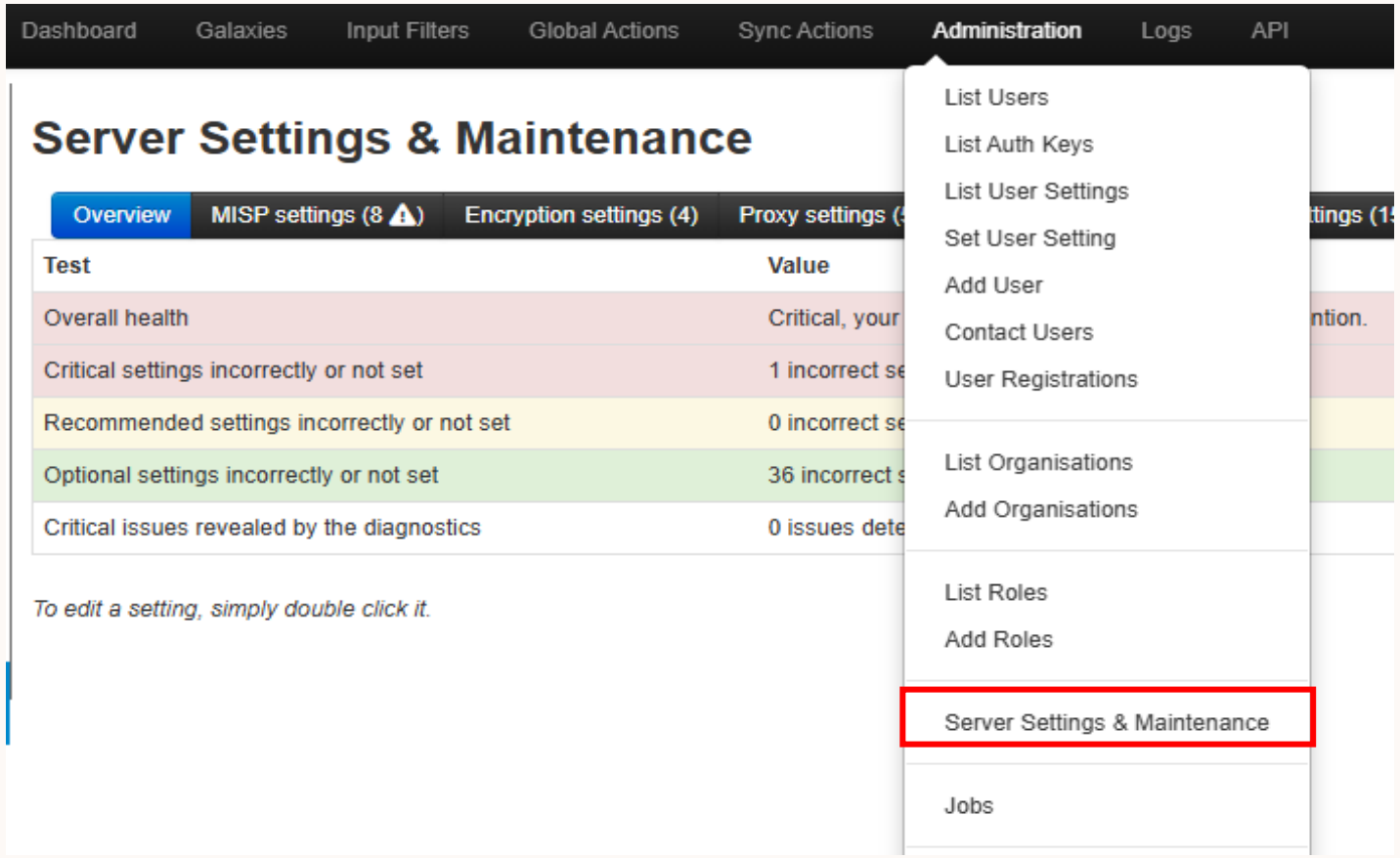
MISP: Alert Email

```
class EmailConfig {
    public $default = array(
        'transport' => 'Smtp',
        'from' => array('morfeenslak@gmail.com' => 'MISP Server'), //
Replace with your from address and name
        'host' => 'smtp.gmail.com',
        'port' => 587,
        'timeout' => 30,
        'username' =>
        'password' =>
        'client' => null,
        'log' => false,
        'tls' => true,
        'charset' => 'utf-8',
        'headers' => array('Precedence' => 'bulk')
    );

    // Fast email configuration
    public $fast = array(
        'from' => 'morfeenslak@gmail.com',
        'transport' => 'Smtp',
        'host' => 'smtp.gmail.com',
        'port' => 587,
        'timeout' => 30,
        'username' =>
        'password' =>
        'client' => null,
        'log' => false,
        'tls' => true
    );
}
```

MISP: Alert Email

- Click Administration
- Select Server Settings& Maintenance



MISP: Alert Email

Server Settings & Maintenance

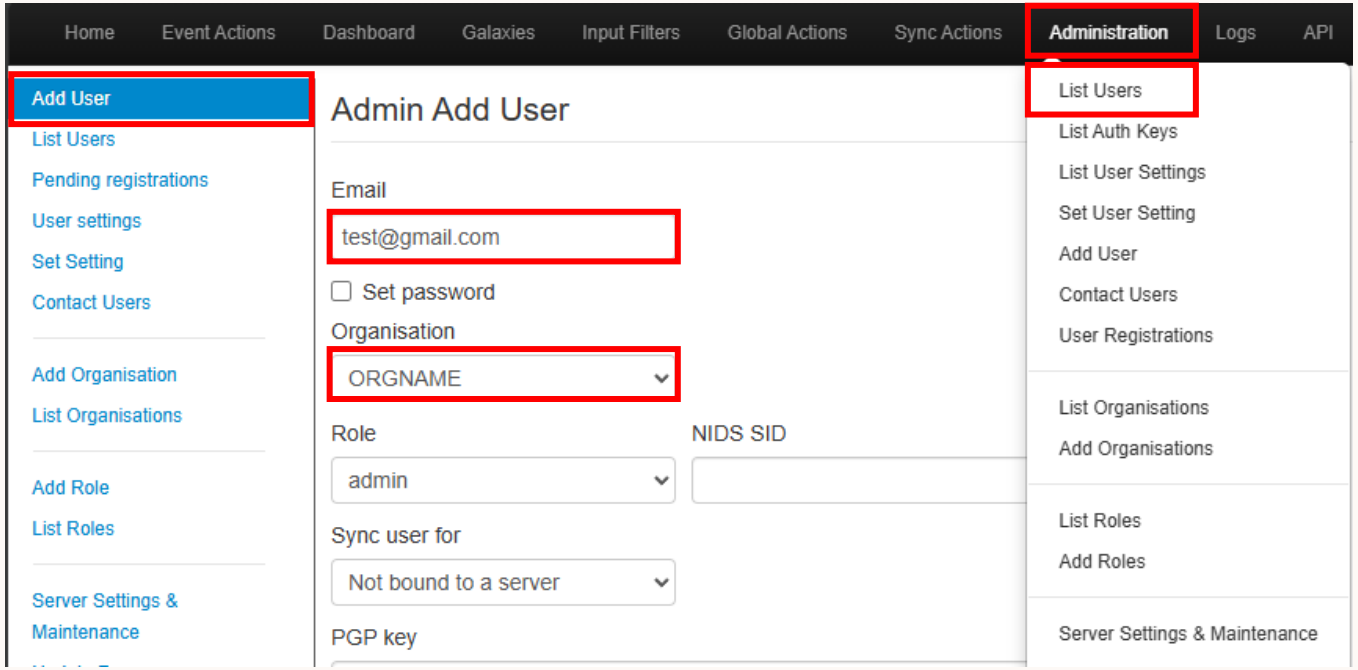
Overview | MISP settings (8 ⚠) | Encryption settings (4) | Proxy settings (5) | Security settings (5) | Plugin settings (15) | SimpleBackgroundJobs settings | Diagnostics

email

Priority	Setting	Value	Description	Error Message
Critical	MISP.email	info@admin.test	The e-mail address that MISP should use for all notifications	
Critical	MISP.disable_emailing	false	You can disable all e-mailing using this setting. When enabled, no outgoing e-mails will be sent by MISP.	
Recommended	MISP.disable_user_login_change	false	When enabled only Site admins can change user email. This should be enabled if you manage user logins by external system.	
Recommended	MISP.event_alert_republish_ban_threshold	5	If the MISP.event_alert_republish_ban setting is set, this setting will control how long no alerting by email will be done. Expected format: integer, in minutes	

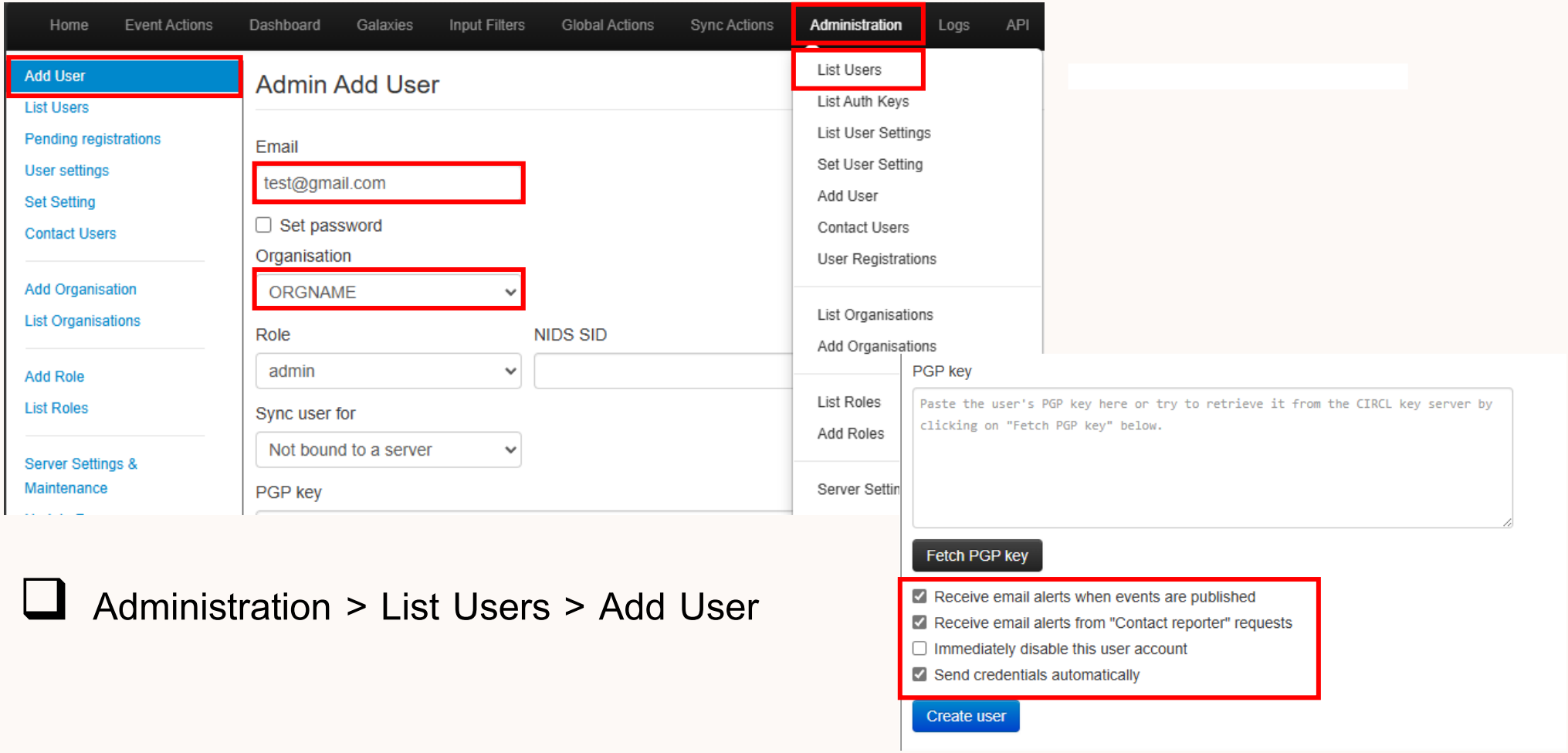
MISP settings > Search “ email “ > MISP.disable_emailing “ false ”

MISP: Alert Email



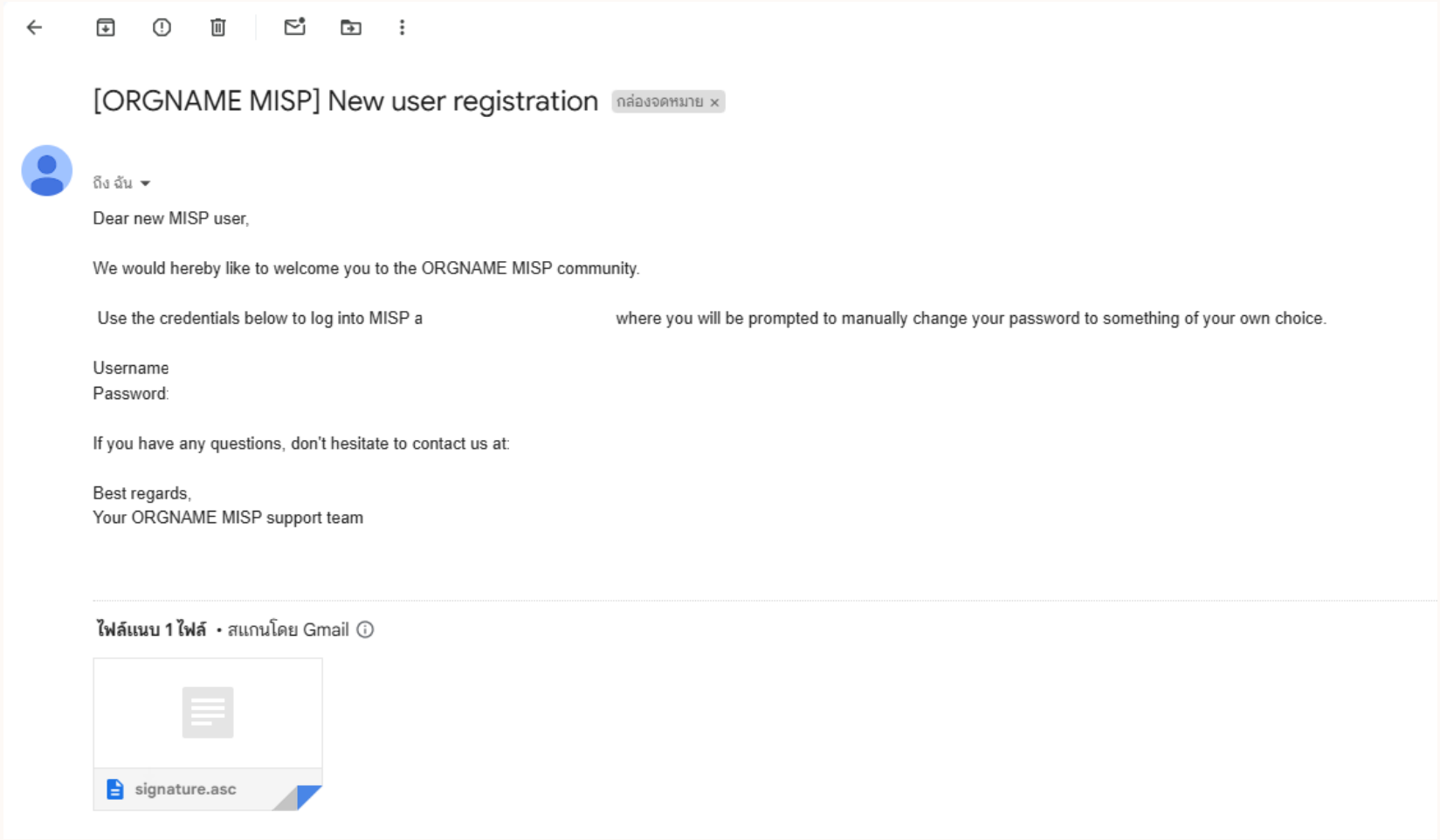
- Administration > List Users > Add User

MISP: Alert Email



- Administration > List Users > Add User

MISP: Alert Email



[ORGNAME MISP] New user registration กล่องจดหมาย ×

ถึง ฉัน

Dear new MISP user,

We would hereby like to welcome you to the ORGNAME MISP community.

Use the credentials below to log into MISP a where you will be prompted to manually change your password to something of your own choice.

Username
Password:

If you have any questions, don't hesitate to contact us at:

Best regards,
Your ORGNAME MISP support team

ไฟล์แนบ 1 ไฟล์ • สแกนโดย Gmail

signature.asc

https://www.tnetitsolution.co.th

tnetitsolution

tnetitsolution

tnetitsolution

+66(0)-8-8874-4741

Info@tnetitsolution.co.th

Search T-NET IT Solution