



SysAdmin Day
Live in Vientiane
(Fri) July 26
2024



The starting point to protect against
cyber attacks with threat intelligence

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”

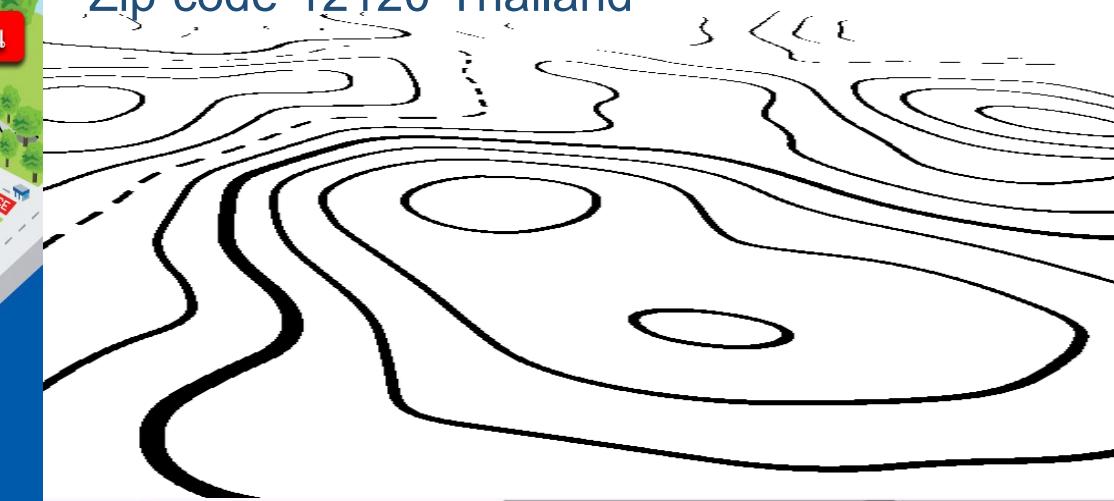


Location



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

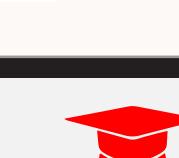
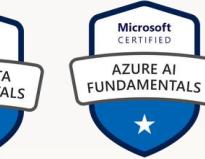
Designed IT Architecture. Development software

Implementation Cybersecurity Standard and Cybersecurity Act.

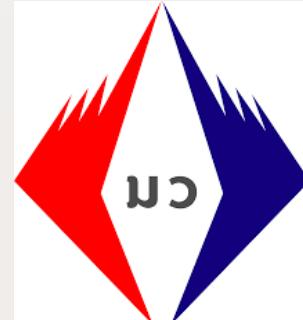
Company Services



Our Certification



Company portfolio



Speaker

- นาย เจริญ 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: ผู้ดูแลกลุ่มสอนแยกแบบหมู่ ๆ
- Website : www.tnetitsolution.co.th

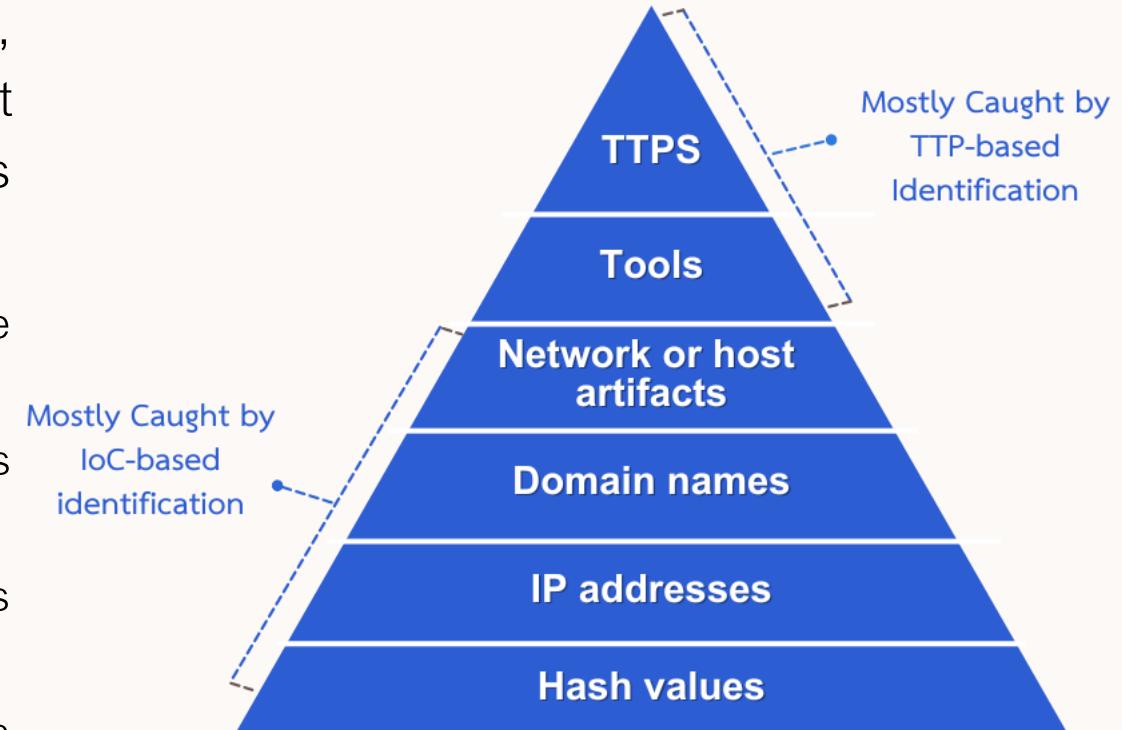




Cyber Threat Intelligence

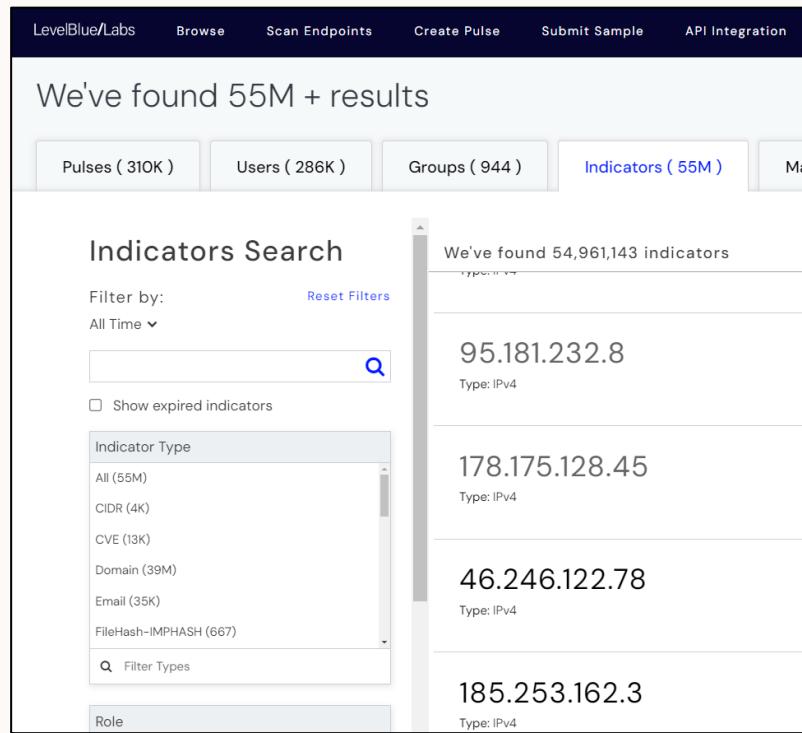
What is cyber threat intelligence?

- ❑ 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>



We've found 55M + results

Pulses (31OK) Users (286K) Groups (944) **Indicators (55M)** Map

Indicators Search

Filter by: All Time ▾

Indicator Type: All (55M), CIDR (4K), CVE (13K), Domain (39M), Email (35K), FileHash-IMPHASH (667)

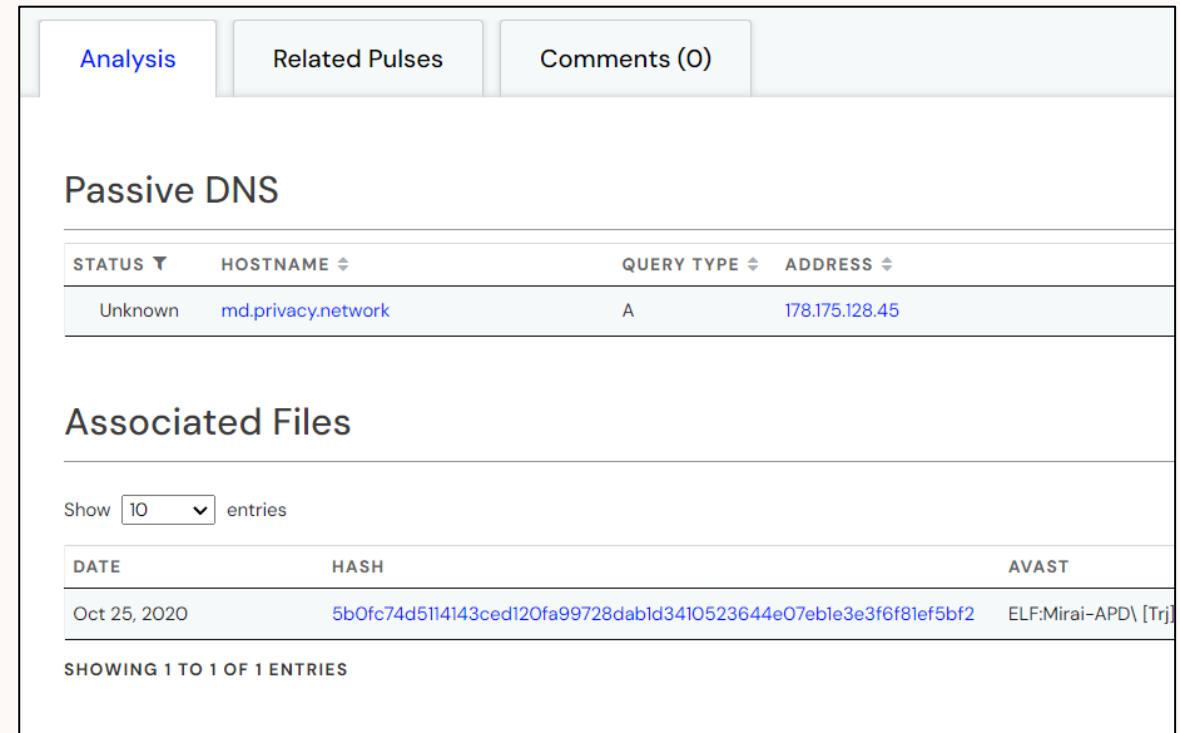
Show expired indicators

Role

We've found 54,961,143 indicators

95.181.232.8	Type: IPv4
178.175.128.45	Type: IPv4
46.246.122.78	Type: IPv4
185.253.162.3	Type: IPv4

IP addresses Indicators



Analysis Related Pulses Comments (0)

Passive DNS

STATUS	HOSTNAME	QUERY TYPE	ADDRESS
Unknown	md.privacy.network	A	178.175.128.45

Associated Files

Show 10 entries

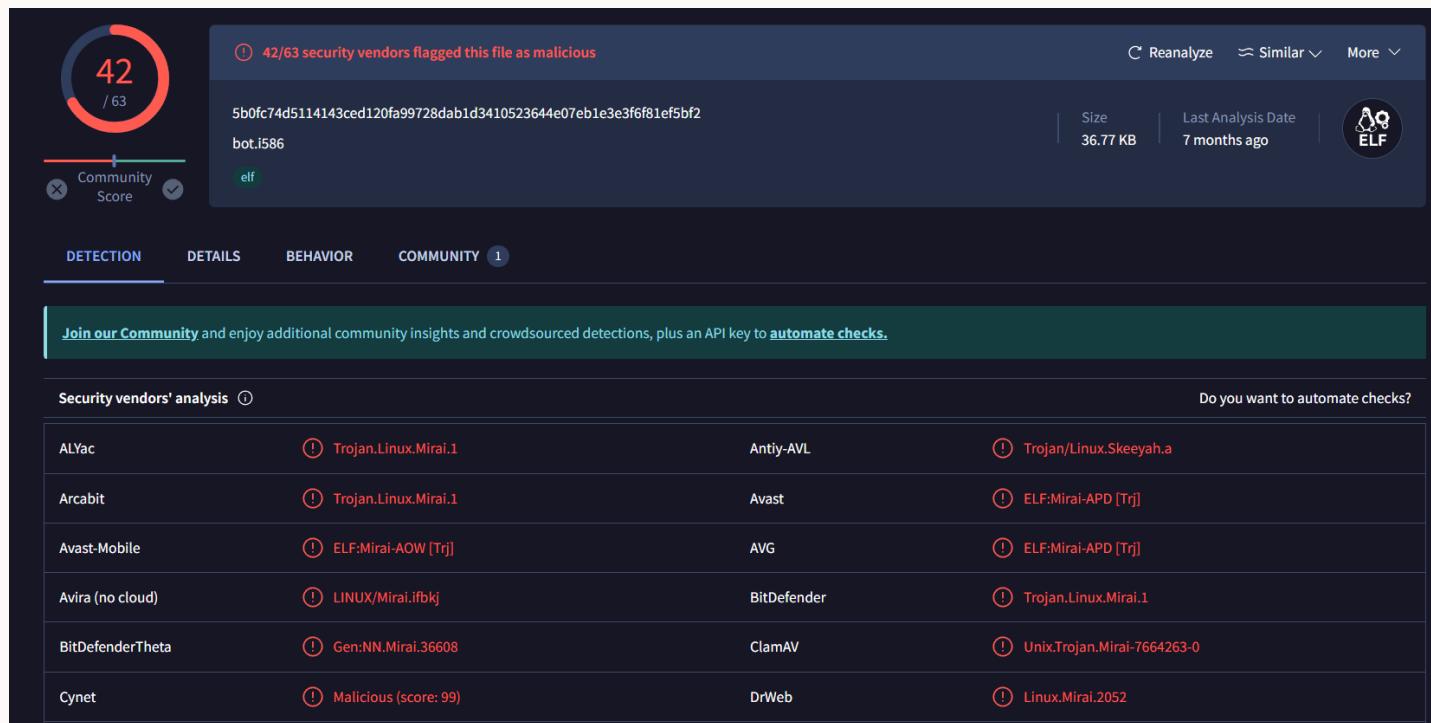
DATE	HASH	AVAST
Oct 25, 2020	5b0fc74d5114143ced120fa99728dab1d3410523644e07eb1e3e3f6f81ef5bf2	ELF:Mirai-APD\ [Tr]

SHOWING 1 TO 1 OF 1 ENTRIES

Hash Values

Example Indicators of Compromise

□ <https://www.virustotal.com>



Security vendor's analysis	Detection	Do you want to automate checks?	
ALYac	① Trojan.Linux.Mirai.1	Antiy-AVL	① Trojan/Linux.Skeeyah.a
Arcabit	① Trojan.Linux.Mirai.1	Avast	① ELF:Mirai-APD [Trj]
Avast-Mobile	① ELF:Mirai-AOW [Trj]	AVG	① ELF:Mirai-APD [Trj]
Avira (no cloud)	① LINUX/Mirai.ifbkj	BitDefender	① Trojan.Linux.Mirai.1
BitDefenderTheta	① Gen>NN.Mirai.36608	ClamAV	① Unix.Trojan.Mirai-7664263-0
Cynet	① Malicious (score: 99)	DrWeb	① Linux.Mirai.2052

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.

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 botter/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
 ① Tactic: Resource Development
 ① Platforms: PRE
 Version: 1.0
 Created: 01 October 2020
 Last Modified: 15 April 2021

[Version Permalink](#)

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

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	7 techniques	9 techniques	12 techniques	19 techniques	13 techniques	39 techniques	15 techniques	27 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (5)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	BITS Jobs	Boot or Logon Autostart Execution (14)	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Clipboard Data	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Build Image on Host	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Data from Cloud Storage Object	Data Encoding (2)	Data Manipulation (3)	Data
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (2)	Browser Extensions	Boot or Logon Initialization Scripts (5)	Deploy Container	Forge Web Credentials (2)	Cloud Service Discovery	Cloud Service Dashboard	Data from Configuration Repository (2)	Data Obfuscation (3)	Defacement (2)	Exfiltration Over C2 Channel
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Create or Modify System Process (4)	Direct Volume Access	Input Capture (4)	Container and Resource Discovery	Dynamic Resolution (3)	Data from Information Repositories (2)	Fallback Channels	Exfiltration Over Other Network Medium (1)	Endpoint Denial of Service (4)
Search Closed Sources (2)	Stage Capabilities (5)	Scheduled Task/Job (7)	Shared Modules	Create Account (3)	Domain Policy Modification (2)	Domain Policy Modification (2)	Man-in-the-Middle (2)	Domain Trust Discovery	Replication Through Removable Media	Data from Local System	Ingress Tool Transfer	Firmware Corruption	Inhibit System Recovery
Search Open Technical Databases (5)	Supply Chain Compromise (3)	Shared Modules	Create Account (3)	Escape to Host	Execution Guardrails (1)	Exploitation for Defense Evasion	Modify Authentication Process (4)	File and Directory Discovery	Network Service Scanning	Data from Network	Multi-Step	Exfiltration Over Web Service (2)	Network Denial of Service (2)
Search Open Websites/Domains (2)	Trusted Relationship	Software Deployment Tools	Create or Modify System Process (4)	Event Triggered Execution (15)	File and Directory Permissions Modification (15)	File and Directory Permissions Modification (15)	Network Sniffing	Taint Shared					Resources
	Valid		Event Triggered		Exploitation for								

ATT&CK Enterprise Tactics

ID	Name	Description
TA0043	Reconnaissance	รวบรวมข้อมูลก่อนการโจนตี ทำข้อมูลของเป้าหมายให้ได้มากที่สุด
TA0042	Resource Development	เตรียมทรัพยากรที่จำเป็นต้องสำหรับภารกิจ เช่น ข้อมูลทางการเงิน รหัสผ่าน บัญชี ฯลฯ
TA0001	Initial Access	การโจนตีเป้าหมาย หรือ เริ่มต้นต่อไปยังระบบเครือข่ายที่ต้องการโจนตี
TA0002	Execution	สั่งการโปรแกรมที่เตรียมไว้ หรือ Code ที่อันตรายที่เป้าหมาย
TA0003	Persistence	สร้างรากฐานว่าการสั่งการไม่ถูกขัดขวาง คงอยู่ได้ตลอด
TA0004	Privilege Escalation	ยกสิทธิการเข้าถึงระบบ ให้สามารถเข้าถึงได้ทุกระบบ
TA0005	Defense Evasion	หลบเลี่ยงโปรแกรมตรวจสอบจับหรือโปรแกรมสังเกตความผิดปกติ
TA0006	Credential Access	ขโมยรหัสและบัญชีผู้ใช้ และทำการเข้าสู่ระบบ
TA0007	Discovery	ตรวจสอบข้อมูลความสามารถในการเริ่มต้นต่อระบบ ที่มีการใช้งาน เพื่อไขนโยบายเครื่องอุปกรณ์ต่อ
TA0008	Lateral Movement	เคลื่อนย้ายไปค่าใหม่ , เครื่อง หรือเป้าหมายที่มีข้อมูลที่ต้องการ
TA0009	Collection	ทำการตรวจสอบข้อมูลออกจากระบบ หรือ เป้าหมาย
TA0011	Command and Control	ทำการเชื่อมต่อเครื่องเป้าหมายไปสู่เครื่องเก็บข้อมูลลักษณะของผู้โจมตี
TA0010	Exfiltration	ทำการส่งข้อมูล นำข้อมูลออก
TA0040	Impact	ทำลายหลักฐานการเมือง หรือ การเรียกค่าไถ่ หรือทำลายระบบทั้งหมด

TACTICS

- Enterprise
- Reconnaissance**
- Resource Development
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration
- Impact
- Mobile

Reconnaissance

The adversary is trying to gather information they can use to plan future operations.

Reconnaissance consists of techniques that involve adversaries actively or passively gathering information that can be used to support targeting. Such information may include details of the victim organization, infrastructure, or staff/personnel. This information can be leveraged by the adversary to aid in other phases of the adversary lifecycle, such as using gathered information to plan and execute Initial Access, to scope and prioritize post-compromise objectives, or to drive and lead further Reconnaissance efforts.

Techniques

ID	Name	Description
T1595	Active Scanning	Adversaries may execute active reconnaissance scans to gather information that can be used during targeting. Active scans are those where the adversary probes victim infrastructure via network traffic, as opposed to other forms of reconnaissance that do not involve direct interaction.
.001	Scanning IP Blocks	Adversaries may scan victim IP blocks to gather information that can be used during targeting. Public IP addresses may be allocated to organizations by block, or a range of sequential addresses.
.002	Vulnerability Scanning	Adversaries may scan victims for vulnerabilities that can be used during targeting. Vulnerability scans typically check if the configuration of a target host/application (ex: software and version) potentially aligns with the target of a specific exploit the adversary may seek to use.
T1592	Gather Victim Host Information	Adversaries may gather information about the victim's hosts that can be used during targeting. Information about hosts may include a variety of details, including administrative data (ex: name, assigned IP, functionality, etc.) as well as specifics regarding its configuration (ex: operating system, language, etc.).

ID: TA0043

Created: 02 October 2020

Last Modified: 18 October 2020

Version Permalink

Techniques: 10

ATT&CK Matrix for Enterprise

Home > Techniques > Enterprise > Active Scanning

Active Scanning

Sub-techniques (2)

Adversaries may execute active reconnaissance scans to gather information that can be used during targeting. Active scans are those where the adversary probes victim infrastructure via network traffic, as opposed to other forms of reconnaissance that do not involve direct interaction.

Adversaries may perform different forms of active scanning depending on what information they seek to gather. These scans can also be performed in various ways, including using native features of network protocols such as ICMP.^{[1][2]} Information from these scans may reveal opportunities for other forms of reconnaissance (ex: Search Open Websites/Domains or Search Open Technical Databases), establishing operational resources (ex: Develop Capabilities or Obtain Capabilities), and/or initial access (ex: External Remote Services or Exploit Public-Facing Application).

Mitigations

ID	Mitigation	Description
M1056	Pre-compromise	This technique cannot be easily mitigated with preventive controls since it is based on behaviors performed outside of the scope of enterprise defenses and controls. Efforts should focus on minimizing the amount and sensitivity of data available to external parties.

Detection

Monitor for suspicious network traffic that could be indicative of scanning, such as large quantities originating from a single source (especially if the source is known to be associated with an adversary/botnet). Analyzing web metadata may also reveal artifacts that can be attributed to potentially malicious activity, such as referer or user-agent string HTTP/S fields.

Much of this activity may have a very high occurrence and associated false positive rate, as well as potentially taking place outside the visibility of the target organization, making detection difficult for defenders.

Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access.

ID: T1595
Sub-techniques: T1595.001, T1595.002
 ① **Tactic:** Reconnaissance
 ① **Platforms:** PRE
 ① **Data Sources:** Network Traffic: Network Traffic Content, Network Traffic: Network Traffic Flow
 Version: 1.0
 Created: 02 October 2020
 Last Modified: 15 April 2021

Version Permalink

Ref: <https://attack.mitre.org>

Types of Indicators of Compromise

File-Based
Indicators

1

Network-
Based
Indicators

2

Behavior-
Based
Indicators

3

Email-Based
Indicators

4

Endpoint-
Based
Indicators

5

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

Dissemination

Translating analysis into digestible format for stakeholders

Analysis

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

Requirements

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

Collection

Gather information from various sources to satisfy the defined objectives.



Six Process



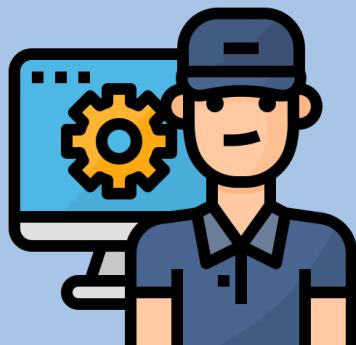
use cases by function

Function	Use Cases
Sec/IT Analyst	<ul style="list-style-type: none"> ▪ Integrate TI feeds with other security products ▪ Block bad IPs, URLs, domains, files etc
SOC	<ul style="list-style-type: none"> ▪ Use TI to enrich alerts ▪ Link alerts together into incidents ▪ Tune newly deployed security controls
CSIRT	<ul style="list-style-type: none"> ▪ Look for information on the who/what/why/when/how of an incident ▪ Analyze root cause to determine scope of the incident
Intel Analyst	<ul style="list-style-type: none"> ▪ Look wider and deeper for intrusion evidence ▪ Review reports on threat actors to better detect them
Executive Management	<ul style="list-style-type: none"> ▪ 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



G R E Y N O I S E
INTELLIGENCE



O P E N C T I



Pulsedive



M I S P
Threat Sharing



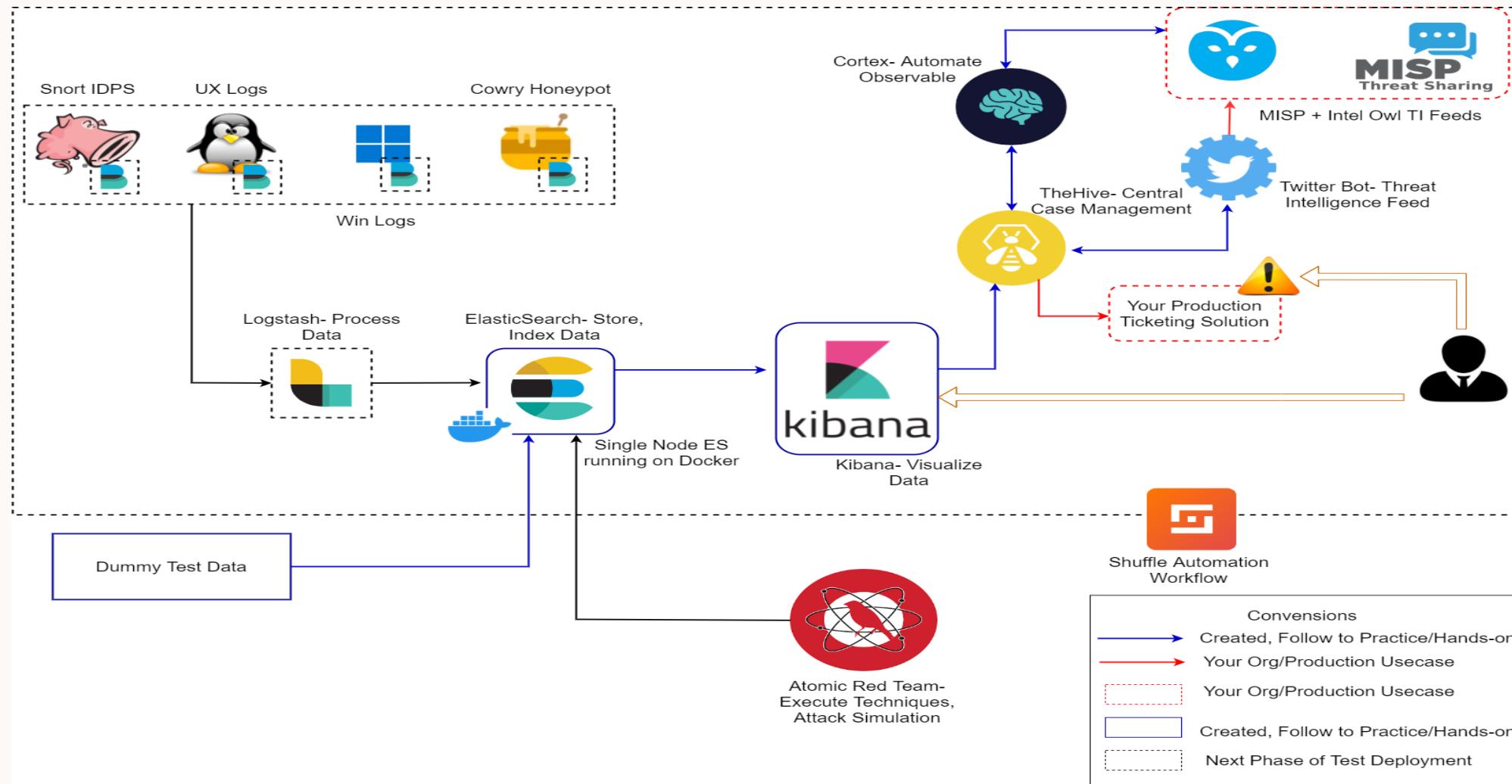
Malware Information Sharing Platform: MISP

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>

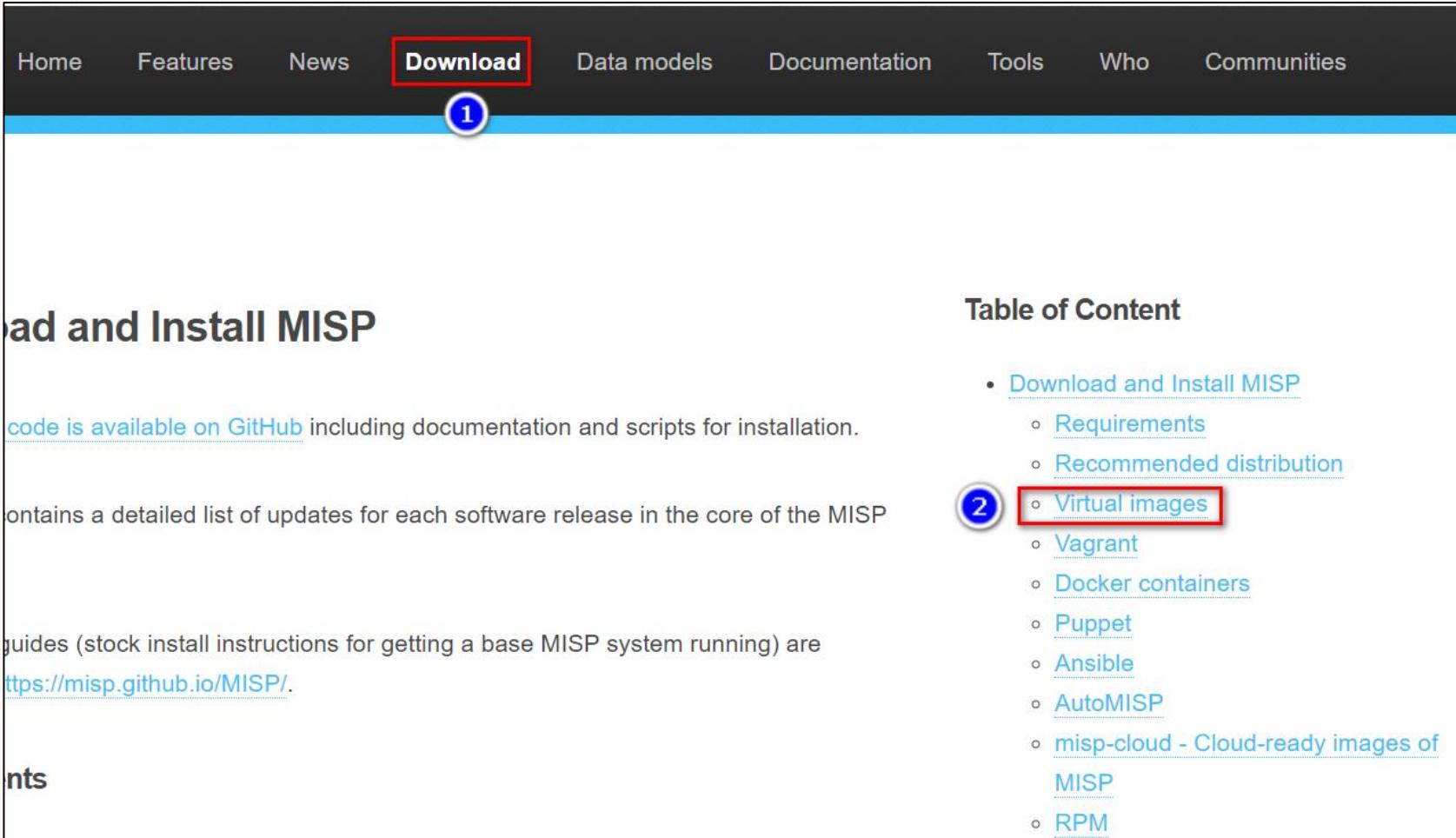


Architecture-Diagram



MISP: Download and Install

MISP: Download



The screenshot shows the MISP Download page. At the top, there is a navigation bar with links: Home, Features, News, Download (which is highlighted with a red border and has a blue circle with the number 1 below it), Data models, Documentation, Tools, Who, and Communities.

ad and Install MISP

code is available on GitHub including documentation and scripts for installation.

ontains a detailed list of updates for each software release in the core of the MISP

guides (stock install instructions for getting a base MISP system running) are <https://misp.github.io/MISP/>.

nts

Table of Content

- [Download and Install MISP](#)
 - [Requirements](#)
 - [Recommended distribution](#)
 - [Virtual images](#) (highlighted with a red border and has a blue circle with the number 2 below it)
 - [Vagrant](#)
 - [Docker containers](#)
 - [Puppet](#)
 - [Ansible](#)
 - [AutoMISP](#)
 - [misp-cloud - Cloud-ready images of MISP](#)
 - [RPM](#)

- 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/>.³ 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>

vm.misp-project.org//latest/

Index of Latest

Search

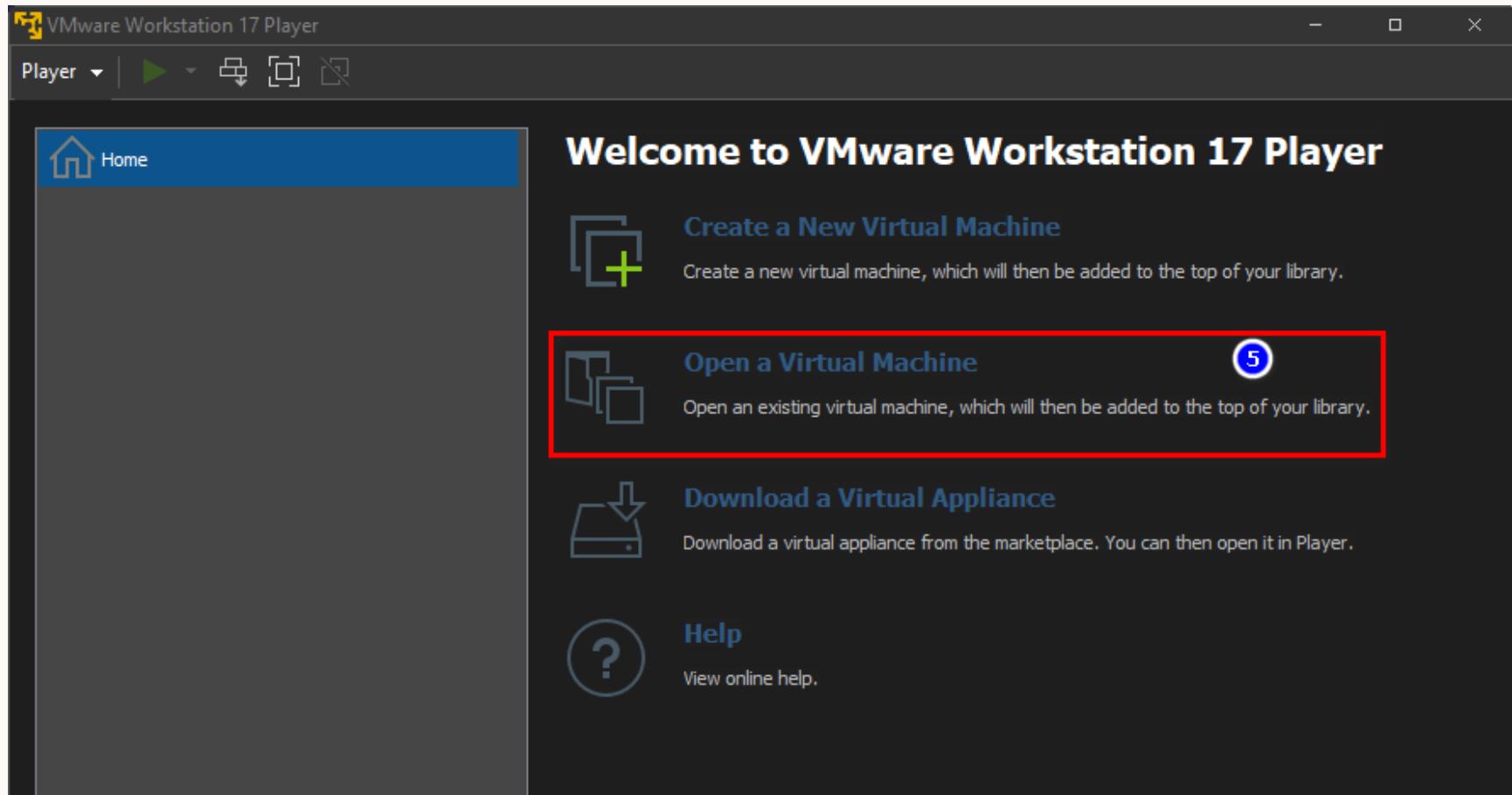
Please find the virtual images generated automatically from MISP Project code repository.

Images are accessible per [git commit](#). You can also get the [latest version](#). Or the archive of [VMs per version](#).

Name	Last modified	Size	Description
< Parent Directory	-	-	
checksums/	2 years ago	-	
MISP_v2.4.158@3aad442-VMware.zip.asc	2 years ago	819	GZIP compressed archive
MISP_v2.4.158@3aad442.ova.asc	2 years ago	819	
verify.txt	2 years ago	4.4K	Plain text file
MISP_v2.4.158@3aad442-VMware.zip	2 years ago	3.0G	GZIP compressed archive
MISP_v2.4.158@3aad442.ova	2 years ago	3.1G	

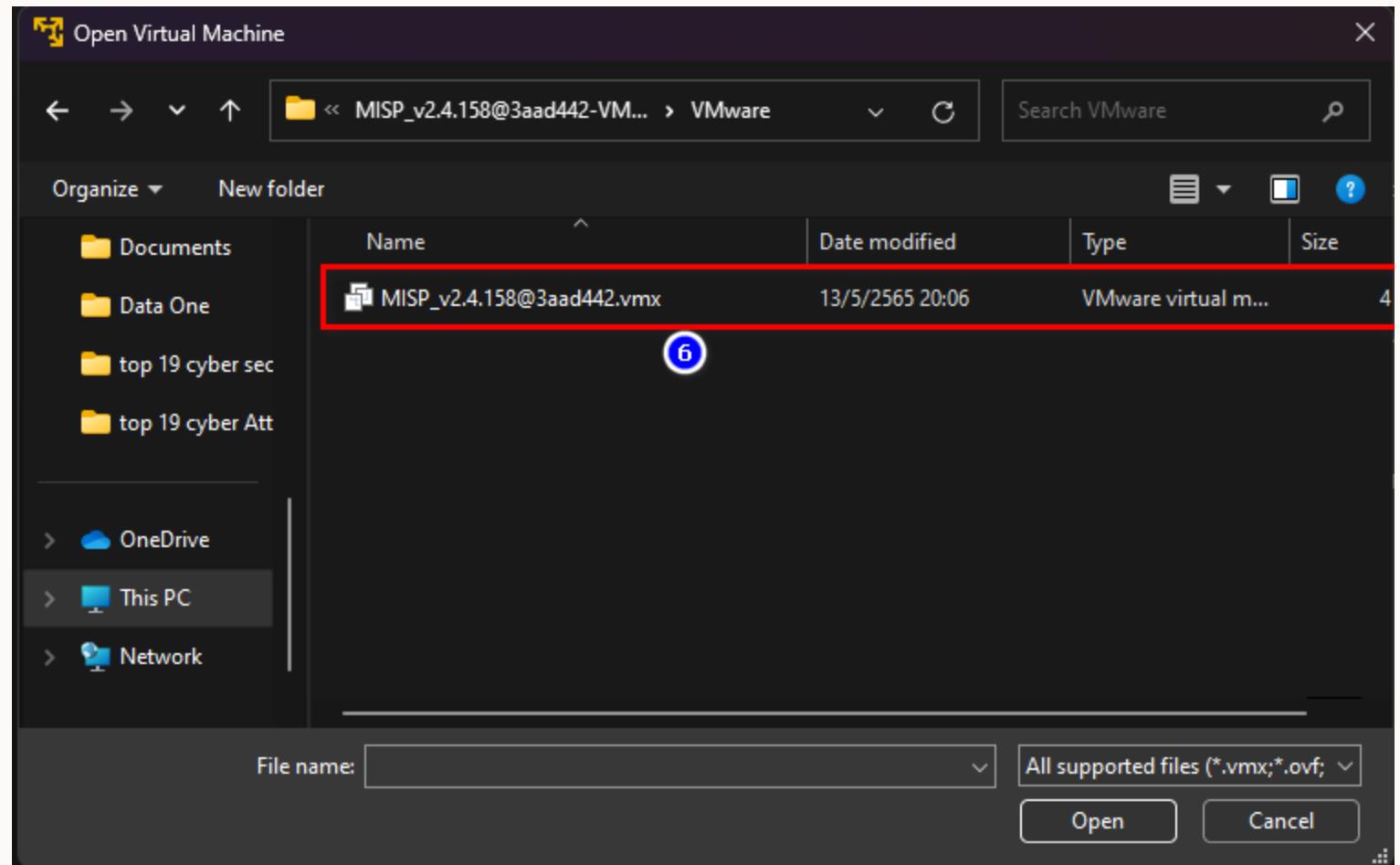
MISP: Open File

- ❑ Click Open a Virtual Machine



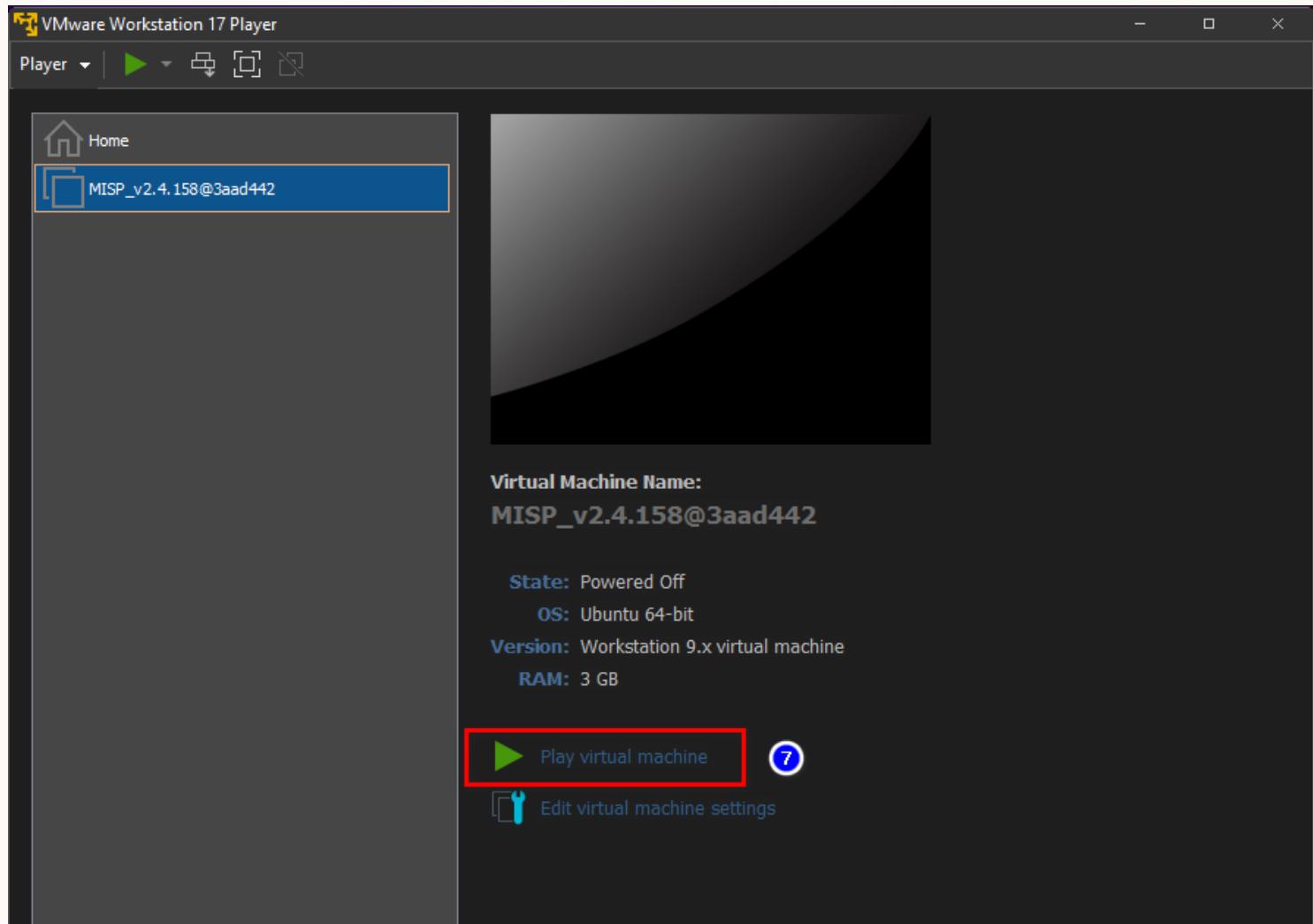
MISP: Open File on Vmware

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



MISP: Open File on Vmware

- Click Play virtual machine



MISP: Open File on Vmware



MISP_v2.4.158@3aad442 - VMware Workstation 17 Player

Player | II |

Ubuntu 18.04.1 LTS misp tty1

Welcome to the MISP Threat Sharing VM.

IP address: 192.168.116.148

MISP	http://192.168.116.148	admin@admin.test / admin
	https://192.168.116.148	
MISP-modules (API)	http://192.168.116.148:6666	(no credentials)
MISP-dashboard	http://192.168.116.148:8001	(no credentials)
Viper-web	http://192.168.116.148:8888	admin / Password1234
jupyter-notebook	http://192.168.116.148:8889	

The default system credentials are: misp / Password1234

On VirtualBox port-forwarding from your host to the guest is in place.
Below are the forwards as we need to use ports >1024 for some.

MISP → 8080 and :8443
ssh → 2222
misp-modules → 1666

If this fails, make sure the host machine is not occupying one of the forwarded ports or a firewall is active.

misp login:

System

User: misp

Pass: Password1234

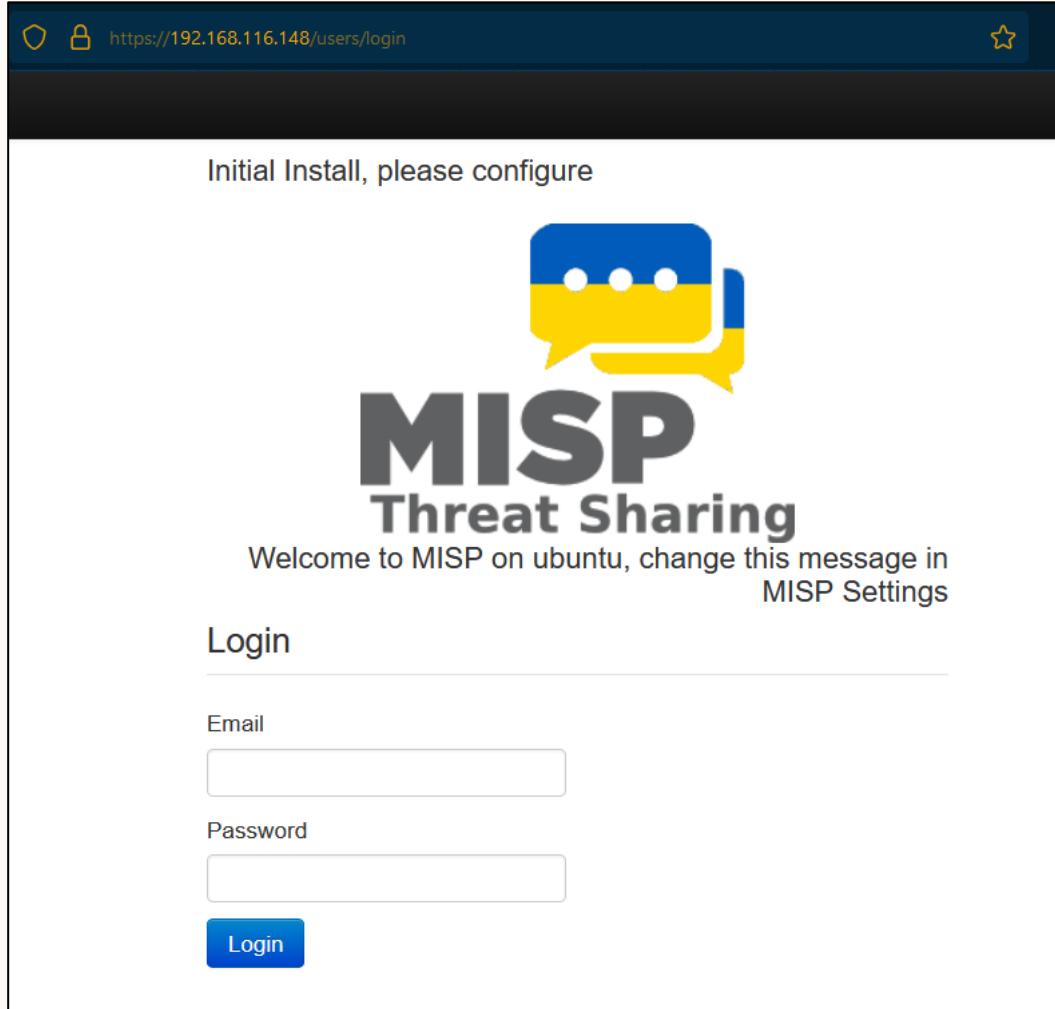
MISP: Web Interface

□ https://192.168.116.148

Web interface

User: admin@admin.test

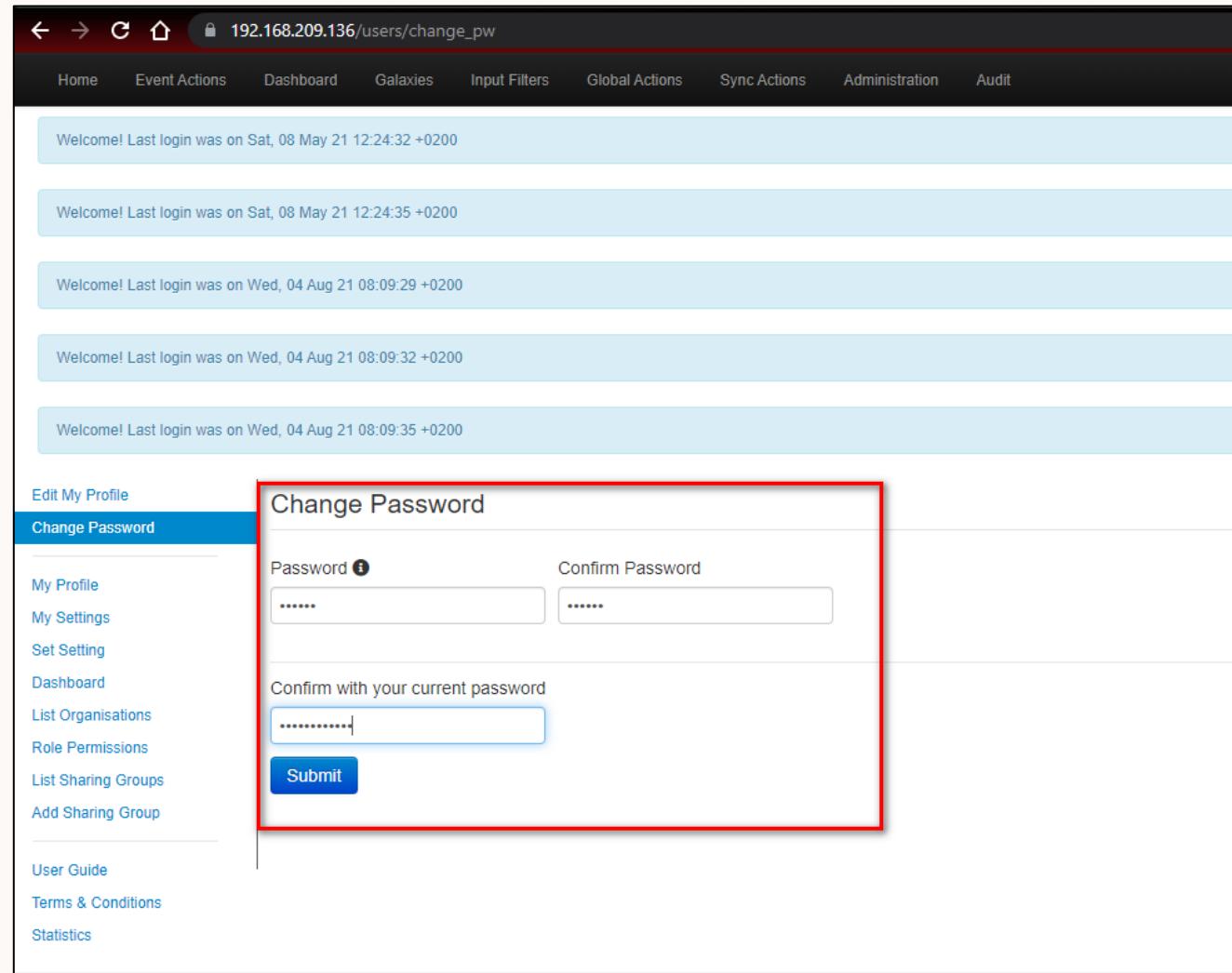
Pass: admin



The screenshot shows a web browser window for the URL <https://192.168.116.148/users/login>. The page displays a message: "Initial Install, please configure". Below this is the MISP Threat Sharing logo, which consists of two speech bubbles (one blue, one yellow) with three dots each, followed by the text "MISP Threat Sharing". A sub-message says, "Welcome to MISP on ubuntu, change this message in MISP Settings". The page has a "Login" section with fields for "Email" and "Password", and a "Login" button.

MISP: Change Password

- Change Password
- Click Submit



The screenshot shows a web browser window for the URL `192.168.209.136/users/change_pw`. The page title is "Change Password". On the left, there is a sidebar with the following menu items:

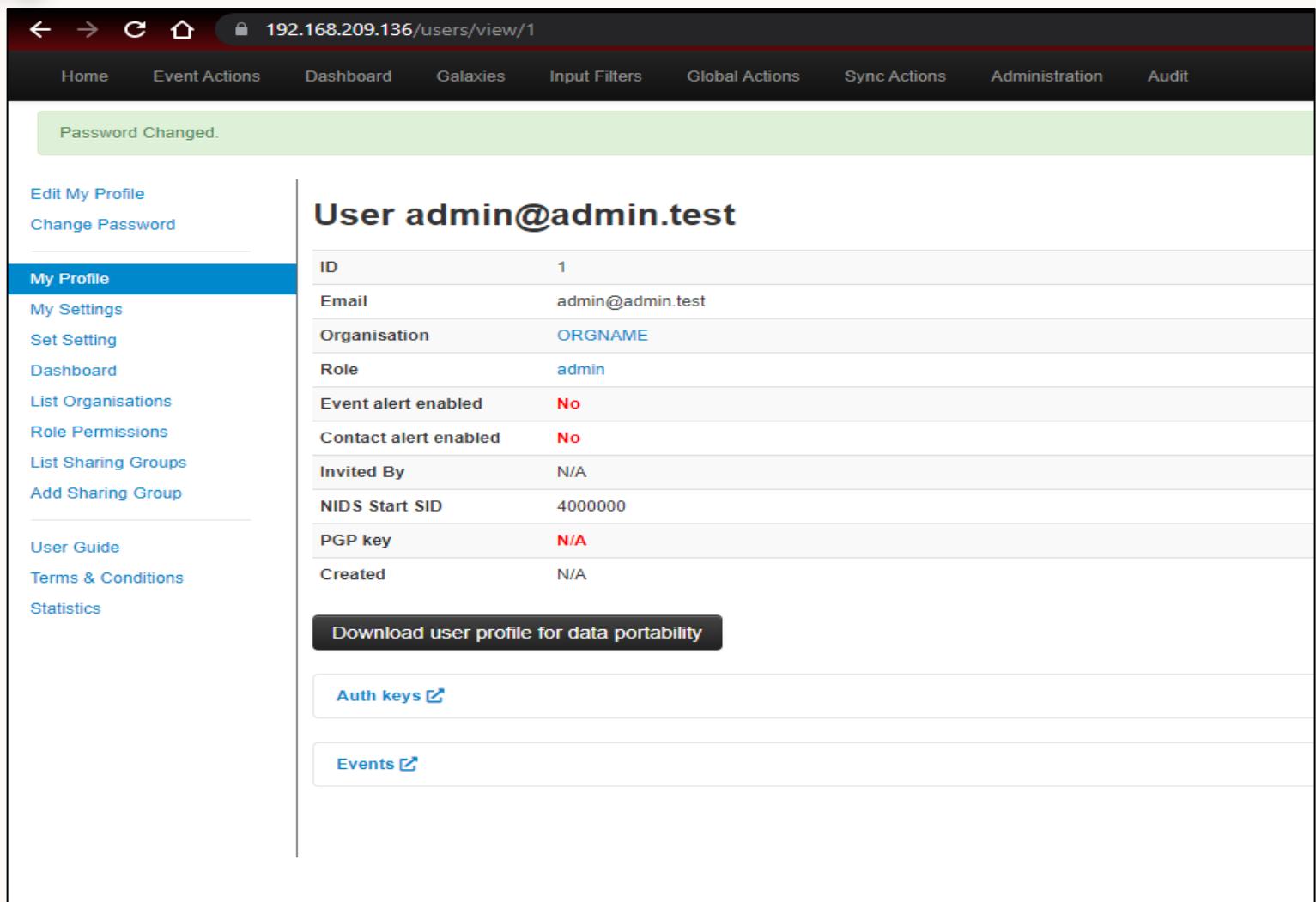
- [Edit My Profile](#)
- [**Change Password**](#) (This item is highlighted with a blue background)
- [My Profile](#)
- [My Settings](#)
- [Set Setting](#)
- [Dashboard](#)
- [List Organisations](#)
- [Role Permissions](#)
- [List Sharing Groups](#)
- [Add Sharing Group](#)

Below the sidebar, there is a link to "User Guide" and "Terms & Conditions", followed by a "Statistics" link.

The main content area contains five identical welcome messages, each reading "Welcome! Last login was on Sat, 08 May 21 12:24:32 +0200". Below these messages is the "Change Password" form, which is enclosed in a red rectangular border. The form has two input fields: "Password" and "Confirm Password", both containing masked text. Below these fields is a third input field labeled "Confirm with your current password" also containing masked text. At the bottom of the form is a blue "Submit" button.

MISP: My Profile

Click My Profile



The screenshot shows the 'My Profile' section of the MISP web interface. The URL in the browser bar is 192.168.209.136/users/view/1. The top navigation bar includes Home, Event Actions, Dashboard, Galaxies, Input Filters, Global Actions, Sync Actions, Administration, and Audit.

A green message box at the top left says "Password Changed." Below it is a sidebar with the following links:

- Edit My Profile
- Change Password
- My Profile** (selected)
- My Settings
- Set Setting
- Dashboard
- List Organisations
- Role Permissions
- List Sharing Groups
- Add Sharing Group
- User Guide
- Terms & Conditions
- Statistics

The main content area displays the user details for "User admin@admin.test":

ID	1
Email	admin@admin.test
Organisation	ORGNAME
Role	admin
Event alert enabled	No
Contact alert enabled	No
Invited By	N/A
NIDS Start SID	4000000
PGP key	N/A
Created	N/A

Below the user details are three buttons:

- Download user profile for data portability
- Auth keys
- Events

Threat Intelligence Feeds

MISP: List Feeds

Sync Actions → List Feeds

https://192.168.116.148/feeds/index/scope:default

Home Event Actions Dashboard Galaxies Input Filters Global Actions Sync Actions Administration Logs API MISP Admin Log out

List Feeds

Search Feed Caches

Add Feed

Import Feeds from JSON

Feed overlap analysis matrix

Export Feed settings

Feeds

Generate feed lookup caches or fetch feed data (enabled feeds only)

Load default feed metadata Cache all feeds Cache freetext/CSV feeds Cache MISP feeds Fetch and store all feed data

« previous next »

Default feeds		Custom feeds		All feeds		Enabled feeds		Enter value to search		Filter									
ID	Enabled	Caching	Name	Format	Provider	Org	Source	URL	Headers	Target	Publish	Delta	Override	Distribution	Tag	Visible	Caching	Actions	
1	x	x	CIRCL OSINT Feed	misp	CIRCL		network	https://www.circl.lu/doc/misp/feed-osint		Feed not enabled	x	x	x	All communities	x	Not cached			
2	x	x	The Botvrij.eu Data	misp	Botvrij.eu		network	https://www.botvrij.eu/data/feed-osint		Feed not enabled	x	x	x	All communities	x	Not cached			

MISP: Enable Feeds

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

https://192.168.116.148/feeds

2 feeds enabled.

Feeds

Generate feed lookup caches or fetch feed data (enabled feeds only)

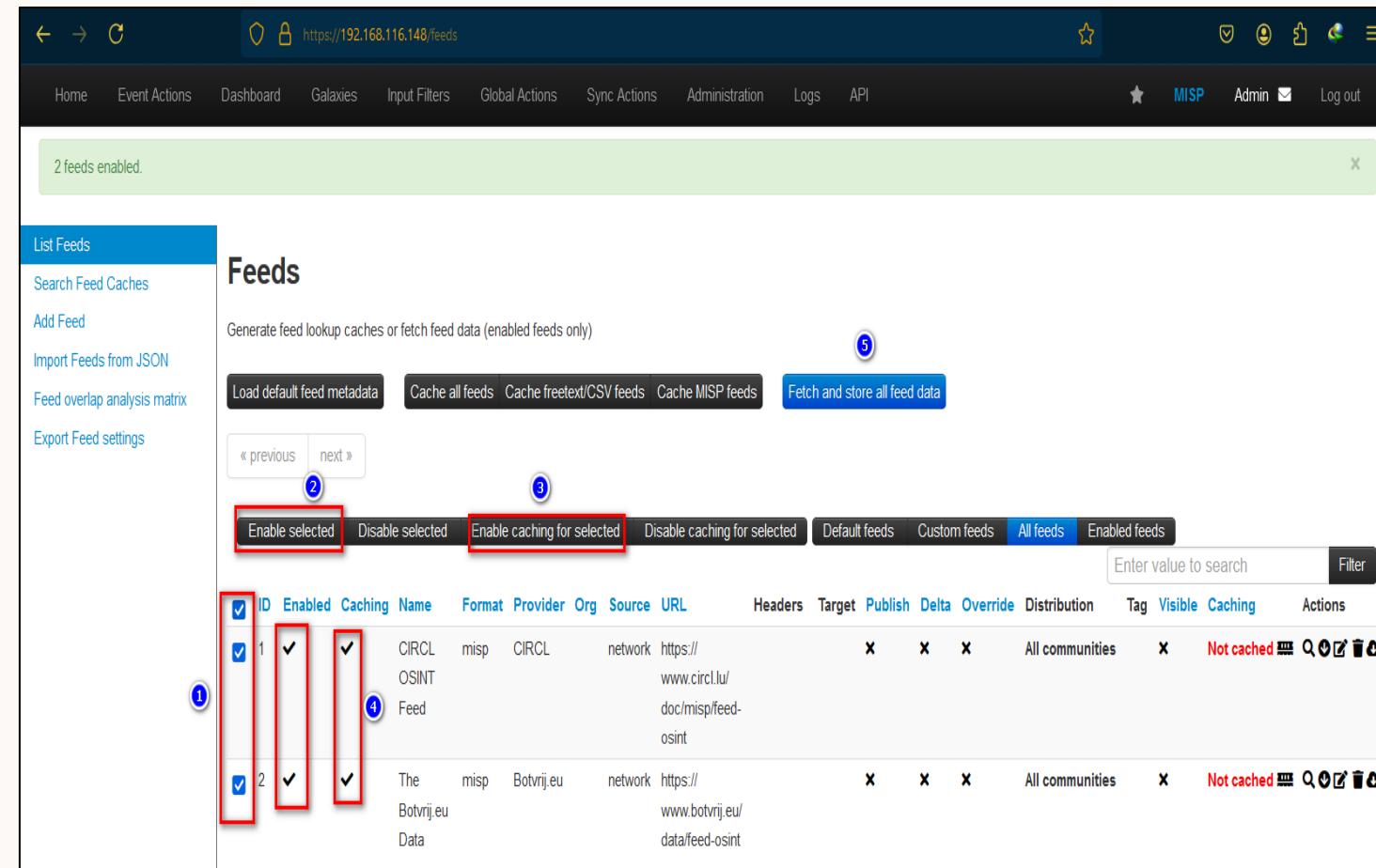
Load default feed metadata Cache all feeds Cache freetext/CSV feeds Cache MISP feeds Fetch and store all feed data

ID	Enabled	Caching	Name	Format	Provider	Org	Source	URL	Headers	Target	Publish	Delta	Override	Distribution	Tag	Visible	Caching	Actions	
1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	CIRCL	misp	CIRCL	network	https://www.circ1.lu/doc/misp/feed-osint	x	x	x			All communities	x	Not cached			
2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	The Botvrij.eu Data	misp	Botvrij.eu	network	https://www.botvrij.eu/data/feed-osint	x	x	x			All communities	x	Not cached			

1 2 3 4 5

Enable selected Disable selected Enable caching for selected Disable caching for selected Default feeds Custom feeds All feeds Enabled feeds

Enter value to search Filter



Threat intelligence platform



[AlienVault](#)

<https://otx.alienvault.com>



[VirusTotal](#)

<https://www.virustotal.com>

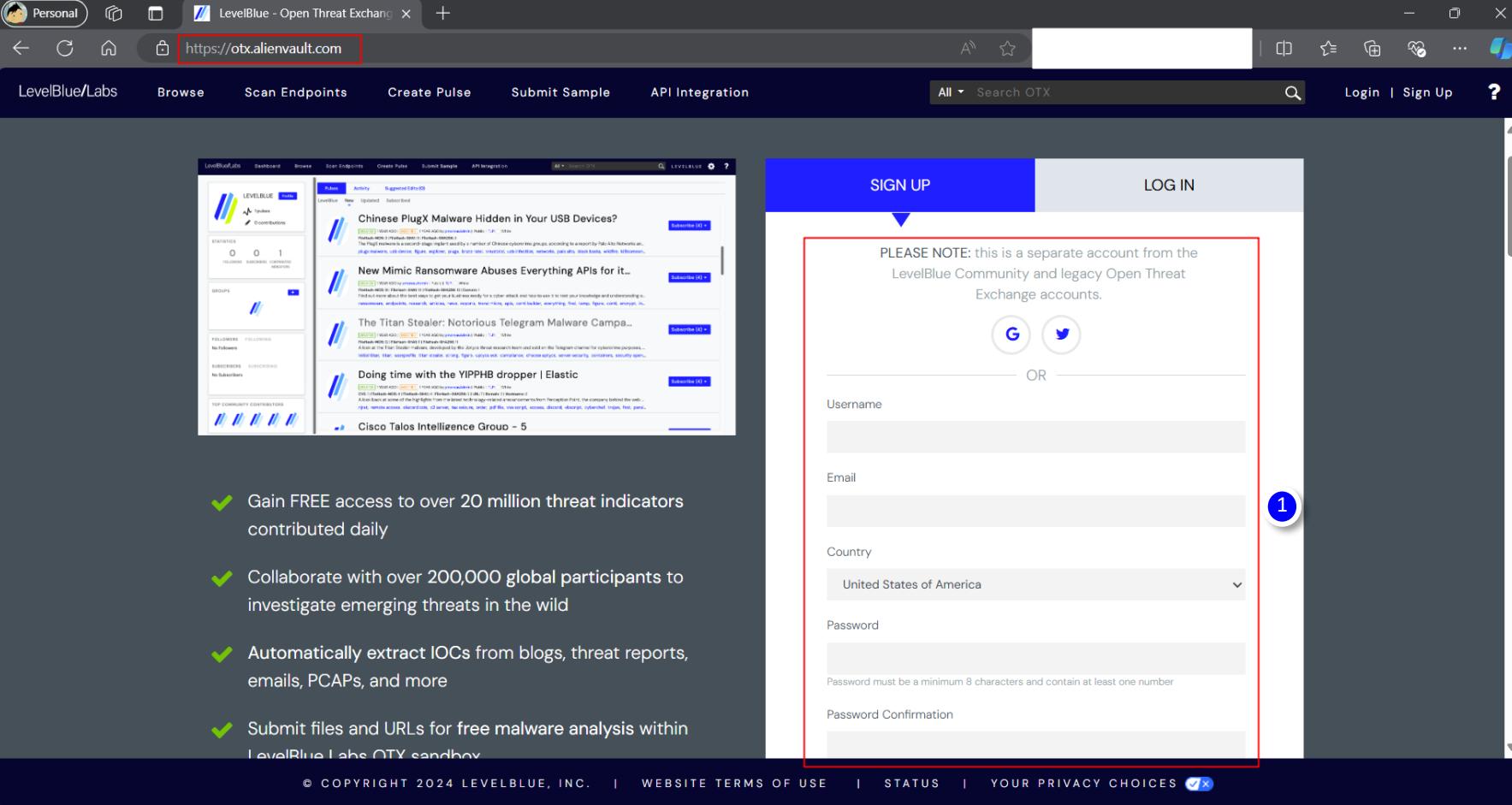


[PhishTank](#)

<https://www.phishtank.com>

Threat Intelligence Feeds: API

MISP: Add API Feeds



The screenshot shows a web browser displaying the LevelBlue - Open Threat Exchange website at <https://otx.alienvault.com>. The main navigation bar includes links for Personal, Browse, Scan Endpoints, Create Pulse, Submit Sample, API Integration, Search OTX, Login, and Sign Up.

The left sidebar shows the LevelBlue/Labs dashboard with sections for Activity, Statistics (0 followers, 0 following), Groups, Followers, Subscribers, and Top Community Contributors. The main content area displays several threat intelligence feeds:

- Chinese PlugX Malware Hidden in Your USB Devices
- New Mimic Ransomware Abuses Everything APIs for it...
- The Titan Stealer: Notorious Telegram Malware Campa...
- Doing time with the YPPHB dropper | Elastic
- Cisco Talos Intelligence Group – 5

Below these feeds, there is a list of benefits:

- Gain FREE access to over 20 million threat indicators contributed daily
- Collaborate with over 200,000 global participants to investigate emerging threats in the wild
- Automatically extract IOCs from blogs, threat reports, emails, PCAPs, and more
- Submit files and URLs for free malware analysis within LevelBlue Labs OTX sandbox

The right side of the screen features a sign-up form with fields for Username, Email, Country (set to United States of America), Password, and Password Confirmation. A note above the form states: "PLEASE NOTE: this is a separate account from the LevelBlue Community and legacy Open Threat Exchange accounts." There are also "SIGN UP" and "LOG IN" buttons. A red box highlights the sign-up form, and a blue circle with the number "1" points to the "Country" dropdown field.

MISP: Add API Feeds

DirectConnect API

The OTX DirectConnect API allows you to easily synchronize the Threat Intelligence available in OTX to the tools you use to monitor your environment. Using the DirectConnect agents you can integrate with your infrastructure to detect threats targeting your environment. If there is no pre-built agent for the products you are using, leverage the DirectConnect SDK (available in Java and Python) to develop your own integration for the community.

[Resources](#)
[Docs](#)
[TAXII](#)
[Example API Uses](#)

Example API Uses

Do you know of any OTX API integrations we're missing here, or planning on writing your own?

We've love to hear - Let us know via cs-otx-support@att.com or the feedback form.

 Search:

NAME	DESCRIPTION	LANGUAGE
OpenCTI Connector	Imports OTX threat data into the OpenCTI platform	Python
MISP Importer	Imports pulses into a MISP instance	Python
Splunk Importer Tutorial	Splunk and Sysmon via a CSV export	Python
Bro Importer	Integrate Bro with LevelBlue Labs OTX	Python
OTX 2 CRITS	Imports pulses into CRITS	Python
The Hive	Incident Response Platform	Python

DirectConnect API Usage

Your OTX Key: [03b973e639b3852bcda7feecd5b335802ce...](#) 

Using API: 

Connect to LevelBlue USM™ or LevelBlue OSSIM™

Already using LevelBlue USM or LevelBlue OSSIM? If so, use your OTX API key with USM / OSSIM and get the benefits of the DirectConnect API immediately.

Don't have LevelBlue USM? [Try LevelBlue USM.](#)

MISP: Add API Feeds

List Feeds

Search Feed Caches

Add Feed

Import Feeds from JSON

Feed overlap analysis matrix

Export Feed settings

③

Add MISP Feed

Add a new MISP feed source.

Enabled

Caching enabled

Lookup visible

Name
AlienVault OTX

Provider
AlienVault

Input Source
Network

URL
<https://otx.alienvault.com/api/v1/pulses/subscribed>

Source Format
MISP Feed

Any headers to be passed with requests (for example: Authorization)

```
Authorization: Bearer
03b973e639b3852bcda7fecd5b335802ce7e6803fa8a53983953ddda6995cb7f
Content-Type: application/json
```

Add Basic Auth

- Name: AlienVault OTX
- Provider: AlienVault
- Input Source: Network
- URL:
<https://otx.alienvault.com/api/v1/pulses/subscribed>
- Source Format: MISP Feed
- Headers:
- Authorization: Bearer
848249a584bdabb281287fd9d9297da25e26
d2b392c925109e156b48f20fa115
- Content-Type: application/json

MISP: Add API Feeds

Any headers to be passed with requests (for example: Authorization)

```
Authorization: Bearer  
03b973e639b3852bcd47fec5b335802ce7e6803fa8a53983953ddda6995cb7f  
Content-Type: application/json
```

Add Basic Auth

Distribution

All communities

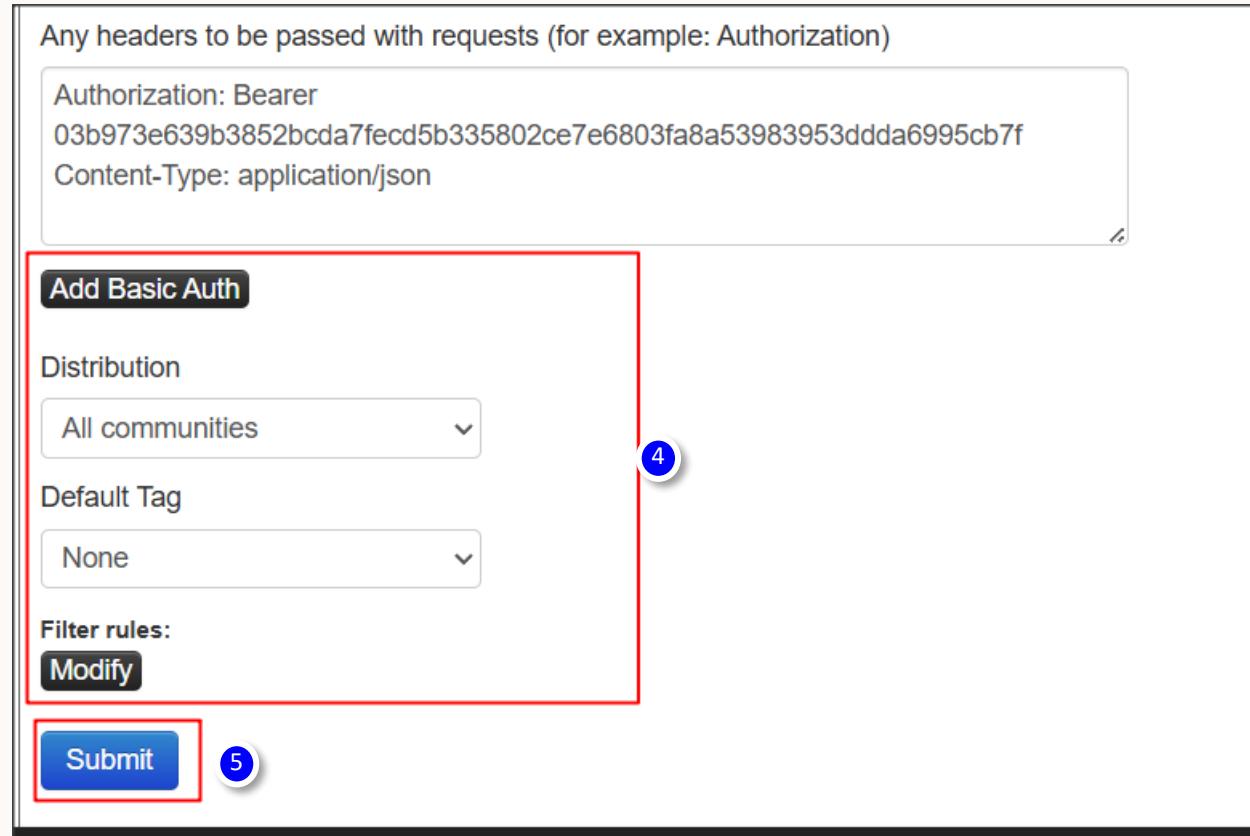
Default Tag

None

Filter rules:

Modify

Submit



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

MISP: Add API Feeds

Feeds

Generate feed lookup caches or fetch feed data (enabled feeds only)

[Load default feed metadata](#) [Cache all feeds](#) [Cache freetext/CSV feeds](#) [Cache MISP feeds](#) [Fetch and store all feed data](#)

[**« previous**](#) [**next »**](#)

Default feeds	Custom feeds	All feeds	Enabled feeds						
<input type="checkbox"/>	ID	Enabled	Caching	Name	Format	Provider	Org	Source	URL
<input type="checkbox"/>	1	x	x	CIRCL OSINT Feed	misp	CIRCL		network	https://www.circl.lu/doc/misp/feed-osint
<input type="checkbox"/>	2	x	x	The Botvrij.eu Data	misp	Botvrij.eu		network	https://www.botvrij.eu/data/feed-osint

SHA256

<input type="checkbox"/> 10 ✓ ✓	AlienVault OTX	misp	AlienVault	network	https://otx.alienvault.com/api/v1/pulses/subscribed	Authorization: Bearer 03b973e639b3852bcda7fecd5b335802ce7e6803fa8a53983953ddda6995cb7f	Content-Type: application/json
---------------------------------	----------------	------	------------	---------	---	--	--------------------------------

Threat Intelligence Feeds: CSV

MISP: Add CSV Feeds

Home Event Actions Dashboard Galaxies Input Filters Global Actions Sync Actions Administration Logs API

List Feeds Search Feed Caches Add Feed Import Feeds from JSON Feed overlap analysis matrix Export Feed settings **Edit Feed** View Feed

Edit MISP feed

Add a new MISP feed source.

Enabled

Caching enabled

Lookup visible

Name: MalwareBazaar SHA256

Provider: Abuse.ch

Input Source: Network

URL: <https://bazaar.abuse.ch/export/txt/sha256/full/>

Source Format: Simple CSV Parsed Feed

Any headers to be passed with requests (for example: Authorization)

Line break separated list of headers in the "headername: value" format

Add Basic Auth

- 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

MalwareBazaar csv Abuse.ch ORGNAME network https://bazaar.abuse.ch/export/txt/sha256/full/
SHA256

New event each pull x x

AlienVault OTX misp AlienVault network https://otx.alienvault.com/api/v1/pulses/subscribed Authorization: Bearer 03b973e639b3852bcda7fec5b335802ce7e6803fa8a53983953ddda6995cb7f Content-Type: application/json

x x

List Feeds		Feeds									
Search Feed Caches	Add Feed	Generate feed lookup caches or fetch feed data (enabled feeds only)									
Import Feeds from JSON	Feed overlap analysis matrix	Load default feed metadata	Cache all feeds	Cache freetext/CSV feeds	Cache MISP feeds	Fetch and store all feed data					
Export Feed settings	« previous next »										
Default feeds Custom feeds All feeds Enabled feeds											
<input type="checkbox"/>	ID	Enabled	Caching	Name	Format	Provider	Org	Source	URL		
<input type="checkbox"/>	1	x	x	CIRCL OSINT Feed	misp	CIRCL		network	https://www.circl.lu/doc/misp/feed-osint		
<input type="checkbox"/>	2	x	x	The Botvrij.eu Data	misp	Botvrij.eu		network	https://www.botvrij.eu/data/feed-osint		

MISP: Add CSV Feeds

<input type="checkbox"/>	<input checked="" type="checkbox"/>	CthulhuSPRL.be ORGNAME — 244 Threat Actor   	 type:OSINT  tip:white	143	1	admin@admin.test 2015-07-08 2020-08-03 08:31:12	OSINT Prof level attack Sym
<input type="checkbox"/>	<input checked="" type="checkbox"/>	ORGNAME ✓ 73	 type:OSINT  tip:white  malware_classification:malware-category="Ransomware"  osint:source-type="blog-post"	6		admin@admin.test 2016-04-08 2018-12-12 14:53:11	OSINT encr world
<input type="checkbox"/>	<input checked="" type="checkbox"/>	CthulhuSPRL.be ORGNAME — 354 Threat Actor   	 tip:green  APT  misp-galaxy:mitre-enterprise-attack-intrusion-set="APT28"	1522	13	admin@admin.test 2015-04-20 2018-07-25 13:29:31	Exp share with dom
<input type="checkbox"/>	<input checked="" type="checkbox"/>	CthulhuSPRL.be ORGNAME ↗ 325 Tool   	 type:OSINT  tip:green	35	2	admin@admin.test 2014-12-04 2018-03-18 22:50:02	Regi
<input type="checkbox"/>	<input checked="" type="checkbox"/>	CthulhuSPRL.be ORGNAME — 289 Threat Actor   	 type:OSINT  tip:white	58	1	admin@admin.test 2015-04-13 2018-03-18 21:57:30	OSINT dete Scar by F
<input type="checkbox"/>	<input checked="" type="checkbox"/>	CthulhuSPRL.be ORGNAME ? 194	 type:OSINT  tip:green	7440	26	admin@admin.test 2014-11-20 2018-02-05 08:53:58	Imp publ malv

MISP: Events

□ Event Actions → List Events

https://192.168.116.148/events/index

Home Event Actions Dashboard Galaxies Input Filters Global Actions Sync Actions Administration Logs API MISP Admin Log out

List Events Add Event Import from... REST client

Events

« previous 1 2 next »

	My Events	Org Events	Filter	Enter value to search	Event info	Filter							
	Published	Creator org	Owner org	ID	Clusters	Tags	#Attr.	#Corr.	Creator user	Date	Last modified at	Info	Distribution
<input type="checkbox"/>	<input checked="" type="checkbox"/>	 ORGNAME	 72			 type:OSINT  tlp:white  malware_classification:malware-category="Ransomware"  osint:source-type="blog-post"	6		admin@admin.test	2016-04-08	2018-12-12 14:53:11	OSINT - Locky: the encryptor taking the world by storm	All ↗
<input type="checkbox"/>	<input checked="" type="checkbox"/>	 ORGNAME	 11	Threat Actor	  type:OSINT  tlp:white   Packrat  	154		admin@admin.test	2015-12-09	2016-12-30 12:55:05	OSINT - Packrat: Seven Years of a South American Threat Actor	All ↗	

MISP: Events

1 **Add Event**

Date: 2024-07-23

Distribution: This community only (2)

Threat Level: Low (3)

Analysis: Initial (4)

Event Info: Test Check IP Undified (5)

Extends Event: Event UUID or ID. Leave blank if not applicable.

Submit (6)

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

MISP: Events

Test Check IP Undified

Event ID	1740
UUID	736de76c-0fea-45c3-8774-b8f0acce4025 
Creator org	ORGNAME
Owner org	ORGNAME
Creator user	thanapol.k@tnetitsolution.co.th
Protected Event (experimental) 	 Event is in unprotected mode  Switch
Tags	7   <div style="border: 1px solid #ccc; padding: 5px; display: inline-block;"> <input data-bbox="678 1058 857 1101" type="text" value="tlp:white"/> X </div> 8  9
Date	2024-07-
Threat Level	Low
Analysis	Initial
Distribution	This community only 

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

MISP: Events

10

View Event	
View Correlation Graph	
View Event History	
Edit Event	
Delete Event	
Add Attribute	
Add Object	
Add Attachment	
Add Event Report	
Populate from...	
Enrich Event	
Merge attributes from...	
Publish Event	
Publish (no email)	
Publish event to ZMQ	
Contact Reporter	
Download as...	

Test Check IP Undified

Event ID	1740
UUID	736de76c-0fea-45c3-8774-b8f0acce4025 +≡
Creator org	ORGNAME
Owner org	ORGNAME
Creator user	thanapol.k@tnetitsolution.co.th
Protected Event (experimental) i	🔒 Event is in unprotected mode. 🔒 Switch to protected mode
Tags	t!ip:white x + +
Date	2024-07-23
Threat Level	▼ Low
Analysis	Initial
Distribution	This community only i 🔗
Warnings	Content: Your event has neither attributes nor objects, whilst this can have legitimate reasons (such as purely creating an event with an event report or galaxy clusters), in most cases it's a sign that the event has yet to be fleshed out.

□ Click Add Attribute

MISP: Events

View Event History

Edit Event

Delete Event

Add Attribute

Add Object

Add Attachment

Add Event Report

Populate from...

Enrich Event

Merge attributes from...

Publish Event

Publish (no email)

Publish event to ZMQ

Contact Reporter

Download as...

List Events

Add Event

Category i

Network activity i 11

Type i ip-src 12

Distribution i

Your organisation only

Value

192.168.10.10 13
192.168.10.11

Contextual Comment

For Intrusion Detection System
 Batch Import 14

Disable Correlation

First seen date calendar Last seen date calendar

First seen time clock Last seen time clock

HH:MM:SS.ssssss+TT:TT HH:MM:SS.ssssss+TT:TT

Expected format: HH:MM:SS.ssssss+TT:TT Expected format: HH:MM:SS.ssssss+TT:TT

Submit 15

- 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

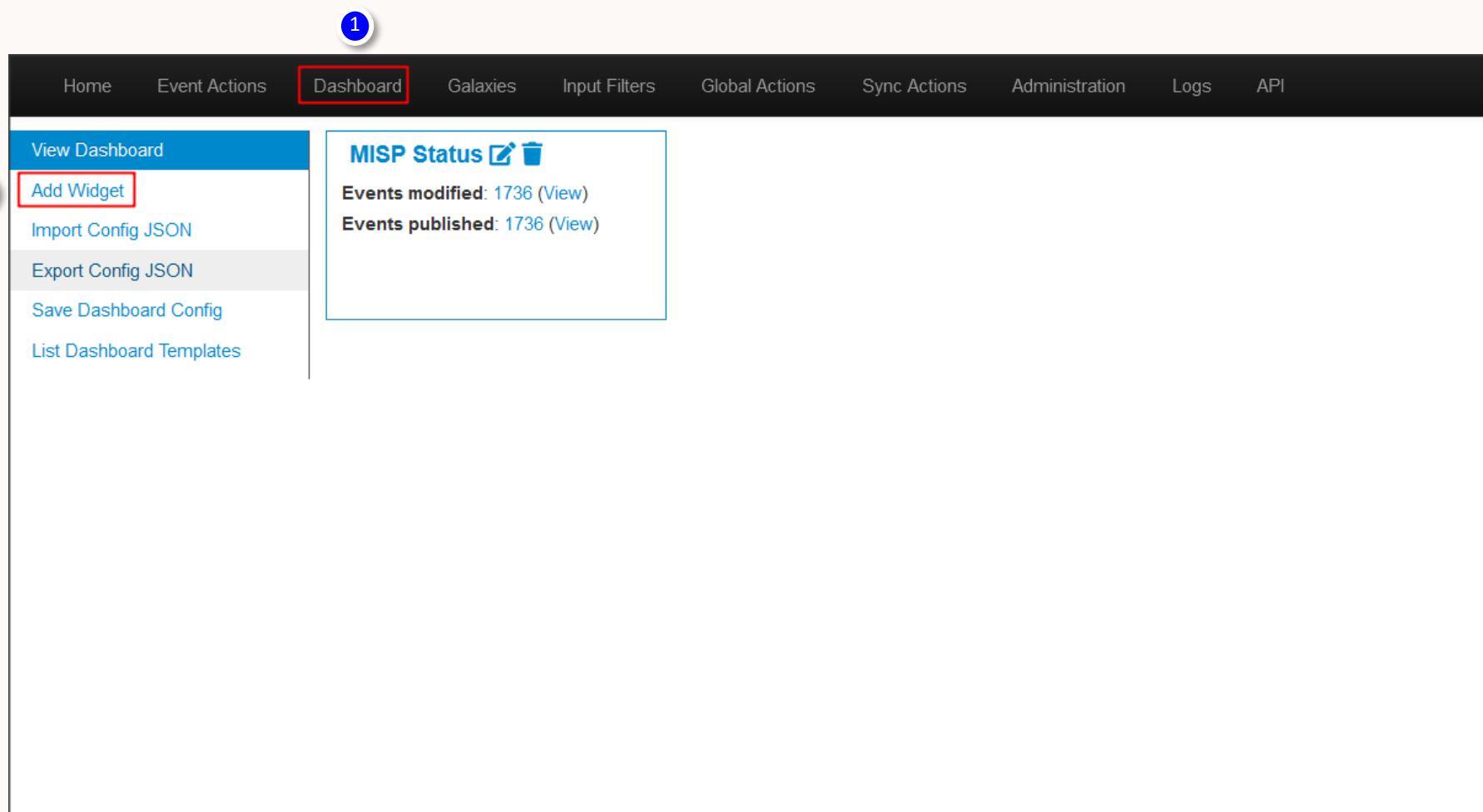
MISP: Events

Events

Events										
<input type="text"/> Enter value to search Event info ▾ Filter										
#	Attr.	#Corr.	Date	Last modified at ↗	Published at	Info	Distribution	Actions		
1	x	ORGNAME	ORGNAME	▼ 1740	ttx:white	2	2024-07-23	2024-07-23 12:16:02	Test Check IP Undified	
2	✓	ORGNAME	ORGNAME	▼ 1329	<input checked="" type="checkbox"/> ttx:white <input checked="" type="checkbox"/> misp-galaxy:misp-attack-pattern="Initial Access - Phishing [T1566]" <input checked="" type="checkbox"/> misp-galaxy:misp-attack-pattern="Defense Evasion - Impair Defenses: Disable or Modify Tools [T1562.001]" <input checked="" type="checkbox"/> misp-galaxy:stix-2.1-attack-pattern="3cbb3d7b-4cae-4c7e-a682-e8b70e3f1ee4" <input checked="" type="checkbox"/> misp-galaxy:stix-2.1-attack-pattern="2c373316-6ce5-4f43-9daf-02c94cb0c0a5" <input checked="" type="checkbox"/> misp-galaxy:misp-attack-pattern="Impact - Inhibit System Recovery [T1490]" <input checked="" type="checkbox"/> misp-galaxy:stix-2.1-attack-pattern="f0a904f4-b3f5-4e42-b565-418dc6932d44"	247	2024-05-10	2024-07-19 15:41:32	2024-07-23 11:16:40	CISA - AA24-131A #StopRansomware: Black Basta

Event Add Success

MISP: Alert Events



The screenshot shows the MISP dashboard interface. At the top, there is a navigation bar with links: Home, Event Actions, Dashboard, Galaxies, Input Filters, Global Actions, Sync Actions, Administration, Logs, and API. The 'Dashboard' link is highlighted with a red border. Below the navigation bar, there is a sidebar on the left containing the following options: View Dashboard, Add Widget (highlighted with a red border), Import Config JSON, Export Config JSON, Save Dashboard Config, and List Dashboard Templates. To the right of the sidebar, there is a main content area titled 'MISP Status' with icons for refresh and delete. It displays two statistics: 'Events modified: 1736 (View)' and 'Events published: 1736 (View)'. A blue circle with the number '1' is positioned above the navigation bar, and a blue circle with the number '2' is positioned above the 'Add Widget' button in the sidebar.

- Click Dashboard
- Click Add Widget

MISP: Alert Events

- Select : Event Stream
- Click Submit

Add Widget

Monitor incoming events

Parameters

tags: A list of tagnames separated by commas. An exclamation mark to negate.

orgs: A list of organisation names separated by commas. An exclamation mark to negate.

published: Boolean flag to filter published or not published events.

limit: How many events to display.

fields: A list of fields to include in the output. Default fields are: id, org, info, date, analysis, date.

Widget

3 **Event Stream**

Width

4 2

Config

4 **Submit** Cancel

Event Stream

#	Org	Info
1740	ORGNAME	Test Check IP Undified
1736	CUDESO	MuddyWater replaces Atera by custom MuddyRot implant in a recent campaign
1735	CUDESO	New North-Korean based backdoor packs a punch
1734	CUDESO	Malicious activities linked to the Nobelium intrusion set
1733	CUDESO	Operation Crimson Palace: Sophos threat hunting unveils multiple clusters of Chinese state-sponsored activity targeting Southeast Asian government

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

```
root@misp:/home/misp# sudo nano /etc/postfix/sasl_passwd
```

sudo nano /etc/postfix/sasl_passwd

```
GNU nano 2.9.3                               /etc/postfix/sasl_passwd
[smtp.gmail.com]:587 [REDACTED] :obyqrdjkxrgqqpejk
```

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

```
root@misp:/home/misp# sudo nano /etc/postfix/sasl_passwd
root@misp:/home/misp# sudo nano /etc/postfix/sender_canonical
root@misp:/home/misp#
```

sudo nano /etc/postfix/sender_canonical

```
GNU nano 2.9.3                               /etc/postfix/sender_canonical
root@mailserver.home [REDACTED]
```

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

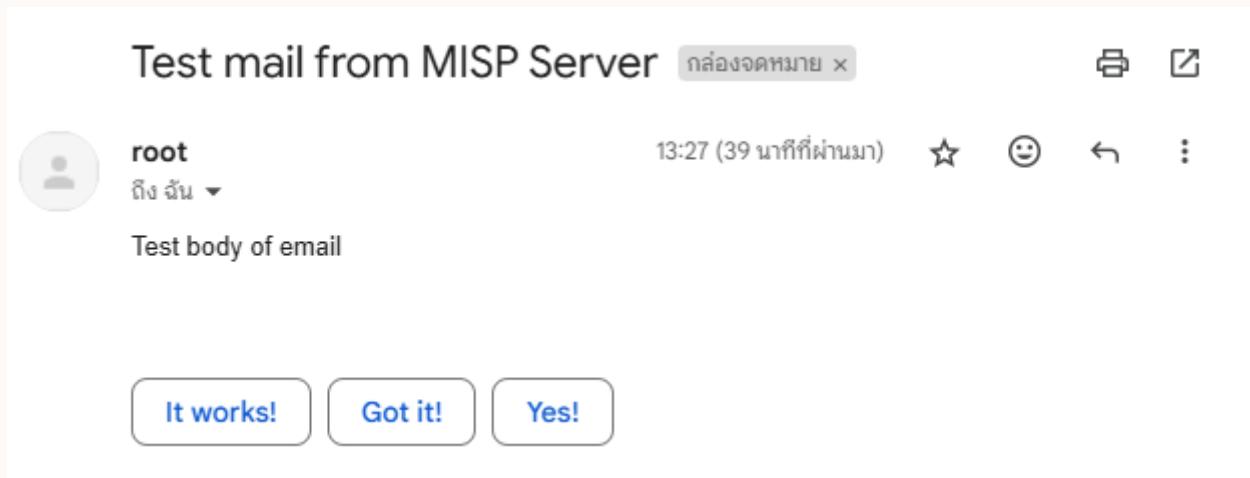
sudo postmap /etc/postfix/sender_canonical

sudo systemctl reload postfix

MISP: Alert Email

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

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
```

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

```
class EmailConfig {
    public $default = array(
        'transport' => 'Smtp',
        'from' => array('mordeenslak@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' => 'mordeenslak@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

Screenshot of the MISP web interface showing the "Server Settings & Maintenance" page.

The top navigation bar includes: Dashboard, Galaxies, Input Filters, Global Actions, Sync Actions, Administration (highlighted in blue), Logs, and API.

The left sidebar lists various administration options:

- List Users
- List Auth Keys
- List User Settings
- Set User Setting
- Add User
- Contact Users
- User Registrations
- List Organisations
- Add Organisations
- List Roles
- Add Roles
- Server Settings & Maintenance** (highlighted with a red border)
- Jobs

The main content area is titled "Server Settings & Maintenance". It features a table with the following data:

Test	Value
Overall health	Critical, your server has 8 critical issues.
Critical settings incorrectly or not set	1 incorrect setting detected.
Recommended settings incorrectly or not set	0 incorrect settings detected.
Optional settings incorrectly or not set	36 incorrect settings detected.
Critical issues revealed by the diagnostics	0 issues detected.

A note at the bottom states: "To edit a setting, simply double click it."

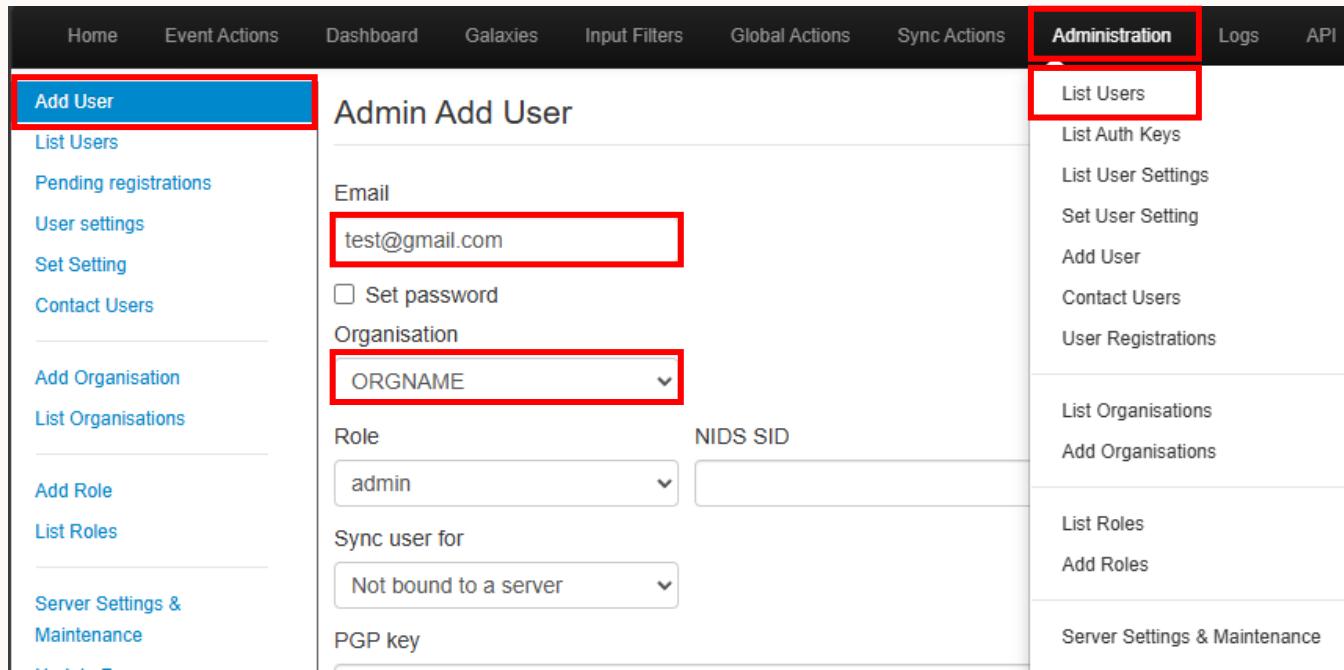
MISP: Alert Email

Server Settings & Maintenance

Server Settings & Maintenance					
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



The screenshot shows the MISP administration interface. The top navigation bar includes links for Home, Event Actions, Dashboard, Galaxies, Input Filters, Global Actions, Sync Actions, Administration (which is highlighted with a red box), Logs, and API. On the left, a sidebar menu lists Add User (highlighted with a blue box), List Users, Pending registrations, User settings, Set Setting, Contact Users, Add Organisation, List Organisations, Add Role, List Roles, Server Settings & Maintenance, and more. The main content area is titled "Admin Add User" and contains fields for Email (test@gmail.com), Organisation (ORGNAME), Role (admin), NIDS SID, Sync user for (Not bound to a server), and PGP key.

□ Administration > List Users > Add User

MISP: Alert Email

Home Event Actions Dashboard Galaxies Input Filters Global Actions Sync Actions **Administration** Logs API

Add User List Users Pending registrations User settings Set Setting Contact Users

Email test@gmail.com Set password Organisation ORGNAME Role admin NIDS SID Sync user for Not bound to a server PGP key

List Users List Auth Keys List User Settings Set User Setting Add User Contact Users User Registrations

List Organisations Add Organisations PGP key Paste the user's PGP key here or try to retrieve it from the CIRCL key server by clicking on "Fetch PGP key" below.

List Roles Add Roles Server Settings & Maintenance

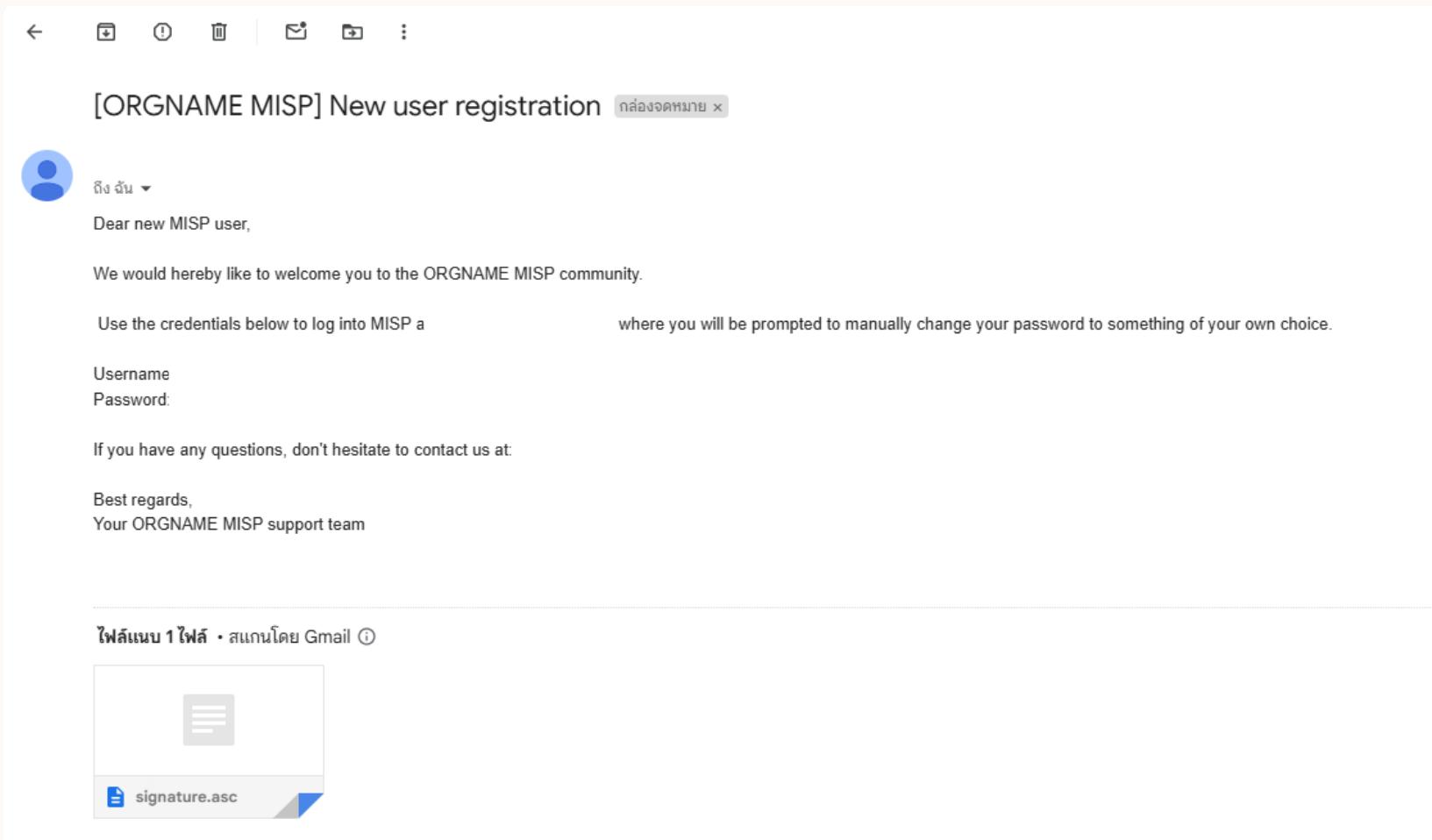
Fetch PGP key

Receive email alerts when events are published
 Receive email alerts from "Contact reporter" requests
 Immediately disable this user account
 Send credentials automatically

Create user

Administration > List Users > Add User

MISP: Alert Email



[ORGNAME MISP] New user registration คลื่งจดหมาย x

ผู้ใช้งาน ▾
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

