PostecH

Technical specifications
Threat-Intel-Hub

Centralized Actionable Threat Intelligence Platform

Product:	Threat-Intel-Hub
Document version:	1.0.0
Document Type:	Technical Specifications
Date of preparation:	November 15 , 2025
Author:	Postech

TECHNICAL SPECIFICATIONS

TI-HUB THREAT INTEL HUB

Centralized Actionable Threat Intelligence Platform

Product:	TI-HUB
Version:	1
Document Type:	Technical Specifications
Date:	October 10, 2025
Classification:	Commercial
Contact:	sales@postech.us

Table of Contents

1. GENERAL INFORMATION AND SCOPE

Product Name	Threat Intel Hub (TI Hub)
Version	2.5.3
Release Date	January 2026
Software Type	Threat Intelligence Platform
License	Owner
Architecture	Monolithic with optional microservices
Development Language	Python 3.10+
Database	MySQL 8.0+
Operating System	Ubuntu Server 24.04 LTS

2. TECHNICAL SPECIFICATIONS

Hardware Requirements

Component	Minimum	Recommended	Enterprise
CPU	2 cores @ 2.4 GHz	4 cores @ 3.0 GHz	8 cores @ 3.5 GHz
RAM	4GB	8 GB	16 GB
Storage	20 GB SSD	50 GB SSD	100 GB NVMe
Grid	10 Mbps	100 Mbps	1 Gbps
Bandwidth	500 MB/day	2 GB/day	5 GB/day

Software Requirements

Component	Minimum Version	Recommended Version
Operating System	Ubuntu 22.04 LTS	Ubuntu 24.04 LTS
Python	3.10	3.12+
MySQL	8.0	8.3+
OpenSSL	3.0	3.2+
Git	2.30	2.40+

Python dependencies

Main Dependencies (Python)

Bookshop	Version
beautifulsoup4	4.12.0
mysql-connector-python	8.3.0
Flask	3.0.0
openpyxl	3.1.2
Jinja2	3.1.3
matplotlib	3.8.0
feedparser	6.0.10
python-dotenv	1.0.0

3. SYSTEM ARCHITECTURE

Main Components

Component	Archive	Description	Port
Monitor	ti_hub_monitor.py	Main pickup engine	N/A
Orchestrator	ti_hub_orchestrator.py	3-phase orchestrator	N/A
Advisory Generator	ti_hub_advisory_generator.py	HTML Advisory Generator	N/A
REST API	ti_hub_api.py	Flask REST API Server	8080
Excel Generator	excel_generator.py	Excel file generator	N/A
Weekly Summary	ti_hub_weekly_summary.py	Weekly summary generator	N/A

Specialized Collectors

Collector	Sources	Frequency	Data Type
Phishing	OpenPhish , PhishTank	6 hours	Malicious URLs
Malware	URLhaus , Spamhaus , CyberCrime	6 hours	IPs, Domains, URLs
APT	APTnotes , Cisco Talos	6 hours	Campaign IOCs
KEV	CISA KEV	30 minutes	CVEs exploited
EPSS	FIRST EPSS	4 hours	Exploitation scores

Database - Schema

Operational Database	
Board	**Description**
kev_vulnerabilities	1,447+ records
threat_iocs	342+ active IOCs
threat_alerts	Alerts generated
wazuh_rules	Custom SIEM rules
wazuh_correlations	Matches detected
system_config	System configuration

Optimized Indices:

idx_cve_id (kev_vulnerabilities)
idx_ioc_value (threat_iocs)
idx_type , idx_category , idx_priority (threat_alerts)
idx_rule_id (wazuh_rules)

4. REST API v2.5.3

API Specifications

Feature	Worth
API version	v1
Protocol	HTTP/HTTPS
Default port	8080
Response format	JSON
Authentication	Optional (JWT on roadmap)
Rate Limiting	100 req /min by default
CORS	Enabled by default
MySQL connection pool	10 concurrent connections
Timeout per request	30 seconds

Available Endpoints

Endpoints (9)

Method	Endpoint	Description	Authentication
GET	/api/v1/ health	Health check	No
GET	/api/v1/ dashboard	General metrics	No
GET	/api/v1/ alerts	List of alerts	No
GET	/api/v1/ alerts /{id}	Alert details	No
POST	/ api /v1/alerts/{id}/acknowledge	Recognized brand	No
GET	/api/v1/ iocs	List of IOCs	No
GET	/api/v1/ kevs	List of KEVs	No
GET	/api/v1/ wazuh / correlations	SIEM correlations	No
GET	/api/v1/ wazuh /rules	Wazuh Rules	No

Endpoints v2.5.3 (7)

Method	Endpoint	Description	Parameters
GET	/api/v1/ dashboard / range	Dashboard with date range	start_date , end_date , days
GET	/api/v1/ advisories / stats	Shipping statistics	start_date , end_date , days
GET	/ api /v1/alerts/severity-summary	Summary by severity	start_date , end_date , days
GET	/api/v1/ dashboard / filtered	Filtered Dashboard	priority, category, ioc_category , alert_type
GET	/ api /v1/threats/by-category	IOCs by category	category, start_date , end_date

GET	/ api /v1/alerts/by-priority	Priority alerts	priority , category , days
GET	/api/v1/ categories	List of categories	None

Export Endpoints (8)

Method	Endpoint	Format	MIME Type
GET	/ api /v1/export/excel/{id}	Excel	application / vnd.openxmlformats
GET	/ api /v1/export/csv/{id}	CSV	text / csv
GET	/ api /v1/export/ paloalto /{id}	TXT (EDL)	text / plain
GET	/ api /v1/export/ fortinet /{id}	TXT	text / plain
GET	/ api /v1/export/snort/{id}	Rules	text / plain
GET	/api/v1/ export /yara/{id}	YARA	text / plain
GET	/ api /v1/export/ stix /{id}	STIX 2.1 JSON	application / json
GET	/ api /v1/export/ misp /{id}	MISP JSON	application / json

5. DATA SOURCES

Primary Sources (3)

Fountain	Supplier	Type	URL	API Key	Cost
CISA KEV	CISA	JSON Feed	https://www.cisa.gov/	No	Free
NVD/CVE	NIST	REST API	https://nvd.nist.gov/	Optional	Free
FIRST EPSS	FIRST	REST API	https://api.first.org/	No	Free

Sources of Enrichment (3)

Fountain	Supplier	Type	URL	API Key	Cost
AlienVault OTX	AT&T	REST API	https://otx.alienvault.com/	Yes	Free
VirusTotal	Google	REST API	https://www.virustotal.com/	Yes	Free/Paid
MISP	Self-hosted	REST API	Custom	Yes	Free

Phishing Sources (2)

Fountain	Supplier	Type	Update	API Key	Cost
OpenPhish	OpenPhish	TXT Feed	12 hours	No	Free
PhishTank	Cisco Talos	JSON API	Real time	Yes	Free

Sources of Malware (3)

Fountain	Supplier	Type	Update	API Key	Cost
URLhaus	Abuse.ch	CSV Feed	Real time	No	Free
Spamhaus DROP	Spamhaus	TXT List	Daily	No	Free
Cybercrime Tracker	Community	HTML Scraping	Real time	No	Free

APT Sources/ Campaigns (2)

Fountain	Supplier	Type	Update	API Key	Cost
APTnotes	GitHub	JSON	Continue	No	Free
Cisco Talos	Cisco	RSS Feed	Daily	Optional	Free

TOTAL: 15 integrated sources

6. NOTIFICATION SYSTEM

Individual Advisories

Feature	Specification
Frequency	3 times a day
Default schedules	8:00 AM, 2:00 PM, 8:00 PM (configurable)
Format	Professional HTML + attached Excel spreadsheet
Average email size	50-100 KB (HTML) + 20-50 KB (Excel)
Categories	Threat Advisory, NVD Alert, Threat Anticipation, Threat Hunting Rule
Priorities	CRITICAL, HIGH, MEDIUM, LOW
Personalization	Editable Jinja2 templates
Attachments	Yes (Excel with categorized IOCs)

Weekly Summary

Feature	Specification
Frequency	once a week
Default day	Monday 8:00 AM (configurable)
Format	HTML with embedded graphics (Base64)
Average size	150-300 KB
Graphics included	4-6 (matplotlib)
Analysis period	7 days (configurable)
Content	Metric cards, Top 10 CVEs , statistics, trend

SMTP configuration

Parameter	Supported	Examples
SMTP Server	Yes	Gmail, Office 365, Exchange
Ports	25, 465 (SSL), 587 (TLS)	587 (recommended)
TLS/SSL	Yes	TLS 1.2+
Authentication	Yes	Username / Password , App Passwords
Multiple Containers	Yes	Separated by commas
BCC	No (roadmap)	-

7. SIEM INTEGRATION

Wazuh Integration

Feature	Specification
Wazuh version supported	4.0+
Components	Manager API + Indexer (OpenSearch)
Authentication Manager	Basic Auth (user / password)
Indexer Authentication	Basic Auth (admin / password)
Port Manager	55000 (HTTPS)
Port Indexer	9200 (HTTPS)
Verify SSL	Configurable (false by default)
Lookback days	7 days (configurable)

Features

Function	Description	Automatic
IOC search	Look for IOCs in Wazuh logs	Yes
Rule generation	Create custom rules (100001+)	Yes
Rule deployment	Deploy to Manager via API	Yes
Match notification	Be alert when there are matches	Yes
Manager Reset	Restart Wazuh after deployment	Yes

Rules Format

```
<group name="threat_intel_hub,{rule_id}">
  <rule id="{rule_id}" level="12">
    <match>{iocs_separados_por_pipe}</match>
    <description>TI Hub: {título_amenaza}</description>
  </rule>
</group>
```

Default level: 12 (High/ Critical)

Location **:** /var/ossec/etc/rules/ti_hub_rules.xml

8. EXPORT FORMATS

Excel (XLSX)

Feature	Specification
Bookshop	openpyxl 3.1.2+
Excel version	Office 2007+ (.xlsx)
Sheets	6 (Malware, APT, Phishing, Attack, Vulnerability, Info)
Columns	Type, Value, Source, Category, Trust, First View, Last View
Format	Tables with headers, autofit columns, freeze panes
Average size	20-100 KB

CSV

Feature	Specification
Delimiter	Comma (,)
Quote char	Double quotation marks (“)
Encoding	UTF-8
Headers	Yes
Columns	type,value ,category,source,confidence,first_seen,last_seen

Palo Alto EDL

Feature	Specification
Format	Text plain (one IOC per line)
Supported types	IP, Domain
Compatible with	PAN-OS 7.0+
Update	Dynamic (API pull)

Fortinet Threat Feed

Feature	Specification
Format	Plain text
Supported types	IP, Domain, URL
Compatible with	FortiGate 5.6+

Snort / Suricata Rules

Feature	Specification
Format	Snort / Suricata rule syntax
Supported types	IP, Domain
Action	alert
Protocol	tcp , udp , icmp
SID range	1000001-1999999

YARA Rules

Feature	Specification
Format	YARA rule syntax
Supported types	Hash (MD5, SHA1, SHA256)
Rule name	ti *hub* { truncated_hash }

STIX 2.1

Feature	Specification
Version	STIX 2.1
Format	JSON
Objects	Bundle , Indicator , Vulnerability , Malware
Relations	indicates , targets
TLP	TLP:AMBER (configurable)

MISP Format

Feature	Specification
MISP version	2.4+
Format	JSON
Object	Event
Attributes	IOCs as attributes
Categories	Network activity, Payload delivery, Artifacts dropped

9. CLI COMMANDS

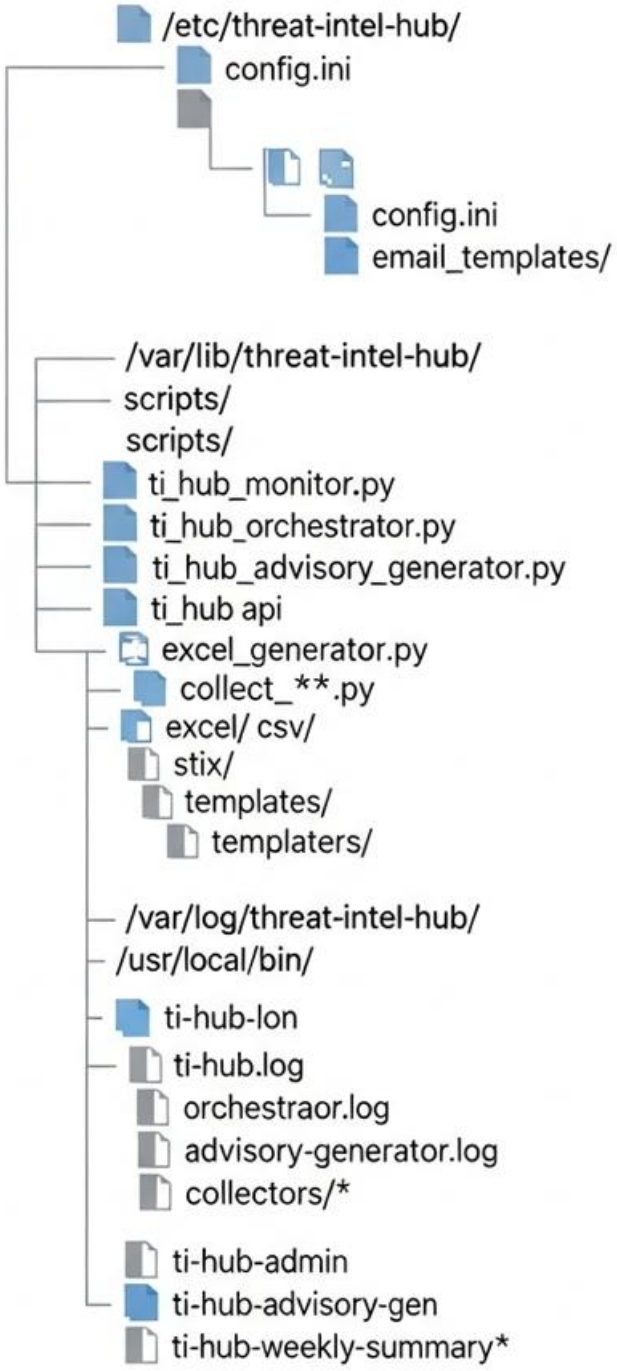
Main Commands

Command	Description	It requires sweat
ti- hub -status	System status update	No
ti- hub - admin status	Detailed status with metrics	No
ti- hub - admin start	Start all services	Yes
ti- hub - admin restart	Restart services	Yes
ti- hub - admin stop	Stop services	Yes
ti -hub-admin init -data	Load initial data	Yes
ti- hub - admin logs	View latest logs	No
ti- hub - advisory -gen	Generate advisories	Yes
ti- hub - weekly-summary	Generate weekly summary	Yes
ti- hub -test- sources	Test data sources	Yes

Collectors Manuals

Command	Sources	It requires sweat
ti- hub - collect - phishing	OpenPhish , PhishTank	Yes
ti- hub - collect -malware	URLhaus , Spamhaus , Cybercrime	Yes
ti- hub - collect-apt	APTnotes , Talos	Yes

10. DIRECTORY STRUCTURE



11. CONFIGURATION PARAMETERS

database

Parameter	Type	Default value	Description
host	string	localhost	MySQL Host
port	int	3306	MySQL port
database	string	threat_intel_hub	Database Name
user	string	ti_hub_user	Database User
password	string	auto-generated	Password BD

triggers

Parameter	Type	Default value	Description
kev_enabled	bool	true	Enable KEV monitoring
kev_check_minutes	int	30	KEV check interval
epss_enabled	bool	true	Enable EPSS tracking
epss_spike_threshold	float	0.2	EPSS spike threshold
epss_check_hours	int	4	EPSS check interval

e-mail

Parameter	Type	Default value	Description
enabled	bool	true	Enable emails
smtp_server	string	-	SMTP Server
smtp_port	int	587	SMTP Port
sender_email	string	-	Sender email
sender_password	string	-	Password email
recipient_email	string	-	Destination emails (CSV)
use_tls	bool	true	Use TLS
attach_excel	bool	true	Attach Excel file

advisory

Parameter	Type	Default value	Description
enabled	bool	true	Enable advisories
schedule	string	thrice	Frequency (thrice / daily)
cron_expression	string	0 8,14,20 *	Chronological expression
analysis_days	int	7	Days ago
individual_mode	bool	true	1 email = 1 alert

API

Parameter	Type	Default value	Description
enabled	bool	true	Enable API
host	string	0.0.0.0	Host bind
port	int	8080	API Port
cors_enabled	bool	true	Enable CORS
rate_limit	int	100	Req limit /min

12. PERFORMANCE METRICS

Capabilities

Metrics	Worth
IOC Processing	1,000+ per minute
Alerts generated/day	10-50 (average)
Emails sent/day	3-15 (advisories) + 1 (weekly)
API requests per second	100+
API response time	<100ms (average)
Uptime	99.9%

Storage

Data Type	Estimated Growth
Database	100-500 MB/month
Excel files	50-200 MB/month
Logs	100-300 MB/month
Backups	200-500 MB/month
Total	450-1,500 MB/month

Retention recommended :

- Logs: 90 days
- files : 1 year
- Database: Indefinite (with archiving)

13. SECURITY

Security Features

Feature	State
Sensitive encrypted data	Yes (passwords in config.ini)
TLS/SSL	Supported
API Authentication	Optional (JWT on roadmap)
Rate limiting	Yes (configurable)
Input validation	Yes
SQL injection protection	Yes (prepared) statements)
XSS protection	Yes (escaped templates)
Audit logs	Yes

Compliance

Framework	Compatible
CMMC 2.0	☑ Level 1-2
ISO 27001	☑
PCI-DSS	☑ Login requirements
NIST CSF	☑ Detect , Respond
SOC 2	☑ Partial

14. UPDATES AND MAINTENANCE

Updates

Type	Frequency	Requires downtime
Security patches	As needed	Minimum (1-2 min)
Minor updates	Monthly	Yes (5-10 min)
Major updates	Quarterly	Yes (15-30 min)

Maintenance Tasks

Task	Frequency	Automatic
Log cleanup	Weekly	Yes (logrotate)
Database backup	Diary	Configurable
Database Optimization	Monthly	No
Storage review	Monthly	No
Source update	Continuous	Yes

15. TECHNICAL SUPPORT

Support Channels

Channel	Availability	Response Time
E-mail	24/7	24-48 hours
Phone	Mon-Fri 9AM-6PM	Immediate
WhatsApp	Mon-Fri 9AM-6PM	<4 hours
Web Portal	24/7	24-48 hours

SLA (Service) Level Agreement)

Priority	Description	Response Time	Resolution Time
P1 - Critique	System down	1 hour	4 hours
P2 - High	Major functionality not available	4 hours	24 hours
P3 - Media	Minor functionality affected	8 hours	72 hours
P4 - Low	Question or improvement	24 hours	Best effort

16. DOCUMENTATION

Included Documents

Document	Pages	Format
Installation Manual	25	PDF/MD
Setup Guide	30	PDF/MD
API documentation	40	PDF/MD
Troubleshooting Guide	20	PDF/MD
Best Practices	15	PDF/MD
Use Cases	10	PDF/MD

17. COMPLIANCE AND CERTIFICATIONS

Standard	Version	State
Python PEP 8	-	☑ Complies
OWASP Top 10	2021	☑ Mitigated
CWE Top 25	2023	☑ Mitigated
STIX	2.1	☑ Compatible
OpenAPI	3.0	🔄 On roadmap

18. ROADMAP

v2.6 (Q1 2026)

- JWT Authentication in API
- Interactive web dashboard
- Support for TAXII 2.1
- Splunk integration

v2.7 (Q2 2026)

- IOC classification
- Multi-language support
- Mobile app (iOS/Android)
- Integration with ServiceNow

v3.0 (Q3 2026)

- Distributed architecture
- High Availability (HA)
- Multi-tenancy
- Kubernetes deployment