PostecH

THREAT INTEL HUB

BROCHURE

POSTECH.US

THREAT INTEL HUB

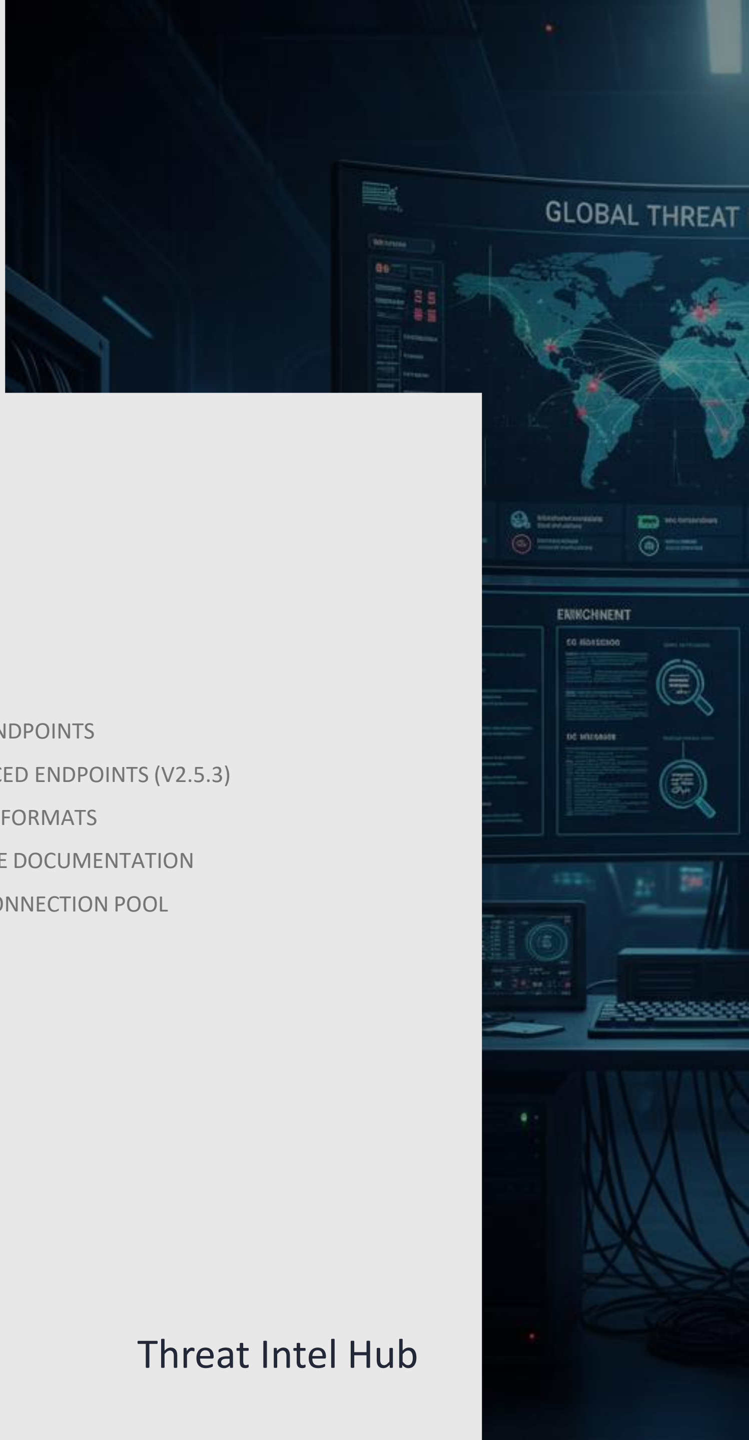
Threat Intel Hub (TI Hub) is a comprehensive cyber threat intelligence platform that automates the collection, enrichment, correlation, and distribution of security information from multiple global sources. The solution is designed for Security Operations Centers (SOCs) and incident response teams that require actionable, real-time intelligence.

COMPREHENSIVE CYBER THREAT INTELLIGENCE PLATFORM
AUTOMFED COLLECTION & ENRICHMENT
Indisators of Compasbee (OO)
Threat Astrs
CORELLATION ENGNE

VALUE PROPOSITION

- Complete automation
- Integrated intelligence sources
- Native SIEM integration
- Multi-level
- Full REST API
- Multi-format export

FEATURES



COLLECTION MODULE

- ✓ INTEGRATION WITH 15+ INTELLIGENCE SOURCES
- ✓ SPECIALIZED COLLECTORS (PHISHING, MALWARE, APT)
- ✓ CONTINUOUS 24/7 MONITORING
- ✓ AUTOMATIC DATA DEDUPLICATION
- ✓ RATE MANAGEMENT LIMITS AND ERRORS

ENRICHMENT MODULE

- ✓ ALIENVAULT OTX INTEGRATION
- ✓ VIRUSTOTAL
- ✓ MISP INTEGRATION (OPTIONAL)
- ✓ AUTOMATIC CATEGORIZATION OF IoCs
- ✓ EPSS PROBABILITY ANALYSIS

CORRELATION MODULE

- ✓ WAZUH SIEM INTEGRATION
- ✓ AUTOMATIC SEARCH IN LOGS (7 DAYS)
- ✓ CUSTOM RULE GENERATION
- ✓ AUTO-DEPLOY OF RULES
- ✓ MATCH NOTIFICATION

DISTRIBUTION MODULE

- ✓ ADVISORIES (HTML + EXCEL)
- ✓ WEEKLY SUMMARY WITH CHARTS
- ✓ 4 TYPES OF NOTIFICATION
- ✓ TEMPLATE CUSTOMIZATION
- ✓ MULTIPLE RECIPIENTS

REST API

- ✓ 9 BASIC ENDPOINTS
- ✓ 7 ADVANCED ENDPOINTS (V2.5.3)
- ✓ 8 EXPORT FORMATS
- ✓ COMPLETE DOCUMENTATION
- ✓ MYSQL CONNECTION POOL

ADMINISTRATIVE COMMANDS

- ✓ 12+ CLI COMMANDS
- ✓ SERVICE MANAGEMENT
- ✓ SOURCE TESTING
- ✓ MANUAL GENERATION OF REPORTS
- ✓ CENTRALIZED LOGS

DATABASE

- ✓ MYSQL 8.0+ OPTIMIZED
- ✓ 5 MAIN TABLES
- ✓ OPTIMIZED INDICES
- ✓ STORED PROCEDURES
- ✓ AUTOMATIC BACKUPS

KEY BENEFITS

80%

REDUCTION IN ANALYSIS TIME

$108K

ESTIMATED ANNUAL SAVINGS

15+

INTEGRATED SOURCES ON A PLATFORM

<24

HOURS FOR FULL IMPLEMENTATION

99.9%

TARGET UPTIME

THANK YOU

sales@postech.us