Technical specifications
CTH

Comprehensive Cybersecurity MDR Platform

Product:	Cyber Threat Hunter
Document version:	1.0.0
Document Type:	Technical Specifications
Date of preparation:	September 1, 2025
Author:	Postech

TECHNICAL SPECIFICATIONS

Managed Platform Detection and Response (MDR)

Product:	Cyber Threat Hunter (CTH)
Product version:	1.1
Document Type:	Technical Specifications
Date:	August 11, 2025
Classification:	Commercial
Contact:	sales@postech.us

Table of Contents

1. General Product Information

1.1 Solution Identification

Attribute	Specification
Product Name	Cyber Threat Hunter (CTH)
Current Version	0.02
Manufacturer	Postech
Solution Type	Managed Detection and Response (MDR) / SIEM
Website	www.postech.us
System ID	7987456321

1.2 General Description

Cyber Threat Hunter (CTH) is a comprehensive Managed platform Detection and Response (MDR) that combines advanced SIEM, SOAR, Threat Intelligence and User capabilities Behavior Analytics in a unified solution. Designed to provide real-time detection, analysis, and response to cyber threats, CTH enables organizations to significantly enhance their security posture without the need to build and maintain a full in-house SOC.

The platform integrates multiple analytics engines including event correlation, behavioral analysis (UEBA), machine learning , and threat analysis . intelligence from more than 209,000 active indicators of compromise (IOCs), providing a defense in depth against known and unknown threats.

1.3 Problem it Solves

Alert Overload: Reduce alert fatigue through automated triage and intelligent prioritization based on context and asset criticality.

Talent Shortage: Provides access to a team of specialized analysts 24/7 without the need for internal recruitment and retention of staff.

Response Time: Automates containment actions to reduce MTTR from hours to minutes.

Fragmented Visibility: Unifies data from multiple security sources into a consolidated view.

1.4 Value Proposition

Covered Safety Pillars

Pillar	Coverage	Mechanisms
Confidentiality	High	TLS 1.2+ encryption, AES-256, RBAC access control, MFA
Integrity	High	Log validation, checksums , change auditing
Availability	High	High-performance architecture, 24/7 monitoring, 99.9% SLA

Main Benefits

KEY BENEFITS
✓ 80% reduction in initial research time
✓ Automated threat containment in less than 5 minutes
✓ SLA compliance exceeding 99%
✓ Unified visibility of the entire security infrastructure
✓ Access to a team of specialized analysts 24/7/365
✓ Significant reduction in the total cost of operation of the SOC
✓ Automatic mapping to MITER ATT&CK, NIST, ISO 27001 frameworks

2. Main Features

2.1 Real-Time Monitoring

CTH provides continuous 24/7/365 monitoring of the client's IT infrastructure, including networks, servers, endpoints , applications, and cloud services. Monitoring is performed by the SOC team, supported by intelligent automation.

Ability	Description
Asset Coverage	Servers (Windows/Linux), endpoints, firewalls, switches, applications , cloud
Polling Frequency	Real-time (streaming) + polling every 5 minutes for reconciliation
Monitored Metrics	Security events, performance, availability, user behavior
Dashboards	Executive (high level) and Operational (technical detail)
Real-Time Alerts	Immediate severity notifications via email, SMS, webhook

2.2 Threat Detection

CTH uses multiple detection engines that work together to identify known and unknown threats:

Engine	Technology	Coverage
Correlation of Events	SIGMA rules, multi-source correlation	Known attack patterns, TTPs
Threat Intelligence	209,565+ active IOCs from 12+ sources	IPs , domains, hashes, URLs
UEBA	Behavioral analysis with ML	Internal threats, compromised accounts
Machine Learning	Supervised and unsupervised models	DGA, exfiltration, lateral movement
Signatures	Database updated daily	Known malware, exploits , vulnerabilities

Types of Threats Detected

COVERED THREATS
✓ Ransomware and advanced malware
✓ Phishing and spear-phishing
✓ **Brute force and** credential attacks stuffing
✓ Lateral movement and privilege escalation
✓ Data exfiltration
✓ Internal threats (insider) threats)
✓ Communication with C2 (Command & Control)
✓ Exploitation of known vulnerabilities (CVE)
✓ DDoS and Denial of Service attacks

2.3 Log and Event Management

CTH collects, normalizes, enriches, and stores security events from multiple sources, providing a unified view for forensic analysis and incident investigation.

Feature	Specification
Supported Sources	Firewalls, IDS/IPS, EDR, AD, servers, applications, cloud , databases
Ingestion Protocols	Syslog (UDP/TCP/TLS), REST API, Beats, Kafka, webhooks
Standardization	parsing with support for CEF, LEEF, JSON, and XML formats
Enrichment	GeoIP , threat intelligence , asset context, user information
Retention	Configurable: 30, 90, 180, 365 days according to compliance requirements
Search	Elasticsearch engine with real-time queries and historical search
Volume	Scalable according to needs (from 1 GB/day to 100+ TB/day)

2.4 Alerts and Reports

Alert System

The MDR features an advanced alert generation and management engine that continuously identifies, correlates, and prioritizes security events. Alerts are automatically classified according to their severity level (low, medium, high, and critical), taking into account the context, potential impact, and risk to the client. Response and escalation times are dynamically adjusted according to defined SLAs, ensuring timely attention in line with established commitments. The platform also supports multiple notification channels, such as email, client portals, ticketing system integrations , and other communication mechanisms, ensuring that relevant alerts reach the responsible teams immediately and effectively.

Severity	Validation Time	Response Time	Notification Channels
Critical	15 minutes	Immediate (Automatic)	Email, SMS, Call, Webhook
High	30 minutes	< 1 hour	Email, SMS, Webhook
Medium	60 minutes	< 4 hours	Email, Webhook
Low	4 hours	< 24 hours	Email, Dashboard

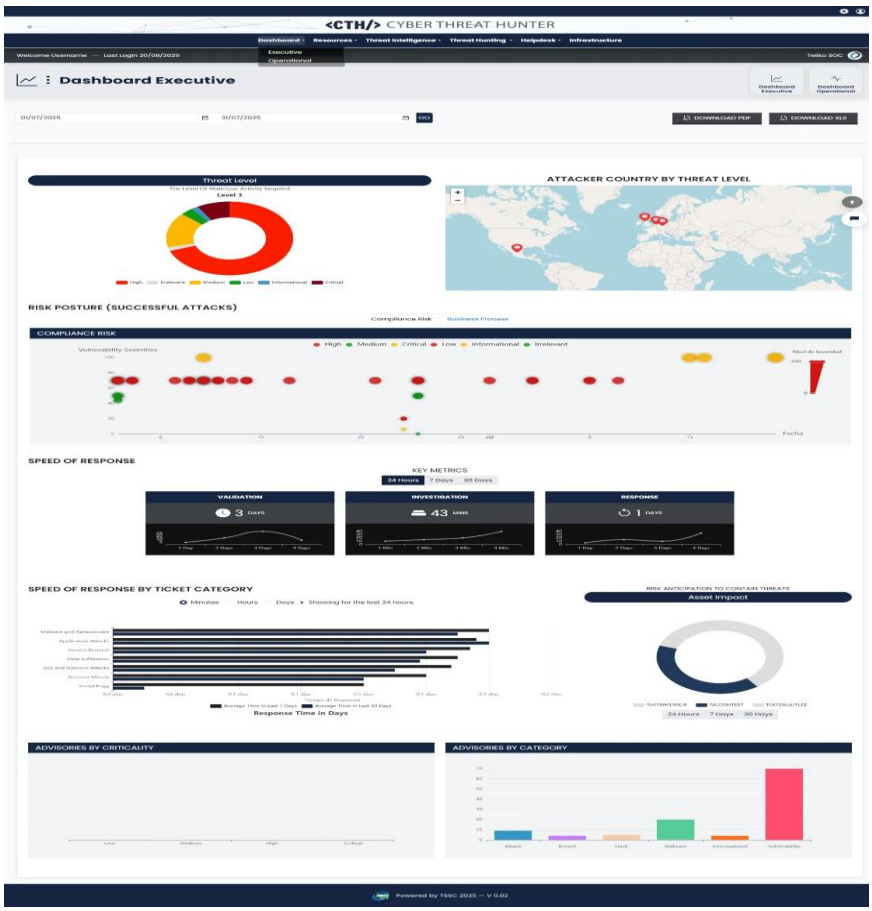
Available Reports

CTH offers advanced custom reporting capabilities that allow reports to be tailored to each client's specific monitoring requirements. The platform enables the definition of reports based on business-relevant metrics, events, and cases, prioritizing critical information and filtering out operational noise. Reports can be configured for specific time periods and present detailed data on alerts, incidents, response times, containment actions, and investigations, aligned with the client's objectives and risks. This ensures clear and actionable visibility into the security status, facilitates informed decision-making, and allows for a precise demonstration of the value and performance of the MDR service.

Report	Frequency	Content
Monthly Executive	Monthly	KPIs, trends, strategic recommendations
Weekly Operational	Weekly	Incidents, response times, exceptions, SLA
Compliance	on demand	Mapping to ISO 27001, NIST CSF, PCI-DSS
Threat Intelligence	Diary	IOCs , active campaigns, advisories
Vulnerabilities	Weekly	CVEs detected, prioritization, remediation

2.5 Visualization (Dashboard)

CTH provides interactive dashboards designed for different audiences and operational needs:



Dashboard	Audience	Key Metrics
Executive	CISO, CIO, Management	Threat level, risk posture, SLA compliance, trends
Operational	SOC Analysts	Active alerts, tickets, investigations, events by source
Threat Intelligence	Threat Hunters	Active IOCs , matches , advisories , impacted assets

Vulnerabilities	Safety Equipment	CVEs by severity, affected assets, remediation
Helpdesk	Service Desk	Open tickets, SLA compliance , response times

3. Technical Requirements and Architecture

3.1 Deployment Platform

Model	Description	Use Case
On -Premise	Complete installation on customer's infrastructure	Maximum data sovereignty, strict regulations
Private Cloud	Deployment in the customer's dedicated cloud	Scalability with data control
Hybrid	Sensitive data on -premises, cloud processing	Balance between control and flexibility
SaaS (Roadmap)	Service fully managed by Postech	Organizations without dedicated infrastructure

3.2 System Requirements

Server (All-in-One)

Component	Minimum	Recommended	Enterprise
CPU	8 cores	16 cores	32+ cores
RAM	32 GB	64 GB	128+ GB
Storage	500 GB SSD	2 TB NVMe	10+ TB NVMe RAID
Grid	1 Gbps	10 Gbps	10 Gbps redundant
Operating System	Ubuntu 22.04 LTS	Ubuntu 24.04 LTS	Ubuntu 24.04 LTS
Events/Second	Up to 1,000 EPS	Up to 10,000 EPS	50,000+ EPS

Database

Component	Specification
Main Engine	PostgreSQL 14+ / MariaDB 10.6+
Search Engine	Elasticsearch 8.x
Cache	Redis 7.x
Message Queue	RabbitMQ 3.12+
Storage Required	Minimum 1 TB for 90-day retention (variable depending on volume)

3.3 Compatibility

Supported Operating Systems (Data Sources)

Operating System	Versions
Windows Server	2016, 2019, 2022
Windows Desktop	10, 11
Linux (RHEL/CentOS)	7, 8, 9
Linux (Ubuntu)	20.04 LTS, 22.04 LTS, 24.04 LTS
Linux (Debian)	10, 11, 12
macOS	11 (Big Sur) and later

Network and Security Devices

Category	Supported Manufacturers/Products
Firewalls	Palo Alto Networks, Fortinet, Check Point, Cisco ASA/Firepower, pfSense
EDR/XDR	CrowdStrike Falcon, Microsoft Defender, SentinelOne , Cytomic EPDR, Cortex XDR
IDS/IPS	Snort, Suricata, Cisco IPS, Palo Alto Threat Prevention
Switches/ Routers	Cisco, Juniper, Arista, HP/Aruba
WAF	Imperva, Cloudflare, AWS WAF, F5
Cloud	AWS (CloudTrail, GuardDuty), Azure (Sentinel), GCP (Security Command Center)
ITSM	ServiceNow , Jira Service Management

3.4 High-Level Architecture

CTH's architecture follows a layered model that guarantees scalability, modularity, and high availability:

Layer	Components	Function
Intake	Collectors, Beats, Syslog , APIs	Data reception and standardization
Prosecution	Correlation, UEBA, ML, TI Engine	Threat analysis and detection
Storage	PostgreSQL, Elasticsearch , Redis	Data persistence and search
Orchestration	RabbitMQ , Workers , Playbooks	Response automation
Presentation	React Dashboard , REST API	User interface and integrations
Management	Docker/K8s, Monitoring , Backup	Operation and maintenance

4. Security and Compliance

4.1 Certifications and Frameworks

CTH is designed to facilitate compliance with key regulatory frameworks and industry standards:

Certification/Framework	State	Coverage
ISO 27001	Compatible	Information security control mapping
NIST Cybersecurity Framework	Compatible	Functions : Identify, Protect, Detect, Respond, Recover
MITRE ATT&CK	Integrated	Mapping of TTPs in detections and advisories
PCI-DSS	Compatible	Logging , monitoring, and incident response requirements
GDPR	Compatible	Personal data protection, breach notification
LFPDPPP (Mexico)	Compatible	Compliance with personal data protection
SOC 2 Type II	In progress	Security, availability and confidentiality controls

4.2 Platform Protection

Data Encryption

Guy	Algorithm	Application
In transit	TLS 1.2 / TLS 1.3	All communications between components and with users
At Rest	AES-256	Database, stored logs, backups
Credentials	Argon2 / bcrypt	User passwords and service accounts
API Keys	SHA-256 HMAC	Integration authentication tokens

Access Control

Mechanism	Description
RBAC	Role-based access control (Administrator , Manager, TMDR, Engineer, Analyst)
MFA	Multi-factor authentication is mandatory for administrative access
SSO	Integration with identity providers (SAML 2.0, OAuth 2.0, LDAP/AD)
Audit	Complete record of all user actions
Sessions	Configurable timeout, session invalidation, concurrent session control

Infrastructure Security

SECURITY CONTROLS
✓ Operating system hardening according to CIS Benchmarks
✓ Host firewall with rules restrictive (deny by default)
✓ Automated security updates
✓ Periodic vulnerability scanning of the platform
✓ Network segregation for critical components
✓ Encrypted backups with integrity verification
✓ File Integrity Monitoring (FIM)
✓ Immutable audit logs

5. Support and Services

5.1 Support Model

Level	Availability	Response Time	Channels
Critical (P1)	24/7/365	15 minutes	Phone, Email, WhatsApp
High (P2)	24/7/365	1 hour	Phone, Email, WhatsApp
Medium (P3)	Monday to Friday 8-20h	4 hours	Email, Portal
Low (P4)	Monday to Friday 9am-6pm	24 hours	Email, Portal

5.2 Included Services

MDR SERVICES INCLUDED
✓ 24/7/365 monitoring by specialized analysts
✓ Triage and validation of alerts
✓ Security incident investigation
✓ Automated threat containment
✓ Proactive threat hunting
✓ Executive and operational reports
✓ Technical support for the platform
✓ Rule and threat updates intelligence
✓ Quarterly security reviews

5.3 Licensing Model

Model	Calculation Basis	Includes
By Assets	Number of monitored endpoints /servers	Agents, monitoring, response
By Volume	GB/day of ingested logs	Storage, processing, retention
Per User	Users with access to the platform	Console licenses, dashboards
Enterprise	All-inclusive package (assets + unlimited volume)	All-inclusive + premium services

The licensing is annual with options for monthly or annual prepayment.

5.4 Guaranteed SLAs

CTH incorporates advanced and flexible SLA management tailored to each client's specific needs, allowing administrators to define and configure service level agreements centrally. These SLAs are applied across the entire system and govern the operational behavior of alerts, automated containment, investigations, and other processes subject to response times and priorities. The platform dynamically adjusts thresholds, escalations, and action windows based on the configured SLAs and continuously monitors compliance, providing real-time visibility, traceability, and performance metrics. This ensures operational consistency, alignment with contractual commitments, and effective control over the quality of service delivered.

Metrics	Aim	Penalty for Non-Compliance
Platform Availability	99.9%	Proportional service credits
Alert Validation Time	According to severity (15-240 min)	Contract extension
Time of Containment	Automatic / < 30 min	Account review
SLA Compliance General	> 99%	Renewal discounts

6. Use Cases

6.1 Ransomware Detection and Containment

Scenery

An employee opens an email attachment containing a ransomware dropper . The malware initiates reconnaissance processes, disables backup services , and begins encrypting files.

CTH detection

Indicator	Detection Motor	Action
Obfuscated PowerShell running	Correlation + EDR	HIGH alert generated
DGA domain connection (algorithmic)	Threat Intelligence + ML	CRITICAL ALERT
Attempt to stop Volume Shadow Copy	SIGMA Correlation	Automatic scaling
Mass file encryption	UEBA (anomalous behavior)	Playbook Trigger

Automated Response

1. Isolation: The infected endpoint is isolated from the network in less than 30 seconds.

2. C2 Blocking: C2 IPs and domains are blocked at the perimeter firewall .

3. Snapshot : A snapshot of critical systems is triggered for recovery.

4. Notification: Response team notified with complete initial analysis.

Result

Containment in under 5 minutes. Impact limited to one endpoint . No data loss thanks to snapshots . Forensic investigation completed in 4 hours with initial vector identification.

6.2 Targeted Phishing Detection

Scenery

A spear-phishing campaign targeting executives of the organization uses lookalike domains to steal corporate credentials.

CTH detection

Threat Intelligence : Domain identified as lookalike registered 48 hours ago.

Correlation: Multiple users accessing the same suspicious domain.

UEBA: Anomalous login patterns from unusual locations post-visit .

Answer

Blocking the malicious domain, forced reset of credentials of affected users, analysis of compromised accounts, notification to users with additional training.

6.3 Unauthorized Access Detection

Scenery

An attacker uses credentials stolen from a third-party breach to attempt to access corporate systems.

CTH detection

UEBA: Login from a geographical location never before seen by the user.

Correlation: Multiple failed attempts followed by successful access.

Threat Intelligence : Source IP associated with commercial VPN used by malicious actors.

Answer

Session terminated immediately, account blocked, alert to legitimate user, activity analysis during access, credentials reset and MFA enabled.

6.4 Insider Threat

Scenery
An employee with privileged access downloads large volumes of confidential information before his planned resignation.

CTH detection

UEBA: Download volume 500% higher than the user's baseline .

DLP Integration : Detection of classified files being copied to USB.

Correlation: Access to systems outside of normal working hours.

Answer

Silent alert to security team (without notifying the employee), complete forensic documentation, coordination with HR and Legal, preservation of evidence for possible legal action.

Specifications Summary

Category	Specification
Product	Cyber Threat Hunter (CTH) v0.02
Guy	Managed Detection and Response (MDR) / SIEM
Manufacturer	Postech
Deployment	On -Premise, Private Cloud, Hybrid
Active IOCs	209,565+
IT Sources	12+ (OTX, CISA, SANS, Talos, etc.)
Detection	Correlation, UEBA, ML, Threat Intelligence , Firms
Minimum Requirements	8 cores, 32 GB RAM, 500 GB SSD
Server OS	Ubuntu 22.04/24.04 LTS
Integrations	EDR, Firewalls, SIEM, Cloud, ITSM
Encryption	TLS 1.2+, AES-256
Authentication	RBAC, MFA, SSO (SAML/OAuth/LDAP)
Frameworks	ISO 27001, NIST CSF, MITER ATT&CK, PCI-DSS
SLA Availability	99.9%
SLA Compliance	> 99%
Medium	24/7 (P1/P2), Email, Phone , WhatsApp
Discharge	By assets, volume, users, or Enterprise

For more information: www.postech.us