PostecH

www.postech.us

Brochure

<CTH/>

CYBER THREAT HUNTER

Managed Platform Detection and Response (MDR) developed by
Postech Cyber Security Solutions

SIEM, SOAR, and Threat capabilities **Intelligence and User Behavior Analytics** for the detection, analysis and response to cyber threats in real time.

Version: 0.02

WHY CTH?

Why implement CTH in your organization?

cyber threat landscape is constantly evolving, confronting organizations with increasingly sophisticated attacks such as ransomware , advanced persistent threats (APTs), vulnerability exploitation, and insider threats.

CTH was designed to address these challenges through a unified platform that integrates multiple data sources and automates incident response.

CTH helps solve:

Alert overload and false positives

Reduction of false positives through automated triage and intelligent correlation.

Long response times to incidents

Automated threat containment in minutes instead of hours.

Lack of unified visibility

Consolidation of data from multiple tools into a single, comprehensive view.

Shortage of specialized talent

Access to expert analysts 24/7 without the need to build an internal SOC.

Silo safety tools

Open integration with EDR, firewalls, SIEM, cloud , and ITSM on a unified platform.

VALUE PROPOSITION:

CTH offers a differentiated value proposition as an MDR solution for companies and organizations:

Advanced Threat Detection

It uses multiple analysis engines: event correlation, UEBA, machine learning and threat intelligence to identify sophisticated threats that evade traditional defenses.

Automated Response

It implements playbooks that allow threats to be contained in seconds, reducing response time (MTTR) and minimizing the impact of incidents.

Unified Visibility

Consolidates information from multiple security sources into executive and operational

Regulatory Compliance

It facilitates compliance with regulatory frameworks such as ISO 27001, NIST CSF and MITRE ATT&CK through automated reporting.

24/7 Operation

Continuous monitoring supported by the team of analysts

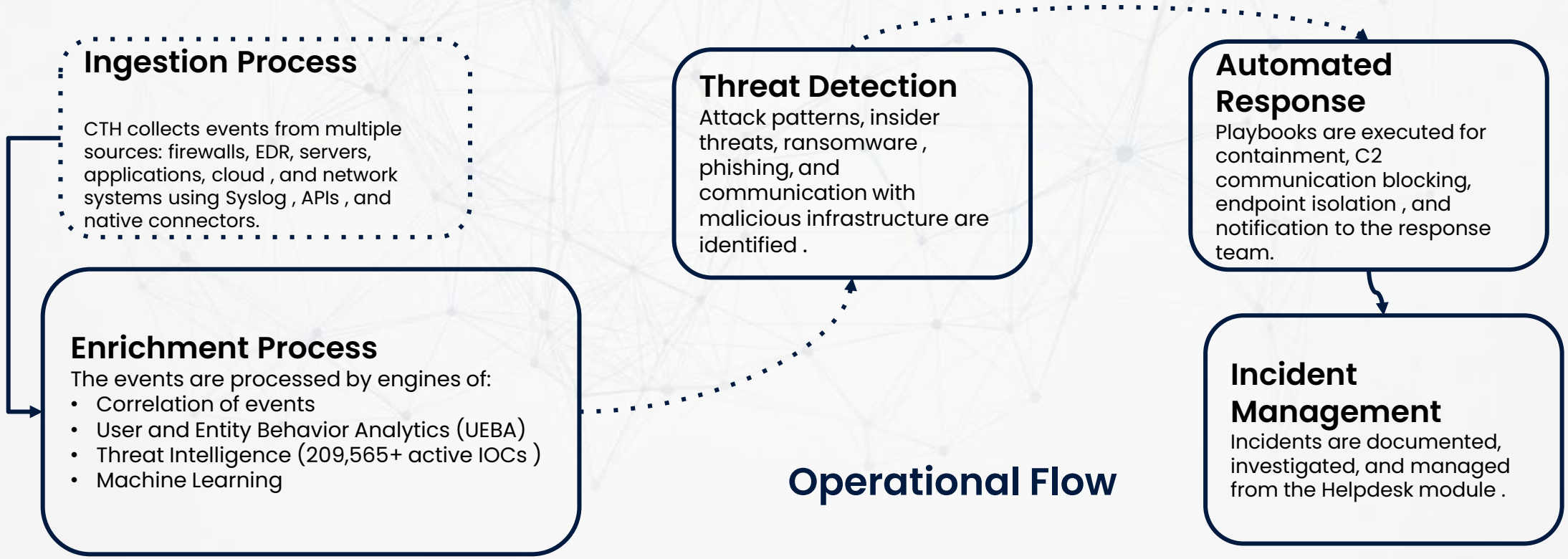
Key Benefits:

- Automated threat containment in less than 5 minutes
- 80% reduction in initial research time
- compliance exceeding 99%
- Significant reduction in the total cost of operation of the SOC

General Architecture

CTH is deployed as a solution:

- On -Premise
- Private Cloud
- Hybrid



MAIN MODULES AND CLOSING

Dashboard
Executive and operational visualizations of the security status.

Resources:
Integrated asset management and data sources.

Threat Threat Intelligence Center with **active** advisories and IOCs .

Threat Hunting:
Proactive threat hunting and vulnerability management.

Helpdesk
Incident lifecycle management: investigations, tickets and SLA metrics.

Settings:
SLA configuration , users and profiles.

<CTH/>

CYBER THREAT HUNTER

THANK YOU

sales@postech.us