



HawkEye CTI

powered by DTS Solution

Hunting Cyber Adversaries

The Cyber Threat Intelligence (CTI) lifecycle is a structured approach used to collect, analyze, and disseminate intelligence that can be used to enhance an organization's cybersecurity posture. This cyclical process helps organizations proactively defend against cyber threats by providing timely, relevant, and actionable insights.

Planning

The process begins with identifying intelligence requirements, setting objectives, and defining the scope of information needed.

Collection

During the Collection phase, data is gathered from various sources, such as threat feeds, OSINT, dark web monitoring, and internal telemetry.

Feedback

The Feedback phase refines the CTI process by evaluating its effectiveness and adjusting for evolving threats.

Processing

The Processing phase refines the CTI process by evaluating its effectiveness and adjusting for evolving threats.



Dissemination

Dissemination ensures that actionable intelligence is shared with relevant stakeholders in a timely and usable format.

Analysis

In the Analysis stage, experts assess the processed information to identify patterns, adversarial tactics, techniques, and procedures (TTPs), and assess potential threats to the organization.

Cyber Threat Intelligence Lifecycle

Planning

- **Define Intelligence Objectives**

Align CTI goals with each client's security needs by identifying critical assets, threats, and risk tolerance.

- **Assess Client-Specific Requirements**

Tailor intelligence efforts to industry, regional, and compliance needs to ensure relevance and support regulatory obligations.

- **Set Collection Priorities**

Focus intelligence collection on key threats, vulnerabilities, and technology stacks used by clients.

- **Allocate Resources Effectively**

Distribute tools, personnel, and analysis efforts based on client-specific threat levels and priorities.

- **Establish Communication Channels**

Develop protocols to ensure timely intelligence sharing, enabling clients to act on high-priority threats.

- **Structure Intelligence Goals**

Deliver actionable, customized insights that improve each client's security posture and adapt to emerging threats.

Collection

- **MISP Integration**

Aggregates data from 72 threat feeds, amassing around 60 million IOCs to provide a broad intelligence base.

- **Supplementary Data Sources**

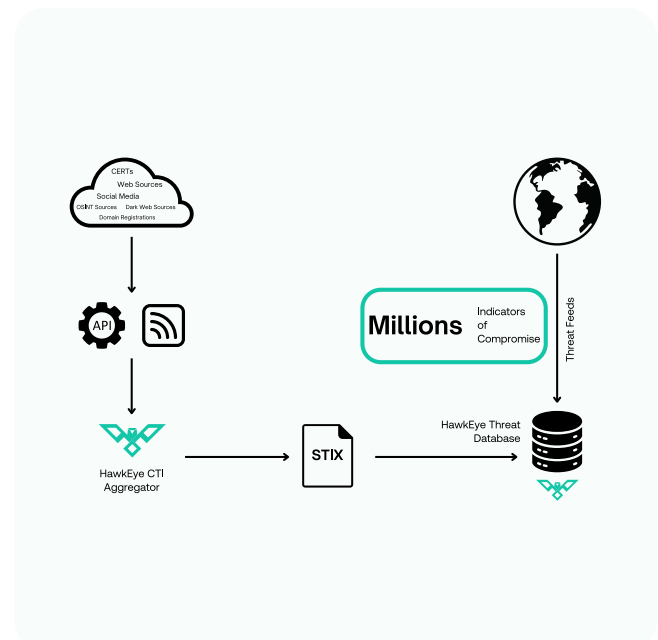
Includes advisories from UAE CSC and KSA NCA CERT, along with 100+ RSS feeds from technology and cybersecurity publications.

- **Social Media API Feeds**

Monitors key Twitter handles and Telegram channels for real-time threat intelligence and emerging trends.

- **Domain Registrations**

Monitors Domain Registrations to identify impersonation domains at early stages.



Processing

- **Customer-Specific Threat Actor Targeting**
Filter for threats from actors specifically focused on individual customers.
- **Industry-Specific Threats**
Identify threat actors targeting industries relevant to each customer.
- **Geolocation-Based Targeting**
Prioritize threats based on regions where customers operate.
- **Vulnerability Filtering**
Focus on vulnerabilities affecting technologies actively used by customers.
- **Exploit Detection**
Highlight exploits involving critical technologies within the customer's environment.
- **Impersonation Domain Checks**
Monitor for domains registered with potential customer brand impersonation, including website content.
- **Data Leaks & Compromise Monitoring**
Detect data breaches or compromises associated with customers or relevant third parties.
- **Alert Refinement**
Deduplicate and Fine tune alerts based on false positives to reduce alert fatigue.

Analysis

CTI Enrichment

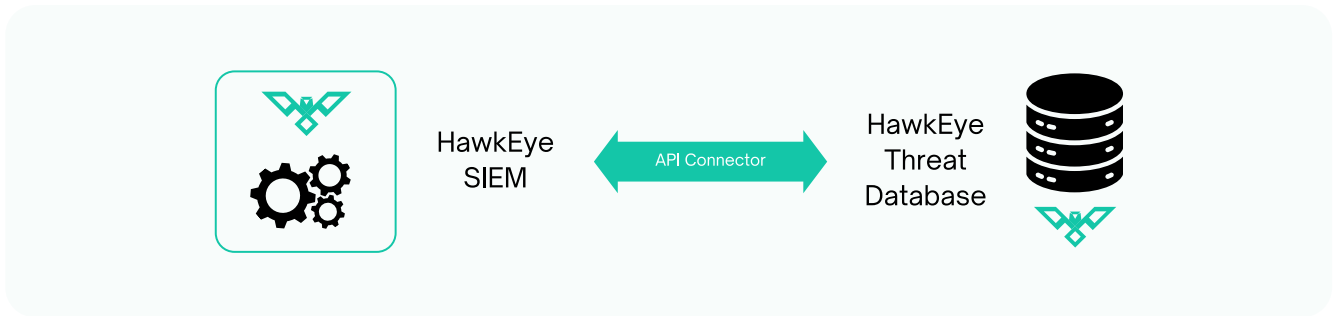
- **Threat Actor Profiling**
Evaluate and categorize threat actors based on tactics, techniques, and procedures (TTPs) to understand their methods, capabilities, and objectives. This helps in identifying potential risks specific to each customer.
- **Trend Analysis**
Examine intelligence for emerging trends, such as new attack vectors, malware variants, or shifts in threat actor behavior. By recognizing these patterns, customers can stay proactive against evolving threats.
- **Attack Surface Assessment**
Map out potential vulnerabilities and points of exposure in customer environments. By analyzing this information, tailored defenses can be suggested to harden key assets.
- **Risk Scoring and Prioritization**
Assign risk scores to analyzed threats based on factors like severity, likelihood, and potential impact on the customer. This helps prioritize response efforts based on the highest-risk threats.

Threat Hunting

- **Analyst Driven Threat Hunt**
Threat hunting based on Tactics, Techniques, and Procedures (TTPs) involves proactively searching for signs of adversarial activity by focusing on known methods and behaviors used by threat actors.

By analyzing TTPs outlined in frameworks like MITRE ATT&CK, threat hunters can identify patterns that suggest ongoing or past compromise within a network.
- **Automated Threat Hunt**
Automated threat hunting streamlines the process of identifying potential threats by continuously scanning artifacts like IP addresses, file hashes, domain names, and email domains against the HawkEye Threat Database.

Using automation, these artifacts are cross-checked against Indicators of Compromise (IOCs) collected from various intelligence sources, ensuring swift detection of any matches that could indicate malicious activity.



Dissemination

- **Dissemination Channels**

Intelligence is shared either through SOC incidents for immediate threats or daily advisories for ongoing awareness, based on the assessed impact.

- **Severity Tagging**

Each alert or advisory is tagged with a severity level, helping recipients understand the potential impact and prioritize response accordingly.

- **TLP Classification**

Alerts are tagged with TLP levels (White, Green, Amber, Red) to indicate the sensitivity and sharing restrictions, ensuring controlled distribution based on information sensitivity.

Feedback


CTI alerts disseminated to customers are regularly reviewed in weekly meetings. These sessions provide an opportunity to discuss recent alerts, assess the relevance and effectiveness of the intelligence provided, and adjust priorities or response strategies based on customer feedback. This collaborative approach ensures that CTI efforts are aligned with the evolving threat landscape and the customer's specific security needs, enhancing the overall value of the intelligence service.



HAWKEYE

HUNTING CYBER ADVERSARIES

 www.hawk-eye.io

 +971 4 338 3365

 hawkeye@dts-solution.com
