



HawkEye XDR Agent

powered by DTS Solution

Hunting Cyber Adversaries

The HawkEye XDR agent is a robust endpoint security threat detection and prevention solution designed for deployment on user devices and server compute infrastructure to provide unparalleled visibility.

It provides continuous data collection, on-demand forensic capabilities, and automated response to evolving threats. With its advanced features, the agent ensures comprehensive protection and real-time visibility across your infrastructure.

HawkEye XDR agent does not replace your existing NGAV or EDR, rather it augments it to work seamlessly with HawkEye XDR platform.



Device Security Posture

- Software Bill of Materials
- Vulnerability Assessments
- Configuration Assessment



Threat Detection & Hunting

- Security Log Enhancement
- Security Log Collection
- File Integrity Monitoring
- Registry Integrity Monitoring



Investigation

- On Demand Forensic Collection
- DFIR Artifact Collection



Threat Containment

- Automated Response
- Device Quarantine

Key Features



Device Security Posture

The HawkEye XDR agent is equipped to perform comprehensive configuration assessments, ensuring your server compute and user devices comply with critical industry regulations and frameworks. These assessments help maintain the security posture and ensure that systems meet the necessary compliance requirements for protecting sensitive data.

In addition to compliance checks, the agent carries out in-depth vulnerability assessments, identifying potential weaknesses and providing actionable insights to address security gaps.

Furthermore, it offers a Software Bill of Materials (SBOM), providing a complete inventory of installed software components, which enhances transparency and helps mitigate risks associated with third-party software vulnerabilities in the supply chain.



Threat Detection and Hunting

The HawkEye XDR agent offers robust and comprehensive threat detection capabilities designed to safeguard your infrastructure. It excels in log collection and enhancement, transforming raw data into enriched, actionable insights for accurate threat identification.

In addition to tracking processes and services, the agent continuously monitors network connections, ensuring that any unusual or suspicious activity is detected in real-time. Its file and registry integrity monitoring further strengthens security by quickly identifying unauthorized changes to critical system components, minimizing the risk of compromise. What sets the agent apart is its ability to facilitate behavioral detection, proactively identifying emerging threats through abnormal activity patterns.

This advanced approach helps mitigate risks before they escalate, providing an essential layer of defense against the ever-evolving threat landscape.



Threat Containment

The HawkEye XDR agent is equipped with powerful automated response capabilities that enable swift and decisive actions against detected threats. Once a threat is identified, the agent can automatically quarantine compromised systems, isolating them from the network to prevent further damage or lateral movement. It also initiates threat containment measures, such as blocking suspicious network connections and disabling malicious processes, ensuring rapid neutralization of potential risks.

Additionally, the agent integrates seamlessly with firewalls and other security controls to block indicators of compromise (IOCs) in real-time, stopping threats at the perimeter. By automating these responses, the HawkEye XDR agent reduces response times, minimizes human error, and allows your security team to focus on more strategic tasks, all while maintaining a strong defensive posture against evolving cyber threats.



Investigation

The HawkEye XDR agent is equipped with advanced forensic investigation capabilities, enabling comprehensive visibility into system activities. It performs detailed offline forensic collection, gathering crucial artifacts such as system processes, running services, file integrity data, network connection history, and browser history.

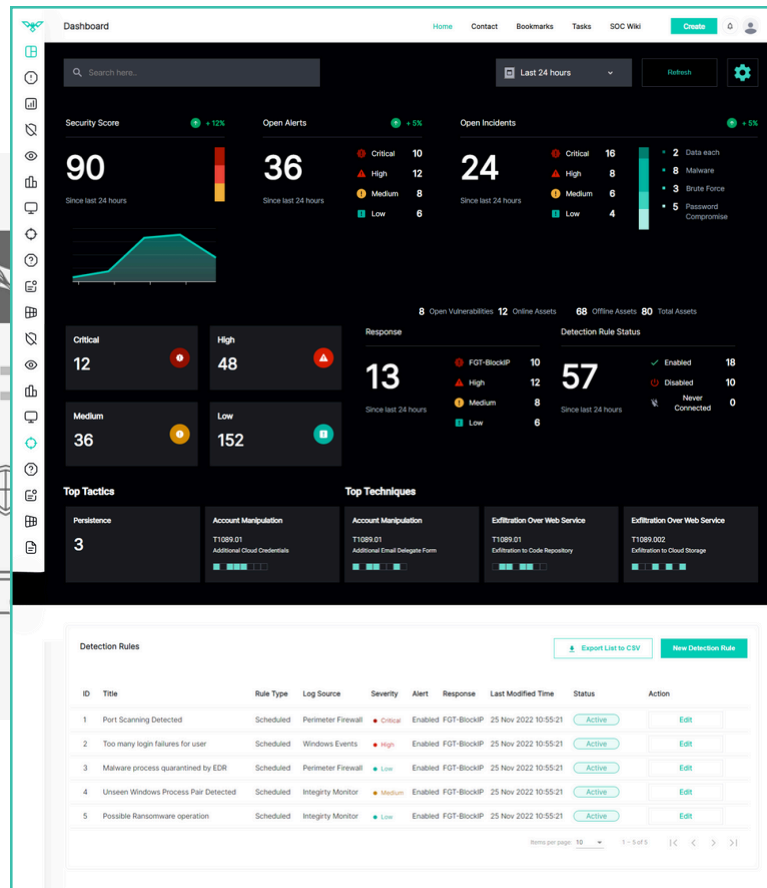
These capabilities allow investigators to trace user activity, analyze potential compromise points, and uncover the origins of suspicious behavior. By collecting detailed system configurations, audit logs, and user activity, the agent provides a full picture of events leading up to an incident.

This deep forensic data allows security teams to conduct thorough investigations, understand root causes, and implement effective remediation measures.



***HACKERS DON'T SLEEP, NEITHER DO WE.
HUNTING CYBER ADVERSARIES WITH HAWKEYE***

powered by **DTS Solution**



Technical Specifications

Device Security Posture

- **Software Bill of Materials**
Maintains the inventory of installed applications and libraries, including the below details.
 - Name
 - Version
 - Vendor
 - Format
 - Size
 - Install Time
 - Architecture
 - Description
 - Filepath
 - Checksum

Device Security Posture

- **Device Inventory**

Device inventory maintained includes the below details.

- Hardware
 - Motherboard Serial Number
 - CPU information
 - Memory Information
- Operating System Information
 - OS Name
 - OS Version
 - OS Platform
 - OS Major Release
 - OS Minor Release
 - Hostname
 - Windows update details
- Network Interfaces
 - Name
 - Adapter
 - State
 - MAC Address
 - Sent Packets
 - Received Packets
 - Sent Bytes
 - Received Bytes
 - Dropped Packets (sent and received)
 - IP Address
 - Netmask
 - Gateway
 - DHCP Status
 - Network Connections

- **Vulnerability Assessment**

Vulnerability detection begins with the HawkEye XDR periodically collecting a Software Bill of Materials (SBOM) from monitored systems, which is then transmitted to a centralized database.

A specialized detection module on the server analyzes the SBOM, comparing it against vulnerability intelligence to identify potential security risks. This analysis is based on Common Vulnerabilities and Exposures (CVE) records, sourced from our Cyber Threat Intelligence (CTI) platform.

- **Security Configuration Assessment**

The Security Configuration Assessment (SCA) module helps security teams identify and address misconfigurations within their infrastructure. Agents scan the monitored endpoints using predefined policy files, which contain specific checks tailored for each system.

This module includes ready-to-use SCA policies based on the security benchmarks established by the Center for Internet Security (CIS). These benchmarks provide essential best practices for securing IT systems and safeguarding sensitive data.

Information thus obtained along with information from other modules such as File Integrity Monitoring, Vulnerability Assessments etc. along with tagged rulesets provide information on compliance with PCI DSS, HIPAA, NIST 800-53, TSC, and GDPR frameworks and standards.

Threat Detection

• Log Collection

Log collection is the primary method for threat detection, centralizing event data from various systems, applications, and devices to provide critical insights for identifying security incidents, monitoring activity, and enabling timely response to potential threats.

The HawkEye Telemetry agent collects logs mainly using the below methods.

- Event log collection
- Logs from flat files
- Remote logs via syslog forwarding
- API based collection for SaaS and PaaS applications
- Docker log collection for containerized applications

Logs thus collected are normalized and shipped to the centralized analysis engine for further enrichment and analysis.

• File Integrity Monitoring

The HawkEye telemetry agent's File Integrity Monitoring (FIM) capability helps track and log all changes to critical files and directories, making it invaluable for maintaining visibility into system modifications.

This feature supports change tracking, ensuring that all adjustments are documented and authorized, which is critical for regulatory compliance.

Additionally, FIM plays a key role in ransomware detection by identifying unauthorized or unexpected file alterations, helping organizations respond quickly to potential attacks and safeguard sensitive data.

• Log Enhancement

The HawkEye telemetry agent offers advanced monitoring capabilities for enhanced threat detection and analysis.

It captures critical data, including detailed event logs for process creation, file and registry changes, network connections, and more, enabling deep visibility into system activities.

- Key Capabilities of the HawkEye Telemetry Agent:
- Process creation and termination tracking
- File creation and modification monitoring
- Registry changes and key tracking
- Network connection logging
- Driver and image load monitoring
- Raw disk access detection
- Thread injection detection

• Registry Integrity Monitoring

The HawkEye telemetry agent includes Registry Integrity Monitoring, which tracks changes to critical registry keys and values in real-time.

This feature is vital for detecting unauthorized or suspicious modifications that could indicate a potential security breach. By keeping a record of all registry alterations, it aids in change tracking, ensuring that only approved modifications are made. This capability also supports regulatory compliance by maintaining a secure baseline configuration.

Additionally, it enhances ransomware detection by identifying malicious registry changes that are often associated with such attacks.

Investigation

- **Real-time system queries:** Allows for live data collection across endpoints, providing visibility into processes, services, and configurations.
- **Forensic data collection:** Enables retrieval of disk, memory, and log data for detailed offline investigation.
- **Automated artifact retrieval:** Simplifies the collection of critical data to accelerate incident response and remediation efforts.
- Digital artifacts thus collected include the below.
 - **File and directory metadata:** Captures information on file creation, modification, and deletion.
 - **Network connections:** Logs active network connections and associated processes.
 - **Process and service information:** Tracks running processes and service changes over time.
 - **Registry modifications:** Monitors changes to critical registry keys.
 - **Memory and disk snapshots:** Collects forensic data from memory and disk for offline analysis.
 - **Event log capture:** Gathers system, application, and security event logs for investigation.

Containment

The HawkEye telemetry agent features an **Automated Response** capability that enables swift, rule-based actions in response to detected threats. This automation allows the agent to mitigate risks in real-time, such as blocking malicious IP addresses, isolating infected systems, or stopping suspicious processes.

Example Automated Response Actions

- Block connections to specific IP addresses using host firewall
- Isolate the device from the network
- Trigger a custom script when a particular event is logged.
- Trigger collection of DFIR Artefacts to remote server when a particular event is logged.


Operating System Compatibility

Operating System	Compatibility
Windows 11	Fully compatible
Windows 10	Fully compatible
Windows 8.1	Fully compatible
Windows 7 (EOL)	Partially compatible (Some features may not work)
Windows Vista (EOL)	Partially compatible (Some features may not work)
Windows XP (EOL)	Partially compatible (Some features may not work)
Windows Server 2022	Fully compatible
Windows Server 2019	Fully compatible
Windows Server 2016	Fully compatible
Windows Server 2012 R2	Fully compatible
Windows Server 2008 R2 (EOL)	Partially compatible (Some features may not work)
Ubuntu (All supported versions)	Partially compatible (Some features may not work)
RHEL (All supported versions)	Partially compatible (Some features may not work)
CentOS (All supported versions)	Partially compatible (Some features may not work)



HAWKEYE
HUNTING CYBER ADVERSARIES

 www.hawk-eye.io

 +971 4 338 3365

 hawkeye@dts-solution.com
