HAWKEYE

HawkEye Managed CSOC and XDR

powered by DTS Solution

Hunting Cyber Adversaries

Security Orchestration, Automation and Response (SOAR)

Security Orchestration, Automation and Response (SOAR)

SOAR (Security Orchestration, Automation, and Response) is a category of security solutions that combine three core functions — **orchestration, automation,** and **response** — into a unified platform. SOAR platforms are designed to improve the efficiency and effectiveness of Security Operations Centers (SOCs) by automating routine security tasks, orchestrating complex workflows, and enabling faster, more consistent incident response.

1. Orchestration

SOAR platforms integrate various security tools and processes, enabling them to work together in a coordinated manner. This integration allows for seamless communication between tools such as SIEMs, firewalls, EDR systems, and threat intelligence platforms, thereby reducing the need for manual intervention.

2. Automation

SOAR automates repetitive, time-consuming tasks, such as data collection, enrichment, and incident triage. By automating these tasks, SOAR reduces the manual workload on security analysts, allowing them to focus on more complex issues that require human expertise.

3. Response

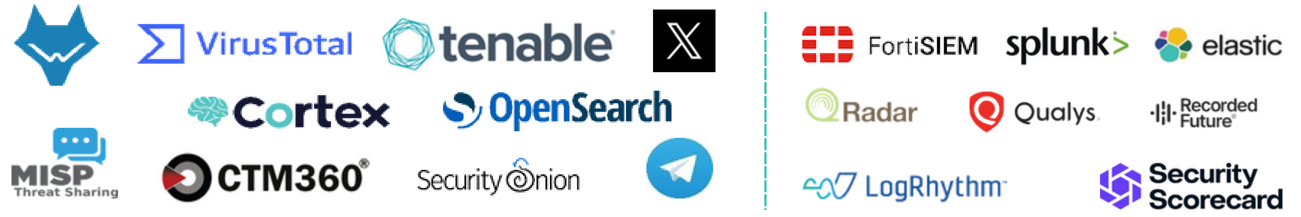
SOAR facilitates faster and more accurate incident response by providing predefined playbooks and workflows that guide analysts through the response process. This ensures that incidents are handled consistently and in accordance with best practices, reducing the likelihood of errors and improving overall response times.

This datasheet discusses the SOAR capabilities of HawkEye Managed CSOC and XDR.

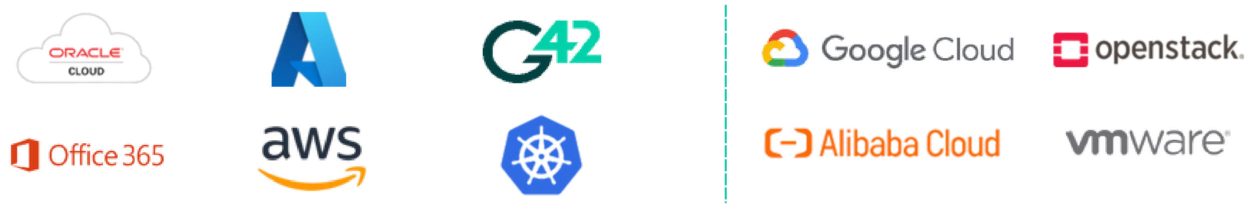
Integration Capabilities and Supported Platforms

HawkEye CSOC integrates with a wide range of industry-leading tools and platforms to enhance our SOAR capabilities. All platforms and solutions with an API interface is supported for integration.

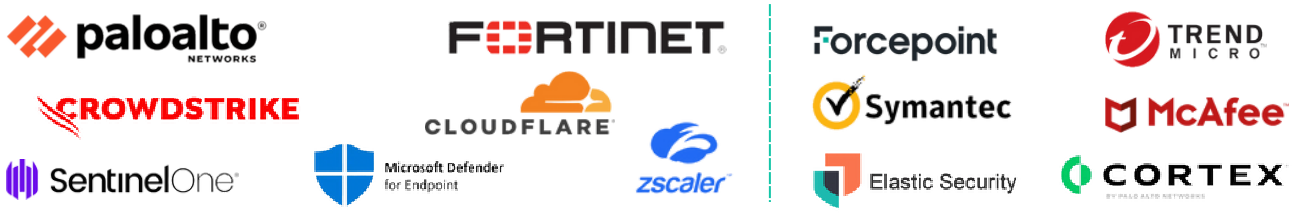
SIEM AND CYBER THREAT INTELLIGENCE



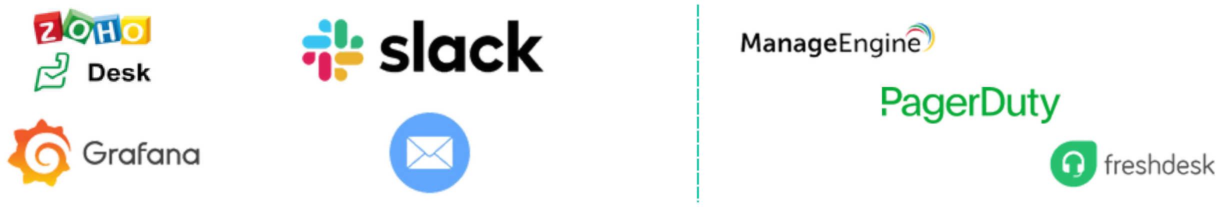
CLOUD AND SAAS



NETWORK AND ENDPOINT SECURITY



ALERTS AND INCIDENT RESPONSE



SOAR Use Cases

HawkEye SOAR use cases are divided into categories as seen below.

01 Collect

Aggregating and centralizing data from various sources to ensure comprehensive visibility and real-time analysis in the SOC.

02 Enrich

Enhancing raw data with contextual information, such as threat intelligence and geolocation, to improve the accuracy of threat detection and investigation.

03 Detect

Identifying potential security incidents through advanced analytics, machine learning, and correlation of enriched data against known threat patterns.

04 Respond

Automating and orchestrating actions to contain, mitigate, and remediate security incidents swiftly and effectively.

05 Verify

Continuously validating the effectiveness of security measures, monitoring the threat landscape, and ensuring the integrity of response actions.

> ***HACKERS DON'T SLEEP, NEITHER DO WE.***
> ***HUNTING CYBER ADVERSARIES WITH HAWKEYE***
>
> powered by **DTS Solution**

Sample Use Cases

Below are a few sample use cases for each of the categories.

01 Collect

Our collection capabilities are designed to seamlessly integrate various data sources into our SIEM, enabling comprehensive monitoring and analysis.

- EDR to SIEM
- Cloud to SIEM (API)
- Cloud to SIEM (Webhook)

02 Enrich

We enhance our collected data with additional context, allowing for more informed decision-making and improved threat detection.

- Enrichment of SIEM events with Cyber Threat Intelligence
- Enrichment of SIEM events with Geo-IP data

03 Detect

Our detection capabilities employ advanced algorithms and machine learning to identify threats across our monitored environments.

- SIEM Logs to ML Framework
- Scheduled SIEM aggregated searches

04 Respond

We automate responses to detected threats, ensuring rapid containment and mitigation of risks.

- Trigger Scans on EDR
- Quarantine Hosts
- Block IOCs on Firewall

05 Verify

Verification processes are in place to ensure the continuous effectiveness of our security measures.

- Discover Vulnerabilities
- Web service health checks
- Monitoring threat landscape
- Monitoring for impersonating domains
- Automated email reports

HAWKEYE

HUNTING CYBER ADVERSARIES

www.hawk-eye.io

+971 4 338 3365

hawkeye@dts-solution.com