HAWKEYE

Managed CSOC and XDR
powered by DTS Solution

Hunting Cyber Adversaries

Your Cyber Guardian

HAWKEYE Managed CSOC and XDR powered by DTS Solution helps you stay ahead of the cyber threat and adversary landscape.

We strategize, develop, build, and manage your security operations from our state-of-the-art Next Generation Cybersecurity Operations Center.

We continuously monitor your digital assets whilst detecting and protecting from threat actors.

Our aim is always to stay one-step ahead of an ever-changing threat and adversary cyberspace and delivering the necessary in-depth visibility you need without having to develop and build cyber capabilities, so that you can focus on your core business.

Managed SOC as a Service

HAWKEYE Cyber Security Operations Center (CSOC) and XDR powered by DTS Solution is based out of Dubai and Abu Dhabi, United Arab Emirates (UAE) and with regional coverage of Europe, Middle East and Africa.

→ Cyber Threat Detection with Advanced Machine Learning

→ Power of Big Data Security Analytics at Lightning Speed

→ Leader in SecOps and Threat Intel Fusion

→ Agile, Dynamic, Award Winning and Deep Technical Expertise

Key Features

HAWKEYE – SOC-as-a-Service by DTS Solution is a cost effective solution that drastically improves the security posture of your organization whilst reducing significant costs that are ordinarily attributed to security incidents.

→

Real-Time Monitoring

- 24x7 Managed CSOC and XDR
- NG-SIEM, UEBA and Open XDR
- Machine Learning driven CSOC
- Proactive and Predictive Cybersecurity Monitoring
- Deep Security Analytics leveraging Big Data
- Security Events and Log Correlation
- Managed Extended Detection and Response (XDR)

→

Cyber Threat Management

- Threat Hunting as a Service
- Threat Adversary Detection
- Use Case Development
- Attack Surface Management
- Threat Intelligence
- OSINT and DARKINT
- Brand Monitoring
- Managed Endpoint Detection and Response
- Managed Phishing and Security Awareness
- Vulnerability Risk Prioritization

→

Incident Management

- Incident Management Process and Plan
- Incident Notification and Response
- Security Incident Response Triage
- Managed SOAR - Security Automation and Orchestration
- Incident Digital Playbooks
- Breach Attack Simulation
- Managed Digital Forensics

→

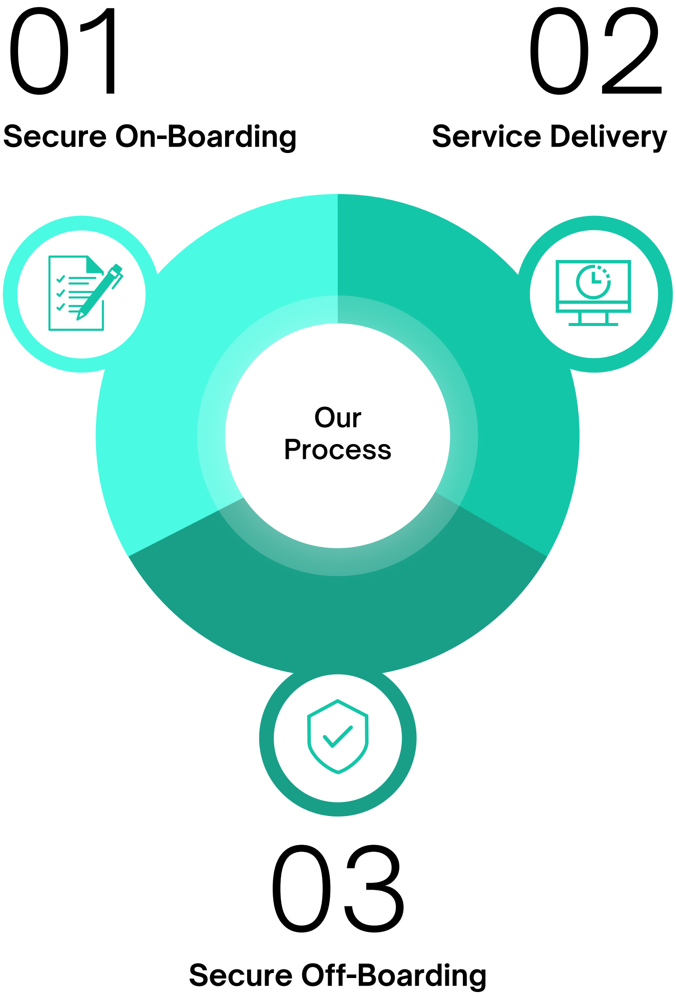
Operational Compliance

- CSOC Policies, Processes and Procedures
- Compliance Monitoring
- Hardening Policy Compliance
- Change Management Monitoring
- Configuration Management Monitoring
- Security Audit Monitoring
- 3rd Party Access Monitoring
- Supply Chain Risk Monitoring
- Privileged Access and Activity Monitoring
- Developer Access and Activity Monitoring
- Application, Infrastructure, and Cloud Threat Modeling

Our Process

We will perform an onsite discovery workshop with the customer to understand the current inherent risk profile based on a series of questions that has been designed to understand current maturity, threat level, exposure and organizational and business value.

The score is then bench-marked across our recommended package matrix to define which service model would be the most appropriate based on the inherent risk profile and types of advanced cyber security monitoring services required.



> **_HACKERS DON'T SLEEP, NEITHER DO WE. HUNTING CYBER ADVERSARIES WITH HAWKEYE_**
>
> powered by
>
> **DTS SOLUTION**

Subscription Packages

We have tailored our subscription packages in four tiers to accommodate varying cyber risk levels posed to your organization, budgets and business requirements to ensure maximum cyber resiliency.

24 x 7 cyber guardian services, active cyber threat monitoring and full-access to customized use case and much more are included in Premium.

Outsourced Remote Monitoring – Managed / Hybrid (On-premise SIEM)

→ Remote Monitoring

Ideal for organizations that already have an on-premise SIEM platform and need to have a fully managed or co-managed CSOC (8×5 or 24×7). We manage your SIEM platform through staff augmentation in a dedicated, shared, onshore or offshore model.

- 8×5 or 24×7 CSOC *eyes on-screen* coverage
- Managed or Co-Managed customer owned SIEM / NG-SIEM / UEBA/EDR
- Secure Onboarding and Integration of Log Sources
- Continuous Cyber Threat Monitoring as a Service
- Enrichment with HawkEye Cyber Threat Intelligence and Fusion
- SIEM Operations, Optimization and Enrichment
- EDR Operations, Optimization and Enrichment
- Use Cases Development and Enhancements
- Incident Management and Reporting
- CSOC Dashboards and Metrics
- Managed Digital Forensics and Incident Response
- Vulnerability Assessment and Penetration Testing
- Quarterly SIEM Health-Check
- Annual/semi-annual Compromise Assessment
- Optional: Augmentation with XDR

SOC-as-a-Service – Managed / Hybrid (Off-premise SIEM)

→ Lite BRONZE

Suitable for organizations that need to monitor the Internet Perimeter. Ideal for SMEs that need to outsource security monitoring services.

→ Baseline SILVER

Suitable for organizations that need to monitor internet perimeter and critical systems. Ideal for SMEs that need to outsource security monitoring services.

→ Advanced GOLD

Ideal for organizations that need to monitor the IT systems. Ideal for large organizations that need to outsource security monitoring services that involves an internal team.

→ Premium PLATINUM

Ideal for organizations that need to monitor the internet perimeter. Ideal for large organizations that need to augment security monitoring services with their internal IT security and operations team.

Features	Lite BRONZE	Baseline SILVER	Advanced GOLD	Premium PLATINUM
NG-SIEM, UEBA and Open XDR	Y	Y	Y	Y
Cyber Threat Intelligence	Y	Y	Y	Y
Machine Learning Threat Detection	Y	Y	Y	Y
Managed Detection and Response (MDR) Log Sources	Y	Y	Y	Y
No. of Log Sources	Up to 50	50 - 100	100 - 200	200 - 300
Log Sources	On-Premises and Cloud IaaS			
Office 365 Monitoring	Y	Y	Y	Y
Hot Storage	3 Months			
Warm Storage	6 Months			
Cold Storage	12 Months			
Events per Second	1000	2000	3000	5000
Access to CSOC Dashboards (Read-Only)	Y	Y	Y	Y
Reports	Monthly and Quarterly Report		Weekly, Monthly and Quarterly Report	
Leverage In-House Library of Threat Detection Use Cases	Y	Y	Y	Y
MITRE ATT&CK Coverage	Y	Y	Y	Y
Threat Hunting	Y	Y	Y	Y
Call Center Support	Y	Y	Y	Y
Managed Digital Forensics and Incident Response	X	X	X	Y
Customized Use Cases Support	X	X	Y	Y
Digital Forensics and Incident Response (Add-On)	Y	Y	Y	X
Managed Vulnerability Assessment (Add-On)	X	Y	Y	Y
Managed Perimeter Penetration Testing (Add-On)	X	Y	Y	Y
Managed Web Application Scanning (Add-On)	X	Y	Y	Y
Managed SOAR (Add-On)	X	X	Y	Y
Attack Surface Management (Add-On)	X	X	Y	Y
Managed OSINT and DARKINT (Add-On)	X	X	Y	Y
Managed Security Awareness (Add-On)	X	X	Y	Y
Managed Phishing (Add-On)	X	X	Y	Y
Network Detection and Response – NDR (Add-On)	X	X	Y	Y
Brand Monitoring (Add-On)	X	X	Y	Y
Managed CASB (Add-On)	X	X	Y	Y
Managed Compromise Assessment (Add-On)	X	X	Y	Y

HAWKEYE

HUNTING CYBER ADVERSARIES

www.hawk-eye.io

☎ +971 4 338 3365

✉ hawkeye@dts-solution.com