DTS SOLUTION
CYBER SECURITY REDEFINED

SERVICE DESCRIPTION

HAWKEYE ADVANCED

HAWKEYE

DTS has developed the Managed SOC cyber security center service in four tiers to accommodate varying cyber risk levels posed to your organization, budgets and business requirements to ensure cyber resiliency.
The HAWKEYE Advanced service has been tailored to meet the needs of medium to large organizations that require internet perimeter and internal network monitoring to understand their external and internal cyber risk exposure and monitoring capabilities on cyber-attacks aimed at the organization.

The most effective approach to cyber security hygiene starts with visibility into all activities on systems, networks, databases, and applications. The internet perimeter of any organization poses one of the highest cyber risk factors which needs to be constantly monitored, round the clock to ensure your internal networks and systems are not compromised. Monitoring internal IT environment ensures cyber breaches such as malware infections and virus outbreaks are quickly identified.

HAWKEYE Advanced: HAWKEYE Advanced has been tailored to meet the needs of medium to large organizations that require internet perimeter and internal network monitoring. This service provides complete internet perimeter and internal network monitoring designed and developed by DTS security experts.

We collect events and logs from the critical components of your perimeter, internal network and applications such as Next-Generation Firewall (NGFW), (Web Application Firewall) WAF, Intrusion Prevention Systems (IPS), Mail Security, Internet Routers, Active Directory, Exchange, Endpoint Security, Applications (Web and Database) and so on (up to a maximum of twenty five log sources). DTS cyber security center will continuously monitor the internet perimeter and internal network on a 24/7 basis by our highly trained cyber security professionals and analysts.

This service supports a standard log retention period of all collected event and log data of six months. HAWKEYE Advanced supports up to twenty standard use cases that violate security best practices to quickly identify the scope of the cyber-attacks whether it is external or internal, determining the mitigation options and notification on the remedial activities to the point of contact from your organization.

Pre-defined cyber security dashboards and reports are automatically generated and provided to your organization on daily, weekly and monthly basis that summarize your cyber risk posture on the internet and internal networks. Customized reports are also part of the package based on your unique business needs and requirements.

The monthly report contains a summary of security incidents identified. Security incidents identified are reported in real-time to ensure breaches and compromised are contained.

HAWKEYE Advanced provides security monitoring of your external and internet IT environment through a fully manned cyber security center providing round the cloud 24/7 coverage. Providing both automated and manual alerting and notifications in real-time when security incidents are identified.

Key Features

HAWKEYE Advanced – Security Event Logging and Monitoring Service

- Log capturing for customer's critical perimeter and internal network, systems and application components
- Enhanced Log retention
- Event monitoring, correlation, analytics and alerting
- Advanced Machine Learning based Threat Correlation
- Reporting (daily, weekly, monthly)
- Real-time incident notification

HAWKEYE Features	Lite | Bronze	Baseline | Silver	Advanced | Gold	Premium | Platinum
Number of Log Source Integration (maximum)	5	15	25	50
Online Log Retention in Months	3	3	3	3
Events Per Second (EPS)	250	500	1000	2000
SOC Dashboard Access (Multi-Tenancy / RBAC)	X	3	3	3
Standard Use Cases Reports	5	10	20	30
Customized Use Cases Reports	X	X	5	10
Event Log Receiver / Collector (Hawkeye Cloud)	3	3	3	3
Event Log Receiver / Collector Onsite (VM based)	X	X	X	TBC
8 x 5 Security and Threat Monitoring Team	3	3	3	3
24 x 7 Security and Threat Monitoring Team	X	3	3	3
Email Support 8 x 5	3	3	3	3
Call Center Support 24 x 7	X	3	3	3
Service Level Agreement	3	3	3	3
Service Integration Team 8 x 5 (Log Integration)	X	3	3	3
Service Integration Team 8 x 5 (Use Case Dev.)	X	X	3	3
Security Vulnerability and Threat Management Team 8 x 5	3	3	3	3
Service Integration Team 8 x 5 (Log Integration)	3	3	3	3

DTS SOLUTION
CYBER SECURITY REDEFINED

HAWKEYE SOC-as-a-Service Add-Ons

Add-Ons	Available
Additional Log Source	3
Additional Online Log Retention in Months	3
Additional Events Per Second (per 250 block)	3
SOC Dashboard Access (Multi-Tenancy / RBAC)	3
Additional Use Cases Development and Report	3
Managed Vulnerability Assessment (per IP blocks)	3
Managed Penetration Testing (per IP blocks)	3
Continuous Perimeter Monitoring	3
Cloud Services (SaaS) Monitoring	3
Threat Intelligence Enrichment Services	3