Logicom Solutions

MANAGED SECURITY SERVICES

Proactive. Reactive. Always On.

solutions.logicom.net

HAWK360°

MANAGED SECURITY SERVICES

Our Managed Security Service is not just about monitoring; it’s about creating a resilient security posture that adapts to today’s dynamic threat environment. By combining cutting-edge tools, skilled professionals and tailored processes, we deliver an effective, reliable and competitive solution for your cybersecurity needs.

Logicom Solutions

The Key Challenges Being Faced Today

Resource & Expertise Constraints

SHORTAGE OF SKILLED SECURITY PROFESSIONALS
Finding and retaining top cybersecurity talent is a growing challenge. Most organizations struggle with limited in-house expertise, making it harder to detect, respond to and prevent evolving cyber threats.

REGULATORY AND COMPLIANCE COMPLEXITY
Keeping up with evolving regulations like DORA, NIS2 and ISO standards demands continuous effort, expertise and resources. Non-compliance can lead to financial penalties, operational disruptions and reputational damage.

COST & COMPLEXITY OF SECURITY OPERATIONS
Building and managing an in-house SOC, governance framework and security testing requires significant investment, skilled resources and ongoing maintenance, making it a costly and complex challenge for organizations.

Gaps in Security Coverage & Strategy

FRAGMENTED SECURITY APPROACH
Many providers focus solely on SOC monitoring, neglecting critical areas like governance, security awareness and risk management, failing to address the full scope of the cybersecurity threat landscape.

LACK OF CONTINUOUS SECURITY AWARENESS
Employees remain one of the top attack vectors, yet ongoing training and phishing simulations are often overlooked, leaving organizations vulnerable to human error and social engineering attacks.

INADEQUATE VULNERABILITY & RISK MANAGEMENT
Periodic assessments alone aren't sufficient. Continuous monitoring and proactive remediation are essential to stay ahead of evolving vulnerabilities and minimize risk exposure.

Evolving Threat Landscape & Incident Response Challenges

INCREASING ATTACK SOPHISTICATION
Cyber threats are rapidly evolving through AI and automation, rendering traditional defences inadequate against advanced, adaptive attacks.

INEFFECTIVE INCIDENT RESPONSE & REMEDIATION
Organizations often lack structured plans for effective response, containment, and recovery, leading to delayed action and prolonged exposure during security incidents.

LIMITED THREAT INTELLIGENCE & PROACTIVE DEFENSE
Organizations often rely on reactive security measures, failing to leverage threat intelligence and proactive, offensive security strategies to stay ahead of emerging risks.

HAWK360°
MANAGED SECURITY SERVICES

When the stakes are high, we turn cyber challenges into opportunities for strength and growth.

HAWK360°

MANAGED SECURITY SERVICES

VISION

Centered around empowering organizations to succeed by addressing their most critical security needs. By delivering top-tier Managed Security Solutions, we aim to create an environment where businesses can focus on their core operations with confidence, knowing that their digital assets are secure.

MISSION

Protecting businesses and empowering trust by delivering tailored cybersecurity solutions that adapt, defend, and ensure compliance in an ever-evolving digital world.

Logicom Solutions

HAWK360°

MANAGED SECURITY SERVICES

MANAGED SECURITY SERVICES

Logicom Solutions

HAWK360°
MANAGED SECURITY SERVICES

MANAGED SECURITY SERVICES

Managed SOC Services

Continuous threat monitoring, detection, and response powered by advanced security analytics.

Adversary Attack Simulations

Real-world attack simulations to identify security gaps and strengthen defenses. This also includes Managed ongoing Vulnerability Assessments.

Phishing Campaigns & Infosec Trainings

Engaging simulations and training programs to enhance employee security awareness.

Secure Code Review

In-depth analysis of application code to uncover vulnerabilities before exploitation.

CISO-AS-A-SERVICE

Get a team, not just an individual, to strengthen your cybersecurity. From day one, we assess, strategize and establish strong governance while supporting both technical teams and leadership. With a hands-on approach, we drive assessments, roadmaps and initiatives, making security a continuous journey, not just a checkbox.

Dark Web and Brand Monitoring

Proactive surveillance of illicit forums to detect threats targeting your brand and data.

Infra Monitoring Service

Continuous health and availability monitoring of critical IT infrastructure.

Logicom Solutions

HAWK360°
MANAGED SECURITY SERVICES

Logicom Solutions

DESIGN OF THE SOLUTION OF OUR MSOC

HAWK360°
MANAGED SECURITY SERVICES

Our service delivery model

Safeguarding your IT Environment and operations

Threat Monitoring and Incident Response

The MSOC will deliver continuous monitoring of all log sources, utilizing a world leading SIEM platform, integrated with custom threat detection use cases. Automated and manual correlation of multi-source event logs will ensure early detection of sophisticated threats, with predefined playbooks for rapid incident response.

Dynamic Asset Categorization and Risk Prioritization

Leveraging a continuously updated asset inventory, the MSOC will classify servers and networking devices into risk tiers based on their criticality, exposure, and operational dependencies. Risk scores will be dynamically adjusted through integrations with vulnerability scanners and ongoing behavioral analysis to prioritize remediation efforts.

Advanced Threat Intelligence Integration and Correlation

The service will incorporate real-time global threat intelligence feeds, enriched with sector-specific intelligence. This data will be dynamically correlated with your organization's environment to identify emerging threats, including zero-day vulnerabilities and advanced persistent threats (APTs) targeting critical infrastructure.

Advanced Log and Anomaly Analysis with Machine Learning (ML)

Utilizing machine learning algorithms, the MSOC will analyze the events from all log sources. Behavioral baselines for devices, users, and network traffic will be created and continuously updated to detect anomalies indicative of insider threats, lateral movement, or compromised systems.

Continuous visibility

By maintaining logs for a period of 1 year in hot storage, we ensure these are always available for search and threat hunting, as if they were from the previous day. This allows for continuous visibility into historical data, enabling rapid analysis and investigation of potential threats across extended time frames. Our approach ensures that organizations can efficiently search, correlate, and respond to security incidents, leveraging historical logs for advanced threat hunting and incident forensics without any delays.

Logicom Solutions

HAWK360°
MANAGED SECURITY SERVICES

Our service delivery model

Safeguarding your IT Environment and Operations

Proactive Threat Hunting and Vulnerability Validation

Security analysts will conduct proactive threat-hunting activities, leveraging historical log data, behavioral patterns, and threat intelligence to identify potential weaknesses. This includes validation of vulnerabilities across the infrastructure through simulated attack vectors, ensuring actionable recommendations are provided in real-time.

Granular Reporting and Compliance Monitoring

The MSOC will generate detailed reports tailored to multiple compliance frameworks (e.g., GDPR, ISO 27001, NIS Directive) and operational needs. Customized dashboards will provide visibility into KPIs, threat trends, and incident statuses. Periodic compliance gap analyses will help maintain alignment with regulatory requirements and internal policies.

Orchestrated Response with Automated Workflows

The MSOC will enable semi-automated response mechanisms through integration with SOAR (Security Orchestration, Automation, and Response) platforms. For example, detected threats will trigger automated actions such as isolating compromised systems, updating firewall rules, or notifying administrators via predefined escalation protocols. This minimizes downtime while ensuring accountability through detailed audit trails.

Logicom Solutions

Managed SOC – The Architecture & Key Components

A conceptual overview of our SOC Infrastructure & Security Capabilities

HAWK360°
MANAGED SECURITY SERVICES

COLLABORATION HUB | **DASHBOARDS** | **PLAYBOOKS PORTAL** | **REPORTS**

Google SecOps

SIEM | **SOAR** | **THREAT INTEL**

HAWK360°
MANAGED SECURITY SERVICES

CUSTOMER

ON PREM

FORWARDER

CONNECTOR | CONNECTOR | CONNECTOR | CONNECTOR

- **OS** (Win, Linux)
- **Other** (Security, Net)
- **Custom** (Apps, DB)

Multi - SIEM Integrations

Multi - XDR Integrations

Cloud Solutions

Response Actions (Indicative)

- Isolate compromised endpoint
- Block malicious IP addresses & URLs
- Create/assign/edit ticket in client ITSM
- Contain malicious spam campaigns
- Collaborative response activities
- Kill processes and quarantine malicious files
- Engage client's incident response service

Logicom Solutions

Leveraging Google's Advanced Threat Intelligence

Unmatched visibility, real-time threat insights and actionable intelligence from Mandiant, VirusTotal and Google's Global Ecosystem

Mandiant

Industry-leading incident response and threat intelligence

More than 1.000 incidents per year

Monitoring more than 350 Threat Actors

VIRUSTOTAL

World's largest malware database and analysis platform

Intelligence for early threat detection

Crowdsourced threat detection with 70+ antivirus engines

Google Threat Intelligence

Powering cybersecurity with unparalleled intelligence

Threat intelligence from Google's vast ecosystem (GCP, Android, Chrome, YouTube, Gmail and more)

Dark Web Monitoring / Attack Surface Management to support organizations detect, analyze and mitigate cyber threats

HAWK360°
MANAGED SECURITY SERVICES

Logicom Solutions

HOW WE DELIVER

HAWK360°
MANAGED SECURITY SERVICES

Our Approach

What is included in each phase of our MSOC service

A 4-Phased approach towards the enablement of the service

PHASE 1

DISCOVERY

The Discovery phase focuses on understanding the client's environment, identifying critical needs, and defining the scope for the SOC implementation.

PHASE 2

ANALYSIS & DESIGN

The Analysis and Design phase covers the SOC design and operational strategies are developed, ensuring alignment with organizational goals and threat management needs.

PHASE 3

IMPLEMENTATION

The Implementation phase involves deploying the SOC components, integrating tools, and ensuring the system is fully operational and tested.

PHASE 4

MONITORING & RESPONSE

The Monitoring and Response phase centers on the continuous monitoring of security events, leveraging the SOC's tools and processes to detect, analyze, and respond to threats in real-time.

Logicom Solutions

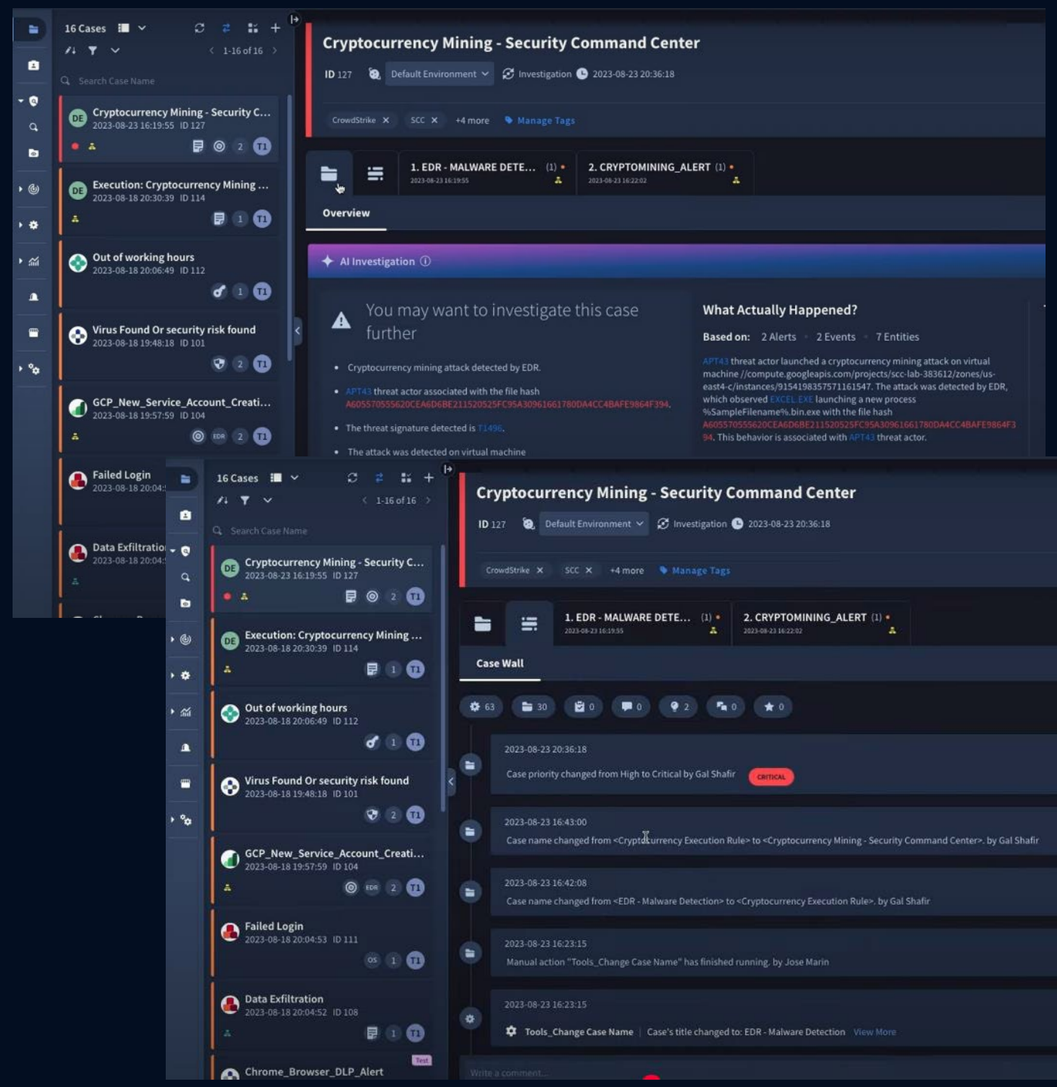
REDEFINING CYBERSECURITY WITH CLARITY AND CONTROL

We handle the complexity, you get a seamless and secure experience

HAWK360°
MANAGED SECURITY SERVICES

Hawk360 enhances your organization's cybersecurity operations by turning the complexities of the security landscape into an intuitive, seamless experience. Through a single-pane interface, customers gain unified access to real-time insights and actionable recommendations, enabling them to make informed decisions swiftly and effectively. Hawk360 streamlines cybersecurity management, empowering your team to focus on what matters most “Safeguarding critical assets and ensuring continuous operations”.

- **Unified SOC Interaction Portal**
- **Real-Time Incident Monitoring**
- **Direct Analyst Communication**
- **AI-Powered Case Summarization**
- **Comprehensive Event Analysis**
- **Interactive Playbook Automation**



Logicom Solutions

Logicom Solutions

Cyprus Head Office
50 John Kennedy Avenue 1076
Nicosia, Cyprus
Tel: +357 22 551 010

Greece Office
44 Kifissias Ave., Monumental Plaza, Building B
4th floor, 151 25 Marousi, Greece
Tel: +30 2111822800

Email: solutions@logicom.net

Web: solutions.logicom.net

HAWK360°
MANAGED SECURITY SERVICES