Managed Security Operations Centre (SOC)

Continuous Threat Monitoring & Rapid Incident Response for Financial Markets

Beeks

OVERVIEW

The Need for a Proactive Security Approach

Financial institutions are high-value targets for cyber threats, requiring **real-time detection and rapid response** to protect trading platforms, infrastructure, and sensitive data. Traditional security solutions are reactive, leaving institutions vulnerable to evolving attack tactics.

The **Beeks Managed SOC Service** delivers continuous monitoring, real-time threat detection, and expert-led incident response, ensuring **rapid containment and mitigation of cyber risks.**

KEY FEATURES

- **Leverages Microsoft Sentinel SIEM:** Its core platform for real-time analytics and anomaly detection
- **Security Orchestration & Automation (SOAR):** Enhances threat response by reducing false positives and enabling faster containment
- **Threat Intelligence Feeds:** Provides continuous updates on Indicators of Compromise (IOCs)
- **Log Data Collection:** All customer logs reside within segregated Azure environments, ensuring secure and compliant data management

COST PER DEVICE: £100 per month

FULLY MANAGED SECURITY CYCLE

DEFINE SECURITY SCOPE

Identify log sources, assets, and customer data sources to establish attack surface visibility

LOG COLLECTION & INTEGRATION

Secure log collection and threat detection setup to ensure real-time threat intelligence

CONTINUOUS THREAT MONITORING

Beeks SOC analysts triage alerts from Microsoft Sentinel SIEM to detect and prioritise security risks

INCIDENT TRIAGE & RESPONSE

Classify threats and initiate remediation guidance to ensure rapid containment of security events

SECURITY REVIEW & REPORTING

Provide security insights, compliance tracking, and improvements for ongoing optimisation of threat defence

beeksgroup.com americas@beeksgroup.com | apac@beeksgroup.com | emea@beeksgroup.com

Here are four key features that make Beeks SOC service stand out:

1. ESCALATION TO COMPUTER SECURITY INCIDENT RESPONSE TEAM (CSIRT)

- **24/7 Monitoring & Triage**
  – Beeks SOC analysts continuously assess alerts generated from the Microsoft Sentinel SIEM platform
- **Intelligent Alert Prioritisation**
  – Alerts are classified based on severity, ensuring that critical threats are addressed first
- **Actionable Incident Response**
  – Alerts trigger an incident ticket in the Jira Customer Portal, with remediation guidance
- **Remote Expert Support**
  – Up to 2 hours per alert of remote containment and mitigation assistance
- **Escalation to CSIRT**
  – High-priority incidents can be escalated to the Computer Security Incident Response Team (CSIRT)* for forensic analysis

2. THREAT INTELLIGENCE & USE CASE DEVELOPMENT

- **Dynamic Threat Detection**
  – Beeks continuously updates Microsoft Sentinel SIEM use cases to reflect evolving threats
- **Industry-Standard Intelligence**
  – Uses internal and external threat intelligence sources, including:
  - Incident response findings
  - Malware reverse engineering
  - Threat hunting insights
- **MITRE ATT&CK Framework Integration**
  – Identifies attacker tactics and techniques to reduce false positives and improve detection accuracy

3. ESCALATION TO DIGITAL FORENSICS & INCIDENT RESPONSE TEAM (DFIR)

- **Collaborative Incident Handling**
  – If a threat cannot be contained within 2 hours, customers can invoke additional forensic services
- **Invoke DFIR Service**
  – Incidents requiring deeper investigation can be escalated to Digital Forensics & Incident Response (DFIR)* for advanced forensic analysis

4. SERVICE MANAGEMENT & REPORTING

- **Security Customer Portal**
  – Incident summaries and remediation guidance are available on demand via the Customer Portal
- **Regulatory Compliance Support**
  – Supports ISO 27001, SOC2, NIS2, DORA, FCA, and GDPR security requirements with audit-ready reporting
- **Continuous Security Improvement**
  – Beeks provides on-going continuous security improvement in collaboration with customers as threats continue to evolve

* escalated incidents requiring CSIRT or DFIR forensic analysis are subject to an additional fee

WHY CHOOSE BEEKS MANAGED SOC SERVICE?

◇ **24/7 Security Operations Centre:**
Round-the-clock monitoring and immediate threat triage

◇ **Real-Time Threat Intelligence:**
Beeks continuously updates SIEM use cases and detection models

◇ **Rapid Incident Response & Containment:**
Remote remediation support with escalation to forensic teams when needed

◇ **Security Customer Portal:**
Jira-based reporting and incident tracking

◇ **Cloud & On-Premise Security:**
Designed for financial markets, low-latency environments, and hybrid infrastructures

Take the next step in securing your infrastructure
Get in touch to discuss how Beeks SOC can enhance your security.

beeksgroup.com americas@beeksgroup.com | apac@beeksgroup.com | emea@beeksgroup.com