Managed Vulnerability Scanning (MVS) Service

Beeks

Continuous Threat Visibility for Financial Markets

OVERVIEW

Cyber risks evolve daily, and financial institutions must **detect and mitigate vulnerabilities before they become security incidents**. Traditional, periodic assessments leave gaps—exposing trading platforms, infrastructure, and customer data to potential breaches.

Beeks Managed Vulnerability Scanning (MVS) Service provides continuous monitoring and risk prioritisation, **ensuring that vulnerabilities are identified before they can be exploited**.

KEY FEATURES

- **Continuous Threat Discovery:** Regular scanning to identify risks before attackers do
- **Real-World Threat Simulation:** Surfaces vulnerabilities that would be targeted by real-world attackers
- **Risk-Based Prioritisation:** High/Critical vulnerabilities are triaged, ensuring the most urgent threats get addressed first
- **Regulatory Compliance Support:** Helps meet security standards like ISO 27001, FCA, GDPR, with audit-ready reporting
- **Cloud, Remote & Hybrid Ready:** Designed for modern trading environments, low-latency platforms, and mobile workforces.

FULLY MANAGED SECURITY CYCLE

AUTOMATED INFRASTUCTURE SCANNING

Regular assessments of internal & external environments

LIGHT-TOUCH CONTINUOUS MONITORING

Scanning methods are non-intrusive, avoiding disruption to financial operations

CLOUD & ON-PREM SUPPORT

Offers both host-based scanning and traditional network scanning for flexible deployment

FAST REMEDIATION TIMEFRAMES

Identified vulnerabilities are made available within 4 business hours

COMPREHENSIVE VULNERABILITY TESTING

Includes network surveying, port scanning, firewall testing, and exploit verification

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

Here are three key areas where Beeks MVS stands out:

1. IDENTIFY & PRIORITISE SECURITY GAPS

- Detects vulnerabilities across internal & external infrastructure.
- Flags outdated software, misconfigurations, and unsupported OS.
- Identifies exploitable services, including remote access systems and outdated frameworks (e.g., PHP).

2. ADVANCED DETECTION & THREAT ACTOR SIMULATION

- Uses non-intrusive, continuous scanning to surface live hosts and services.
- Generates a complete map of publicly accessible services and their configurations.
- Highlights weak firewall rules, unpatched vulnerabilities, and high-risk exposures.

3. RISK-BASED REPORTING & ACTIONABLE INSIGHTS

- Security Dashboard for real-time vulnerability tracking.
- Common Vulnerability Scoring System (CVSS)-based prioritisation.
- Remediation guidance to reduce business risk and enhance security posture.

STAGE 1

Define your Assets

We work with your team to determine the IPs and URLs to be scanned

STAGE 2

Deploy Scanning Agents

Host-based scanning for cloud workloads or network-based scanning for traditional infrastructure

STAGE 3

Continuous Monitoring

Automated scans identify and score vulnerabilities based on risk impact

STAGE 4

Actionable Risk Reports

Risk dashboards and reports, including detailed remediation guidance

STAGE 5

Ongoing Support & Review

Our experts are available to assist with risk assessment and provide remediation advice to reduce exposure

WHY CHOOSE BEEKS MSV SERVICES?

◇ **Continuous Threat Discovery:**
Regular scanning to identify risks before attackers do

◇ **Real-World Threat Simulation:**
Surfaces vulnerabilities that would be targeted by real-world attackers

◇ **Risk-Based Prioritisation:**
High/Critical vulnerabilities are triaged, ensuring the most urgent threats get addressed first

◇ **Regulatory Compliance Support:**
Helps meet security standards like ISO 27001, FCA, NIS2, DORA, GDPR, with audit-ready reporting

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

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