VULNERABILITY SCANNING
Managed Security Services

KUDELSKI SECURITY

Protect your critical assets and shift the operational burden of identifying and prioritizing vulnerabilities to our Cyber Fusion Center.

Most cyber attacks exploit known vulnerabilities that could have been mitigated with regular security patches or software updates. Vulnerability scanning can dramatically improve cyber resilience by ensuring vulnerabilities are quickly identified, classified, and prioritized for remediation, before attackers have the opportunity to act. Managing such a program, however, requires a constant level of attention that most organizations find difficult to maintain.

Kudelski Security's Managed Vulnerability Scanning Service shifts the burden of scanning and prioritization to the Cyber Fusion Center (CFC) and allows clients to focus their attention on strategic priorities. Vulnerability scans provide clients the information they need to quickly and effectively prioritize mitigation and patching efforts, in order to significantly reduce risk.
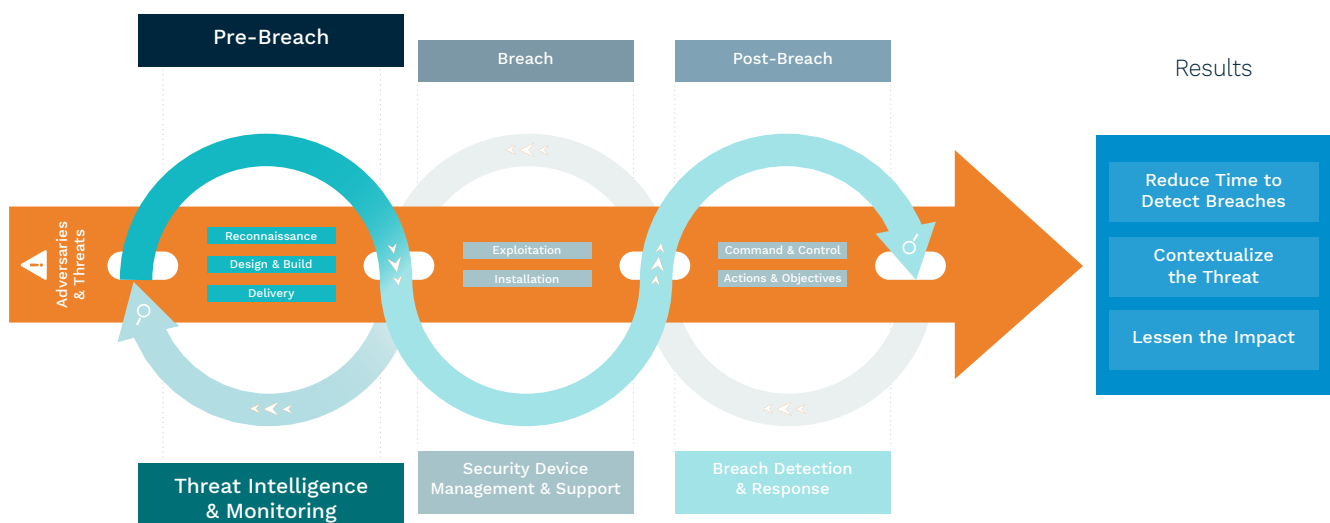
Vulnerability Scanning Service – How It Works

Kudelski Security's Vulnerability Scanning Service continuously identifies, classifies and analyzes vulnerabilities across your IT infrastructure, services, or web applications. If a critical security vulnerability is identified, the CFC will immediately notify your team and provide custom remediation recommendations.

Automated scan reports are generated by the CFC and delivered via the MSS Client Portal. Vulnerability scan reports include categorized scan results, prioritized by criticality, and remediation recommendations to facilitate mitigation activity by in-house IT operations teams.

Clients using both our Vulnerability Scanning and Threat Monitoring Services provide our CFC security analysts the business intelligence they need to identify and prioritize relevant threat activity against known vulnerable systems within their environments. This additional business intelligence allows the CFC Threat Analysis team to make smarter decisions, provide customized remediation recommendations based on vulnerability data, and reduce time to detection.

DISRUPTING THE KILL CHAIN WITH KUDELSKI SECURITY

How We Engage

Kudelski Security's Managed Security Services are built from the ground up, driving greater value to the client. They leverage a proven four-phase onboarding and operational process.

Phase 1: Pre-implementation

Project scope is defined, network architecture is reviewed and documented, and scan probes are deployed.

Phase 2: Implementation

The MSS Implementation team establishes connectivity to the scan probes, configures scans (scan scope, schedule, and policies), and tunes the scan engine.

Phase 3: Go-live

The CFC Threat Analysis team thoroughly validates the service to ensure smooth day-to-day operations and monitoring.

Phase 4: Ongoing Operations

Once the service is operational, CFC threat analysts monitor and manage the service daily through several activities:

- Health & performance monitoring for scan probes
- Change & configuration management
- Automated scanning notifications
- Notification of critical vulnerabilities
- Automated vulnerability scan reports with prioritized remediation recommendations (available via the MSS Client Portal)

Key Benefits

Kudelski Security's Vulnerability Scanning Service is powered by our 24x7x365 Cyber Fusion Center, with global reach, multilingual support and operations in the United States and Switzerland.

- Move to a proactive risk management and mitigation approach by leveraging prioritized vulnerability reports with clear remediation guidance

- Reduce operational costs and burden of running a vulnerability scanning program

- Meet regulatory and compliance requirements

- Get 24x7x365 guidance and support from our CFC expert analysts

- Access scan results, reports, dashboards and remediation recommendations from the MSS Client Portal, on demand

KUDELSKI SECURITY