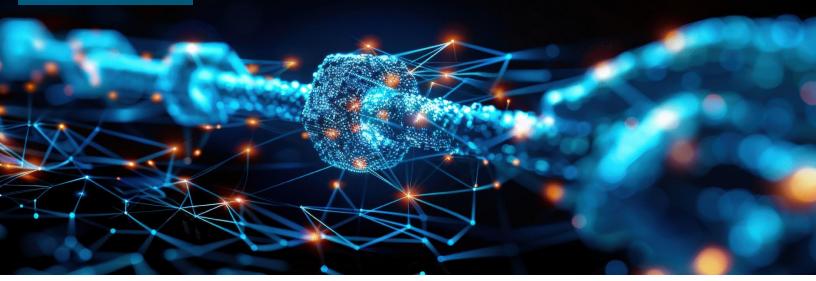# Discover and Remediate Cryptographic Vulnerabilities on Your Endpoints

CrowdStrike and InfoSec Global Federal (ISG) have joined forces to deliver next-generation cybersecurity solutions focused on cryptographic management, threat intelligence, and automated remediation. InfoSec Global Federal's AgileSec Analytics discovers, inventories, and analyzes all cryptographic assets across an agency's enterprise while replacing and remediating unauthorized, weak, or compromised assets. AgileSec Analytics integrates with the CrowdStrike Falcon platform by leveraging CrowdStrike Falcon Fusion workflows and real-time response (RTR) to seamlessly discover and retrieve cryptographic findings across all endpoints. With this cryptographic device context, AgileSec Analytics can identify cryptographic objects that are vulnerable to exploitation and replace those assets without any mission disruption.

Key Benefits

Threat Detection & Analysis
CrowdStrike's industry-leading threat intelligence enriched with cryptographic risk insights from ISG identifies and remediates cryptographic vulnerabilities before they become exploitable attack vectors.

Comprehensive Cryptographic Inventory
Gain current visibility into all cryptographic assets with a real-time, dynamic Cryptographic Bill of Materials (CBOM).

Automated Compliance & Remediation
Ensure cryptographic compliance through ISG's AgileSec analytics with automated policy enforcement.

Continuous Monitoring
CrowdStrike's File Integrity Monitoring (FIM) proactively detects and remediates weak, outdated, foreign, and other malicious algorithms for complete cryptographic security.

Automated Host Isolation
Prevent harmful lateral movement within systems to mitigate the spread of ransomware or other malware and prevent costly data exfiltration and exploitation.

Rapid Incident Response
Quickly contain, remediate, and recover from ransomware, exploited cryptographic objects, data breaches, and other cyberattacks.

Operational Efficiency and Reduced Human Error
Workflow automation reduces the need for manual intervention, enhancing speed and accuracy during incident response.
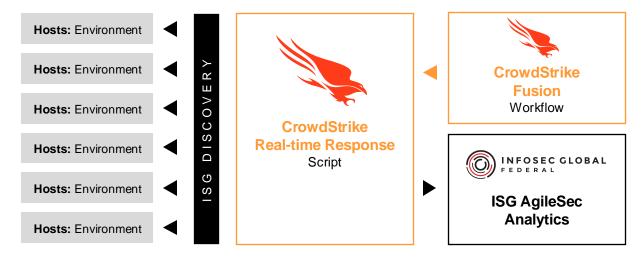
Seamless Integration
Extend threat analysis capabilities with cryptographic threat detection, lateral movement analysis, and advanced reporting.

Featured Use Case

Enhanced Vulnerability Discovery, Reporting, and Response

Integrating cryptographic inventory management capabilities with CrowdStrike Falcon capabilities, Fusion workflows, and real-time response helps government agencies maintain compliance with full visibility and control over all cryptographic assets. By enhancing CrowdStrike's threat detection with cryptographic analytics, agencies can identify and mitigate advanced cryptographic threats at the endpoint, enrich data with cryptographic threat insights, and remediate cryptographic vulnerabilities before adversaries exploit them.

Integration Architecture

Hosts: Environment

Hosts: Environment

Hosts: Environment

Hosts: Environment

Hosts: Environment

Hosts: Environment

ISG DISCOVERY

CrowdStrike Real-time Response
Script

CrowdStrike Fusion
Workflow

INFOSEC GLOBAL FEDERAL

ISG AgileSec Analytics

Value: Cryptographic Management

Discover
Cryptography Ecosystem

Analyze
Cryptographic Compliance, Security & Correlation

Automate
Cryptographic Processes

Hosts: Environment

Falcon Platforms

INFOSEC GLOBAL   CROWDSTRIKE   **Cryptographic Management**

Cryptographic Dashboards   Inventory (CBOM)   Vulnerabilities   Compliance   Threat Graph

- Compliance
- Response
- CM DB
- And More

Learn more at:
merlincyber.com

Contact:
info@merlincyber.com