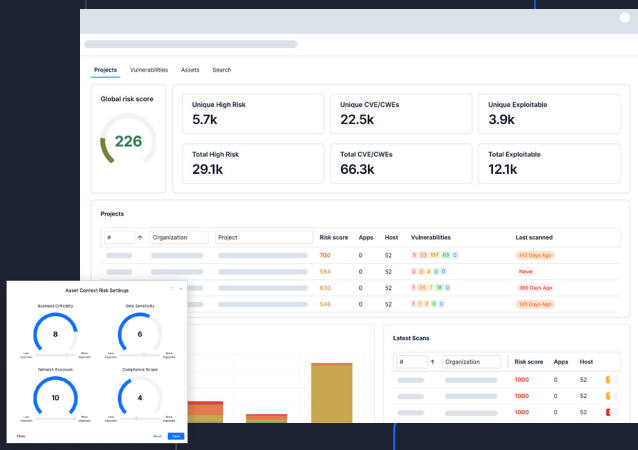
nucleus

Securing Your Mission, Advancing Your Cybersecurity Maturity

Government Grade Vulnerability and Exposure Management for Today's Digital Challenges



FR NIST FISMA

Trusted by Government Agencies

FedRAMP Moderate and fully compliant with key government frameworks, including **NIST, FISMA, CMMC**, and **Zero Trust**. Our platform has a proven track record of success across federal, state, and local government agencies.

Core Capabilities:

Continuous Risk Management: Gain complete visibility across your IT ecosystem with automated asset management. Nucleus helps you identify and prioritize critical vulnerabilities, delivering actionable insights for fast, effective risk mitigation.

Advanced Vulnerability Management: Advance from basic monitoring to scalable, automated workflows. Nucleus eliminates manual processes, helping security teams mature quickly and manage vulnerabilities efficiently.

Compliance and Auditing Excellence: Streamline audit prep with automated dashboards and reports. Nucleus captures every action and tracks risk mitigation to keep you continuously compliant with FISMA, NIST, and more.

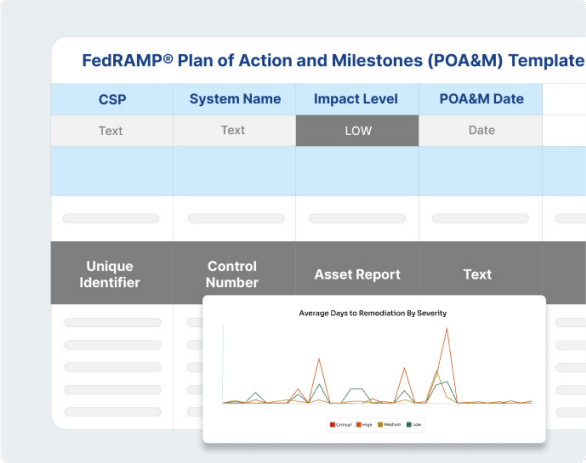
AI-Driven Vulnerability Intelligence to Act Faster, Smarter, and in Full Compliance

Federal teams are inundated with vulnerability data, but Nucleus leverages AI-driven enrichment and correlation to deliver the critical context needed for rapid, informed decision-making—dramatically reducing manual analysis and accelerating the full vulnerability management lifecycle.

By going beyond basic CVSS scores, Nucleus uses predictive exploit intelligence trained on global threat data to help agencies anticipate which vulnerabilities are most likely to be weaponized, even before appearing on standard watchlists.

Synthesizing real-time exploit data, malware analysis, security advisories, and the CISA KEV catalog, Nucleus provides highly contextualized, actionable intelligence that enables agencies to prioritize the most immediate threats, optimize remediation efforts, and meet federal mandates like **FISMA, EO 14028, and CISA BOD 22-01** with greater speed and efficiency.

"Nucleus uses predictive exploit intelligence trained on global threat data to help agencies anticipate which vulnerabilities are most likely to be weaponized..."



Key Capabilities

1. Risk-Based Prioritization Aligned with CISA BOD 22-01:

Automatically identify and prioritize KEVs by cross-referencing scan data with CISA's catalog, enabling rapid remediation of high-risk vulnerabilities and ensuring BOD 22-01 compliance.

2. Automated Asset & Vulnerability Data Aggregation:

Aggregate data from diverse tools to create a unified, real-time view of assets and vulnerabilities, accelerating compliance with BOD 23-01 and laying the groundwork for Zero Trust (OMB M-22-09).

3. Automated POA&M Management for FISMA Readiness:

Streamline the creation and tracking of POA&Ms linked to vulnerabilities, reducing manual effort and supporting continuous monitoring in line with NIST SP 800-53 and FISMA.

4. Workflow Automation to Accelerate Remediation:

Route high-priority vulnerabilities to the right teams instantly via integrations with systems like ServiceNow or Jira, cutting remediation timeframes and supporting EO 14028 and BOD 22-01 goals.

5. Simplified Compliance & Executive Reporting:

Generate dashboards and reports on vulnerability status, remediation efforts, and POA&M progress to support FISMA, NIST 800-53, and SA&A activities with minimal manual effort.

Why Choose Nucleus?

Scalable & Automated: Seamlessly handle growing security needs with automated tools that evolve alongside your agency's cybersecurity maturity.

Centralized Control: Consolidate vulnerability management, compliance tracking, and reporting into one unified system for better efficiency and clarity.

Secure, Future-Ready Protection: Stay ahead of the evolving cyber threat landscape with continuous monitoring and proactive risk monitoring strategies.

CMMC Compliance Checklist

Nucleus meets key CMMC requirements, including:

- ✓ **Configuration Management (CM):** Ingests and normalizes asset data, tracks and alerts on mis-configuration findings, identifies risky, blacklist and unauthorized software.
- ✓ **Risk Management (RM):** Prioritizes vulnerabilities based on exploitability, severity and asset importance.
- ✓ **Security Assessment (SA):** Automated continuous correlation supported with built-in risk acceptance, ticketing integration and workflow management as a POA&M.

Take the Next Step in Cybersecurity Maturity

See how Nucleus can protect your agency, accelerate your security transformation, and ensure compliance with evolving regulations.

Request a Demo Today