nucleus

NUCLEUS: A FORCE MULTIPLIER FOR AGENCY CYBER DEFENSE

Operational Efficiency in Federal Vulnerability Management

Federal Cybersecurity Teams Face Mounting Pressure

Digital attack surfaces are expanding, regulatory mandates are tightening, and personnel resources remain constrained. Nucleus acts as a force multiplier—streamlining vulnerability management operations from ingestion to closure to help agencies maintain mission resilience at scale.

By operationalizing compliance with frameworks such as FISMA, NIST RMF, and CISA BOD 22-01, Nucleus empowers federal agencies to accelerate risk reduction with fewer resources—without compromising auditability, mission assurance, or operational continuity.

Real-World Federal Efficiency Gains

- **80% reduction in analyst triage workload** through automation and normalized data views
- **50% drop in high-risk vulnerability exposure** within 90 days using contextual prioritization
- **Automated remediation workflows** integrate with existing ticketing systems, cutting cycle times

Fulfill Mandates with Minimal Overhead

Nucleus aligns with critical federal cybersecurity directives and control frameworks—enabling agencies to meet strategic and statutory requirements without adding operational burden.With Nucleus, Federal agencies gain clear auditability, reduced manual tracking, and faster time to compliance.

- **EO 14028 & OMB M-22-09**: Supports modernization and Zero Trust architecture through centralized asset visibility, cross-system correlation, and automated remediation workflows
- **CISA BOD 22-01 & Known Exploited Vulnerabilities (KEV) Catalog**: Provides continuous tracking of KEV exposure, remediation timelines, and SLA adherence across assets and enclaves
- **FISMA & NIST SP 800-53 / NIST SP 800-37 (RMF)**: Automates POA&M generation and lifecycle tracking, supports continuous monitoring (ConMon), and enforces SLA deadlines for finding closure
- **CNSSI 1253/IC NIST Overlay**: Supports mapping to intelligence community-specific control baselines for high-assurance environments
- **DoD RMF & STIG Alignment**: Facilitates control mapping and remediation tracking for systems subject to DISA STIGs and DoD RMF compliance

Unified Ingestion and Normalization

- Consolidates vulnerability and asset data from over 160 sources—including Tenable, Qualys, Rapid7, AWS, and GitHub—into a centralized system of record.
- Normalizes findings into a unified schema, enabling correlation across disparate tools without manual reconciliation.
- Supports OMB M-22-09, EO 14028, and NIST SP 800-137 by enabling asset visibility and cross-domain data integration. mitigation is infeasible, keeping teams focused work.

Context Aware Prioritization

- Enriches vulnerabilities with overlays from CISA KEV, EPSS, commercial threat intel, and internal asset criticality tags.
- Enables agencies to define mission-aligned scoring logic based on business impact, enclave classification, or system criticality.
- Operationalizes FISMA and NIST SP 800-53 RA-3 (Risk Assessment) and RA-5 (Vulnerability Scanning) controls by supporting, risk-based decision making.

Workflow Automation Across the Lifecycle

- Automates remediation routing based on asset tags, mission context, severity, and ownership—minimizing triage delays and handoff risk.
- Pushes prioritized findings into Jira, ServiceNow, or Azure DevOps with full bidirectional sync, aligning with existing ITSM workflows.
- Auto-generates POA&Ms, enforces SLA deadlines, and ensures lifecycle tracking—fulfilling requirements from NIST SP 800-37 (RMF), FISMA, and FedRAMP Continuous Monitoring obligations.

AI-Driven Enrichment and Decision Support

- Applies machine learning to map vulnerabilities against exploitability indicators, threat actor TTPs, and real-time asset posture.
- Surfaces pre-KEV vulnerabilities likely to be exploited, allowing defenders to preempt threat activity and shrink exposure windows.
- Supports CISA BOD 22-01 (Reducing the Significant Risk of Known Exploited Vulnerabilities) by filtering noise and ensuring attention on exploitable threats.

Deployment Aligned to Federal Environments

- ✓ Supports air-gapped, self-hosted, AWS GovCloud, and hybrid deployments
- ✓ Fully compatible with multi-tenant and classified enclave models
- ✓ Offers role-based access control and strict data segmentation by project or agency
- ✓ FedRAMP Moderate Authorized to meet federal cybersecurity and compliance mandates

Efficiency is Now a Security Imperative

Manual, siloed approaches to vulnerability management are not scalable. Nucleus delivers measurable efficiency gains for agencies tasked with defending critical systems at national scale. It centralizes operations, prioritizes by risk, and automates at every stage—allowing federal cyber programs to reduce dwell time and improve outcomes without expanding staff or tools.

If you're assessing platforms to modernize vulnerability management with minimal operational overhead, Nucleus is already delivering at scale across intelligence missions and civilian public service.

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