nucleus

DATASHEET

Nucleus Insights

AI-Powered Exploit & Threat Intelligence for Vulnerability Management and Security Operations

FROM NOISE TO THREAT-INFORMED ACTION

Reduce Exposure, Disrupt Kill Chains, and Prevent Breaches

Cut Through the Noise of Traditional Threat Feeds

Traditional threat intelligence feeds were never designed to support the day-to-day vulnerability management operations. Multiple sources that inundate security teams with constant streams of conflicting data simply add to the noise.

Nucleus Insights, an AI-enriched, analyst-curated exploit and threat intelligence feed, is purpose-built for vulnerability management and security operations.

Nucleus Insights, an AI-enriched, analyst-curated exploit and threat intelligence feed, is purpose-built for vulnerability management and security operations. It consolidates CVE disclosures, CISA KEV updates, exploit-chatter, threat actor, and malware activity into actionable enrichment that's embedded across the Nucleus Platform, VIP, and API.

Each vulnerability is scored with the Nucleus Threat Rating (NTR), a dynamic, daily indicator of real-world exploit pressure, allowing teams to enforce SLAs, auto-ticket, and drive fixes at scale.

Business Outcomes

Prevent Ransomware Attacks

Pin-point vulnerabilities that can lead to ransomware before they are exploited.

Reduce Exposure Faster

Focus remediation on what's actively exploited or most likely to be next.

Disrupt Exploit Chains

Pin-point vulnerabilities that can lead to ransomware before they are exploited.

Automate at Scale

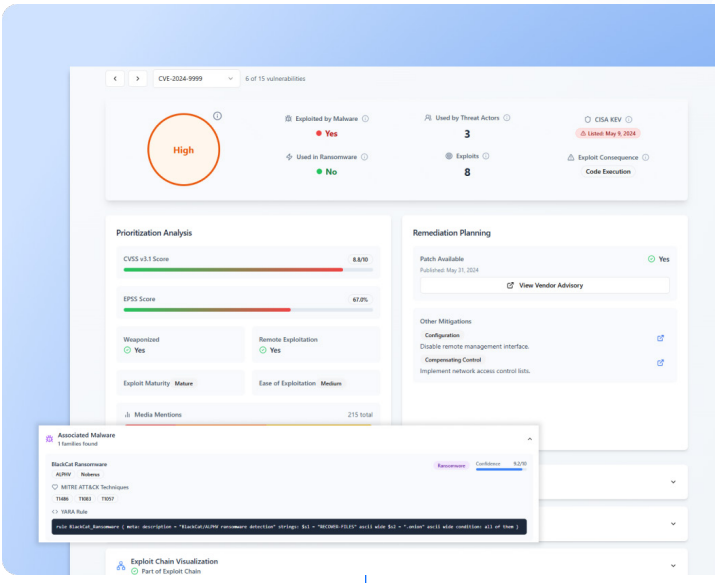
Use Threat Indicators and NTR thresholds to route, ticket, and enforce policy across tools and teams.

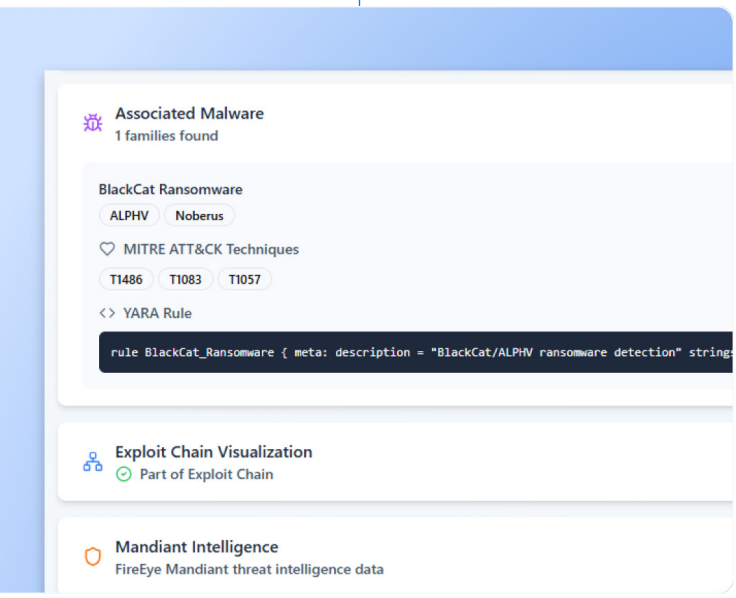
Integrate Your Stack

Embedded in Nucleus and available via API.

Key Capabilities

- **AI-enriched, expert curated:** AI-Powered Context & Threat Enrichment expertly curated and validated.
- **Executive Summary:** Brief, exec-ready description of the vulnerability, relevant threat groups, and malware.
- **Expert Analysis:** Deep dive on exploit technique, observed activity, and operational implications.
- **Operational Exploitability Flags:** Exploited, Likely to be Exploited, Public Exploit Available, Exploited by Malware, Impacts OT.





- **Exploit-Chain Enrichment:** CVEs commonly chained, including in Ransomware attacks, with the primary CVE (pre-exploit enablers, co-exploitation, post-exploitation escalation/lateral movement/persistence/exfiltration).
- **Indicators of Compromise (IOCs)**: Known IOCs to accelerate threat hunting and SOC workflows.
- **Branded Names & Media Mentions:** Popular names, mention volume, and source coverage to inform comms and executive briefings.
- **OT/IoT Impact:** Flags issues affecting ICS/SCADA/IoT.

Exploit & Malware Signals

- **Exploit Availability & Difficulty:** Public vs. private availability; difficulty from Very Easy → Very Hard.
- **Observed & Remote Exploitation:** In-the-wild status and internet-reachability.
- **Zero-day Status & Consequence:** Code/command execution, data exfiltration, DoS, unauthorized access, privilege escalation, service disruption.
- **Malware & Ransomware Usage:** Malware categories leveraging the CVE; YARA rules (when available); MITRE ATT&CK mappings.

Mitigation Intelligence

- **Mitigation Type:** Patch, configuration change, IPS/IDS signature, segmentation, disable feature, user education, monitoring/detection.
- **Mitigation URL & Description:** Linked guidance for execution in IT/OT workflows.

Threat Group Context

- Aliases, Industries/Sectors, Motivations
- References & ATT&CK Techniques
- Group-specific IOCs

Nucleus Threat Rating (NTR)

A daily, threat-centric label that complements severity and contextual risk, capturing real attacker behavior for every CVE, not just those scored by NVD.

Level	Operational Guidance
Existential	Immediate, org-wide risk; treat as an incident and coordinate with IR.
Critical	Confirmed in-the-wild exploitation (often ransomware/KEV); enforce urgent SLAs.
High	Strong evidence (public PoCs, lower-sophistication actor use); prioritize by exposure and business context.
Medium	Limited evidence; monitor for escalation and triage by asset criticality.
Low	No known exploitation; defer unless business context elevates risk.

How It Works

- **Aggregate signal:** Public and proprietary exploit telemetry, commercial feeds, and OSINT.
- **AI + experts:** AI assists analysis and drafting; Nucleus experts validate the signal.
- **Continuously refreshed:** NTR updates frequently to capture shifts in exploitation and is embedded across the Nucleus Platform, VIP, and API.

Where Teams Use It

- **Prioritization & SLAs:** Trigger tickets when NTR ≥ Critical or when exploitation flags trip.
- **Operations & Reporting:** Filter “Active Vulns,” brief leadership on real exposure, verify remediation.
- **Early Warning:** Track vendor/tech-stack risk and KEVs in real time.

Why Nucleus?

Threat Signal You Can Automate

Daily NTR and exploit flags (Exploited, Public Exploit, Exploited by Malware, Impacts OT) are embedded across the Nucleus Platform, VIP, and API's so you can trigger tickets, enforce SLAs, and orchestrate fixes automatically.

Enterprise Scale Operations

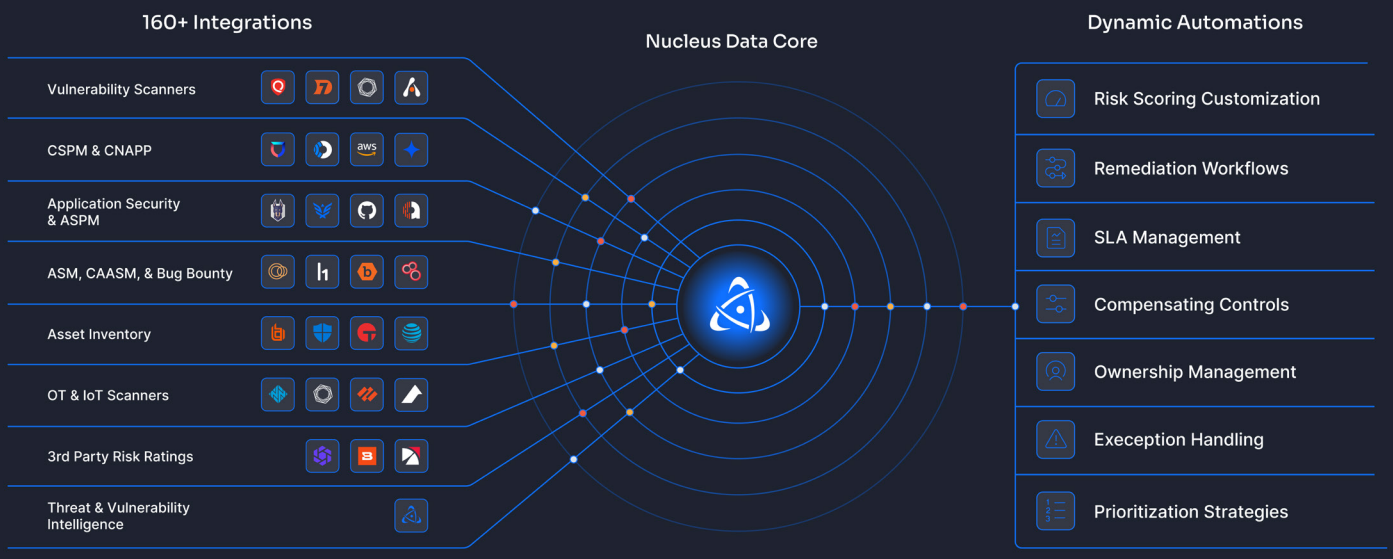
160+ integrations via FlexConnect, patent-based de-duplication and normalization, bi-directional ticketing (Jira/ServiceNow/GitHub/ADO), and an unlimited API keep data clean and workflows moving.

Trusted By Leaders

400+ organizations across the commercial and public sectors rely on Nucleus to reduce exposure at scale.

Public Sector Ready

FedRAMP-compliant options: AWS GovCloud multi-tenant, dedicated GovCloud, or self-hosted/air-gapped deployments.



Proven Outcomes

86% reduction in critical vulnerabilities at a Tier-1 airline.

92% remediation rate and 30% faster response at a global health enterprise.

89% remediation of millions of findings, powered by 200+ automation workflows and 22+ M&A onboarded at a Fortune 500 payments company.

nucleus

Nucleus transforms vulnerability and exposure management for enterprises and government agencies by unifying data, automating workflows, and enabling faster, scalable risk mitigation. Founded in 2019 by former Department of Defense security experts, Nucleus is trusted by over 400 organizations, including Motorola, Paychex, and Mastercard. Our platform is designed by practitioners, for practitioners, to simplify complex vulnerability management processes and deliver measurable impact.

mastercard. CBRE American Airlines motorola DELTA DENTAL

www.nucleussec.com | hello@nucleussec.com

Version 1.0 | Published May 2025

Get a Demo