nucleus

NUCLEUS CASE STUDY

How a Global Health Enterprise Scaled Risk Reduction with Nucleus

1 Customer Overview

Overview

Customer: Global Health Company

Location: United States

Solution

The Nucleus Security Platform

Business Impact

- **92% vulnerability remediation rate**, driven by automation and risk-based prioritization
- **30% faster response times**, accelerating remediation of critical vulnerabilities
- **110K+ assets normalized**, improving CMDB accuracy and visibility
- **Reliable ticketing automation**, reducing errors and improving SLA compliance

"One of our biggest challenges was trusting the data. Scans uncovered assets missing from the CMDB, and even known assets lacked critical details—like ownership or business importance. That made it nearly impossible to assign tasks accurately or focus on what truly mattered. With Nucleus, we finally have clear ownership and can prioritize patching based on real risk."

-Director of Vulnerability Management

About the Customer

A large health organization operating in more than 100 countries. The company offers portfolio of medicines, vaccines, diagnostics, and technologies that help predict, prevent, detect, and treat diseases.

The Challenge: Overcoming Security Silos and Manual Processes

As the organization adopted new scanning tools to improve their security coverage and risk visibility, a new challenge emerged: scale. Vulnerability data volumes multiplied—but the underlying processes for analysis, validation, prioritization, and ticketing remained manual. These outdated processes quickly became a bottleneck. Teams were overwhelmed by labor-intensive steps, prone to human error, and unable to keep pace with the flood of new findings. To make matters worse, the vulnerability prioritization lacked both organizational context and threat intelligence. It failed to reflect the real-world risk to the business. Without focused guidance, remediation teams wasted valuable time chasing false positives. As a result, critical exposures were often missed, while effort was wasted on issues that posed little to no threat. it harder to drive accountability and demonstrate program outcomes to the executive leadership teams.

"With so many vulnerabilities, understanding what to fix and how our risk was impacted was nearly impossible. We couldn't keep working this way. Nucleus provided the scalable risk-based automation we needed take our program to the next level."

2 Nucleus Solution

The Solution: Nucleus Security Platform

The customer selected Nucleus as the backbone of their vulnerability and exposure management program to effectively scale risk-based workflows. Nucleus provided the platform capabilities to unify, prioritize, and operationalize vulnerability data—across tools, teams, and environments. By consolidating data from their core scanners, asset inventories, CI/CD pipelines, and threat intelligence feeds, Nucleus transformed fragmented signals into a centralized, actionable dataset that teams could trust.

Unified Data Core

Nucleus normalized and deduplicated findings across infrastructure, application, and cloud environments—delivering a single source of truth for risk decisions.

Native Ticketing Integration

Integrated directly with systems like Jira and ServiceNow to embed remediation into the engineering lifecycle—automating ticket creation, enrichment, and policy-based closure criteria.

Dynamic Asset Grouping

Automatically organized assets into meaningful, flexible groups based on tags and metadata such as business units, environments, or ownership. This enabled precise scoping of risk, automation, and reporting.

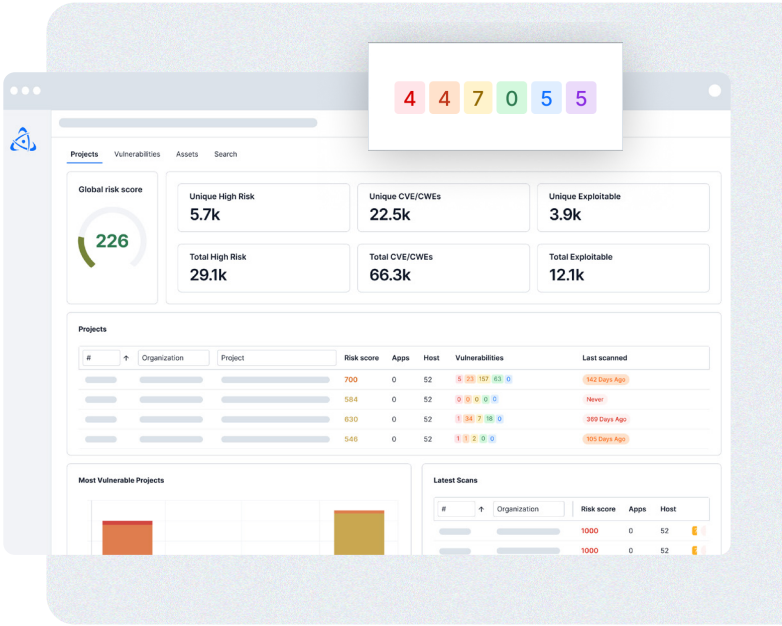
Risk-Based Automation

Replaced fragile manual workflows with adaptive automation. Ownership, escalation, and ticketing scaled cleanly across business units without rule sprawl or operational drag.

Contextual Risk Scoring

Applied dynamic, transparent scoring that combined vulnerability intelligence with business-specific context. This enabled teams to prioritize based on true organizational risk not just CVSS scores.

Nucleus provided the platform capabilities to unify, prioritize, and operationalize vulnerability data across tools, teams, and environments



3 Business Outcomes

Business Quantified Risk Reduction and Operational Gains

Since deploying Nucleus, the organization has realized significant improvements in remediation effectiveness, asset visibility, and process efficiency:

- **92% remediation rate** across all discovered vulnerabilities, demonstrating high operational throughput powered by automation.
- **Accelerated time-to-remediate** cutting response times by over 30% compared to historical baseline.
- **Improved CMDB accuracy** with 110,000+ assets consolidated and normalized..
- **Automated reliable ticket assignments** boosting trust, reducing errors and driving SLA compliance.

> There were significant improvements in remediation effectiveness, asset visibility, and process efficiency.

Strategic Outcome: Scalable Risk Reduction

At an organizational level, Nucleus enabled the enterprise to fully automate ticketing throughout the vulnerability management lifecycle. Manual handoffs were eliminated. Tickets were automatically created, enriched, prioritized, and routed to the appropriate teams—accelerating remediation and reducing operational overhead across the board.

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 500 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