



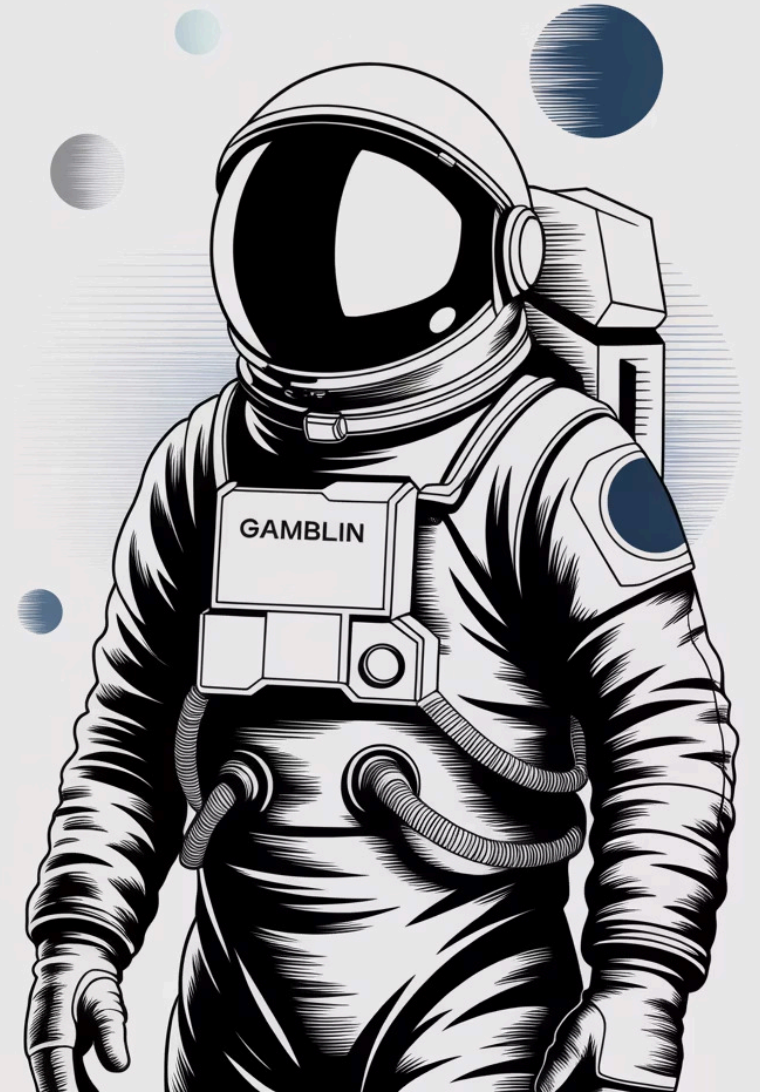
Navigating the CVE Crisis: The State of Vulnerability Disclosure

Our vulnerability disclosure ecosystem is under unprecedented pressure.

Meet Jerry Gamblin

A security researcher, builder, and hacker, Jerry Gamblin is a passionate advocate for robust vulnerability management. He is an industry-recognized visionary who applies hands-on expertise to solve complex security challenges through code and strategic communication. His work focuses on developing innovative open-source solutions to ensure digital resilience in an evolving threat landscape.

- Speaker at leading industry conferences.
- Founder of RogoLabs, an open-source venture focused on creating tools for vulnerability intelligence.
- Creator of open-source projects like cve.icu, cveforecast.org, and cnascorecard.org which are designed to bring clarity to vulnerability data.
- Author and contributor to numerous cybersecurity publications and a widely featured blogger and security researcher.





US Program Crisis

Examine CVE funding issues, NVD backlogs, and CISA's evolving role in our traditional ecosystem.



Global Alternatives

Explore rising players like ENISA and alternative vulnerability databases across the galaxy.



Navigation Strategies

Chart your course through this fragmented landscape with actionable guidance.



The Perfect Storm: Multiple Systems Under Pressure

CVE Funding Crisis

Near-critical resource shortage threatens program stability and consistency.

NVD Backlogs

Analysis delays create widening vulnerability windows for organizations.

Volume Explosion

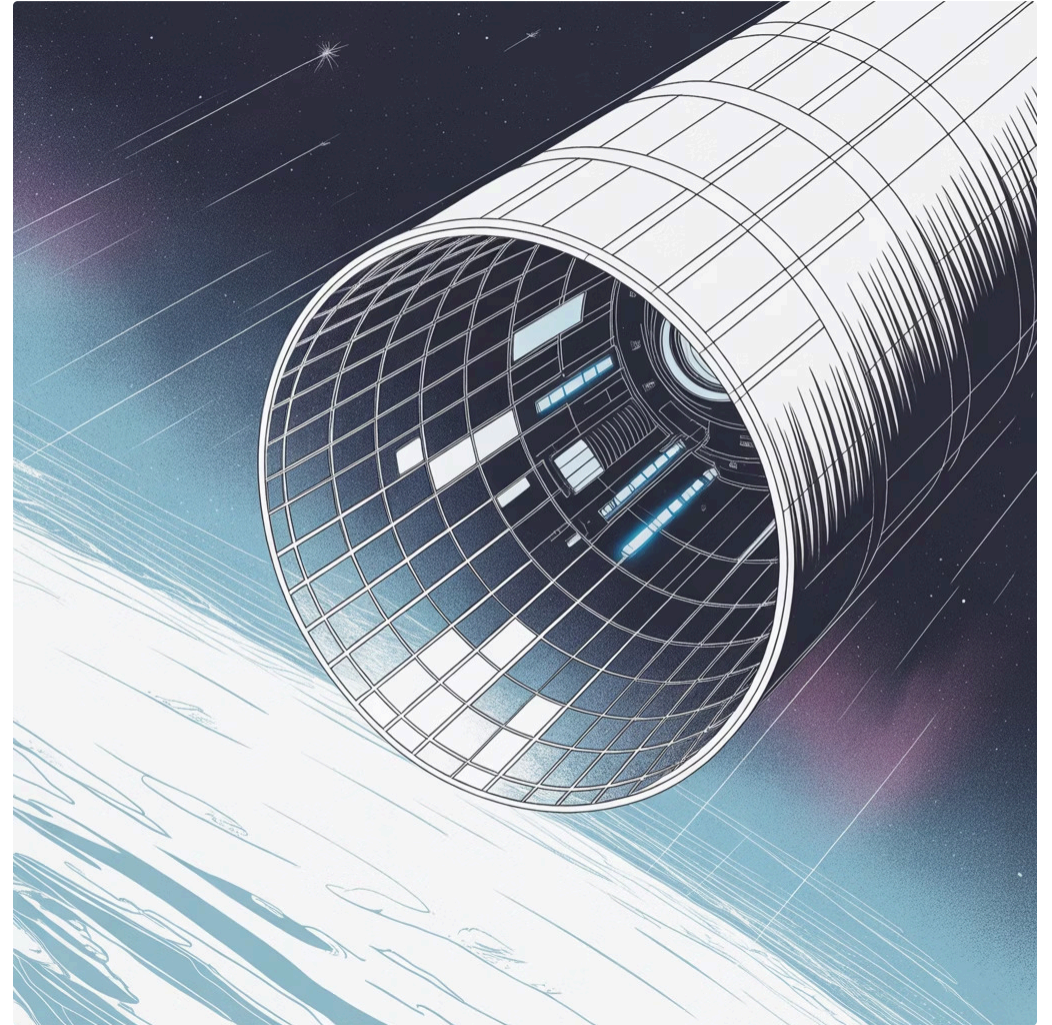
Exponential growth in vulnerabilities overwhelms existing infrastructure.

CVE Program: Mission Critical Systems Failing

The Foundation We Depend On

CVE serves as the universal identifier system that powers vulnerability management across the industry. When this foundation shakes, everything built on top becomes unstable.

- Industry-wide dependency on CVE IDs
- Critical for compliance frameworks
- Essential for tool integration



The Funding Crisis

Resource Constraints

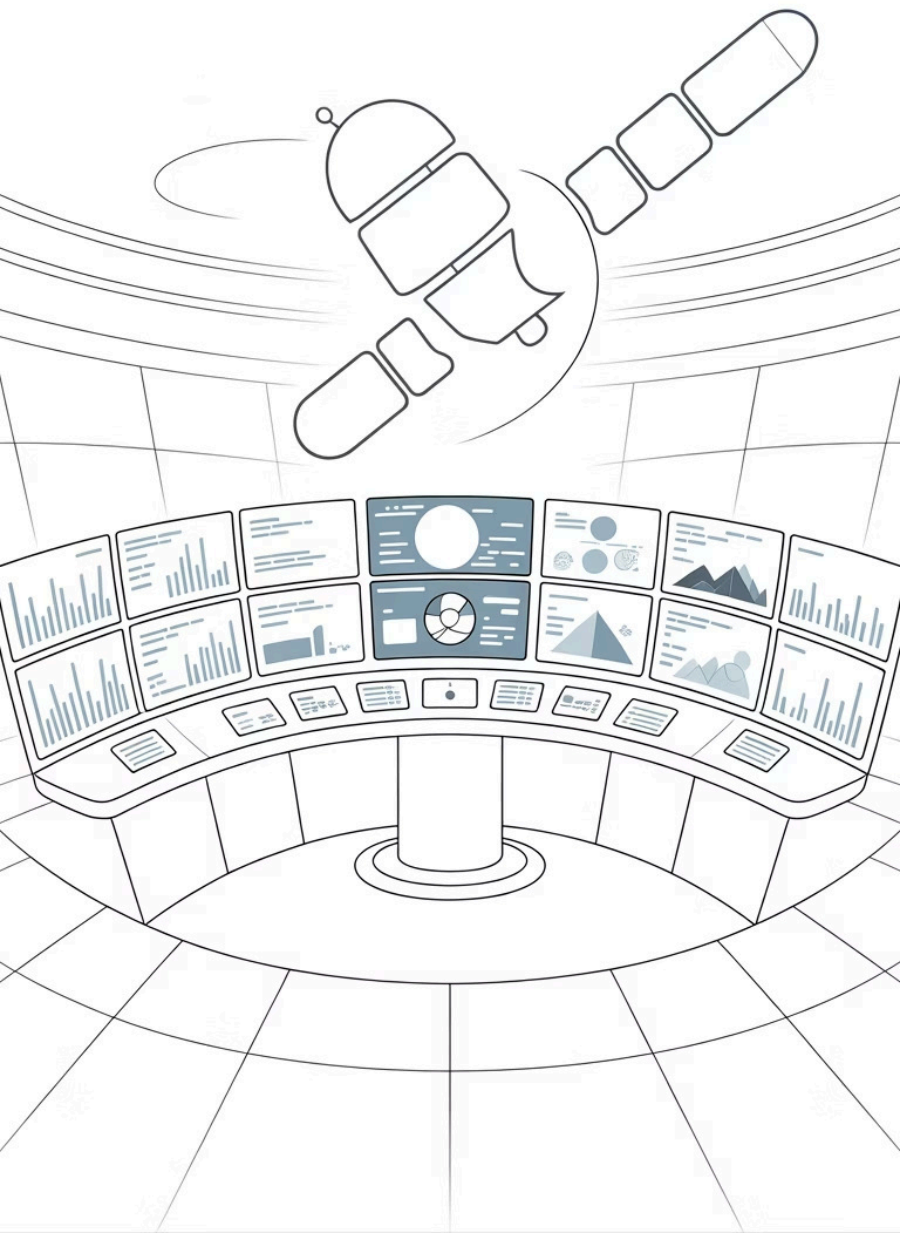
Inadequate funding threatened operational continuity and forced difficult prioritization decisions across the program.

Assignment Inconsistencies

Reduced capacity led to delays and quality variations in CVE assignments, impacting downstream users.

Cascading Effects

Problems rippled through the entire vulnerability management ecosystem, affecting tools and processes.



NVD: Houston, We Have a Backlog

15K+

Unanalyzed CVEs

Vulnerabilities waiting
for enrichment and
scoring

120+

Day Delays

Average time from
publication to analysis
completion

40%

Coverage Gap

Vulnerabilities lacking
complete CVSS
scoring

CISA: Adapting to Fill the Void



KEV Catalog

Known Exploited Vulnerabilities list provides critical prioritization data



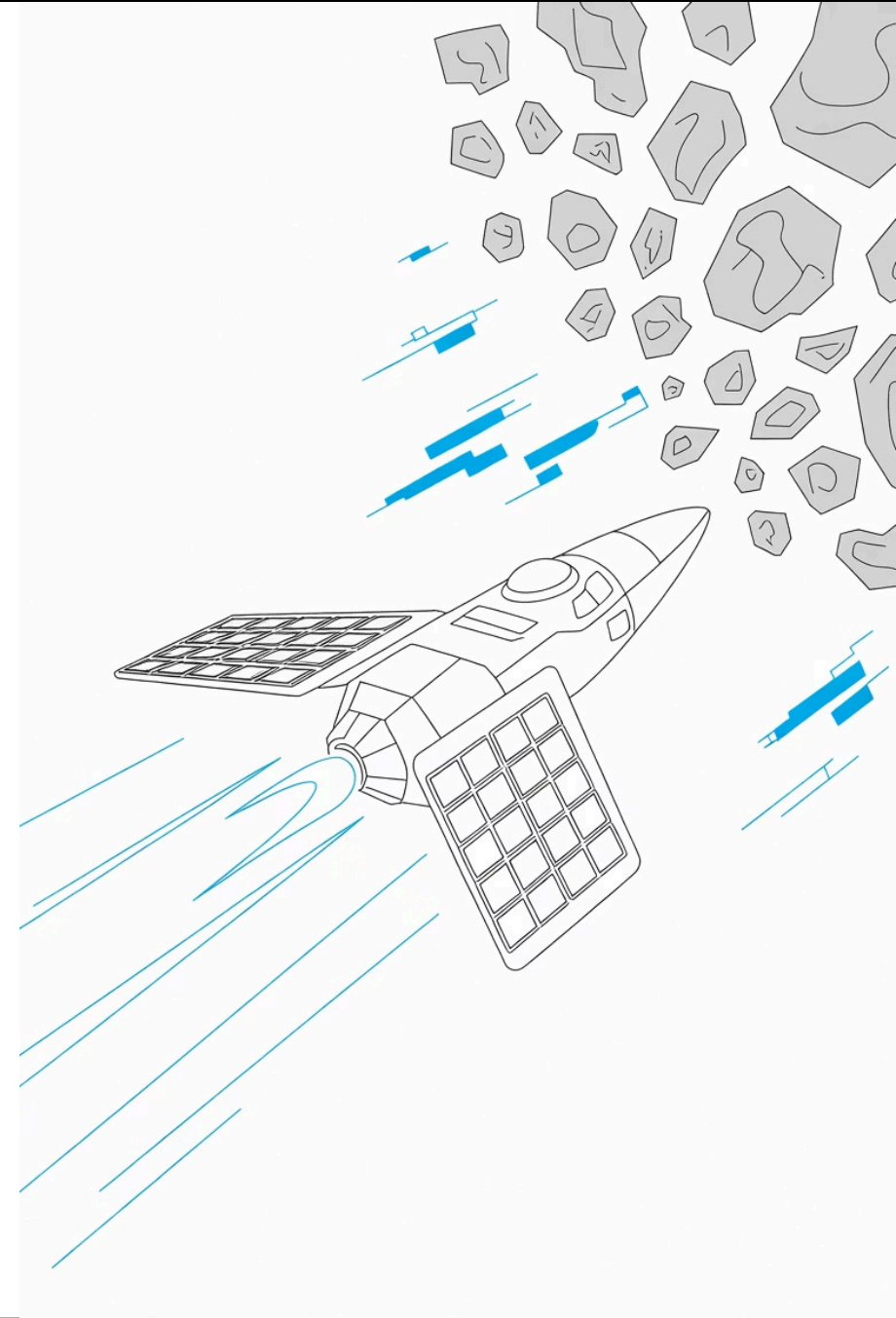
Direct Advisories

Independent vulnerability alerts bypass traditional channels



Industry Coordination

Enhanced communication with vendors and security community



Impact on Security Professionals

1

Increased Workload

Manual research and validation required to fill data gaps left by delayed or incomplete vulnerability information.

2

Prioritization Struggles

Without timely CVSS scores and enrichment data, risk assessment becomes significantly more challenging.

3

Trust Erosion

Inconsistent data quality forces teams to seek alternative sources and validation methods.



New Players Enter the Galaxy

As traditional systems struggle, innovative alternatives emerge to fill critical gaps in vulnerability intelligence.

ENISA: Europe's Rising Star

Strategic Mandate

EU Agency for Cybersecurity positions itself as a key coordinator for European vulnerability management efforts.

- Threat landscape reporting
- Cross-border coordination
- Strategic guidance for member states
- Industry collaboration initiatives



ENISA provides a regional alternative that complements but sometimes diverges from US-centric approaches.

The Alternative Database Constellation



Commercial Solutions

Platforms like Vulners and VulnDB offer enhanced data, faster updates, and commercial-grade reliability.



Open Source Initiatives

OSV.dev and GitHub Advisories provide community-driven vulnerability intelligence with developer focus.



National CSIRTs

Country-specific computer security incident response teams offer localized intelligence and rapid response.

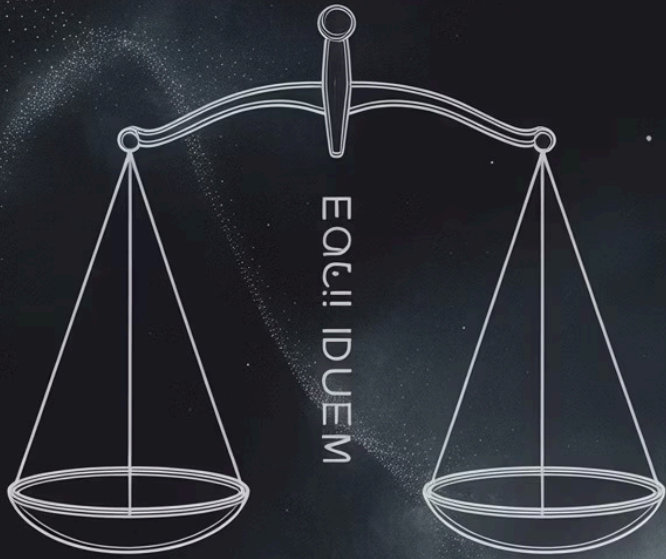
Comparative Analysis: Strengths vs. Weaknesses

Advantages

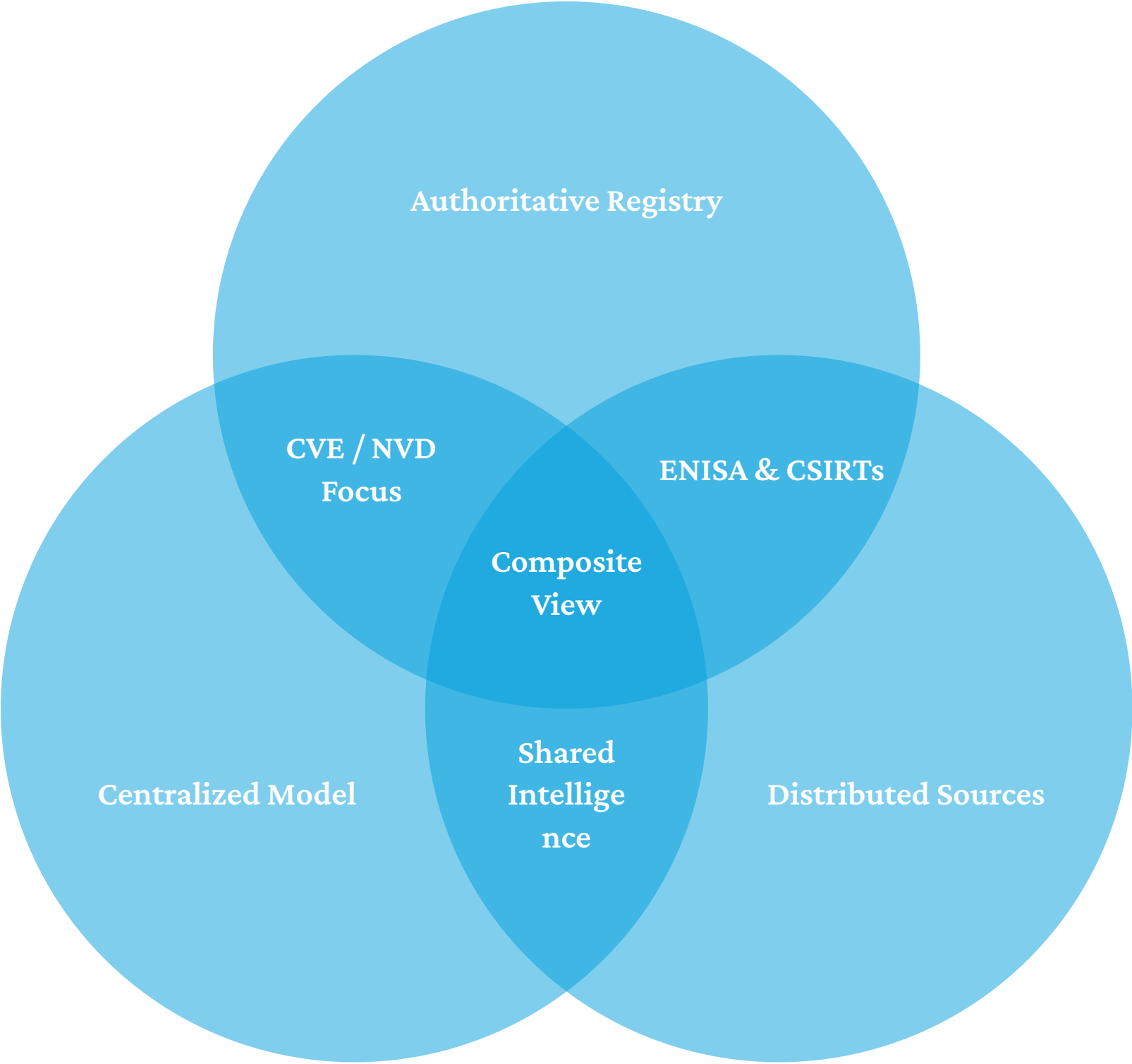
- Faster publication and analysis
- Specialized domain coverage
- Enhanced contextual information
- Reduced dependency on single source
- Innovation in data presentation

Challenges

- Data quality inconsistencies
- Potential commercial bias
- Integration complexity
- Cost considerations
- Lack of standardization

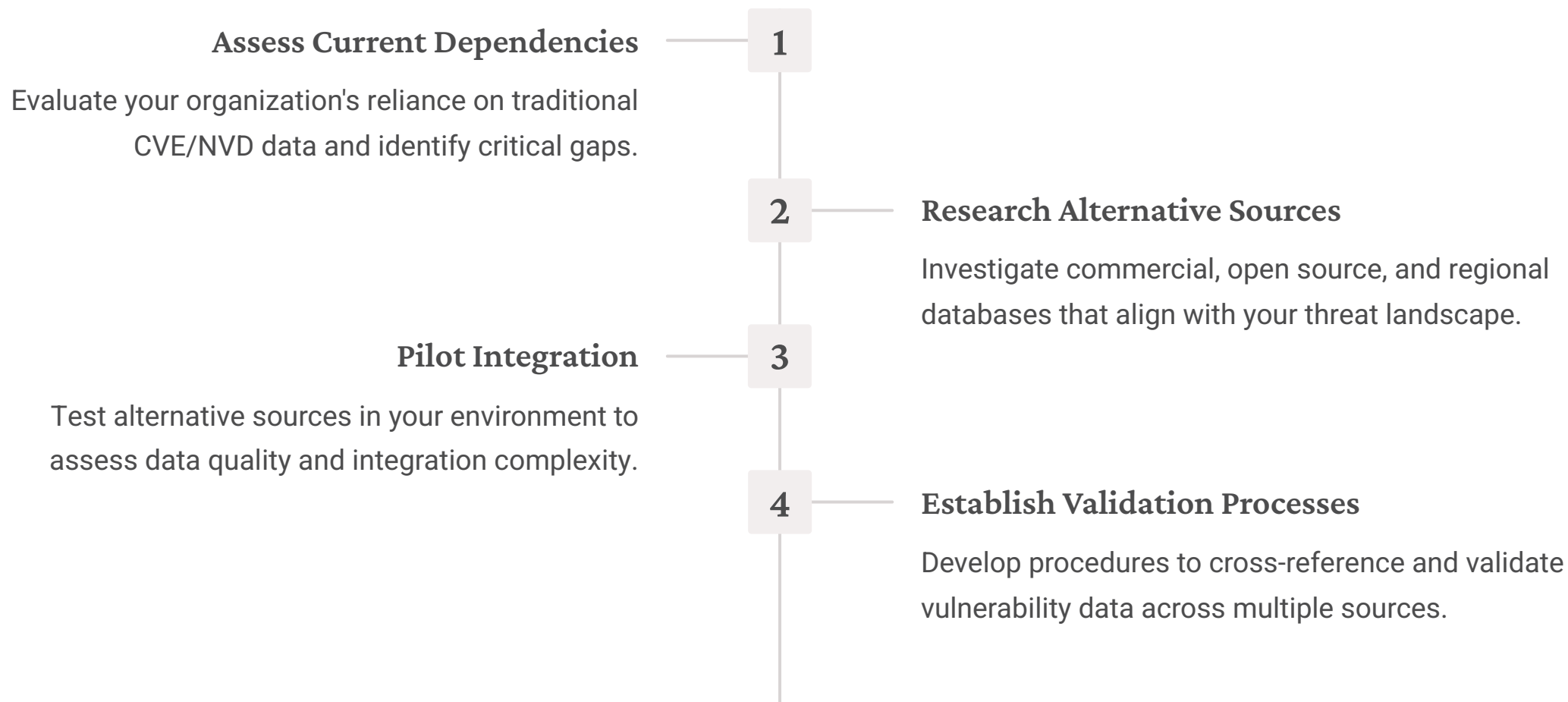


The Fragmenting Universe



The shift from centralized to distributed vulnerability intelligence creates both opportunities and challenges for practitioners.

Mission Planning: Diversify Your Intelligence Sources



Prioritization in the New Era

Context Over Scores

Focus on exploitability data and threat intelligence rather than relying solely on CVSS ratings.

KEV Integration

Leverage CISA's Known Exploited Vulnerabilities catalog for immediate prioritization guidance.

EPSS Adoption

Incorporate Exploit Prediction Scoring System data for probability-based risk assessment.



Tools for the Multi-Source Reality

1

Data Aggregation Platforms

Implement tools that can collect and normalize vulnerability data from multiple sources automatically.

2

Correlation Engines

Deploy systems that can identify relationships and duplicates across different vulnerability databases.

3

Quality Scoring Mechanisms

Establish metrics to evaluate and weight the reliability of different vulnerability sources.

Future Mission Trajectory

1

Reform Potential

Traditional systems may stabilize with increased funding and modernization efforts.

2

AI Integration


Automation and machine learning will accelerate vulnerability analysis and dissemination.

3

Federated Models

Collaborative frameworks may emerge to standardize and coordinate global vulnerability intelligence.

Key Takeaways for Your Mission



Embrace the Multi-Source Reality

The days of single-source vulnerability intelligence are ending. Diversification is now a necessity, not a luxury.



Context Beats Convenience

Prioritize exploitability and threat intelligence data over traditional scoring methods for better risk assessment.



Prepare for Continued Evolution

The landscape will keep changing. Build flexible processes that can adapt to new sources and methods.

Safe Travels, Space Rangers

The vulnerability disclosure ecosystem is evolving rapidly. By understanding these changes and adapting our approaches, we can navigate this complex landscape and maintain strong security postures despite the challenges.

- ❏ Remember: In this new reality, adaptability and diversification are your most valuable navigation tools.

