Navigating the Volatile Vulnerability Landscape

Building resilience in an era of fragmented intelligence and regulatory divergence

BSides Munich 2025

November 17th, 2025

A Little About Me

I am a security researcher and data scientist, focusing on vulnerability management. I run a personal innovation lab called Rogolabs.net, where I develop and share open-source tools and independent research with the cybersecurity community.

Research & Innovation

My work primarily focuses on vulnerability management, where I develop open-source tools and conduct independent research through Rogolabs.net.

Community Contributions

I contribute to the CVE Program and am part of the Exploit Prediction Scoring System (EPSS) Special Interest Group (SIG).

Public Speaking

I enjoy speaking at conferences, sharing insights on how we can use data to better predict and reduce cybersecurity risks.

Hidden Costs of Broken Data

The Struggle is Real

AppSec teams face unprecedented challenges: prioritization paralysis, delayed incident response, and overwhelming alert fatigue. Traditional vulnerability intelligence can no longer keep pace with the threat landscape.

The root cause? Centralized systems are buckling under pressure, forcing teams to make critical security decisions with incomplete or outdated information.

Beyond Traditional Intelligence

Relying solely on legacy vulnerability databases creates dangerous blind spots. Modern threats demand distributed intelligence gathering, cross-correlation of multiple sources, and context-aware prioritization.

The question is no longer *if* you'll diversify your intelligence sources, but *how quickly* you can adapt.

Thesis: Resilience is the New Goal

1

US Ecosystem

Addressing strains in CVE/NVD infrastructure and impact on security ops

2

Global Intelligence

Examining European perspectives (ENISA) and alternative vulnerability data

3

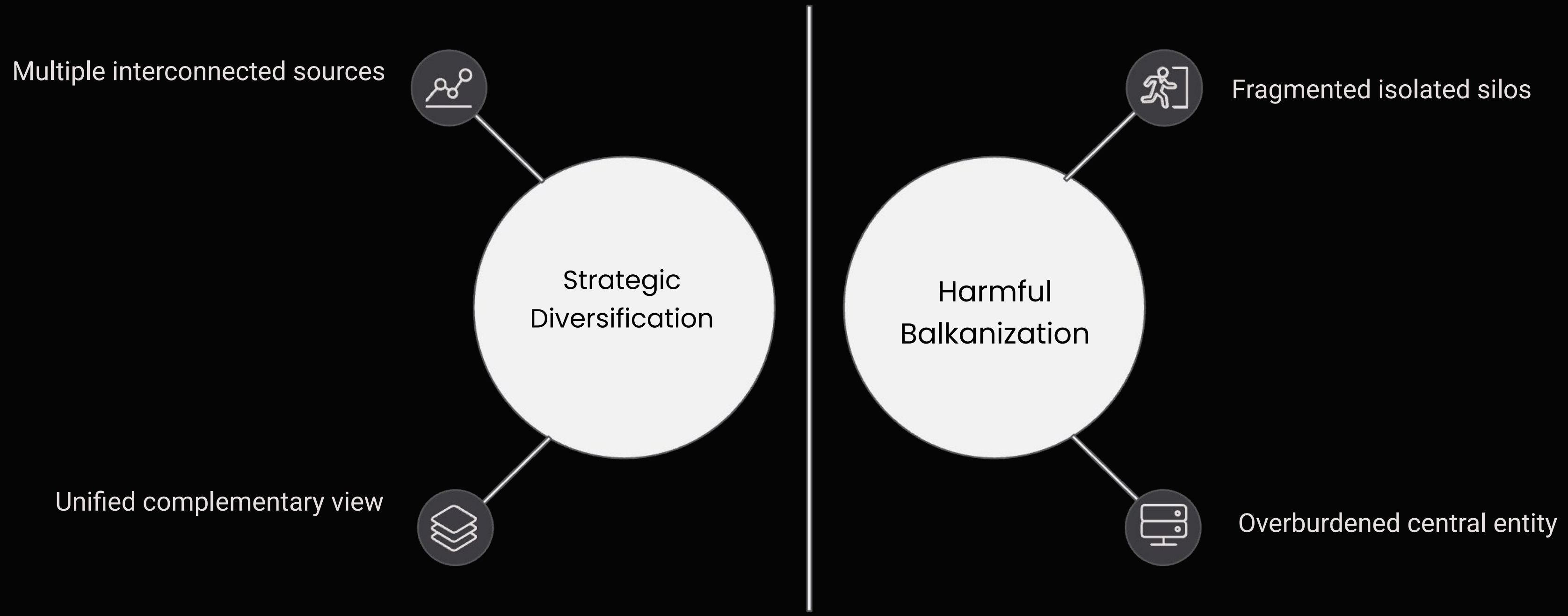
Actionable Strategies

Frameworks for prioritization, automation, and resilient vulnerability management

Diversification vs. Balkanization

This presentation advocates for strategic diversification of vulnerability intelligence, a critical step towards building a truly resilient security posture.

I aim to clarify that this is not a call for harmful balkanization.


Multiple interconnected sources
Unified complementary view
Strategic Diversification
Harmful Balkanization
Fragmented isolated silos
Overburdened central entity

Strategic Diversification

Relying on a single source, like NVD, creates systemic risk. Healthy diversification leverages multiple intelligence feeds, offering complementary insights and reducing single points of failure. Interoperability and common standards are key to a robust ecosystem.

Harmful Balkanization

Without proper integration and standards, multiple intelligence sources can lead to fragmentation. This creates isolated data silos, incomplete views, and prioritization paralysis, ultimately weakening an organization's security posture rather than strengthening it.

The US-Centric Ecosystem Under Strain

Examining the bottlenecks that are reshaping vulnerability management globally

CVE & NVD: The Bottleneck Effect

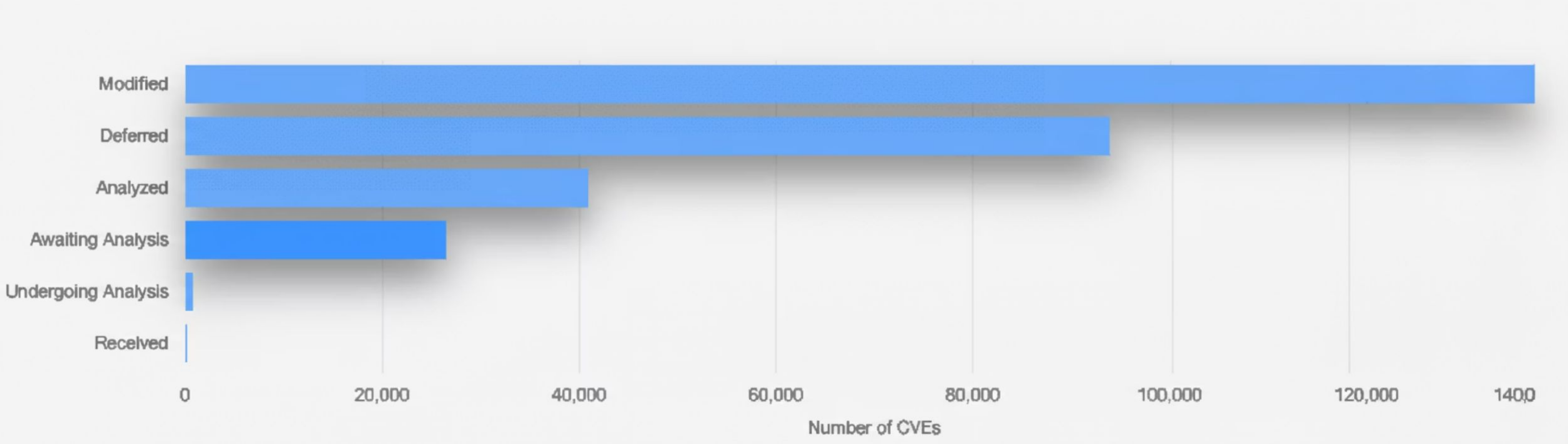
Funding Gaps

Chronic underfunding strains CVE and NVD programs, limiting analyst capacity amidst exploding vulnerability volumes.

Analysis Delays

NVD enrichment backlogs cause significant delays. Critical vulnerabilities lack vital data like CVSS, CWE, and CPE, crippling automated tooling.

NVD Analysis Status: 24,000+ CVEs Awaiting Analysis



Analysis Backlog

With over 24,000 CVEs awaiting processing, the NVD faces significant delays.

This persistent backlog compromises timely vulnerability insights and effective security.

The Data Quality Crisis

> Vulnerability data often lacks standardization, leading to **critical inconsistencies in severity scores, attack vector descriptions, and affected software versions**. This fragmented and unreliable intelligence directly compromises the integrity of our security ecosystem.

CISA KEV: Prioritization by Exploitation

Reactive Innovation

CISA's Known Exploited Vulnerabilities (KEV) Catalog emerged as a direct response to NVD inadequacies. By tracking actively exploited CVEs, CISA provides what NVD cannot: real-time threat intelligence grounded in observed adversary behavior.

KEV represents a philosophical shift: from theoretical risk scoring to evidence-based prioritization. For federal agencies, KEV compliance is now mandatory—a clear signal that traditional CVSS-based approaches are insufficient.

Direct Impact on AppSec Teams

Increased Manual Effort

Without reliable NVD data, teams manually research CVEs, validate applicability, and estimate severity. What automation once handled now consumes analyst hours—hours better spent on remediation.

Widening Risk Windows

Delays in vulnerability intelligence directly extend exposure windows. Attackers exploit CVEs days before NVD publishes analysis, creating asymmetric advantage for adversaries.

Prioritization Without Reliable CVSS

CVSS scores arrive too late or not at all. Teams struggle to triage effectively, often falling back on vendor advisories or incomplete threat intelligence—inconsistent approaches that increase risk.

The Global Shift: Emerging Intelligence Models

Europe and alternative ecosystems are redefining vulnerability intelligence

ENISA: Europe's Growing Intelligence Pillar

Strategic Mandate

The European Union Agency for Cybersecurity (ENISA) is rapidly maturing into a credible alternative to US-centric intelligence. Driven by **NIS2 Directive** requirements and digital sovereignty concerns, ENISA provides vulnerability guidance tailored to **European regulatory contexts**.

Unlike NVD's universal approach, ENISA emphasizes sectoral risk assessments—critical infrastructure, healthcare, finance—aligning intelligence with EU regulatory obligations.

Divergence by Design

ENISA deliberately diverges from US models. European threat landscapes, supply chain dependencies, and regulatory frameworks differ substantially. For multinational organizations, this means **parallel compliance requirements** and intelligence streams that don't always align.

The Proliferation of Alternative Data Sources

OSV.dev

Google's Open Source Vulnerabilities database. Aggregates security advisories across ecosystems (npm, PyPI, Go, Maven). Machine-readable, fast updates, ideal for open-source supply chain visibility.

GitHub Security Advisories

Native integration with dependency graphs and Dependabot. Provides context-specific intelligence for repository dependencies, enabling automated remediation workflows.

Commercial Intelligence & Speed Advantage

Recorded Future

A leading threat intelligence platform, offering real-time insights into emerging threats, adversary tactics, and vulnerabilities across the dark web, open source, and technical sources. Known for its breadth and depth of intelligence.

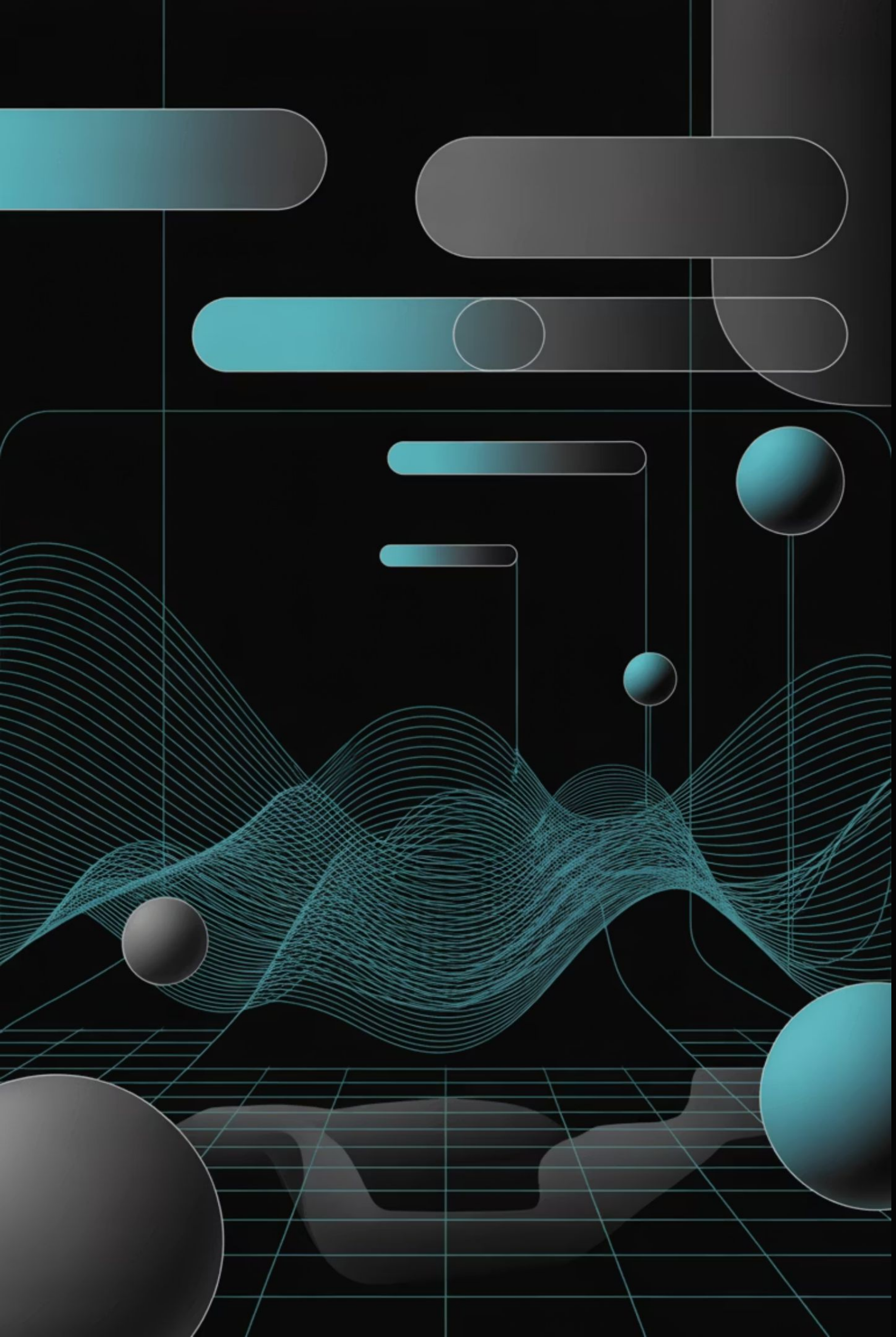
Mandiant (Google Cloud)

Leverages frontline incident response expertise to provide highly curated and actionable threat intelligence. Their insights are often derived from direct engagement with major breaches, offering unique perspectives on attacker methodologies.

CrowdStrike Intelligence

Integrated with their endpoint protection platform, CrowdStrike offers a blend of automated and human-led intelligence, focusing on adversary profiles, campaigns, and indicators of compromise (IOCs) directly relevant to endpoint security.

These commercial platforms offer unparalleled speed and specialization, transforming raw data into actionable intelligence. Their adoption signifies a critical shift for organizations seeking a competitive edge in a rapidly evolving threat landscape, moving beyond generic vulnerability feeds to proactive defense.



The Fragmented Landscape Challenge

> The era of a single source of truth has ended. The new challenge is aggregation, normalization, and correlation across N sources of partial perspective.

Each intelligence source uses different identifiers, severity scales, and update cadences. Building resilient programs now requires sophisticated data engineering—mapping CVE IDs to GHSA IDs to OSV IDs, reconciling conflicting CVSS scores, and maintaining internal knowledge graphs that synthesize external feeds.

Navigating The New Reality

Actionable strategies for building resilient vulnerability management

Strategy 1: Prioritize Beyond CVSS

Exploitability Over Severity

CVSS measures theoretical impact, not likelihood. Shift focus to **exploitability indicators**: proof-of-concept availability, active exploitation, and attacker interest (chatter in forums, dark web marketplaces).

Context is King

A critical RCE in an internal-only service behind segmented networks differs fundamentally from the same CVE in an internet-facing API. Asset criticality, network exposure, and compensating controls must drive prioritization.

Essential Tools for Modern Prioritization

CISA KEV Catalog

Authoritative list of exploited vulnerabilities. If it's in KEV, remediate immediately—adversaries are actively using it.

EPSS (Exploit Prediction Scoring System)

Data-driven probability scores predicting exploitation likelihood within 30 days. EPSS compensates for NVD delays by providing forward-looking risk assessment based on observed threat patterns.

Strategy 2: Diversify and Automate Intelligence

Integrate Multiple Feeds

Vendor security advisories, commercial TI platforms, OSV.dev, GitHub, ENISA, and NVD. Redundancy ensures no single point of failure. Automation tools like vulnerability aggregators or SIEM integrations normalize disparate formats.

Machine-Readable Formats

Leverage **VEX (Vulnerability Exploitability Exchange)** for vendor-provided exploit status and **SBOM (Software Bill of Materials)** for comprehensive dependency mapping. These standards enable automated correlation between discovered vulnerabilities and deployed software.

Orchestration & Enrichment

Build pipelines that automatically enrich CVE data with EPSS scores, KEV status, CISA alerts, and vendor patches. Orchestration platforms (SOAR tools) can trigger workflows: high EPSS + KEV presence = immediate escalation.

Key Technologies: VEX, SBOM, and Integration

VEX

Vulnerability Exploitability Exchange

Standardized format for vendors to communicate exploit status, affected components, and remediation guidance. VEX documents accompany software releases, enabling automated vulnerability assessment without manual vendor advisory parsing.

SBOM

Software Bill of Materials

Comprehensive inventory of software components, dependencies, and versions. SBOMs (SPDX, CycloneDX formats) enable instant impact analysis when new CVEs emerge—identify affected assets within minutes, not days.

Integration

End-to-End Automation

Combine SBOM + VEX + enriched CVE feeds in vulnerability management platforms. Automated matching identifies affected components, filters false positives, and routes actionable findings to responsible teams with complete context.

The Future: Automation and Decentralized Models

1 **AI-Powered Analysis**

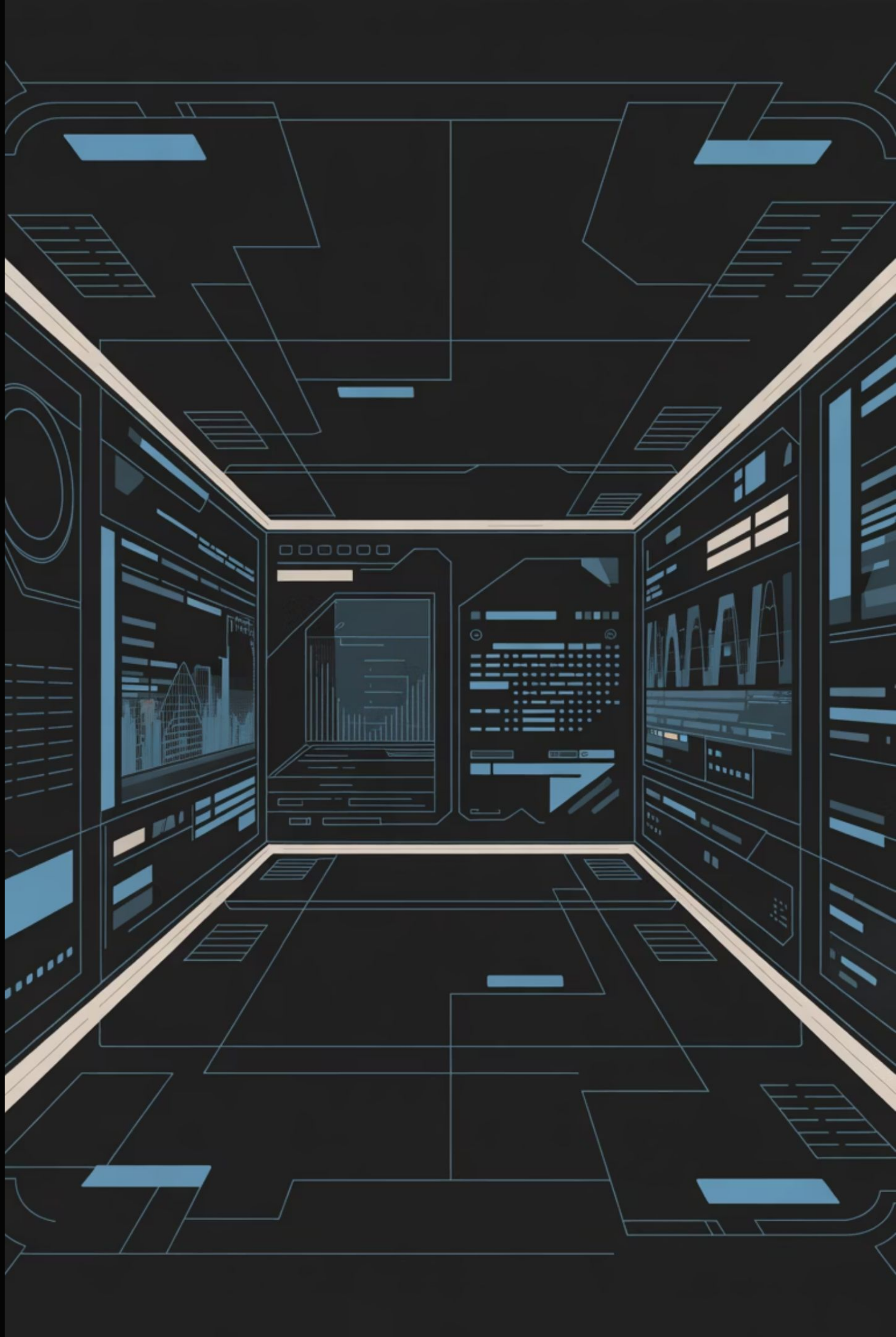
Machine learning models will automate vulnerability classification, exploit prediction, and patch prioritization. Natural language processing extracts intelligence from unstructured sources—security blogs, mailing lists, social media—at scale humans cannot match.

2 **Federated Intelligence**

Decentralized models distribute intelligence generation across community networks. Blockchain-backed vulnerability databases, peer-to-peer threat sharing, and zero-knowledge proof validation improve resilience against single-point failures.

3 **Predictive Defense**

Future systems will predict vulnerabilities before public disclosure. AI analyzing code patterns, binary analysis, and fuzzing results will identify exploitable weaknesses proactively—shifting left from reactive patching to preventive hardening.



Key Takeaways: The New Pillars of Resilience

1. Prioritize with EPSS & KEV

Integrate EPSS probability scores and CISA KEV status for immediate vulnerability triage.

2. Diversify Intelligence Sources

Layer vendor advisories, OSV.dev, GitHub, ENISA, and commercial TI for comprehensive coverage beyond NVD.

3. Automate with VEX & SBOM

Implement machine-readable vulnerability exchange (VEX) and software bills of materials (SBOM) to accelerate response.

4. Build for Fragmentation

Engineer systems to aggregate, normalize, and correlate across multiple intelligence feeds.

Thank You

Questions & Discussion

The vulnerability landscape has fundamentally changed.

Adaptation is no longer optional—it's survival.