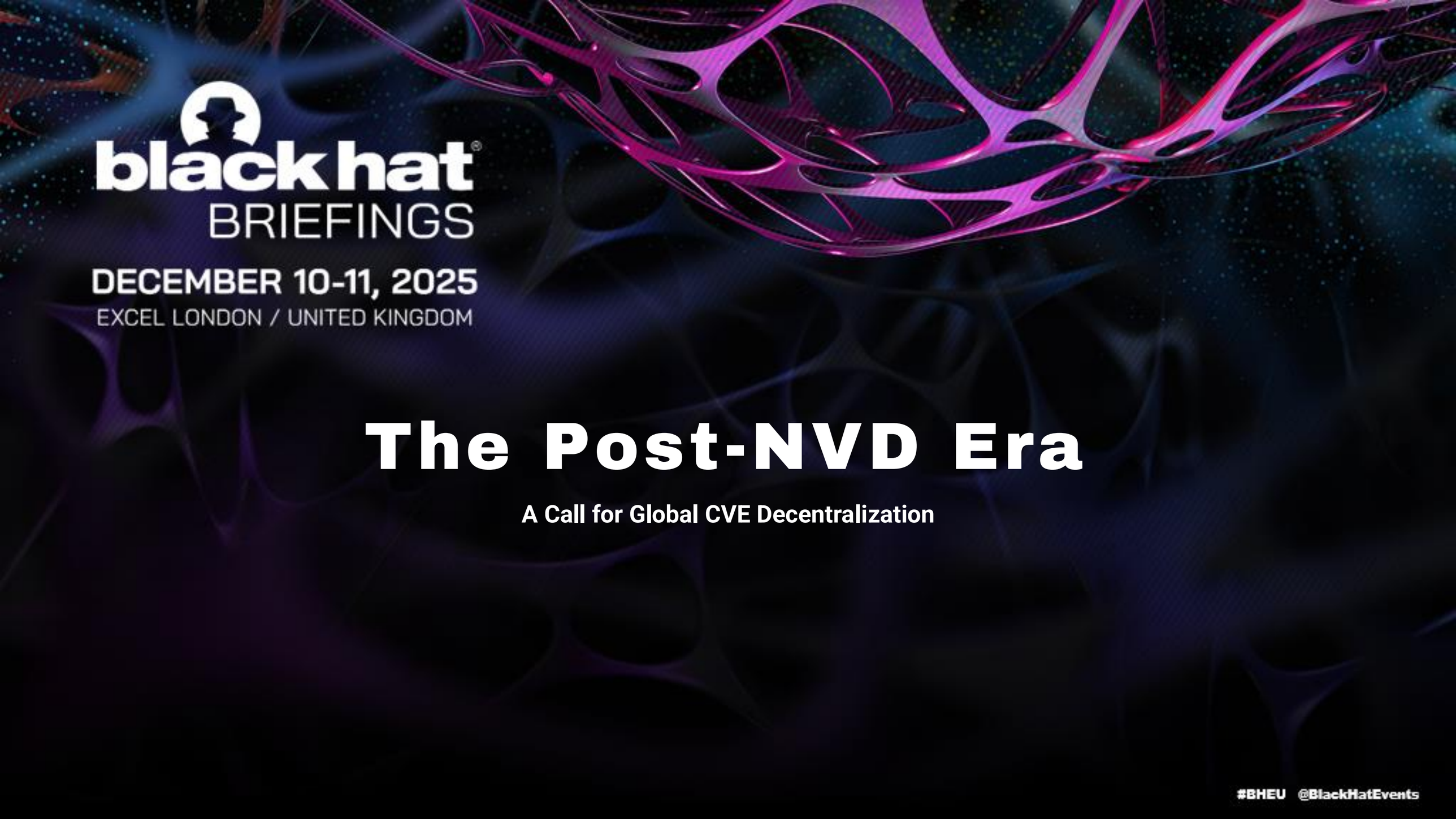


The Post-NVD Era

A Call for Global CVE Decentralization

The Post-NVD Era: A Call for Global CVE Decentralization

The NVD was the cornerstone of vulnerability management for twenty years.
Now, the scale of modern threats requires us to evolve from a centralized library to a decentralized network.

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.

Public Data Projects:

- CVE.icu
- CVEForecast.org
- CNAScoreCard.org
- PatchThis.app

Community Contributions

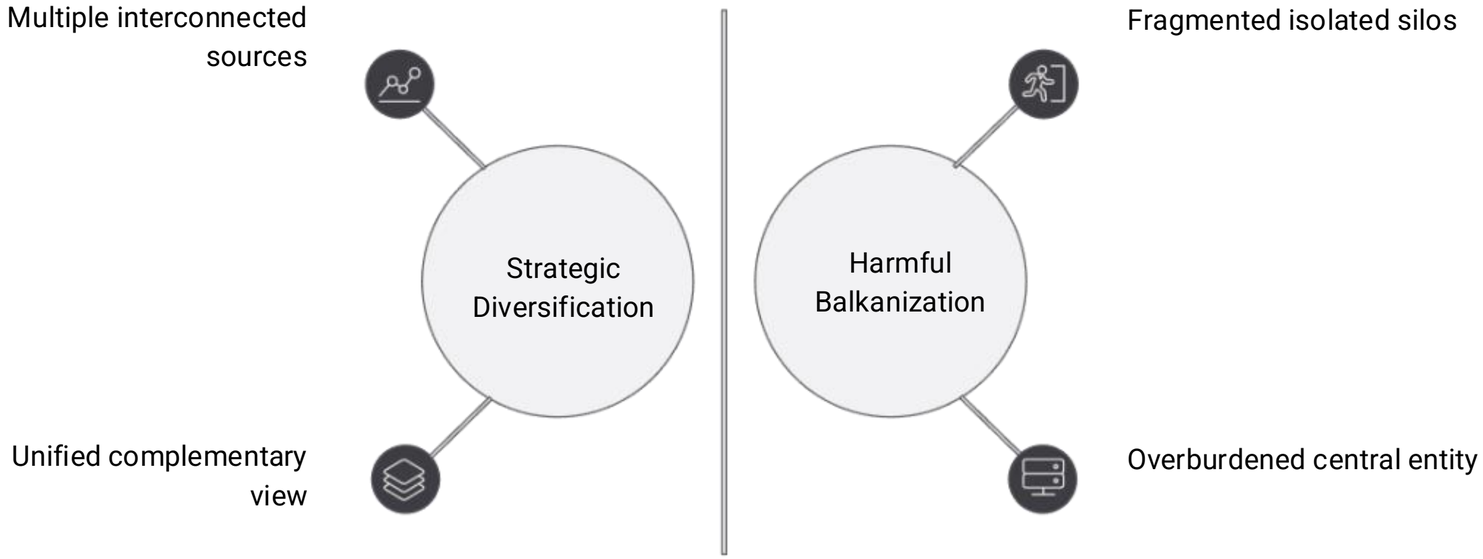
I contribute to the CVE Program and am part of the Exploit Prediction Scoring System (EPSS) Special Interest Group (SIG).

Member of The Following CVE Boards:

- Consumer Working Group (CWG)
- Automation Working Group (AWG)
- Quality Working Group (QWG)

Diversification vs. Balkanization

This presentation advocates for strategic diversification of vulnerability intelligence, a critical step towards building a truly resilient security posture. This not a call for harmful balkanization.

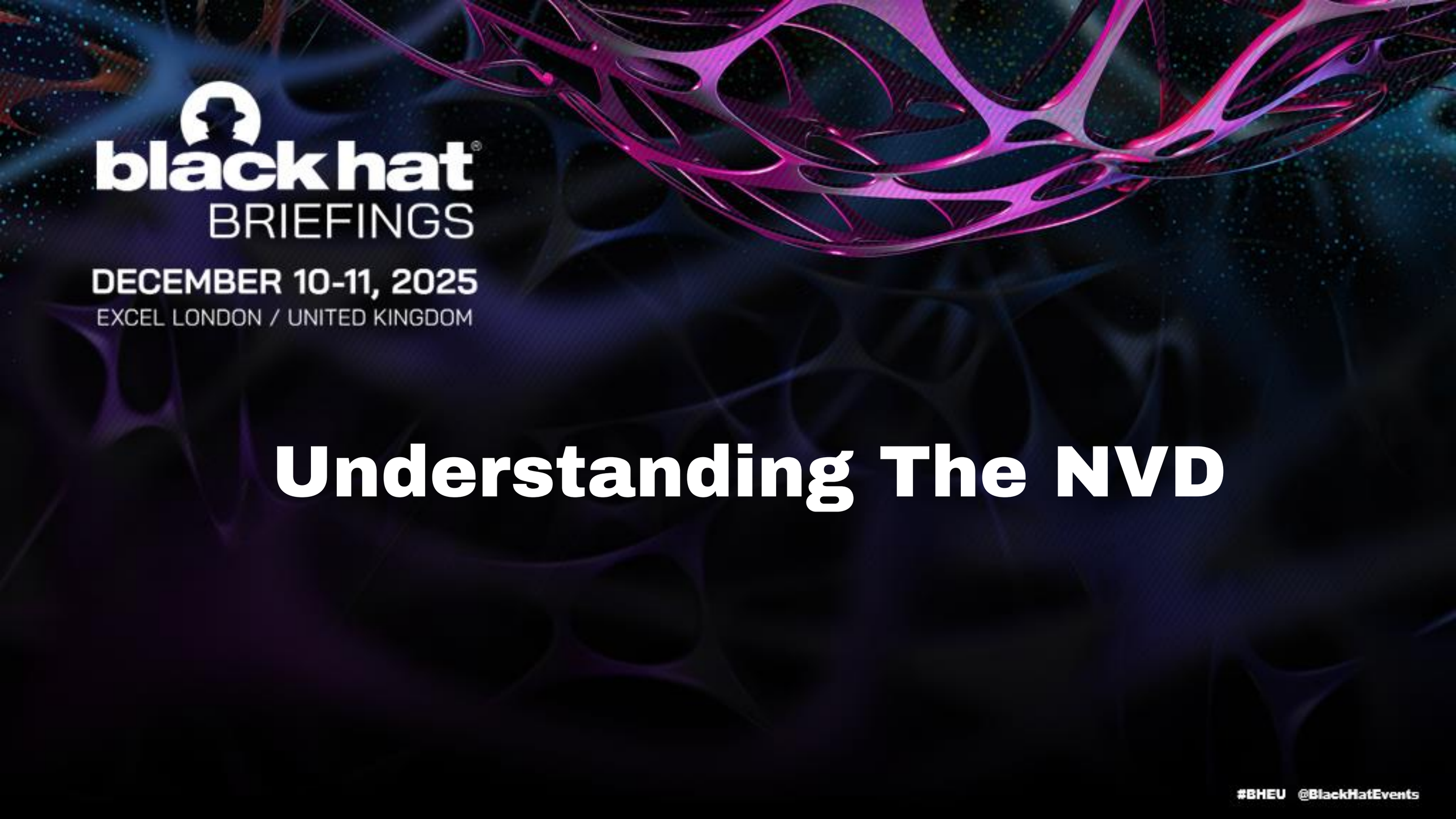


Strategic Diversification

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.



Understanding The NVD

Understanding the NVD's Role

The NVD has operated as the public backbone for cybersecurity operations, performing the critical function of enriching raw CVE identifiers with contextual intelligence. This enrichment transforms a simple vulnerability ID into actionable security intelligence.

Without this enrichment, a CVE is merely a number lacking the severity scores, applicability strings, and weakness classifications that power the global ecosystem of vulnerability scanners, security dashboards, and compliance frameworks.

Critical Enrichment Data

- CVSS severity scores for prioritization
- CPE applicability strings for scanning
- CWE weakness classifications
- Contextual analysis and references

The Centralization Fallacy

Administrative Bottlenecks

Central teams become overwhelmed with requests, slowing response times catastrophically

Single Point of Failure

If the central authority is compromised by attack, budget cuts, or technical debt, the entire dependent ecosystem fails

Inherent Scalability Limits

Monolithic, single-node databases become significant bottlenecks under exponential data growth

Lack of Adaptability

Centralized models struggle to adapt to new formats, unique needs, or evolving threat landscapes

Timeline of Events

2024

February

NIST almost completely stopped enriching new software vulnerabilities, creating the backlog that defined the crisis.

2024

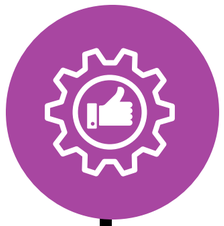
March

CVE publications surged by 38% year-over-year, overwhelming the already strained system.

2024

November

NIST admitted its systems couldn't efficiently process current data flow.

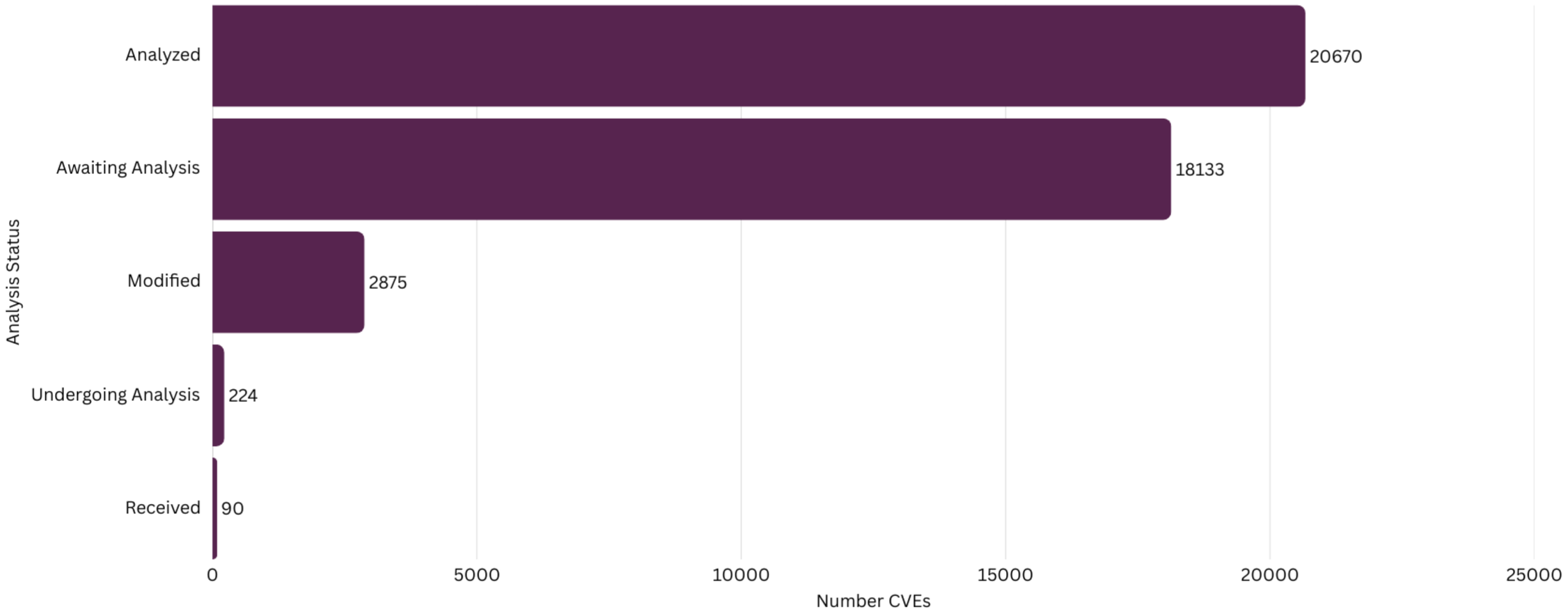


2025

April

NIST made the strategic decision to prioritize emerging threats by permanently deferring analysis on pre-2018 CVEs.

Deferral by Default



The Perfect Storm: Three Converging Failures

Budget Cuts

Lawmakers reduced NIST's budget by nearly 12% in 2024, directly curtailing capacity to fund analysts and infrastructure necessary for NVD operations

Exponential Data Growth

A 32% increase in CVE submissions overwhelmed the system. The centralized, manual-analysis-dependent model was never designed for this volume

Technical Rigidity

Legacy systems built around SCAP protocols proved unable to efficiently ingest modern, heterogeneous data formats even from trusted partners

Architectural Brittleness

> ”Our initial estimate of when we would clear the backlog was optimistic. This is due to the fact that the data on backlogged CVEs that we are receiving from Authorized Data Providers (ADPs) are in a format that **we are not currently able to efficiently import and enhance.**"
>
> — NIST Official Statement, November 13th 2024

Systemic Ripple Effects Across the Ecosystem

Toolchain Disruption

Vulnerability scanners, SIEMs, and security products built to ingest NVD feeds as their canonical source of truth have been blunted

Compliance Uncertainty

Audits and regulatory frameworks referencing NVD severity ratings now operate in a state of dangerous ambiguity

Operational Burden

The security debt of unanalyzed CVEs creates frequent inefficiencies and increased IT maintenance burdens as teams perform manual analysis

The Dangerous Market Shift: Privatization of a Public Good

The analytical work that NVD once provided as a global public good has not disappeared it has simply shifted. This market cost transfer moves enrichment from one public entity to two private sectors:

1. Commercial security vendors rushing to sell proprietary enriched feeds as premium products
2. Individual enterprises forced to absorb manual enrichment costs themselves

This privatization creates a dangerous digital divide where well-funded organizations can buy protection while smaller organizations that relied on NVD as a public good now operate blind, fundamentally fragmenting global collective defense.

The Federated Alternative

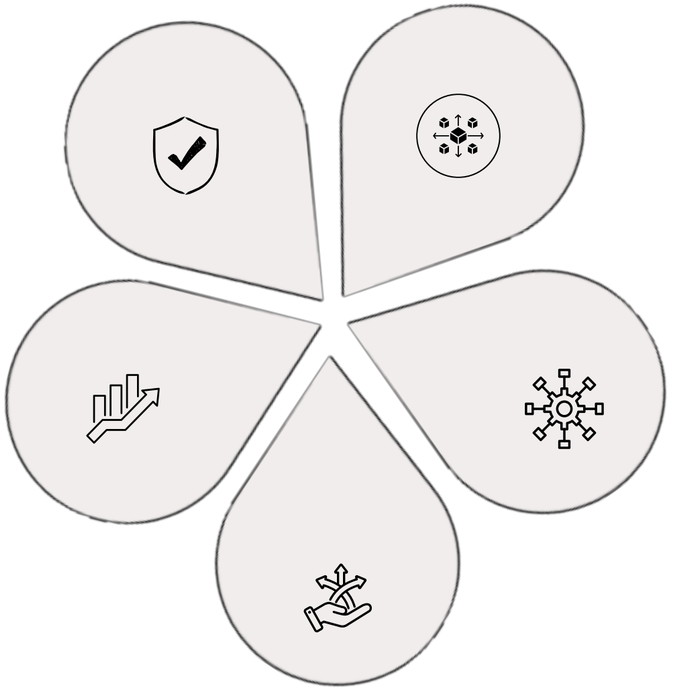
The Federated Alternative: Resilience Through Distribution

Resilience

Eliminates single points of failure—if one node fails, the ecosystem continues operating

Performance

Distributes computational load across multiple sources for faster processing



Scalability

Handles live detection and real-time queries at greater scale through distributed architecture

Autonomy

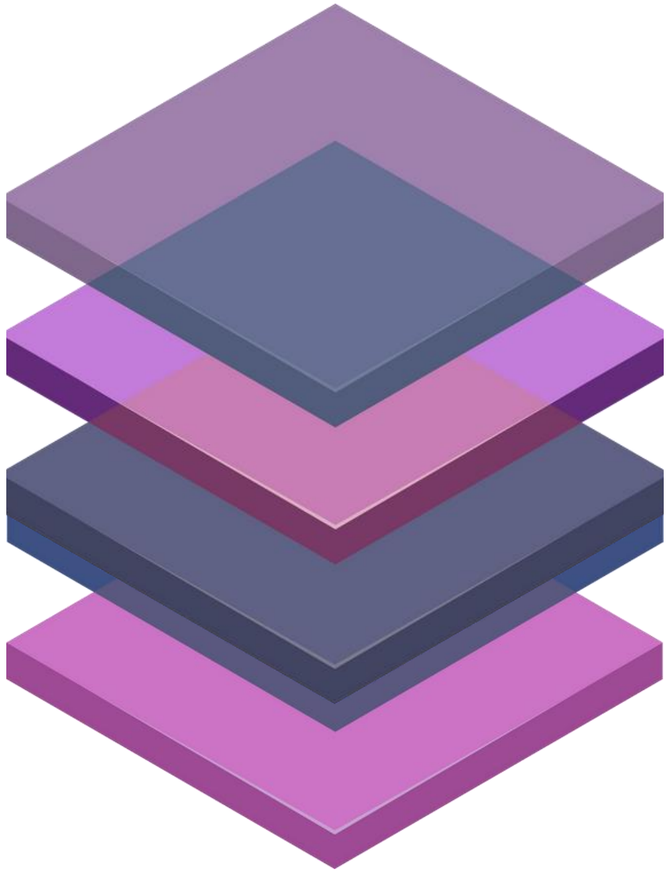
Allows local entities control over their data while adhering to shared standards

Flexibility

Enables adaptation to local needs without central gatekeeper bottlenecks

Not One Replacement, But a Multi-Layered Stack

The Post-NVD Era will not be defined by a single "NVD replacement." Instead, it requires a multi-faceted architectural evolution. The pioneering models under development are not competing solutions—they are complementary layers of a new, decentralized stack.



Allocation Layer

CVE backend system for decentralized CVE identifier distribution.

Enrichment Layer

CSAF/VEX standards for vendor-published vulnerabilities

Consumption Layer

Federated search enabling queries across multiple trusted sources.

Trust Layer

Verification of publisher identity and data integrity.

Federated Allocation (Global CVE)

A Global CVE Allocation System is a European-led proposal designed to enhance flexibility and scalability in vulnerability identifier assignment.

Key Architectural Components

- Global CVE Numbering Authorities (GNAs): Independent entities empowered to allocate identifiers autonomously, removing central bottlenecks.
- Decentralized Publication: New standard allowing GNAs to publish directly via HTTP REST APIs or static files
- Discovery Directory: Central directory used only for discovery, allowing clients to find GNA endpoints and pull from trusted sources

Federated Enrichment (CSAF & VEX)

The Common Security Advisory Framework 2.0 is a machine-readable JSON-based standard for security advisories. The NVD crisis has made this decentralized model increasingly relevant as a resilient alternative.

CSAF Issuers/Publishers

The sources of truth—typically software vendors or researchers who publish advisories only for their own products

CSAF Aggregators

Entities like CISA or national CERTs that collect advisories from various publishers, validate them, and make them available in consolidated, trusted locations

VEX: The Critical Payload

Vulnerability Exploitability eXchange is a machine-readable statement answering the most important defender question: is my specific product affected? It provides clear status—"not_affected," "affected," or "fixed"—enabling mass automation of vulnerability triage.

Federated Consumption (Federated Search)

A federated search architecture allows users to send queries to multiple data sources simultaneously and aggregate results without first moving all data to a centralized data lake. This is the necessary consumer-side architecture for a decentralized world.

Parallel Query Execution

In a Post-NVD ecosystem, a Federated Search would allow an analyst to run a single CVE query that executes in parallel across:

- The Global CVE Directory
- CSAF Aggregator Feeds
- CISA's Vulnrichment data feed
- Industry Specific Threat Intelligence Feeds

The Trust Layer

Several academic proposals suggest a decentralized system for CVE publication to address the most difficult question: who do you trust?

Public Permissioned Architecture

- Permissioned Write: Only authenticated CNAs can submit new vulnerability entries
- Public Read: Anyone can audit the ledger, ensuring complete transparency
- Hybrid Storage: Blockchain stores publisher identity and cryptographic hashes; full CSAF files stored off-chain (e.g., via IPFS)

Promise

Immutable, auditable records providing high trust

Peril

Scalability challenges with slow transaction speeds and complexity

The intelligent application is using blockchain not as a data store, but as a trust directory—providing immutability without crippling scalability bottlenecks.

The New Paradigm: Collective Intelligence

Vendors Publish

Software vendors publish enriched CSAF advisories for their products

Researchers Contribute

Independent researchers and consortia drive standards and publish findings

Aggregators Validate

Trusted aggregators collect, validate, and consolidate feeds

Enterprises Consume

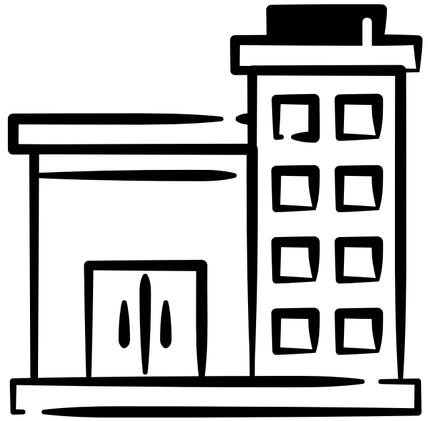
Security teams query multiple sources through federated systems

This model harnesses real-time, insight-level collaboration by sharing information among all stakeholders, creating a resilient ecosystem through collective intelligence.

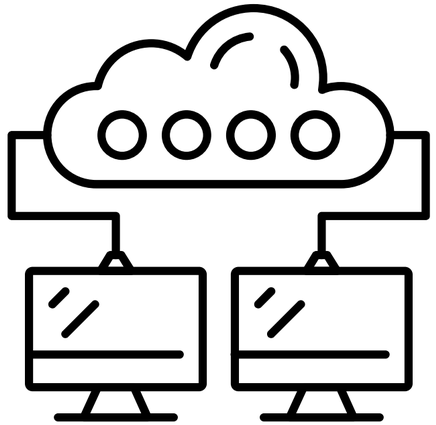
The Architecture Shift: From Mainframe to Cloud

The Legacy Model: Centralized Monolith

The NVD served for decades as a centralized Monolith, operating the entire vulnerability stack. The community acted as passive consumers , creating a systemic single point of failure. This monolithic approach has been outpaced by the exponential scale of modern software."



VS



The Future Model: Federated Ecosystem (IaaS/PaaS)

IaaS (Vendors/CNAs): Provide the raw infrastructure of truth—owning the base data (CSAF/VEX advisories).

PaaS (Aggregators/Gov): Supply the platform—building the standards, directories, and trust layers.

Customers: actively configure their own risk engines using these diverse, high-fidelity feeds.

Evolving Responsibilities

Evolving Responsibilities: Software Vendors & CNAs

Old Responsibility

Optionally assign CVEs and provide some data to central authorities

The Opportunity: Source-Based Truth.

Vendors are best positioned to provide the most accurate data.

By publishing CSAF, you ensure your customers get the highest fidelity information directly from the source.

Evolving the Mission

NVD: From Provider to Facilitator

- Legacy Role: Acting as the centralized data provider..
- Modern Role: Facilitating the ecosystem through standards (CVSS v4.0, SCAP) and federated protocols.

CISA: From Stopgap to Aggregator

- Evolve: From partial "Vulnrichment" program to full-fledged Trusted Data Aggregator
- Focus: Public advisories, critical infrastructure, policy, and Coordinated Vulnerability Disclosure

Government agencies can evolve from being the sole provider to becoming the ecosystem enabler—setting standards and facilitating trust..

Evolving Responsibilities: Enterprise Security Teams

Abandon Single-Source Dependency

Stop relying on one centralized feed as the sole source of vulnerability intelligence

Invest in Multi-Source Infrastructure

Deploy Threat Intelligence Platforms, Federated Search tools, and aggregation capabilities

Develop Correlation Processes

Create workflows to aggregate, correlate, and prioritize data from diverse CSAF feeds, vendor advisories, and commercial intelligence

Evolving Responsibilities: Researchers & Consortia

Security Consortia (OWASP, IST)

Must drive development and adoption of open standards like CSAF and GCVE. Propose new governance frameworks such as the "Global Vulnerability Catalog" to coordinate decentralized efforts.

Bug Bounty Platforms

Evolve from simple brokers to major CSAF Aggregators. Institutionalize the "gig economy" of security research by collecting findings from thousands of independent researchers and publishing verified, enriched CSAF feeds.

Independent Researchers

Become first-class publishers with direct channels to publish verified findings in standardized formats, contributing directly to the federated intelligence ecosystem.

The Future is Distributed

The systemic failure of the National Vulnerability Database is not a crisis to be "fixed" but an evolutionary driver that must be embraced. The global cybersecurity community is not losing a cornerstone—it is outgrowing it.

The move from a fragile, centralized provider to a resilient, federated ecosystem is a sign of the industry's maturation. This new paradigm, built on collective intelligence and a clear shared responsibility model, is the only viable path forward.

The future of vulnerability management is not centralized. The future is distributed.

A Shared Path Forward

For Vendors: Deliver Intelligence Directly

Begin publishing CSAF advisories for your products. You are the source of truth.

For Government: Enable Standardization.

Shift from provider to enabler. Set standards, coordinate efforts, aggregate trusted sources.

For Enterprises: Diversify Your Intelligence

Invest in multi-source consumption infrastructure. The era of single-source dependency is over.

For Researchers: Drive the Standards

Lead the development of open standards and governance frameworks. Your independence is critical.

The time to build the standards, shift the processes, and embrace this collaborative and resilient future is now. Let's build the Post-NVD Era together.


black hat
BRIEFINGS
DECEMBER 10-11, 2025
EXCEL LONDON / UNITED KINGDOM
Thank You!
#BHEU @BlackHatEvents