Common Vulnerabilities and Exposures (CVE)

Scaling Through Federation and Partnership

CVE Program Mission, Goals, and Desired Outcome

Mission

Identify, define, and catalog publicly disclosed cybersecurity vulnerabilities

Goals

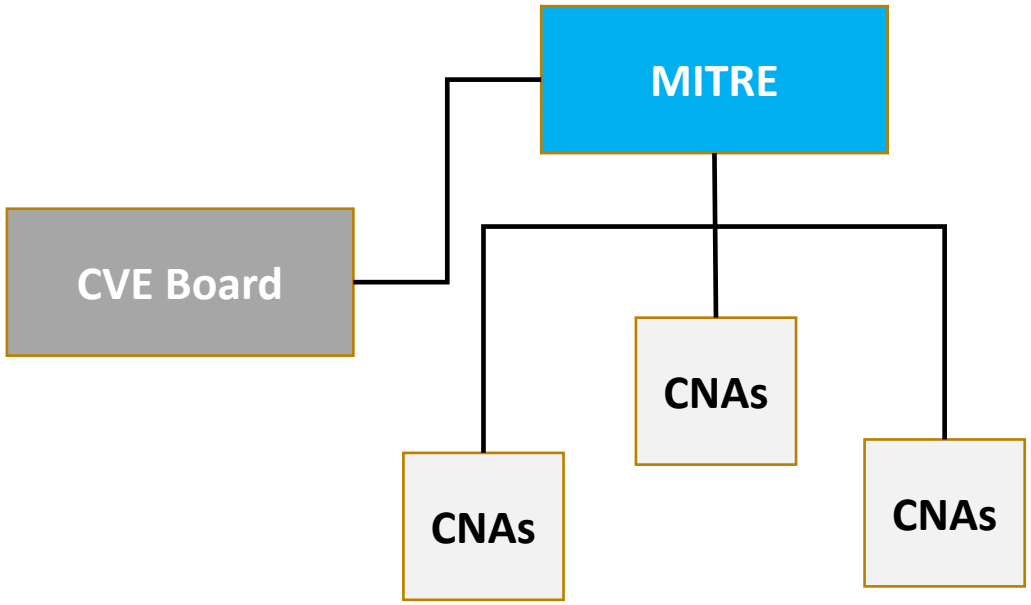
1. Increase CVE Program adoption
   - Increase CVE usage in the vulnerability management ecosystem
2. Increase CVE Program coverage
   - More vulnerabilities get CVE IDs and associated CVE Records

Desired Outcome

More quality CVE Records are produced, faster

The old CVE Program!

- MITRE produced all CVE Records.
- This model of governance and operations does not scale
  - Too many bottlenecks
  - Dated infrastructure
  - Too much manual intervention in all things
  - Not enough partners



Start of 2016: 24 CNAs total

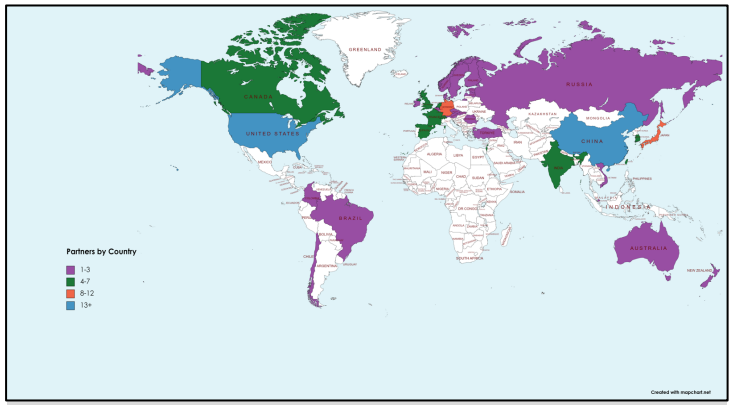
2016-2017: Shift to a Strategy of Federation

- **Reinvigorate the CVE Board**
  - Comprised of industry, government, and academic stakeholders
  - Responsible for the strategic direction of the CVE Program
  - Used to meet annually; now meets every two weeks
- **Chart the pathway forward**
  - Develop strategies to scale the program to meet mission outcomes
    - More CNAs and Roots
    - Authorized Data Publishers
    - Working Groups
    - Automated services
    - JSON 5.0
- **Execute and adjust**
  - Keep doing what works, stop doing what does not

More CNAs and Roots

- **CNA:** An organization responsible for the regular assignment of CVE IDs to vulnerabilities, and for creating and publishing information about the vulnerability in the associated CVE Record. Each CNA has a specific Scope of responsibility for vulnerability identification and publishing.

- **Root:** An organization authorized within the CVE Program that is responsible, within a specific Scope, for the recruitment, training, and governance of one or more entities that are a CNA, CNA of Last Resort (CNA-LR), or another Root.



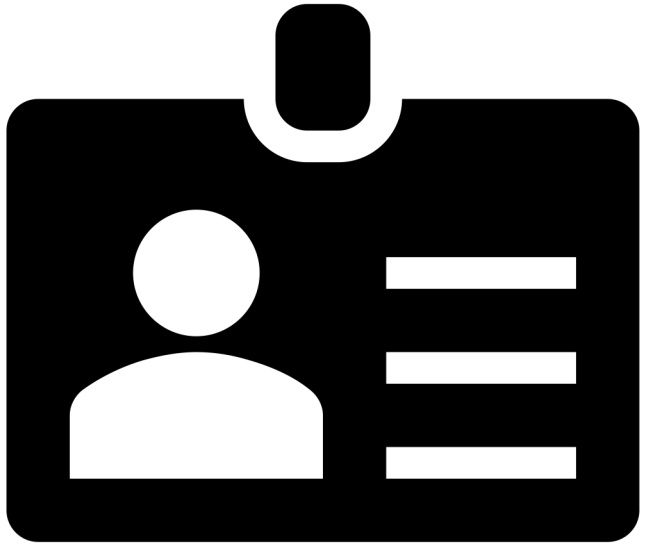
Federation Through Partnership: Impact by the Numbers

Year	Records Published	Number of CNAs
2016	6,457	24 (1 Int.)
2017	14,644	78
2018	16,510	90
2019	17,308	106
2020	18,364	144
2021	20,161	209 (100 Int.)
2022	25,059	263 (123 Int.)

Federated Growth Strategy Implemented

Authorized Data Publishers (Future)

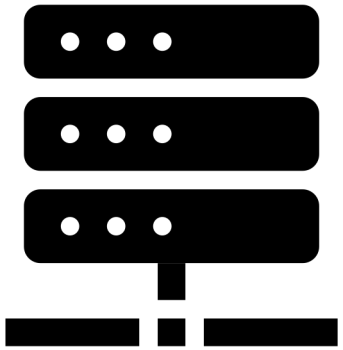
- **An organization authorized by the CVE Program to provide value-added information to CVE Records**
  - Initial pilots planned for 2023
    - References
    - SSVC: The Stakeholder-specific Vulnerability Categorization (SSVC) is a system for prioritizing actions during vulnerability management



Working Groups

- **Automation (Open to the public)**
  - Focused on identifying and advancing proposals for the collaborative design, development, and deployment of automated capabilities that support the efficient management of the CVE Program.
- **Strategic Planning (Invitation only)**
  - Focused on the long-term strategy (1-5 years) and goals of the CVE Program; works closely with the CVE Board to determine goals and objectives and will act to achieve them.
- **Outreach and Communications (Open to the public)**
  - Promotes the CVE Program to achieve program adoption and coverage goals through increased community awareness.
- **CNA Coordination (Must be a CNA)**
  - Provides a forum for more effective communication and participation by the CNAs.
- **Quality (Open to the public)**
  - Focused on identifying areas where CVE content, rules, guidelines, and best practices must improve to better support stakeholder use cases.

Automated Services



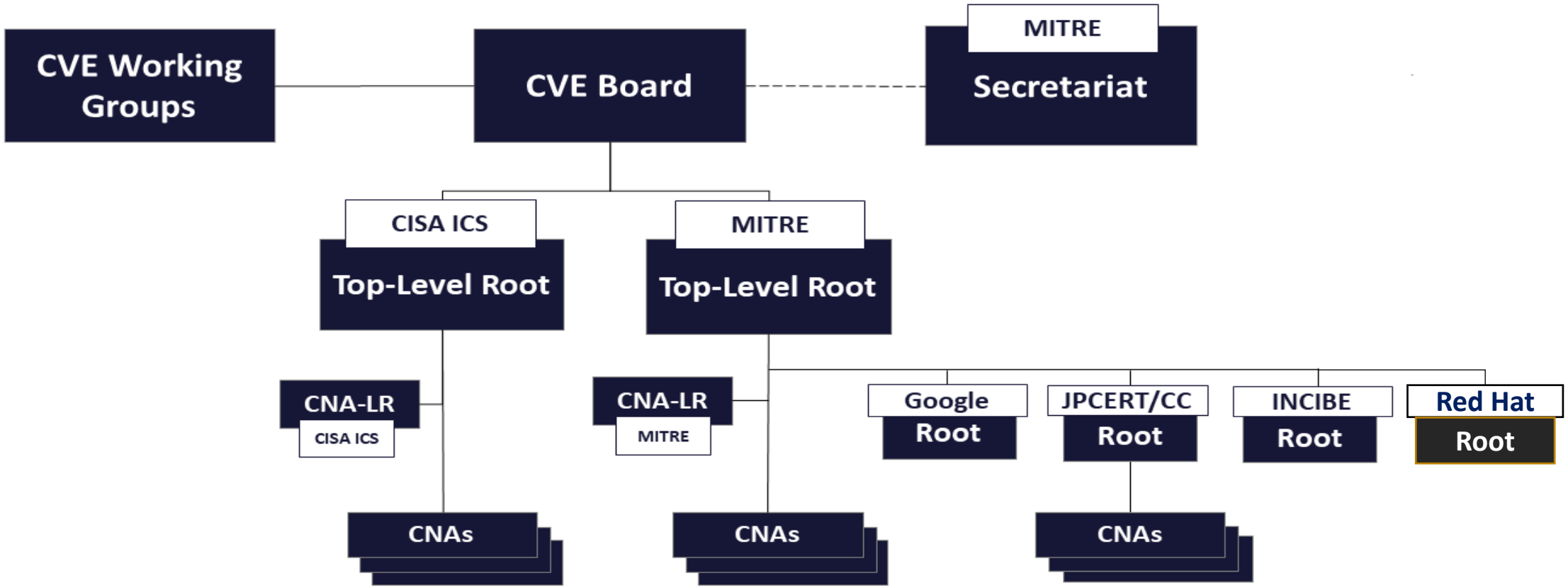
- **CVE Services: A client/server architected web application that provides a series of APIs to CNAs that allows them to reserve CVE IDs, submit, update, and publish CVE Records and manage their CVE Services user pool**
  - **CVE ID Reservation (IDR)**: Self-service allowing CNAs to get either an arbitrary number of non-sequential IDs or sequential IDs
    - Status: Deployed December 2020
  - **Record Submission and Upload Subservice (RSUS): Self service allowing CNAs to submit/upload CVE information directly into the CVE Repository, without the need for manual review**
    - Status: Deployed October 2022
  - **CVE User Registry: CVE Program User Provisioning and User management functions that will enable single sign on/single point for service and distributed CVE Service Pool management**
    - Status**:** Initial capability deployed in June/2021/Enhancements in 2023

CVE Program JSON 5.0 Data Format

- **JSON 5.0 enables the submission of value-added information associated with a CVE Record**
  - Deployed October 2022
- **All records will ultimately be submitted using JSON 5.0**
- **All downloads will ultimately only be available in JSON 5.0**


```
},
"impact": {
 "cvss": {
  "attackComplexity": "LOW",
  "attackVector": "NETWORK",
  "availabilityImpact": "HIGH",
  "baseScore": 8.8,
  "baseSeverity": "HIGH",
  "confidentialityImpact": "HIGH",
  "integrityImpact": "HIGH",
  "privilegesRequired": "LOW",
  "scope": "UNCHANGED",
  "userInteraction": "NONE",
  "vectorString": "CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H",
  "version": "3.0"
```

What the CVE Program Looks Like Today



CVE Program Media Channels

- **NEW CVE Website (Beta)**
- **Twitter & LinkedIn**
  - @CVEannounce, @CVEnew
  - CVE Program on LinkedIn
- **YouTube**
  - CVE Program Channel
- **"We Speak CVE" Podcast**
  - CVE website, Buzzsprout, YouTube
- **CVE Blog**
  - CVE website & Medium

CVE Program Terminology (1 of 2)

- **CVE Record:** The descriptive data about a Vulnerability associated with a CVE ID, provided by a CNA. This data is provided in multiple human and machine-readable formats.

- **A CVE Record is associated with one of the following states**:
  - **Reserved:** The initial state for a CVE Record; when the associated CVE ID is Reserved by a CNA.
  - **Published:** When a CNA populates the data associated with a CVE ID as a CVE Record, the state of the CVE Record is Published. The associated data must contain an identification number (CVE ID), a prose description, and at least one public reference.
  - **Rejected:** If the CVE ID and associated CVE Record should no longer be used, the CVE Record is placed in the Rejected state. A Rejected CVE Record remains on the CVE List so that users can know when it is invalid.

***Reference:** https://www.cve.org/ResourcesSupport/Glossary#

CVE Program Terminology (2 of 2)

- **CVE Board:** Establishes the strategic direction, governance, operational structure, policies, and rules of the CVE Program.
- **Secretariat:** Hosts and maintains the CVE Program's infrastructure and provides administrative and logistical support for the CVE Board, CVE Working Groups, and other elements of the CVE Program.
- **Top-Level Root:** Manages one or more Roots, CNAs, and/or CNAs of Last Resort. Reports to the CVE Board.
- **CNA-Last Resort**: Assigns CVE IDs and creates and publishes CVE Records for vulnerabilities not covered by the Scope of another CNA. Reports to a Root or a Top-Level Root.
- **Root:** Manages one or more CNAs, CNAs-LR, ADPs, or another Root, within a specific area of Scope. Reports to a Top-Level Root.
- **CNA:** Assigns CVE IDs to vulnerabilities and creates and publishes information about the vulnerability in the associated CVE Record. Each CNA has a specific Scope of responsibility for vulnerability identification and publishing. Reports to a Root.

***Reference:** https://www.cve.org/ResourcesSupport/Glossary#

The mission of the CVE Program is to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities.

There is one CVE Record for each vulnerability in the catalog. The vulnerabilities are discovered then assigned and published by organizations from around the world that have partnered with the CVE Program. Partners publish CVE Records to communicate consistent descriptions of vulnerabilities. Information technology and cybersecurity professionals use CVE Records to ensure they are discussing the same issue, and to coordinate their efforts to prioritize and address the vulnerabilities.

Learn more www.cve.org