

DEV  
SEC  
OPS  
D A Y S

PITTSBURGH

**Carnegie  
Mellon  
University**  
Software  
Engineering  
Institute

# DevSecOps for the Community: Building, Provisioning and Deploying CVE's Infrastructure and Services

**MAY 11, 2023**

Shane T .Ficorilli  
Senior Cybersecurity Engineer  
MITRECorp



PITTSBURGH

# Agenda

Carnegie  
Mellon  
University  
Software  
Engineering  
Institute

- Who am I?
- What is CVE?
- DevSecOps Culture
- CVE-Services
- New CVE-Website: [cve.org](https://cve.org)
- Future DevSecOps Improvements
- Questions?



# Who am I? – Shane T. Ficorilli

- **Born and raised in Pittsburgh, PA**
- **Education:**
  - BS in IT/Minor in Computer Science – La Roche College
  - MS in Information Security Policy and Management – Carnegie Mellon University
- **Work Experience:**
  - 2016-2021: DevSecOps/Software Engineer – Software Engineering Institute
  - 2021-Present: Senior Cyber Security Engineer – MITRECorp

DevSecOps for the Community: Building, Provisioning and Deploying CVE's Infrastructure and Services

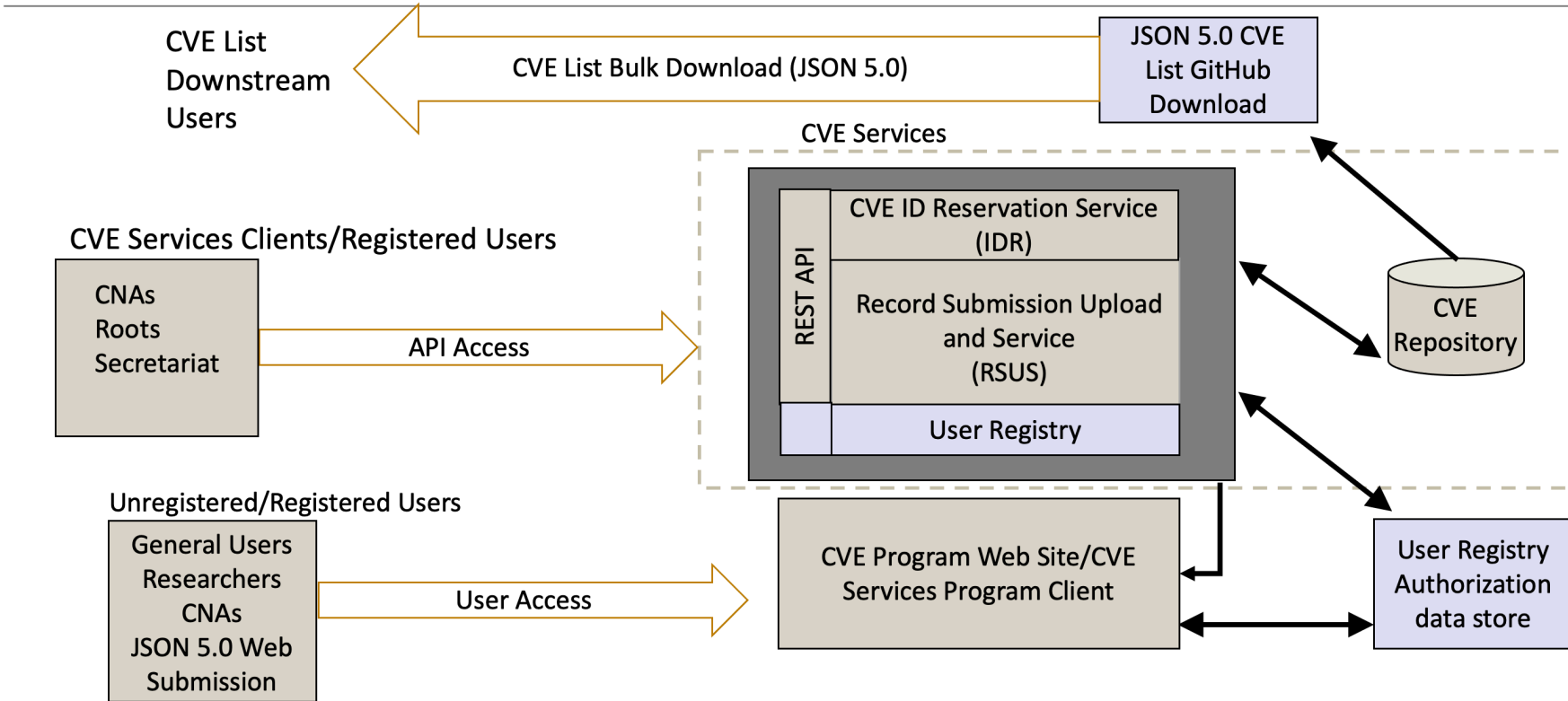
# What is CVE?

# What is CVE?

- Common Vulnerabilities and Exposures (CVE)
- The mission of the CVE® Program is to uniquely identify, catalog and publish helpful information concerning publicly disclosed cybersecurity vulnerabilities
- There is one CVE Record for each vulnerability in the catalog
- The vulnerabilities are discovered then assigned and published by CVE Numbering Authorities (CNAs) that have partnered with the CVE Program
- Launched to the public in September 1999
- Systems operated by MITRE



# What is CVE? – System of Systems



DEV  
SEC  
OPS  
DAYS

PITTSBURGH

DevSecOps for the Community: Building, Provisioning and Deploying CVE's Infrastructure and Services

# DevSecOps Culture

**Carnegie  
Mellon  
University**

Software  
Engineering  
Institute



# DevSecOps Culture

- Development, security and operations teams work closely together
  - Implement new features
  - Track effort/issues
  - Oversee/troubleshoot deployments
  - Alerting/monitoring
- Community Involvement & Feedback– Working Groups
  - Automation Working Group (AWG)
  - Website Working Group (WSWG)



DEV  
SEC  
OPS  
DAYS

PITTSBURGH

DevSecOps for the Community: Building, Provisioning and Deploying CVE's Infrastructure and Services

# CVE-Services

**Carnegie  
Mellon  
University**

Software  
Engineering  
Institute

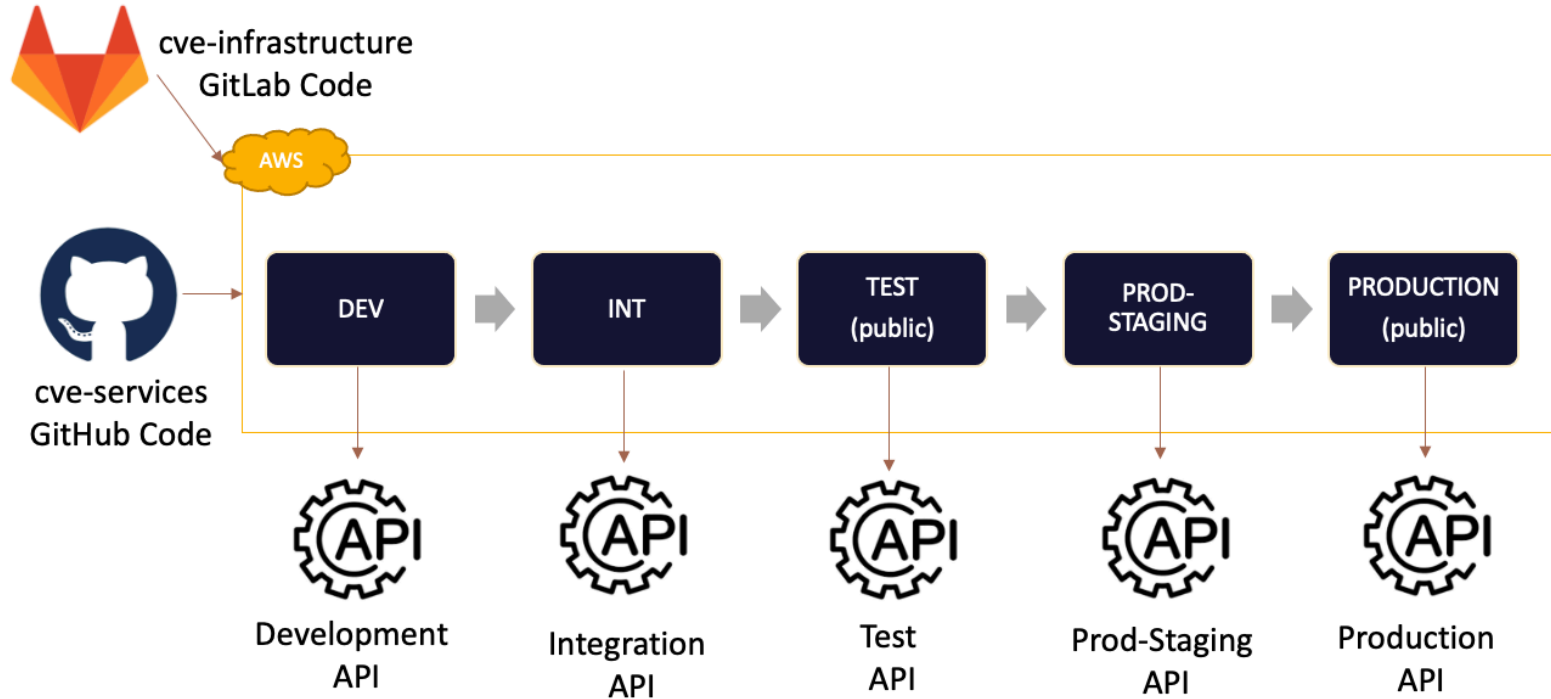
- **A web addressable application for CVE Number Authorities (CNAs)**
- **Comprises a series of RESTful endpoints/Application Programming Interfaces (APIs) to which CNA “clients” will connect to perform common functions such as:**
  - Reserving a CVE ID
  - Submitting/Updating a CVE Record for publication
  - Manage the CVE Services users at your CNA (i.e., create accounts, change password)
- **Instantaneous, Automatic response**
  - No human intervention, no lag time



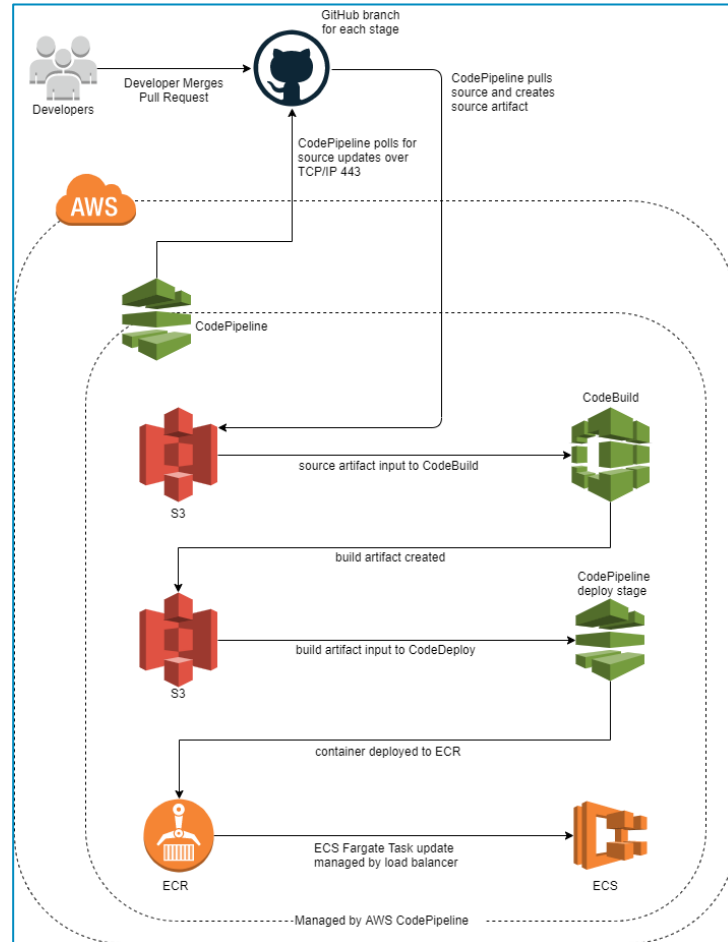
# CVE-Services

- CVE-Services source code lives on GitHub
- All infrastructure created using AWS CloudFormation Templates stored in MITRE's internal GitLab
- Five different environments exist in AWS

# CVE-Services Environments



# CVE-Services CI/CD Architecture





# CVE-Services CI/CD Components

- GitHub Repository
  - GitHub Advanced Security tools:
    - Dependabot scans/alerting
    - CodeQL SAST scans
- AWS
  - Code Pipeline
  - Code Build
  - S3
  - ECR (Elastic Container Registry)
  - ECS (Elastic Container Service: Fargate)

# CVE-Services AWS Components

- Elastic Container Service
- Elastic Container Registry
- DocumentDB EC2 (Bastion host to access DocumentDB instance)
  - MITRE vetted Amazon Linux2 AMI
- ALB (Application Load Balancer)
- VPC (private/public subnets)
- IAM (Identity and Access Management)
- Cloud Watch (logs)
- WAF (Web Application Firewall)

DEV  
SEC  
OPS  
DAYS

PITTSBURGH

DevSecOps for the Community: Building, Provisioning and Deploying CVE's Infrastructure and Services

# CVE-Website (cve.org)

**Carnegie  
Mellon  
University**  
Software  
Engineering  
Institute

- Old Website hosted on prem by MITRE
- [cve.mitre.org](https://cve.mitre.org)



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

**CVE News**

News has moved to the new CVE website.  
[Go to new News page >>](#)

**CVE Podcast**

Podcasts have moved to the new CVE website.  
[Go to new Podcast page >>](#)

**CVE Blog**

Blogs are moving to the new CVE website.  
[Go to new Blogs page >>](#)


**Become a CNA**

CVE Numbering Authorities, or "CNAs," are essential to the CVE Program's success and every CVE Record is added to the CVE List by a CNA.

**Join today!**

- [Business benefits](#)
- [No fee or contract](#)
- [Few requirements](#)
- [Easy to join](#)


[Go to new CVE website](#)



[Learn How to Become a CNA >>>](#)  
[Watch CNA Onboarding Videos >>](#)

**Newest CVE Records**

**Tweets from @CVEnew**

 **CVE**  
@CVEnew · 44m

CVE-2023-2310 A Channel Accessible by Non-Endpoint vulnerability in the Schweitzer Engineering Laboratories SEL Real-Time Automation Controller (RTAC) could allow a remote attacker to perform a man-in-the-middle (MITM) that could result in denial ...  
[cve.mitre.org/cgi-bin/cvenam...](https://cve.mitre.org/cgi-bin/cvenam...)

[Follow @CVEnew >>](#)

- New Website hosted by MITRE owned AWS infrastructure

- cve.org

The screenshot shows the CVE website homepage. At the top, there is a navigation bar with links for 'About', 'Partner Information', 'Program Organization', 'Downloads', and 'Resources & Support', along with a 'Report/Request' button. Below the navigation is a search bar with the placeholder text 'Enter CVE ID (CVE-YYYY-NNNN)' and a 'Find' button. A secondary search bar labeled 'Site Search' is also present. A message below the search bar states: 'Welcome to the new CVE Beta website! CVE Records have a new and enhanced format. View records in the new format using the CVE ID lookup above or download them on the Downloads page. CVE List keyword search will be temporarily hosted on the legacy cve.mitre.org website until the transition is complete.'

The main content area features the 'CVE® Program Mission' section, which states: 'Identify, define, and catalog publicly disclosed cybersecurity vulnerabilities. Currently, there are 202,059 CVE Records accessible via Download or Search'. Below this is a call to action box: 'The CVE Program partners with community members worldwide to grow CVE content and expand its usage. Click below to learn more about the role of CVE Numbering Authorities (CNAs) and Roots.' with 'Learn More' and 'Become a Partner' buttons.

On the right side, there is a 'News' section with several items: '“CVE Global Summit Spring 2023”', 'Minutes from CVE Board Teleconference Meeting on April 12 Now Available', 'Solidigm Added as CVE Numbering Authority (CNA)', and '42Gears Added as CVE Numbering Authority (CNA)'. Below the news items is a 'MORE NEWS' link.

At the bottom, there are three columns of links: 'Access' (List of Partners, CNA Rules, CVE Record Lifecycle, CVEProject on Github for Development), 'Learn' (About CVE, Process, Program Organization, Related Efforts, Terminology, CVE Services for CNAs), and 'Report/Request' (Report vulnerability/Request CVE ID, Request CVE Record be published/updated, Report the use of a reserved CVE ID).

At the very bottom right, there is an 'Events' section with one item: '35th Annual FIRST Conference June 4, 2023 — June 9, 2023 | Montréal, Quebec, Canada + Virtual'.

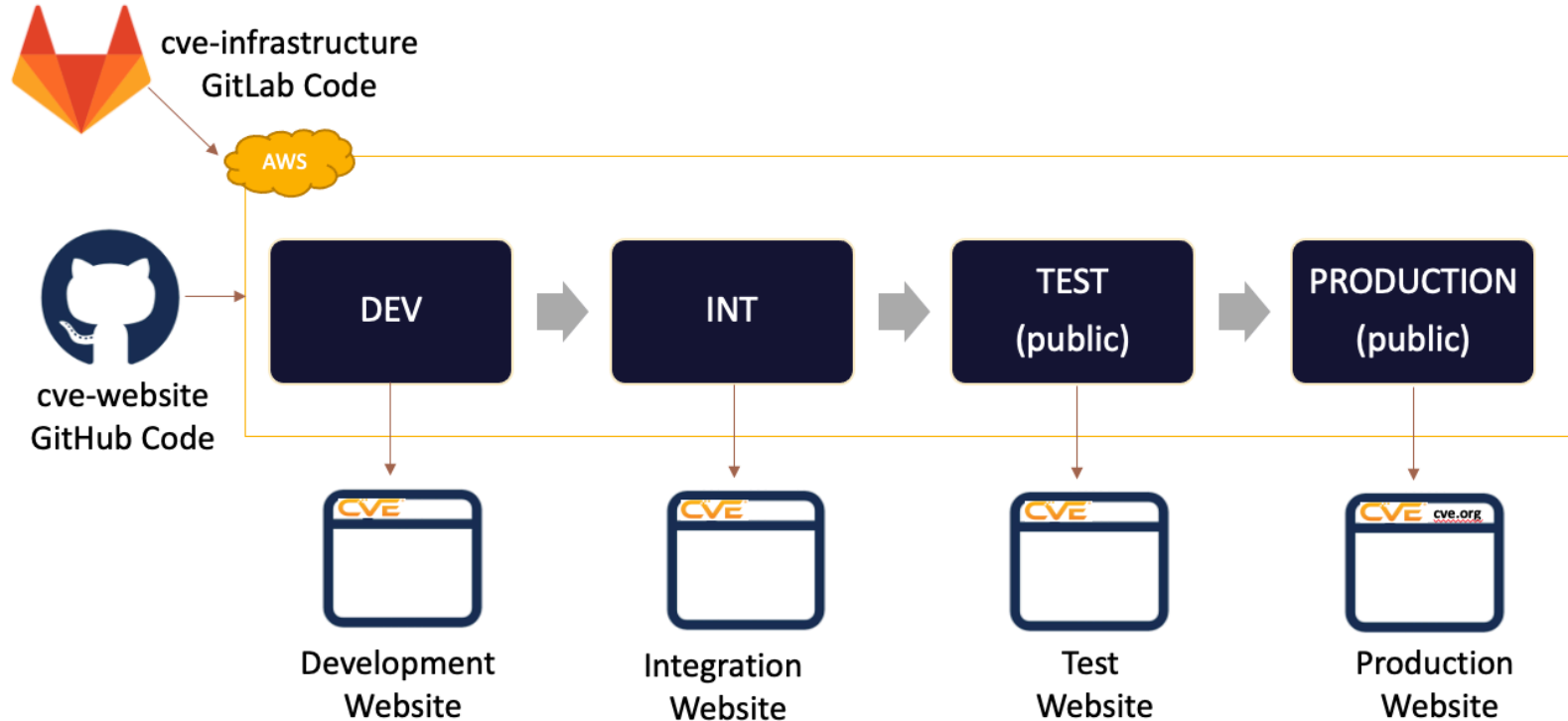




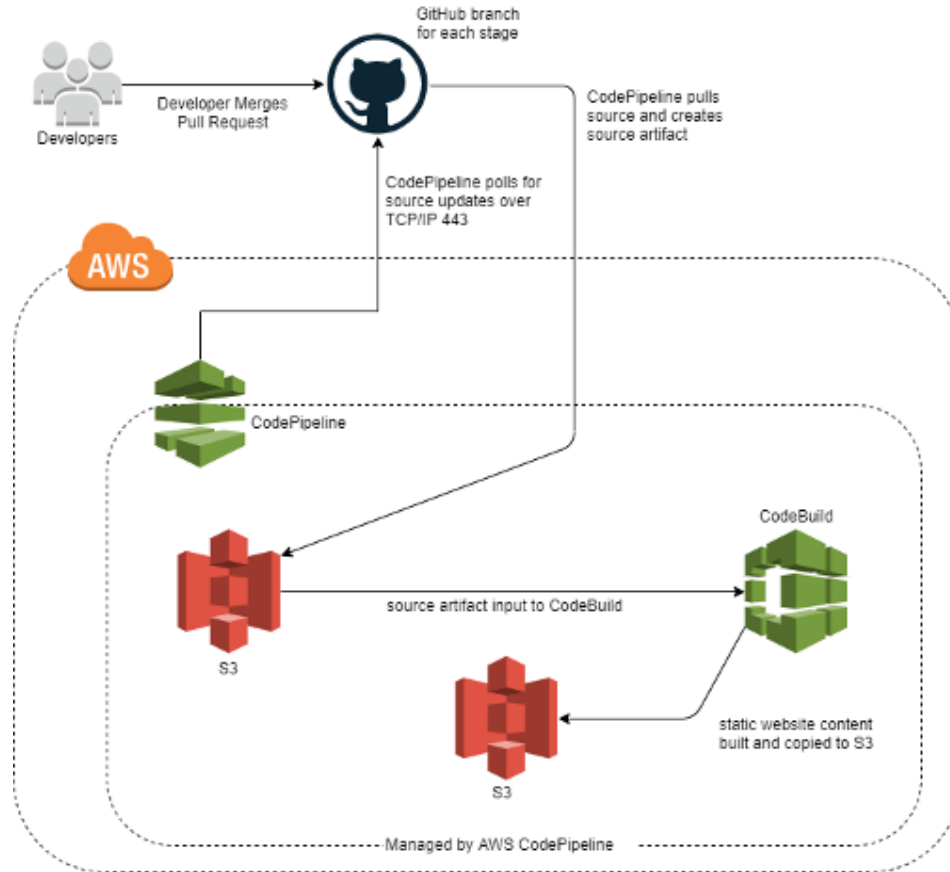
# CVE-Website

- Static website using CVE-Services API to dynamically generate content
- CVE-Website source code lives on GitHub
- All infrastructure created using AWS CloudFormation Templates stored in MITRE's internal GitLab
- Four different environments exist in AWS (separate account)

# CVE-Website Environments



# CVE-Website CI/CD Architecture



# CVE-Website CI/CD Components

- GitHub Repository
  - GitHub Advanced Security tools:
    - Dependabot scans/alerting
    - CodeQL SAST scans
- AWS
  - Code Build
  - Code Pipeline
  - S3
  - CloudFront



# CVE-Website AWS Components

- S3
- Cloud Front
- Cloud Watch
- Lambda
- API Gateway
- Route53
- VPC
- IAM
- SES (Simple Email Service)
- WAF



DEV  
SEC  
OPS  
DAYS

PITTSBURGH

DevSecOps for the Community: Building, Provisioning and Deploying CVE's Infrastructure and Services

# Future DevSecOps Improvements

**Carnegie  
Mellon  
University**

Software  
Engineering  
Institute



# Future DevSecOps Improvements

- Dynamic Application Security Testing (DAST)
  - Currently no automated DAST solutions in place
    - Burp Suite
    - OWASP Zap
  - Improved Monitoring Strategy
    - Additional AWS resource monitoring
    - MITRE internal security monitoring
    - DevSecOps metrics

DEV  
SEC  
OPS  
DAYS

PITTSBURGH

DevSecOps for the Community: Building, Provisioning and Deploying CVE's Infrastructure and Services

# Questions?

**Carnegie  
Mellon  
University**  
Software  
Engineering  
Institute

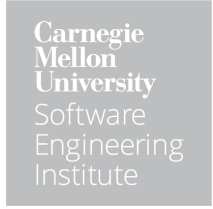
# References

- <https://github.com/CVEProject/cve-services>
- <https://www.cve.org/AllResources/CveServices>
- <https://github.com/CVEProject/cve-website>
- <https://www.cve.org/About/Overview>



PITTSBURGH

# Contact Information



**Shane T. Ficorilli**  
**Senior Cyber Security Engineer**

Email: [sficorilli@mitre.org](mailto:sficorilli@mitre.org)