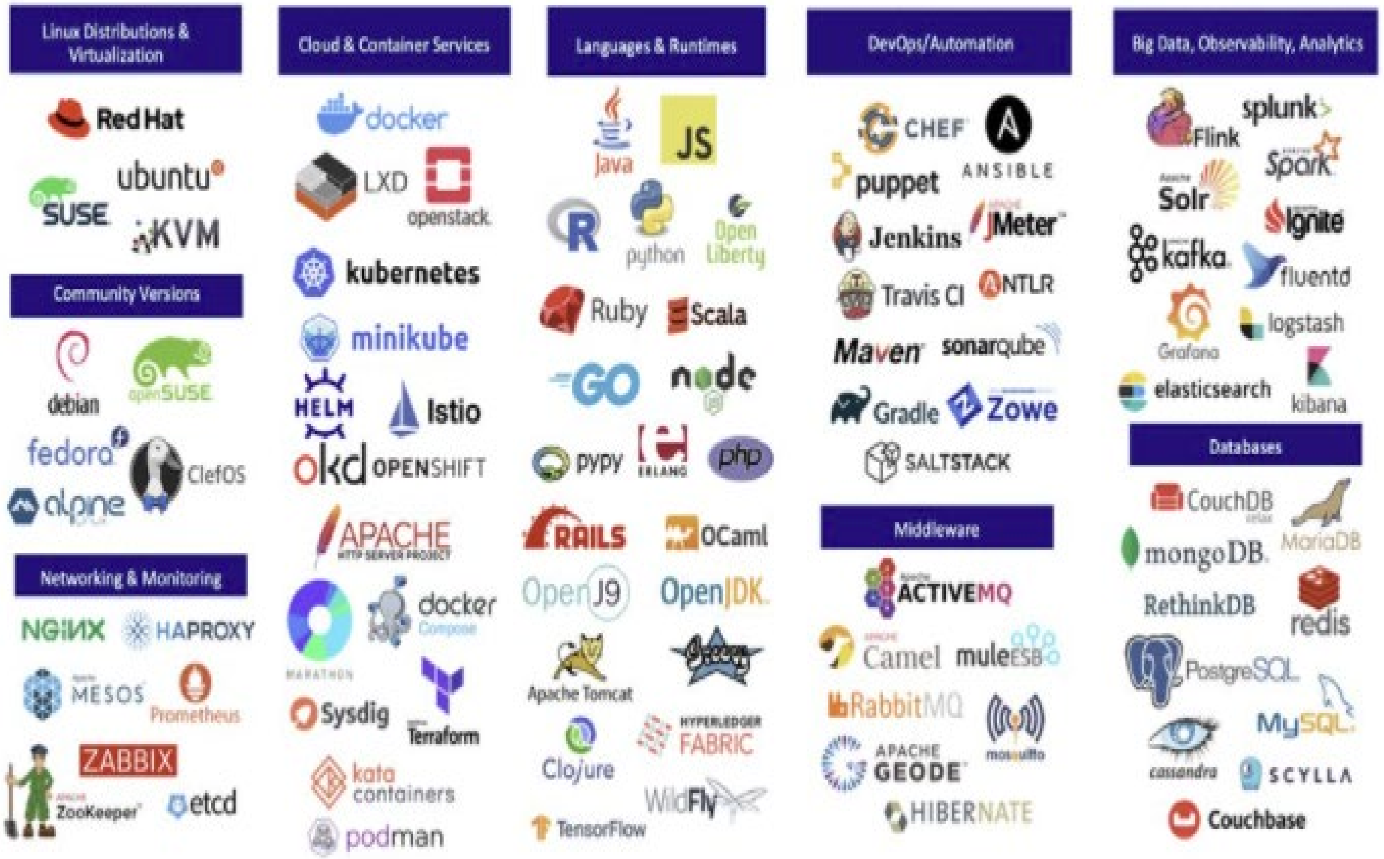
# Securing the Software Supply Chain: Transparency in the Age of the Software Driven Society

Chris Hughes

CISO & Co-Founder @ Aquia Inc.

# Open Source Adoption – The **Good**

- Open Source expedites innovation
- Creates a robust community and ecosystem
- Enables cross-organizational collaboration
- Metrics:
  - 97% of organizations are using OSS
  - 77% of organizations have increased OSS use
  - 79% of organizations sponsor OSS organizations
  - Highest increases involve OSS DevOps and Cloud-native CI/CD Tools


Linux Distributions & Virtualization

Community Versions

Networking & Monitoring

Cloud & Container Services

Languages & Runtimes

DevOps/Automation

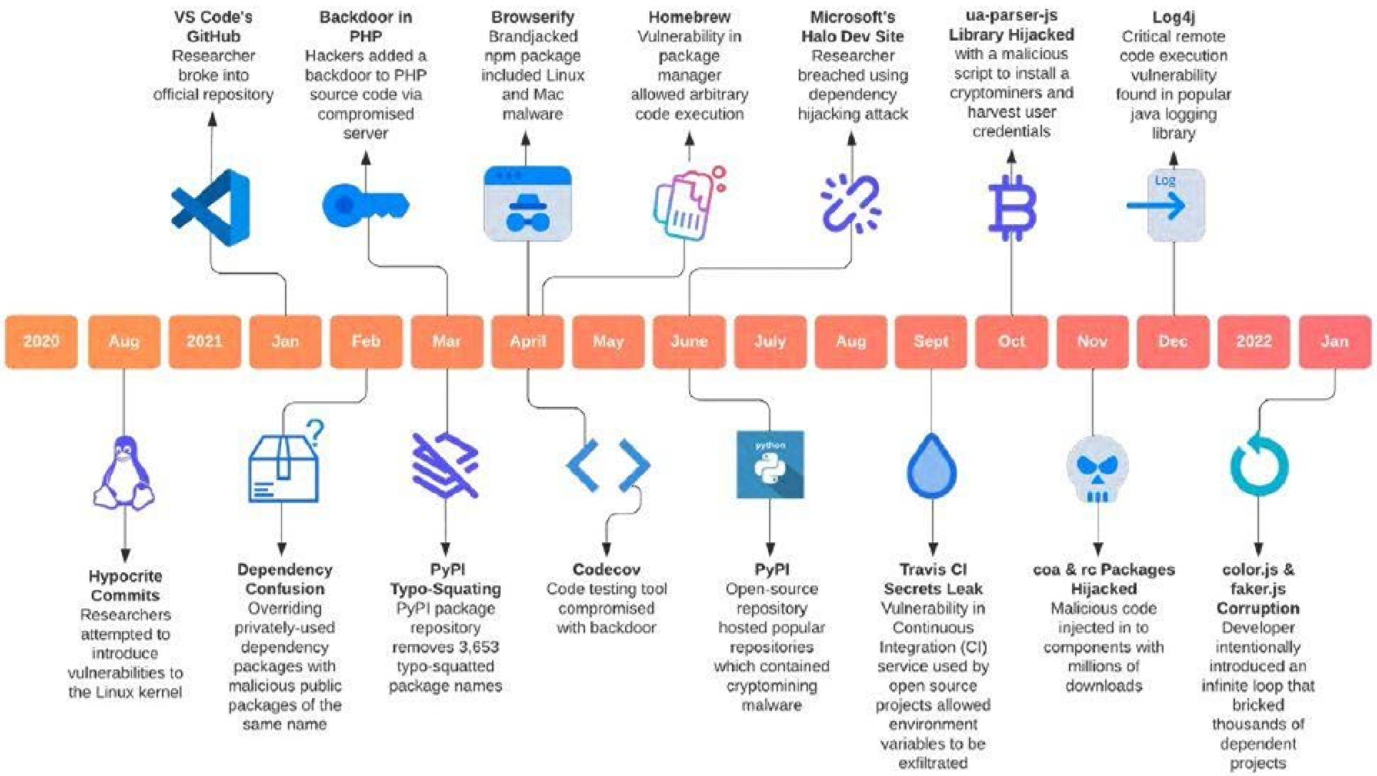
Middleware

Big Data, Observability, Analytics

Databases

# Open Source Adoption – The **Bad**

- Experts estimate 60-80% of modern software is comprised of OSS (Linux Foundation)
- Software supply chain attacks on the rise
- Many projects supported by unpaid volunteers
- Incidents such as Log4j send organizations scrambling – lack of visibility at the component level



**VS Code's GitHub** Researcher broke into official repository

**Backdoor in PHP** Hackers added a backdoor to PHP source code via compromised server

**Browserify** Brandjacked npm package included Linux and Mac malware

**Homebrew** Vulnerability in package manager allowed arbitrary code execution

**Microsoft's Halo Dev Site** Researcher breached using dependency hijacking attack

**ua-parser-js Library Hijacked** with a malicious script to install a cryptominers and harvest user credentials

**Log4j** Critical remote code execution vulnerability found in popular java logging library

2020 Aug 2021 Jan Feb Mar April May June July Aug Sept Oct Nov Dec 2022 Jan

**Hypocrite Commits** Researchers attempted to introduce vulnerabilities to the Linux kernel

**Dependency Confusion** Overriding privately-used dependency packages with malicious public packages of the same name

**PyPI Typo-Squating** PyPI package repository removes 3,653 typo-squatted package names

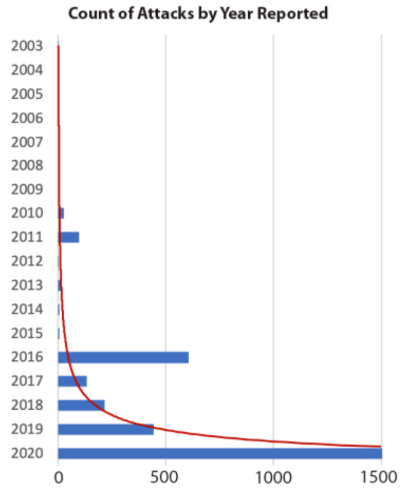
**Codecov** Code testing tool compromised with backdoor

**PyPI** Open-source repository hosted popular repositories which contained cryptomining malware

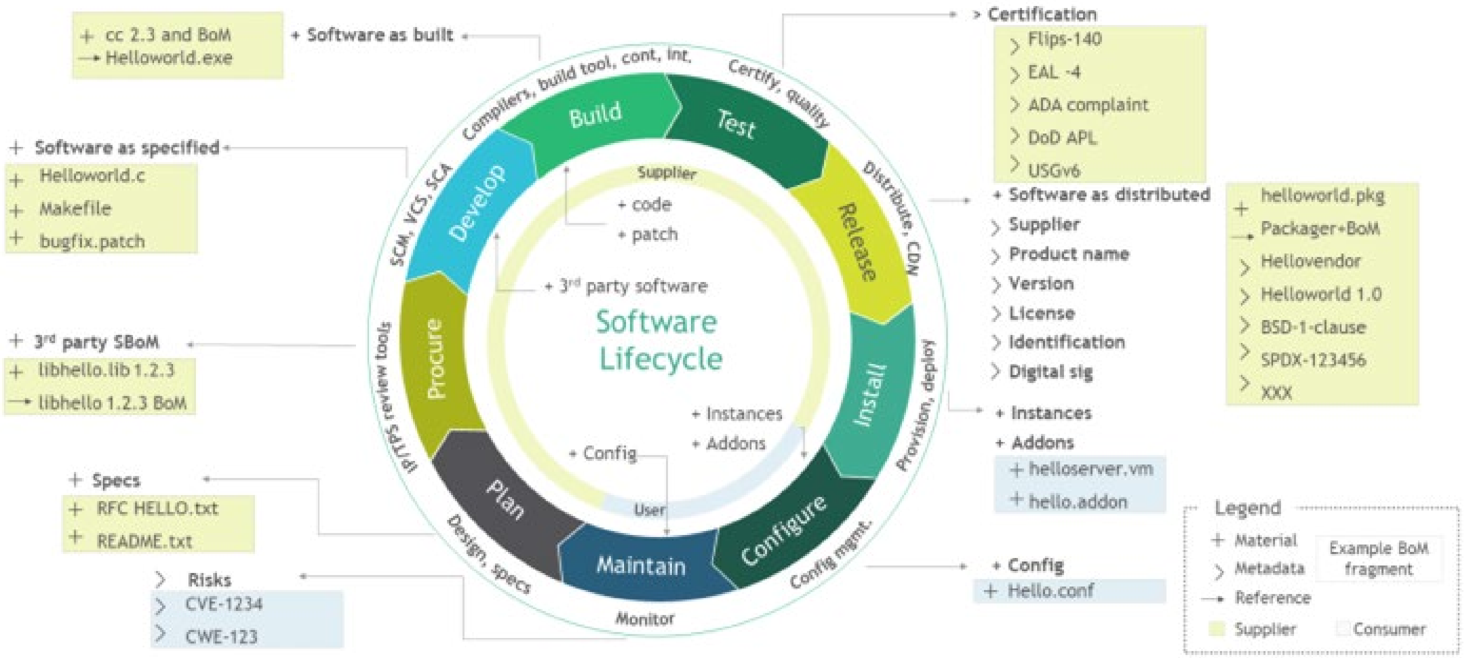
**Travis CI Secrets Leak** Vulnerability in Continuous Integration (CI) service used by open source projects allowed environment variables to be exfiltrated

**coa & rc Packages Hijacked** Malicious code injected in to components with millions of downloads

**color.js & faker.js Corruption** Developer intentionally introduced an infinite loop that bricked thousands of dependent projects



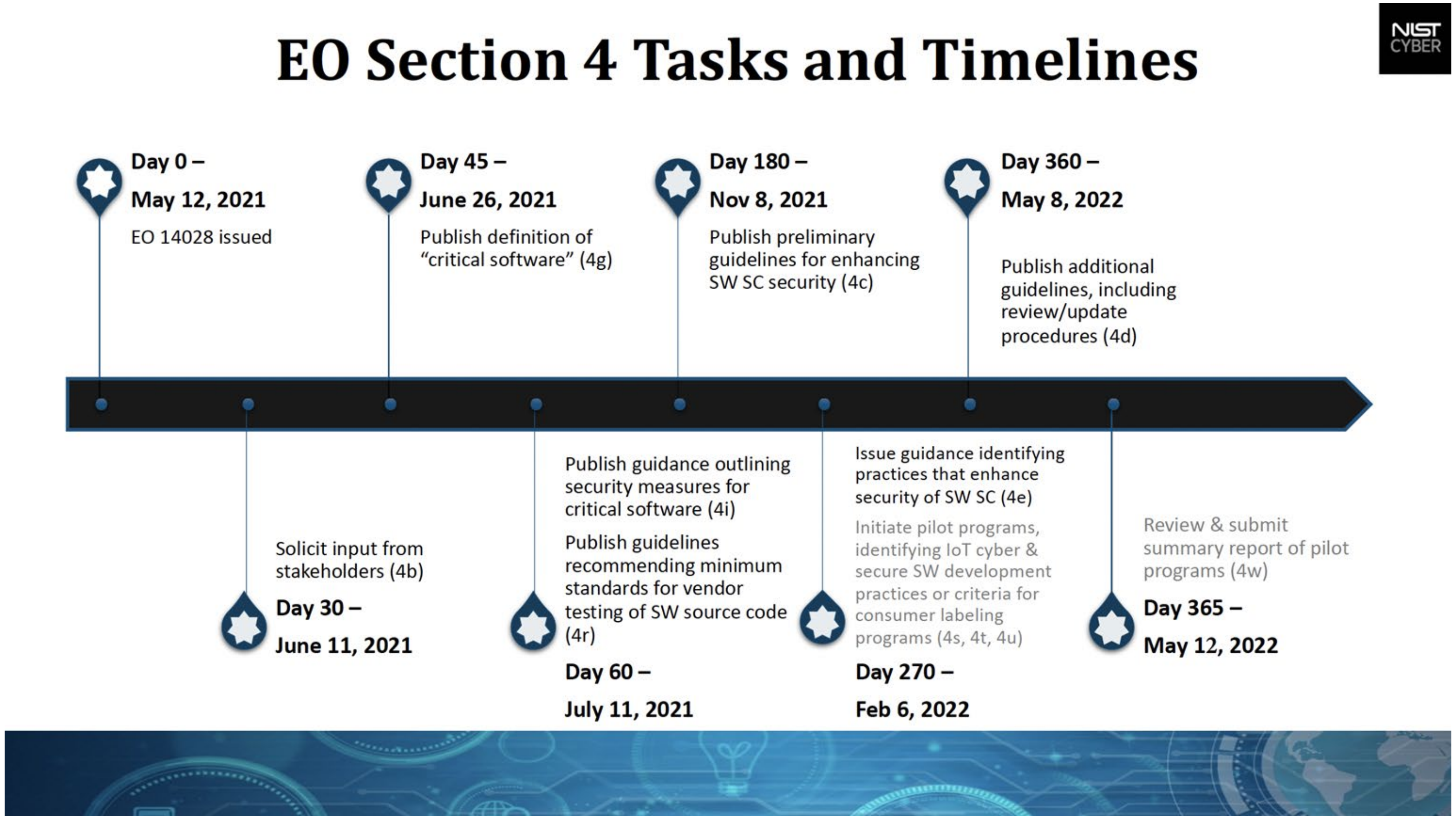
# OSS Adoption – What To Do?



- Establishing a robust Cybersecurity Supply Chain Risk Management (C-SCRM) program is a great step forward
- Engage with orgs such as OpenSSF, LinuxFoundation and others
- Crowdsourcing is catching on
- NIST 800-161r1 – Cyber Supply Chain Risk Management Practices for Systems and Organizations – Appendix F
  - Foundational, Sustaining and Enhancing Capabilities
  - SCA/SBOM/VEX, Centralized Hardened Internal Repos of OSS etc.

# Timeline of Notable Federal Focus

- May 12th – Cyber EO served as the primary driver for enforcing Federal focus on SW Supply Chain – Specifically Section 4
- NIST has:
  - Held workshops on enhancing C-SCRM
  - Published new Secure Software Development Framework (SSDF)
  - Published C-SCRM Guidance 800-161 Rev1 (May 5th, 2022)



## EO Section 4 Tasks and Timelines

**Day 0 – May 12, 2021**
EO 14028 issued

**Day 30 – June 11, 2021**
Solicit input from stakeholders (4b)

**Day 45 – June 26, 2021**
Publish definition of "critical software" (4g)

**Day 60 – July 11, 2021**
Publish guidance outlining security measures for critical software (4i)

Publish guidelines recommending minimum standards for vendor testing of SW source code (4r)

**Day 180 – Nov 8, 2021**
Publish preliminary guidelines for enhancing SW SC security (4c)

**Day 270 – Feb 6, 2022**
Issue guidance identifying practices that enhance security of SW SC (4e)

Initiate pilot programs, identifying IoT cyber & secure SW development practices or criteria for consumer labeling programs (4s, 4t, 4u)

**Day 360 – May 8, 2022**
Publish additional guidelines, including review/update procedures (4d)

**Day 365 – May 12, 2022**
Review & submit summary report of pilot programs (4w)

# NIST Software Security in Supply Chains: Open Source Software Controls

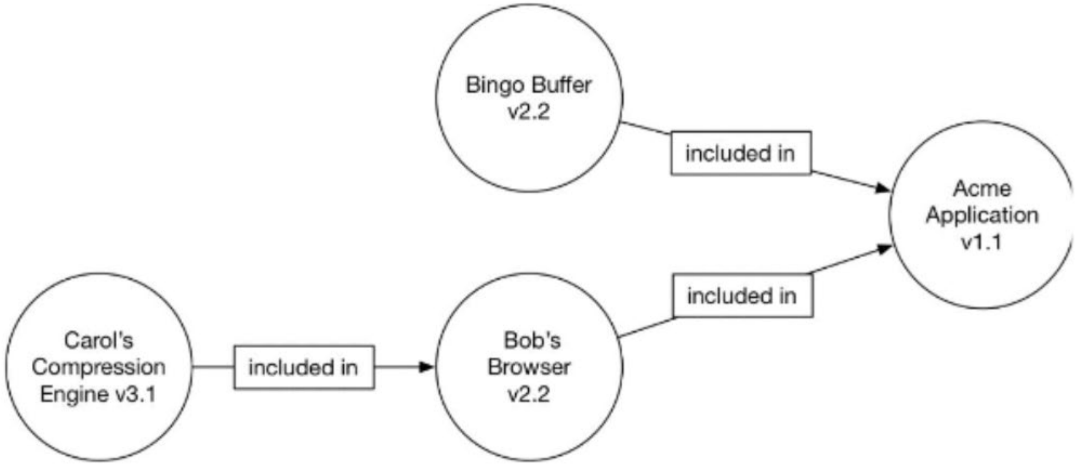
**Published capabilities across levels of maturity**

- **Foundational**
  - Utilize SSDF Protect/Response guidance
  - Ensure OS components are acquired via secure channels from trustworthy repos
- **Sustaining**
  - Utilize SCA on in-house codebases to look for vulnerable components
  - Create/maintain internal repos or libraries of known/good OSS components for developers to use
- **Enhancing**
  - Prioritize the use of more secure programming languages
  - Automate the pipeline of collecting, storing and scanning OSS components for internal repos prior to introduction to the dev environments
- **OMB Memo M-22-18 "Enhancing the Security of the Software Supply Chain through Secure Software Development Practices"**
  - Agencies MUST obtain self-attestation to conformity with secure software development practices for all third-party software used by the agency (e.g. SSDF and NIST Cyber EO Software Supply Chain Guidance)
  - Agencies may determine a third-party assessment/3PAO is required
  - SBOM's may be required by agencies in solicitation requirements (must be in formats as defined by NTIA)

# CISA/NTIA SBOM Efforts

- Originated at NTIA and now moved over to CISA, along with Dr. Allan Friedman
- Held "SBOM-o-Rama" in late 2021
- SBOM Workstreams 2022
    - Cloud & Online Applications
    - On-Ramps & Adoption
    - Sharing & Exchanging
    - Tooling & Implementation
- Leading Formats
    - SWID
    - CycloneDX
    - SPDX

| **Baseline Software Component Information** |
|---|
| Supplier Name |
| Component Name |
| Unique Identifier |
| Version String |
| Component Hash |
| Relationship |
| Author Name |



# Notable Industry Efforts

- White House held Software Security Summit in early 2022
- 3 High Level Goals
  - Securing OSS Production
  - Improving Vulnerability Discovery & Remediation
  - Shorten Ecosystem Patching Response Time
- Key Focus Areas:
  - Developer Education/Certification
  - Digital Signatures
  - OpenSSF IR Team
  - SBOM Everywhere
  - Risk Assessment Dashboard – 10k OSS Projects

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

THE LINUX FOUNDATION

WHITEPAPER
The Open Source Software Security Mobilization Plan

# Guidance Galore

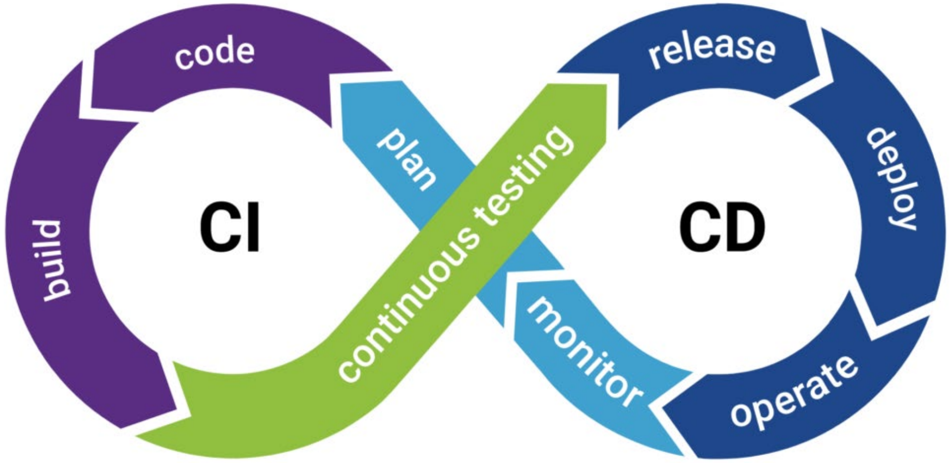
- NIST Secure Software Development Framework (SSDF)
- Supply Chain Levels for Software Artifacts (SLSA)
- NSA/CISA - Securing the Software Supply Chain for Developers
- OWASP Software Component Verification Standard (SCVS)
- Cloud Native Computing Foundation (CNCF) - Software Supply Chain Best Practices

Long story short, we have no shortage of guidance and emerging best-practices but we need to bridge the divide from theory to practice.

Many of the recommended best-practices and guidance also may be difficult particularly for SMB's to meet, further consolidating access to innovative SMB's and technologies for the Federal Government

# CI/CD Pipelines – The Good

- CI/CD ADOPTION HAS CHANGED THE WAY DEVELOPERS DELIVER SOFTWARE
- HAS ENABLED SECURITY TOOLING AUTOMATION AND INTEGRATION – E.G. "SHIFTING SECURITY LEFT"
- ENABLES ROBUST TOOLCHAINS TO ACHIEVE FULL CI/CD CAPABILITIES AND SECURITY REQUIREMENTS



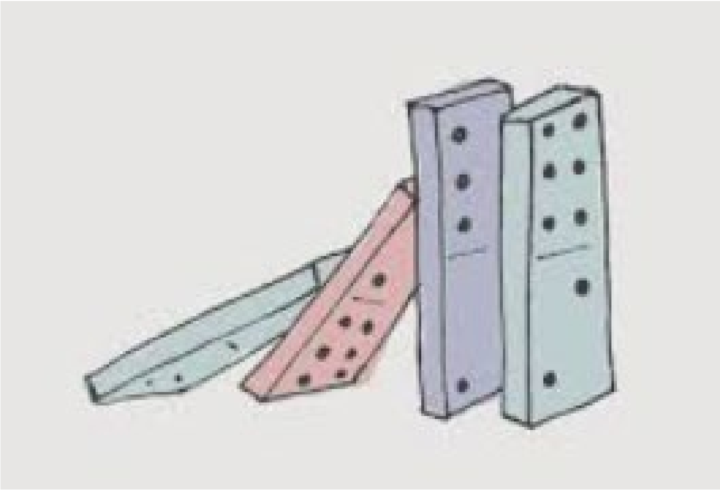
# CI/CD Pipelines – The Bad

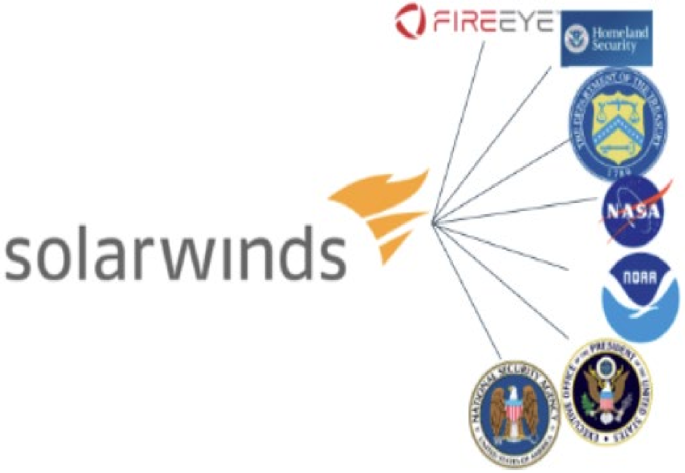
Many organizations haven't adopted unified CI platforms, leading to a myriad of integrations and complexity

While the Pipeline(s) facilitate secure delivery, they are part of your attack surface – organizations must address this

A compromise of the pipeline leads to massive supply chain security concerns and cascading impacts

Malicious actors are even compromising signing systems and releasing signed malicious payloads

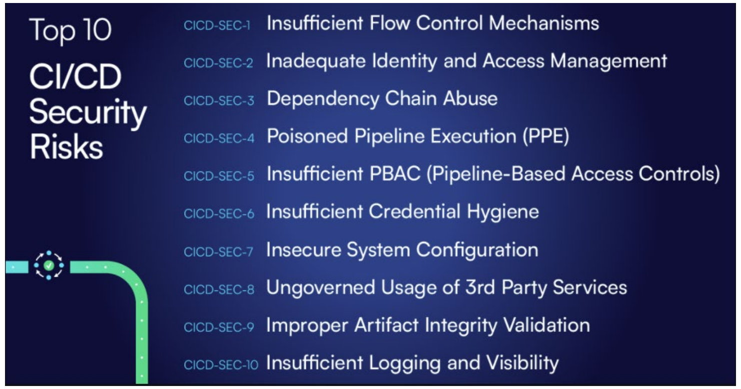




# CI/CD Pipelines – What to do

SLSA

- Your CI/CD pipeline enables value delivery but also can be a threat vector
- Cider Security has released excellent CI/CD Risk Lists and Best Practices
- Threat Model/Adversary Emulation
- Supply chain Levels for Software Artifacts (SLSA) - security framework
  - Prevent tampering
  - Improve Integrity
  - Secure Packages



Top 10 CI/CD Security Risks

| | |
|---|---|
| CICD-SEC-1 | Insufficient Flow Control Mechanisms |
| CICD-SEC-2 | Inadequate Identity and Access Management |
| CICD-SEC-3 | Dependency Chain Abuse |
| CICD-SEC-4 | Poisoned Pipeline Execution (PPE) |
| CICD-SEC-5 | Insufficient PBAC (Pipeline-Based Access Controls) |
| CICD-SEC-6 | Insufficient Credential Hygiene |
| CICD-SEC-7 | Insecure System Configuration |
| CICD-SEC-8 | Ungoverned Usage of 3rd Party Services |
| CICD-SEC-9 | Improper Artifact Integrity Validation |
| CICD-SEC-10 | Insufficient Logging and Visibility |

# Kubernetes & Containers – Don't Neglect Security

- Palo Alto's Unit 42 discovered 99% of Kubernetes Helm charts in Artifact Hub have insecure configurations
- Public Container Registries such as Docker Hub, Quay and Google Container Registry containers include critical findings in up to 91% of images
- Recommendations:
  - Utilize Container/Manifest Scanning
  - Pre-Hardened Images
  - Image Signing/Hashing
  - Leverage Guidance such as CIS, CNCF, DoD Container Hardening Guide and Kubernetes STIG
  - Scan Containers throughout lifecycle
  - Update IR Plans and Playbooks to account for Kubernetes and Containers
  - These insecure configurations and vulnerabilities exist in IaC too

# Kubernetes & Containers

- Kubernetes and Containers are closely linked with Cloud-native architecture and DevSecOps Adoption
- Up to 75% of global organizations have adopted Containers
- Kubernetes is the de-facto Container Orchestration tool of choice
- Reduced development timelines, cost optimization and improved scalability

# SaaS Security - The overlooked Software Supply Source

- Organizations are increasingly consuming applications and software in the form of SaaS
- Large enterprises are consuming upwards of 200~ SaaS applications, adding up to 10 new SaaS apps a month
- IT/Security control roughly 20% of SaaS usage
- SaaS consumers should implement SaaS Governance/Security, including SBOM's
- Recent Twilio incident involved 130 other SaaS providers