Cloud Native SecurityCon

EUROPE

Cloud Native SecurityCon EUROPE

Secure the Software Supply Chain

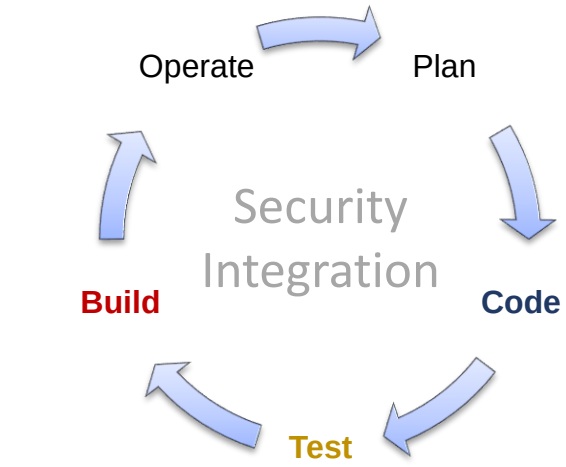
Guide and Enhance your Code Security Posture with the CNCF Best Practices Document

Ryan Gibbons – 

Conor Rogers – 

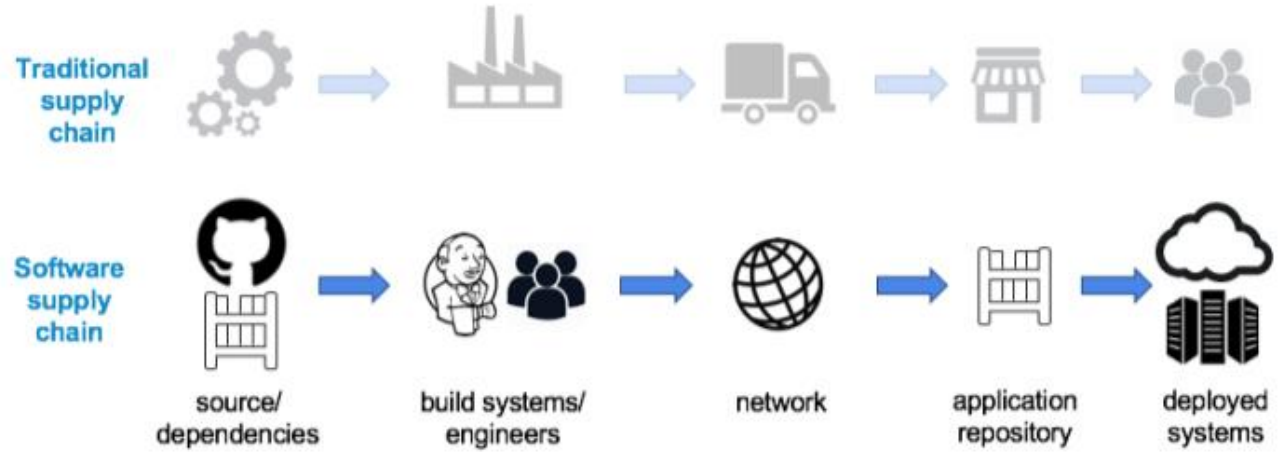
The Situation

- Security threats shifting left
- Broad lack of awareness of software supply chain security practices
  - Knowledge gaps
  - Data gaps
- Limited guidance on how to secure the software supply chain tooling
  - Started to get some movement with SLSA
  - Most guidance focuses on application security outcomes and not the underlying capabilities
- A large company with a diverse technical environment



Capture the Imagination

- Tell the story
- Introduce a simple term – Software Supply Chain



- Leverage current society awareness of supply chains
- Company aware – 3M knows supply chains

- Enhance the story with data and discovery
- Use current events to enhance the narrative
  - SolarWinds, Log4j
- Build trust through effective services and clear direction

Our Starting Place

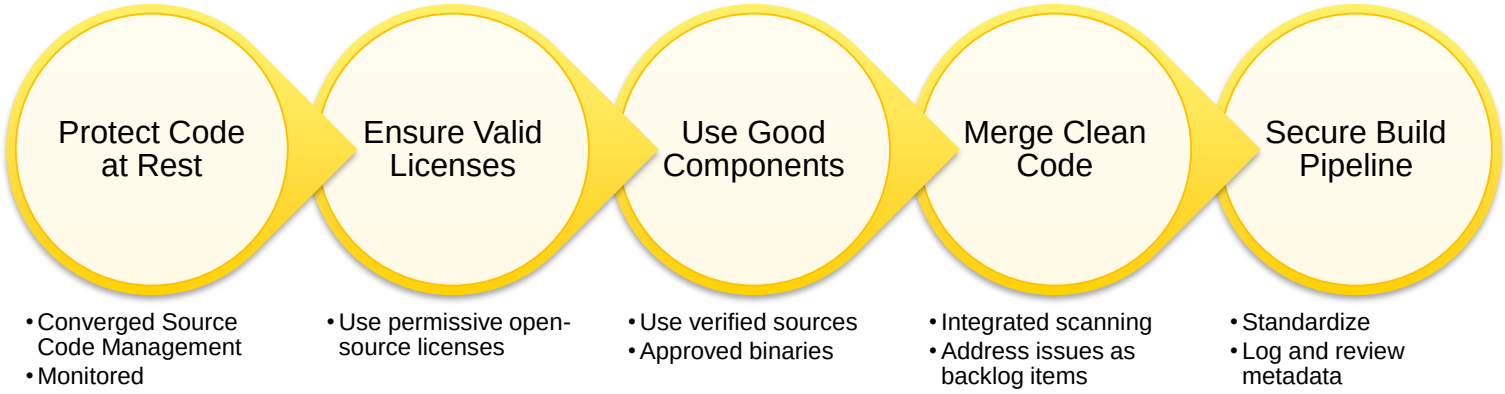
- Had an existing program to enhance our application code security practice
- Already communicating the vision and strategy for shifting security left
- Actively leveraging contemporary best practices for secure software development
- Delivered additional capabilities for software supply chain
  - Goal of avoiding dumping problems on developers

Along the way…

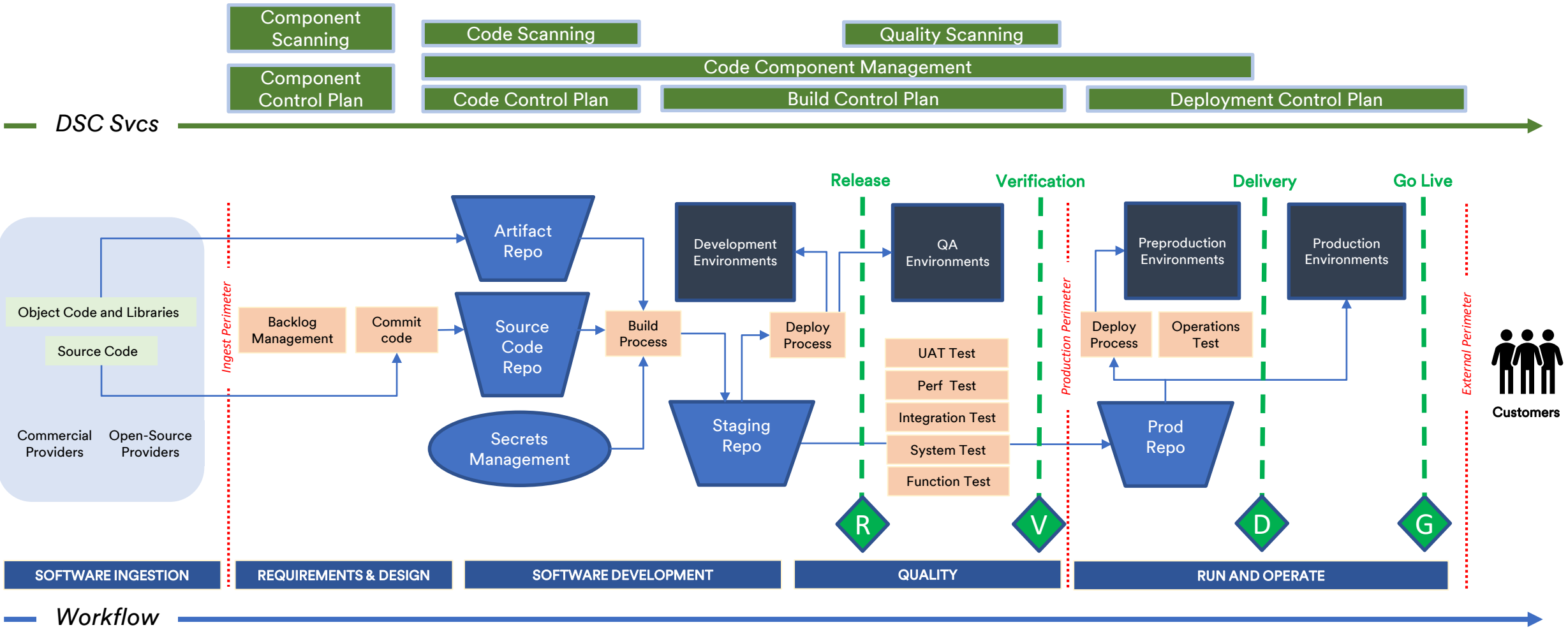
- Respond to events like SolarWinds and Log4j
- Review new industry recommendations like SLSA, the Biden executive order and CNCF Software Supply Chain Best Practices

Initial Strategy (Pre-SSCP)

2021 – Strategic View : Completing the Next-Generation Application **Code Security Capability Set**



Software Supply Chain Architecture



May 12th 2021

Cloud Native SecurityCon EUROPE

THE WHITE HOUSE

MENU

BRIEFING ROOM

Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

The requirement for the standards based SBOM

CNCF Software Supply Chain Security Best Practices (SSCP)

Cloud Native SecurityCon EUROPE

SAN FRANCISCO, Calif. – May 14, 2021 – The Cloud Native Computing Foundation® (CNCF®), which builds sustainable ecosystems for cloud native software, today announced a new paper, Software Supply Chain Security Best Practices, designed to provide a holistic approach to supply chain security by highlighting the importance of layered defensive practices. The paper was compiled by members of the CNCF Security Technical Advisory Group (TAG), which produces resources that enable secure access, policy control, and safety for operators, administrators, developers, and end users across the cloud native ecosystem.

https://project.linuxfoundation.org/hubfs/CNCF_SSCP_v1.pdf

SSCP - The Principles

1. Trust: Every step in a supply chain should be “trustworthy” due to a combination of cryptographic attestation and verification.

2. Automation: Automation is critical to supply chain security and can significantly reduce the possibility of human error and configuration drift.

3. Clarity: The build environments used in a supply chain should be clearly defined, with limited scope.

4. Mutual Authentication: All entities operating in the supply chain environment must be required to mutually authenticate using hardened authentication mechanisms with regular key rotation.

SSCP – The Practices

1.Securing The Source Code: 24 practices which can be applied to enhance the security posture covering integrity, identity and access , attestation, automation, security testing, verification, authentication, reporting and controlled environments

2.Securing Materials: 33 best practices covering risk management, OSS health, verification, automation, SCA and license scanning, control and management, attestation and the SBOM

3.Securing Build Pipelines: 55 best practices and guidance for securing all components of the build pipeline, its components , the infrastructure, the build workers , the environments , automation , verification, authorization and access , orchestration and staging

4.Securing The Artefacts: 11 best practices to secure the software packages covering authentication verification, access authorization, attestation signing and controlled environments

5.Securing the Deployments: Best practices for securing the deployments which covers trust, integrity, resilience and integrity and greatly references the Update Framework (TUF)

SSCP – How We Used

Cloud Native SecurityCon EUROPE

Learn

- Solidified new terms
- New knowledge asset
- Parsed into clauses and practices
- Created a controls list

Align to Strategy

- Well matched to our 2021 objectives
- Combined artefacts and deployments sections
- Carefully matched the language to the org vernacular

Adjust to the Environment

- Added specific evaluation criteria
- Merged with existing controls (monitoring, etc)
- Moved some controls around (DAST) to fit our strategy and security testing better

Evaluate

- Assessed capabilities supporting the software supply chain
  - Code repo
  - Component store
  - Build and deploy pipelines
  - Other

Example

ID	Control objective	Category	Control	Assurance Level	Implementation Guidance	Evidence Required	Control Owner	Target System	Capability Status

Example

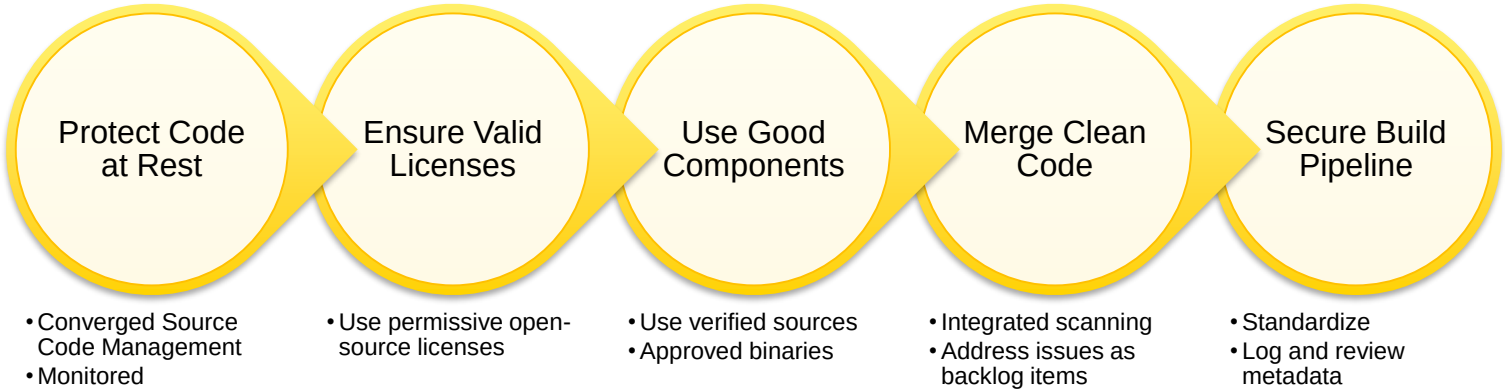
ID	Control objective	Category	Control	Assurance Level	Implementation Guidance	Evidence Required	Control Owner	Target System	Capability Status
SC-1.1.1	Securing the Source Code	Verification	Require Signed Commits	Moderate	Sign source code commits and tags to ensure integrity and non-repudiation of code using GPG or s/mime keys	*	* Lucky Person	Source Code Control System	*
SM-1.5.2	Securing Materials	Verification	Track dependencies	Moderate	Generate and maintain a supply chain inventory to help identify the software vendors, suppliers, and sources used in an organization with the associated software and versions	*	* Lucky Person 2	Artifact Manager	*

SSCP - It Really Helped!

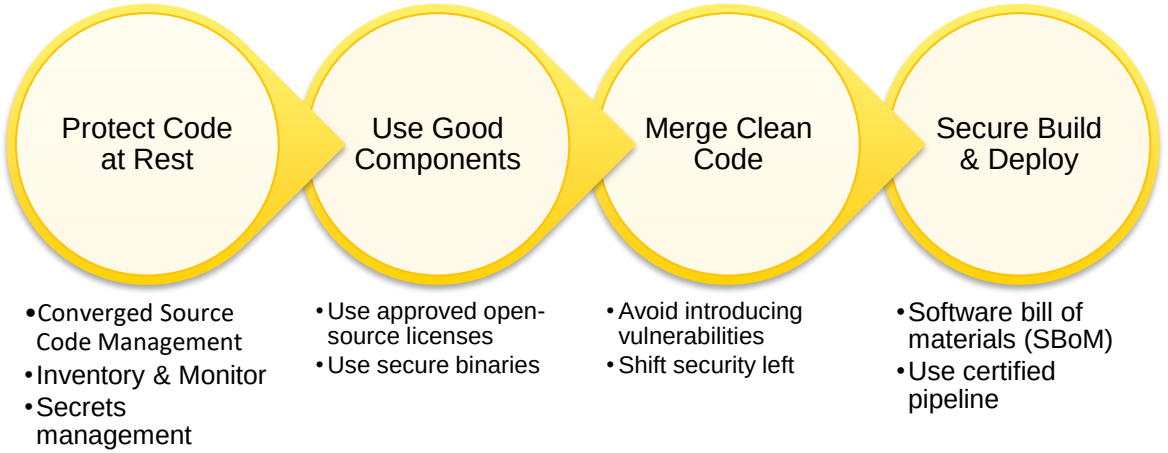
- Our vision and strategy was reinforced by an industry reference paper
- Provided a clear view of best practices to inform our program and priorities
- Added control and requirement detail for tooling supporting SDLCs
- Gave a good benchmark to assess our strengths and weaknesses across the SDLC
- Generated organizational awareness and excitement (indirectly)

Strategy Evolution

2021 – Strategic View : Completing the Next-Generation Application **Code Security Capability Set**



2022 – Strategic View : **Secure Software Supply Chains**



Advice

- Be transparent and report openly and visually
  - Real environment data really helped advance the story
- Create alliances and coalitions with cooperation, collaboration and partnership
  - Create hard partnerships – great feedback!
- Know your executives, sponsors and stakeholders and their needs and constraints
  - Find high level champions. Sell it as modern and career enhancing
- Provide platform solutions and a paved road
  - Make it easier for developers to do the right thing – provide solutions
  - Make it harder for developers to do the wrong thing – harden policy
- Get mileage out of current events
  - Plenty to pick from lately…
- Provide effective training
- Market and evangelize the capabilities of the application security function
- Measure and report cost savings delivered while increasing security posture