DevOps Trends: Enterprise DevOps Strategy for Compliance and Keeping Code Secure

Vaughn Marshall, Product Manager
Tom McQuitty, Technical Consultant

February 2026

Abstract

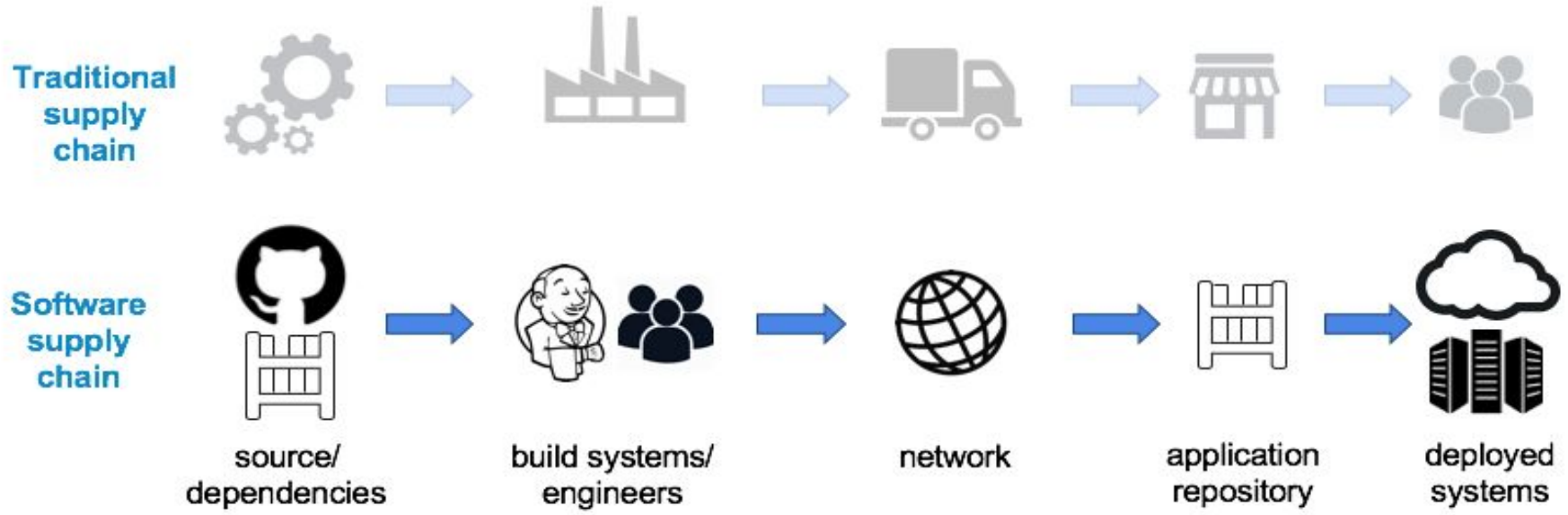
As application architectures evolve towards ever greater complexity, the job of security and compliance officers only increases. During this session we'll share the trends we've seen evolving in this space, from the rise of static application analysis to SBOMs and more.

Evolving Workloads

- It’s no longer just COBOL and traditional z/OS workloads
- Java with 3rd party libraries
- NodeJS & Python
  - 3rd party packages

Software Supply Chain - Defined

A process of getting a product to the customer



CNCF Software Supply Chain Best Practices

Ignoring Supply Chain Security has Real Consequences

U.S. SECURITIES AND EXCHANGE COMMISSION

Search SEC.gov

COMPANY FILINGS

ABOUT | DIVISIONS & OFFICES | ENFORCEMENT | REGULATION | EDUCATION | FILINGS | NEWS

- Newsroom
- Press Releases
- Speeches and Statements
- SEC Stories
- Securities Topics
- Media Kit
- Press Contacts
- Events
- Webcasts
- Media Gallery

Press Release

SEC Charges SolarWinds and Chief Information Security Officer with Fraud, Internal Control Failures

Complaint alleges software company misled investors about its cybersecurity practices and known risks

FOR IMMEDIATE RELEASE
2023-227

Washington D.C., Oct. 30, 2023 — The Securities and Exchange Commission today announced charges against Austin, Texas-based software company SolarWinds Corporation and its chief information security officer, Timothy G. Brown, for fraud and internal control failures relating to allegedly known cybersecurity risks and vulnerabilities. The complaint alleges that, from at least its October 2018 initial public offering through at least its December 2020 announcement that it was the target of a massive, nearly two-year long cyberattack, dubbed "SUNBURST," SolarWinds and

Related Materials

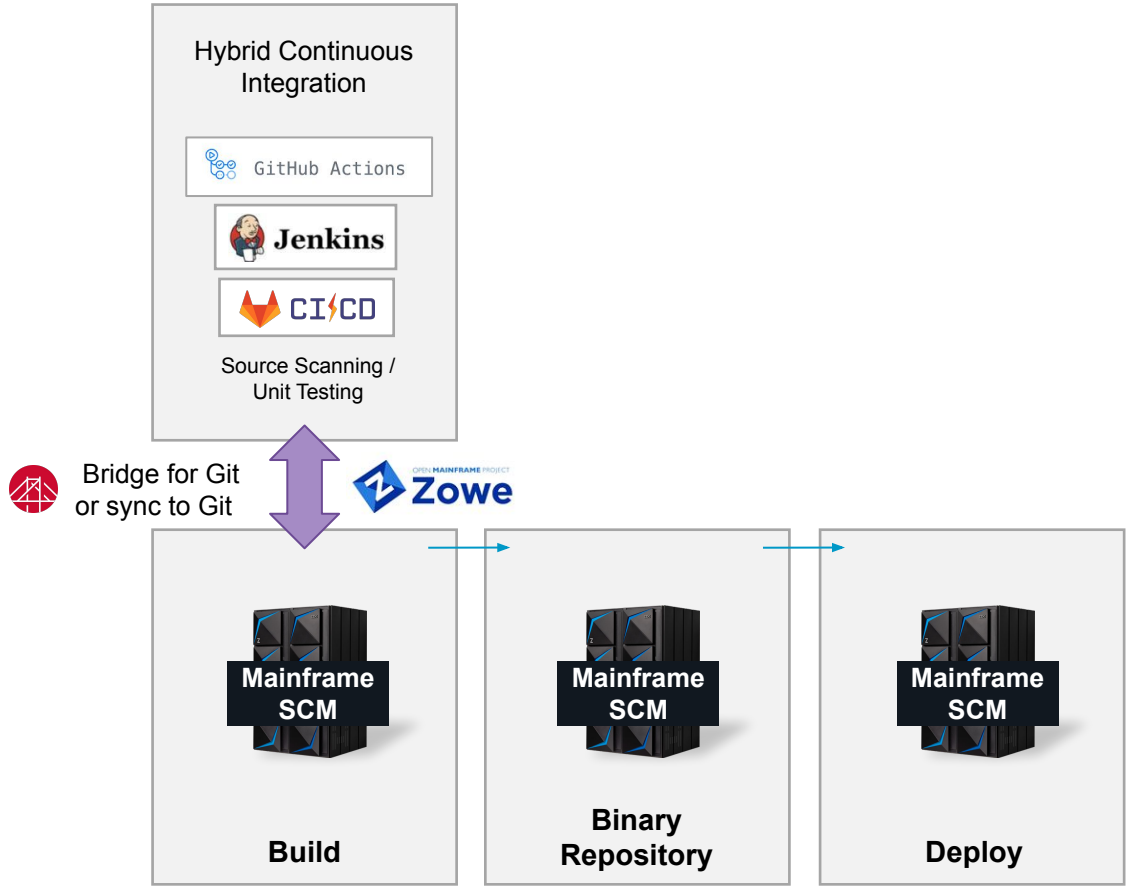
- SEC Complaint

Code Reviews

- Peer review of changes mandated part of SDLC
- Best Practices:
  - Focus on Small Chunks
  - Establish Clear Guidelines: Use a checklist with defined criteria (security, performance, maintainability).
  - Promote a Positive Culture - avoid fault finding
- Tooling:
  - Pull / Merge Requests in Enterprise Git Server
  - Endevor Package Approvals UI

Static Application Analysis

- Scanning of application source to:
  - Find bugs
  - Enforce code styles
  - Find security issues
- Shifts Quality Left
  - Issues found earlier in life cycle are less costly to fix
- Best Practices:
  - Enforce quality gates
  - Mirror z/OS Code off host for hybrid pipelines / tooling
  - Leverage OOTB Git integrations
- Tooling:
  - SonarQube, Checkmarx, Veracode

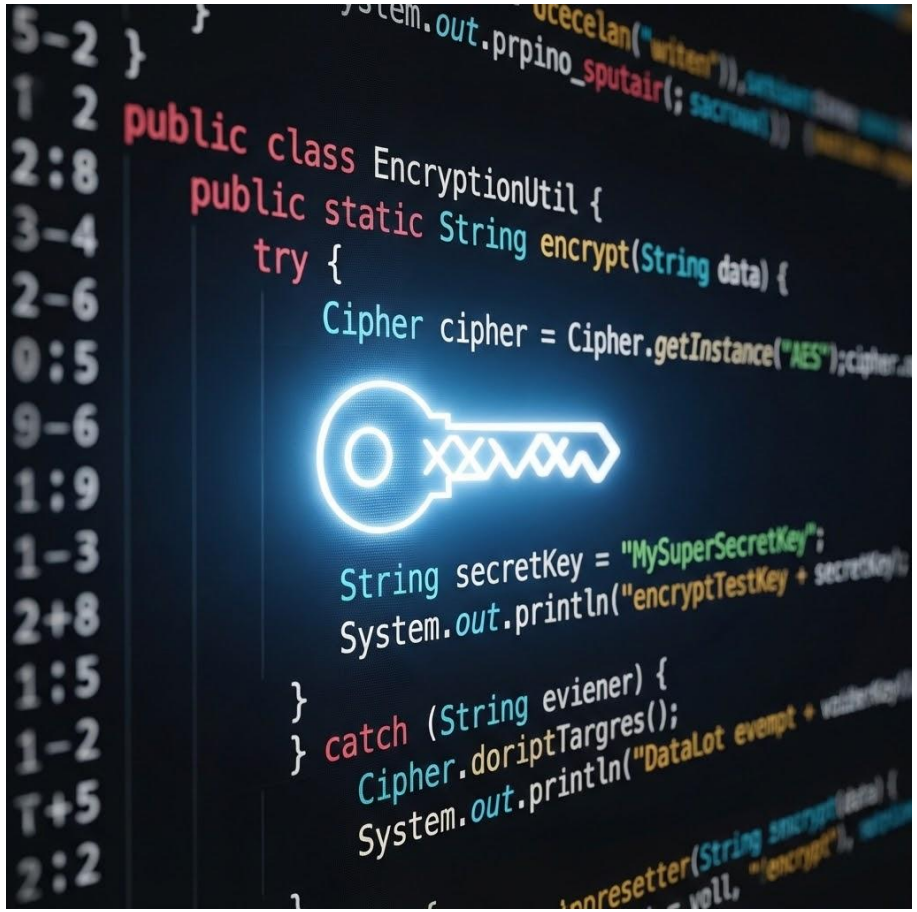


Software Composition Analysis

- SCA is the scanning of application code and dependencies to determine the content of an application
- Identifies:
  - 3rd party libraries
  - Licenses
  - Vulnerabilities
- Especially relevant for Java applications or applications with heavy 3rd party or open source dependencies
- Helps create Software Bills of Materials (SBOMs)
- Tooling:
  - Blackduck, Snyk, JFrog Xray

Secrets Scanning

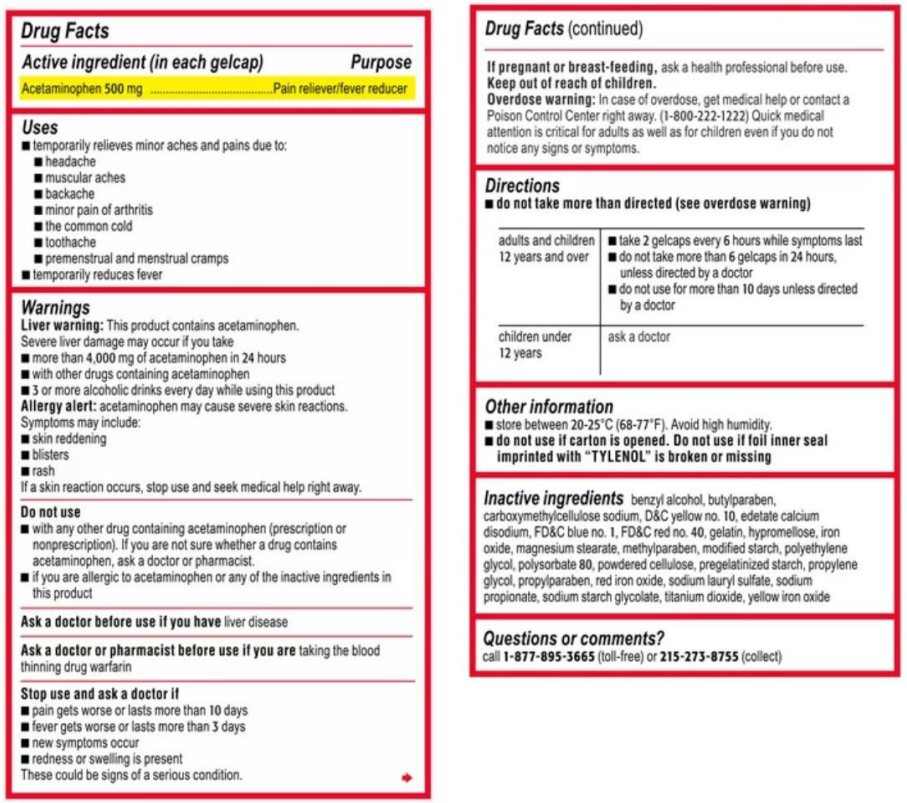
- Automated secrets scanning finds credentials in source code
- This practice prevents accidental exposure of sensitive keys and tokens
- Shift Left Security
- Best Practices:
  - Integrate into the pipeline for automated enforcement
- Tools:
  - Cycode, Integrated Enterprise Git Tooling (GitHub Secret Scanning, GitLab Secret Detection), Gitleaks
- Standards
  - SOC2 and ISO27001



Software Bill of Materials (SBOM)

SBOMs are like real-world product ingredient lists, an SBOM answers the question:

What's in the software?



Drug Facts

Active ingredient (in each gelcap) — **Purpose**

Acetaminophen 500 mg ..... Pain reliever/fever reducer

Uses

- temporarily relieves minor aches and pains due to:
  - headache
  - muscular aches
  - backache
  - minor pain of arthritis
  - the common cold
  - toothache
  - premenstrual and menstrual cramps
- temporarily reduces fever

Warnings

Liver warning: This product contains acetaminophen.
Severe liver damage may occur if you take

- more than 4,000 mg of acetaminophen in 24 hours
- with other drugs containing acetaminophen
- 3 or more alcoholic drinks every day while using this product

Allergy alert: acetaminophen may cause severe skin reactions.
Symptoms may include:

- skin reddening
- blisters
- rash

If a skin reaction occurs, stop use and seek medical help right away.

Do not use

- with any other drug containing acetaminophen (prescription or nonprescription). If you are not sure whether a drug contains acetaminophen, ask a doctor or pharmacist.
- if you are allergic to acetaminophen or any of the inactive ingredients in this product

Ask a doctor before use if you have liver disease

Ask a doctor or pharmacist before use if you are taking the blood thinning drug warfarin

Stop use and ask a doctor if

- pain gets worse or lasts more than 10 days
- fever gets worse or lasts more than 3 days
- new symptoms occur
- redness or swelling is present

These could be signs of a serious condition.

Drug Facts (continued)

If pregnant or breast-feeding, ask a health professional before use.
Keep out of reach of children.
Overdose warning: In case of overdose, get medical help or contact a Poison Control Center right away. (1-800-222-1222) Quick medical attention is critical for adults as well as for children even if you do not notice any signs or symptoms.

Directions

- **do not take more than directed (see overdose warning)**

adults and children 12 years and over	■ take 2 gelcaps every 6 hours while symptoms last ■ do not take more than 6 gelcaps in 24 hours, unless directed by a doctor ■ do not use for more than 10 days unless directed by a doctor
children under 12 years	ask a doctor

Other information

- store between 20-25°C (68-77°F). Avoid high humidity.
- **do not use if carton is opened. Do not use if foil inner seal imprinted with "TYLENOL" is broken or missing**

Inactive ingredients benzyl alcohol, butylparaben, carboxymethylcellulose sodium, D&C yellow no. 10, edetate calcium disodium, FD&C blue no. 1, FD&C red no. 40, gelatin, hypromellose, iron oxide, magnesium stearate, methylparaben, modified starch, polyethylene glycol, polysorbate 80, powdered cellulose, pregelatinized starch, propylene glycol, propylparaben, red iron oxide, sodium lauryl sulfate, sodium propionate, sodium starch glycolate, titanium dioxide, yellow iron oxide

Questions or comments?
call **1-877-895-3665** (toll-free) or **215-273-8755** (collect)

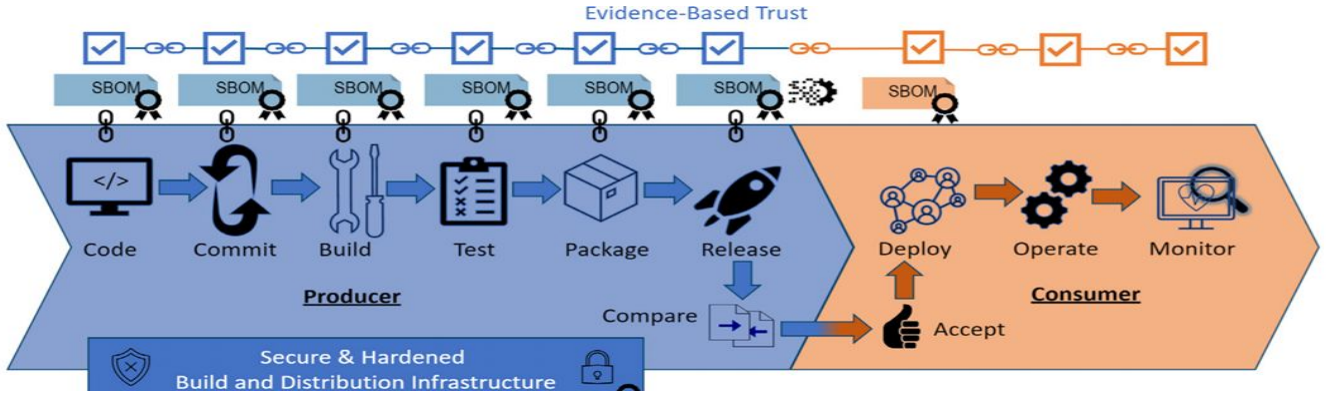
- *Enables transparency and decreases risk*

SPDX

CycloneDX

SBOM Use Cases

- SBOMs by themselves provide transparency only
- It's what you do with them that increases security
- Example use cases
  - Automated vulnerability scanning (grype, OWASP Dependency Track)
  - Ensuring runtime locations match expected contents
  - Securing handoffs between machines
  - Automated Policy Enforcement (Policy-as-Code)



Source: MITRE – Deliver Uncompromised: Securing Critical Software Supply Chains, 2021, Clancy, Ferraro, et al

What is a Policy?

- A policy is a rule that governs operations
- Policies required for compliance or maintaining standards
- Some policies are best practices, others may even be legislated

Traditional Policy Enforcement

- Maintained in policy documents or quality systems
- Validated manually (change review boards, governance meetings, checklists)
- Audited periodically to ensure compliance

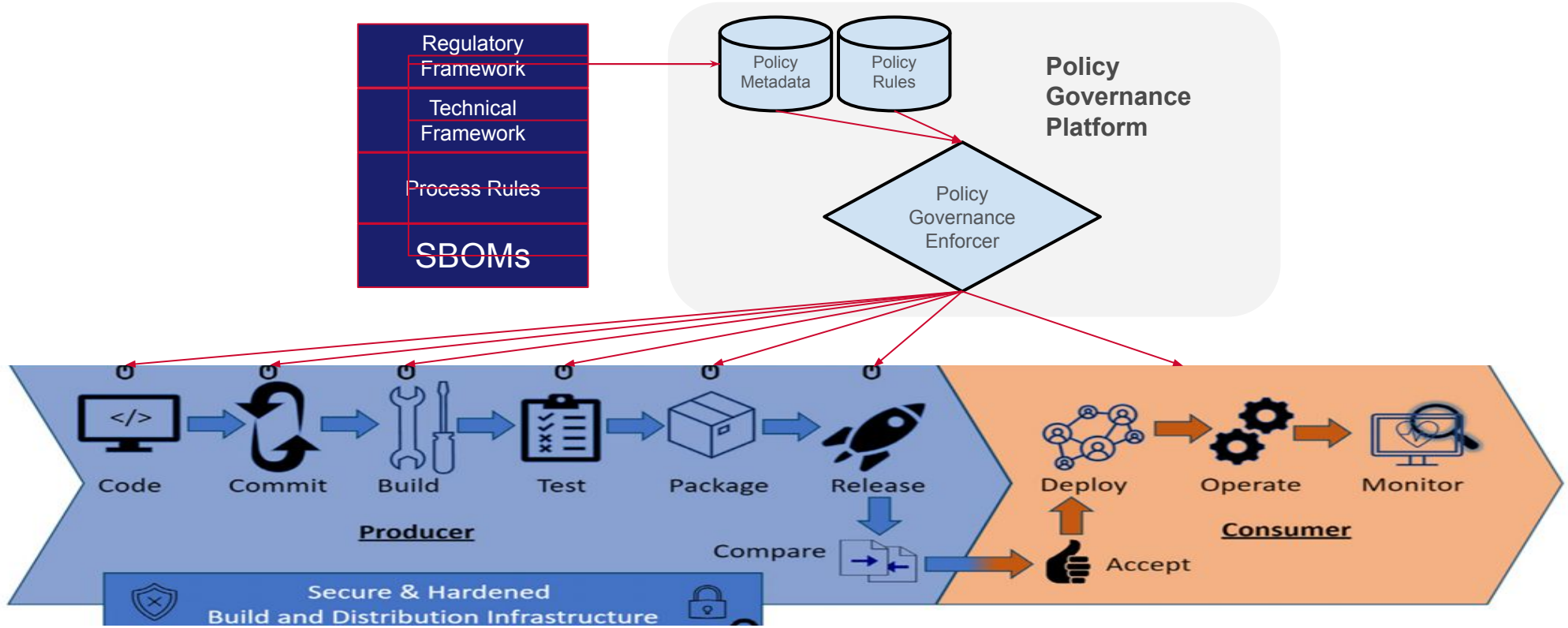
- Can be open to individual interpretation
- Large potential for human error, missed steps
- Not scalable – can’t audit every change!

Policy-as-Code

- Policies codified in standard format (e.g. OPA's Rego)
- Versioned in SCM, Changed via established process for code
- Continuously and automatically enforced
- Not open to interpretation – system behaves the same way every time
- Changes are controlled and auditable
- Policies are centralized and transparent
- No room for human error, continuous compliance, policies are consistently applied

SBOMs + Policy-as-Code: Improving Software Supply Chain Security

Policy Governance Automation is a continuously automated way to apply and enforce policy requirements as software supply chain artifacts are driven through pipelines from creation to production



Open Source Package Management

- Many languages / runtimes include automated package management
  - Python (pip), NodeJS (npm), Java (Maven)
- Enterprises should block public repositories
  - Major source of supply chain attacks
- Use an internal, private repository
  - Curation of packages
  - Quarantine packages for 24-48 hours to prevent attacks like NPM maintainer compromise
  - Enforce dependency pining to specific versions
  - Regularly audit contents for stale or unauthorized packages

Containers

- Secure the Image Supply Chain
- Create and maintain approved, hardened base images
- Regularly scan base image
- Manage Security Advisories for image consumers
- Scan product-level components added on top of base images
- Manage network policy around containers

GenAI Considerations

- Discover and Inventory all AI
  - Sanctioned and Shadow AI Discovery
- Policy and Governance
  - Define data handling and acceptable use
  - Access controls
  - Local or Hosted
- Secure Data Flows using DLP, encryption, and data anonymization
- Monitor and respond with observability
- Tooling:
  - Teramind, BrowseControl,

Final Thoughts

- Automate & enforce Security throughout the SDLC
- Shift security left where possible
- Nominate security champions
  - Organizational
  - Team representatives
- More Information: https://dora.dev/capabilities/pervasive-security

Technical Education Direct from the Experts

In-Person	Virtual	In-Person
European MTE Prague, Czech Republic Apr. 21-23, 2026	Virtual MTE Held Virtually June 23-25, 2026	North American MTE Plano, TX Oct. 20-22, 2026

Join a Mainframe Technical Exchange

- Network with peers and Mainframe technical experts
- Participate in technical how-to sessions and hands-on workshops, hear product updates, provide feedback
- No registration fee!

"The event covered all the relevant topics, and the content was amazing. The hands-on experience was also a good way to get actual experience with the tools."

Senthil Mathur, Manager, Accenture

Your feedback is important!

Submit a session evaluation for each session you attend:

www.share.org/evaluation

BROADCOM®
MAINFRAME SOFTWARE

Thank You


BROADCOM®