Qualys

Managing the Risk of Software Supply Chain Attacks

Mark Hahn, Nirav Kamdar, Alex Kreilein
Qualys
SREcon EMEA, October 2024

tcbtech.com/sw-risk

Overview

Threats:

Open-Source Software (OSS) are flourishing and are getting used by at least 90% of companies†. Modern applications are built on webs of open-source code, APIs, and third-party integrations.

89% of IT leaders believe enterprise open source is as secure or more secure than proprietary software‡.

† 2024 State of Open Source Report – OpenLogic, OSI, Eclipse

‡ The State of Enterprise Open Source: A Red Hat report

Background

Threats:

Modern tooling is increasingly detecting straight forward attacks, so instead of targeting end-users, hackers are compromising weak links in existing software supply chains.

Software supply chain (SSC) threats include tampering with updates (tainted updates), compromised third-party libraries, vulnerabilities in open-source packages, malicious code or malware in packages etc.

Threat

Software Supply Chain attacks have an average increase of 156% per year and there have been over 500 millions discovered malicious packages†.

Gartner predicts that by 2025, 45% of organizations worldwide will have experienced attacks on their software supply chains, a three-fold increase from 2021 ‡.

We have already seen the impacts of SolarWinds hack, Log4Shell, NotPetya, XZ Utils etc. In terms of dollar value, Software Supply Chain Attacks to Cost the World $60 Billion By 2025.

† Sonotype 10th Annual State of the Software Supply Chain report

‡ Gartner Identifies Top Security and Risk Management Trends for 2022

Qualys

Your software supply chain is bigger than you think

tcbtech.com/sw-risk

Your software supply chain is bigger than you think

Your software supply chain contains a lot more than code an libraries. It is a nexus of code, process and people that interact in very complex ways that can fail at any point.

Code

Libraries

Test Code

Test Framework

Prod Application

Prod Host Infra

CICD Pipeline

CICD Host OS

Code Repo Sys

Code Repo Host

Dev Laptop OS

SRE Laptop OS

3rd Party Apps

Browser Eco

Devs / DevOps

Workers

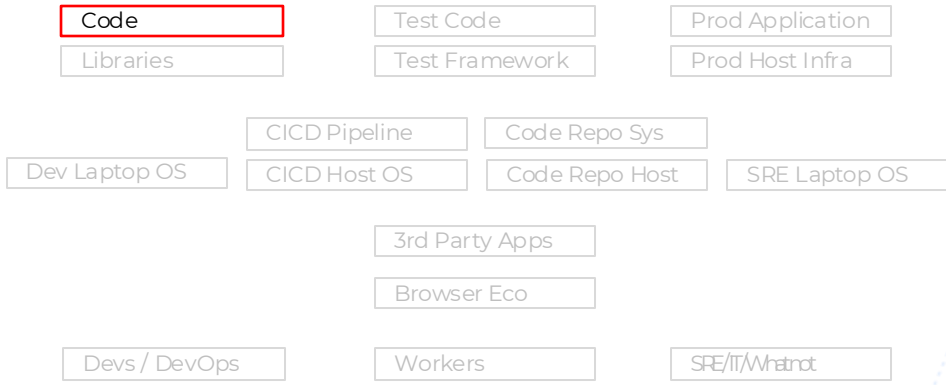
SRE / IT / Whatnot

Qualys

Your software supply chain is bigger than you think

tcbtech.com/sw-risk

Code



Threats:

Hard coded Passwords

https://nvd.nist.gov/vuln/detail/CVE-2024-20439

https://www.google.com/search?q=site%253Anvd.nist.gov+CWE-798+cisco

Injection Flaws - https://cwe.mitre.org/data/definitions/74.html

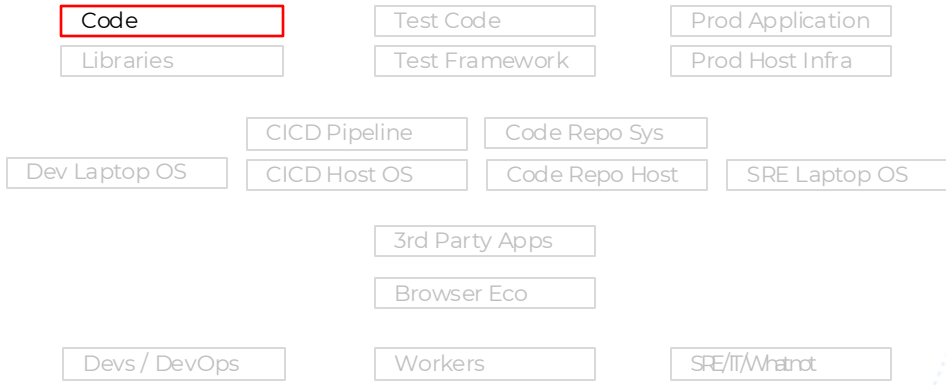
VMWare – Authenticated SQL Injection to RCE

https://nvd.nist.gov/vuln/detail/CVE-2024-38814

Fortinet: Unauthenticated RCE

https://nvd.nist.gov/vuln/detail/CVE-2024-47575

Code



Recommendations:

Don’t be your own worst enemy

OWASP top 10

https://owasp.org/www-project-top-ten/

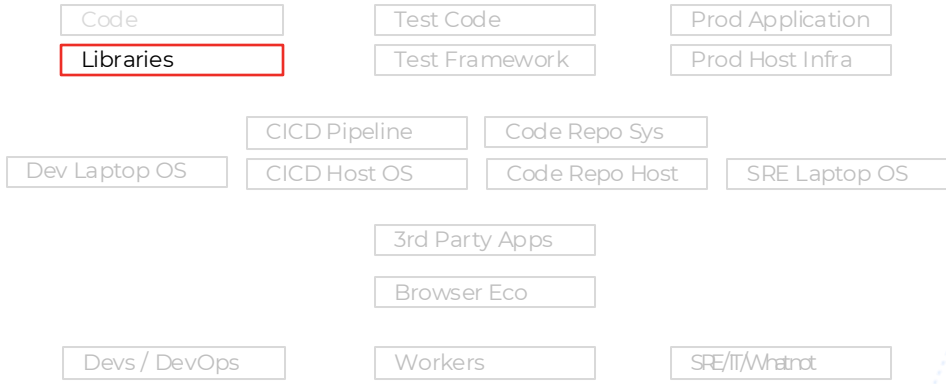
SANS Top 25

https://www.sans.org/top25-software-errors/

Static Application Security Testing Tools

SemGrep, SonarQube

Libraries



Threats:

Log4Shell

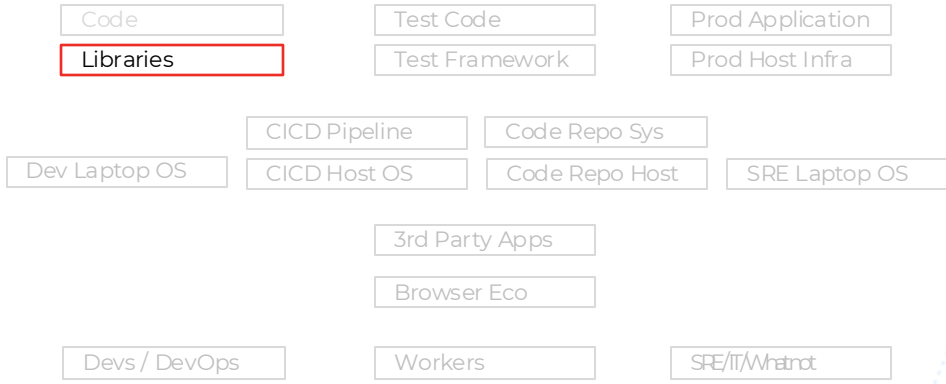
https://nvd.nist.gov/vuln/detail/CVE-2021-44228

https://en.wikipedia.org/wiki/Log4Shell

Leftpad

https://en.wikipedia.org/wiki/Npm_left-pad_incident

Libraries



Recommendations:

Vulnerability Scanning

- npm Audit
- OWASP dependency-check

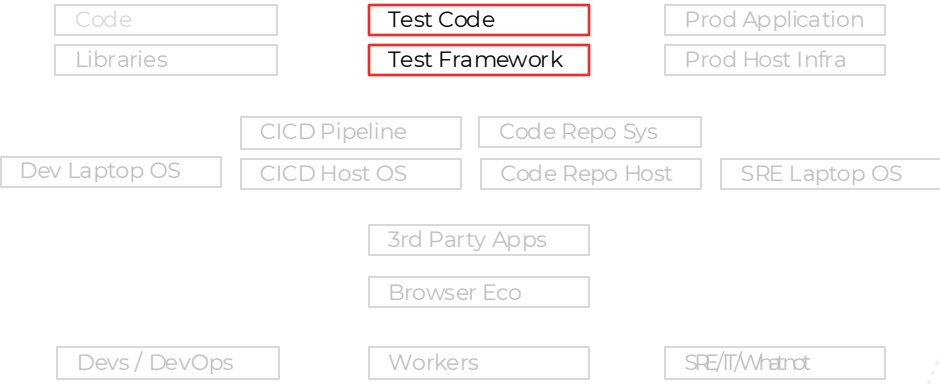
All dependencies come from a local curated repository

- Run static analyzers over the repository

Build a Software Bill of Materials (SBOM) / Vex

- Golden SBOM – approved for this specific application

Test Code / Test Libraries

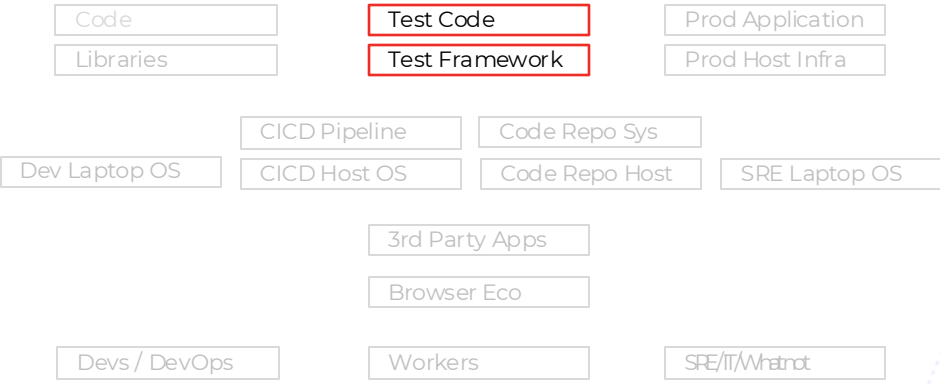


Threats:

XZ Utils

https://en.wikipedia.org/wiki/XZ_Utils_backdoor

Test Code / Test Libraries



Recommendations:

Vuln Scanning of test frameworks

- npm Audit
- OWASP dependency-check

All dependencies come from a local curated repository

- Run static analyzers over the repository

Production Application / Production Infrastructure Threats:

Apache Struts

https://nvd.nist.gov/vuln/detail/CVE-2023-50164

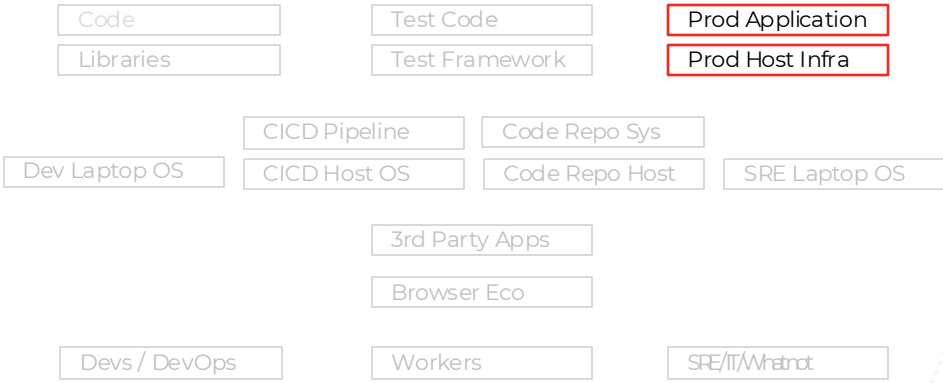
PHP RCEs:

https://nvd.nist.gov/vuln/detail/CVE-2024-8926

NodeJS

https://nvd.nist.gov/vuln/detail/CVE-2024-27980

Production Application / Production Infrastructure Recommendations:



Scan for vulnerabilities on your servers

Patch, patch, patch – or deploy, deploy, deploy

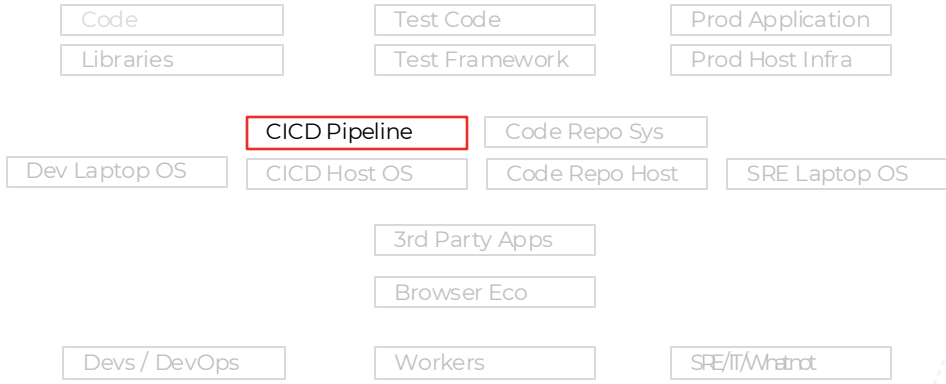
File Integrity Monitoring

Observability tools

Endpoint detection

Minimal, immutable OS distributions

CI/CD Pipeline

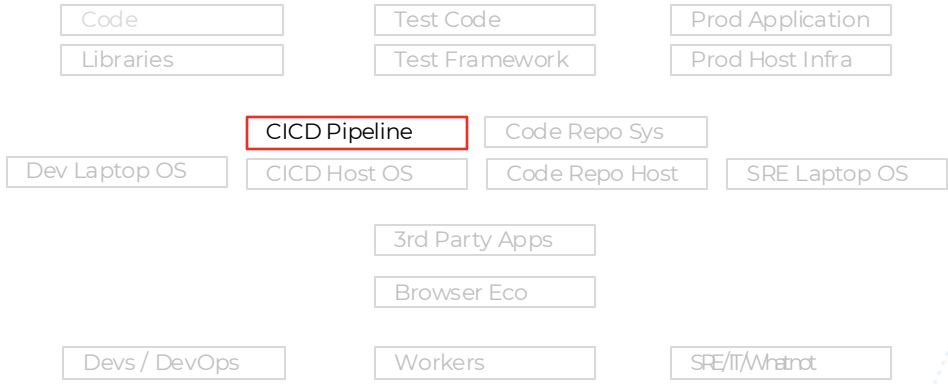


Threats:

CloudFlare Thanksgiving Day 2023 Incident

https://blog.cloudflare.com/thanksgiving-2023-security-incident/

CI/CD Pipeline



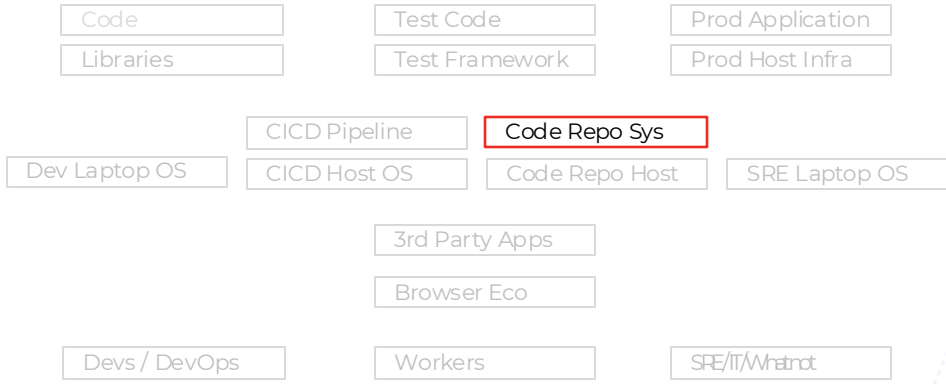
Recommendations:

Review pipeline changes as code changes

Limit who can modify pipeline code

Use OIDC in pipeline to access infrastructure

Code Repo System



Threats:

Stash

https://nvd.nist.gov/vuln/detail/CVE-2024-32231

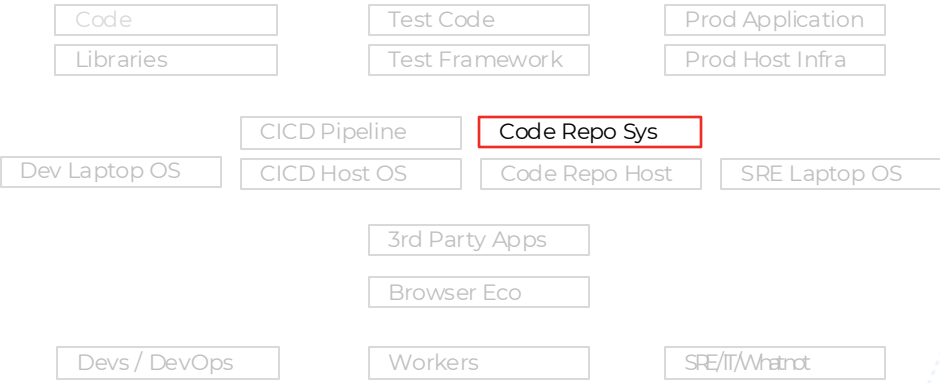
GitLab

https://nvd.nist.gov/vuln/detail/CVE-2024-6678

Gitea

https://nvd.nist.gov/vuln/detail/CVE-2024-6886

Code Repo System

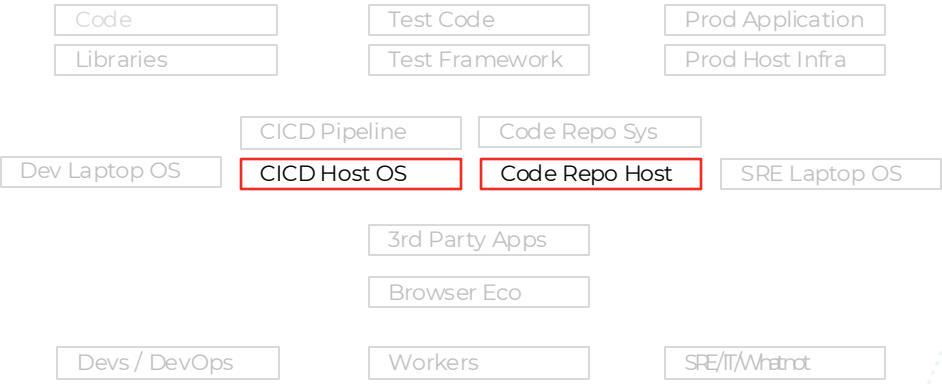


Recommendations:

Use a cloud provider; don’t self host

Patch, Patch Patch

Tooling Hosting



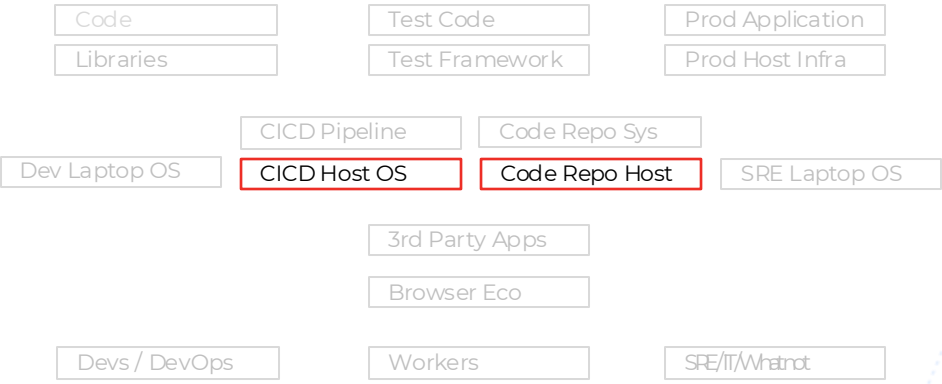
Threats:

Jenkins

https://www.jenkins.io/security/advisory/2024-01-24/

https://www.jenkins.io/security/advisory/2024-08-07/

Tooling Hosting



Recommendations:

Limit access to servers

Use a cloud provider, don’t self host

Patch, Patch, Patch

Development Systems

Threats:

Phishing emails

https://circleci.com/blog/jan-4-2023-incident-report/

Development Systems

Recommendations:

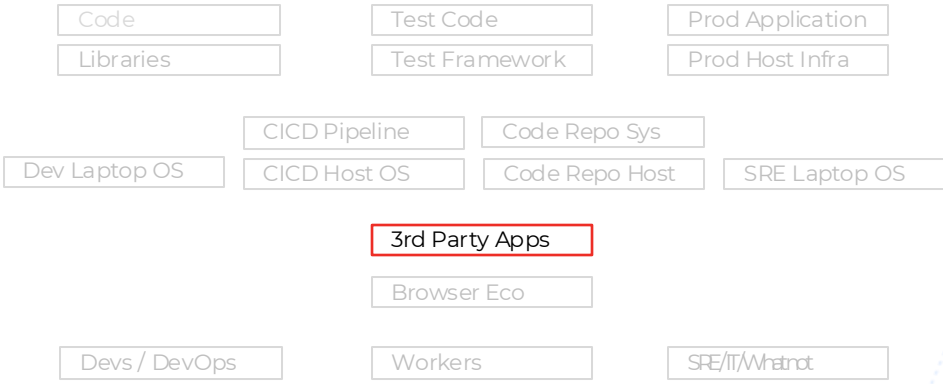
Multi-Factor Authorization

Enterprise Credential Stores / Password Managers

Endpoint Protection

SEIM / Data Loss Prevention (DLP)

Third Party Applications



Threats:

Email, Identity provider, chat

Okta

https://en.wikipedia.org/wiki/Okta,_Inc.#Security_incidents

Microsoft

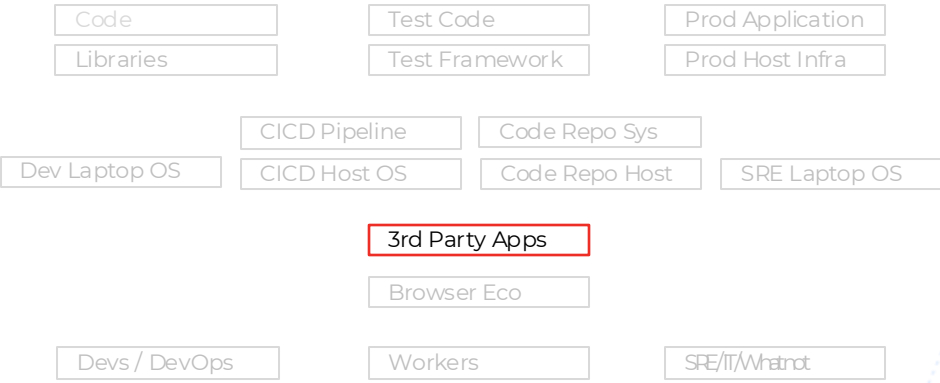
https://en.wikipedia.org/wiki/Cozy_Bear#Intrusion_into_Microsoft_(2024)

https://msrc.microsoft.com/blog/2024/03/update-on-microsoft-actions-following-attack-by-nation-state-actor-midnight-blizzard/

SolarWinds

https://en.wikipedia.org/wiki/2020_United_States_federal_government_data_breach

Third Party Applications



Recommendations:

Email, Identity provider, chat

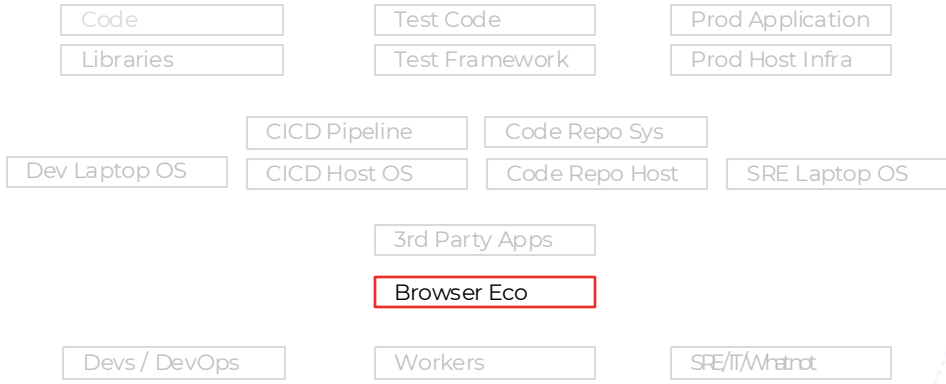
Security Assessment Questionnaire (SAQ)

Obtain and review the Vendor's SOC 2 or ISO 27001 reports

Multi-Factor Authentication

Build and test a response plan

Browser Ecosystem



Threats:

Plugins

TLS and Certificate Authorities

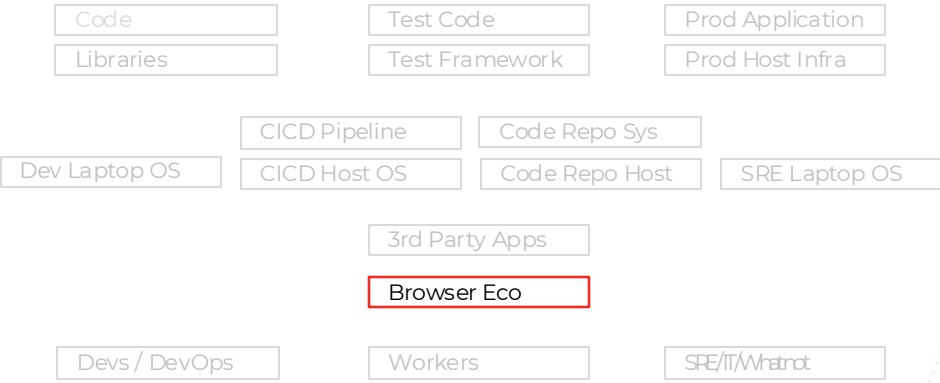
Javascript

https://nvd.nist.gov/vuln/detail/CVE-2024-5274

https://nvd.nist.gov/vuln/detail/CVE-2024-4671

https://nvd.nist.gov/vuln/detail/CVE-2024-4947

Browser Ecosystem



Recommendations:

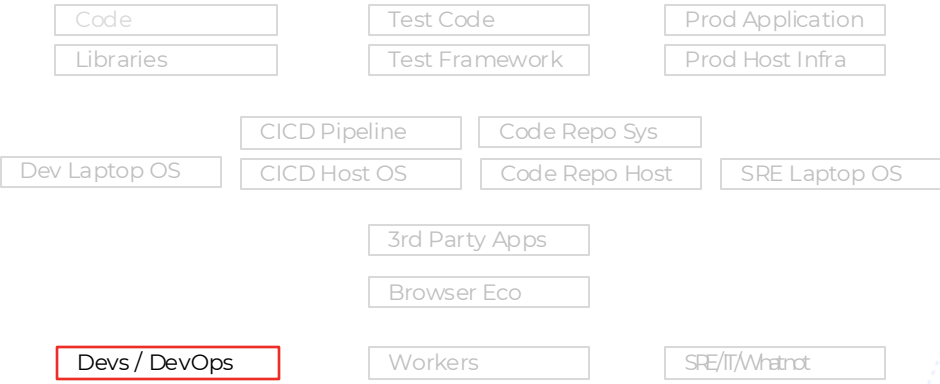
Keep browser up to date

Limit (or eliminate) plugins

Consider keeping password manager plug-ins

Avoid browser mono-culture

Developers



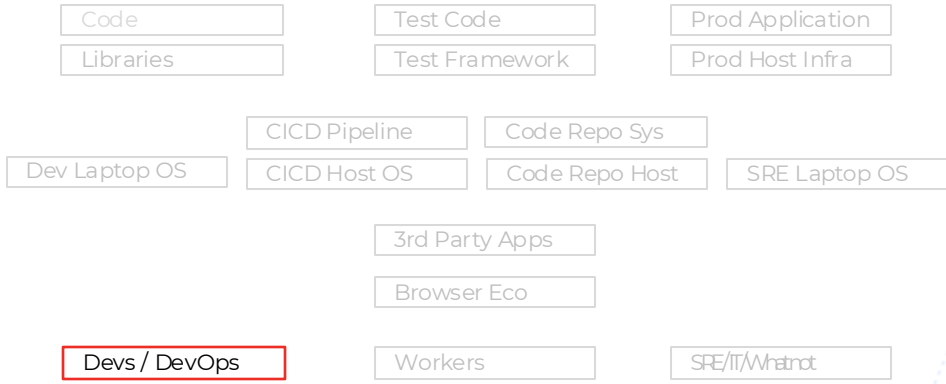
Threats:

North Korean IT worker

https://blog.knowbe4.com/how-a-north-korean-fake-it-worker-tried-to-infiltrate-us

https://www.justice.gov/opa/pr/justice-department-disrupts-north-korean-remote-it-worker-fraud-schemes-through-charges-and

Developers



Recommendations:

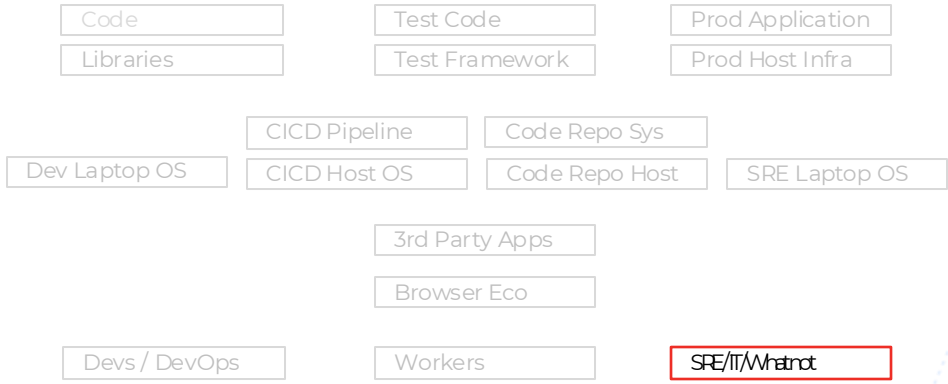
Watch for weird and suspicious activities

https://blog.knowbe4.com/north-korean-it-worker-threat-10-critical-updates-to-your-hiring-process

Principle of Least Privilege:

https://www.ncsc.gov.uk/collection/developers-collection/principles/secure-your-development-environment

SRE



Threats:

APT

https://www.darkreading.com/cloud-security/china-evasive-panda-apt-cloud-hijacking

SRE

Recommendations:

Training

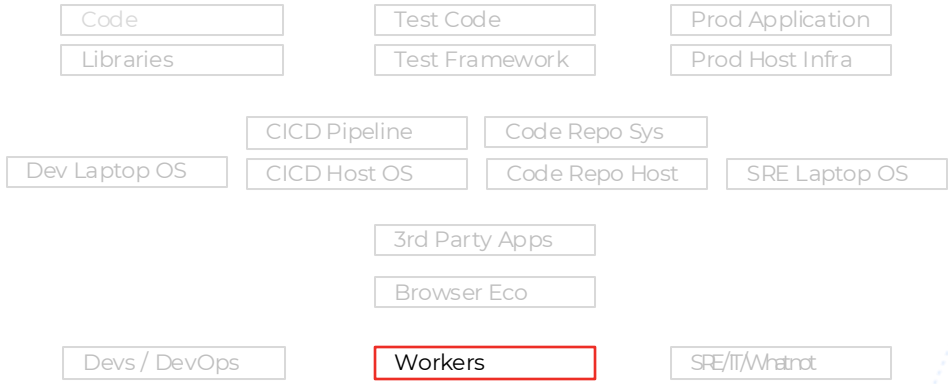
Multi-factor APIs

Key Vaults

Dual points of control

Short term elevated privileges

People



Threats:

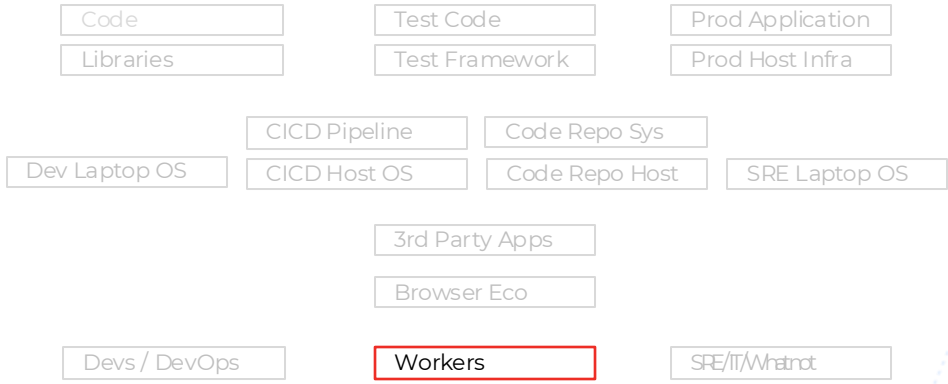
Insider Threats

Contractors

https://campusguard.com/post/hacking-building-controls-the-target-breach-5-years-later/

Terminated employees

People



Recommendations:

Process for termination

Observability of that process

Data Leak Protection

SIEM

Qualys

Your software supply chain is bigger than you think

tcbtech.com/sw-risk

Additional References

tcbtech.com/sw-risk

Software Bill of Materials Specifications

https://cyclonedx.org/capabilities/

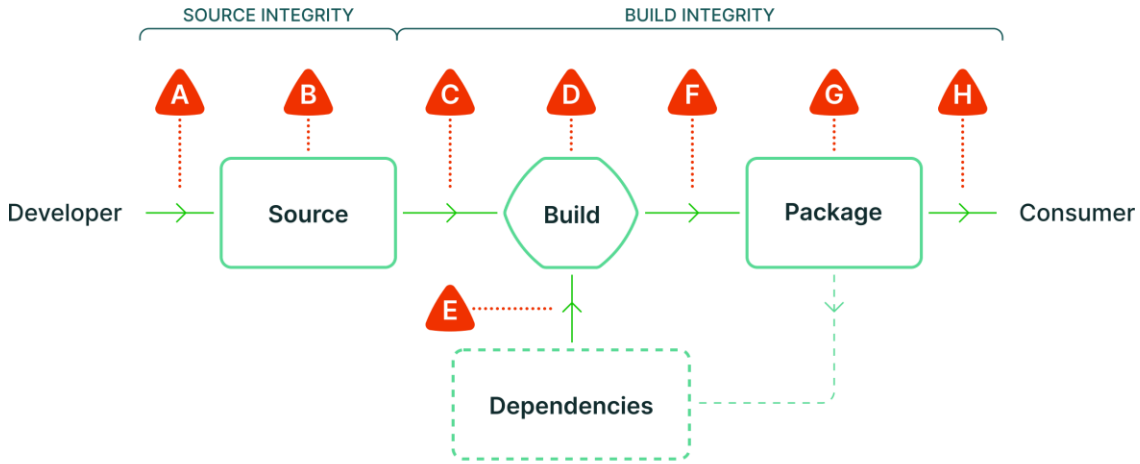
OWASP CycloneDX is a full-stack Bill of Materials (BOM) standard that provides advanced supply chain capabilities for cyber risk reduction. The specification supports:

- Software Bill of Materials (SBOM)
- Cryptography Bill of Materials (CBOM)
- Vulnerability Exploitability eXchange (VEX)
- CycloneDX Attestations (CDXA)
- . . . more

SLSA – Supply-chain Levels for Software Artifacts

https://slsa.dev/spec/v1.0/

- SLSA is a specification for describing and incrementally improving supply chain security, established by industry consensus. It is organized into a series of levels that describe increasing security guarantees.



Cloud Native Security Con 2024

Vision for a secure software supply chain

Where does your software really come from?

Vexing the Cloud Native Landscape

Generate Vex automatically for your project

Open Source tools to manage vulnerabilities in containers

Decision Trees for Evaluating Vulnerability Response

- https://insights.sei.cmu.edu/documents/606/2021_019_001_653461.pdf
  - “We eliminated numerical scores; this may make some practitioners uncomfortable. . . . CVSS contains false precision, we still must contend with the fact that, psychologically, users find that comforting. “
  - Pg 33 Prioritization Tree
  - Pg 52 Table 17

Shameless plug

OIDC and CICD: Why Your CI Pipeline Is Your Greatest Security Threat

Security Lifecycle for Cloud Native Applications

Mark Hahn Speaker History

Qualys®

tcbtech.com/sw-risk