

Rootconf 2025

Around the Supply Chain in 80 Slides

Nemo, endoflife.date

indie games
skating physical events open data
open standards interoperability
cloud security verifiable computing
self-hosting supply chain security
arch linux reinforcement learning tech policy
payments
sbom CCC EOL
puzzles rfc takshashila
iitr sds labs
rss feeds librefin foss
playdate
mastodon
kubernetes reverse engineering
speedcubing recurse center
boardgames

Pantheon



Nemo

A detailed historical map of Rome, Italy, showing the city's layout, including the Tiber River, various districts, and landmarks. The map is rendered in a sepia tone. A large, semi-transparent yellow rectangle with a black border is overlaid on the center of the map. Inside this rectangle, the word "Quick" is written in a large, bold, black sans-serif font. The map features numerous labels in Italian, such as "Valle dell'Inferno", "Monte", "Porta Angelica", "Castello S. Angelo", and "Piazza di S. Spirito". The word "Quick" is positioned centrally, partially obscuring the map's details.

Quick

A detailed historical map of Rome, Italy, showing the city's layout, including the Tiber River, various districts, and landmarks. The map is rendered in a sepia tone. A large, semi-transparent white rectangle with a black border is centered over the map, containing the text "Catch-up" in a bold, black, sans-serif font. The map features numerous labels in Italian, such as "Valle dell'Inferno", "Monte Mario", "Porta Angelica", "Vigna Barbera", and "Castello S. Angelo". The text "CATCH-UP" is also visible in the upper left quadrant of the map, partially obscured by the overlay.

Catch-up



Deep

A detailed historical map of Rome, Italy, showing the city's layout, including the Tiber River, various districts, and landmarks. The map is rendered in a sepia tone. Overlaid on the map is a large, white rectangular box with a black border. Inside this box, the word "Inspire" is written in a large, bold, black sans-serif font. The map features numerous labels in Italian, such as "Valle dell'Inferno", "Monte", "Porta Angelica", "Castello S. Angelo", and "Borgo S. Spirito". The word "Inspire" is centered horizontally and vertically within the white box.

Inspire

A detailed historical map of Rome, Italy, showing the city's layout, including the Tiber River, various districts, and landmarks. The map is oriented with North at the top. The Tiber River flows from the top left towards the bottom right. The city is divided into numerous districts, each labeled with its name. The map is a monochrome engraving, likely from a 19th-century travel guide or historical atlas. The text "Not Exhaustive" is superimposed over the center of the map in a large, bold, black font.

Not Exhaustive

A detailed historical map of Florence, Italy, serves as the background for the slide. The map shows the city's layout, including the Arno river, various streets, and landmarks. The title is centered in a large, bold font, with 'Attack' in dark red and 'Not' in dark green.

Supply Chain **Attack** or **Not**

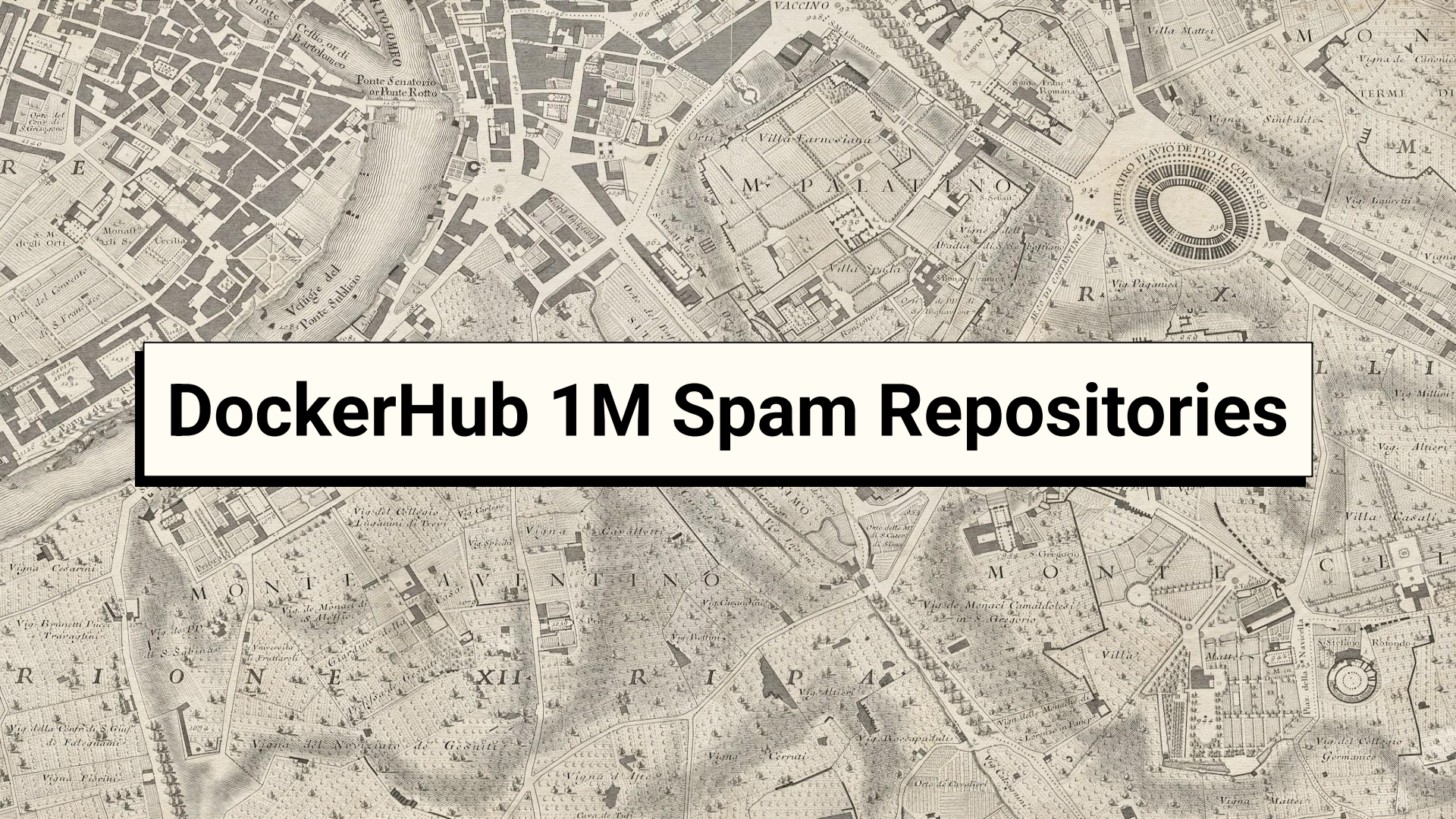
A detailed historical map of Rome, Italy, showing the city's layout, including the Tiber River, the Colosseum, and various landmarks. The map is in a sepia tone with black ink. The text "pypi.org/package/python-requests" is overlaid on the map, centered in a white box with a black border. The text is in a large, bold, sans-serif font. The background map shows various districts and landmarks, including the Colosseum, the Tiber River, and the Vatican. The text is in a large, bold, sans-serif font. The background map shows various districts and landmarks, including the Colosseum, the Tiber River, and the Vatican.

[pypi.org/package/
python-requests](https://pypi.org/package/python-requests)

A detailed historical map of Rome, Italy, showing various landmarks and districts. The map is oriented with North at the top. Key features include the Tiber River flowing through the center, the Colosseum (Anfiteatro Flavio) in the upper right, the Palatine Hill (M. Palatino) in the center, and the Aventine Hill (M. Aventino) in the lower right. Numerous streets, bridges, and religious sites are labeled in Italian. The map is rendered in a sepia tone with fine lines and shading to represent terrain and buildings.

npm

All Systems Down



DockerHub 1M Spam Repositories

Linux Kernel Source Repository Hack

A detailed historical map of Rome, Italy, showing the city's layout, including the Tiber River, various streets, and landmarks. The map is oriented with North at the top. A large white box with a black border is superimposed over the center of the map, containing the text '~ /aws/credentials'. A large yellow arrow points downwards from this box to another white box with a black border at the bottom of the map, which contains the text 'gist.github.com'.

~/aws/credentials

gist.github.com

A detailed historical map of Rome, Italy, showing the city's layout, including the Tiber River, the Colosseum, and various landmarks. The map is divided into sections labeled with letters and numbers. A large white box with a black border is superimposed over the center of the map, containing the text "Secrets logged on private CI".

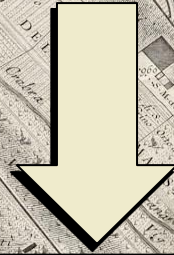
Secrets logged on private CI



Malicious Package built on your CI

A detailed historical map of Rome, Italy, showing the city's layout, including the Tiber River, various bridges, and numerous streets and landmarks. The map is in a sepia tone with black text labels for various locations.

**Bribe Customer
Support**



Data Breach

A detailed historical map of Rome, Italy, showing the city's layout, including the Tiber River, various hills (Monte Aventino, Monte Celio), and numerous landmarks and buildings. The map is rendered in a sepia tone with black outlines for buildings and streets. A large, semi-transparent white box with a black border is centered over the map, containing the word "Definitions" in a large, bold, black sans-serif font.

Definitions

A detailed historical map of Rome, Italy, serves as the background for the slide. The map is a woodcut-style print showing the city's layout, including the Tiber River, various districts, and landmarks. The title 'Software Supply Chain Attack' is prominently displayed in a white box with a black border in the upper left corner.

Software Supply Chain *Attack*

Insertion of nefarious code
into trusted software before
delivery.

Russ Cox. 2025.

Fifty Years of Open Source Software Supply Chain Security

Software Supply Chain *Vulnerability*

An exploitable weakness in trusted software caused by a third-party, component of that software.

Russ Cox. 2025.

Fifty Years of Open Source Software Supply Chain Security

The background of the slide is a detailed, historical-style map of a city, likely Rome, showing streets, buildings, and a prominent castle (Castello S. Angelo) in the lower right. The map is rendered in a light, textured style.

Software Supply Chain Security

The engineering of defenses
against software supply
chain attacks and
vulnerabilities.

Russ Cox. 2025.

Fifty Years of Open Source Software Supply Chain Security

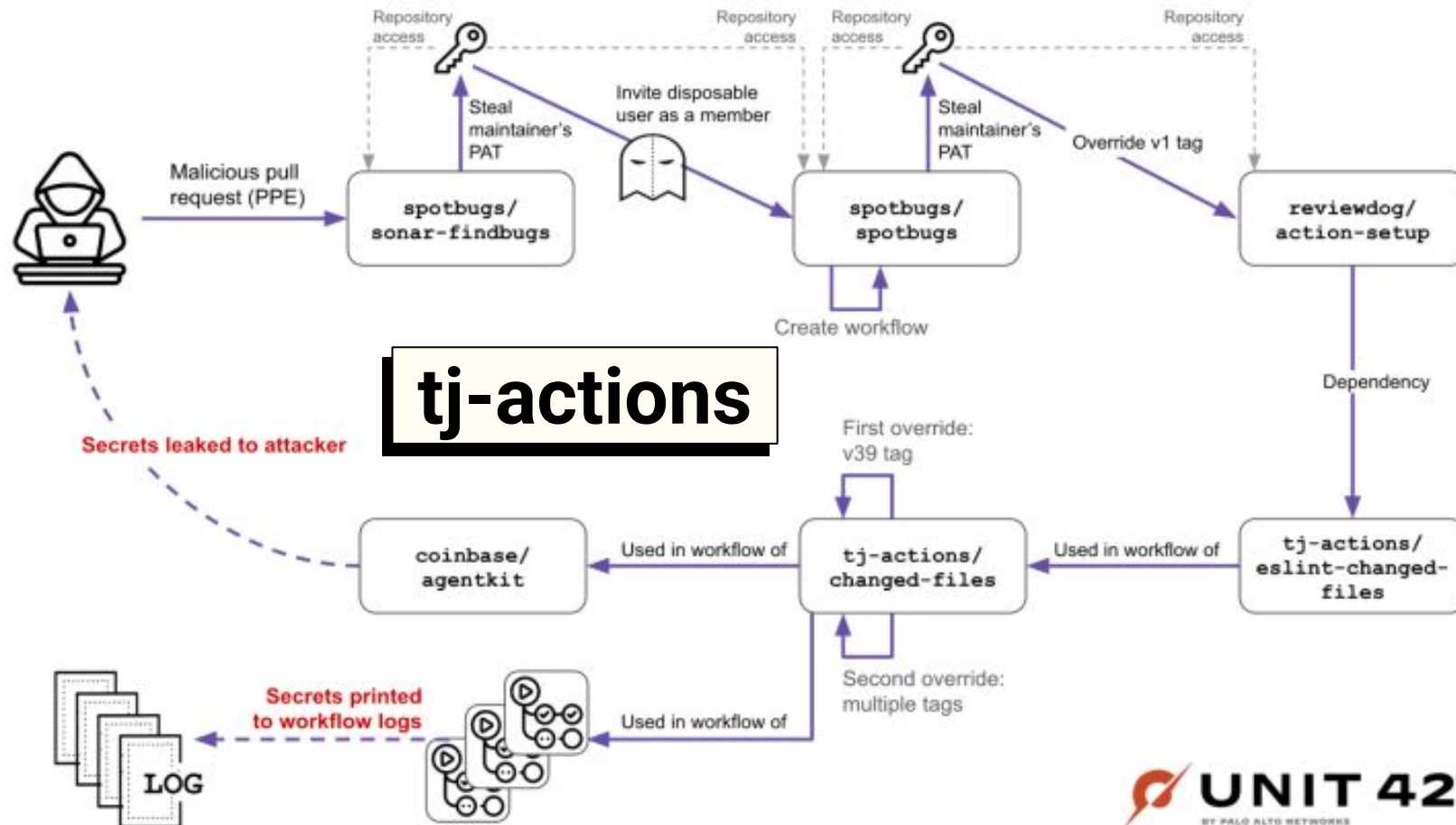
A detailed historical map of Rome, Italy, showing the city's layout, including the Tiber River, various districts, and landmarks. The map is rendered in a sepia tone with fine lines and text. The title "Open Source* Software Supply Chain" is overlaid on the map in a white box with a black border.

Open Source* Software Supply Chain

A detailed historical map of Rome, Italy, showing the city's layout, including the Tiber River, the Colosseum, the Pantheon, and various neighborhoods. The map is in a sepia tone with black text labels for streets and landmarks. Two white rectangular boxes with black borders are overlaid on the map, containing the text 'tj-actions' and 'xz-utils'.

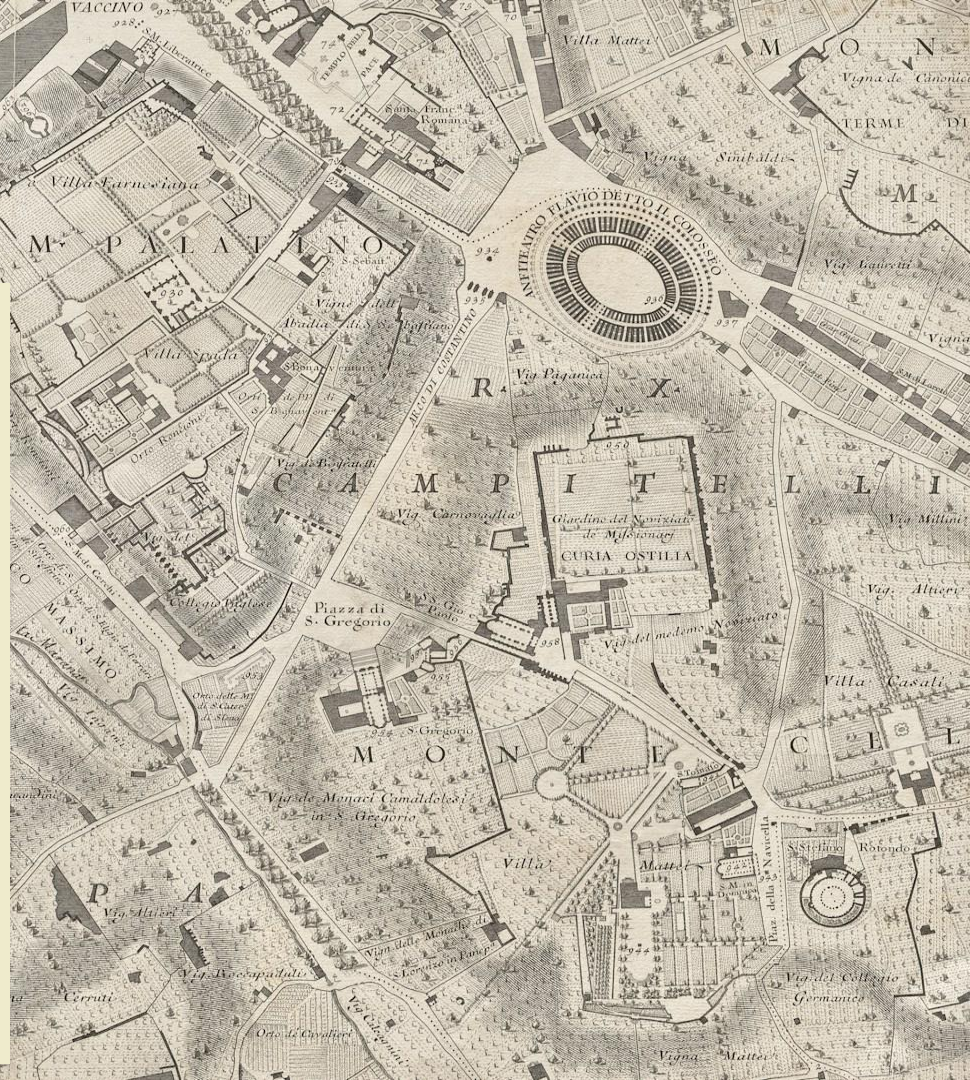
tj-actions

xz-utils



tj-actions

- Immutable GitHub Actions
- Transparency Logs
- Version Pinning
- Tag Protection
- Malicious Fork/Branch Scans
- Vulnerable CI Scans



A detailed historical map of Rome, Italy, showing various landmarks and districts. The map is in a sepia tone and includes labels for places like 'VILLA FARNESIANA', 'M. PALA', 'VILLA MATTEI', and 'TERME DI'. It also shows the 'Vigna de' and 'Vigna de' areas. The map is used as a background for the presentation slides.

tj-actions

- Immutable GitHub Actions
- Transparency Logs
- Version Pinning
- Tag Protection
- Malicious Fork/Branch Scans
- Vulnerable CI Scans

xz-utils

- ~~o3z fuzz~~
- Minimal Dependency
- Dynamic Loading
- Source/Release diffs
- Security Audits

Software Supply Chain Security

Source



Build



Delivery

A detailed historical map of Florence, Italy, showing the city's layout, including the Arno river, various streets, and landmarks. The map is in a sepia tone with black text labels for various locations.

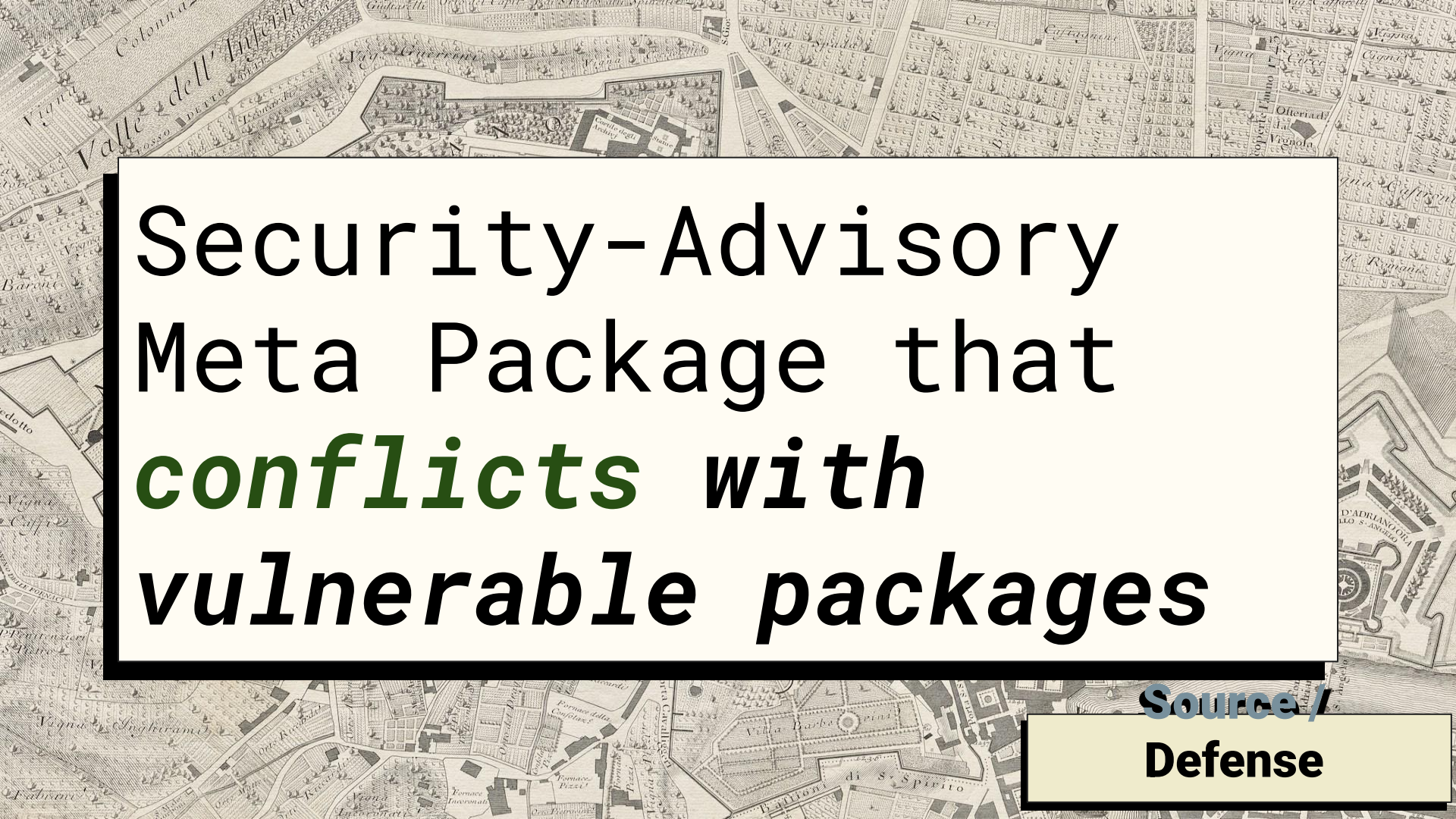
Detect *Obviously* *Malicious* TM Packages

**Source /
Defense**

A detailed historical map of a city, likely from the 17th or 18th century, serves as the background. The map shows a complex network of streets, buildings, and a river. A large, white rectangular box with a black border is centered over the map, containing the main title. The title is written in a mix of green and black fonts, with 'Prevent' in green and the rest in black. The background map includes various labels such as 'Valle dell'Inferno', 'Colonna', 'Vigna', 'Fabbica', 'Porta Cavallotti', 'Vigna di S. Spirito', and 'Castello S. Ambrogio'.


Prevent Obviously Malicious Package Installation

Source /
Defense

A detailed historical map of Florence, Italy, showing the city's layout, including the Arno river, various streets, and landmarks. The map is in a sepia tone with black text labels for various locations.

Security-Advisory
Meta Package that
conflicts with
vulnerable packages

Source /
Defense

A detailed historical map of Rome, Italy, showing the city's layout, including the Tiber River, various districts, and landmarks. The map is rendered in a sepia tone with black outlines for buildings and streets. The title 'Typosquatting Slopsquatting' is overlaid on the map in a large, bold, sans-serif font. The word 'Typo' is in red, and 'Squatting' is in black. The word 'Slo' is in red, and 'psquatting' is in black. The map shows the city's expansion from the center towards the edges, with labels for various areas like 'Valle dell'Inferno', 'Monte Mario', and 'Castello'. The map is oriented with North at the top.

TypoSquatting Slopsquatting

Source / Attack

Improve Security Scan cadence



Source /
Defense

A detailed historical map of Rome, Italy, showing the city's layout, including the Tiber River, various districts, and landmarks. The map is oriented with North at the top. The title "Smarter CVE* Prioritization" is overlaid on the map in a large, bold, black font, enclosed in a white rectangular box with a black border. The background map shows various districts and landmarks, including the "Valle dell'Inferno" (Valley of Hell) and the "Colonna Traiana" (Trajan's Column).

Smarter CVE* Prioritization

Source /
Defense

End-of-Life Tracking

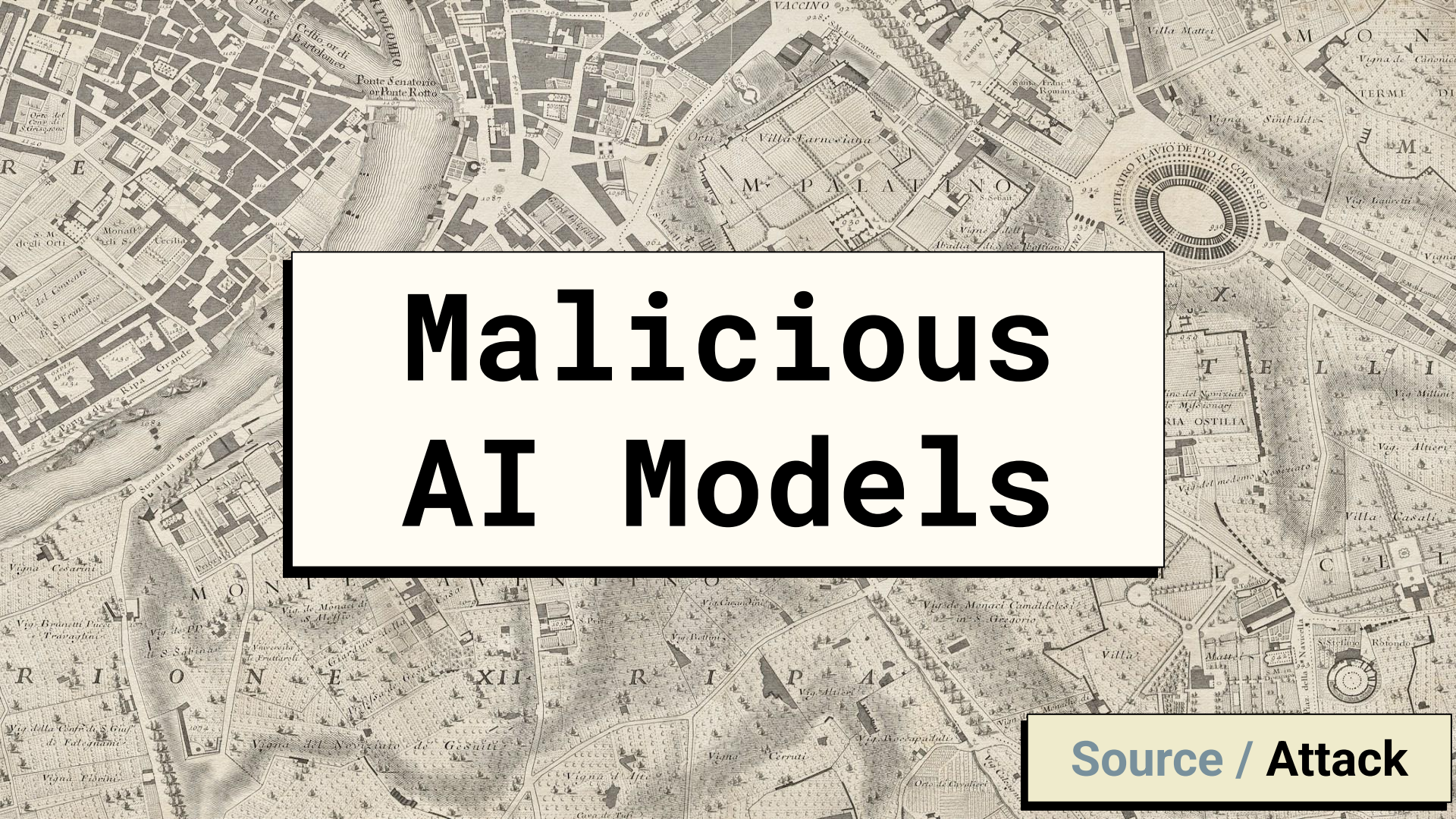


Source /
Defense

A detailed historical map of Rome, Italy, showing the city's layout, including the Tiber River, the Colosseum, and various districts. The map is rendered in a sepia tone with fine lines and text labels for various locations.

Trusted OSS Supplier

Source /
Defense

A detailed historical map of Rome, Italy, showing the city's layout, including the Tiber River, the Colosseum, and various landmarks. The map is in a sepia tone with black text labels for various locations.

Malicious AI Models

Source / Attack

A detailed historical map of Rome, Italy, showing the city's layout, including the Tiber River, the Colosseum, and various landmarks. The map is in a sepia tone with black text labels for various locations. A large white rectangular box with a black border is centered over the map, containing the title text.

OpenSSF Scorecard

Source / Defense

A detailed historical map of Rome, Italy, showing the city's layout, including the Tiber River, the Colosseum, and various landmarks. The map is in a sepia tone with black text labels for various locations. A large white rectangular box with a black border is superimposed over the center of the map, containing the text 'Audit your SBOMs'.

Audit your SBOMs

Source / Defense

A detailed historical map of Rome, Italy, showing the city's layout, including the Tiber River, the Colosseum, and various landmarks. The map is in a sepia tone with black text labels for various locations. A large white rectangular box with a black border is superimposed over the center of the map, containing the text 'Score your Dependencies'.

Score your Dependencies

Source / Defense

A detailed historical map of Rome, Italy, showing the city's layout, including the Tiber River, various bridges, and numerous landmarks. The map is oriented with North at the top. The Tiber River flows from the bottom left towards the top right. Key landmarks include the Colosseum (labeled 'ANFITEATRO') in the upper right, the Curia Ostilia (labeled 'CURIA OSTILIA') in the center, and the Villa of the Paterfamilias (labeled 'VILLA PATERFAMILIAS') in the lower right. The map is divided into several regions, including the Monti (labeled 'MONTI') and the Trastevere (labeled 'TRASTEVERE'). The map is a sepia-toned engraving with fine lines and text labels for various streets, buildings, and landmarks.

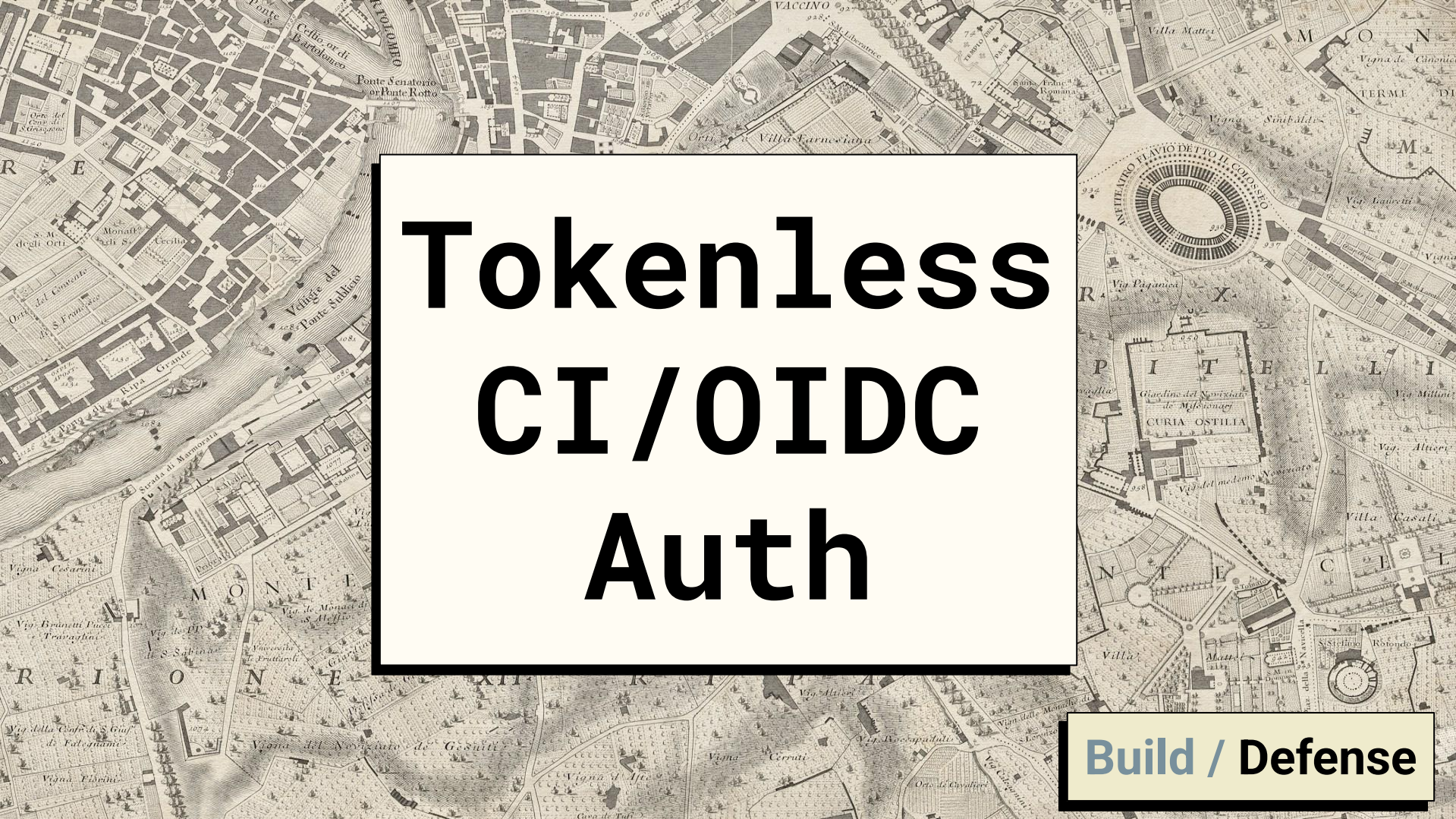
Security Commons Funding

Source / Vulnerability

A detailed historical map of Rome, Italy, showing the city's layout, including the Tiber River, various bridges, and landmarks. The map is oriented with North at the top. The Tiber River flows from the top left towards the bottom right. Key landmarks include the Colosseum (Amfiteatro Flavio) in the upper right, the Curia Ostilia in the center, and the Villa of the Papyri in the lower right. The map is labeled with various Roman names and numbers, indicating its historical nature.

Commit /Release Signing

Build / Defense



Tokenless CI/OIDC Auth

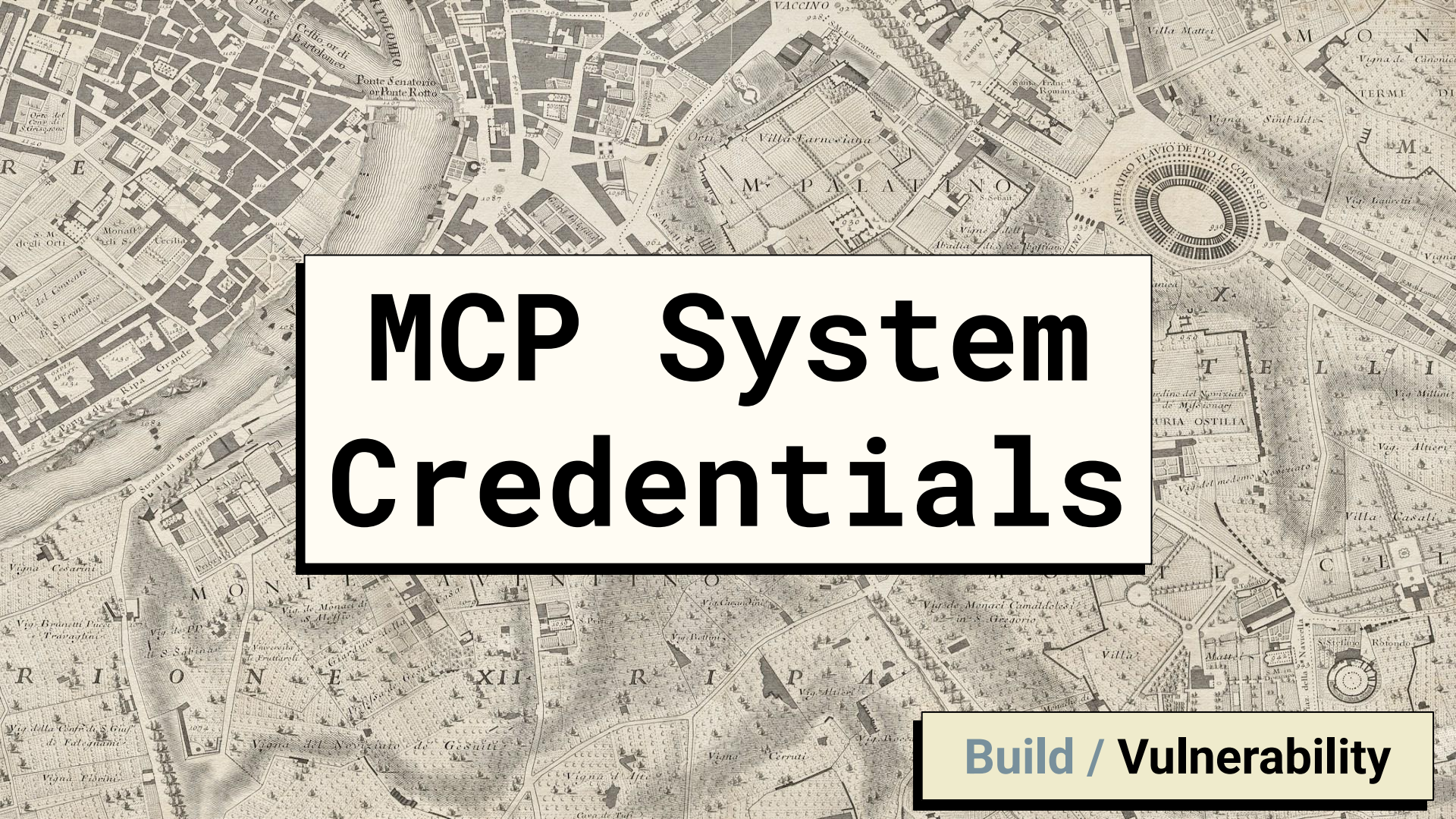
Build / Defense

Build / Defense

A detailed historical map of Rome, Italy, showing the city's layout, including the Tiber River, various bridges, and numerous landmarks. The map is oriented with North at the top. The Tiber River flows from the top left towards the bottom right. Key landmarks include the Colosseum (Amphitheatrum Flavium) in the upper right, the Curia Ostilia in the center, and the Villa Palatina in the lower right. The map is labeled with various districts and landmarks in Italian, such as 'M. PALATINO', 'M. AVENTINO', and 'M. EURINOMEO'.

Lower CI Perms

Build / Defense

A detailed historical map of Rome, Italy, showing the city's layout, including the Tiber River, the Colosseum, and various landmarks. The map is in a sepia tone with black text labels for various locations.

MCP System Credentials

Build / Vulnerability

A detailed historical map of Rome, Italy, showing the city's layout, including the Tiber River, the Colosseum, and various landmarks. The map is in a sepia tone with black text labels for various locations. The title 'Insecure CI Configuration' is overlaid in a large, bold, black font on a white rectangular background.

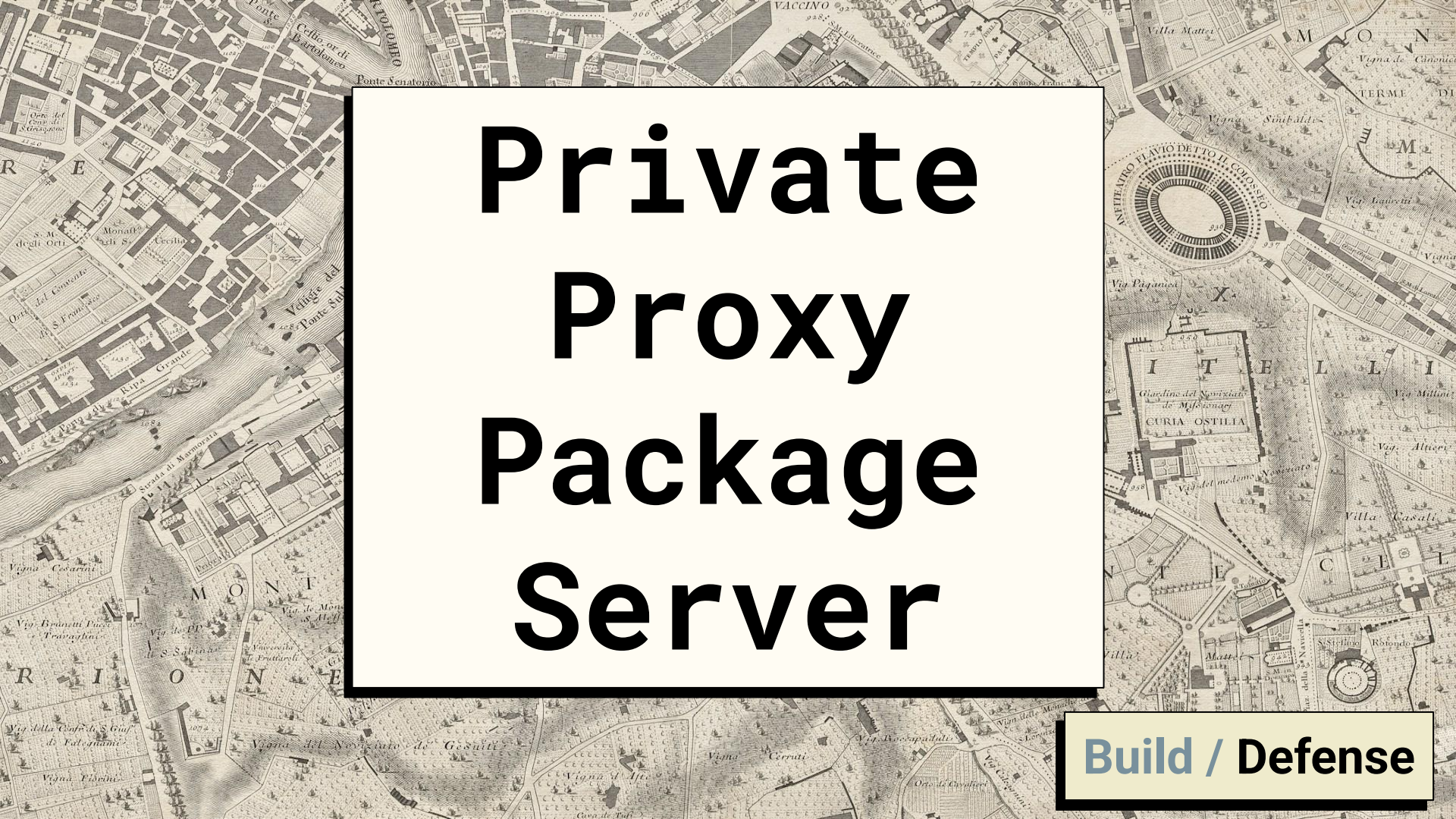
Insecure CI Configuration

Build / Vulnerability

A detailed historical map of Rome, Italy, showing the city's layout, including the Tiber River, the Colosseum, the Palatine Hill, and the Aventine Hill. The map is rendered in a sepia tone with black outlines for buildings and streets. Various landmarks and districts are labeled in Latin and Italian. A large white rectangular box with a black border is superimposed over the center of the map, containing the text 'Lockfiles'.

Lockfiles

Build / Defense

A detailed historical map of Rome, Italy, showing the city's layout, including the Tiber River, various districts, and landmarks. The map is in a sepia tone with black text labels for streets and locations. The title 'Private Proxy Package Server' is overlaid in a large, bold, black font on a white rectangular background in the center of the map.

Private Proxy Package Server

Build / Defense

A detailed historical map of Rome, Italy, showing the city's layout, including the Tiber River, the Colosseum, and various landmarks. The map is in a sepia tone with black text labels for various locations.

Publish SBOMs

Delivery / Defense

A detailed historical map of Rome, Italy, showing the city's layout, including the Tiber River, the Colosseum, and various landmarks. The map is in a sepia tone with black text labels for various locations.

Release Attestations

Delivery / Defense

A detailed historical map of Rome, Italy, showing the city's layout, including the Tiber River, the Colosseum, and various landmarks. The map is in a sepia tone with black text labels for various locations.

Trusted Publishing

Delivery / Defense

A detailed historical map of Rome, Italy, showing the city's layout, including the Tiber River, various bridges, and landmarks. The map is oriented with North at the top. The Tiber River flows from the top left towards the bottom right. Key landmarks include the Colosseum (Amphitheatrum Flavium) in the upper right, the Curia Ostilia in the center, and the Villa Palatina in the lower right. The map is labeled with various districts and landmarks in Italian, such as "M. PALATINO", "M. AVENTINO", and "M. EURINOMEO".

Release Diff Alerts

Delivery / Defense

A detailed historical map of Rome, Italy, showing the city's layout, including the Tiber River, the Colosseum, the Pantheon, and various districts like M. PALATINO and M. AVENTINO. The map is in a sepia tone with black text labels for landmarks and streets.

Token Theft

Delivery / Attack

A detailed historical map of Rome, Italy, showing the city's layout, including the Tiber River, various districts, and landmarks. The map is rendered in a sepia tone with fine lines and text labels for various locations.

Supply Chain Security Maturity Model

RedHat / Sonatype

A detailed historical map of Rome, Italy, showing the city's layout, including the Tiber River, the Colosseum, and various landmarks. The map is in a sepia tone with black text labels for streets and landmarks.

Unmanaged

Exploration

Ad-Hoc

Control

Monitor & Measure

The background of the entire image is a detailed, sepia-toned historical map of Rome, Italy. It shows various landmarks, streets, and the Tiber River. Labels like 'VACCINO', 'CIRCO', and 'Vigna' are visible. The map is oriented with North at the top.

**Policy Governance
Compliance**

**Consistency /
Build & Release**

**Inventory /
Supplier Hygiene /
Transparency**

**Resilience /
Remediation**

3

**Policy Governance
Compliance**

4

**Consistency /
Build & Release**

2

**Inventory /
Supplier Hygiene /
Transparency**

2

**Resilience /
Remediation**

Biggest challenges for OSS Software Supply Chains



#1

Vulnerability and patch management



#2

Insufficient visibility of software dependencies or software supply chain



#3

Trustworthiness of software source*



#4

Short upstream security maintenance/support periods



#5

Lack of in-house skills and experience

IDC Survey, Q4 2024 by Canonical/Google

A detailed historical map of Rome, Italy, showing the city's layout, including the Tiber River, various districts, and landmarks. The map is rendered in a sepia tone with fine lines and text labels for various locations.

Secure Supply Chain Consumption Framework

OpenSSF / Microsoft

Ingest

Inventory

Update

Enforce

Audit

Scan

Rebuild

Fix+Upstream

Level 1



Minimum OSS Governance Program

- Use package managers [ING-1]
- Local copy of artifact [ING-2]
- Scan with known vulns [SCA-1]
- Scan for software licenses [SCA-2]
- Inventory OSS [INV-1]
- Manual OSS updates [UPD-1]

Level 2



Secure Consumption and Improved MTTR

- Scan for end of life [SCA-3]
- Have an incident response plan [INV-2]
- Auto OSS updates [UPD-2]
- Alerts on vulns at PR time [UPD-3]
- Audit that consumption is through approved ingestion method [AUD-2]
- Validate integrity of OSS [AUD-3]
- Secure package source file configuration [ENF-1]

Level 3



Malware Defense and Zero-Day Detection

- Deny list capability [ING-3]
- Clone OSS source [ING-4]
- Scan for malware [SCA-4]
- Proactive security reviews [SCA-5]
- Enforce OSS provenance [AUD-1]
- Enforce consumption from curated feed [ENF-2]

Level 4



Advanced Threat Defense

- Validate the SBOMs of OSS consumed [AUD-4]
- Rebuild OSS on trusted infrastructure [REB-1]
- Digitally sign rebuilt OSS [REB-2]
- Generate SBOM for rebuilt OSS [REB-3]
- Digitally sign protected SBOMs [REB-4]
- Implement fixes [FIX-1]

s2c2f

A detailed historical map of Rome, Italy, showing the city's layout, including the Tiber River, various districts, and landmarks. The map is rendered in a sepia tone. Overlaid on the map is a large, semi-transparent yellow rectangle with a black border. Inside this rectangle, the letters "SLSA" are written in a large, bold, black, sans-serif font. The map features numerous labels in Italian, such as "Valle dell'Inferno", "Monte", "Porta Angelica", "Castello S. Angelo", and "Piazza di S. Spirito". The "SLSA" text is centered horizontally and vertically within the yellow rectangle.

SLSA

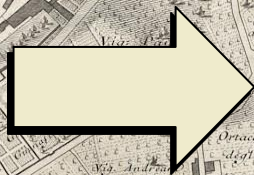


Open Software Supply Chain Attack Reference (OSC&R)

A detailed historical map of Rome, Italy, showing various districts, streets, and landmarks. The map is in a sepia tone and includes labels for various locations such as 'Ponte Sublico', 'Monte Aventino', 'Monte Mario', and 'Vigna del Collegio'.

Software Supply Chain Security

Source



Build



Delivery

Rootconf 2025



Around the Supply Chain in 80 Slides

Nemo, endoflife.date