Rootconf 2025

# Around the Supply Chain in 80 Slides

Nemo, endoflife.date


Pantheon

Nemo

Valle dell' Inferno
MONTE VATICANO
Porta Angelica
Porta Castello
MAUSOLEO D'ADRIANO ORA CASTELLO S. ANGELO
Porta Fabbrica
Porta Cavalleggeri
Villa Barberini
Bastioni di S. Spirito
BORGO S. SPIRITO
BORGO VECCHIO
Vestigie del Ponte Trionfale
Ponte S. Angelo
Piazza di Ponte
Vestigie del CIRCO D'ADRIANO
Orto della Fabbrica di S. Pietro
Vigna di S. Spirito
Orto Incoronati
XIV

# Quick

# Catch-up


Porta Angelica
Porta Fabbrica
Porta Cavalleggeri
Vigna di S. Spirito
Vigna Barberini
Bastioni di S. Spirito
Mausoleo d'Adriano o il Castello S. Angelo
Borgo S. Spirito
Veduta del Ponte Trionfale
Ponte Adriano or Sant'Angelo
Piazza di Ponte
Valle dell'Inferno
Colonna
Vigna Cantelli
Vigna Inglesi
Orto Guerrini
Fornace Ricardi
Fornace della Cristofore
Fornace Pizzi
Fornace Incoronati
Fondi
Barone
Vigna Caffi
Vigna Cafarelli
Vigna Mattei
Vigna di Romani
Vigna Ferrari
Vigna Bartolini
Via Spada
Cartagrani
Circo
Osteria
Vignola
Veduta del Circo di Adriano
Porta Castello
Porta Sisto
Porta Santo Spirito
Fabbrica
Colonna Antonina
Vigna Guerrini
Vigna di Spirito
Giardino Sforza
Giardino Pontificio
Giardino Vaticano
Statue
XIV


Valle dell' Inferno
Colonna
Vigna
MONTE VATICANO
Giardino Pontificio
Cortile degli Archivi
Statue
PONTIFICIO
XIV
Porta Angelica
Giardino Salterni
Orto Spada
Castagnini
Osteria da Vignola
Vestigie del CIRCO D'ADRIANO
Vigna Castroni
Vig. de Romanis
Porta Castello
MAUSOLEO D'ADRIANO ORA CASTELLO S. ANGELO
Vigna di S. Spirito
Orto della Fabbrica di S. Pietro
Acquedotto dell' Acqua Paola
Vigna Caffi
Orto Incoronati
Porta Fabbrica
Vig. Candolfi
Vigna Inghirami
Fornace Riccardi
Fornace della Confolazione
Fornace Pizzi
Fornace Incoronati
Porta Cavalleggeri
Villa Barberini
Bastioni di S. Spirito
BORGO VECCHIO
BORGO S. SPIRITO
Ponte Adriano or S. Angelo
Vestigie del Ponte Trionfale
Piazza di Ponte
Baroni
Fabbrica

# ~~Deep~~


Valle dell' Inferno
Colonna
Vigna
Baroni
Vig. Guerrini
Vigna Spada
Orto
Castagnini
Vigna Cafarelli
Vigna Ciccolini
Cortile degli Archivi
Statue
PONTIFICIO
MONTE VATICANO
Giardino PONTIFICIO
XIV
Porta Angelica
Giardino Salerni
Vestigie del CIRCO D'ADRIANO
Osteria da Vignola
Vigna Colarelli
Vigna Castroni
Vig. de Romanis
Porta Castello
Vig. della Ritamara
Orto della Fabbrica
Vigna di S. Spirito
Acquedotto dell' Acqua Paola
Vigna Cafi
MAUSOLEO D'ADRIANO ORA CASTELLO S. ANGELO
BORGO VECCHIO
BORGO S. SPIRITO
Orto Incoronati
Porta Fabbrica
P. Penitenzieri S. Pietro
Vig. Candolfi
Fornace Riccardi
Fornace della Confolaz.
Porta Cavalleggeri
Villa Barberini
Bastioni di S. Spirito
Vestigie del Ponte Trionfale
Ponte Adriano or S. Angelo
Piazza di Ponte
Vigna Inghirami
Fornace Incoronati
Fornace Pizzi

# Inspire

# Not Exhaustive

# Supply Chain Attack or Not

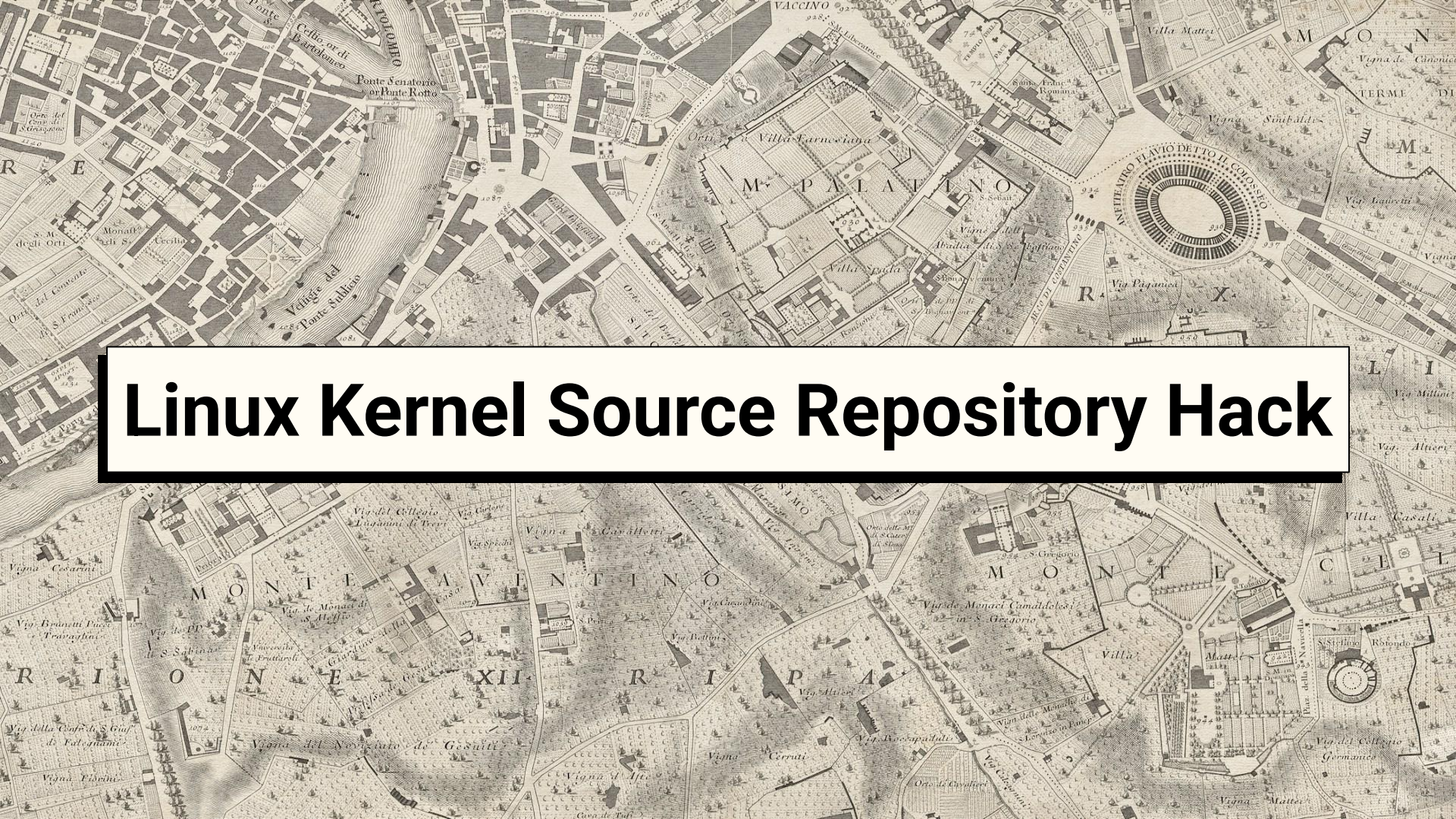
# pypi.org/package/
# python-requests


npm

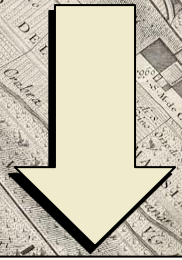
All Systems Down


# DockerHub 1M Spam Repositories

# Linux Kernel Source Repository Hack



~/aws/credentials



gist.github.com

# Secrets logged on private CI

# Malicious Package built on your CI

# Bribe Customer Support

# Data Breach


# Definitions

## 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

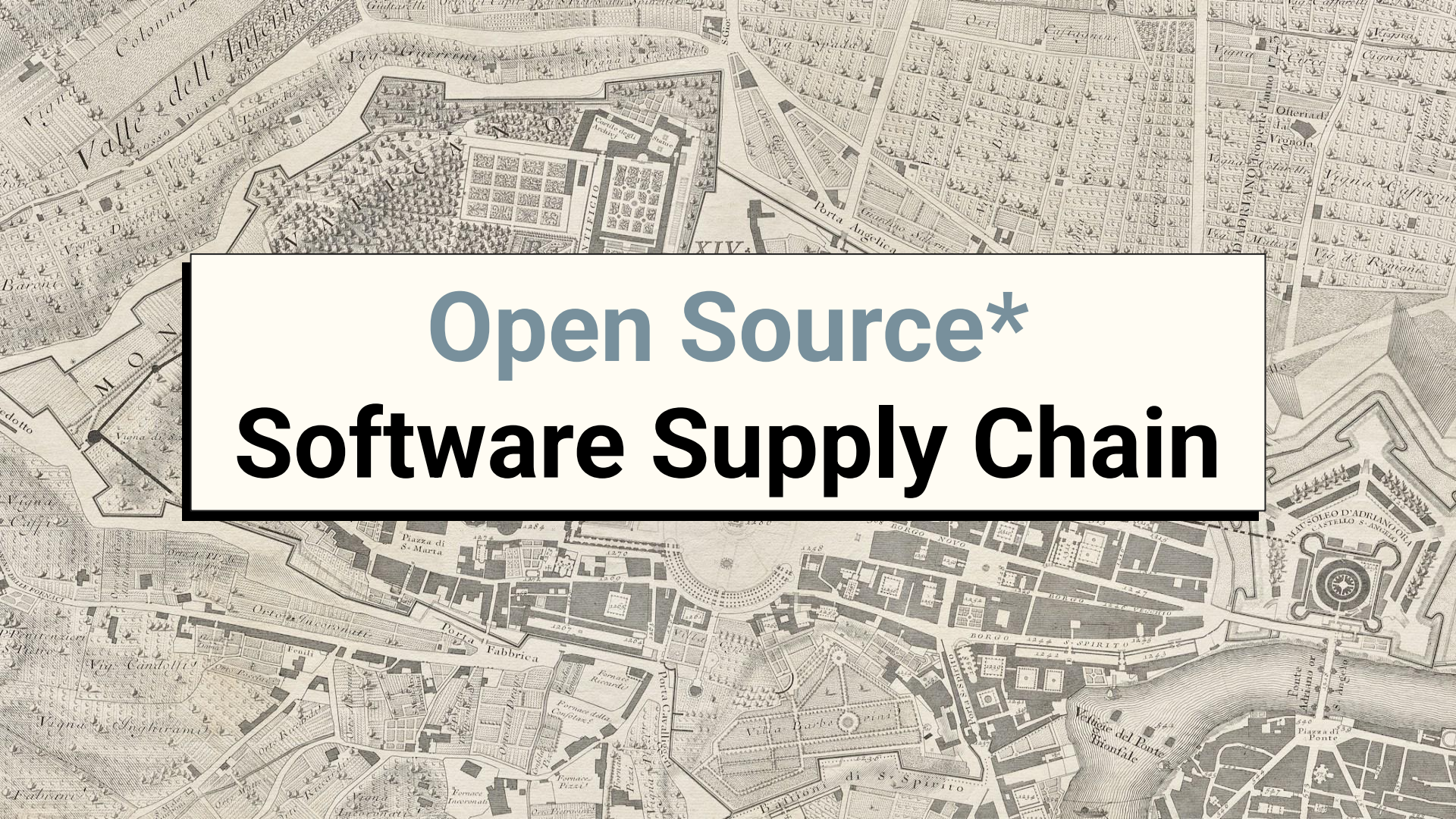
# Software Supply Chain *Security*

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

Russ Cox. 2025.
Fifty Years of Open Source Software Supply Chain Security

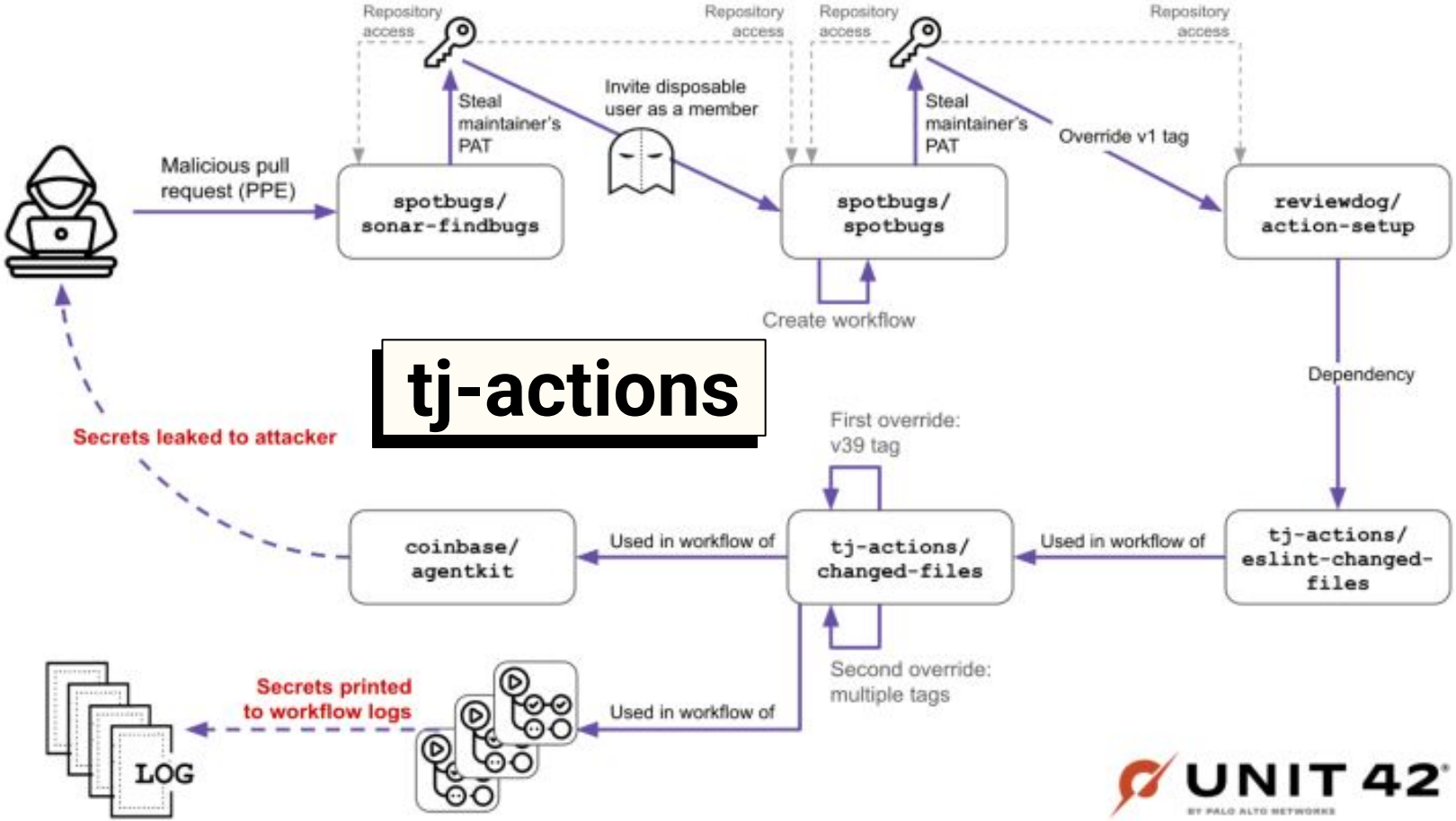
# Open Source*

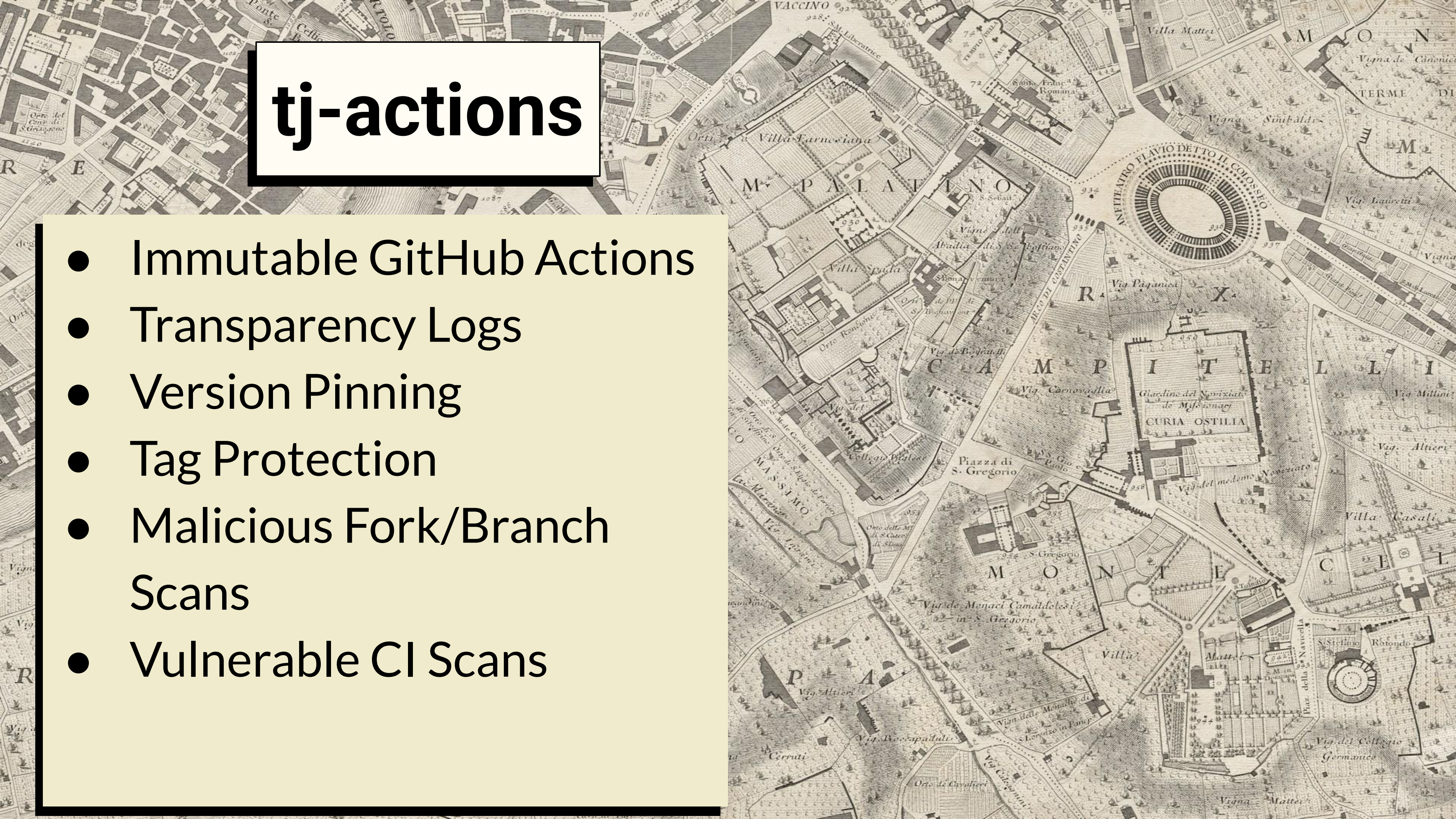
# Software Supply Chain




# tj-actions

# xz-utils


Repository access
Repository access
Repository access
Repository access
Steal maintainer's PAT
Invite disposable user as a member
Steal maintainer's PAT
Override v1 tag
Malicious pull request (PPE)
spotbugs/ sonar-findbugs
spotbugs/ spotbugs
reviewdog/ action-setup
Create workflow
Dependency
tj-actions
Secrets leaked to attacker
First override: v39 tag
coinbase/ agentkit
Used in workflow of
tj-actions/ changed-files
Used in workflow of
tj-actions/ eslint-changed-files
Second override: multiple tags
Secrets printed to workflow logs
Used in workflow of
LOG
UNIT 42
BY PALO ALTO NETWORKS



# tj-actions

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

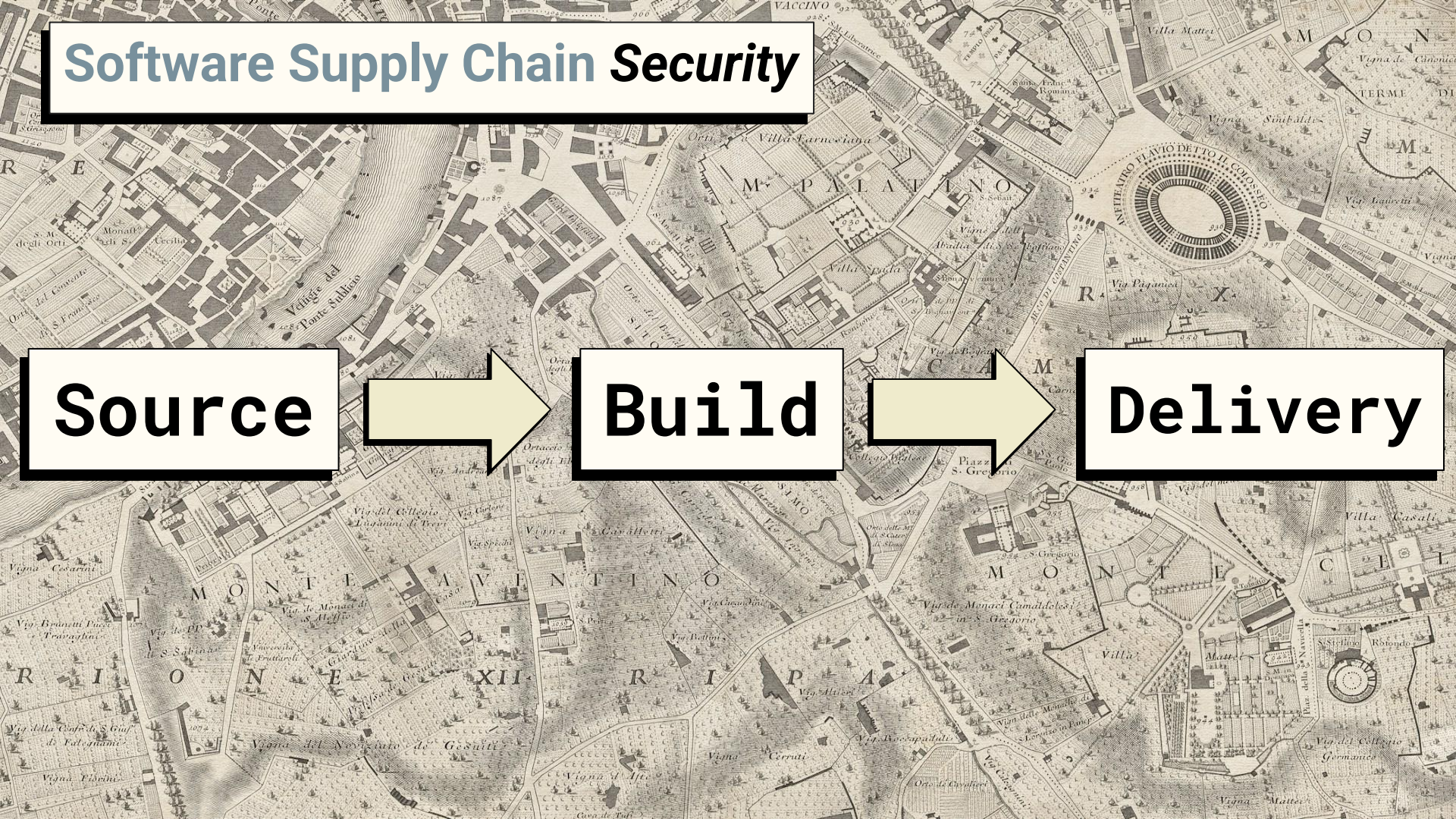
## tj-actions

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

## xz-utils

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

# Software Supply Chain *Security*



# Detect *Obviously Malicious* Packages™

Source / Defense

# Prevent *Obviously Malicious* Package Installation

Source / Defense

# Security-Advisory Meta Package that ***conflicts with vulnerable packages***

**Source / Defense**

# Typosquatting
# Slopsquatting

Source / Attack

# Improve Security Scan cadence ⏰

Source / Defense

# Smarter CVE* Prioritization

Source / Defense

# End-of-Life Tracking ⌛

Source / Defense

# Trusted OSS Supplier

Source / Defense

# Malicious AI Models

Source / Attack

# OpenSSF Scorecard

Source / Defense

# Audit your SBOMs

Source / Defense

# Score your Dependencies

Source / Defense

# Security Commons Funding

Source / Vulnerability

# Commit /Release Signing

Build / Defense

# Tokenless CI/OIDC Auth

Build / Defense

# Lower CI Perms

Build / Defense

# MCP System Credentials

Build / Vulnerability

# Insecure CI Configuration

Build / Vulnerability

# Lockfiles

Build / Defense

# Private Proxy Package Server

Build / Defense

# Publish SBOMs

Delivery / Defense

# Release Attestations

Delivery / Defense

# Trusted Publishing

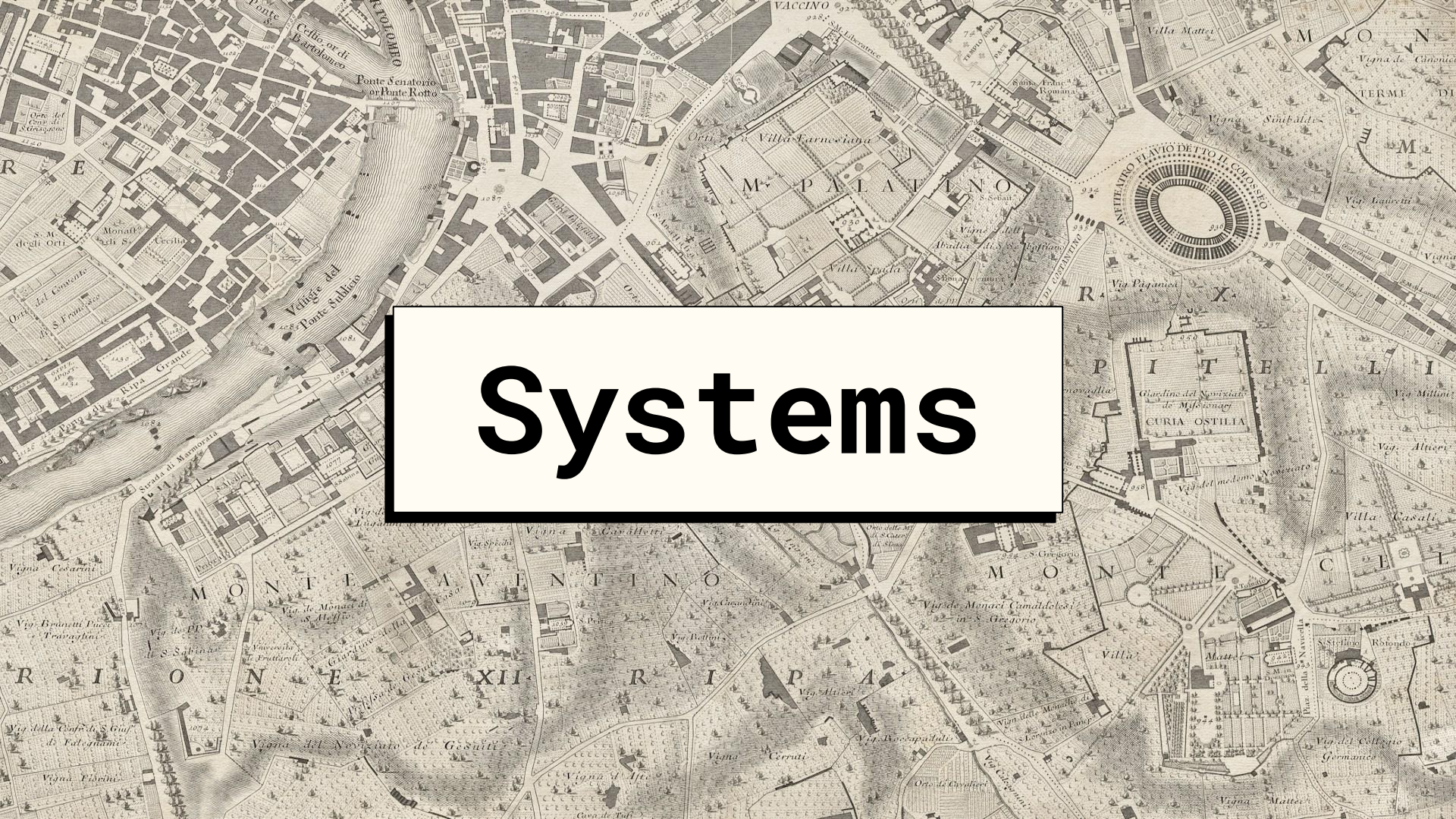
Delivery / Defense

# Release Diff Alerts

Delivery / Defense

# Token Theft

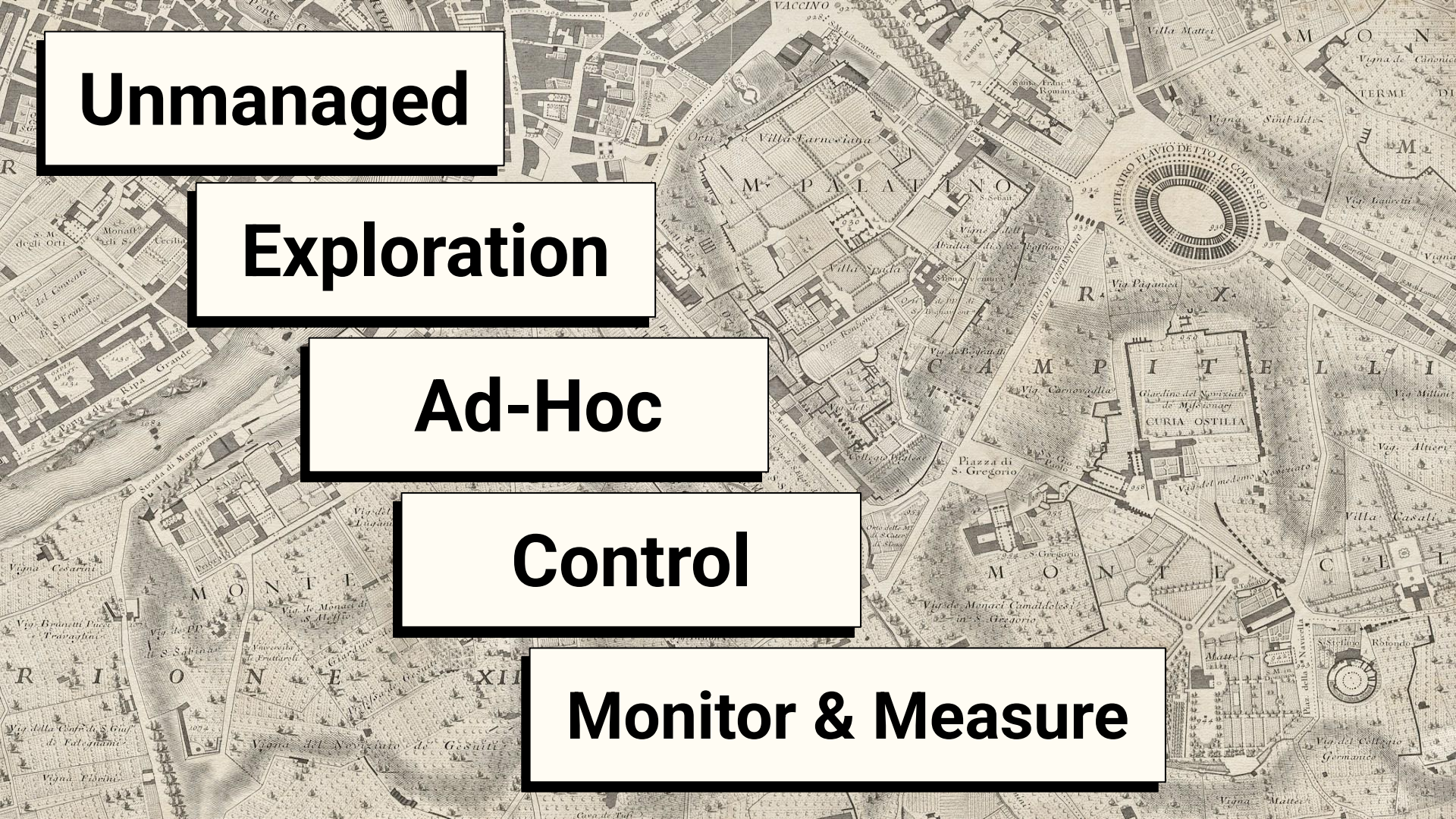
Delivery / Attack


Ponte Senatorio
or Ponte Rotto
Ponte Sublicio
Villa Farnesiana
M. PALATINO
ANFITEATRO FLAVIO DETTO IL COLOSSEO
CURIA OSTILIA
MONTE AVENTINO
MONTE CELIO
Vigna del Noviziato de' Gesuiti
Villa Casali
Villa Mattei

# Systems

# Supply Chain Security Maturity Model

RedHat / Sonatype



Unmanaged

Exploration

Ad-Hoc

Control

Monitor & Measure

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

# 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**


Colonna
Valle dell' Inferno
Vigna
Vig. Guerrini
Vigna Spada
Orto Castagnini
Cortile degli Archivj
Statue
Giardino Pontificio
Monte Vaticano
XIV
Porta Angelica
Giardino Salterj
Osteria da Vignola
Vigna Castrone
Vig. de Romanis
Vestigie del Circo d'Adriano
Porta Castello
Barone
Vigna di S. Spirito
Orto della Fabbrica di S. Pietro
Acquedotto dell' Acqua Paola
Vigna Caffri
Mausoleo d'Adriano ora Castello S. Angelo
Borgo Vecchio
Borgo S. Spirito
Orto Incoronati
Porta Fabbrica
Vig. Candolfi
Fornace Riccardi
Fornace della Consolaz.
Porta Cavalleggeri
Villa Barberini
Vigna Inghirami
Fornace Pizzi
Fornace Incoronati
Bastioni di S. Spirito
Vestigie del Ponte Trionfale
Ponte Adriano or S. Angelo
Piazza di Ponte

# SLSA

# Open Software Supply Chain Attack Reference (OSC&R)

# Software Supply Chain *Security*

**Source** → **Build** → **Delivery**

Rootconf 2025

# Around the Supply Chain in 80 Slides

Nemo, endoflife.date