Elections Infrastructure ISAC®

Managing Election Supply Chain Security Through Procurement

Grace Mozingo
EI-ISAC

Jared Marcotte
President, The Turnout

June 23, 2026

Overview

- Why supply chain risk matters
- Resources to guide you through procurement
- Threat modeling
- Connecting procurement to verification
- Case study

Why It Matters

- **Supply Chain: a network of organizations, individuals, resources, and information that, together, recreate and move a product or service to its final customer or end user**
- **Anything developed outside of an election technology provider's organization is impacted by supply chain**
- **What risk is acceptable?**

Supply Chain Attack Types

1. Developer tool compromise
2. Insider threats
3. Patch site corruption
4. Source or executable code modification
5. Download site compromise
6. Backdoor insertion
7. Third-party hardware/firmware corruption

Election Security Resources

- Handbook for Elections Infrastructure Security
- Essential Guide to Election Security
- Guide for Ensuring Security in Election Technology Procurements
- Security Best Practices for Non-Voting Election Technology

Threat Modeling

- Component
- IT Capabilities & Description
- Most Likely Attack Types
- Likelihood and Mitigations

Highest-Likelihood Threats Across Components

- Election Management System (EMS) - External Media
- Ballot Marking Device (BMD) - Processing
- Tabulation – Internal Memory & External Memory

Election Management System (EMS)

Example of Threat Modeling

- **Capability:** External Media (all data input & output)
- **Most Likely Attack Type:** Source or Executable Code
- **Mitigations:**
  - Firmware Boot/Runtime Verification
  - Strategic Sourcing
  - Device Allow-Listing (Whitelisting)
  - No Media Re-Use

Ballot Marking Devices (BMD)

Example of Threat Modeling

- **Capability:** Processing
- **Most Likely Attack Types:**
  - Firmware or Software Corruption Through:
    - Patch Site
    - Source or Executable Code
- **Mitigations:**
  - Firmware Update or Verification
  - Firmware Boot/Runtime verification
  - Secure Boot Devices
  - Digital Signature
  - Strategic Sourcing

Tabulation

Example of Threat Modeling

- **Capability:** Internal Memory
- **Most Likely Attack Type:** Source or Executable Code
- **Mitigations:**
  - Hardware and Firmware Verification
  - Digital Signatures
  - Strategic Sourcing

Tabulation

Example of Threat Modeling

- **Capability:** External Memory
- **Most Likely Attack Type:** Source or Executable Code
- **Mitigations:**
  - Device Allow-Listing (Whitelisting)
  - Digital Signatures
  - No Media Re-Use
  - Strategic Sourcing

Attacker Goals

- Confidentiality
- Integrity*
- Availability*

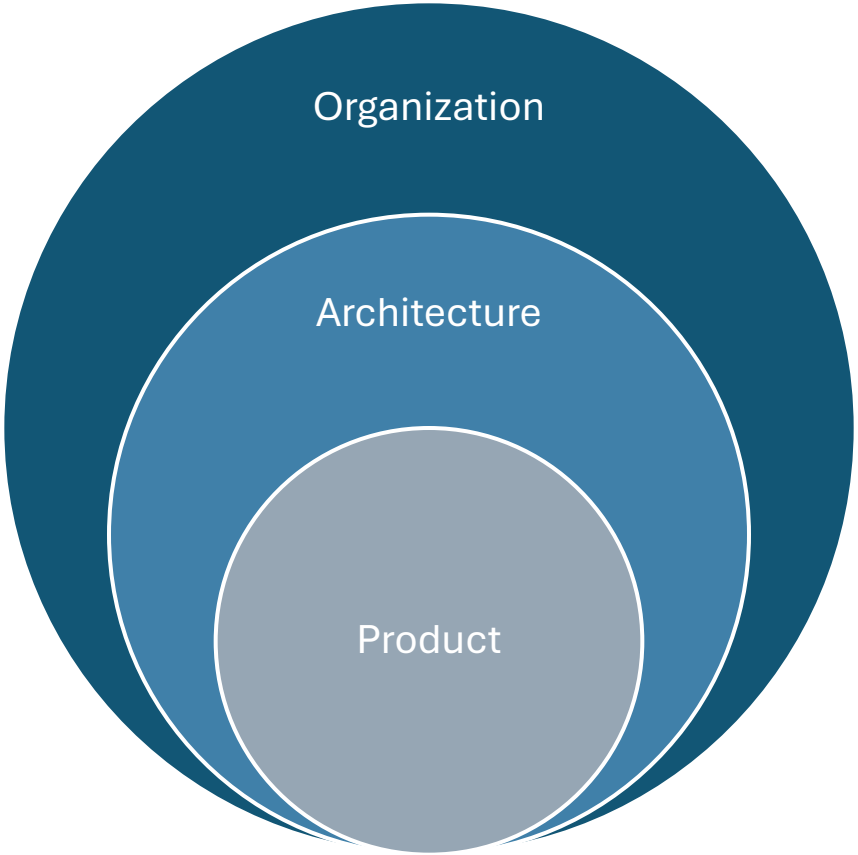
How do you know?

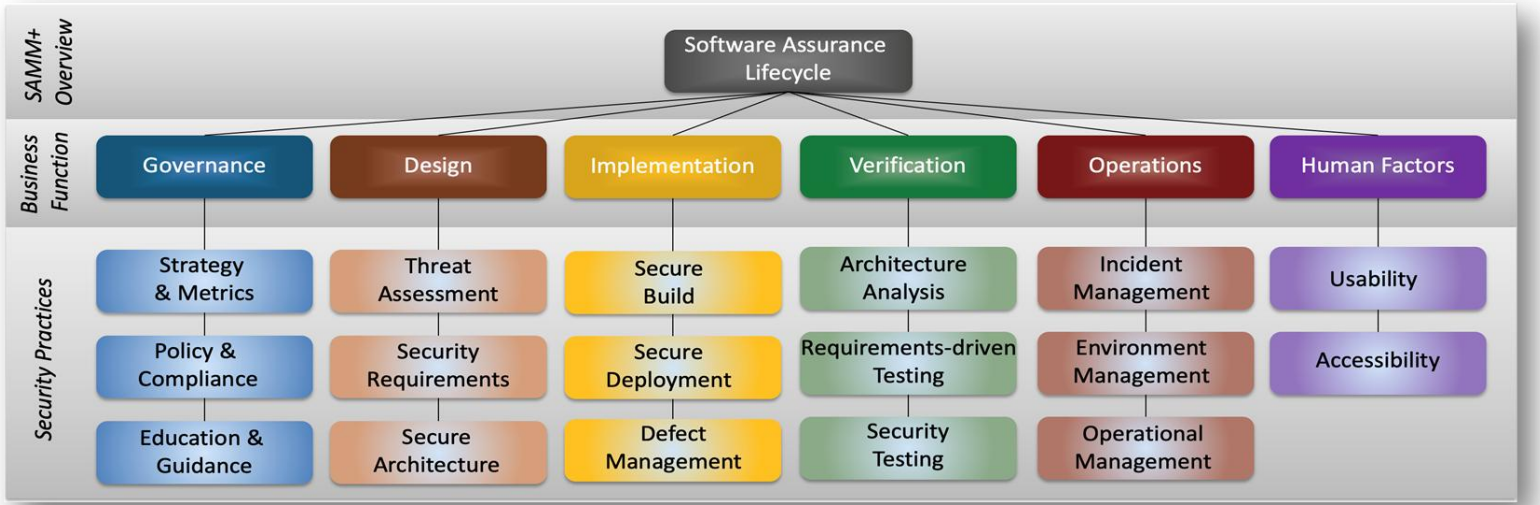
A Guide for

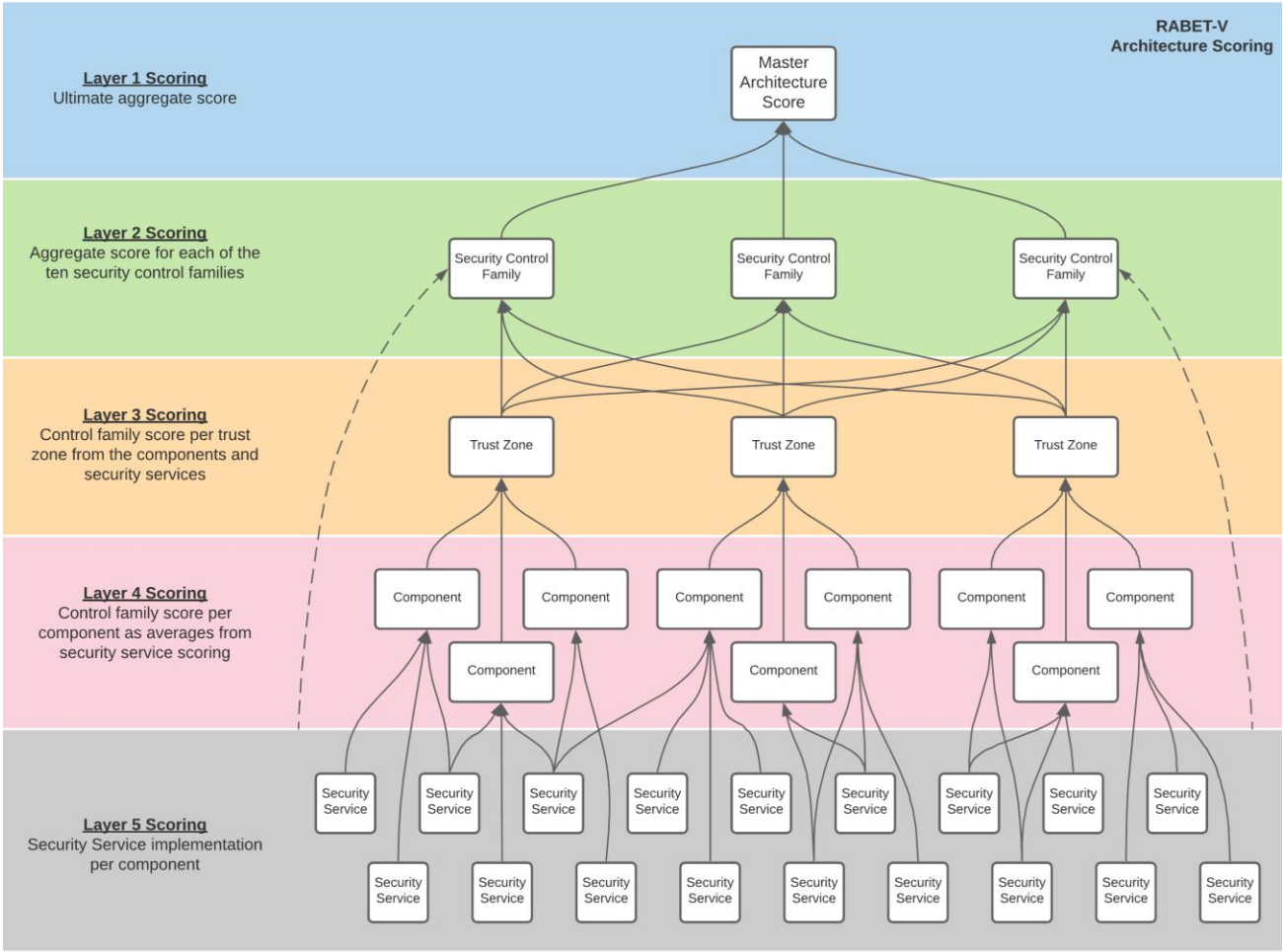
Ensuring Security in Election Technology Procurements

Scope of RABET-V™

- **Any software-based product**
  - One exception: voting systems


Organization
Architecture
Product

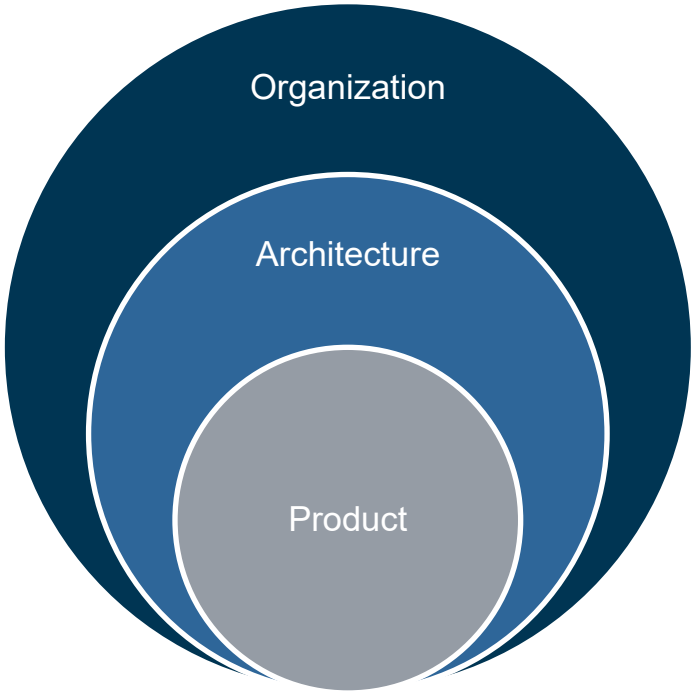

SAMM+ Overview
Software Assurance Lifecycle
Business Function
Governance
Design
Implementation
Verification
Operations
Human Factors
Security Practices
Strategy & Metrics
Policy & Compliance
Education & Guidance
Threat Assessment
Security Requirements
Secure Architecture
Secure Build
Secure Deployment
Defect Management
Architecture Analysis
Requirements-driven Testing
Security Testing
Incident Management
Environment Management
Operational Management
Usability
Accessibility


RABET-V
Architecture Scoring
Layer 1 Scoring
Ultimate aggregate score
Master Architecture Score
Layer 2 Scoring
Aggregate score for each of the ten security control families
Security Control Family
Security Control Family
Security Control Family
Layer 3 Scoring
Control family score per trust zone from the components and security services
Trust Zone
Trust Zone
Trust Zone
Layer 4 Scoring
Control family score per component as averages from security service scoring
Component
Component
Component
Component
Component
Component
Component
Component
Component
Layer 5 Scoring
Security Service implementation per component
Security Service

Product Verification

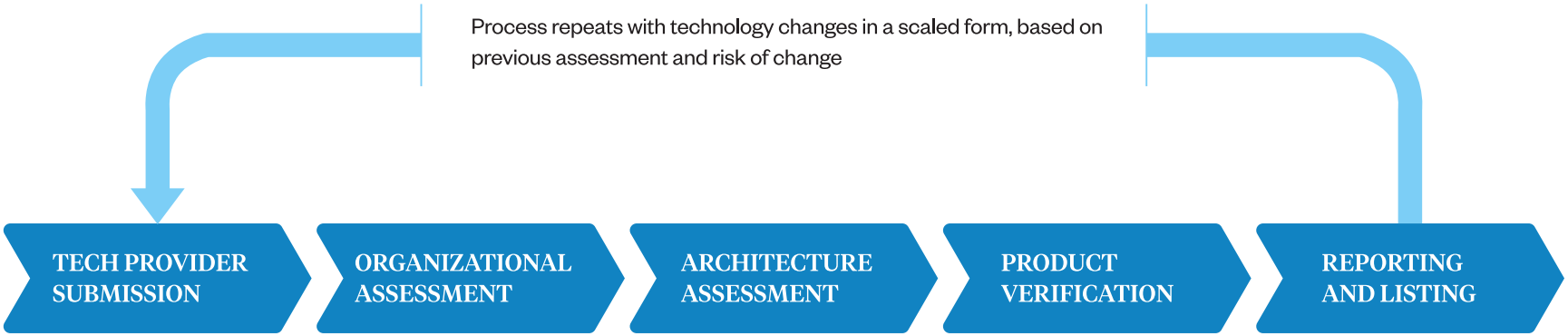
- Penetration Testing
- Compliance Audit
- Functional Testing

Defense in depth for verification



- **Organization:** *"Are their processes mature?"*
- **Architecture:** *"Is it built securely?"*
- **Product:** *"Does it behave securely?"*

The RABET-V Lifecycle: After the RFP



Tech provider submits a product to the RABET-V administrator, gets an initial scoping review, and is linked with accredited assessors.

Based on OWASP Software Assurance Maturity Model, RABET-V analyzes an organization's product development process to measurably determine its effectiveness at managing risks.

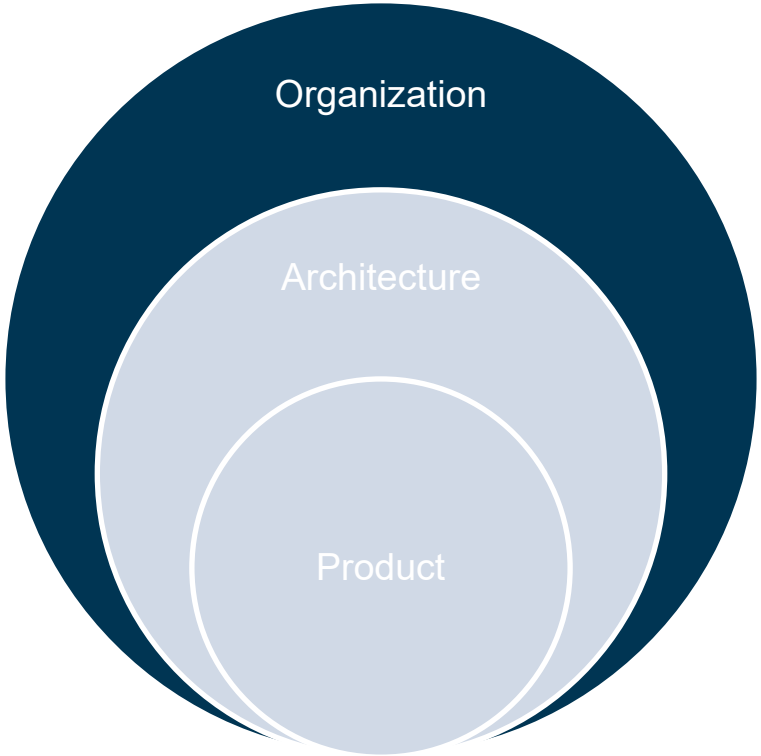
RABET-V analyzes a product's technology stack to determine if it is designed with modern techniques that lower the risk of failures and successful attacks.

RABET-V assessors determine whether a product appropriately mitigates risk and meets the tech provider's claims regarding security, usability, and accessibility.

Full reports for each step of the RABET-V process go to the tech provider and verified product versions are listed on RABET-V public listing site.

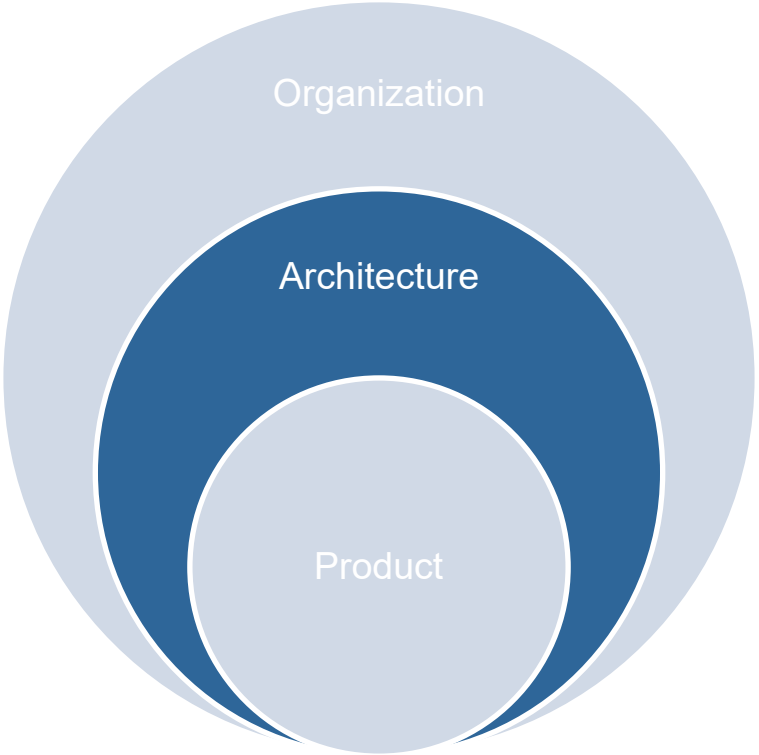
Process Assurance → Organizational Assessment

RFP → Organizational



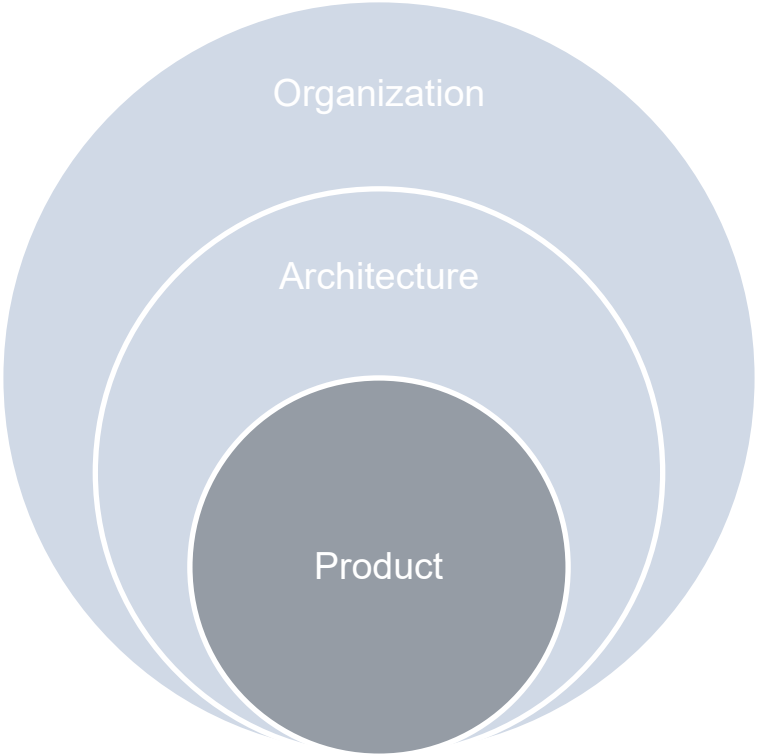
Architectural Integrity → Architecture Assessment

RFP → Organizational → Architecture



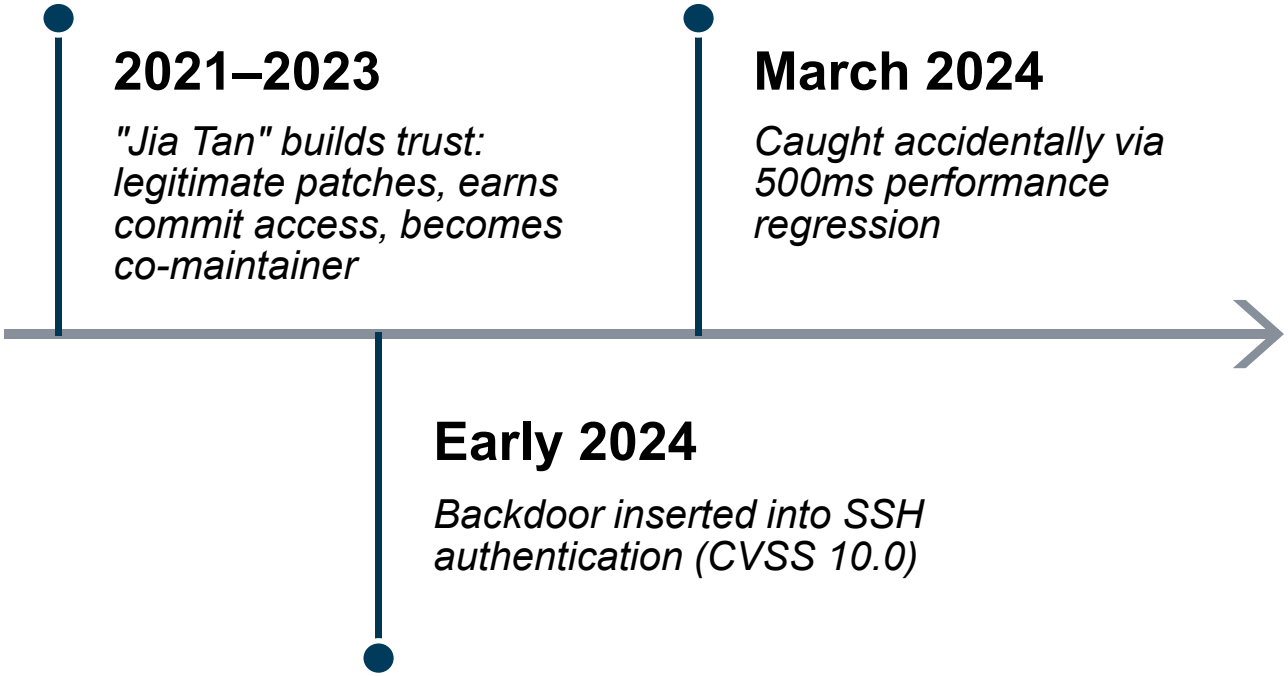
System Behavior → Product Verification

RFP → Organizational → Architecture → Product Verification



CIS tells you what to ask for. RABET-V tells you whether you got it.

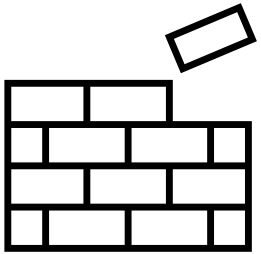
XZ Utils — CVE-2024-3094



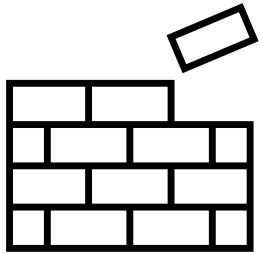
Three CIS Attack Types — One Incident

1. Developer tool compromise
2. **Insider threats**
3. Patch site corruption
4. **Source or executable code modification**
5. Download site compromise
6. **Backdoor insertion**
7. Third-party hardware/firmware corruption

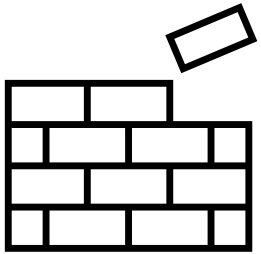
Defense-in-Depth Works



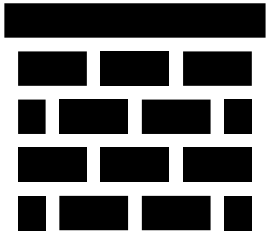
Code review



Trusted maintainer process



Cryptographic signing



Performance monitoring

Mapping the Attack to Procurement + RABET-V

Layer	What It Would Have Caught
Procurement (CIS)	*Visibility* into the dependency and its maintenance structure
Organizational Assessment	*Single-maintainer risk* and lack of independent review
Architecture Assessment	*The component itself*, scored for reliability and maintenance posture
Product Verification	*Anomalous behavior* in the deployed product

Supply Chains Change Over Time

Prior to July 2024

Polyfill.io

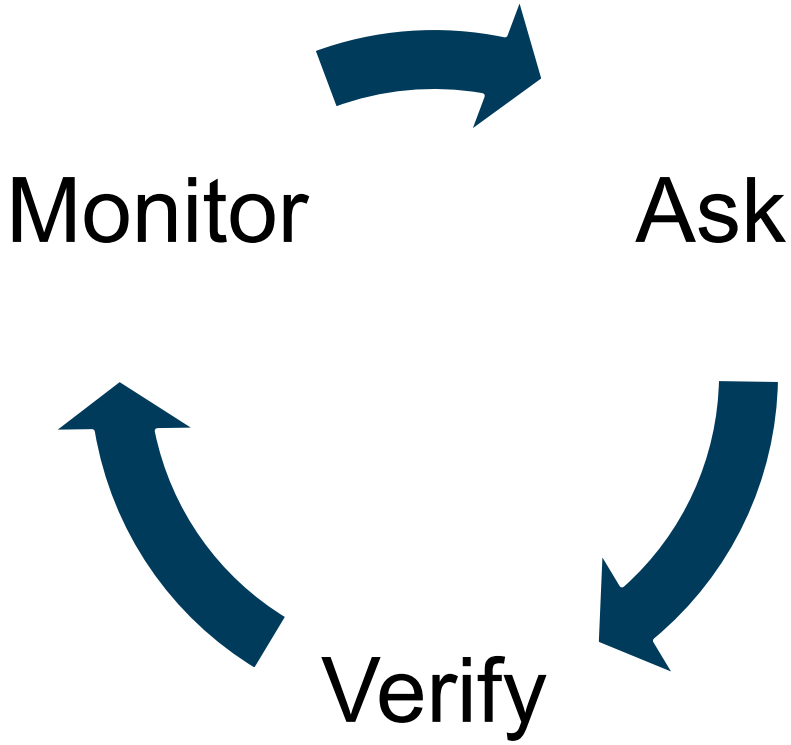
- **Trusted domain** 

July 2024

Polyfill.io

- **Nope!** 

Building a Continuous Assurance Ecosystem



What You Can Do

- Review the CIS's Guide to Election Technology Procurements
- Ask your vendors about their RABET-V verification status
- Start a supply-chain inventory
- Bring these resources back to your jurisdiction

CIS tells you what to ask for. RABET-V tells you whether you got it.

Resources

- **“The CIS Guide to Election Technology Procurements,” https://election-procurement.docs.cisecurity.org/en/latest/readme.html**
- **“Incorporating RABET-V into Government Procurement Policies,” Grace Gordon, https://turnout.rocks/our-blog/incorporating-rabet-v-into-government-procurement-policies/**

Guide

Article

Elections Infrastructure ISAC®

Thank You!

elections@cisecurity.org
team@rabetv.org