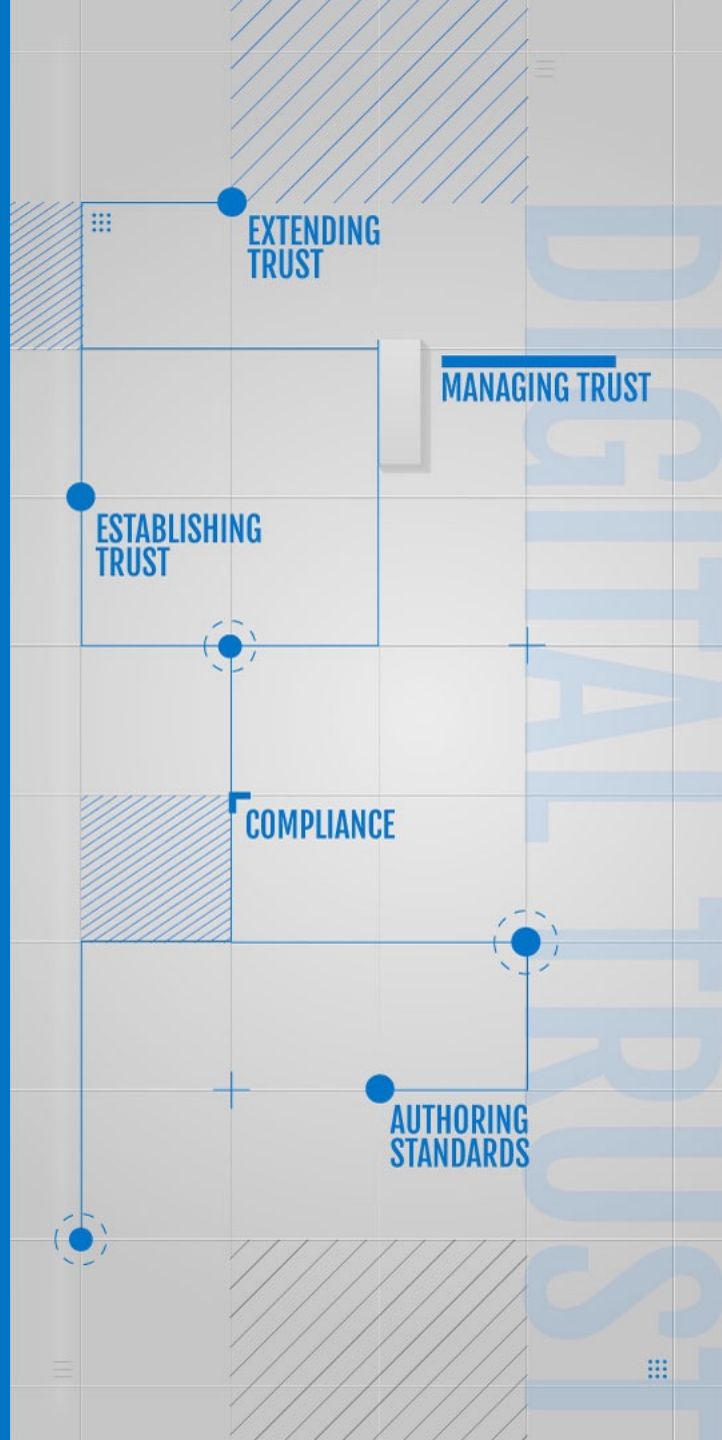
SECURING YOUR SOFTWARE DEVELOPMENT LIFECYCLE

5 Strategies to Protect Your Software Development Teams from Software Supply Chain Attacks

digicert®



SOFTWARE ATE THE WORLD




PRACTICALLY EVERY BUSINESS IS A SOFTWARE BUSINESS.





Financial | Healthcare | Transportation | Infrastructure | Retail | Agriculture | Industrial | Insurance | Communications | Tech | Entertainment

91%

of businesses reported
a software supply chain attack last year

-- Data Theorem

LOST REVENUE, MARKET SHARE, REPUTATION

CRASHES, ACCIDENTS

NotPetya malware estimated by US Dept of Homeland Security to cause $10B in world-wide damages

CUSTOMER DATA BREACH

CIVIL FINES

LIABILTY

ALL COMPANIES ARE AT RISK

BLEEPINGCOMPUTER

Hackers compromise 3CX desktop app in a supply chain attack

A digitally signed and trojanized version is reportedly being used to target the company's customers in an ongoing supply chain attack.

The Hacker News

Malware Attack on CircleCI Engineer's Laptop Leads to Recent Security Incident

Jan 14, 2023 Ravie Lakshmanan DevOps / Data Security

The CI/CD service CircleCI said the "sophisticated attack" took place on December 16, 2022, and that the malware went undetected by its antivirus software.

Malwarebytes LABS Personal Business Pricing Partners

NEWS | RANSOMWARE

Ransomware attack on MSI led to compromised Intel Boot Guard private keys

slack

circleci

okta

Travis CI

twilio

HEROKU

WHY IS STOPPING THESE ATTACKS SO HARD?

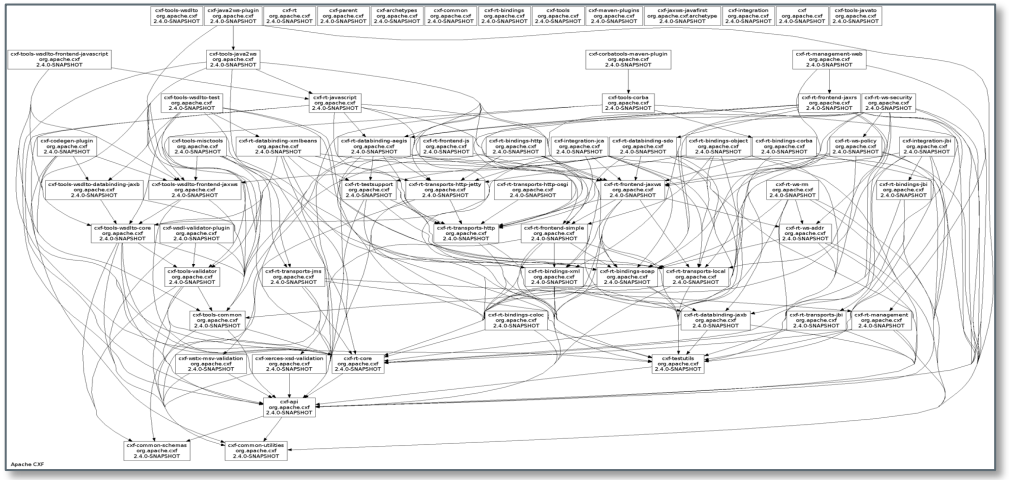
- Modern Software is Complex
- Organizations are Siloed & Understaffed
- Broad Attack Surfaces & Diverse Attacks

MODERN SOFTWARE IS COMPLEX

Stall Warning Computer, Circa 1990

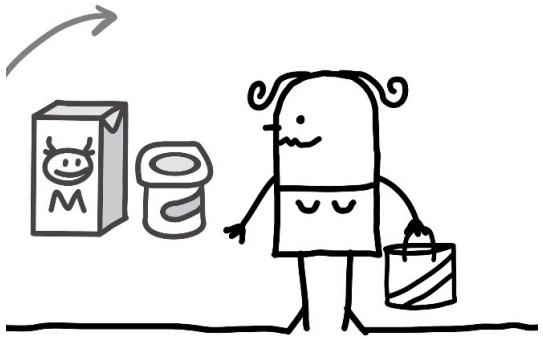
- 1 Software Developer
- 100% of Code Written in House
- 5K SLOC (Assembly Language)
- 1 Software Release a Year
- Not Connected to the Internet

Apache HTTP Project, 2024



- Started In 1995 by 8 Developers
- Since Then, > **630,000 Worldwide Contributors**
- ~ 2M SLOC (Java)
- Multiple Platform Support
- New Releases at Least Quarterly

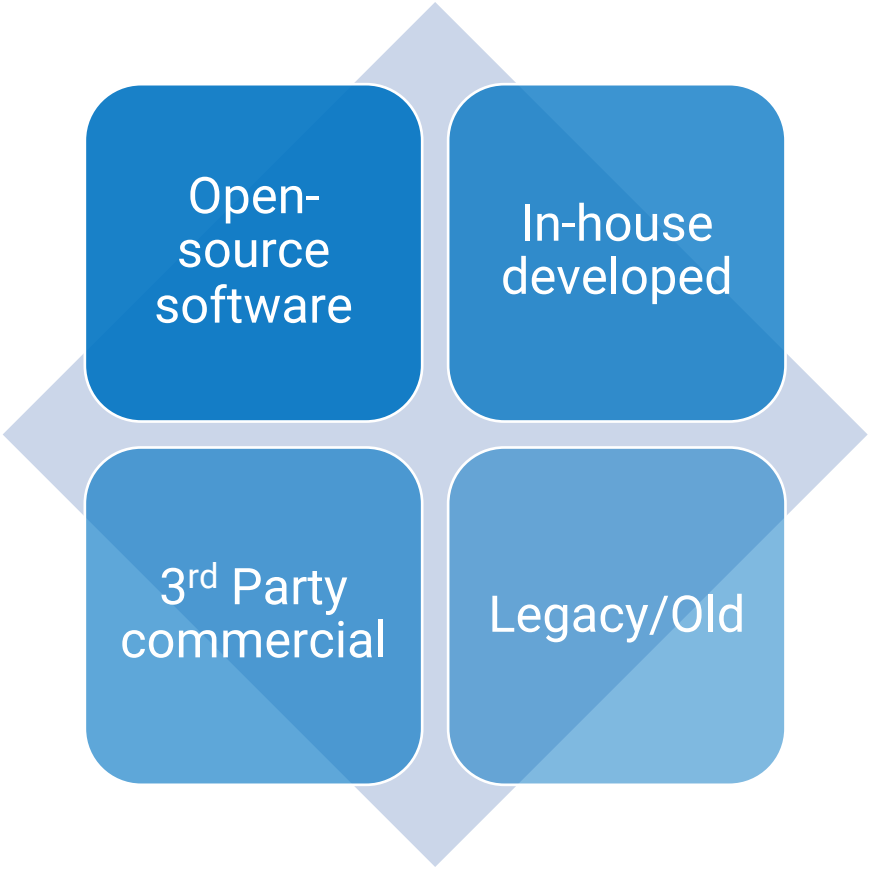
WHAT IS A SUPPLY CHAIN?



SOFTWARE SUPPLY CHAIN

Where Does Your Software Come From?

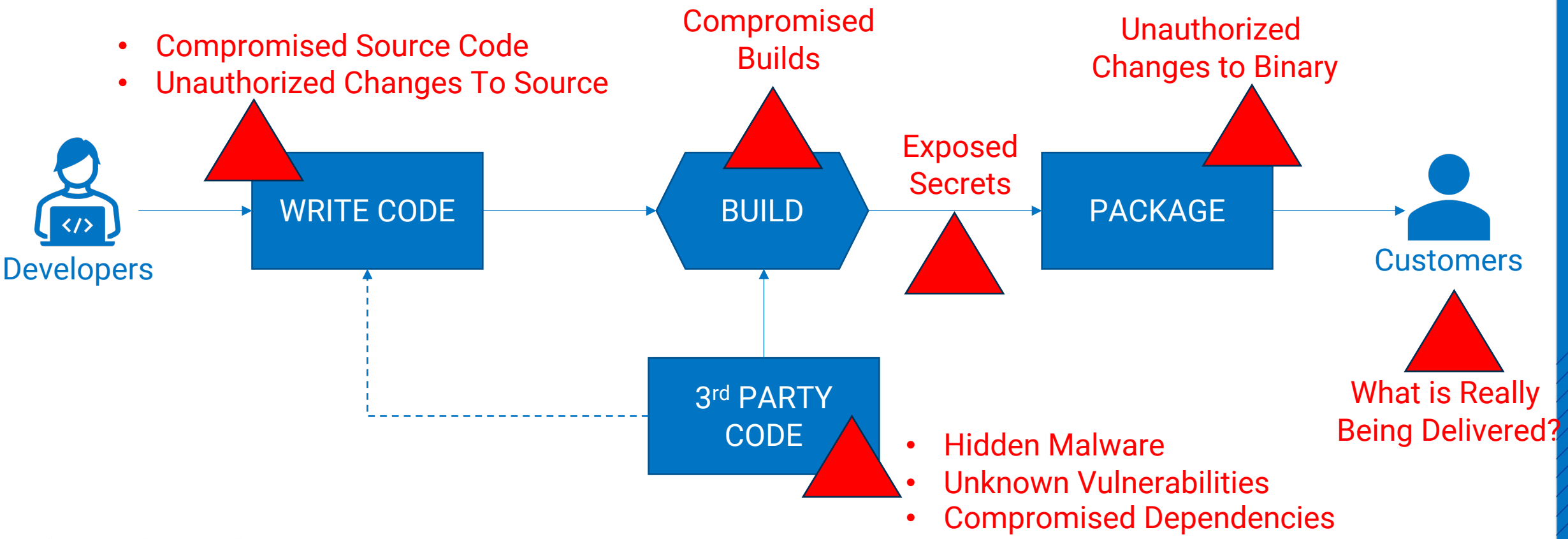
External



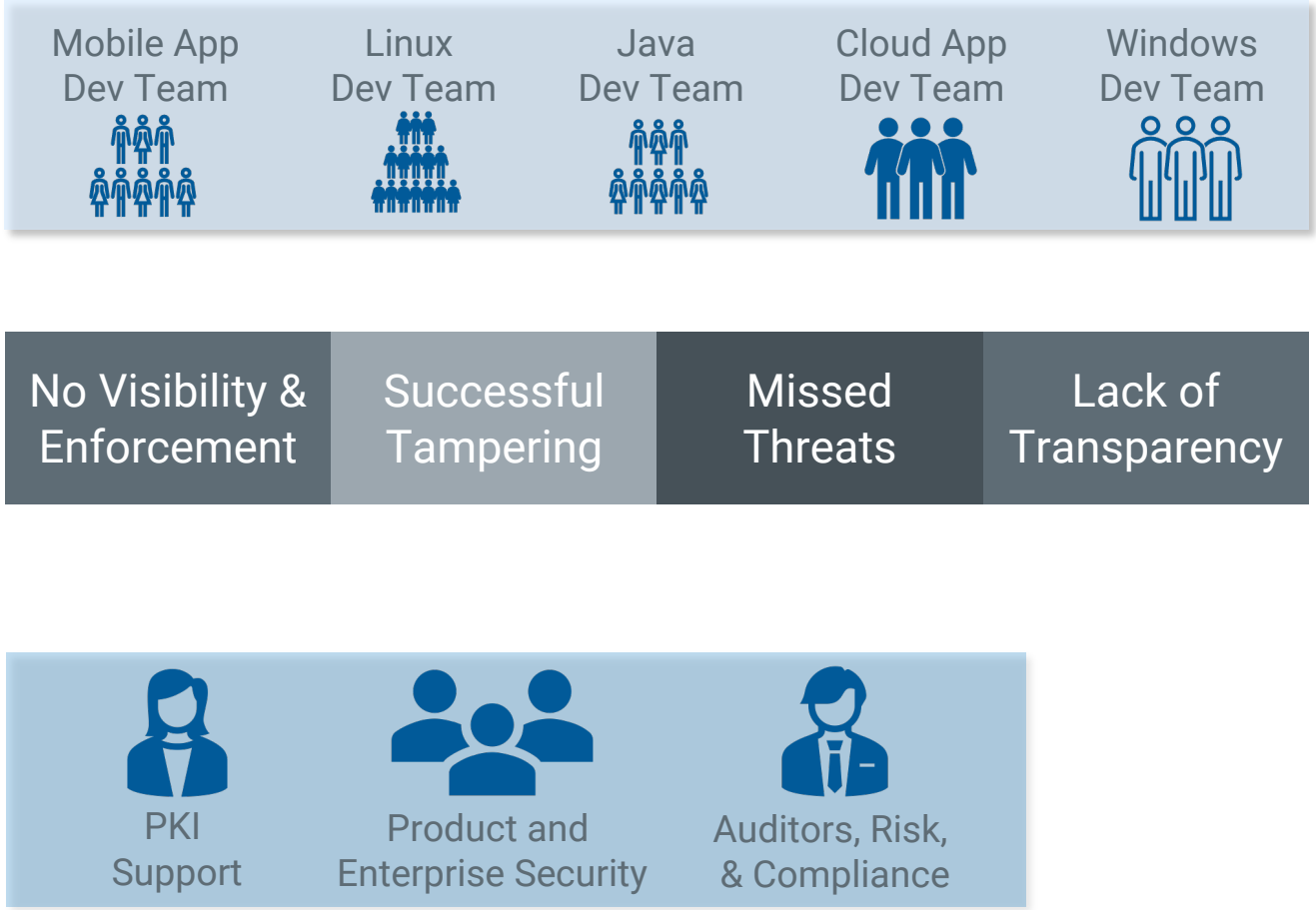
Internal

BROAD ATTACK SURFACE

Attacks Can, and Do, Happen Anywhere During This Process



ORGANIZATIONAL CHALLENGES

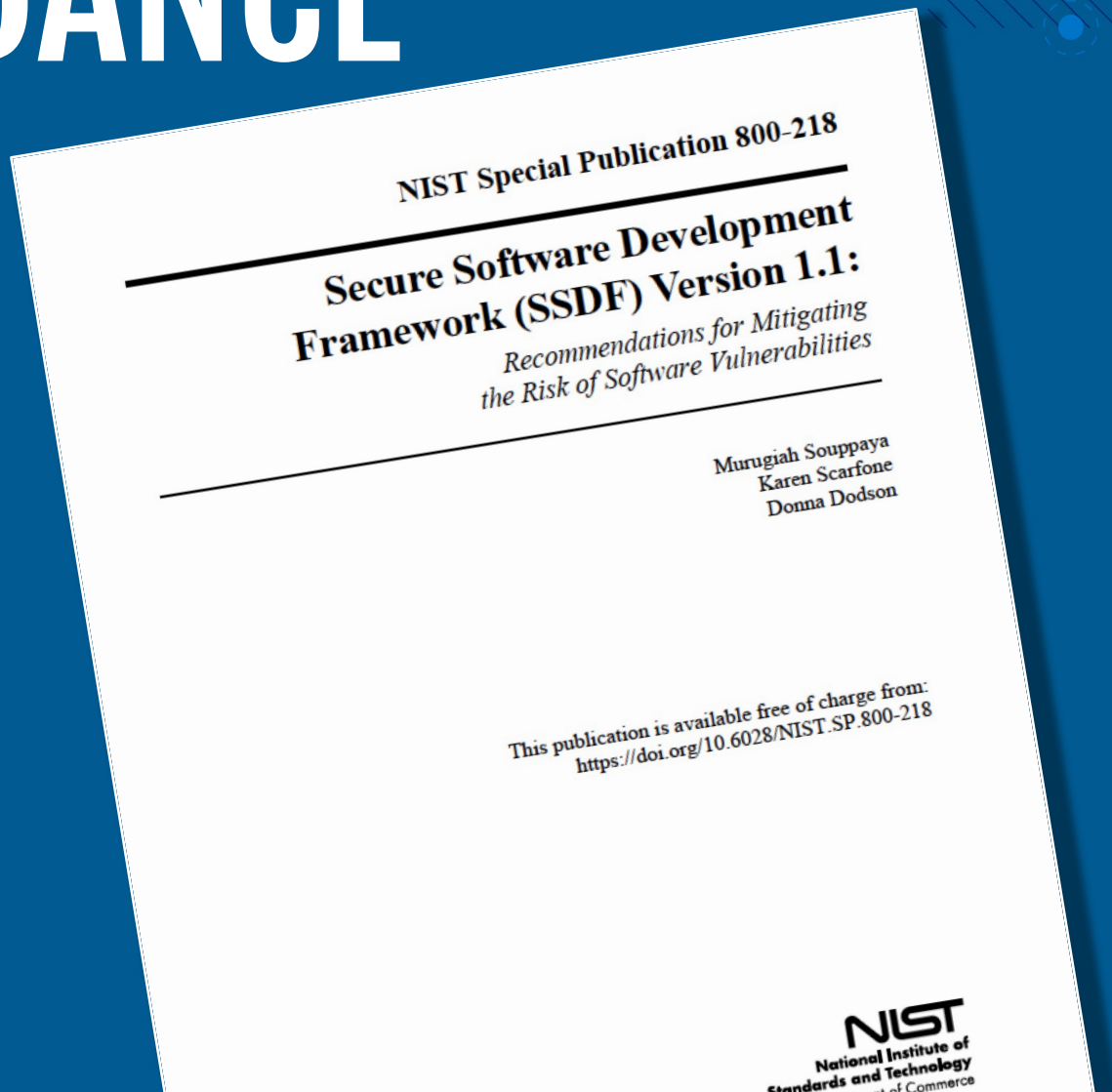


- Software complexity
- People
  - Disparate software teams, tools & methodologies
  - Pressure to do more in less time
  - Security often lower priority than new features
- Organization
  - Siloed teams – people, process, and technology
  - Product security & PKI support often understaffed
  - Security tools not automated and integrated with dev processes

5 STRATEGIES

To Prevent Software Supply Chain Attacks

INDUSTRY GUIDANCE



NIST Special Publication 800-218

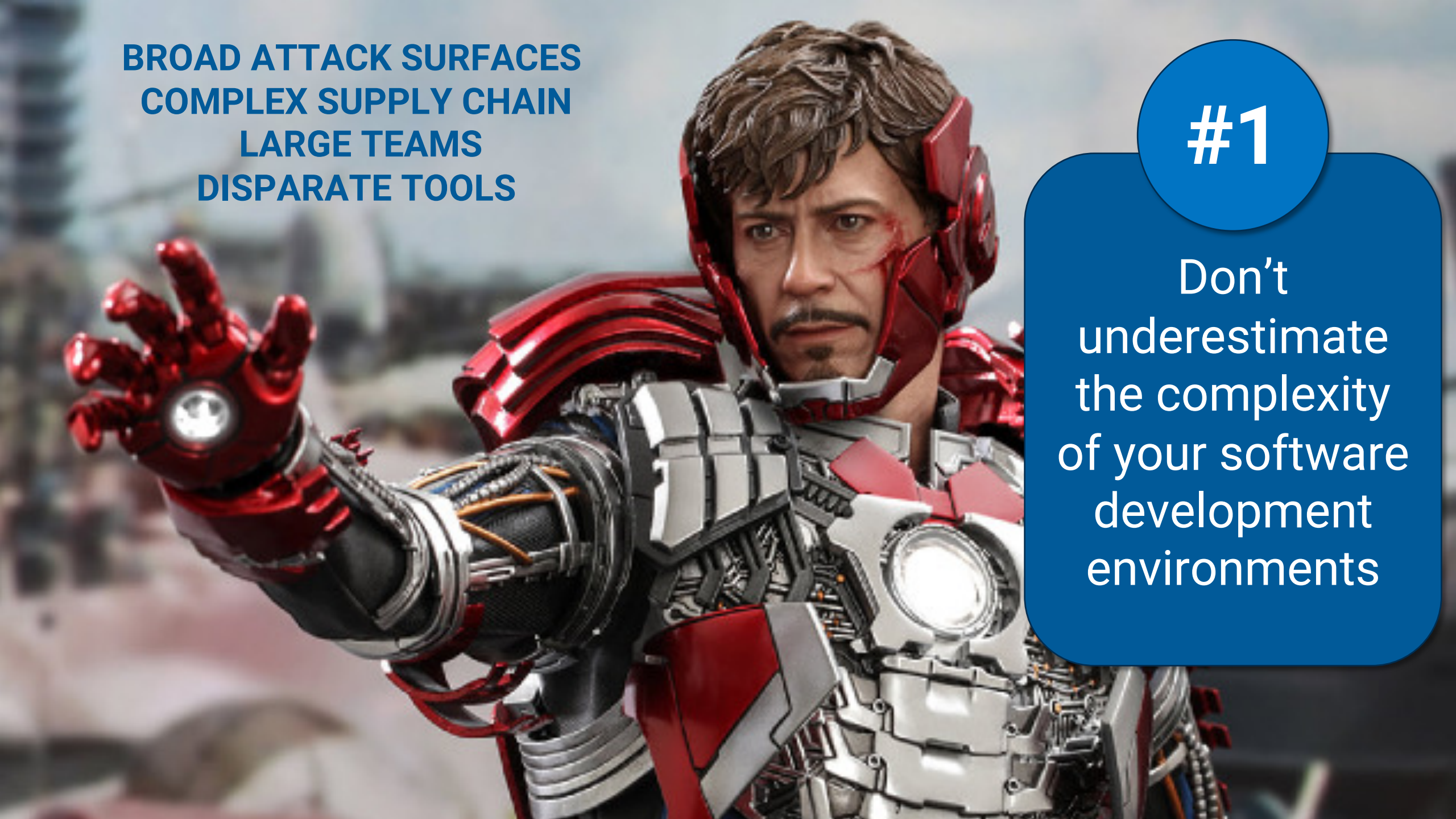
Secure Software Development Framework (SSDF) Version 1.1:

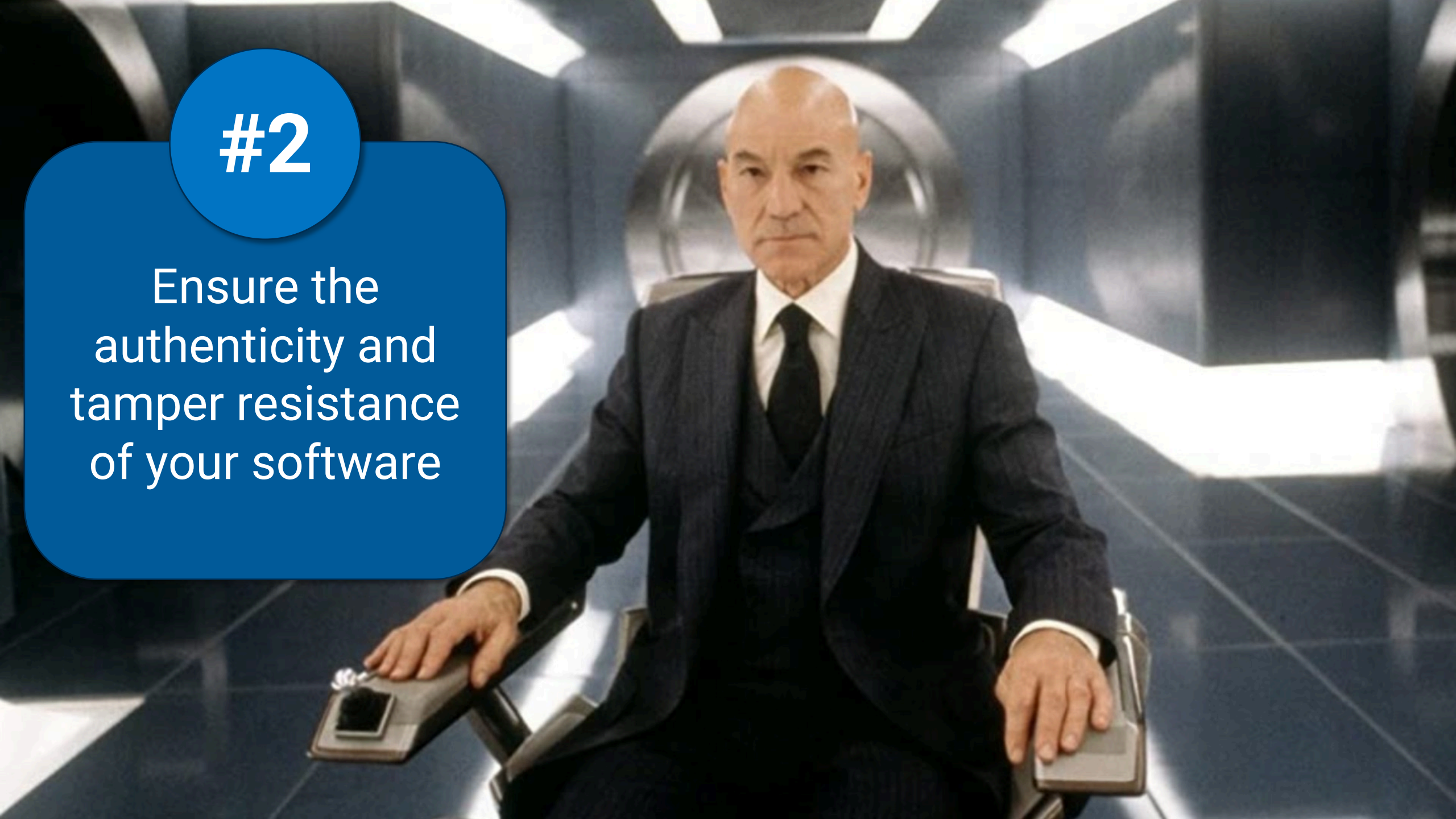
Recommendations for Mitigating the Risk of Software Vulnerabilities

Murugiah Souppaya
Karen Scarfone
Donna Dodson

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-218

NIST
National Institute of Standards and Technology


BROAD ATTACK SURFACES
COMPLEX SUPPLY CHAIN
LARGE TEAMS
DISPARATE TOOLS
#1
Don’t underestimate the complexity of your software development environments



#2

Ensure the authenticity and tamper resistance of your software

CODE SIGNING

A certificate-based digital signature that is used to ‘sign’ software to:

- Verify the author’s identity
- Ensure that it has not been altered or corrupted since it was signed

ANATOMY OF CODE SIGNING

- Requires a code signing certificate obtained from a public certificate authority, like DigiCert

- Private key must always remain secured or else bad actors can sign code in your company's name or change your code

"Like a birth certificate for code"

CODE SIGNING BEST PRACTICES

Secure private key storage is not enough!

- Define separate roles and permissions
  - Signers, approvers, security
- Centralize policy enforcement
  - Certificate & key configurations
  - Who has access
- Centralize visibility of all code signing activities
  - All certificates used
  - Log of all files signed
  - Log of all signatures

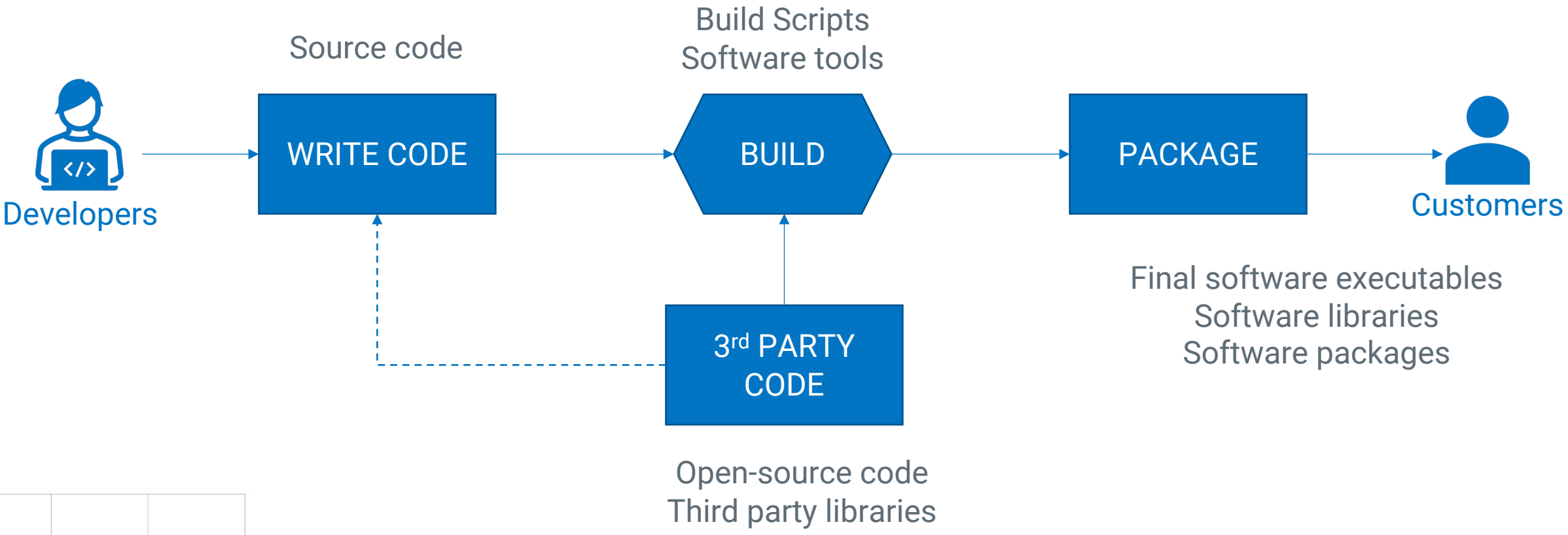
Must be easy for developers to use

Must support multiple software dev environments

SIGN OFTEN AND EVERYTHING

Code signing isn't just for final software executables

Prevents tampering throughout the SDLC & shows authenticity

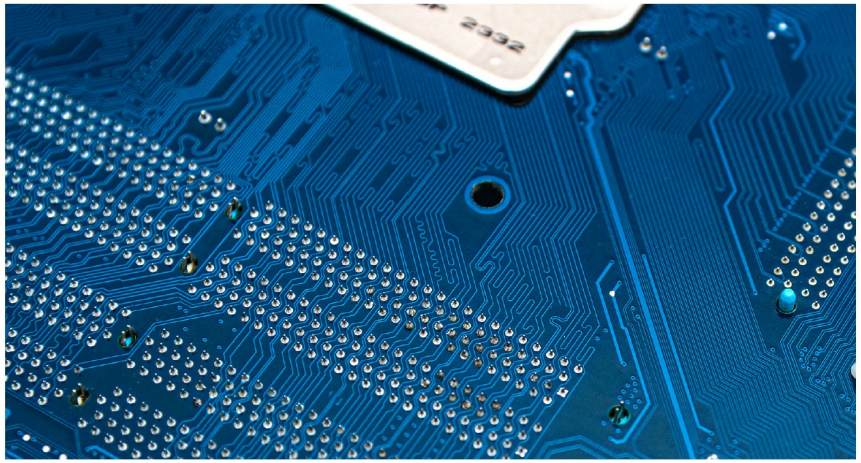


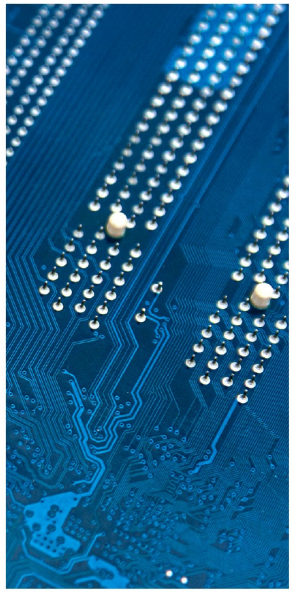
DIGICERT CUSTOMER SUCCESS STORY

Critical software/firmware needed to be protected from supply chain attacks.

Role-based security permissions important to ensure security.

Decentralized workforce made centralized policy enforcement & visibility impossible





ST Case Study

life.augmented

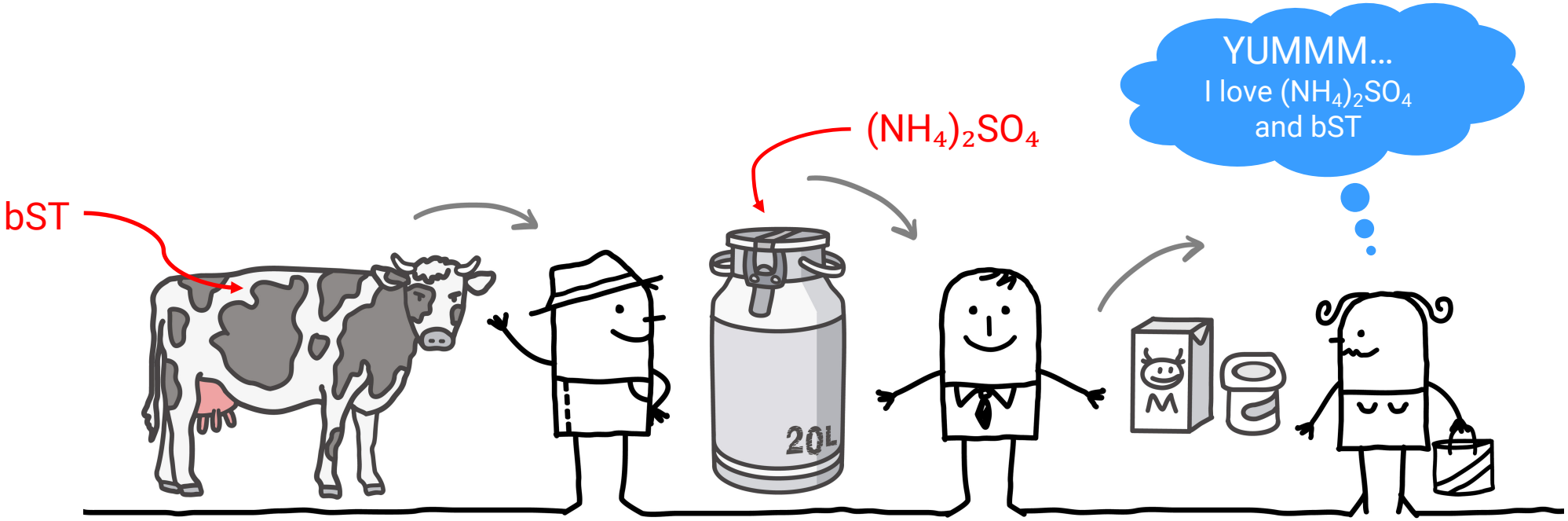
A world leader in hardware provides trust with software signing

digicert®


#3
Scan for threats, vulnerabilities, and malware

SOFTWARE SUPPLY CHAIN

Threats from everywhere

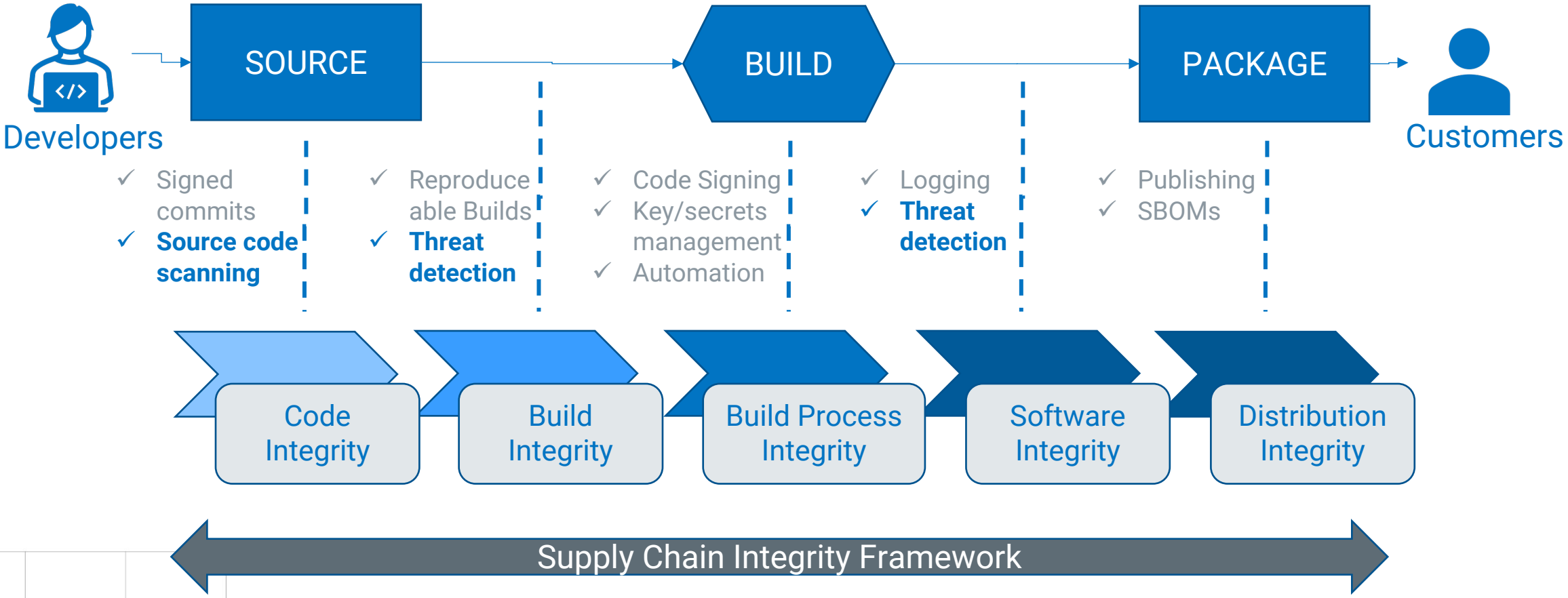


Raw ingredients
(proprietary, open source,
3rd party libraries)

Manufacturing
(software dev)

Distribution

THREAT, VULNERABILITY & MALWARE DETECTION



DIGICERT CUSTOMER SUCCESS STORY

Vulnerability, threat and malware detection

Software for critical infrastructure a frequent target of state-sponsored attacks.

Open-source software widely leveraged.

Frequent software releases

Security team required that scans be completed before final software signed and shipped.

#4

Ensure software transparency

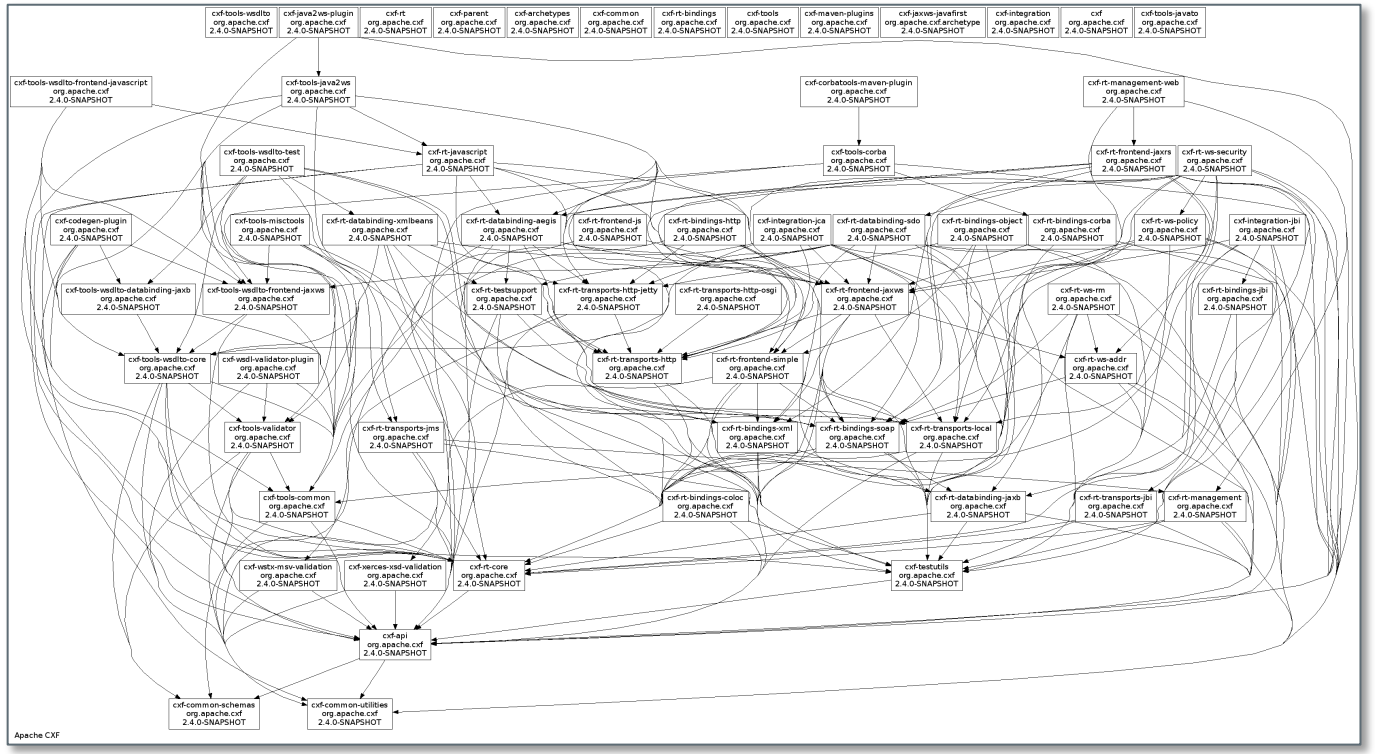
Software Bill of Materials (SBOM)

WHAT ARE SBOMS?

Software Bill of Materials (SBOMs)

- More than just an ‘ingredient list’ for a piece of software:
  - Dependencies & relationships
  - File information
  - Packages
  - Versions
  - Lineage (where components come from)
  - Ascertain the quality of components

- Helps to understand if there are healthy or dangerous ingredients in the software



Apache HTTP Server Dependency Graph – approx. 2M SLOC

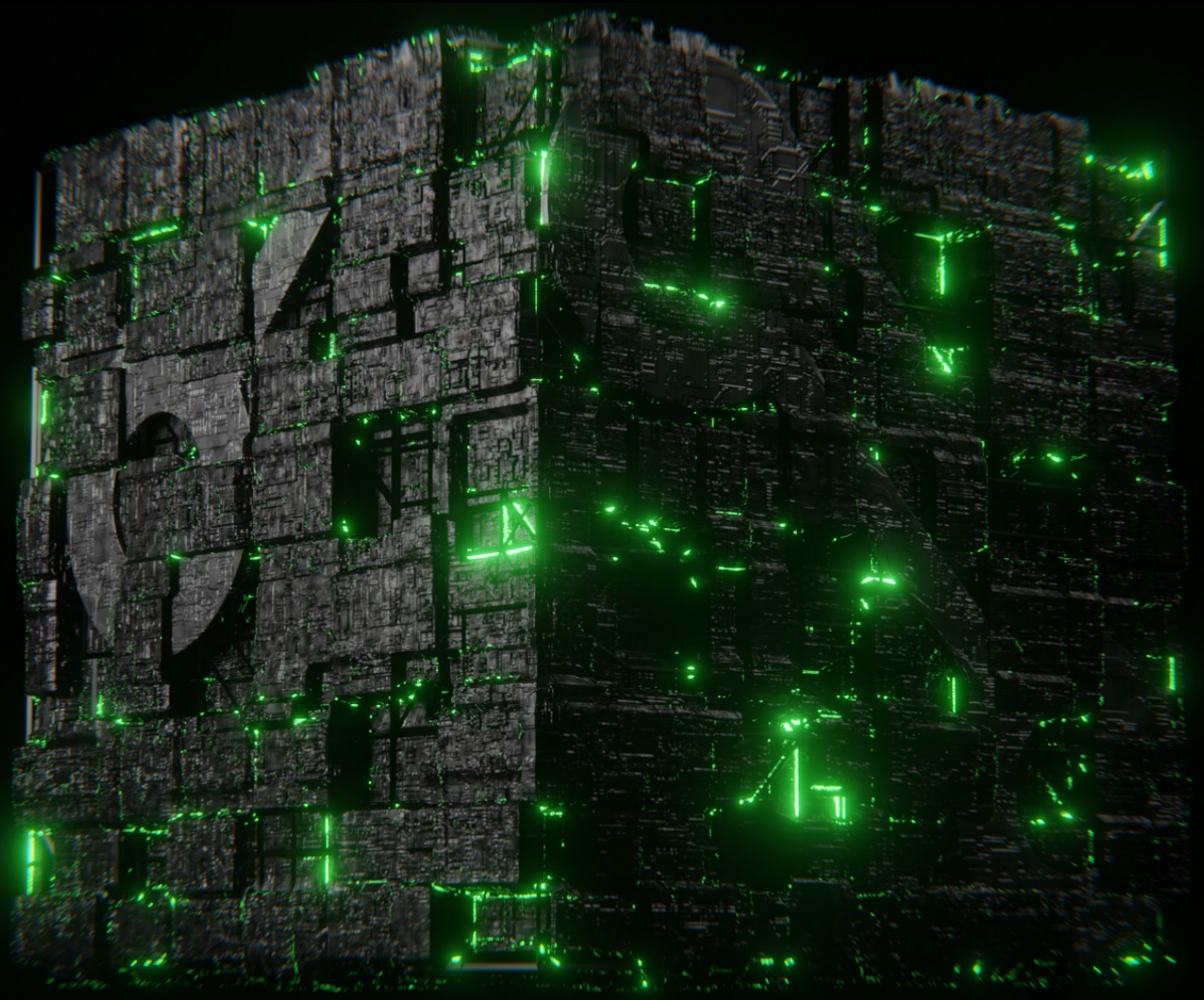
DON'T JUST GENERATE SBOM'S – USE THEM!

Operationalizing SBOMS

- Look for vulnerable or targeted versions of libraries or components
- Look at dependencies
- Check to see if there are missing mandated security patches
- Look for missing mitigations
- Look for insecure code signing practices
- Use for threat modeling

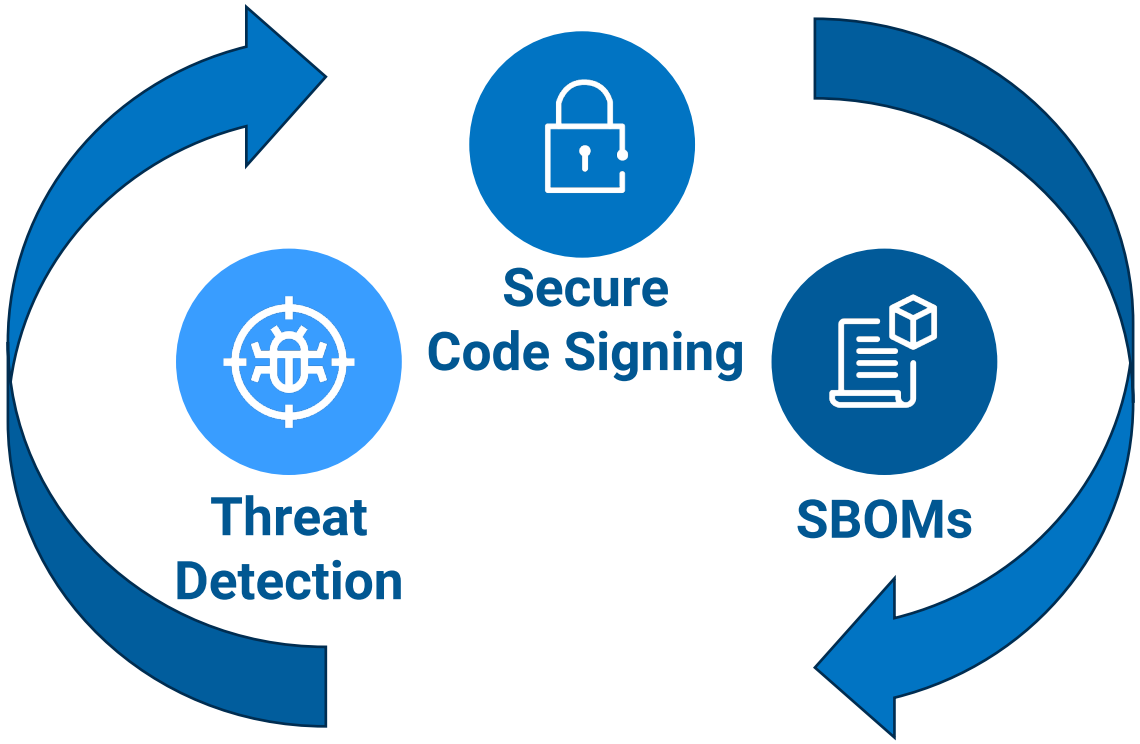
#5

Automate with Enterprise Visibility and Control



EMBED & AUTOMATE THESE ACTIONS IN EVERY RELEASE CYCLE

Threat detection, code signing & SBOMs in a unified security workflow



DIGICERT CUSTOMER SUCCESS STORY

Automated code signing into SDLC.

Secured code signing with secure key storage and role-based access.

Centralized visibility and enforcement across all software teams.

CASE STUDY

DeNA

digicert®

AUTOMATED SIGNING SPEEDS BUILD TIMES WHILE IMPROVING THE USER EXPERIENCE

Delivering Robotic Process Automation

Since April 2020, DeNA Corporation has enabled customers to easily switch between cloud and local execution environments when using its cloud-based Robot Process Automation (RPA) service, Coopel. Coopel performs EV Code Signing at the time of build, so native Windows apps don't display warnings at install time. Initially, DeNA used physical credentials for this service, but that limited operation. In search of a faster, more flexible solution, DeNA turned to DigiCert® Software Trust Manager.

About DeNA

Established in March 1999, DeNA has launched a series of new internet services, including Bitters and Mobage. Today, the company's business is not limited to the internet, but has expanded into sports, healthcare, and urban development. DeNA continues to grow while boldly taking on new challenges. The company places great importance on user delight, something that's reflected in the DeNA logo, emphasizing a mission to "provide each individual with delight beyond imagination."

DeNA Corporation

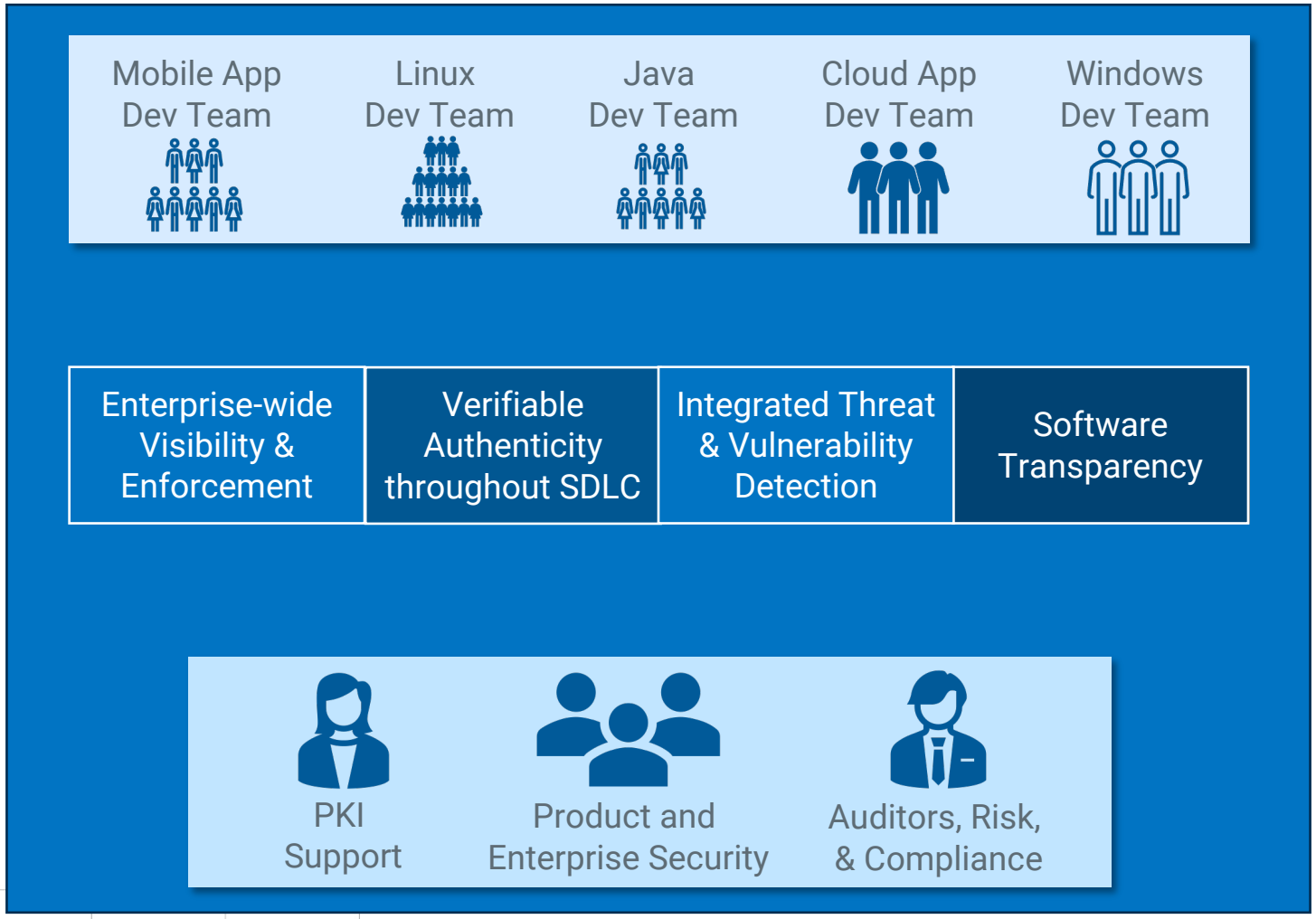
Website: dena.com/intl

Industry: IT Service

Challenge: Reducing the operational burden of EV code signing

Deployment service: DigiCert® Software Trust Manager

DIGICERT SOFTWARE TRUST MANAGER



- Unify Dev, PKI, security, & compliance
- Single pane of glass
- Enforce configurable security controls
- Role based & secure signing
- Automate threat & vulnerability scanning
- Generate comprehensive software bills of materials
- Easy to integrate into build process
- Scale across the enterprise

Free Software Supply Chain Risk Assessment

Scan to schedule a free and no obligation risk assessment with DigiCert software supply chain security experts. We'll spend up to 1 hour with you and your team understanding your current software supply chain practices and providing you with an assessment of your risks and ways to address them.

SUMMARY

Free Software Supply Chain Risk Assessment

https://www.digicert.com/campaigns/digital-trust-and-software-supply-chain-attacks/free-assessment

digicert®

TRUST SUMMIT ROAD SHOW