Software Supply Chain Security

Threats, Defenses, and What You Can Do

Yesenia Yser

Technical Ops Lead, Supply Chain Security, Red Hat Product Security

Red Hat
Product Security

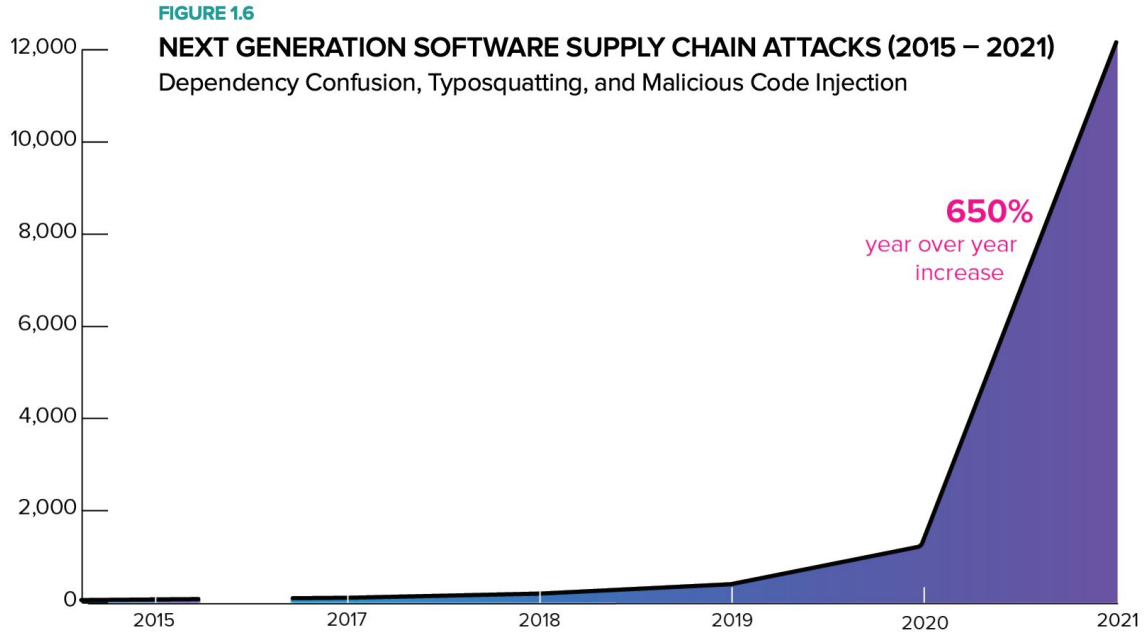
Agenda

- What is Software Supply Chain? Why is it such a hot topic?
- Technical Overview of Supply Chain Security
- Threats and Attack Vectors
- Security Recommendations
- Balancing Act of Security

What is Software Supply Chain?

Why is it such a hot topic?

Global focus in 2022 continues



2021 STATE OF THE SOFTWARE SUPPLY CHAIN REPORT

"Attackers focused on the supplier's code in about 66% of the reported incidents"

-- ENISA report, "Understanding the Increase in Supply Chain Security Attacks"

February 2021

- US Executive Order on supply chains, including software

May 2021

- US Executive Order on software supply chains and cybersecurity
- UK seeking advice on supply chain security
- Germany passes Information Technology Security Act 2.0
- UN releases report that touches on software supply chain security, with guidance

July 2021

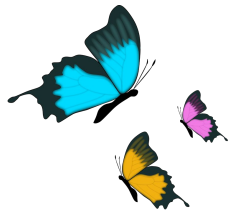
- ENISA issues "Understanding the increase in Supply Chain Security Attacks" report

December 2021

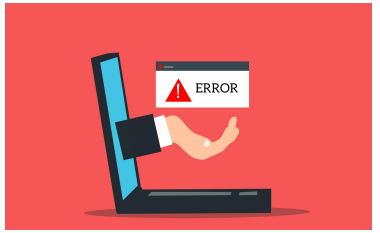
- Software development considered a "key national security concern" by the White House

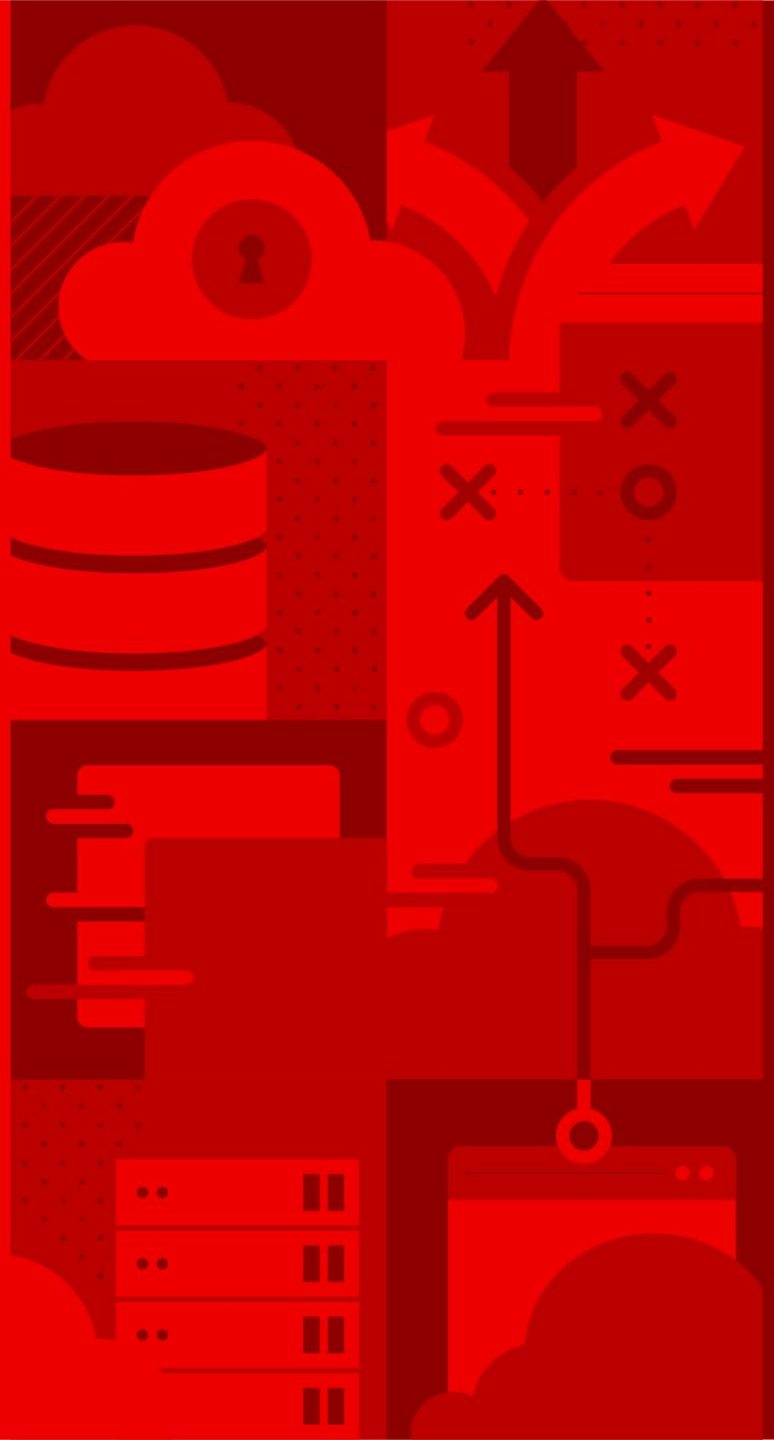
Technical Overview of Supply Chain Security

Basic Assembly Line



What if something fails...?



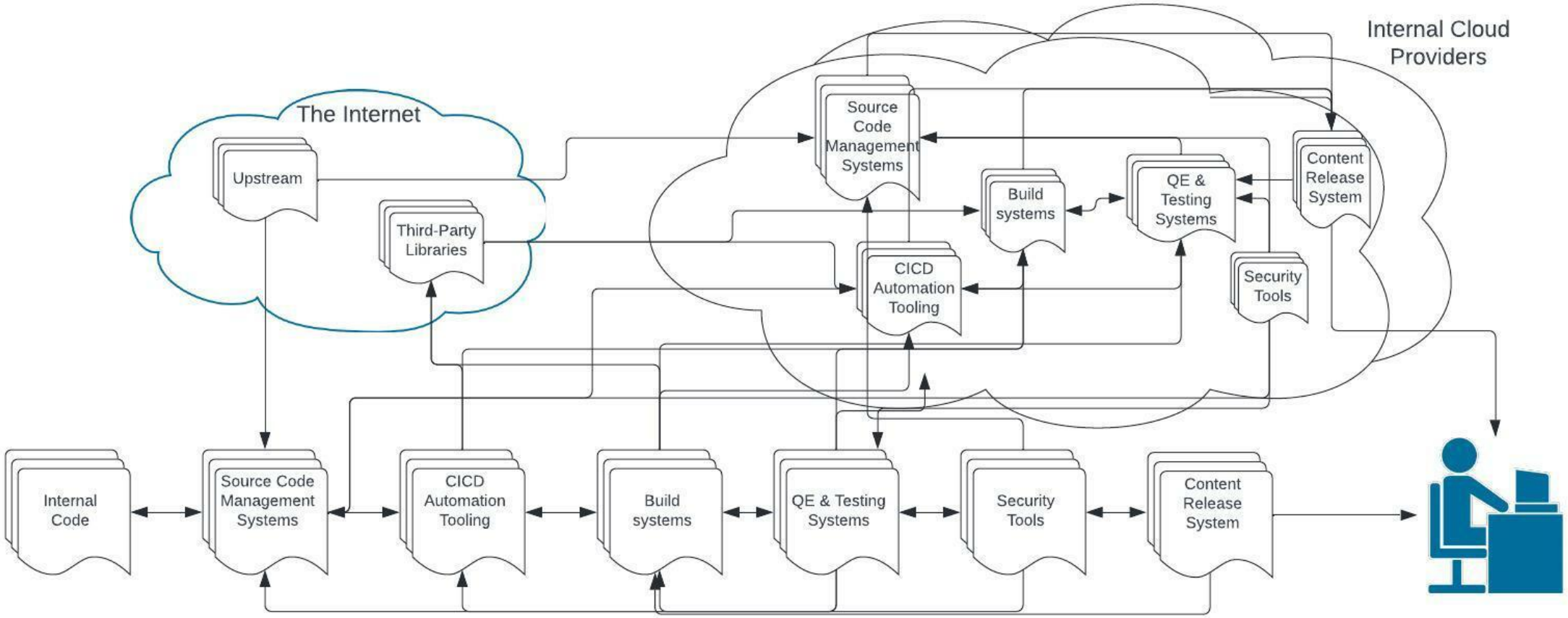


So what could go wrong?

Let's Meet Our Engineers

Red Hat
Product Security

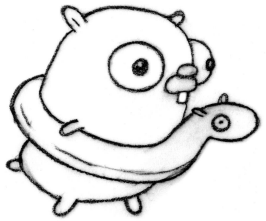
Building out the Supply Chain

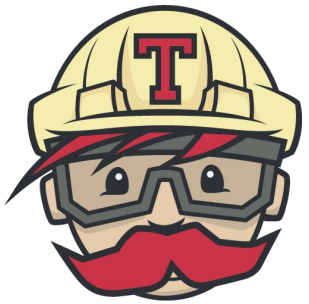


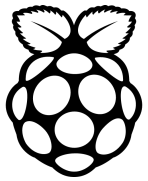
Not Drawn to Scale

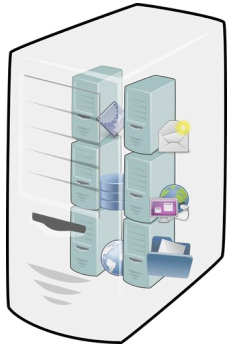
- Networking configuration
  - Regions,
  - Firewalls,
  - Cloud VPCs
  - Internal & External Networks
- Operating Systems
- User Accessibility and Permissions
- The Technical Stack
  - Libraries and Third Party
  - Vendors
  - Versions & Maintenance
  - Source Code Language

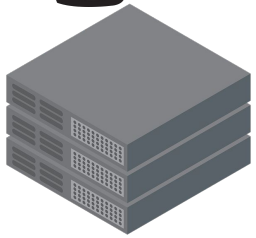
Threats, Attack Vectors, and Intelligence

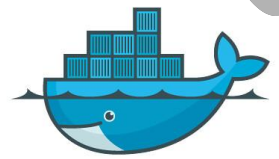


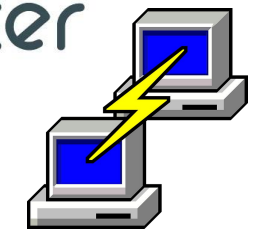








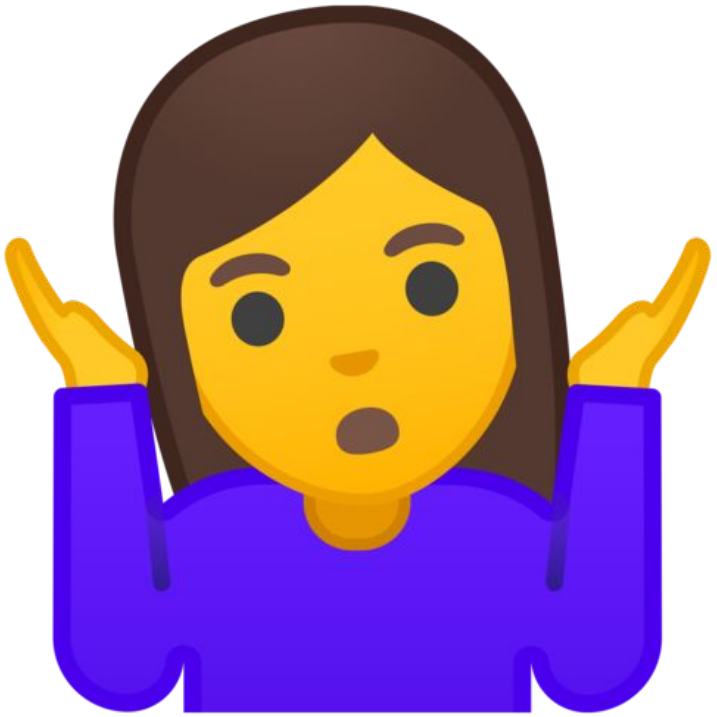




IBM Cloud

TravisCI Source

So, *what* can **YoU** do **NOW**?



First off, *What* is

Your perspective?

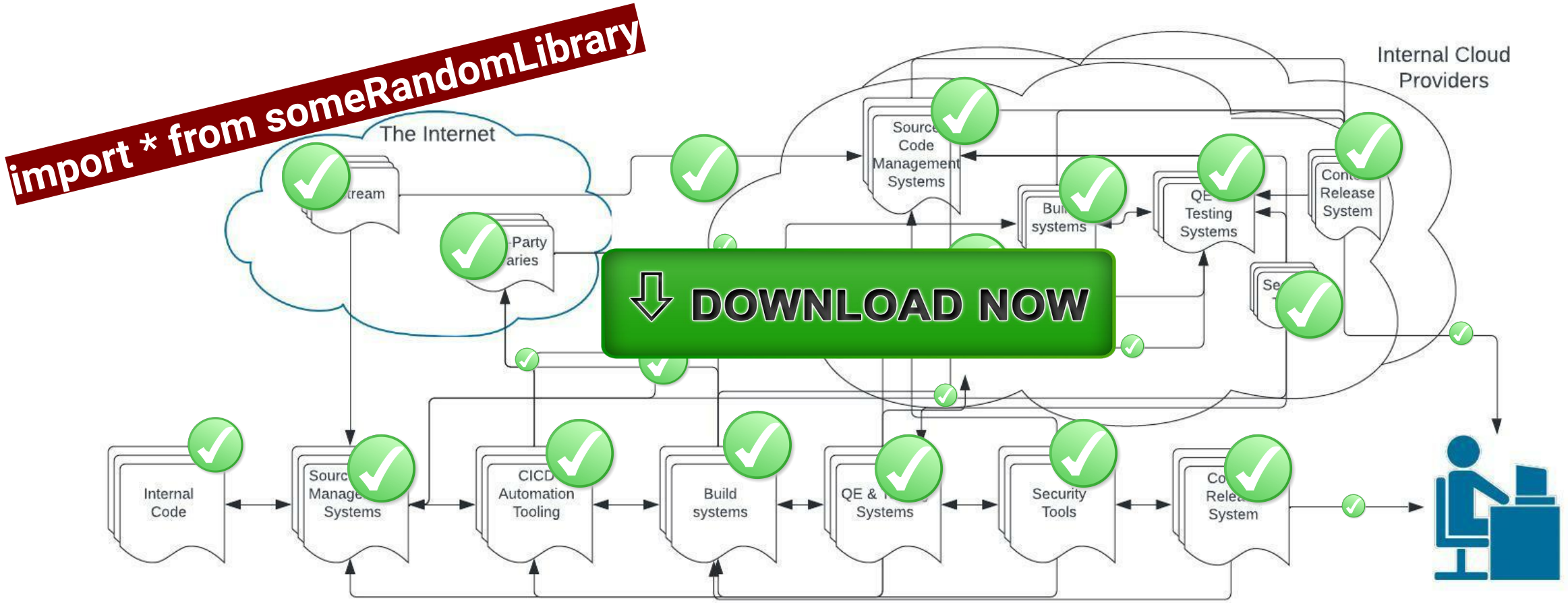
Consumer

Producer

Both?

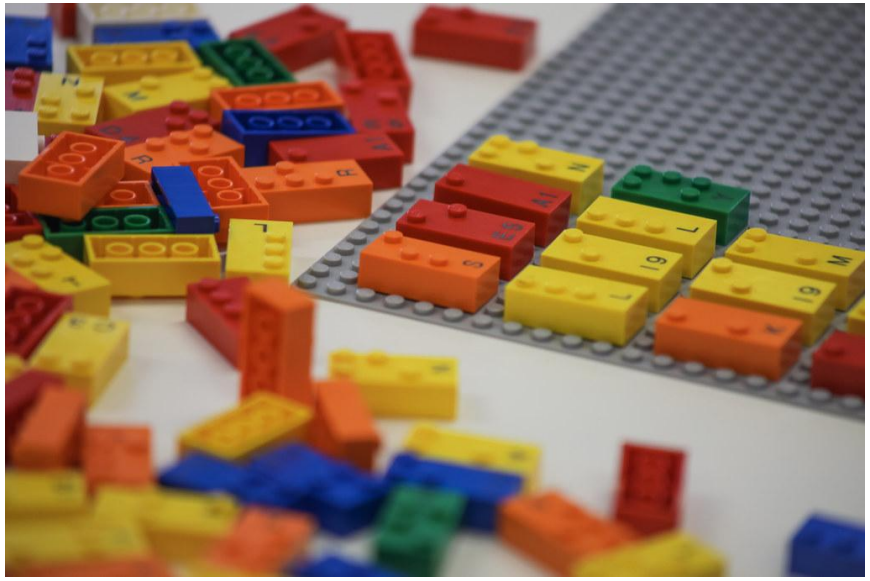
– some may think this –

– but this is **Not** how software is made –


import * from someRandomLibrary
The Internet
Party
aries
Internal Cloud
Providers
Source
Code
Management
Systems
QE
Testing
Systems
Release
System
DOWNLOAD NOW
Internal
Code
CICD
Automation
Tooling
Build
systems
Security
Tools
System

Supply Chain Security Recommendations

During **Development**



- Use Versioned **Source Code Repositories**
- Implement **Code Reviews**
- Use only **trusted** libraries/dependencies
- Use secure base images
- **Scan source code** using scanning tools (SCA, SAST)
- **Scan Base Images** using Clair
- Use an **artifactory**

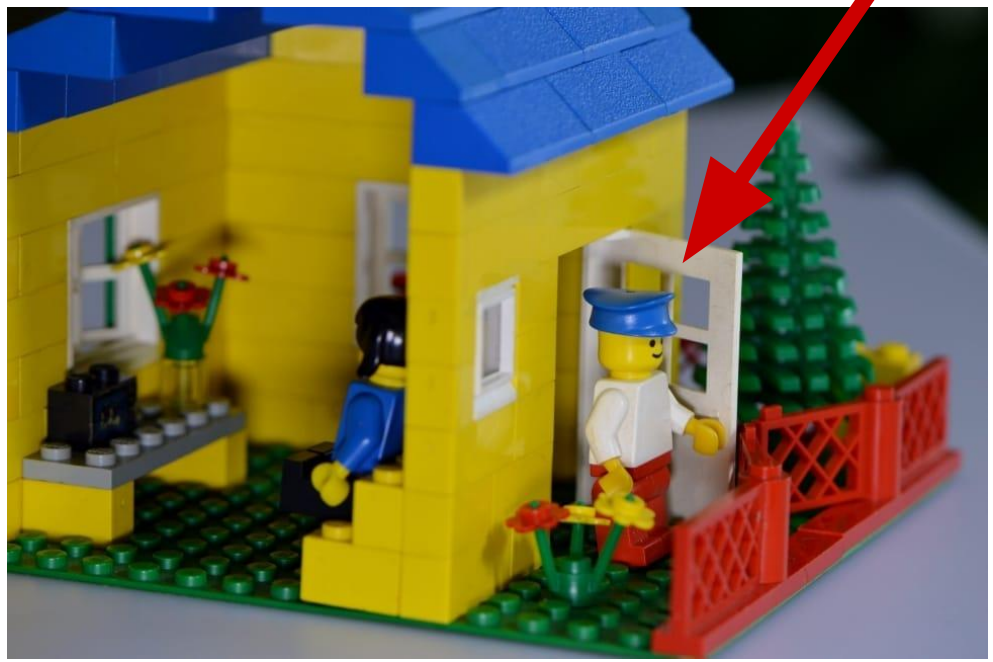
Supply Chain Security Recommendations

During **Build** Phase

- Use an **Isolated Build Service**
- **Build as Code** if possible
- **Gate** build releases if possible
- Enforce **Separation of Duties**

Supply Chain Security Recommendations

At **Delivery**

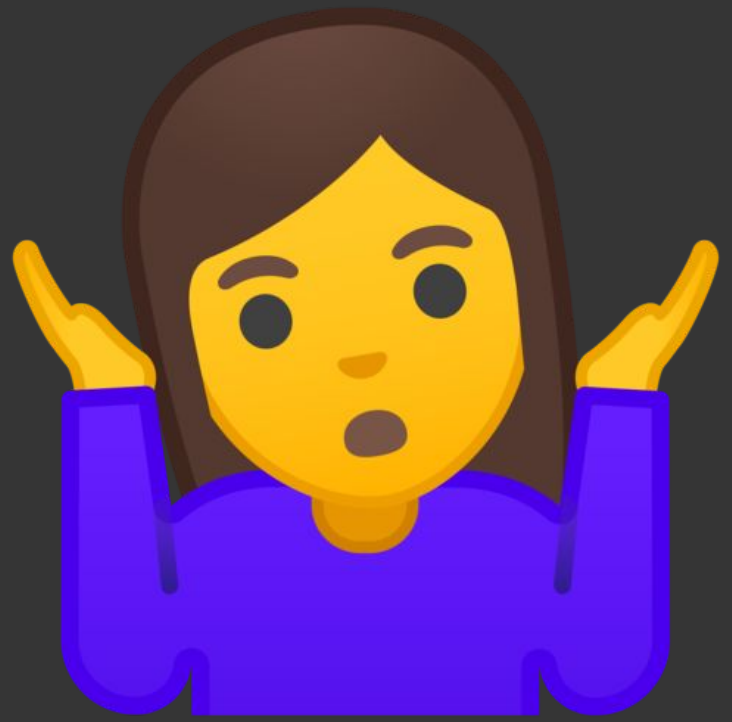


- Ensure you are providing (or receiving if the consumer) a **Provenance** for the delivered artifact that includes:
  - Includes **cryptographic hash**
  - Includes **identity**
  - May include builder, build instructions, its reproducible, non-falsifiable, source, dependencies, etc.

Supply Chain Security Recommendations and **Always**

- Enforce **Separation of Duties**
- **Inventory** every application, system, and network that is involved in your software delivery process
- Keep these **systems Updated**
- **Monitor** these systems for anomalies (antivirus/malware, enforce logging to a centralized system)
- **Limit access** to these systems and applications (implement Identity management, certificates)

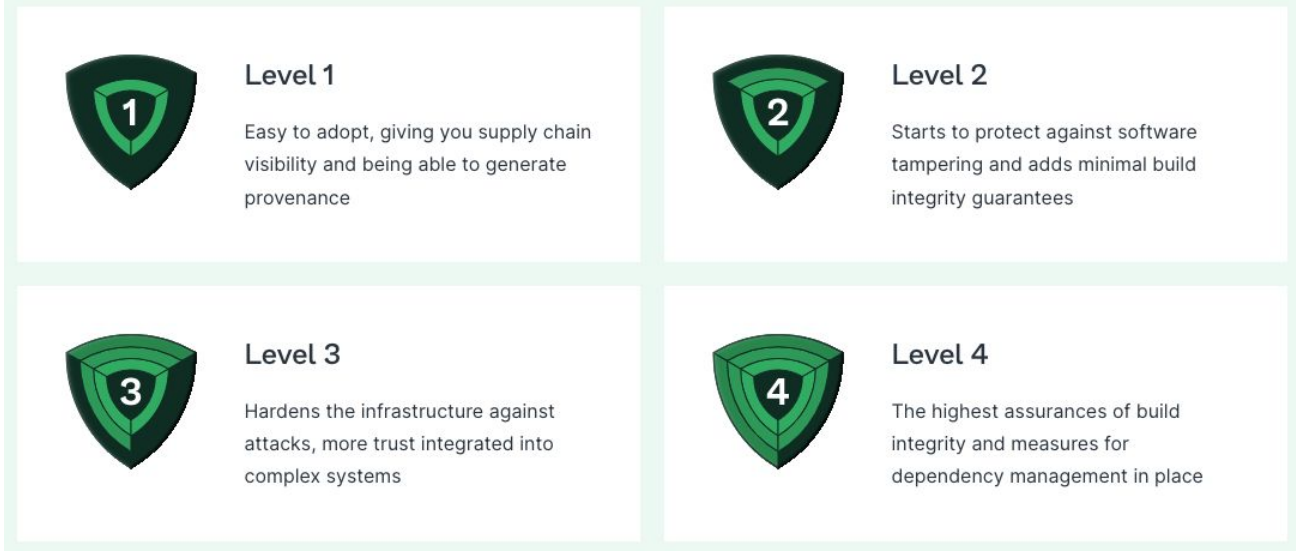
Got it…, **is there** additional **Guidance**



Supply Chain Security Frameworks

and general security guidance

- **NIST** Released Supply Chain Security Guidance [1]
- Open Source Security Foundation (**OpenSSF**) Initiative
  - Supply chain Levels for Software Artifacts (**SLSA**) [2]
- Cloud Native Computing Foundation (**CNCF**) Released a Whitepaper "Sofware Supply Chain Best Practices" [3]
- Secure Development Practices like **NIST SP 800-218** [4] Secure Software Development Framework (SSDF)
- General Network Security Practices
- Use **Red Hat** Services ;)

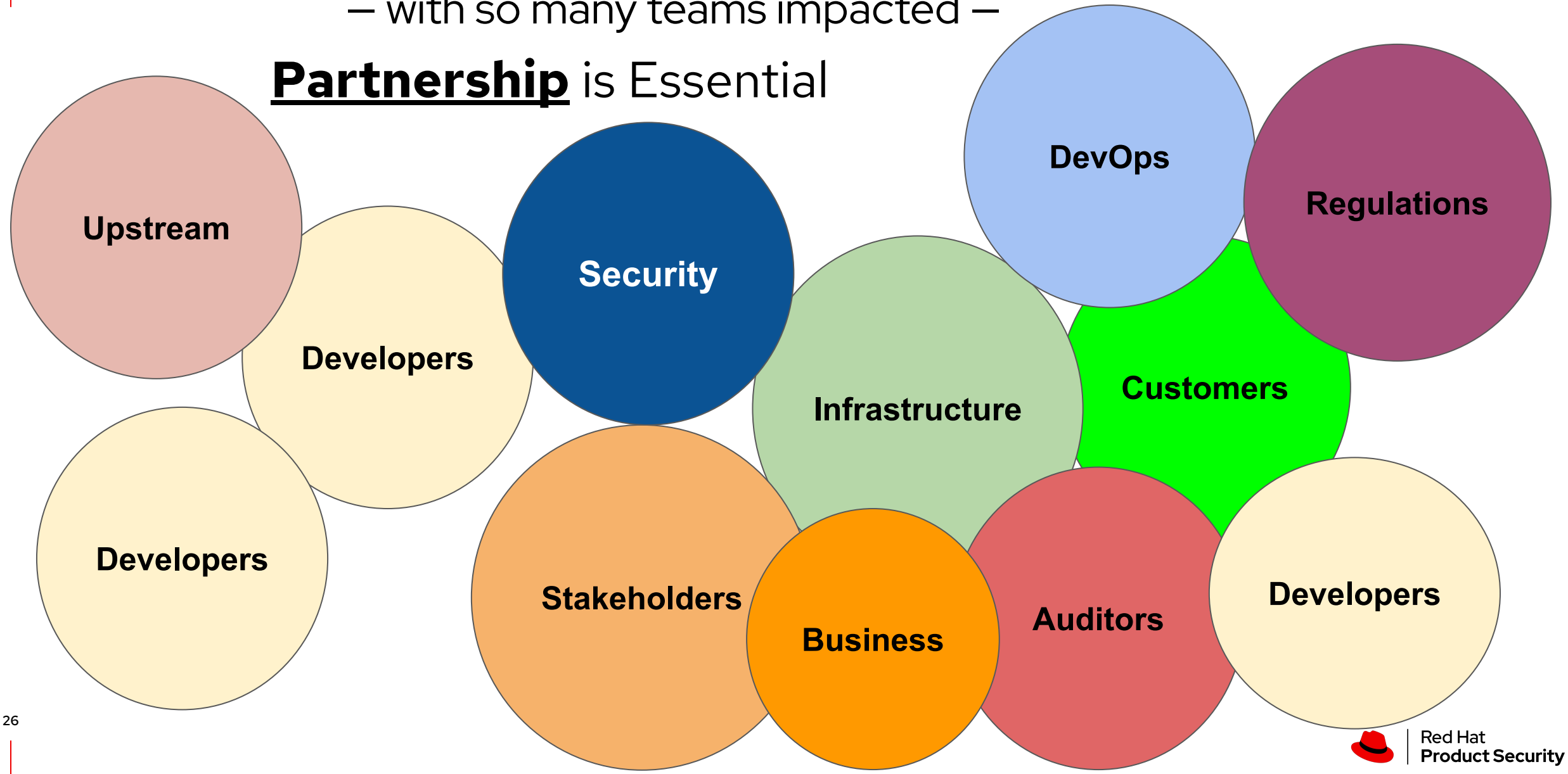


1. https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/software-supply-chain-security
2. https://slsa.dev/
3. https://github.com/cncf/tag-security/blob/main/supply-chain-security/supply-chain-security-paper/CNCF_SSCP_v1.pdf
4. https://csrc.nist.gov/publications/detail/sp/800-218/final

the **Balancing** Act of **Security**

– with so many teams impacted –

Partnership is Essential



Freedom and Accountability

We are all in this together

"Shift left with security"

"Bake security in"

...but what does that mean?

Become core to the development cycle!

Make security easy to understand

And put it in terms of Risk, not check the box security

Thank you

We believe that everyone, everywhere, is entitled to quality information needed to mitigate security and privacy risk as well as the access to do so. We strive to protect communities of customers, contributors and partners from digital security threats. We believe open source principles are the best way to achieve this.

securityblog.redhat.com

access.redhat.com/security/vulnerabilities

twitter.com/RedHatSecurity

Red Hat
Product Security