The Chain

Image Source

HELLO!

CRob, n, adj, and v

Pronunciation: U.S. (K-rowb)

43rd level Dungeon Master

26th level Securityologist

Pirate-enthusiast & hat-owner

There is an invisible chain....

You may never see it, but it binds us all together in a circle that goes around the globe, touching virtually every person.

“Listen to the wind blow, watch the sun rise.”

BIG CONCEPT

Image Source

So what the HECK *__IS__* a software supply chain?

WAT is software supply chain?

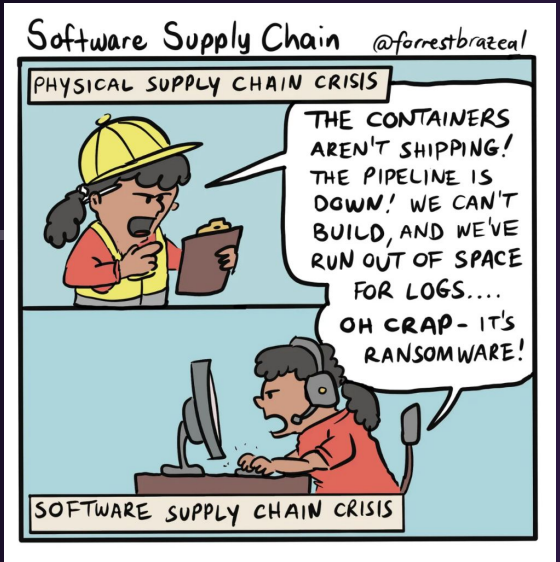


Image Source

Anything and everything that touches software spanning the whole SDLC, from development all the way to consumption and maintenance.

"Reality is a question of perspective; *the further you get from the past, the more concrete and plausible it seems – but as you approach the present, it inevitably seems incredible."*

Salman Rushdie - Midnight's Children, March 12, 1981

“I am not a supplier”

Thomas Depierre
Expert Open Source Developer

I am not a supplier

31 Dec 2022 - Thomas Depierre

For the past few years, we have seen a lot of discussions around the concept of the Software Supply Chain. These discussions started around the time of LeftPad and escalated with multiple incidents in the past few years. The problem of all the work in this domain is that it forgets a fundamental point.

Before we get there, I am going to define what is usually meant by Supply Chain and suppliers, why we are applying to software. And then why attempts at bringing FOSS under that definition are deeply misguided.

https://www.softwaremaxims.com/blog/not-a-supplier

TL/DR: Open Source Software is provided “As Is” with no warranty or support; OSS devs have no relationship with or obligation to downstream consumers

Dan Appelquist
Open Source Standards Expert

DEVSECOPS | OPEN SOURCE

When software isn’t a “supply”

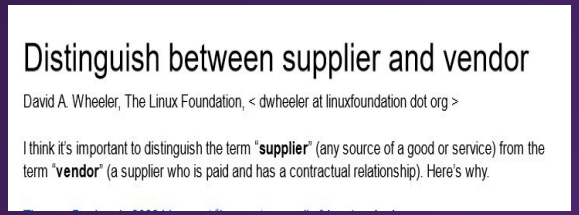
Daniel Appelquist
February 15, 2023

Editor’s note: The following think piece, written by Snyk’s Open Source and Open Standards Strategy Director, Daniel Appelquist, examines the origin of the term “supply chain security” and whether it’s a good fit for today’s open source software development process.

https://snyk.io/blog/when-software-isnt-a-supply/

TL/DR: Our words have meanings; the industry should redefine our terminology

Dr. David A. Wheeler
Prolithic Open Source Security Expert



Distinguish between supplier and vendor

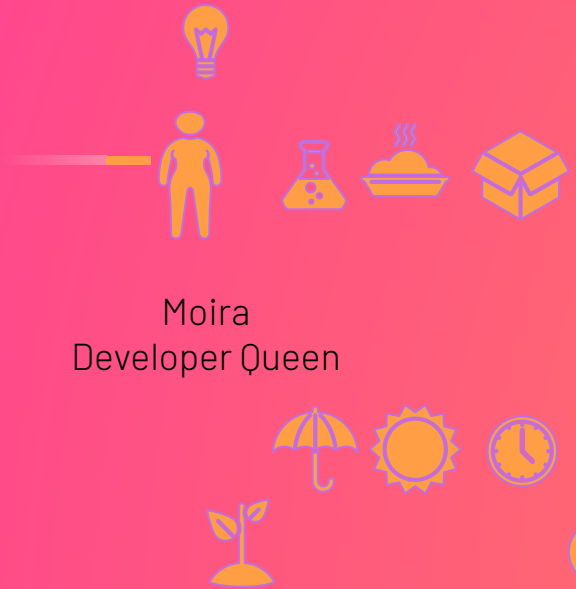
David A. Wheeler, The Linux Foundation, < dwheeler at linuxfoundation dot org >

I think it’s important to distinguish the term “**supplier**” (any source of a good or service) from the term “**vendor**” (a supplier who is paid and has a contractual relationship). Here’s why.

https://openssf.org/blog/

TL/DR: Words matter; OSS Devs ARE the “source”, but not necessarily “vendors” with contracts & obligations; there are means for consumers to get support of OSS

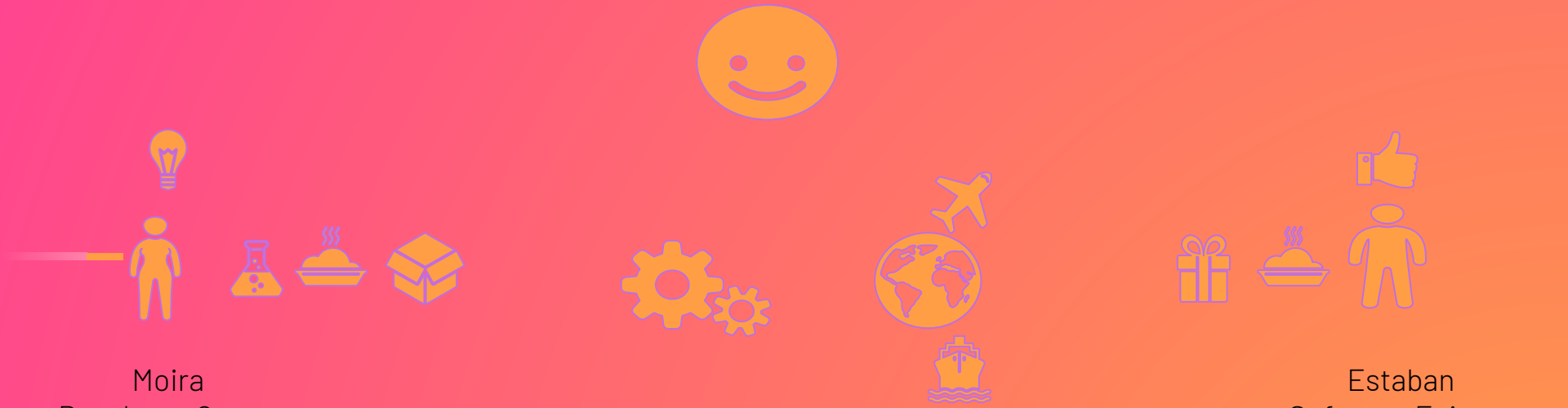
How software moves from an idea to something everyone can enjoy
a.k.a. “the software supply chain”



Moira
Developer Queen

Estaban
Software Enjoyer

How software moves from an idea to something everyone can enjoy
a.k.a. “the software supply chain”



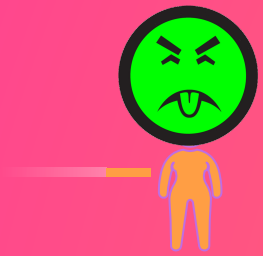
Moira
Developer Queen

Estaban
Software Enjoyer

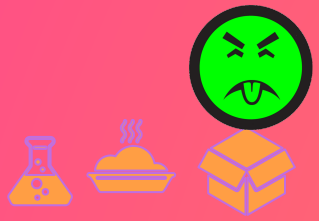
What could **possibly** go wrong?

AV-100 - Develop & Advertise Distinct Malicious Package from scratch

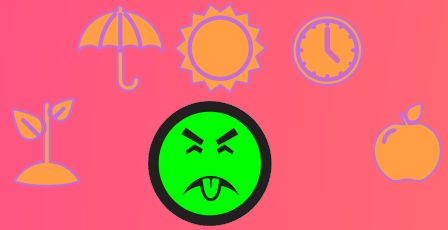
AV500 -Become the Maintainer



AV-001 -Subvert Legitimate Package



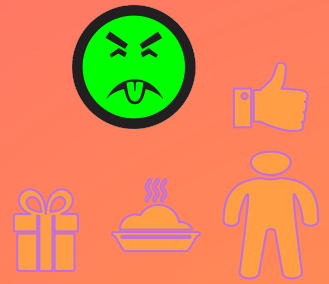
AV-302 Contribute as Maintainer
AV-700 Compromise Maintainer System



AV-200 - Create Name Confusion with Legitimate Package

AV-403 -Tamper with Exposed Build System

AV-500 -Distribute Malicious version of Legitimate Package



AV-701 Exploiting Config Vuln
Counterfeiting
AV-702 Exploiting Software Vuln

...quite a lot, actually

Source : Taxonomy of Attacks on Open-Source Software Supply Chains - https://arxiv.org/pdf/2204.04008.pdf

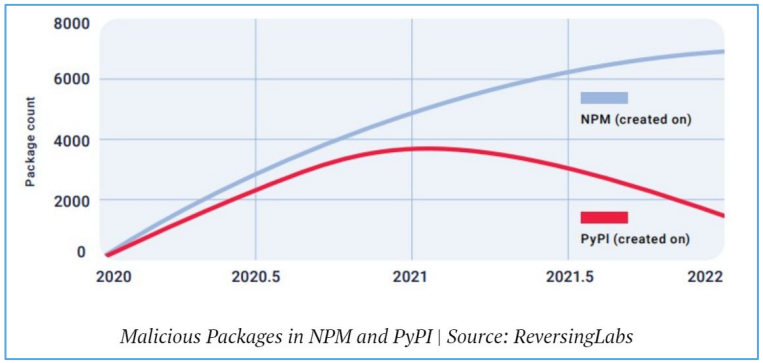
“Listen to the wind blow, down comes the night.”

Back in Days of Yore...

People did some stuff and it was “cool”

Image Source

Semi-complete-ish List of Software Supply Chain "Events" 2010-2023



Malicious Packages in NPM and PyPI | Source: ReversingLabs

Sources - Reversing Labs, Sonatype

RIPPED from the headlines

NEWS ANALYSIS

Supply chain attacks increased over 600% this year and companies are falling behind

Most companies believe they are using no open-source software libraries with known vulnerabilities, but new research finds them in 68% of selected enterprise applications.

By Lucian Constantin

CSO Senior Writer, CSO | OCT 19, 2022 12:03 PM PDT

How NPM Packages Were Used to Spread Phishing Links

Unveiling the Latest NPM Ecosystem Threat: Thousands of SPAM Packages Flood the Network, A New Discovery by Checkmarx

CSO Online Oct 19, 2022:
https://www.csoonline.com/article/3677228/supply-chain-attacks-increased-over-600-this-year-and-companies-are-falling-behind.html

Checkmarx Blog Feb 21, 2023:
https://checkmarx.com/blog/how-npm-packages-were-used-to-spread-phishing-links/

OSS Licensing “Fun Facts”

Here is a snippet from the Apache 2.0 License, which is broadly used, and very similar to other OSS licenses in these two paragraphs.

As always, your mileage varies, read the licenses for the software you consume/use for specifics.

https://www.apache.org/licenses/LICENSE-2.0

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

“But I don’t use open source”

...*sure* you don’t

Heartbleed

April 2014 - Popular open Source cryptographic library. OpenSSL is “just “ used in over 12mil public websites
https://trends.builtwith.com/Server/OpenSSL

Solarwinds

2019 - Solarwinds Orion is a commercial monitoring package. Approx 18k customers downloaded malicious Sunburst package as part of a routine update. SW Used *compromised OSS package* TeamCity to build their software, which injected the malicious code into packages later signed by S.W.
https://www.wired.com/story/the-untold-story-of-solarwinds-the-boldest-supply-chain-hack-ever/

log4shell

Nov 2021 - Popular open source logging package log4j, more widely used than most realized...until the exploit was publicly disclosed.
https://www.wired.com/story/log4j-log4shell-one-year-later/

How do you solve a problem like “software supply chain”?

- Open Source Software is in as much as 96% of the software used within Enterprises (1)
- The **majority** of OSS are single-maintainer projects (2)
- Devs have varied reasons to write and share their software (3) **YOUR** compliance is not one of them

Image Source

1.) Synopsys
2.) Anchore
3.) Linux Foundation

There are many motivations/reasons OSS supply chains are tampered with

Semi-Benign

Curiosity/learning

Made a Mistake

Lack of tooling or controls

Unknown/unexpected dependencies/downstream

Dev retires/quits project

Non-Benign

Hacktivism

Espionage

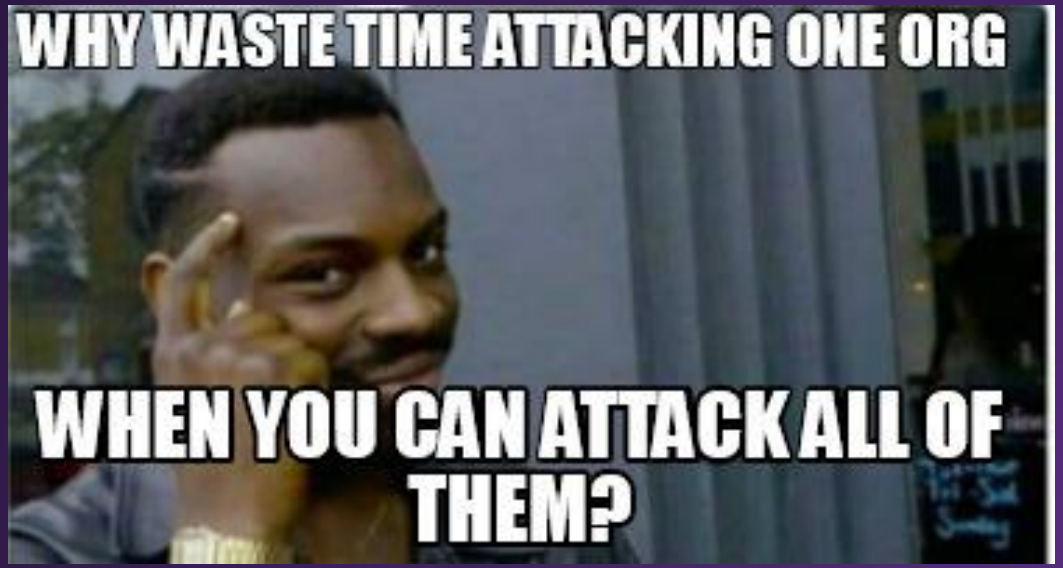
Political Motivation

...

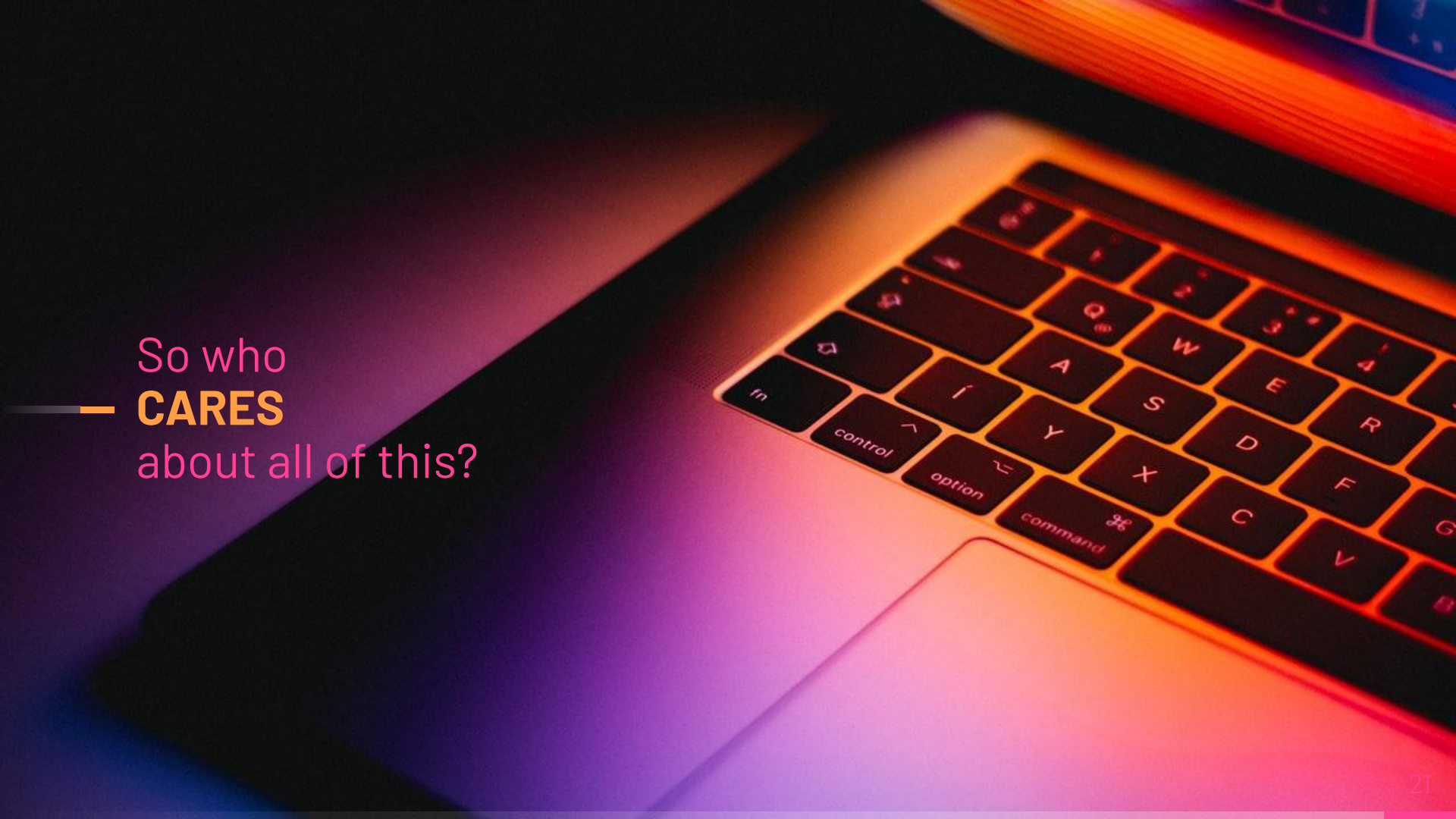
Profit

Why attack just one organization

When you literally can attack
THOUSANDS at once?



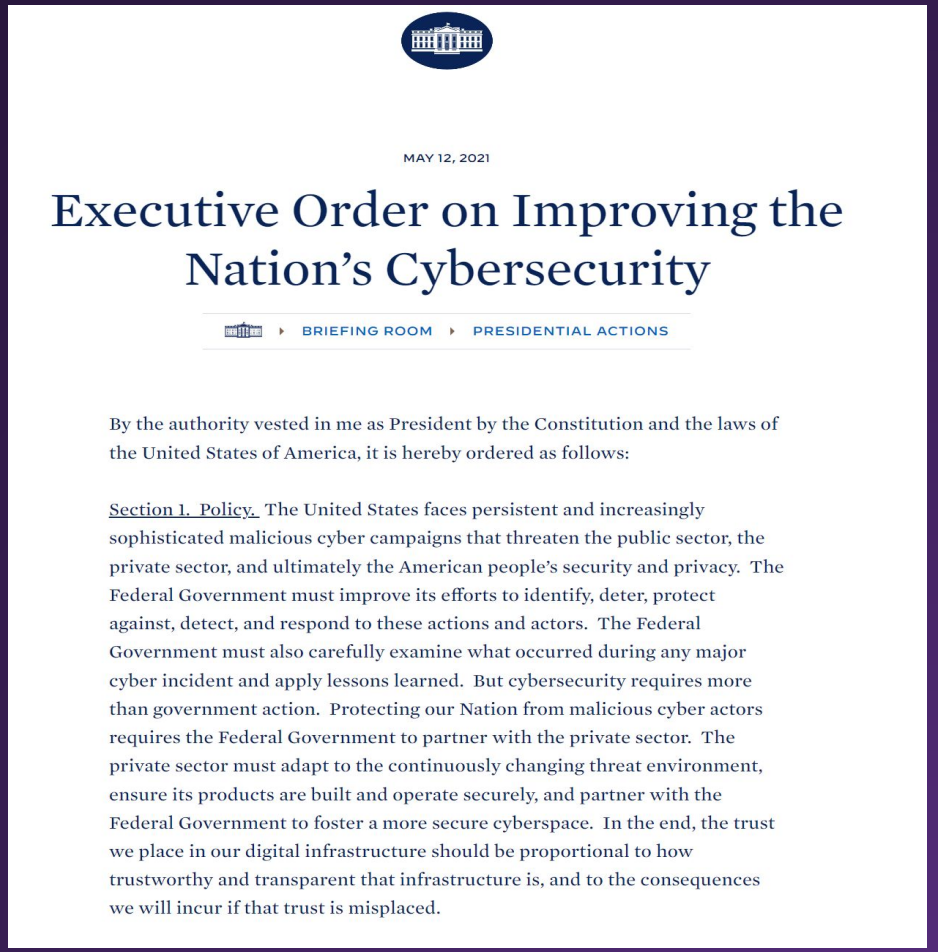
Source - https://memecreator.org/meme/why-waste-time-attacking-one-org-when-you-can-attack-all-of-them


So who
CARES
about all of this?

WH EO 14028

In May of 2021 and followed-up in January of 2022, the U.S. White House issued guidance for improving cybersecurity.

It speaks **directly** to software supply chain, software bill of materials, and secure software development practices



MAY 12, 2021

Executive Order on Improving the Nation's Cybersecurity

BRIEFING ROOM ▸ PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced.

Want to learn more?
https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/

This is an issue of GLOBAL concern

EU - ENISA Threat Landscape for Supply Chain Attacks, Cyber Resilience Act (CRA)

Germany – The Law on the Federal Office for Information Security (BSIG) was updated in 2021 and aligns closely with the EU's Cyber Resiliency Act.

ASEAN – the Association of Southeast Asian Nations (ASEAN) ten members are targeting 2025 for a set of regulations addressing cybersecurity to be made available.

Japan – Draft Law Concerning Promotion of Ensuring Security through Integrated Economic Measures that narrowly focuses on security-sensitive sectors (energy, water supply, information technology, finance, transportation, etc) procurING overseas software.

Source: Activestate

Collectively, these mandate things like...

- Transparency & Reporting cybersecurity incidents & vulnerabilities
- Produce Software Bill of Materials (SBOM)
- Evaluate security practices of developers and within supply chains
- Suppliers must look for and remediate known vulnerabilities
- Education and standards around cyber and development security

What's Up With That?

Image Source

- **SBOM – Software Bill of Materials –** an electronic manifest of all the components in a given piece of software
- **SDLC – Software Development Lifecycle –** mature, phased process for developing software
- **SSDF – Secure Software Development Framework** - US NIST guidance on how software lifecycles should be managed
- **CVD – Coordinated Vulnerability Disclosure –** Practice of disclosing security bugs to affected parties in a managed manner
- **VEX – Vulnerability EXchange –** security advisory format that allows maintainers to express the affectedness of their software to a security issue

“I can still hear you saying

You would never break the chain.”

So is *anyone* DOING anything about this?

A wise man once said:

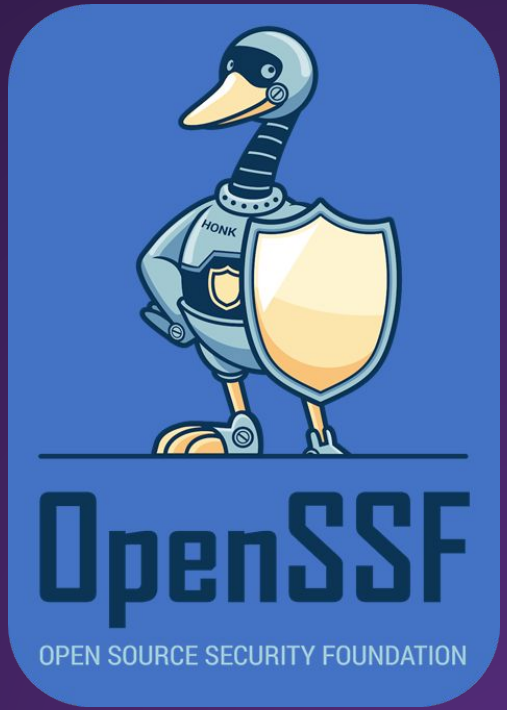
"I've found it is the small things, everyday deeds of ordinary folk that keeps the darkness at bay.

Even the smallest person can change the course of the future."

Image Source

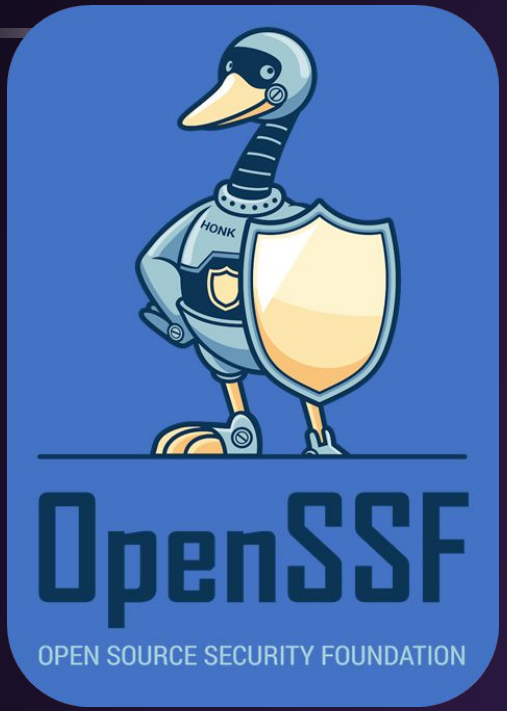
The Rising Tide lifting all boats

- The OpenSSF is a cross-industry collaboration that brings together leaders to improve the security of open source software (OSS) by building a broader community, targeted initiatives, and best practices
- The OpenSSF brings together open source security initiatives under one foundation to accelerate work through cross-industry support. This is beginning with the Core Infrastructure Initiative and the Open Source Security Coalition, and will include new working groups that address vulnerability disclosures, security tooling and more.
- OpenSSF is committed to collaboration and working both upstream and with existing communities to advance open source security for all.



https://openssf.org/

A Gaggle of Geese!

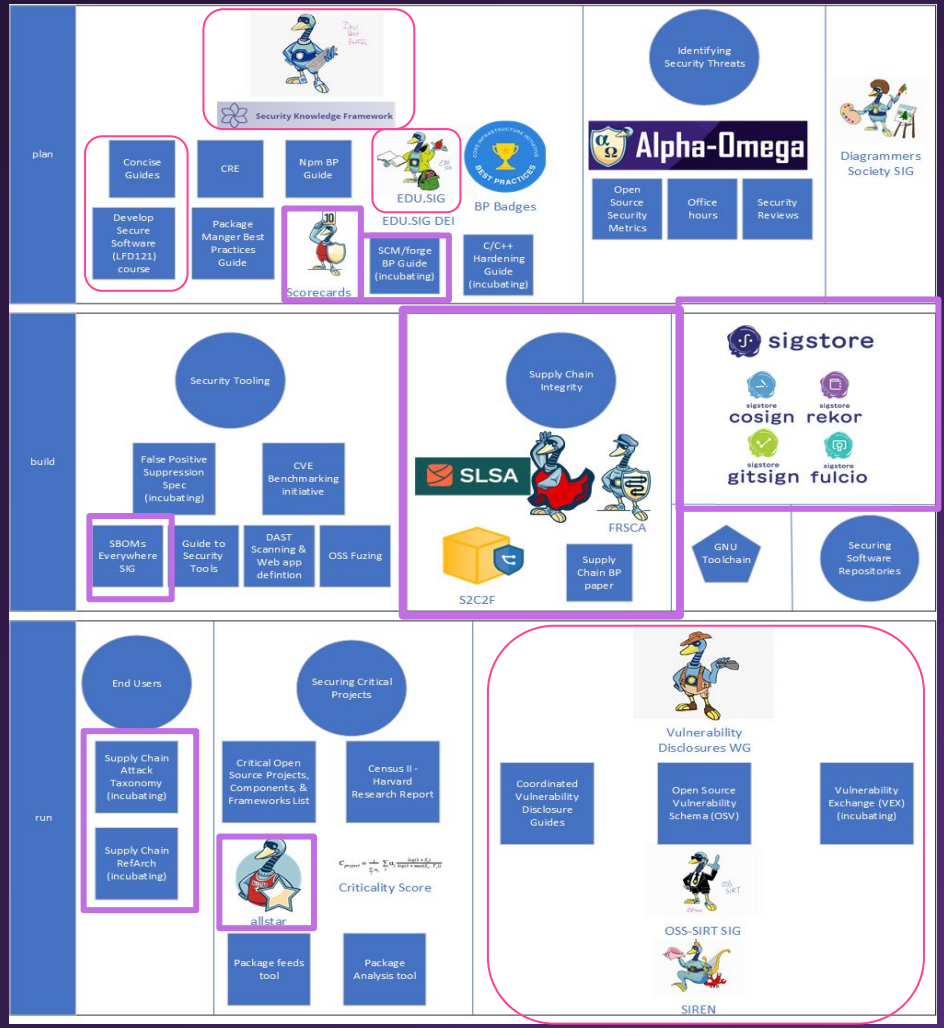


I'm focused on Supply chain!

I'm focused on appsec/SDLC or CVD!

https://openssf.org/community/openssf-working-groups/

What's up with all the Geese?



Projects focused on OSS Supply Chain

SLSA - Supply Chain Levels for Software Artifacts

SLSA (pronounced "salsa") is a security framework from source to service, giving anyone working with software a common language for increasing levels of software security and supply chain integrity. It's how you get from safe enough to being as resilient as possible, at any link in the chain.

https://github.com/slsa-framework/slsa

S2C2F - Secure Supply Chain Consumption Framework

Outlines and defines how to securely consume Open Source Software (OSS) dependencies into the developer's workflow

https://github.com/ossf/s2c2f

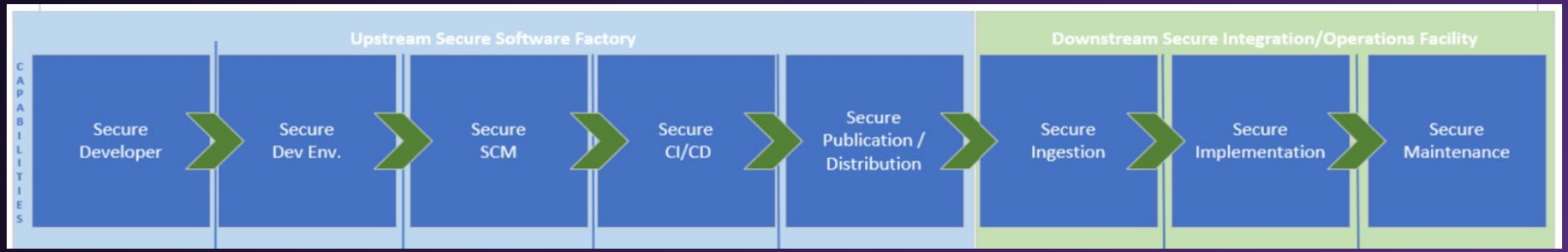
Scorecard

An automated tool that assesses important heuristics ("checks") associated with software security and assigns each check a score of 0-10. Helps to assess the risks that dependencies introduce, and make informed decisions about accepting these risks, evaluating alternative solutions, or working with the maintainers to make improvements.

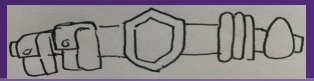
https://github.com/ossf/scorecard

A world where every software package is verifiably trustworthy

The OpenSSF's Security Toolbelt project seeks to tie together people, process, & technology into an understandable reference for all participants within the OSS Supply Chain on how they can implement security practices and tools into the software they make, provide, and consume.



https://github.com/ossf/Diagrammers-Society/tree/main/SecurityToolbelt



Regulatory & Compliance concerns…

SSDF attestation

You may not work for the .gov, but that doesn't mean you can't benefit from their requirements **AND** be held to their standards

https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/software-supply-chain-security-guidance-1

SBOM, SBOM, SBOM

CISA, ENISA, UK's NCSC, AU's ACSC, CA's CSE, or ISO (just to name a few) are recommending suppliers provide them, but once you've got them… what do you ***DO*** with them? And LAWS like the CRA will be making their use mandatory

https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf

https://www.isaca.org/resources/news-and-trends/industry-news/2023/why-are-regulations-demanding-sbom-adoption

Ripples of the EU's CRA

Focused on protecting EU citizens' cyber-health, the CRA will have global effects as OSS developers, suppliers, and foundations (aka "manufacturers") determine their new legal liabilities and obligations, and possibly pull out of supporting OSS

https://techcrunch.com/2023/04/18/in-letter-to-european-commission-open-source-bodies-say-cyber-resilience-act-could-have-chilling-effect-on-software-development/

https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

Calls to Action

Understand YOUR chains

- Where do you get your software?
- Who is your downstream that depends on YOU?
- How secure are your suppliers and how secure are YOU?

Secure your chains

- Take steps to ensure you're providing Due Care and taking the right steps to secure the software you consume and produce
- Understand your obligations in the evolving global compliance landscape

Contribute to securing the ecosystem

- Join a WG or SIG: contribute your expertise and make things better for EVERYONE!
- Take secure development classes and follow industry BEST practices
- Use secure tools and techniques to help bolster your downstreams

The Open Source Consumption Manifesto

“Chain keep us together.”

AWESOME RESOURCES

The Open Source Security Foundation

https://www.openssf.org

The Confidential Computing Consortium

https://confidentialcomputing.io

The Cloud Native Foundation

https://www.cncf.io

open.intel

https://www.intel.com/content/www/us/en/developer/topic-technology/open/overview.html

“The Chain” Lyrics by Fleetwood Mac

https://g.co/kgs/P85zUu

Image Source

Thanks!

CRob_at_Intel_dot_com

@SecurityCRob

@SecurityCRob@infosec.exchange

https://github.com/SecurityCRob

The Security Unhappy Hour,
Chips & Salsa

https://www.linkedin.com/in/darthcrob/

CREDITS

Special thanks to all the people who made and released these awesome resources for free:

- Presentation template by SlidesCarnival
- Photographs by Unsplash
- Illustrations by Pixsellz

PRESENTATION DESIGN

This presentation uses the following typographies:

- Titles: Barlow Bold
- Body copy: Barlow Light

Download for free at:
https://www.fontsquirrel.com/fonts/barlow