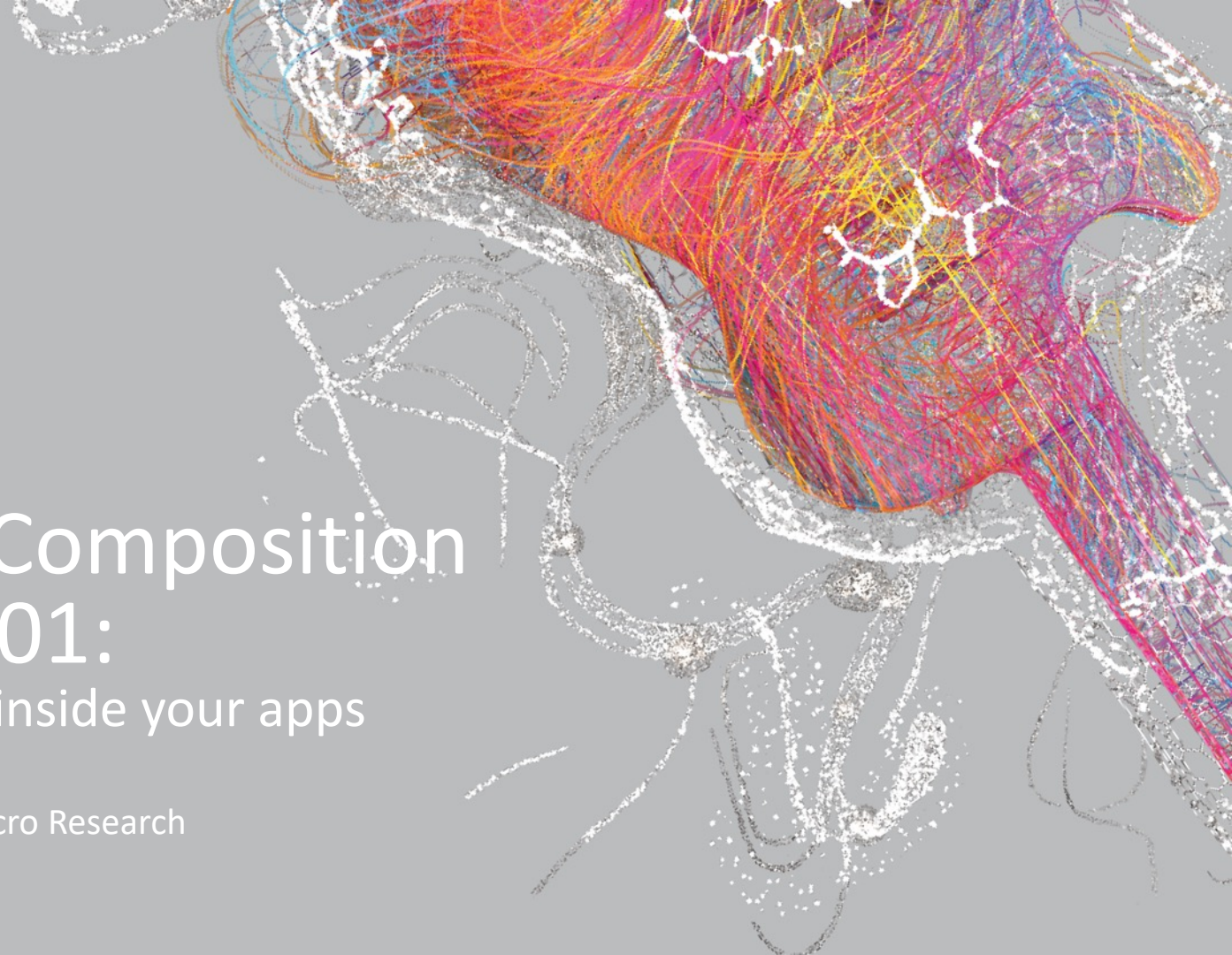


Software Composition Analysis 101:

Knowing what's inside your apps

Magno Logan - Trend Micro Research

@magnologan

- Information Security Specialist @ Trend Micro
- AppSec and DevSecOps Practitioner
- Working with AppSec since 2011
- Deployed multiple SAST, DAST and SCA tools
- Personal blog: katanasec.com

Agenda

- What is SCA, BOM and SBOM?
- Why should I worry?
- Supply Chain Attacks
- SCA Best Practices
- SCA Tools

SCA 101

- Software Composition Analysis
- Aka Library Analysis, 3rd Party Dependency or Open Source Security
- Aimed at providing open source software with governance, security and provenance
- Focuses on the Software Bill of Materials

SCA 101

- Application Manifest - gives instructions on how the software should work
- Dependency Metadata - the metadata related to the dependencies in the code
- Vulnerability Data Sources - database of vulnerability information (private or public)

What's a Bill of Materials?

Bill of Materials JOB: _____ NAME: Abs Chan

ITEM	MANUFACTURER	MODEL	SUPPLIER	UNIT PRICE	QUANTITY REQUIRED	EXTENDED PRICE
Dryer	Maytag	MMEDE500WR	Home Depot	$1198	1	$1198
Washer	Maytag	MHWE450WR	Home Depot	$1198	1	$1198
Stove	Electrolux	22362987310	Sears	$3699.99	1	$3699.99
Toilet	Kohler	K-3386-96	Home Depot	$578.71	3	$1736.13
Tub(M)	Maax	423 095 116 10	Sears	$1149.99	1	$1149.99
Tub(B)	Maax	42209565610	Sears	$999.99	1	$999.99
Washroom Sink(M)	Acri-tec	364719	Home Depot	$182.88	1	$182.88
Washroom Sink(B and P)	American Standard	0419444SG.020	Home Depot	$97.98	2	$195.96
Vanity(M)	Bellini	42179600410	Sears	$339.99	1	$339.99
Vanity(B)	Pegasus	ARAA3734	Home Depot	$792.99	1	$792.99
Vanity(P)	Pegasus	GAEA3622	Home Depot	$708.26	1	$708.26
Kitchen Sink	Blanco	400843	Home Depot	$699	1	$699
Lights(L)	N/A	103803(White)	Sears	$119.99	2	$239.98
Tiles(K)	Mona Serra Ceramique	84665204	Rona	$29.90	66	$1973.40
Shower Head(M)	Aquadis	42309301910	Sears	$199.99	1	$199.99
Shower Door	Maax	42209566610	Sears	$389.99	1	$389.99
Light(M)	IKEA	365+ UTKIK	IKEA	$39.99	1	$39.99
Lights	IKEA	CALYPSO	IKEA	$34.99	6	$209.94
Washroom Light(M, B, and P)	IKEA	GODMORGON	IKEA	$69.99	3	$209.97
Page 1 of 1					Subtotal	$16164.44
					HST	$2010.38
					TOTAL	$18174.82

Software Bill of Materials (SBOM)

- List of componentes in a piece of software
- Software is usually made of open source and sometimes commercial components
- Describes the components in a product
- Similar to a ingredients list for packaged food

SBOM Resources

CycloneDX joins OWASP as a flagship project

Andrew van der Stock

Friday, June 11, 2021

https://owasp.org/executive/director/2021/06/11/cyclonedx-joins-owasp.html

- CycloneDX - lightweight software bill of materials (SBOM) standard
- SPDX - An open standard for communicating software bill of material information
- Dependency Track - allows organizations to identify and reduce risk in the software supply chain

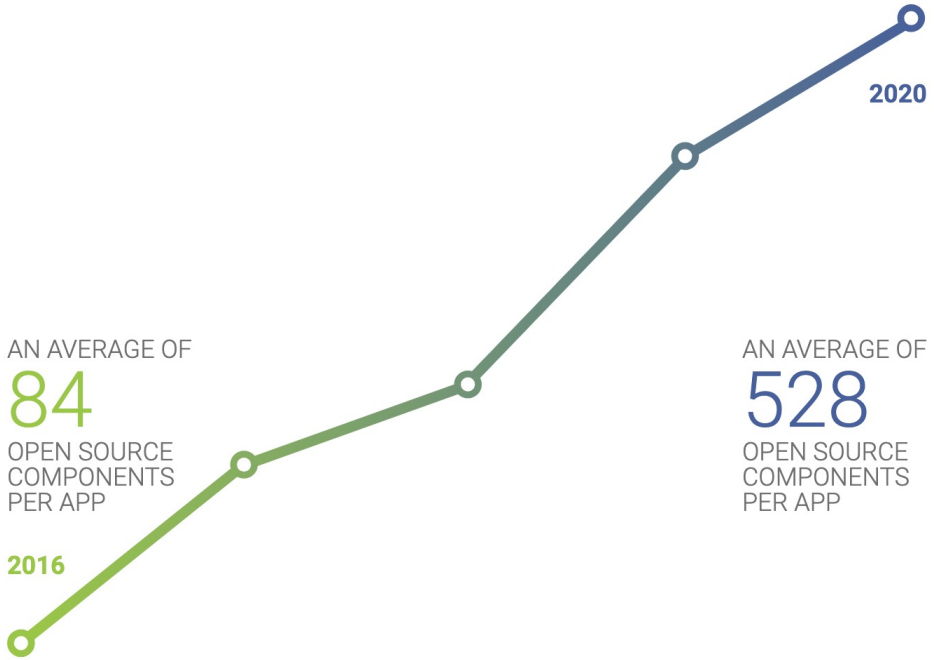
Why should I worry?

84%

OF CODEBASES
HAD AT LEAST ONE
VULNERABILITY
WITH AN AVERAGE OF

158

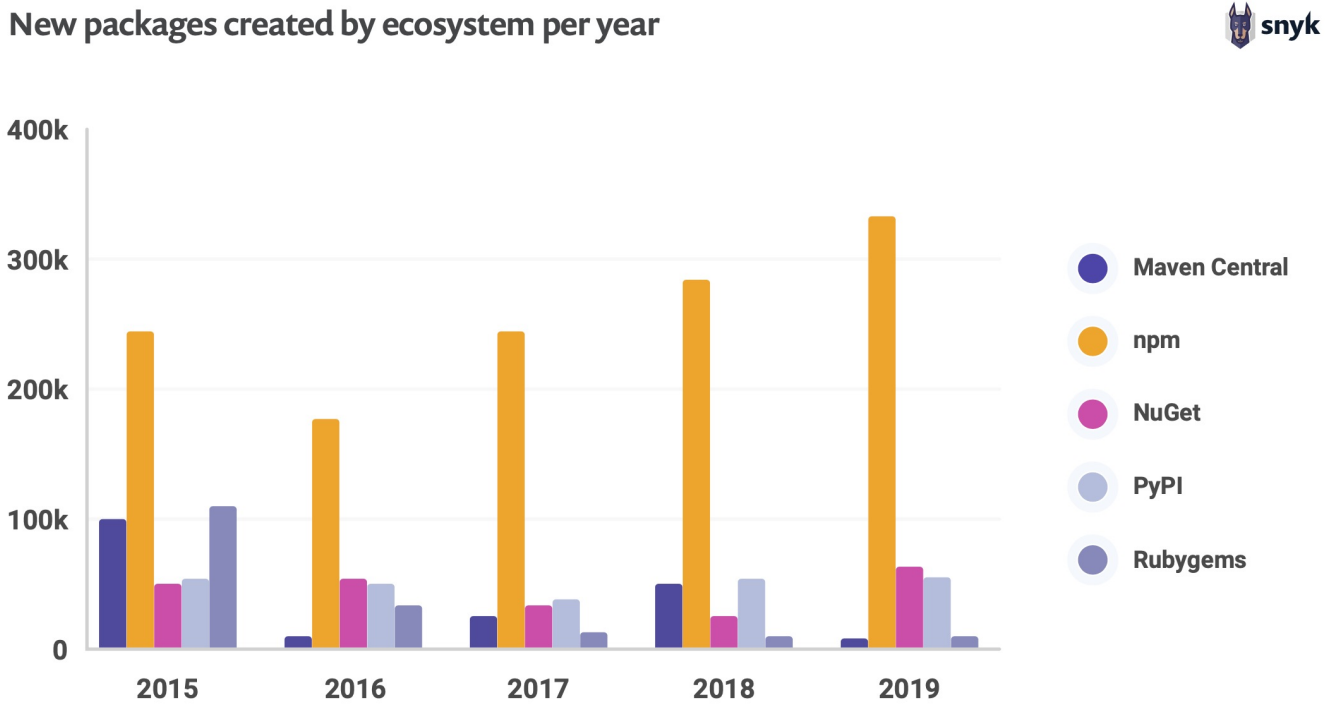
PER CODEBASE



https://synopsys.com/software-integrity/resources/analyst-reports/open-source-security-risk-analysis.html

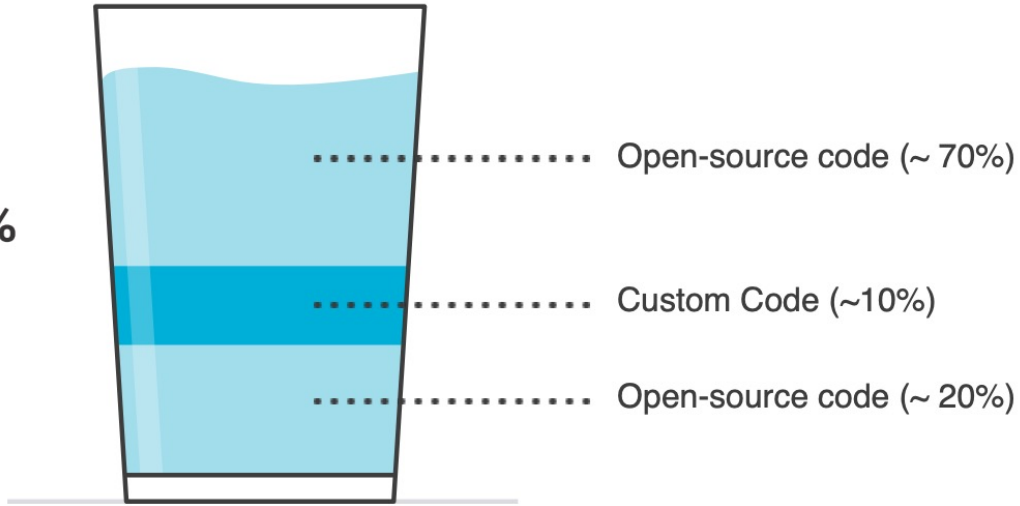
TREND MICRO

State of Open Source Security Report



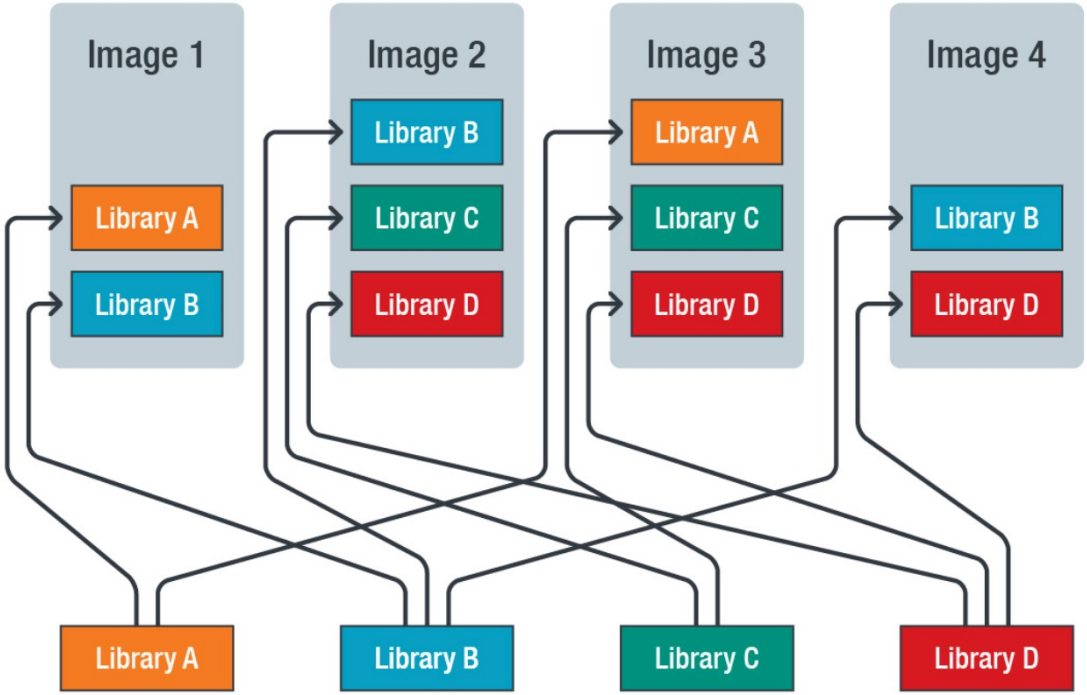
The Code Cocktail

Open Source = ~ 90%



Finding Vulnerabilities and Malware in Open-Source Code at Scale

Direct x Indirect Dependencies

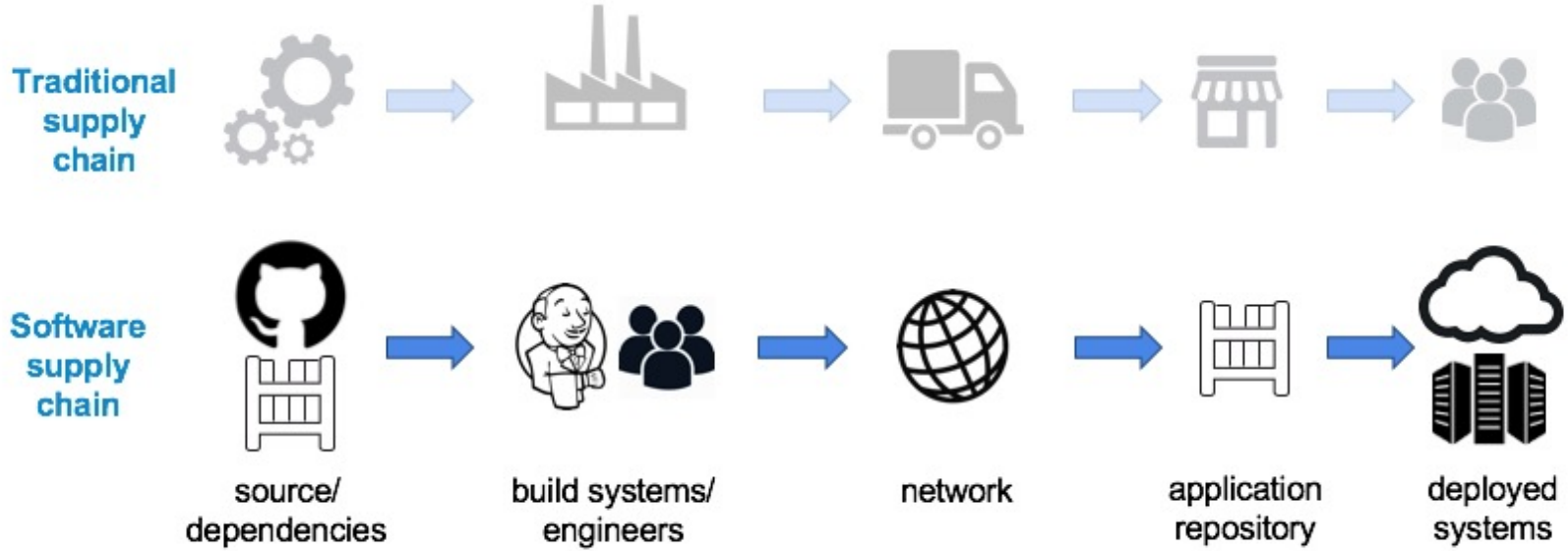


https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/guidance-on-kubernetes-threat-modeling

The OWASP Top 10 – A9:2017

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

Software Supply Chain x Traditional



https://blog.convisoappsec.com/en/is-your-software-supply-chain-secure/

Catalog of Supply Chain Compromises

Name	Year	Type of compromise
Homebrew	2021	Dev Tooling
Codecov	2021	Source Code
VSCode GitHub	2021	Dev Tooling
SUNBURST/SUNSPOT/Solarigate	2020	Publishing Infrastructure
The Great Suspender	2020	Malicious Maintainer
Abusing misconfigured SonarQube applications	2020	Dev Tooling
Octopus Scanner	2020	Dev Tooling
NPM reverse shells and data mining	2020	Dev Tooling
Webmin backdoor	2019	Dev Tooling
purescript-npm	2019	Source Code
electron-native-notify	2019	Source Code
ShadowHammer	2019	Multiple steps
PEAR Breach	2019	Publishing Infrastructure
The event-stream vulnerability	2018	Malicious Maintainer
Dofoil	2018	Publishing Infrastructure
Operation Red	2018	Publishing Infrastructure
Gentoo Incident	2018	Source Code
Unnamed Maker	2018	Publishing Infrastructure
Colourama	2018	Negligence
Foxif/CCleaner	2017	Publishing Infrastructure
HandBrake	2017	Publishing Infrastructure

https://github.com/cncf/tag-security/tree/main/supply-chain-security/compromises

Software Supply Chain Whitepaper

Table of Contents

Software Supply Chain Best Practices

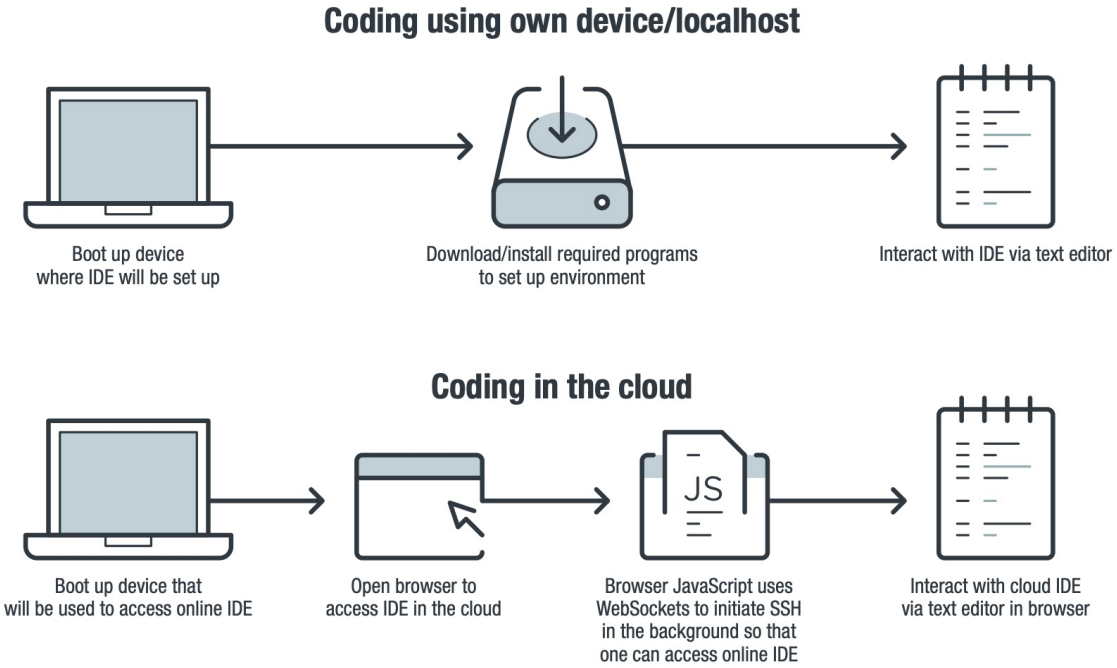
GITHUB.COM/CNCF/TAG-SECURITY

CLOUD NATIVE COMPUTING FOUNDATION

https://github.com/cncf/tag-security/blob/main/supply-chain-security/supply-chain-security-paper/CNCF_SSCP_v1.pdf

TREND MICRO

Supply Chain Attacks in the Age of Cloud Computing



https://www.trendmicro.com/vinfo/in/security/news/virtualization-and-cloud/supply-chain-attacks-cloud-computing

US Executive Order

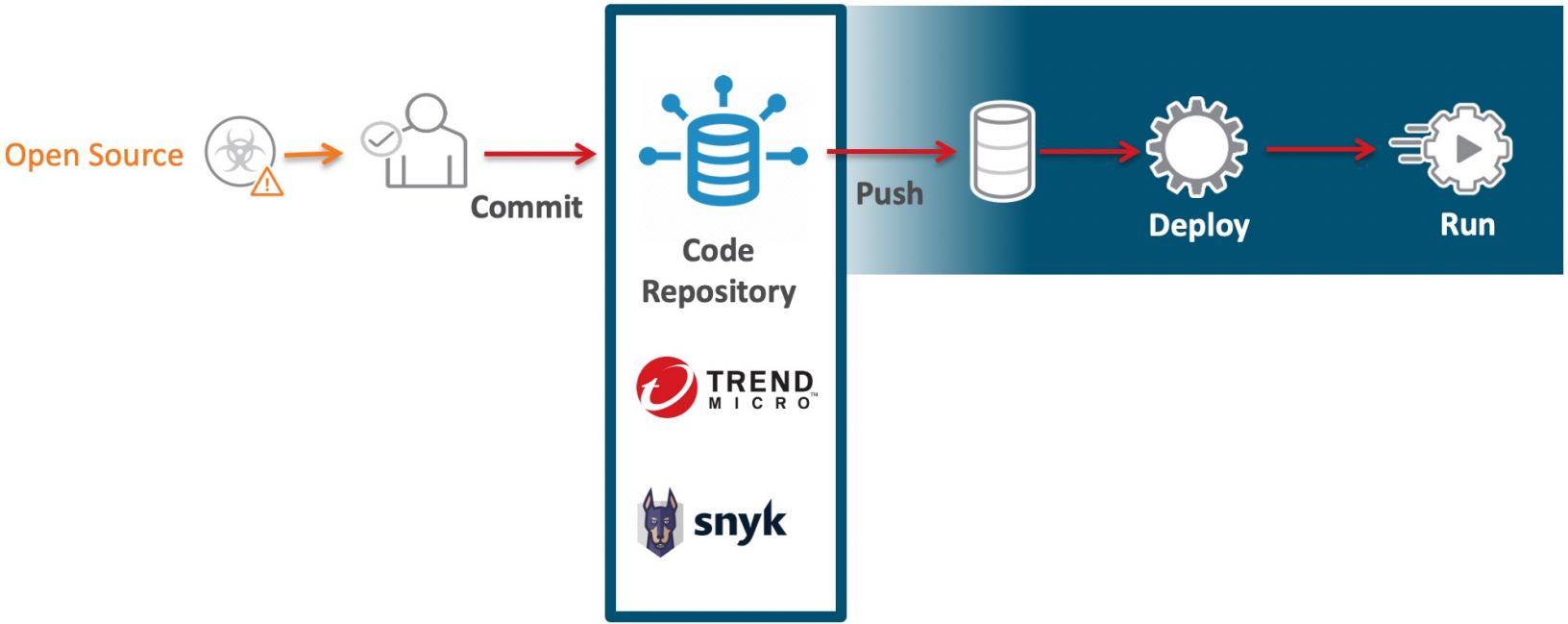
- Published on May 12th 2021
- Sec. 4. - Enhancing Software Supply Chain Security
  - (vi) Maintain accurate and up-to-date data, provenance of software code or components and controls on internal and third-party software (…)

https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

SCA Tools

- OWASP Dependency Check (Free)
- Retire.js (Free)
- Snyk (Free for Open Source)
- Open Source Security by Trend Micro
- Veracode SCA
- Synopsys BlackDuck

Demo Time!



THANK YOU AND HAPPY HACKING!

References

- https://owasp.org/www-project-top-ten/2017/A9_2017-Using_Components_with_Known_Vulnerabilities
- https://gsec.hitb.org/materials/sg2017/KEYNOTE%201%20-%20Mark%20Curphey%20-%20Finding%20Vulnerabilities%20and%20Malware%20in%20Open-Source%20Code%20at%20Scale.pdf
- https://cheatsheetseries.owasp.org/cheatsheets/Vulnerable_Dependency_Management_Cheat_Sheet.html
- https://www.slideshare.net/urma_/software-composition-analysis-deep-dive


TREND MICRO
THE ART OF CYBERSECURITY
Real-time discovery and remediation of cloud vulnerabilities and misconfigurations by Trend Micro.
Created with real data by artist Brendan Dawes.