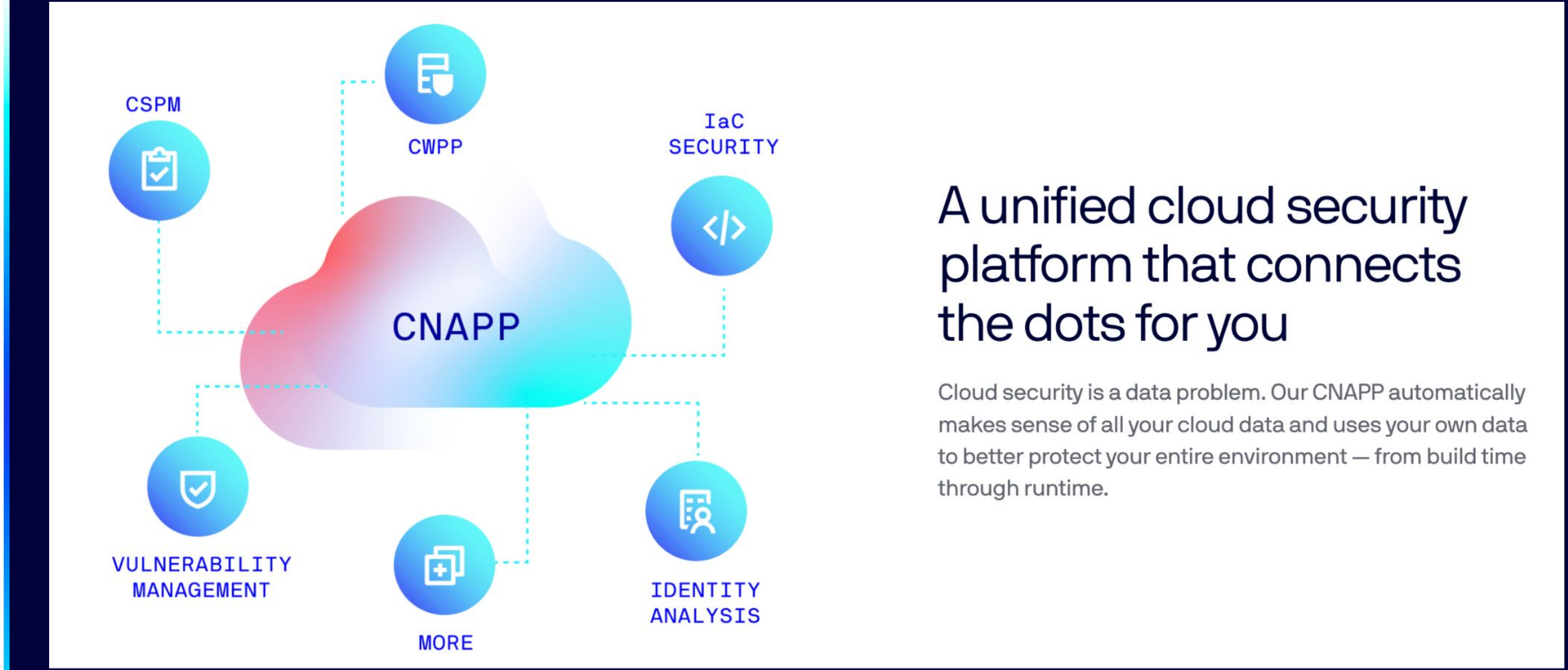
Vulnerability Management 2.0

Patrice Godefroid

Lacework = Cloud Security is a Data Problem



A unified cloud security platform that connects the dots for you

Cloud security is a data problem. Our CNAPP automatically makes sense of all your cloud data and uses your own data to better protect your entire environment — from build time through runtime.

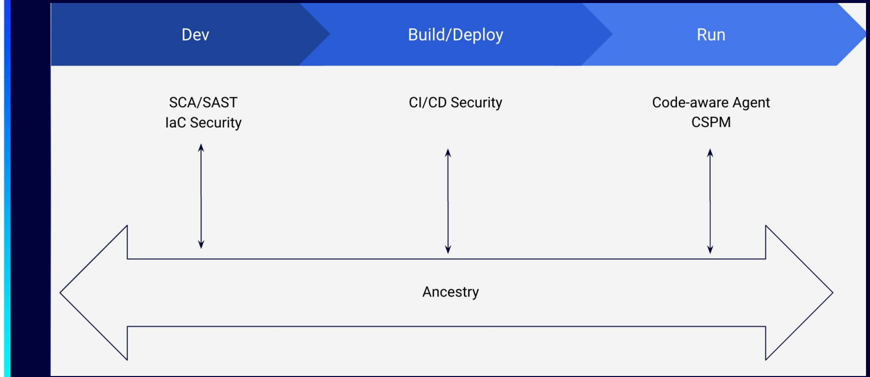
Introducing Code Security @ Lacework [AWS re:Invent, Nov 2023]

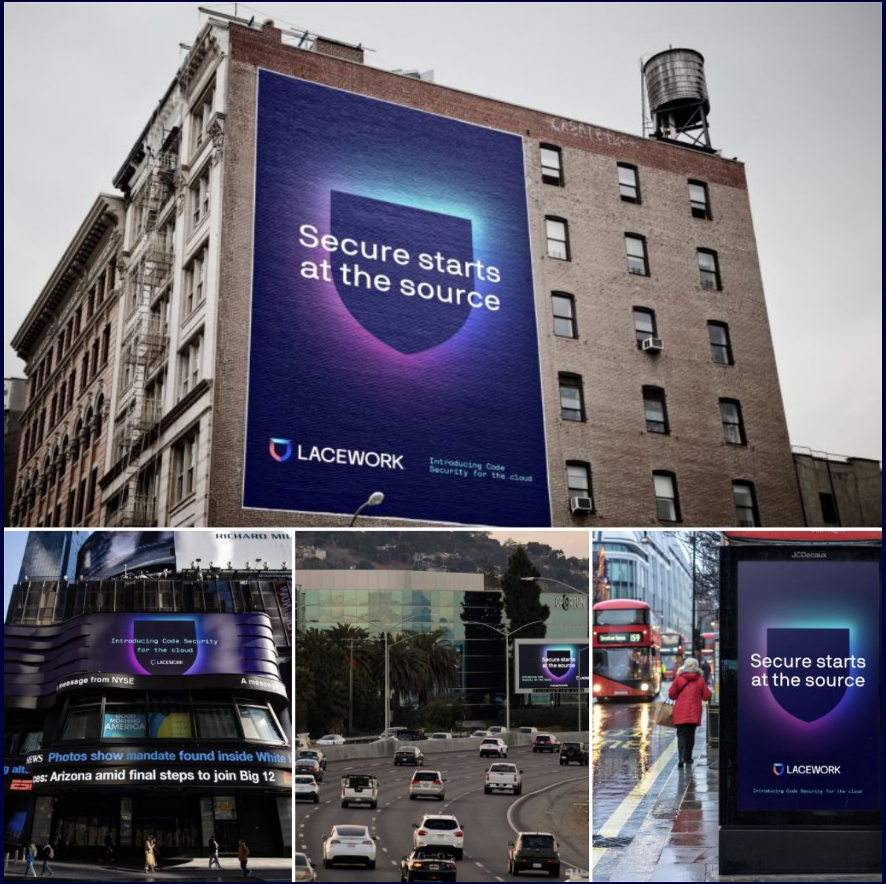
Code Security =

- IaC (Infrastructure as Code)
- SCA (Software Composition Analysis)
- SAST (Static Analysis)
    - Quick
    - Deep

+ Code-Aware Agents [RSA, May 2023]

From Code to Cloud and Back:




Secure starts at the source
LACEWORK
Introducing Code Security for the cloud

LACEWORK

Vulnerability Management

1.0: (today)

- Scan your repos/VMs/containers
- To get list of all 3rd party (OSS) packages (SBOM)
- Cross check that list with vulnerability databases

Outcome: list of vulnerable packages + good luck!

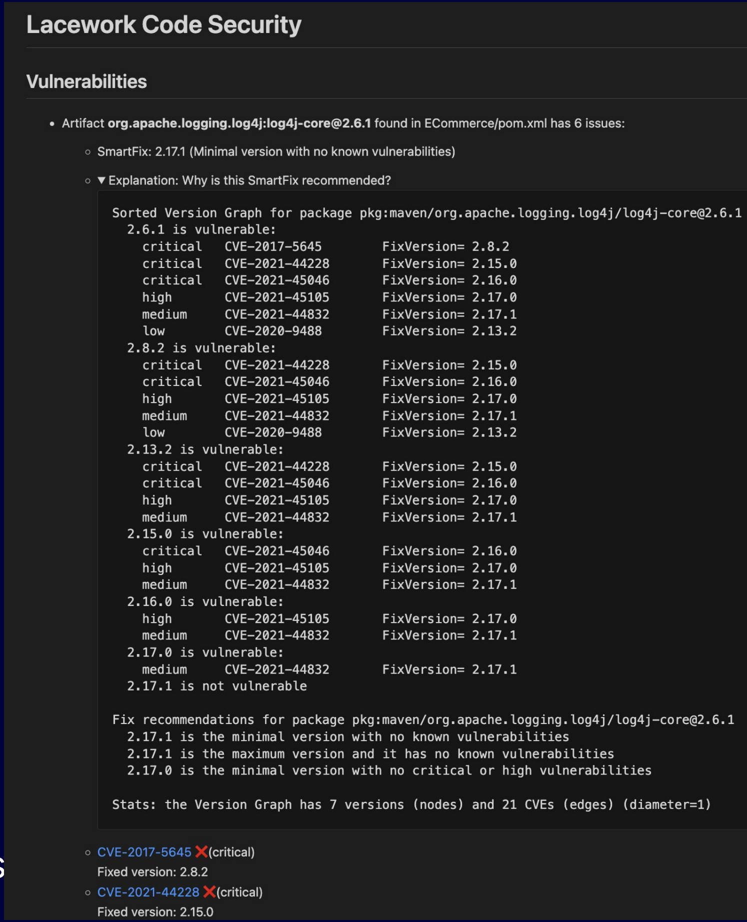
2.0: (tomorrow) 1.0 + automated remediations

- Find the most optimal fix for each package
  - See the new Lacework Smart Fix →

    [RSA, May 2024]
- Automatically generate Pull Requests to fix those
  - Use search (backtrack) in case of failed steps

Goal: 10x to 100x speed ups

- From hours (work) and days (elapsed) to secs
- Automate 90% of security engs and devs tasks



Lacework Code Security

Vulnerabilities

- Artifact **org.apache.logging.log4j:log4j-core@2.6.1** found in ECommerce/pom.xml has 6 issues:
  - SmartFix: 2.17.1 (Minimal version with no known vulnerabilities)
  - ▼ Explanation: Why is this SmartFix recommended?

```
Sorted Version Graph for package pkg:maven/org.apache.logging.log4j/log4j-core@2.6.1
  2.6.1 is vulnerable:
    critical   CVE-2017-5645       FixVersion= 2.8.2
    critical   CVE-2021-44228      FixVersion= 2.15.0
    critical   CVE-2021-45046      FixVersion= 2.16.0
    high       CVE-2021-45105      FixVersion= 2.17.0
    medium     CVE-2021-44832      FixVersion= 2.17.1
    low        CVE-2020-9488       FixVersion= 2.13.2
  2.8.2 is vulnerable:
    critical   CVE-2021-44228      FixVersion= 2.15.0
    critical   CVE-2021-45046      FixVersion= 2.16.0
    high       CVE-2021-45105      FixVersion= 2.17.0
    medium     CVE-2021-44832      FixVersion= 2.17.1
    low        CVE-2020-9488       FixVersion= 2.13.2
  2.13.2 is vulnerable:
    critical   CVE-2021-44228      FixVersion= 2.15.0
    critical   CVE-2021-45046      FixVersion= 2.16.0
    high       CVE-2021-45105      FixVersion= 2.17.0
    medium     CVE-2021-44832      FixVersion= 2.17.1
  2.15.0 is vulnerable:
    critical   CVE-2021-45046      FixVersion= 2.16.0
    high       CVE-2021-45105      FixVersion= 2.17.0
    medium     CVE-2021-44832      FixVersion= 2.17.1
  2.16.0 is vulnerable:
    high       CVE-2021-45105      FixVersion= 2.17.0
    medium     CVE-2021-44832      FixVersion= 2.17.1
  2.17.0 is vulnerable:
    medium     CVE-2021-44832      FixVersion= 2.17.1
  2.17.1 is not vulnerable

Fix recommendations for package pkg:maven/org.apache.logging.log4j/log4j-core@2.6.1
  2.17.1 is the minimal version with no known vulnerabilities
  2.17.1 is the maximum version and it has no known vulnerabilities
  2.17.0 is the minimal version with no critical or high vulnerabilities

Stats: the Version Graph has 7 versions (nodes) and 21 CVEs (edges) (diameter=1)
```

  - CVE-2017-5645 ❌(critical)
    Fixed version: 2.8.2
  - CVE-2021-44228 ❌(critical)
    Fixed version: 2.15.0

LACEWORK