Let's go

#CiscoLive

The bridge to possible

A practical approach

to securing applications and APIs

Chris Jackson, Distinguished Architect @chrijack
Barry Yuan, Technical Solutions Architect @barryyuan

BRKSEC-2174

Chris Jackson, Distinguished Architect
Cisco Live Distinguished Speaker
CCIE #6256, RS & Security

Barry Yuan, Technical Solutions Architect
Cisco Live Distinguished Speaker
CCIE #11860, RS & Security

Cisco Webex App

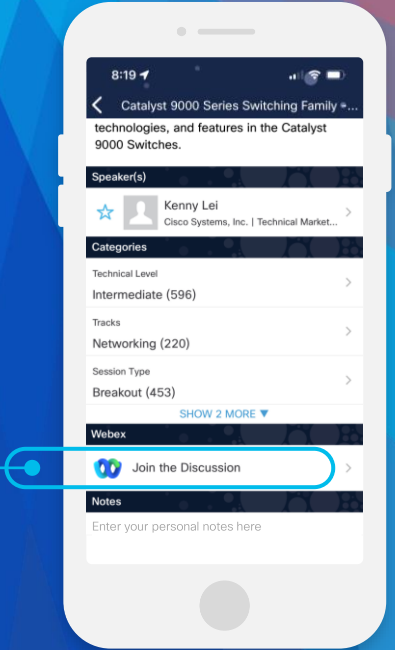
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated
by the speaker until June 9, 2023.



8:19

Catalyst 9000 Series Switching Family ...

technologies, and features in the Catalyst 9000 Switches.

Speaker(s)

Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

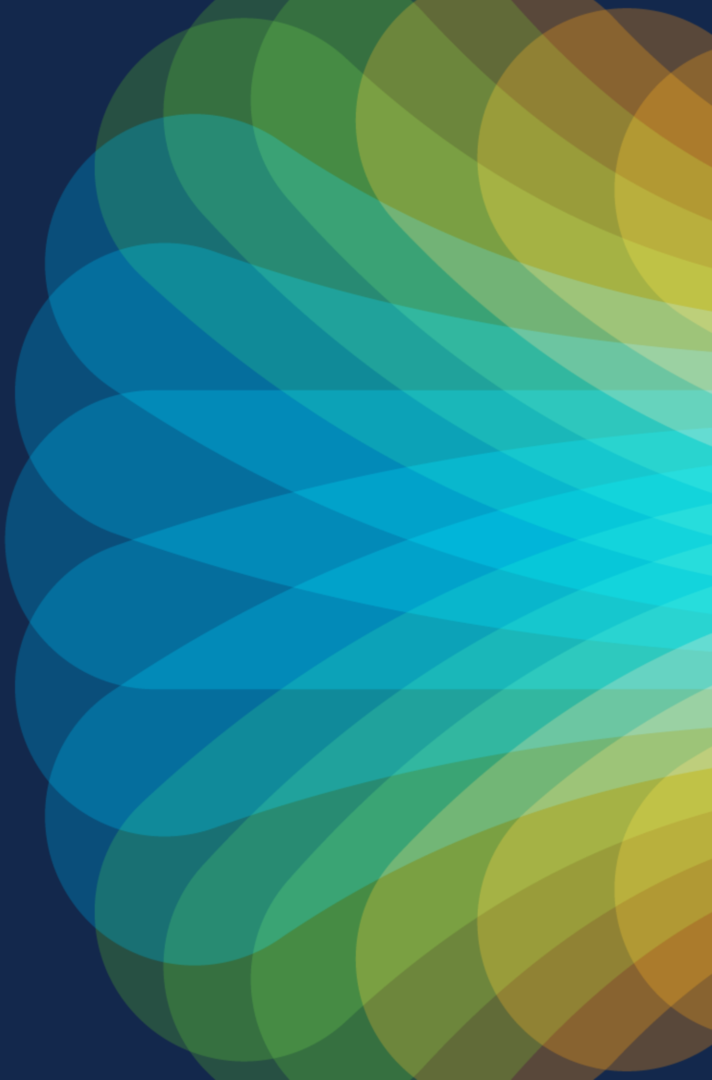
Enter your personal notes here

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2174

Agenda

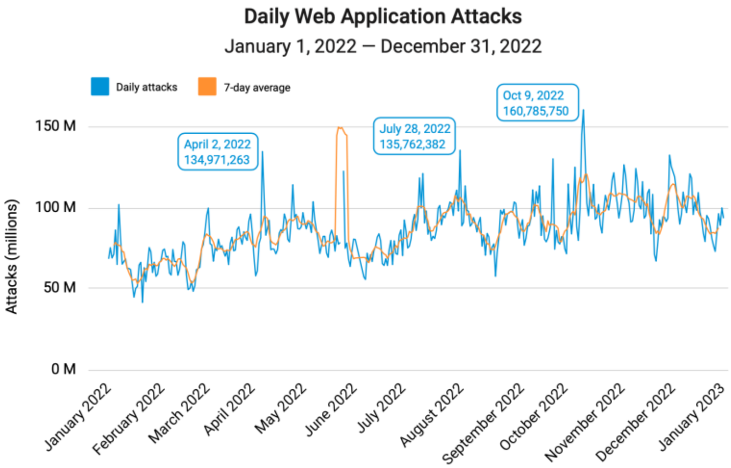
- Why should you care about application and API security?
- Identifying API security issues
- Attacks and defense
- Wrap up / Q&A

Why should you protect APIs?



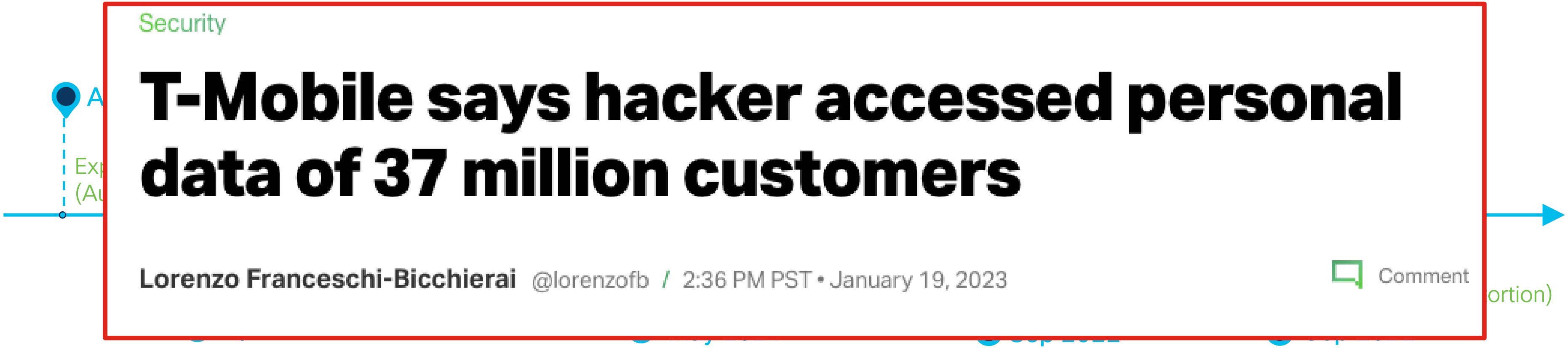
APIs are the attack vector of choice

- 83% of internet traffic volume is API
- Salt Security Q1 2023 State of API Security Report stated that 94% of those surveyed have experienced security problems in production APIs over the past year, with 17% having experienced an API-related breach. 400% increase in number of unique attackers in Q1 2023
- In 90% of investigations, Salt Labs identifies API security vulnerabilities, 50% of which should be considered critical.
  - Salt Security Q1 2023 State of API Security Report



Source: Akamai **Slipping Through the Security Gaps**

Real world API compromises



Security

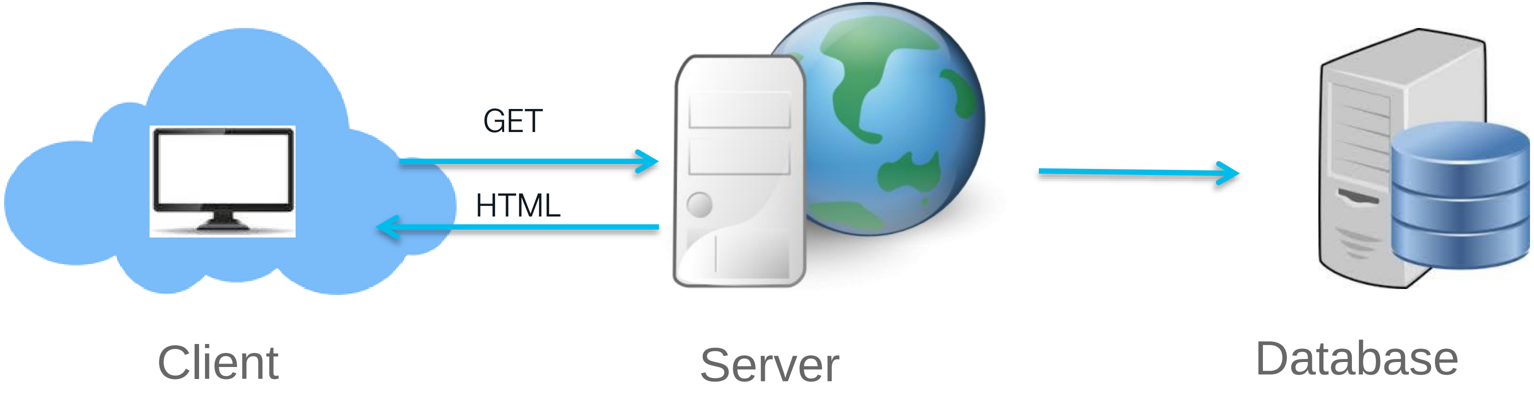
T-Mobile says hacker accessed personal data of 37 million customers

Lorenzo Franceschi-Bicchierai @lorenzofb / 2:36 PM PST • January 19, 2023

Comment

API attacks will become the most-frequent attack vector, causing data breaches for enterprise web applications.
- Gartner, 2022

Traditional Application Architecture



Small and Known Number of Users

Small Number of Complex Components

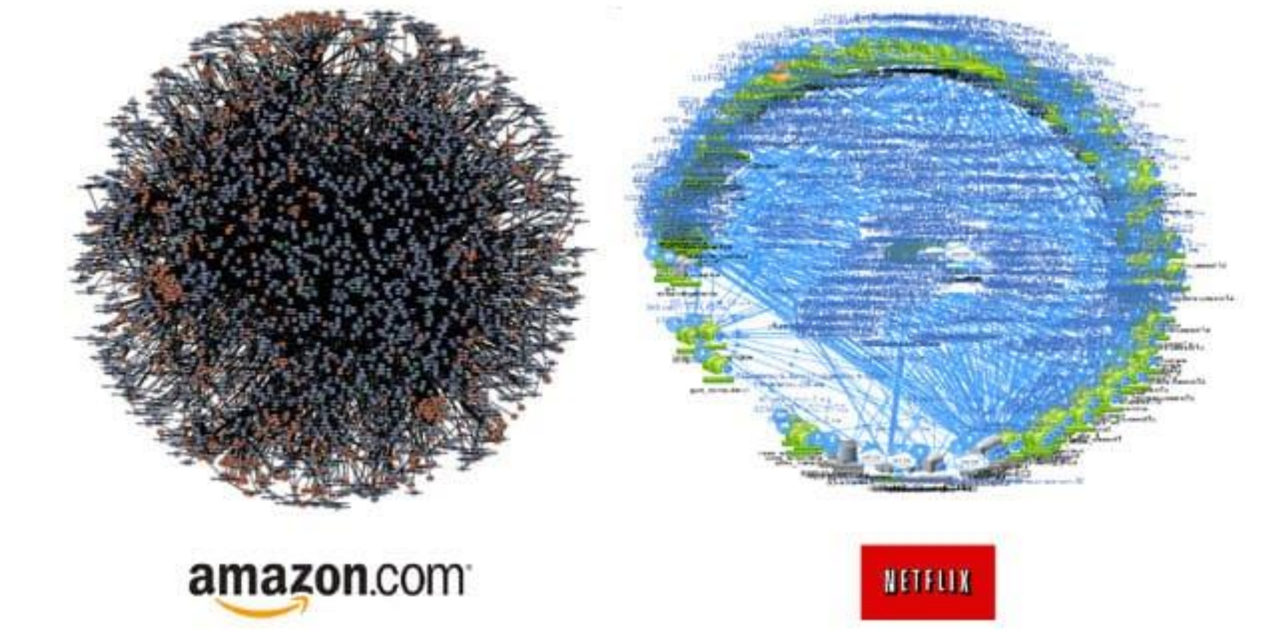
Single Transactional Data Source

Modern App Architecture (Cloud Native)

Request Layer

Client
Reque

Data



Ever Ch
Number of Users

Simple Components

Data Sources
of all Types and Location

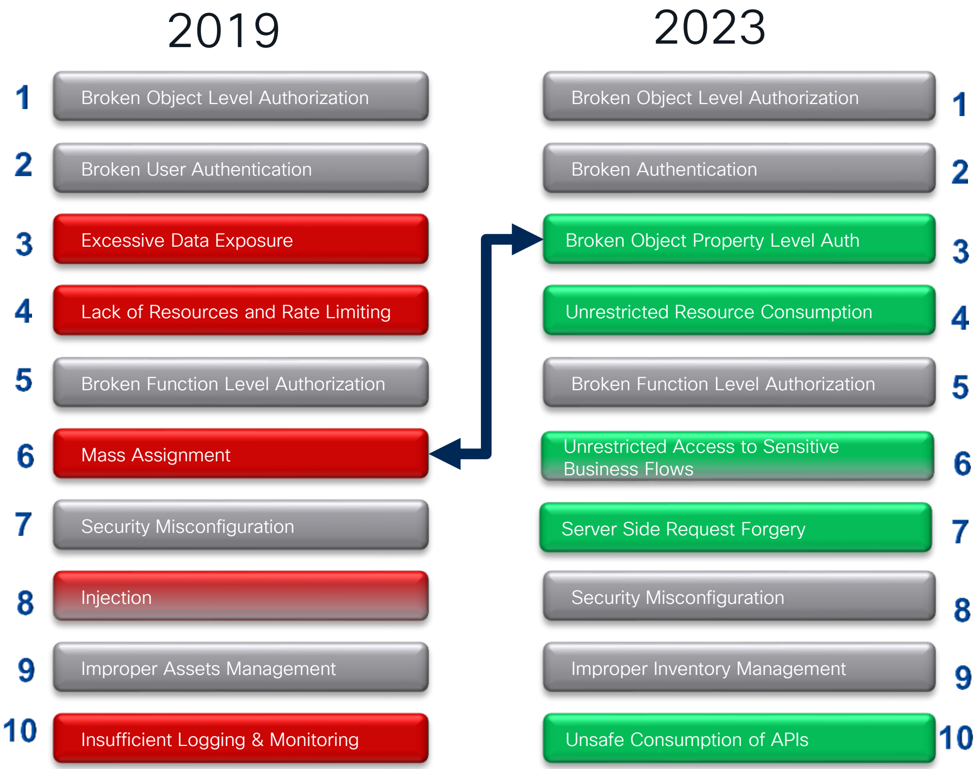
Identifying API security issues

Preventing API vulnerabilities

- What happens before code is written?
  - Training
  - Secure SDLC
  - Threat modeling
  - Threat Intelligence
  - Scope of change detection
  - Peer code review
- Find and fix common security issues before the code is committed to source control system
  - IDE linting
  - Secrets detection
  - SAST
  - Pre-commit hooks

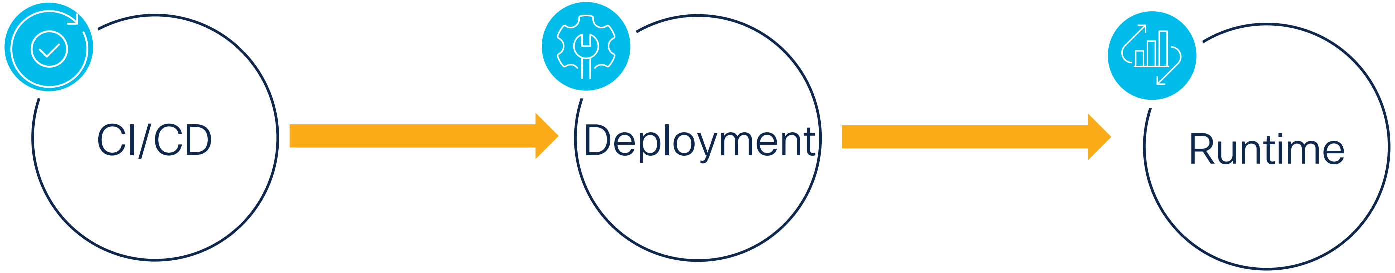
OWASP API Sec top 10

- OWASP project to call attention to key security issues around APIs and their use
- Started in 2019 updated in 2023
- Great starting point to build defenses and countermeasures
- Why is there a separate top 10 for APIs?
  - Similar issues, but scope is different
  - Direct access by attackers
  - Data exfiltration exposure



	2019	2023	
1	Broken Object Level Authorization	Broken Object Level Authorization	1
2	Broken User Authentication	Broken Authentication	2
3	Excessive Data Exposure	Broken Object Property Level Auth	3
4	Lack of Resources and Rate Limiting	Unrestricted Resource Consumption	4
5	Broken Function Level Authorization	Broken Function Level Authorization	5
6	Mass Assignment	Unrestricted Access to Sensitive Business Flows	6
7	Security Misconfiguration	Server Side Request Forgery	7
8	Injection	Security Misconfiguration	8
9	Improper Assets Management	Improper Inventory Management	9
10	Insufficient Logging & Monitoring	Unsafe Consumption of APIs	10

Application pipeline: API security focus areas



- API1: Broken object level authorization
- API2: Broken Authentication
- API3: Broken object property level authorization
- API4: Unrestricted resource consumption
- API5: Broken function level authorization
- API6: Unrestricted Access to Sensitive Business Flows
- API7: Server side request forgery
- OpenAPI spec analysis
- API endpoint fuzz testing

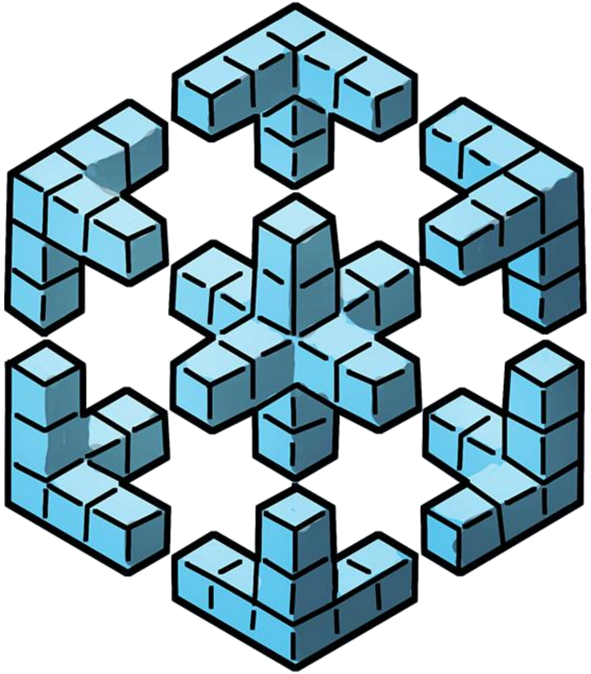
- API8: Security misconfiguration
- API9: Improper inventory management
- API inventory
- API connection Tracking

- API10: Unsafe consumption of APIs
- Protection from automated threats
- API trace analysis

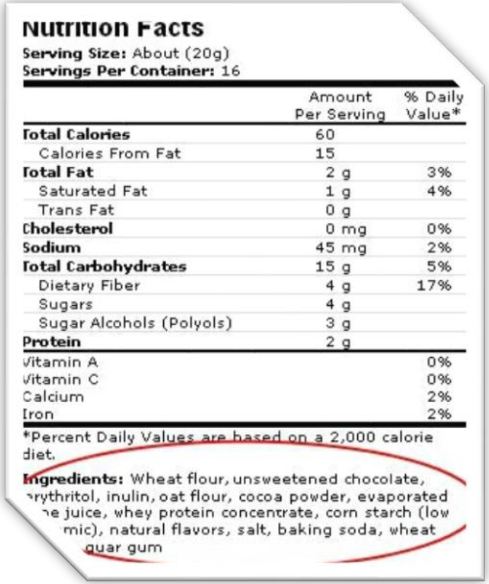
Attacks and defense

Building secure software

- In a CICD pipeline code is built using automated techniques
- Typically involves a CI server and/or integrated into a gitops pipeline
- Includes
  - Software dependency vulnerability checks SBOM/SCA
  - Deploy to test environment
  - Unit tests
  - Security testing (SAST/DAST)
- Results in creation of software artifacts or publishing new image to container repository



What is SBOM (Software Bill of Material)



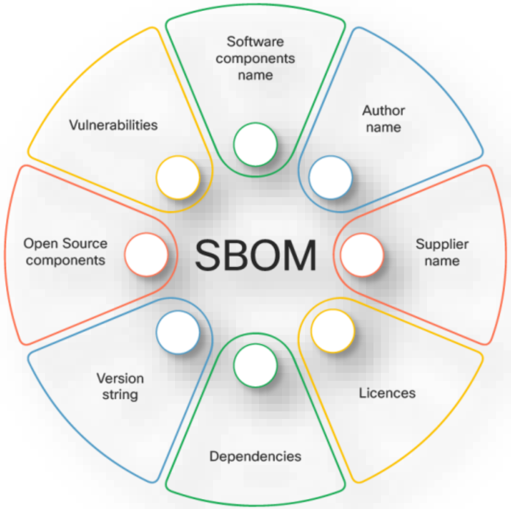
Nutrition Facts

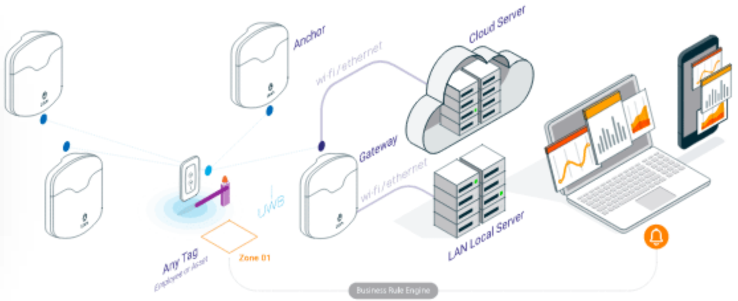
Serving Size: About (20g)
Servings Per Container: 16

	Amount Per Serving	% Daily Value*
Total Calories	60	
Calories From Fat	15	
Total Fat	2 g	3%
Saturated Fat	1 g	4%
Trans Fat	0 g	
Cholesterol	0 mg	0%
Sodium	45 mg	2%
Total Carbohydrates	15 g	5%
Dietary Fiber	4 g	17%
Sugars	4 g	
Sugar Alcohols (Polyols)	3 g	
Protein	2 g	
Vitamin A		0%
Vitamin C		0%
Calcium		2%
Iron		2%

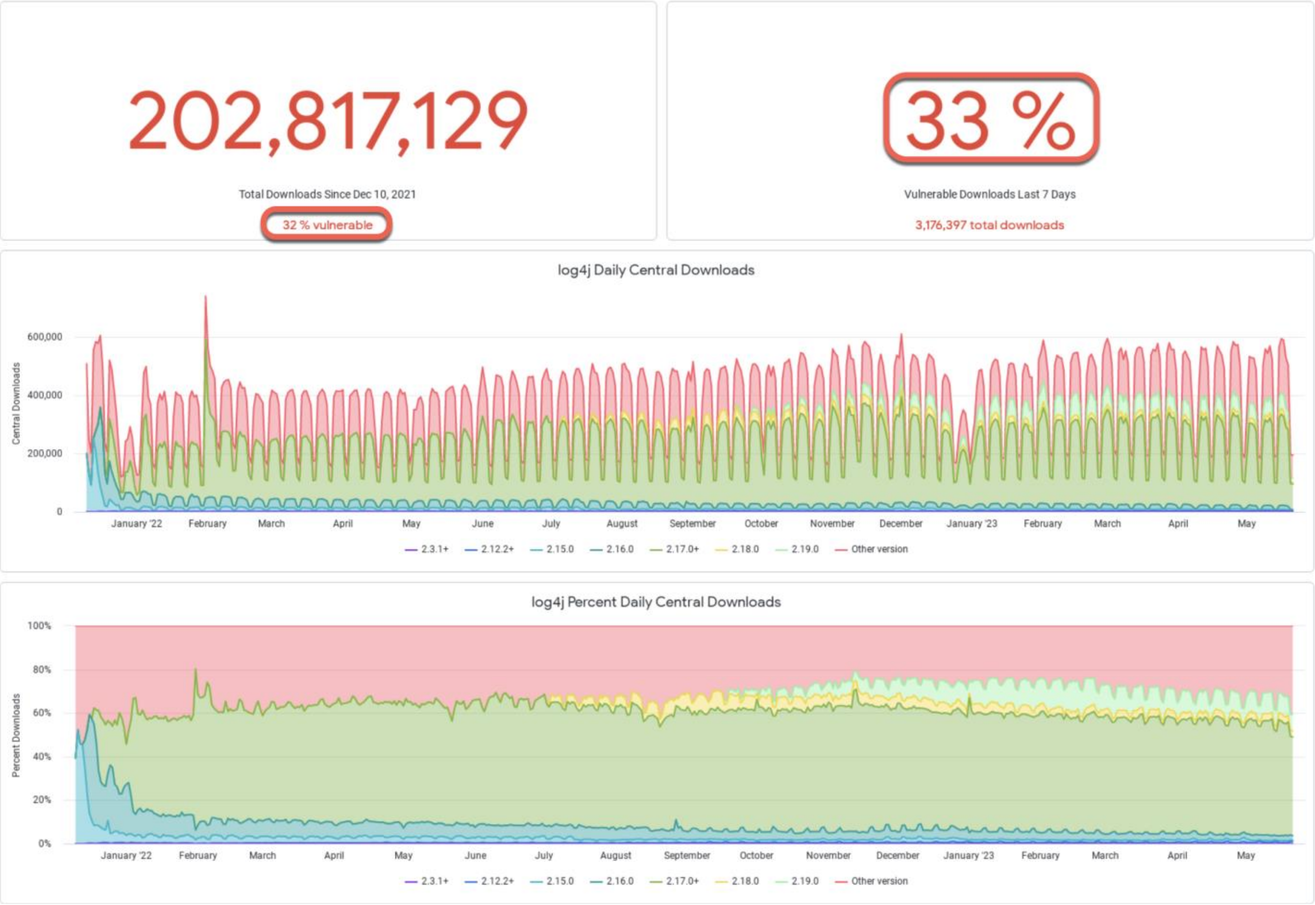
*Percent Daily Values are based on a 2,000 calorie diet.

Ingredients: Wheat flour, unsweetened chocolate, rythritol, inulin, oat flour, cocoa powder, evaporated ne juice, whey protein concentrate, corn starch (low mic), natural flavors, salt, baking soda, wheat guar gum





Log4j – Still relevant after more than a year!



202,817,129

Total Downloads Since Dec 10, 2021

32 % vulnerable

33 %

Vulnerable Downloads Last 7 Days

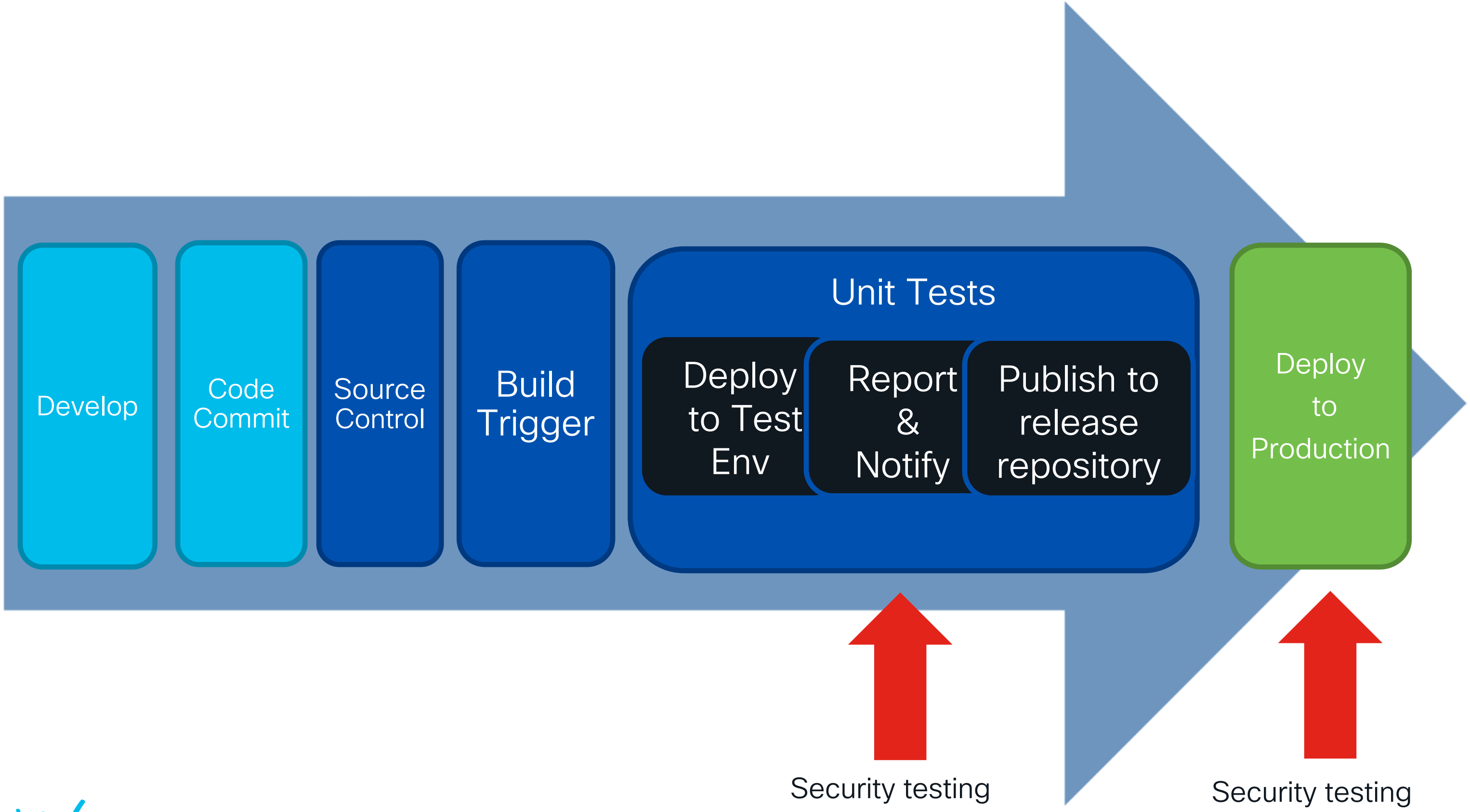
3,176,397 total downloads

log4j Daily Central Downloads

log4j Percent Daily Central Downloads

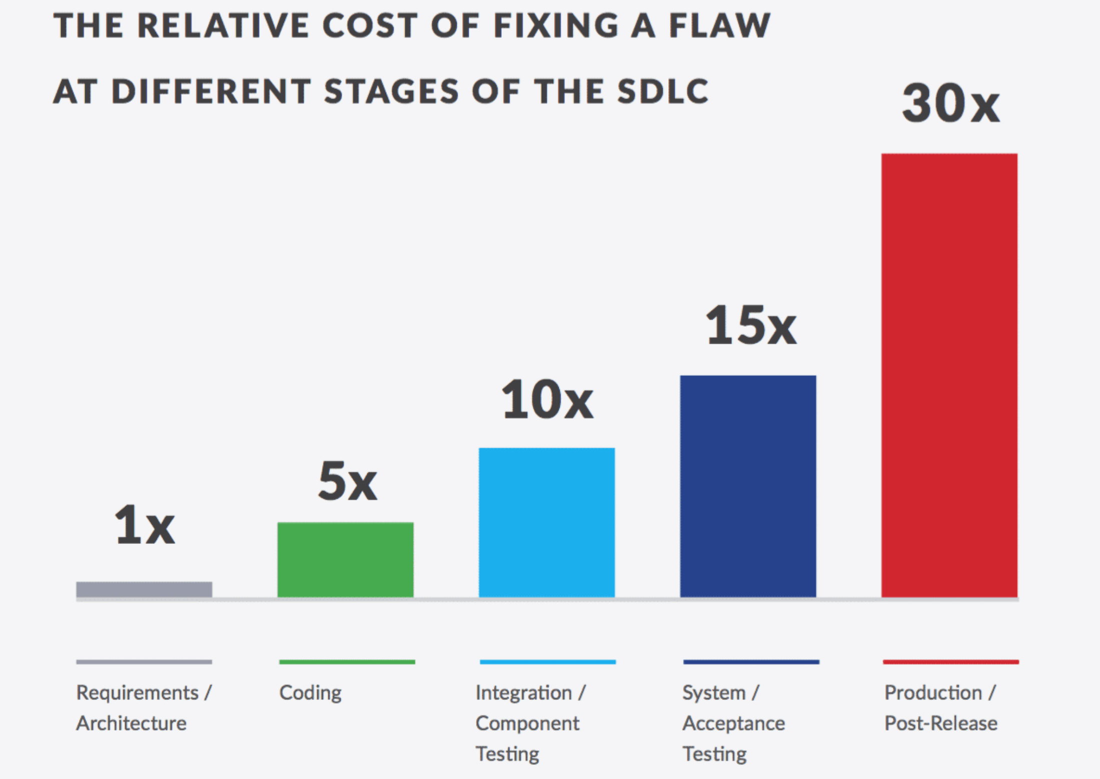
DEMO

CI/CD pipeline



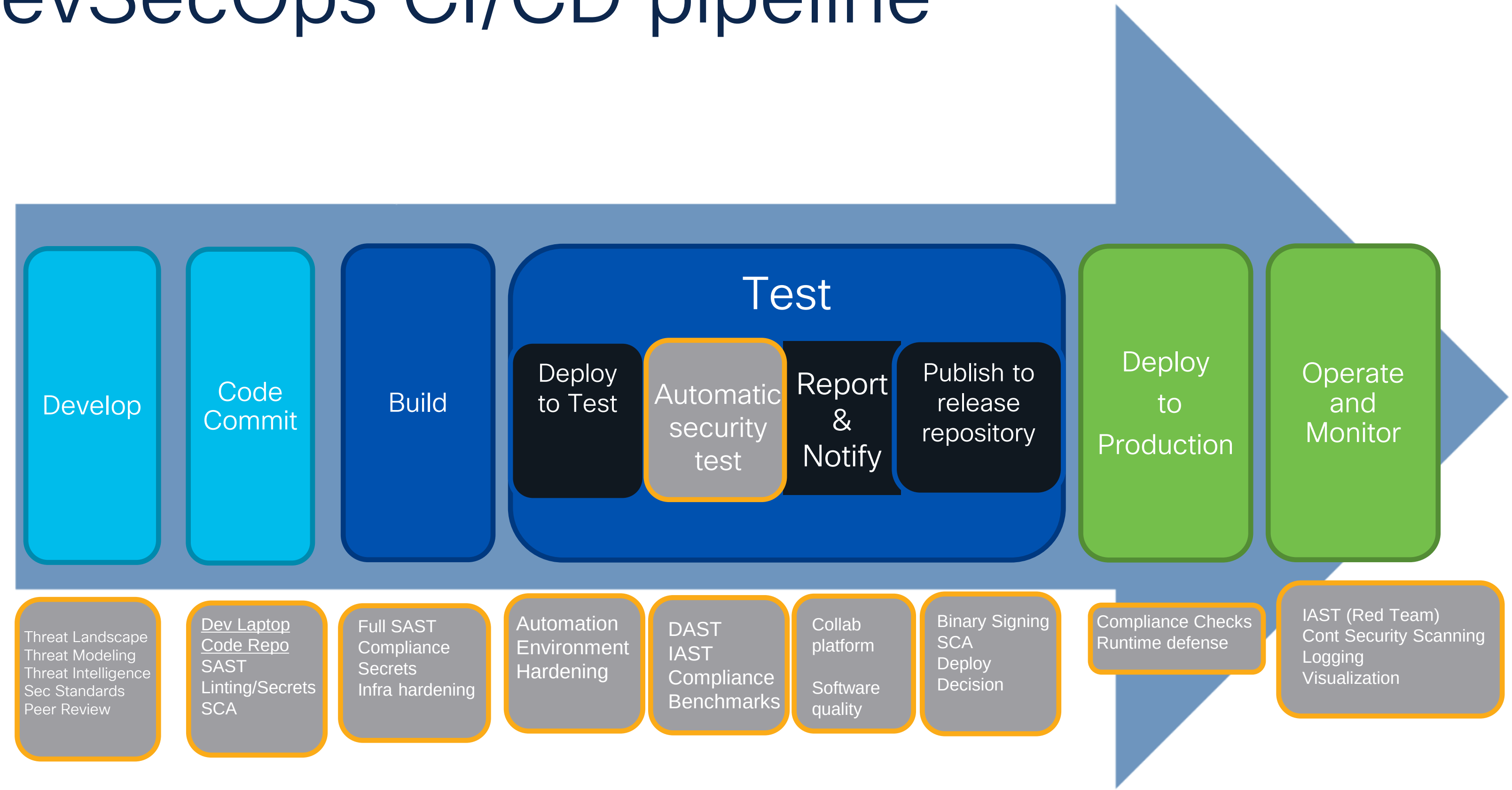
Shift left security

- Security used to be focused on infrastructure and after the fact testing
- DevSecOps moves security earlier in the development pipeline



Source: NIST

DevSecOps CI/CD pipeline



Develop

Code Commit

Build

Test

Deploy to Test

Automatic security test

Report & Notify

Publish to release repository

Deploy to Production

Operate and Monitor

Threat Landscape
Threat Modeling
Threat Intelligence
Sec Standards
Peer Review

Dev Laptop
Code Repo
SAST
Linting/Secrets
SCA

Full SAST
Compliance
Secrets
Infra hardening

Automation
Environment
Hardening

DAST
IAST
Compliance
Benchmarks

Collab platform

Software quality

Binary Signing
SCA
Deploy
Decision

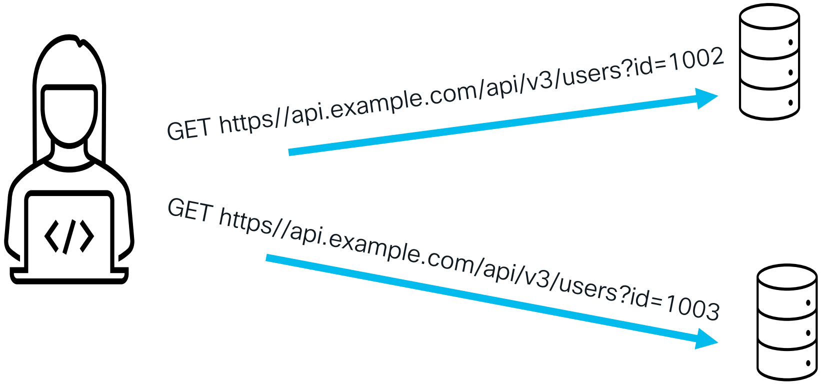
Compliance Checks
Runtime defense

IAST (Red Team)
Cont Security Scanning
Logging
Visualization

CI/CD

Broken object level authorization

- Very common API vulnerability
- Attacker manipulates object IDs to impersonate other users
- Client access is allowed by design
- Authorization needs to be validated against privilege of the logged in user



GET https//api.example.com/api/v3/users?id=1002

GET https//api.example.com/api/v3/users?id=1003

DEMO

CI/CD

Broken authentication

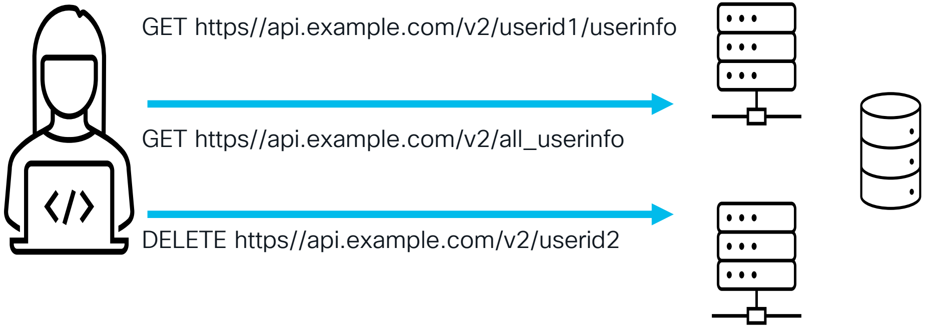
- Caused by weak authentication methods
- Lots of tools to make this easier
- Password reset workflows are another form of authentication

DEMO

CI/CD

Broken function level authorization

- API is used to modify resources of another user
- Often as simple as changing URL parameters or methods
- Can be used to escalate privileges


GET https//api.example.com/v2/userid1/userinfo
GET https//api.example.com/v2/all_userinfo
DELETE https//api.example.com/v2/userid2

DEMO

Security misconfiguration

CI/CD

Deployment

Runtime

- Broad category of vulnerabilities that include anything reduces security based on misconfiguration of security controls
- Attackers use various automaton tools to discover and exploit
- Weak encryption, CORS policy, lack of security hardening, etc.

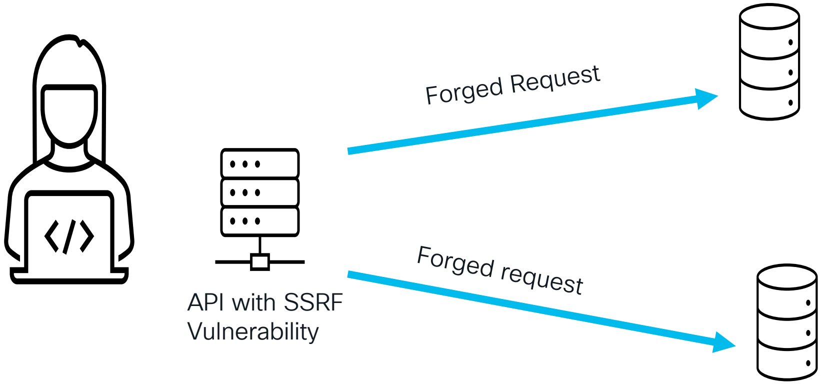
DEMO

Server-side request forgery

CI/CD

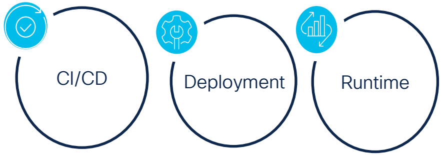
Runtime

- API request to connect to a third-party resource without validating the user supplied URL
- Common design for modern applications
- Webhooks, file fetching from URLs, custom SSO, and URL previews are examples
- Can be used to download and execute malicious code



DEMO

Improper inventory management



- Unauthorized application access through old, deprecated, or unused APIs
- Attackers use automated tools to find and exploit
- Usually, a result of weak visibility of API usage and workflow

DEMO

CI/CD

Deployment

Runtime

API runtime protection strategies

Enable encrypted transport to protect the data your APIs transmit

Use IP address allow and deny lists if you have small numbers of API consumers

Look to dynamic rate limiting and rely on static rate limiting as a last resort

Enforce network security via infrastructure, not in code

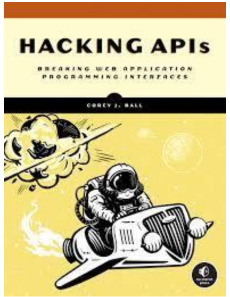
Use an API Gateway

DEMO

Wrap Up / Q&A

Further education

- Hacking APIs: Breaking Web Application Programming Interfaces by Corey Ball
- Free API Security courses
  - https://www.apisecuniversity.com/
- OWASP crAPI (Vulnerable API to practice API Sec top 10)
  - https://owasp.org/www-project-crapi/
- VAPI (Another vulnerable API)
  - https://github.com/roottusk/vapi



OWASP/www-project-crapi

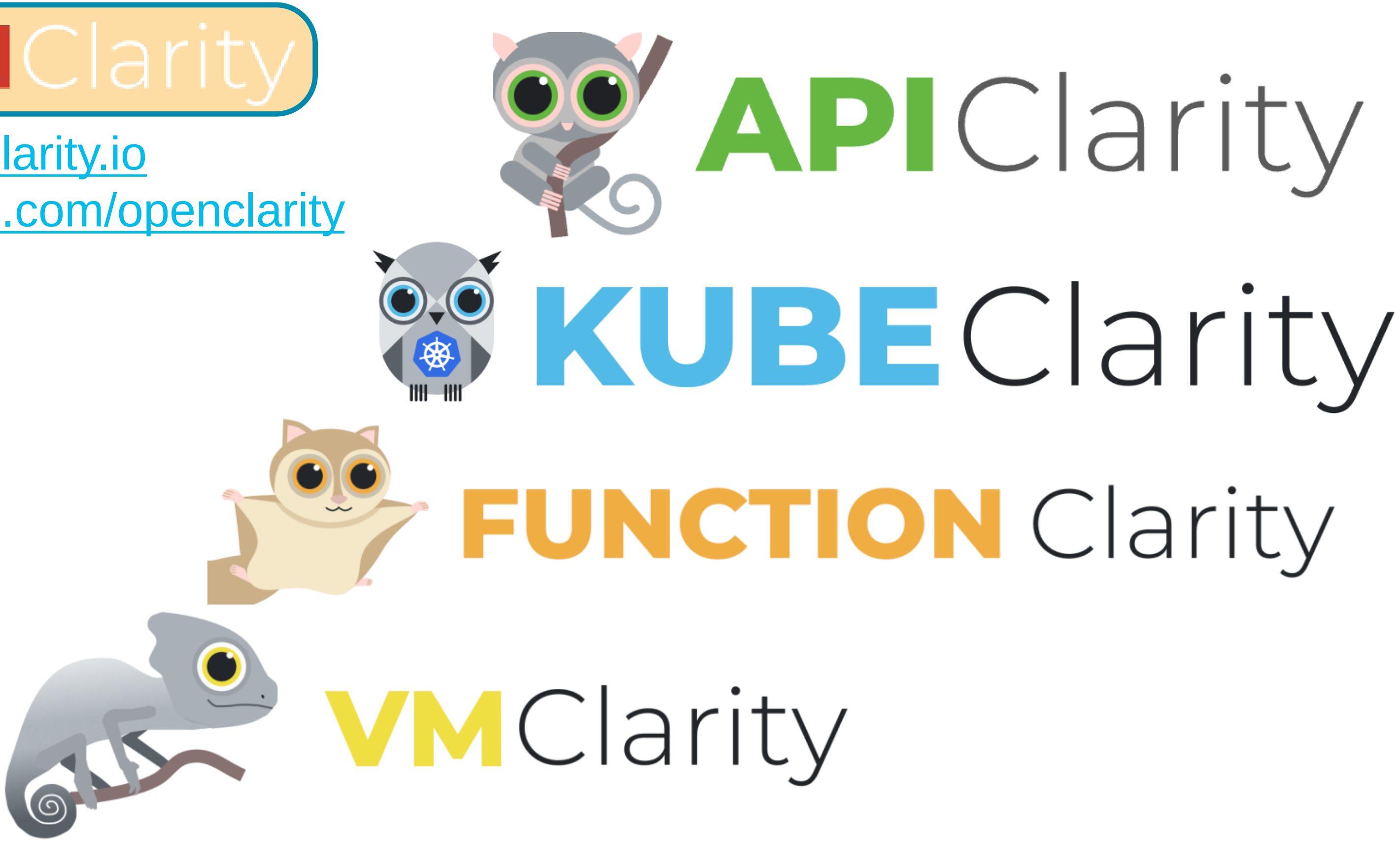
OWASP Foundation Web Respository

5 Contributors · 0 Issues · 2 Stars · 2 Forks

Cisco Open Source for Cloud Native Security

OPENClarity

https://openclarity.io
https://github.com/openclarity



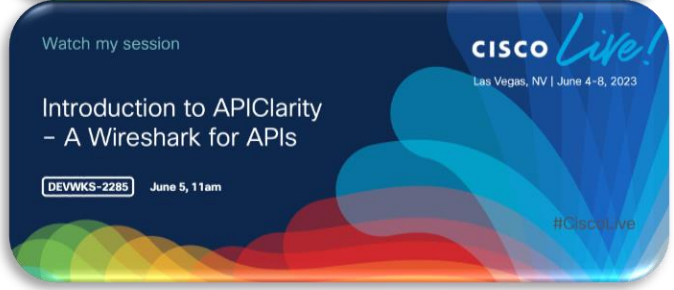
Hands on workshops

Watch my session
Security at the speed of cloud
- Security as code
DEVWKS-2255
June 6, 2pm
CISCO Live!
Las Vegas, NV | June 4-8, 2023
#CiscoLive

Hands on lab covering Panoptica and Secure Workload, https://cs.co/appsec

Watch my session
Cloud Hygiene - KubeClarity
hands-on
DEVWKS-2445
June 6, 11am
CISCO Live!
Las Vegas, NV | June 4-8, 2023
#CiscoLive

Hands on lab covering Kubeclarity, https://cs.co/kubeclarity



Hands on lab covering APIClarity, https://cs.co/APIClarity

Fill out your session surveys!

Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!

Attendees will also earn 100 points in the **Cisco Live Challenge** for every survey completed.

These points help you get on the leaderboard and increase your chances of winning daily and grand prizes

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

The bridge to possible

Thank you

#CiscoLive

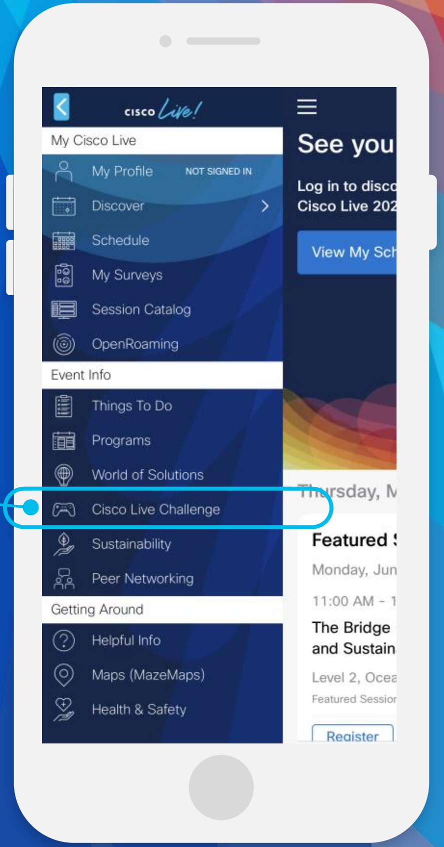
Cisco Live **Challenge**

Gamify your Cisco Live experience!

Get points for attending this session!

How:

1. Open the Cisco Events App.
2. Click on 'Cisco Live Challenge' in the side menu.
3. Click on View Your Badges at the top.
4. Click the + at the bottom of the screen and scan the QR code:



cisco Live!

cisco Live!

Let's go

#CiscoLive