
cisco Live!
Let's go
#CiscoLive

The bridge to possible

Finding and securing APIs in your Kubernetes cluster with APIClarity

Tim Miller, PhD – Technical Marketing Engineer
@broadcaststorm

DEVNET-2124

Cisco Webex App

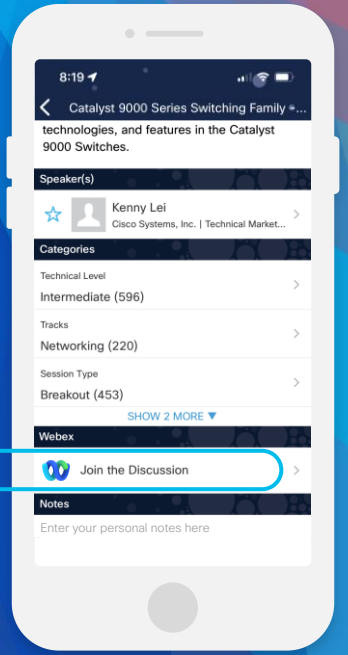
Questions?

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.



https://ciscolive.ciscoevents.com/ciscolivebot/#DEVNET-2124

Agenda

- API Overview
- API Security Review
- APIClarity and How it Works (Demos!)
- Conclusion

Some Expectations

- API Security (You, me, now!)
  - Categories of concerns related to APIs
  - How to discover and assess those concerns

- API Foundational Material (Many DevNet sessions!)
  - Intro to REST APIs (DEVWKS-1185)
  - OpenAPI Standard (BRKDEV-2249)
  - API Design (DEVNET-2092)

- (This slide will be at the end as well!)

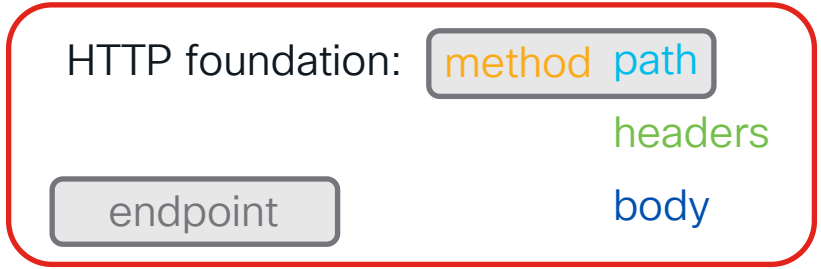
DEVWKS-1185

BRKDEV-2249

DEVNET-2092

API Overview

RESTful API Endpoints
(Application Programming Interface)



GET /reservation/{moid}

Content-type: application/json
Authorization: Bearer abc123

```
{
  "results": [
    "id1": {
      "name": "Tim"
    }
  ]
}
```
response

POST /reservation

Content-type: application/json
Authorization: Bearer abc123

```
{
  "flight": {
    "name": "Tim",
    "dest": "LAS"
  }
}
```
request

```
{
  "results": {
    "id": "id2",
    "status": "good"
  }
}
```
response

RESTful API Endpoints

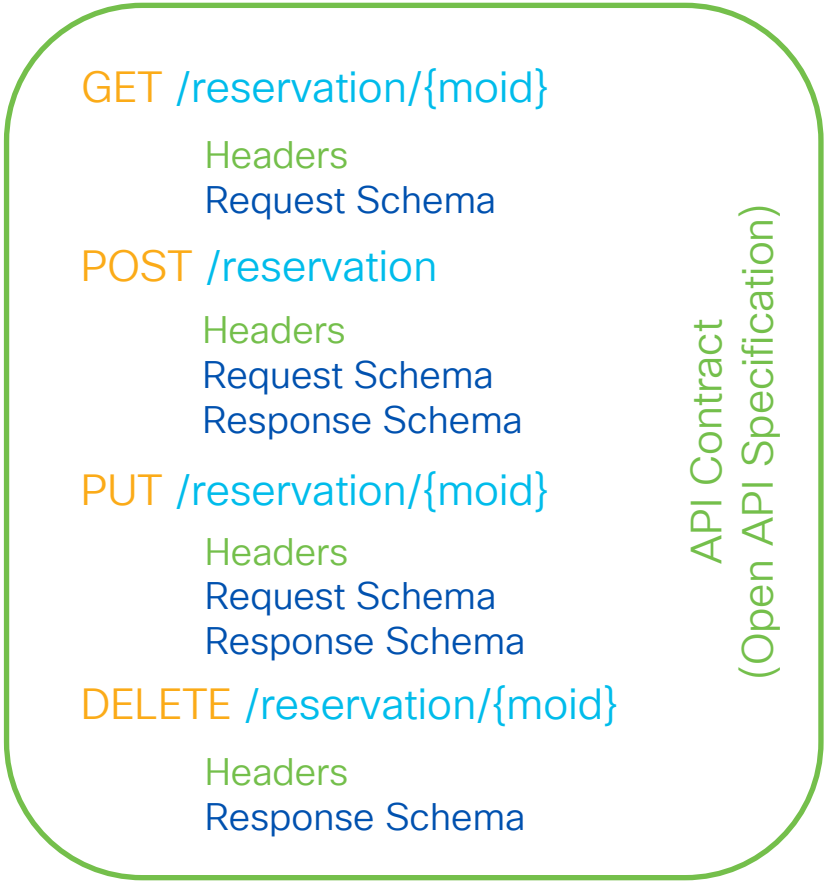
GET /reservation/{moid}

POST /reservation

RESTful API Contract

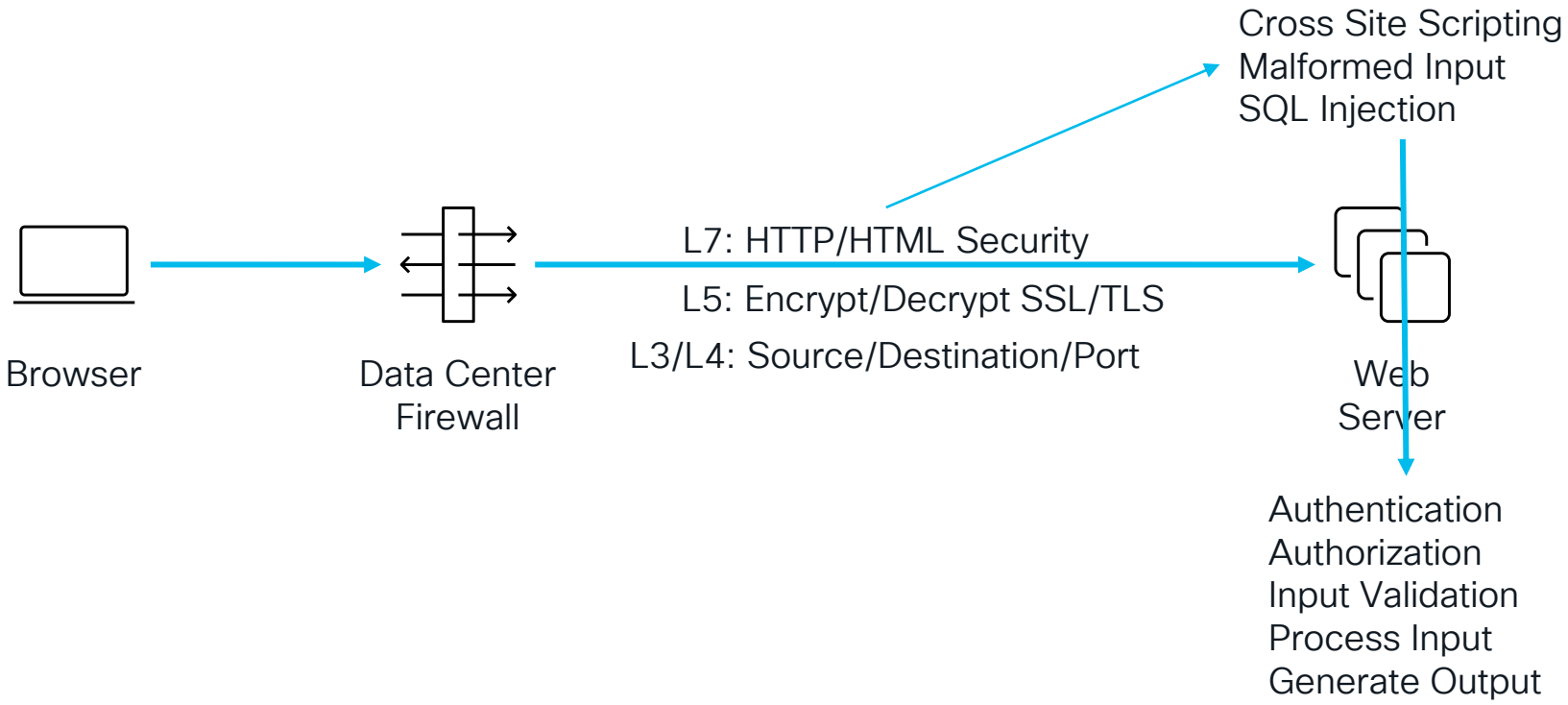
OpenAPI Specification

booking

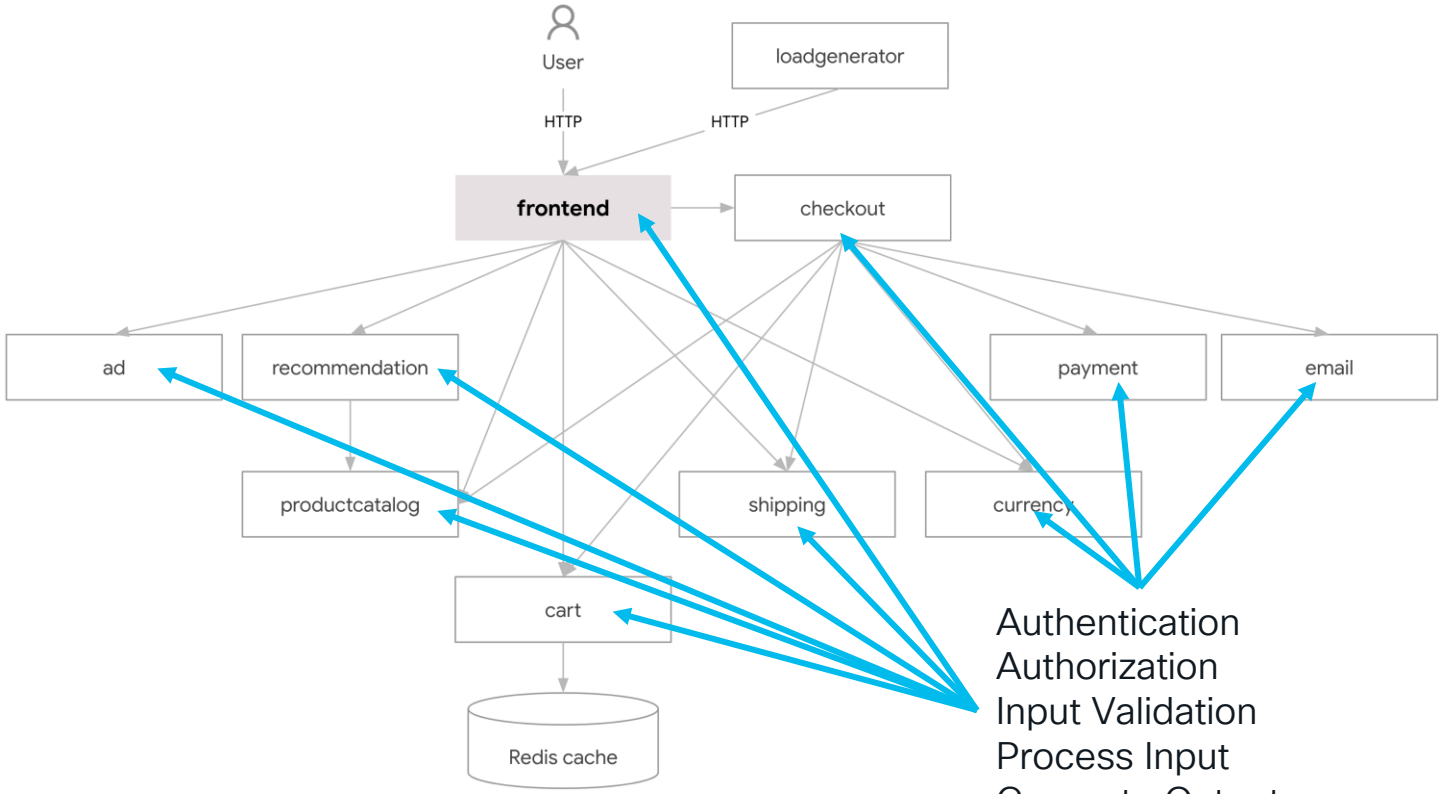


API Security Challenges

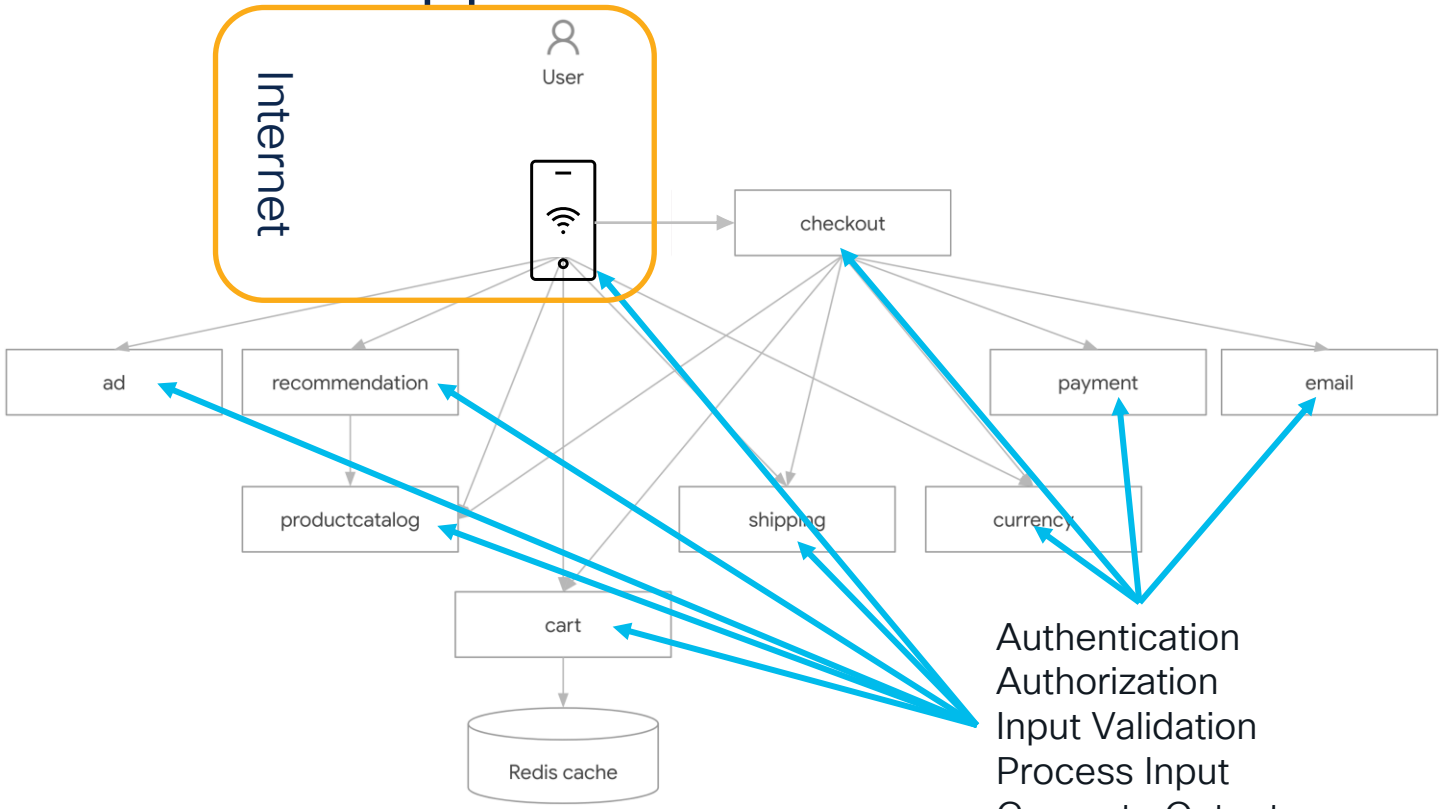
Traditional Web Server Security



Microservices Approach – Larger Attack Surface

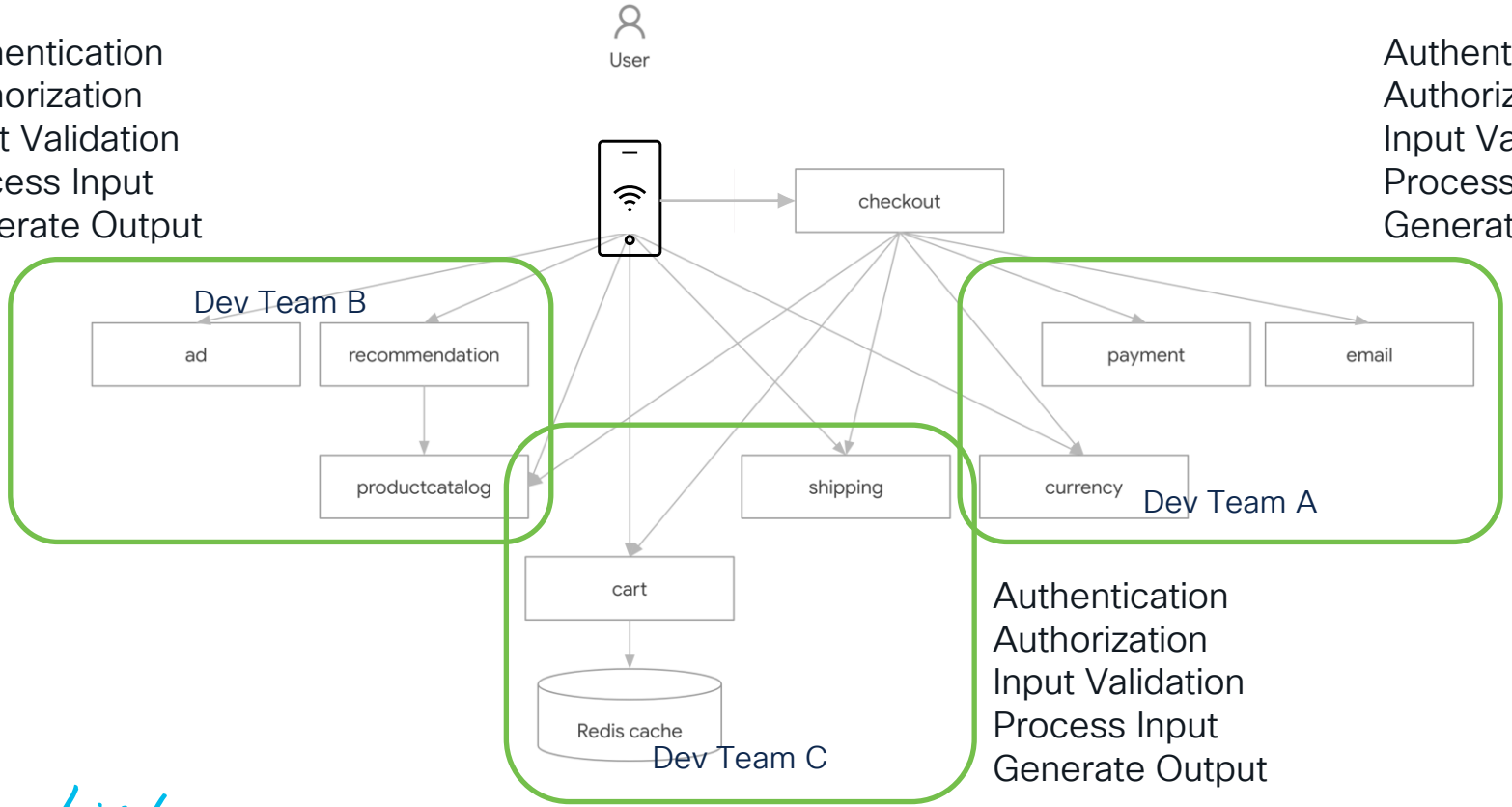


Microservices Approach – Greater Scale



Microservices Approach – Distributed Efforts

Authentication
Authorization
Input Validation
Process Input
Generate Output



Authentication
Authorization
Input Validation
Process Input
Generate Output

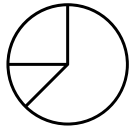
Authentication
Authorization
Input Validation
Process Input
Generate Output

API Security Challenges

Consistency

A single application consists of multiple microservices, typically built by multiple teams.

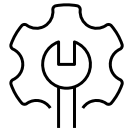
The same authentication and authorization policies must be applied from the client to the various sources of data.



Scale

Direct Internet connections and the explosion of services present a massive scale challenge.

By nature, APIs are susceptible to automation attacks not possible with traditional applications.



Visibility

Features are developed at an increasingly accelerated rate.

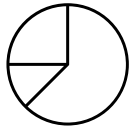
Security teams struggle to know which APIs exist and ascertaining the total risk of breach across all APIs and data sources daunting.

API Security – Unique context but familiar themes

AuthN/AuthZ

The most common security exploits of API endpoints focus on the basics:

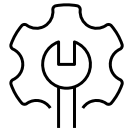
- authenticating access to endpoint (BUA)
- authorization to call the endpoint (BFLA)
- authorization to access the specific data behind the endpoint (BOLA)
- input sanitizing could result in that authorization being exploited (API8)



Granularity

API endpoints are typically written for general use cases, resulting in:

- sensitive data model attributes can be exposed (API3)
- little control exists on the amount of information accessed (API4)
- hidden data attributes can be overwritten (API6)



Operations

The scale of development requires elevating operational rigor to ensure:

- complete visibility into all the APIs deployed (API9)
- comprehensive, dynamic monitoring and logging (API10)
- security configuration best practices are followed in deployments (API7)

APIClarity

Open Source Projects – yes, by Cisco!

OPENClarity

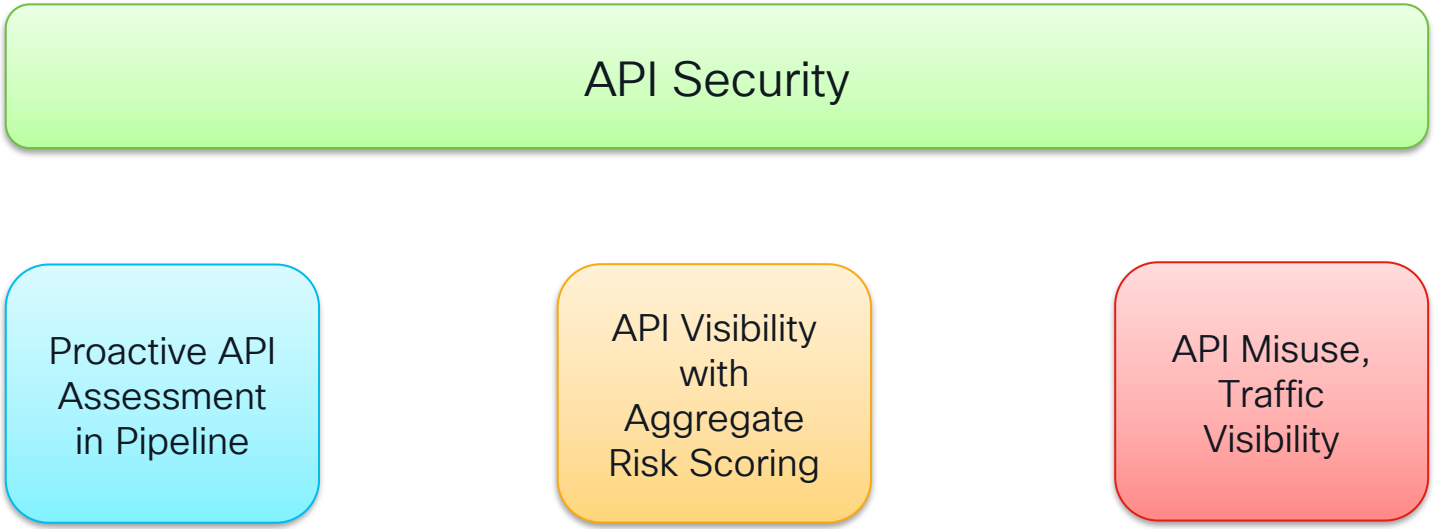
APIClarity

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

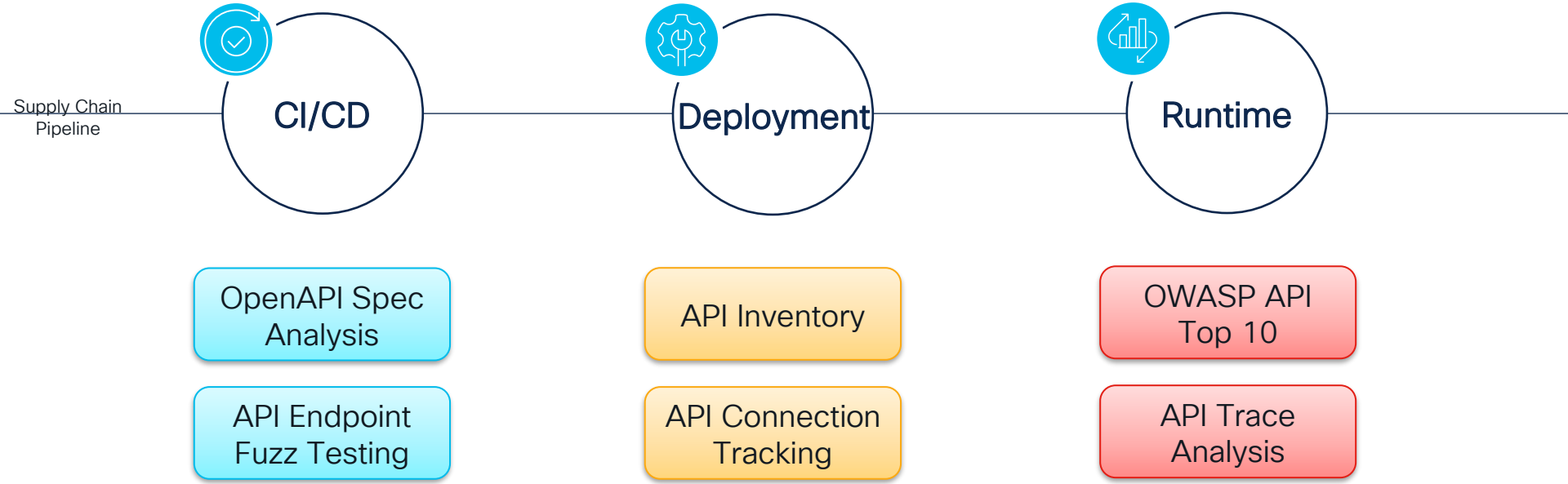
https://apiclarity.io
https://github.com/openclarity/apiclarity

Panoptica
Cloud-Native Application Security, Simplified

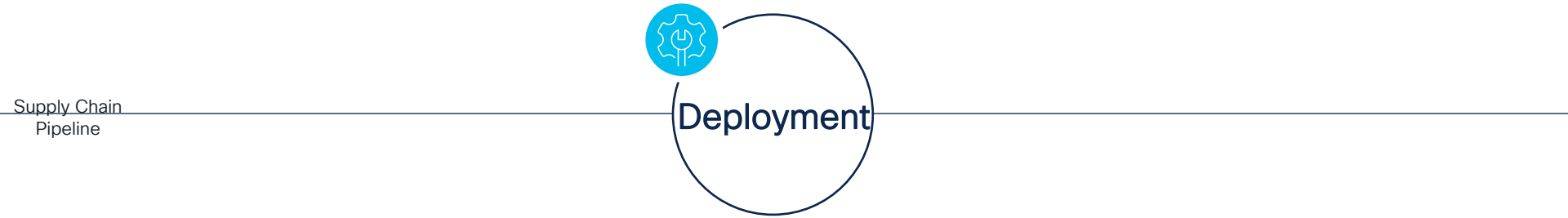
API Security Areas of Focus



Securing APIs from Dev through Production

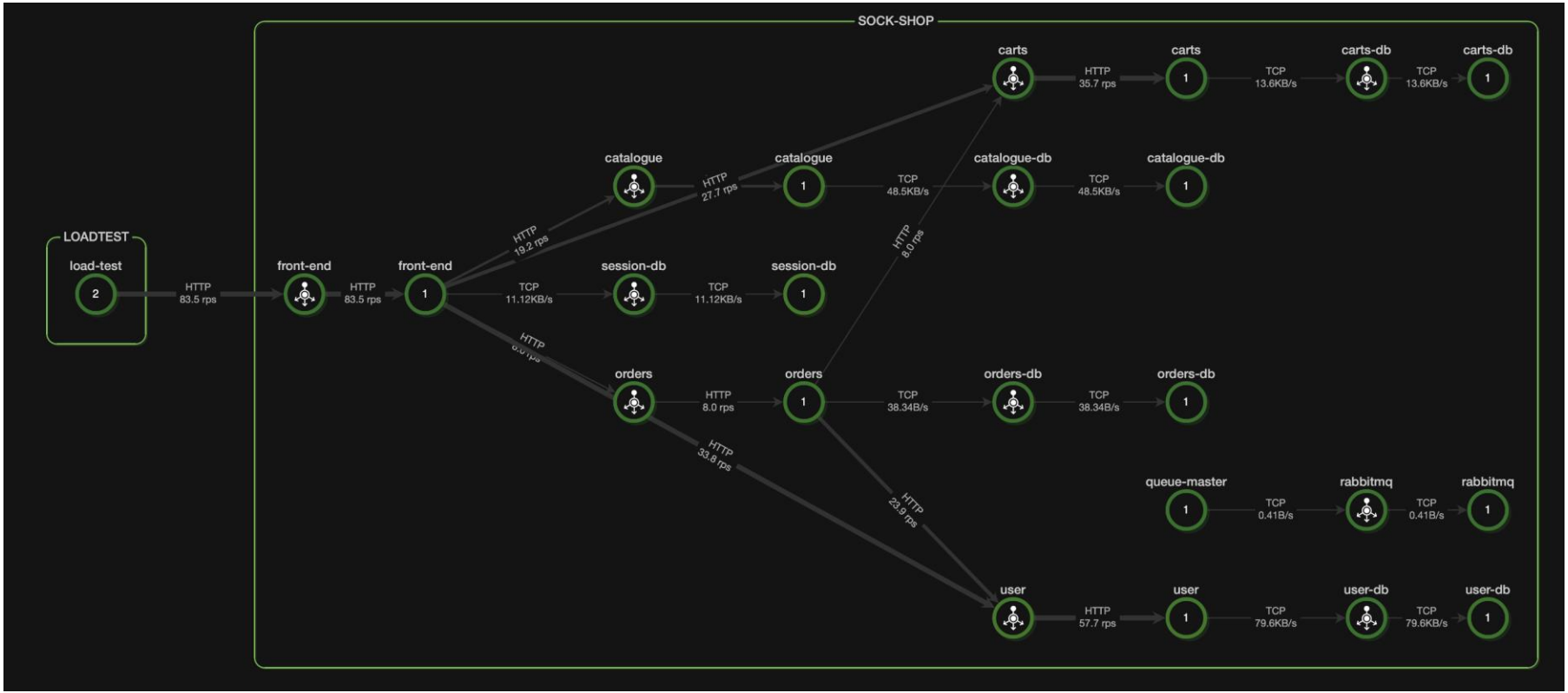


Comprehensive Visibility



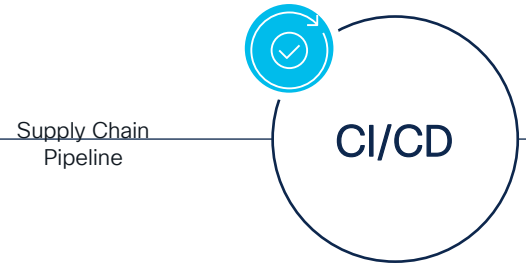
API Inventory	Identify unknown internal and 3rd party APIs, comprehensive risk assessment with workload security context
API Connection Tracking	Visibility into communication patterns between microservices, identify unknown traffic patterns

Sample Application – Sock Shop!



API Inventory Demo

Shifting Security Left for Prevention

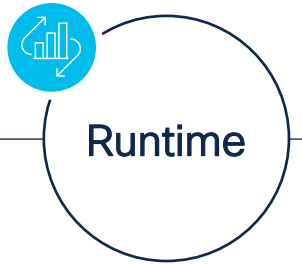


OpenAPI Spec Analysis	Validate API security schemes, authN/authZ methods, poor programming practices, flag non-conformant schemas/methods
API Endpoint Fuzz Testing	Simulate attack behavior before production, provide early detection of potential OWASP API Security Top 10 threats

Spec Analysis Fuzz Testing Demo

Verifying proper security controls with API traces

Supply Chain Pipeline



OWASP API Top 10	Identify broken authN/authZ, anomalous API access behavior
API Trace Analysis	Sensitive data discovery, API endpoint drift (zombie, stealth), insecure credentials in headers

Trace Analysis Demo

Wrap it up!

Critical Element to Modern Application Security

- Cloud native apps are not just workloads!
- By leveraging existing cloud native platform technologies, you can provide a frictionless means to provide visibility and security for your applications.
- By providing an open source assessment engine, we leverage the community to improve and enhance on the capabilities.

DevNet Opportunities for API Education

- API Security (You, me, then!)
  - Categories of concerns related to APIs
  - How to discover and assess those concerns

- API Foundational Material (Many DevNet sessions!)
  - Intro to REST APIs (DEVWKS-1185)
  - OpenAPI Standard (BRKDEV-2249)
  - API Design (DEVNET-2092)

- (Look! This slide is actually at the end!)

DEVWKS-1185

BRKDEV-2249

DEVNET-2092

Additional Resources

- Outshift's Emerging Technology Advocacy (ETA) Blogs!
  - https://techblog.cisco.com
  - APIClarity Series:
    - https://techblog.cisco.com/author/anne-mccormick
- Openclarity.io

Emerging Technologies & Incubation

Cloud Native Security

Explore why a new approach to security is needed for cloud native applications and learn how Cisco is meeting these rapidly evolving security requirements.

START

Monday, June 5 | 9:30 a.m.
BRKETI-1003
Intro to Outshift

Monday, June 5 | 11:00 a.m.
DEVWKS-2285
Introduction to APIClarity - A Wireshark for APIs

Monday, June 5 | 1:00 p.m.
DEVWKS-2974
Securing Cloud Native Applications with Panoptica

Tuesday, June 6 | 10:30 a.m.
BRKAPP-1116
CNAPP and FSO together - Synergies of Cisco Observability and Cloud-Native Application Security

Tuesday, June 6 | 3:00 p.m.
BRKETI-2511
Securing Cloud Native Applications with Panoptica

Wednesday, June 7 | 10:30 a.m.
BRKETI-2903
Why You Need a CNAPP ASAP!

Wednesday, June 7 | 12:00 p.m.
DEVWKS-3002
API Security with Panoptica

Thursday, June 8 | 8:00 a.m.
IBOETI-2001
Bring the Pain! What Are Your Most Painful Cloud Native Security Problems?

Thursday, June 8 | 9:00 a.m.
DEVWKS-3003
5G Core security with Panoptica

FINISH

Thursday, June 8 | 9:30 a.m.
BRKAPP-1115
Cloud Native Application Security: An Integrated CNAPP Approach from Cisco

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 Game** 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

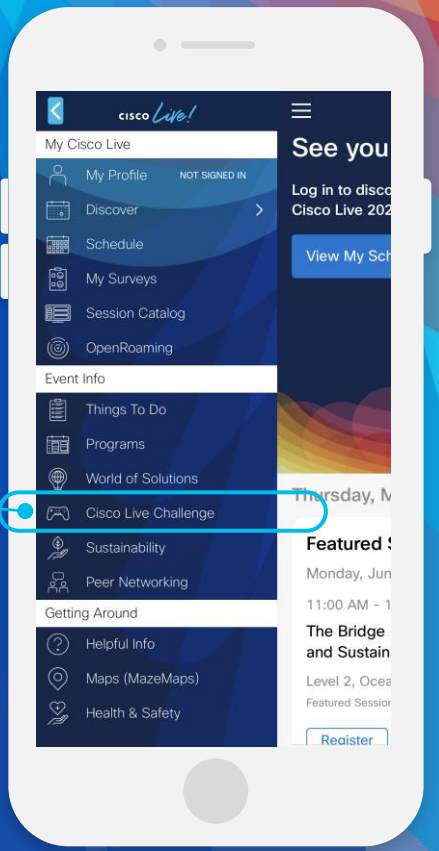
Cisco Live
Challenge

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!
Let's go
#CiscoLive