
cisco Live!
Let's go
#CiscoLive

The bridge to possible

Top 5 Shift left security tools for your open-source projects

Oleksii Borysenko
@alex_dev_k
DEVNET-1067

Cisco Webex App

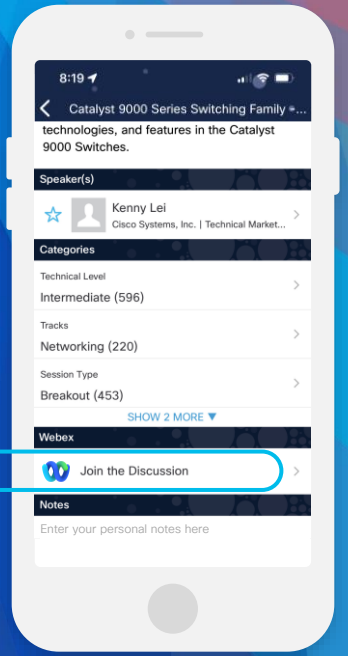
Questions?

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-1067

Agenda

- Introduction
- KubeClarity
- Bank vaults
- API Insights
- API Clarity
- VMClarity

KubeClarity

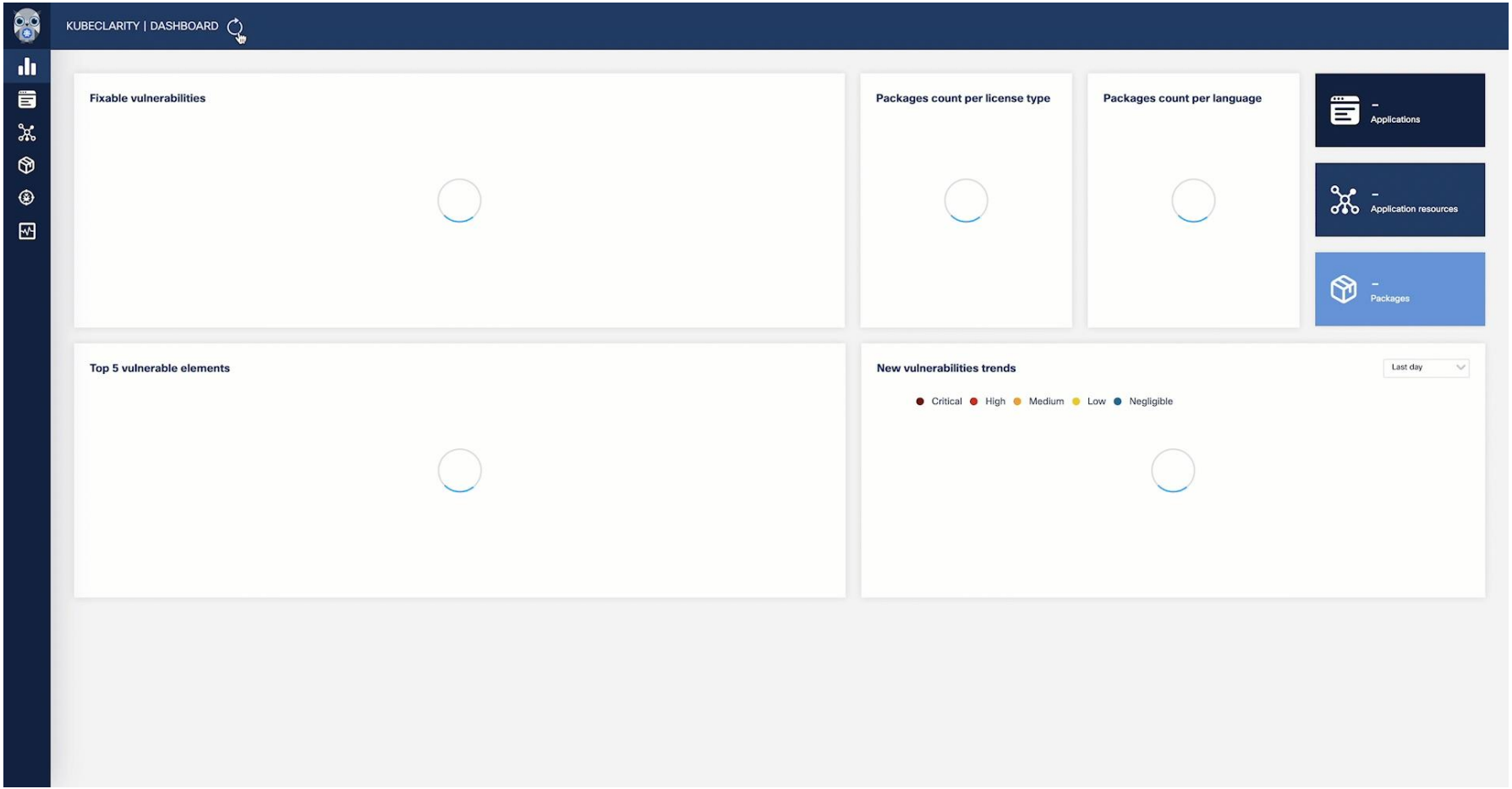
KubeClarity

KubeClarity is a tool for detecting and managing Software Bill Of Materials (SBOM) and vulnerabilities of container images and filesystems. It scans runtime Kubernetes clusters and CI/CD pipelines to enhance software supply chain security.

Vulnerabilities scans

KubeClarity was the first OSS for runtime scanner
Scanning containers images which are used in the cluster (instead of full registry scan)

- Vulnerabilities scans for Containers(images) and Serveless(source-code)
- Creating Software Bill of Material (SBOM) for scanned target
- Enabling multi-scanner option (OSS or paid scanners)
- Adding SBOM attestation metadata
- Adding a "sign" option to scanned images/functions in the CI (similar to Tekton Chains)
  Outcome: The first Universal-Scanner for vulnerabilities and SBOM signing



Integration

KubeClarity integrated into the Code Exchange submission workflow. Once we have evaluated a new use case submission, we send all analytics and security reports to the submitter.

severity	name	installed	fixed-in	path	vulnerability	description
MEDIUM	paramiko	2.6.0		ansible/requirements.txt	CVE-2022-24302	In Paramiko before 2.10.1, a race condition (between creation and chmod) in the write_private_key_file function could allow unauthorized information disclosure.
HIGH	ansible	2.10.7	4.2.0	ansible/requirements.txt	GHSA-2pfh-q76x-gwvm	A flaw was found in Ansible, where a user's controller is vulnerable to template injection. This issue can occur through facts used in the template if the user is trying to put tem perform command injection, which discloses sensitive information. The highest threat from this vulnerability is to confidentiality and integrity.
HIGH	lxml	4.6.3	4.6.5	ansible/requirements.txt	GHSA-55x5-fj6c-h6m8	lxml is a library for processing XML and HTML in the Python language. Prior to version 4.6.5, the HTML Cleaner in lxml.html lets certain crafted script content pass through, as v to lxml 4.6.5 to receive a patch. There are no known workarounds available.
HIGH	pycrypto	2.6.1		ansible/requirements.txt	GHSA-6528-wvf6-f6qg	lib/Crypto/PublicKey/ElGamal.py in PyCrypto through 2.6.1 generates weak ElGamal key parameters, which allows attackers to obtain sensitive information by reading cipherte hold for PyCrypto's ElGamal implementation.
CRITICAL	pycrypto	2.6.1		ansible/requirements.txt	GHSA-cq27-v7xp-c356	Heap-based buffer overflow in the ALGnew function in block_templace.c in Python Cryptography Toolkit (aka pycrypto) allows remote attackers to execute arbitrary code as de
HIGH	lxml	4.6.3	4.9.1	ansible/requirements.txt	GHSA-wrxv-2j5q-m38w	NULL Pointer Dereference allows attackers to cause a denial of service (or application crash). This only applies when lxml is used together with libxml2 2.9.10 through 2.9.14. lib application. The vulnerability is caused by the iterwalk function (also used by the canonicalize function). Such code shouldn't be in wide-spread use, given that parsing + iterwal vulnerable, for example, and there are legitimate use cases for this code sequence. If untrusted input is received (also remotely) and processed via iterwalk function, a crash ca
HIGH	lxml	4.6.3		ansible/requirements.txt	CVE-2021-43818	lxml is a library for processing XML and HTML in the Python language. Prior to version 4.6.5, the HTML Cleaner in lxml.html lets certain crafted script content pass through, as v to lxml 4.6.5 to receive a patch. There are no known workarounds available.
HIGH	lxml	4.6.3		ansible/requirements.txt	CVE-2022-2309	NULL Pointer Dereference allows attackers to cause a denial of service (or application crash). This only applies when lxml is used together with libxml2 2.9.10 through 2.9.14. lib application. The vulnerability is caused by the iterwalk function (also used by the canonicalize function). Such code shouldn't be in wide-spread use, given that parsing + iterwal vulnerable, for example, and there are legitimate use cases for this code sequence. If untrusted input is received (also remotely) and processed via iterwalk function, a crash ca

Bank vaults

Bank vaults

A Vault swiss-army knife: a K8s operator, Go client with automatic token renewal, automatic configuration, multiple unseal options and more. A CLI tool to init, unseal and configure Vault (auth methods, secret engines). Direct secret injection into Pods.

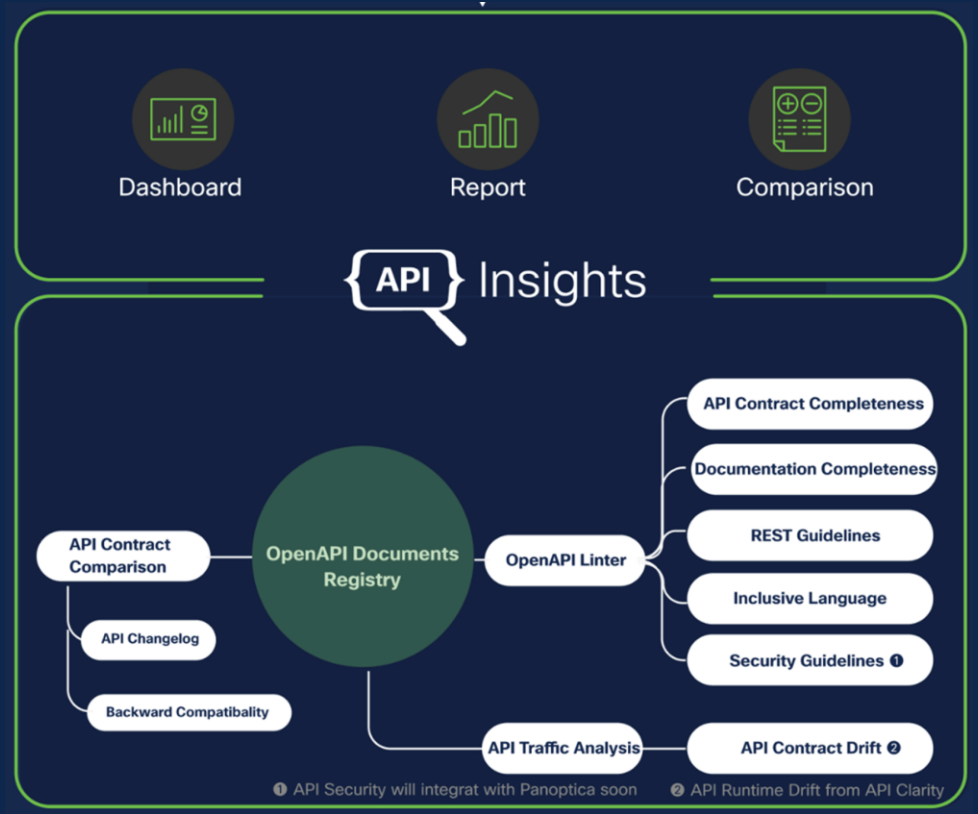
Bank-Vaults is an umbrella project which provides various tools for Vault to make using and operating Hashicorp Vault easier. It's a wrapper for the official Vault client with automatic token renewal and built-in Kubernetes support, dynamic database credential provider for Golang database/sql based clients. It has a CLI tool to automatically initialize, unseal, and configure Vault. It also provides a Kubernetes operator for provisioning, and a mutating webhook for injecting secrets.

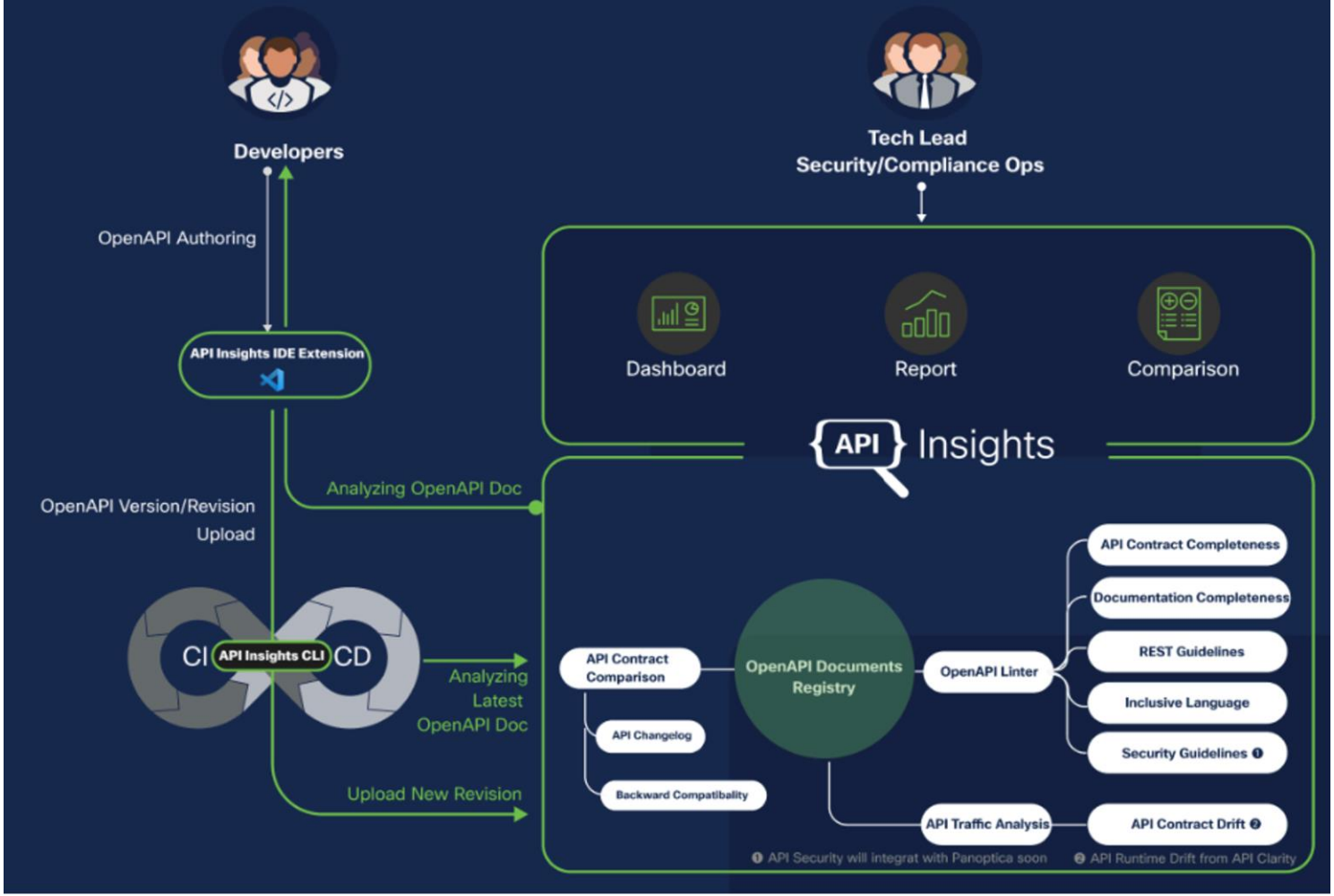
Banzai Cloud
Bank-Vaults

API Insights

API Insights

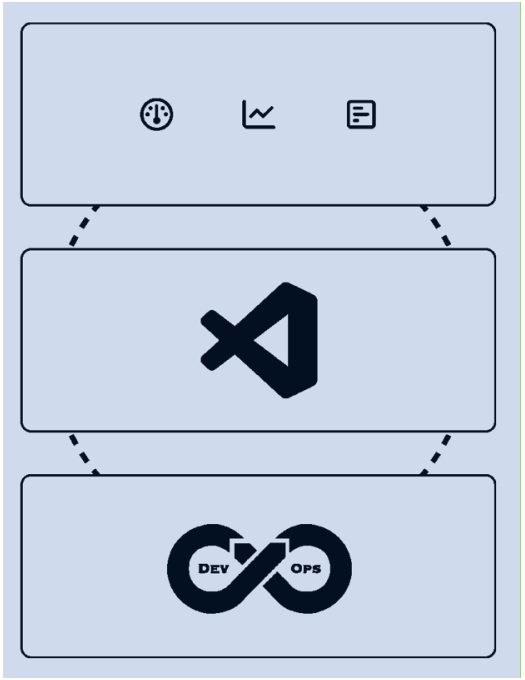
- ✓Score API contracts and documentation
- ✓Check adoption of REST design conventions
- ✓Detect offensive terms
- ✓Generate changelogs for new API releases
- ✓Spot breaking changes to ensure backward compatibility





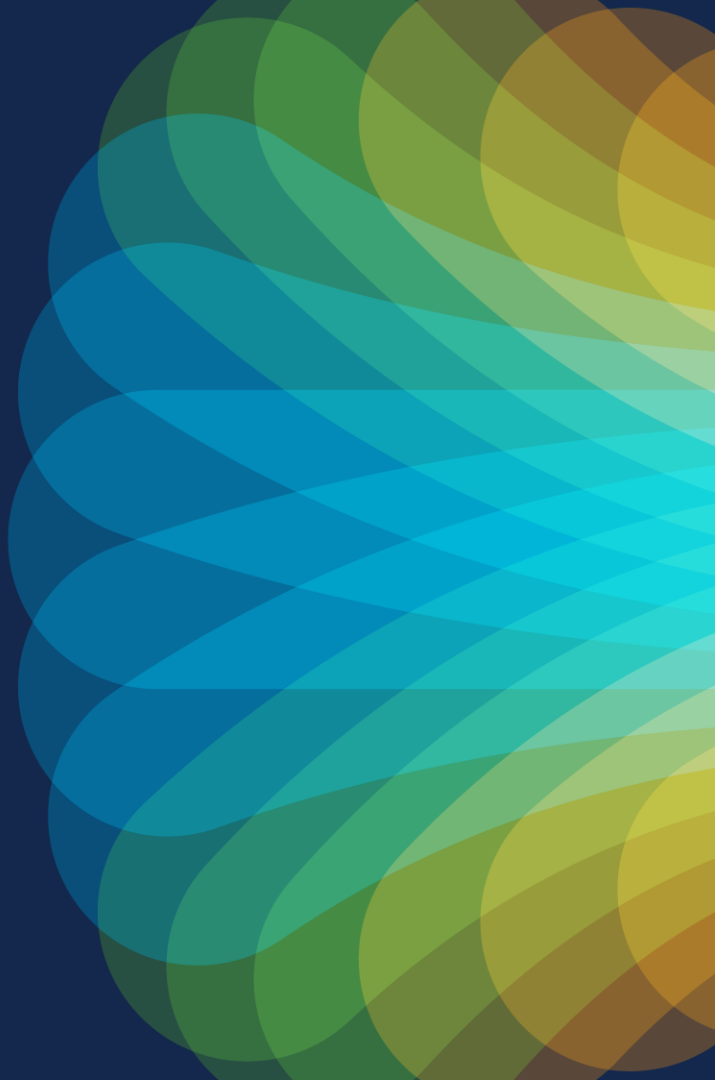
How to use?

- *API Compliance and Lifecycle Dashboard*
- *VS Code IDE Extension*
- *CLI Integration with CI/CD pipeline*



Demo

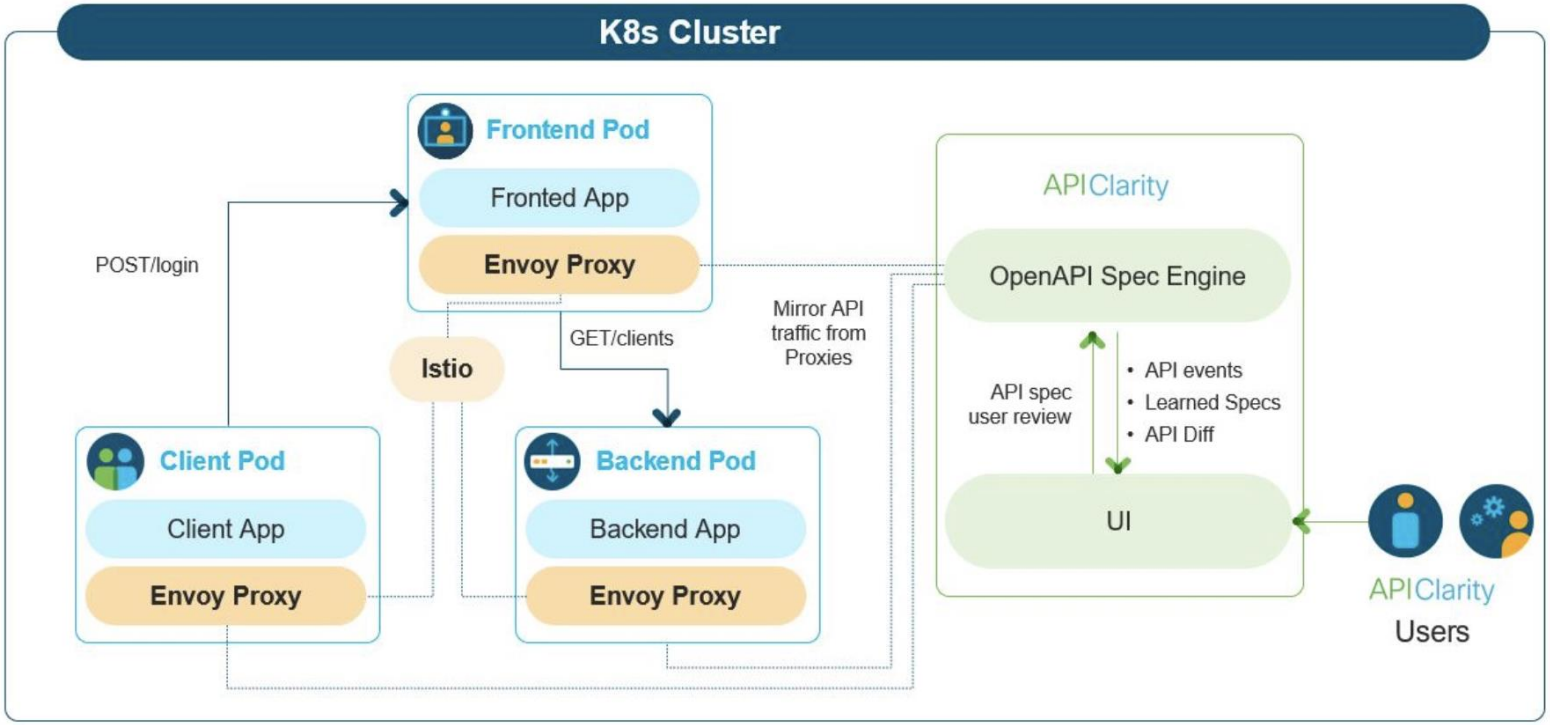
API Clarity



API Clarity

- Capture all API traffic in an existing environment using a service-mesh framework.
- Construct the OpenAPI specification by observing the API traffic.
- Allow the User to upload OpenAPI specs, review, modify and approve generated OpenAPI specs.
- Alert the User on any difference between the approved API specification and the one that is observed in runtime, detects shadow & zombie APIs
- UI dashboard to audit and monitor the API findings

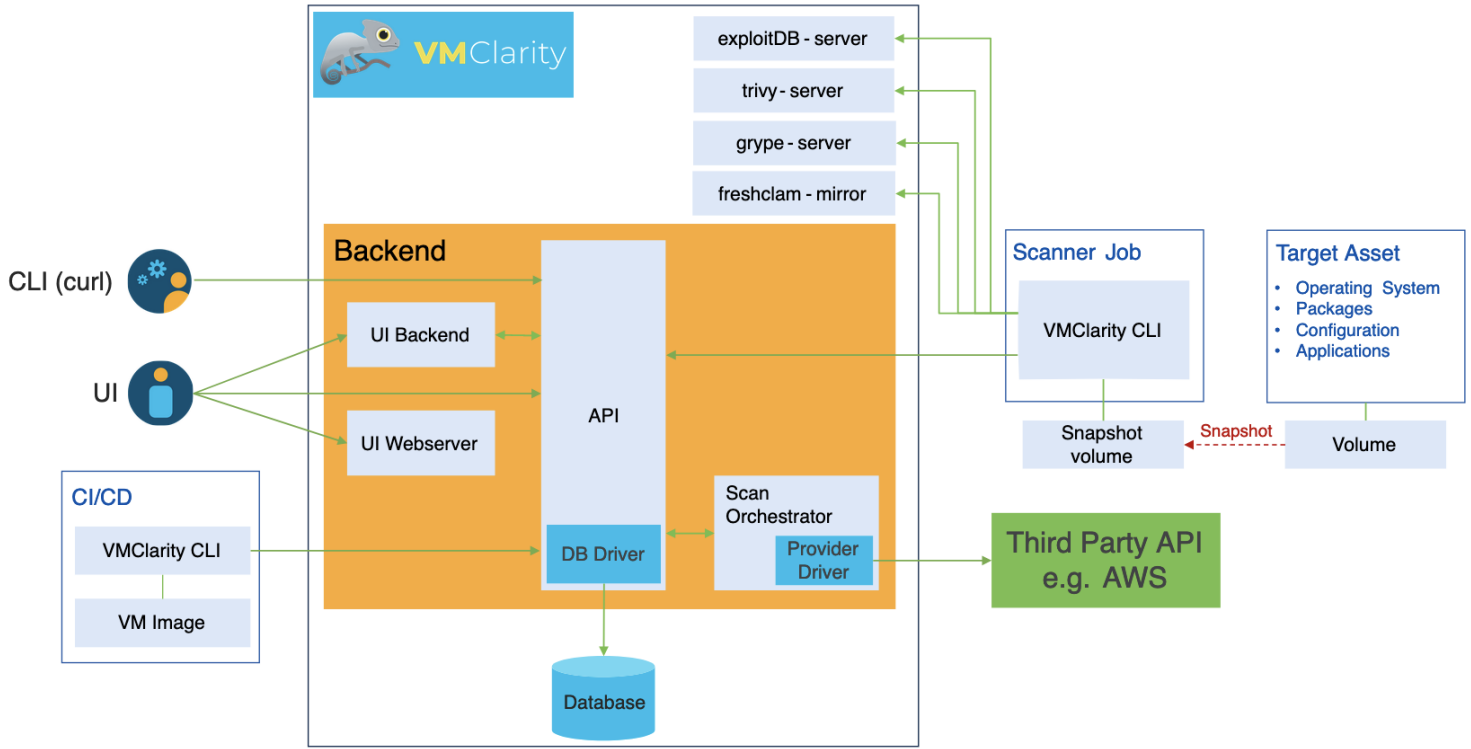
High level architecture



VMClarity

VMClarity is an open source tool for agentless detection and management of Virtual Machine Software Bill Of Materials (SBOM) and security threats such as vulnerabilities, exploits, malware, rootkits, misconfigurations and leaked secrets.

VMClarity



Links

- https://github.com/openclarity/kubeclarity
- https://github.com/banzaicloud/bank-vaults
- https://github.com/cisco-developer/api-insights
- https://github.com/openclarity/apiclarity
- https://github.com/openclarity/vmclarity

Fill out your session surveys!

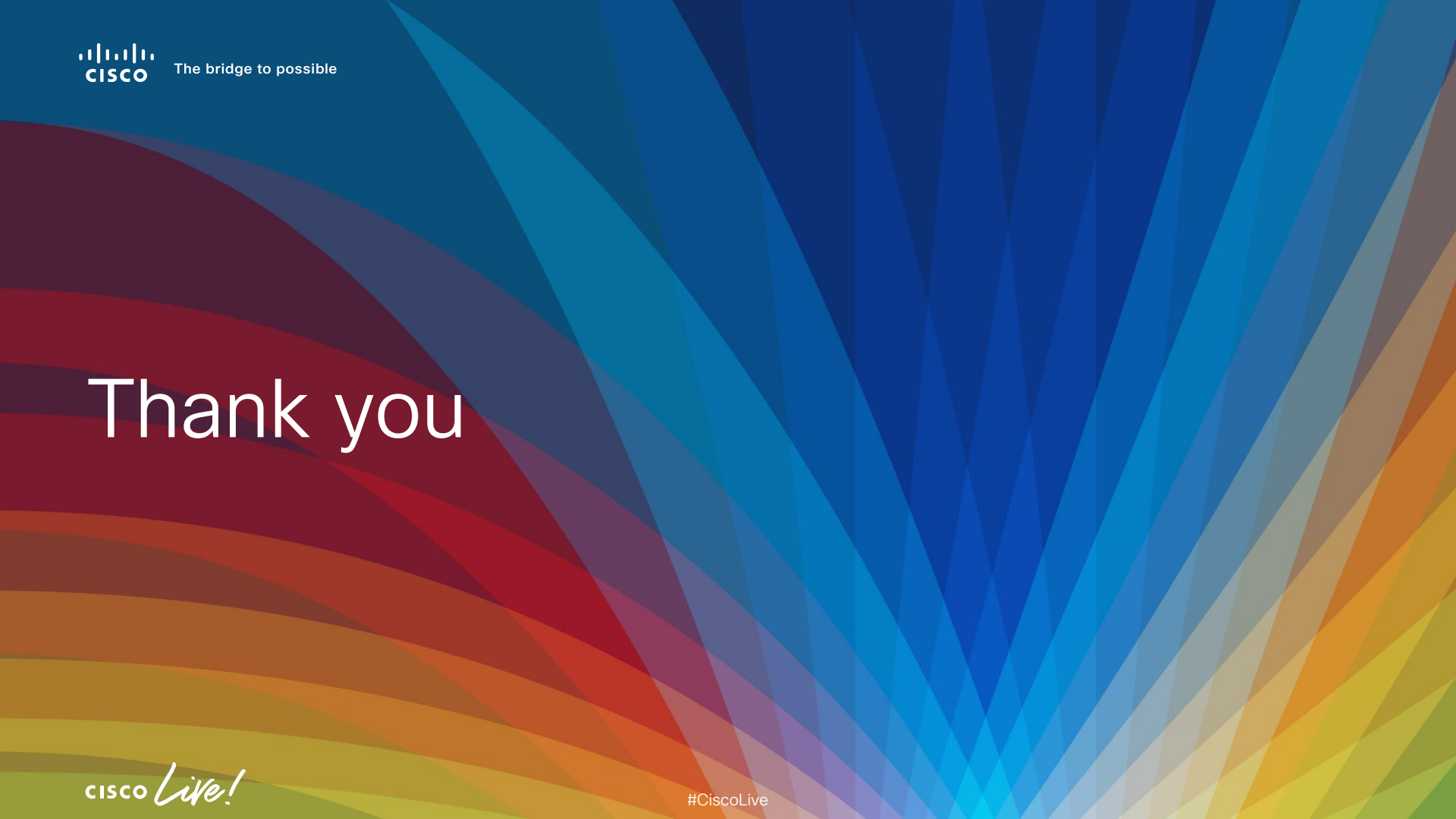
Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!

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


cisco
The bridge to possible
Thank you
cisco Live!
#CiscoLive

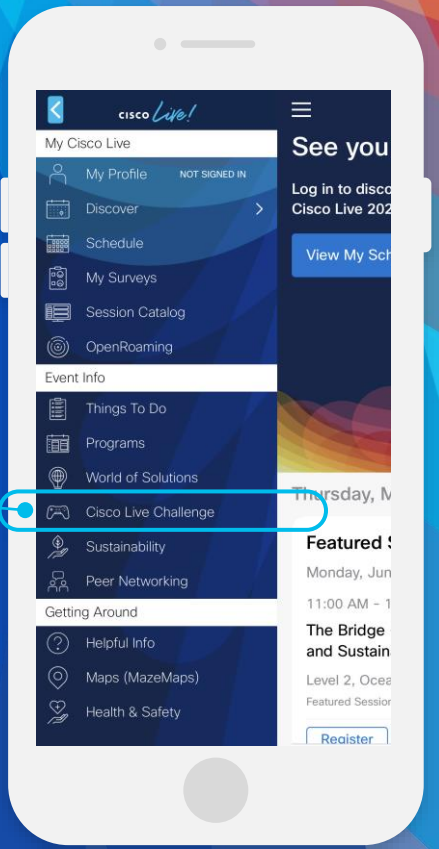
Cisco Live
Challenge

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!
Let's go
#CiscoLive