cisco Live!

Let's go

The bridge to possible

How to Simplify Cloud Native Security in a Hybrid Cloud Environment

Chris Taylor, Principal Security Engineer
CISSP, CCSP #670647
@chtaylo2

BRKCLD-2741

Cisco Webex App

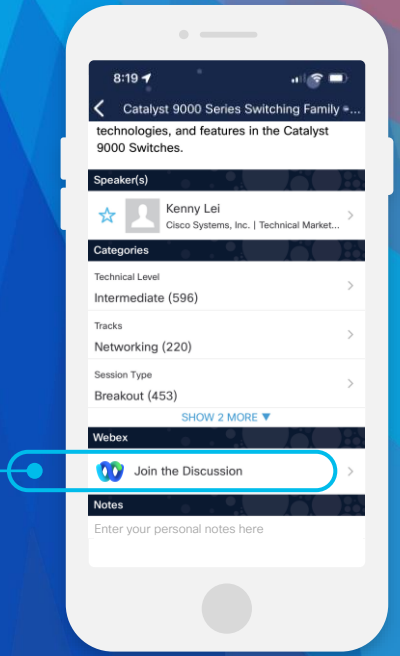
Questions?

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/#BRKCLD-2741

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Please fill out the session survey

Include your email in comments, I'll be sure to respond!

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Agenda

- Introduction
- State of cloud native security
- Secure Containers and code
- Secure Kubernetes (K8s) Clusters
- API Security
- Conclusion

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Who we are – Cisco IT

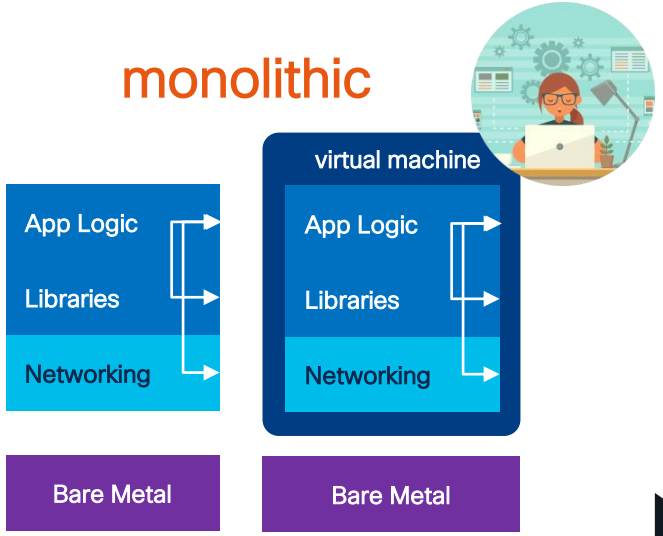
- Cisco IT is customer zero. aka Cisco-on-Cisco

- Cisco IT – Hybrid Cloud environment supporting global clients within Cisco
- On premise running OpenShift, Anthos, K8s, OpenStack, VMWare, Bare Metal
- Public cloud using AWS, GCP, Azure

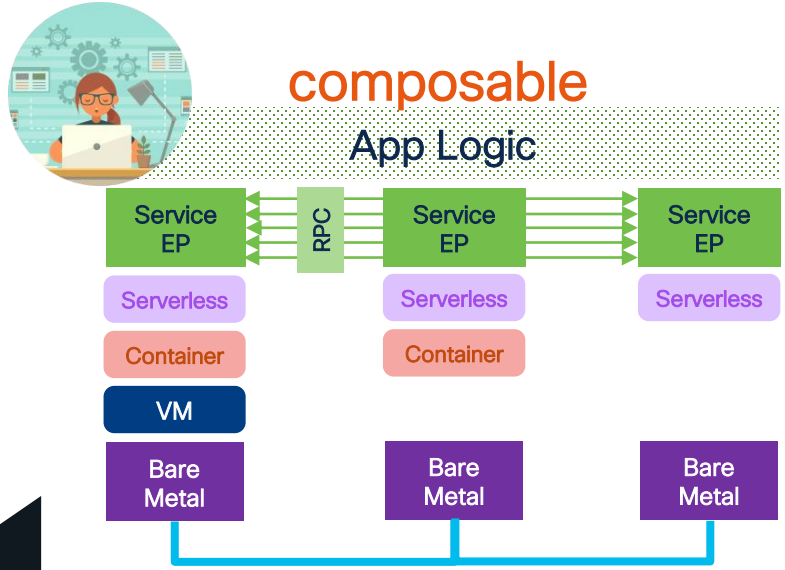
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

State of Cloud Native Security

monolithic

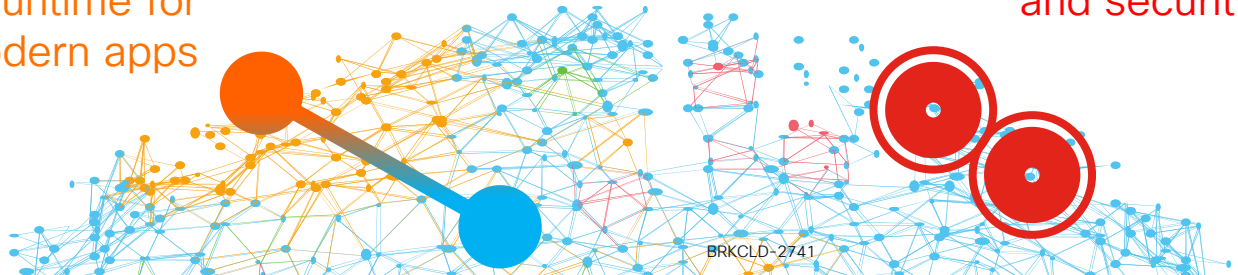


composable

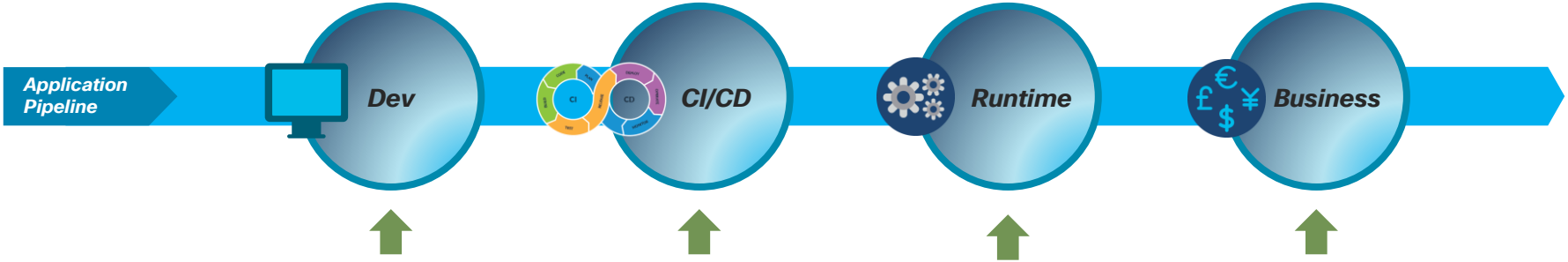


The wide-open Internet is the new runtime for modern apps

The new perimeter of apps and security is diffuse



Application Development Lifecycle



Variety of tools

*Variety of **Application frameworks** for VMs, Containers, Serverless, APIs*

*Lack of **consistency** for **visibility & Security***

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

And the implications couldn't be greater. The longer a vulnerability exists, the more it impacts the bottom line!

93% Of security teams have experienced incident in K8s environment over last 12 months.

Source: RedHat State of Container and Kubernetes Security Report 2022

280+ Average time to identify and contain a data breach

Source: Ponemon Institute 2020

47% Security pros have nothing in place to secure cloud native and serverless

Source: GitLab. 2021 Global DevSecOps Survey

$8.6M (US)
$3.8M (Global)
Average direct cost to contain a data breach

Source: Ponemon Institute 2020

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Top concerns for cloud native application

1 How do we embed security into the software development process?

(AppSec, DevSecOps)

2 What are the hidden vulnerabilities in those components?

3 Can we identify and scan all external APIs consumed automatically?

4 Can we do this with a Single tool across Development & Runtime ?

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Introducing: Panoptica Cloud Native Security

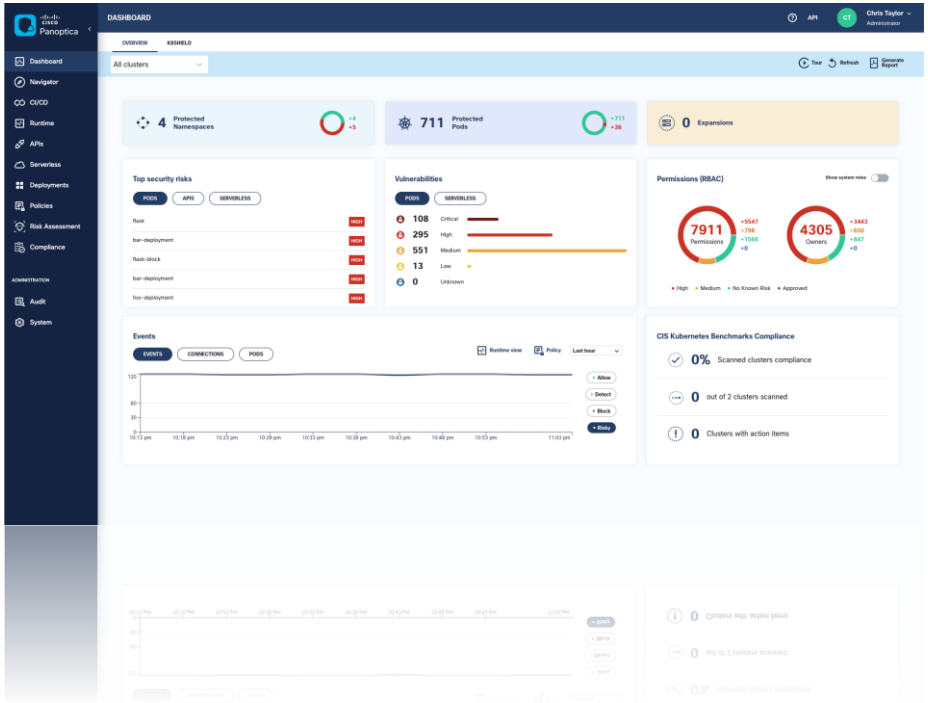
A holistic portal for all things cloud-native app security

Inventory all artifacts of the applications and its vulnerabilities

Control container, images, Software Bill of Materials (SBOM), supply chain, serverless and APIs

Manage the risks through a MITRE ATT&CK® framework

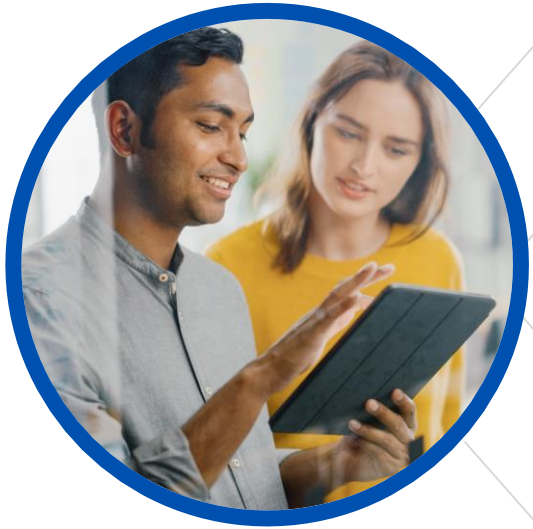
Define and enforce security policies and compliance for the enterprise



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

The Container, fundamental building block for modern applications

Container Security: Our Needs?



- Gain insight on the building blocks of applications, from code to production
- Detect the vulnerable building blocks of my software, even if discovered post deployment
- Correlate vulnerable building blocks across my applications
- Remediation of my applications following a discovered vulnerability

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Panoptica adds Security to CI Pipelines

- Scans Docker images for known vulnerabilities / CIS Benchmarks
- Detect exposed secrets/passwords/keys
- Generate a unique identity for each pod (drift protection)
- Scan results available in CLI output and Panoptica GUI
- Risk based policies which can reject build pipelines upon violation
- Simple failure reasons/fix options which can be actioned by developers

CircleCI Jenkins GitLab TEKTON docker

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Panoptica – Container Image Vulnerability Scan

```
sh-3.2$: securecn_deployment_cli run-vulnerability-scan --access-key $ACCESS_KEY --secret-key $SECRET_KEY --
image-name=nginx:1.22.0

PACKAGE NAME       PACKAGE VERSION          FIXED IN VERSION         VULNERABILITY     SEVERITY
curl               7.74.0-1.3+deb11u3       7.74.0-1.3+deb11u5       CVE-2022-32221    CRITICAL
libcurl4           7.74.0-1.3+deb11u3       7.74.0-1.3+deb11u5       CVE-2022-32221    CRITICAL
libtasn1-6         4.16.0-2                 4.16.0-2+deb11u1         CVE-2021-46848    CRITICAL
openssl            1.1.1n-0+deb11u3         1.1.1n-0+deb11u4         CVE-2023-0215     HIGH
libkrb5-3          1.18.3-6+deb11u2         1.18.3-6+deb11u3         CVE-2022-42898    HIGH
libkrb5support0    1.18.3-6+deb11u2         1.18.3-6+deb11u3         CVE-2022-42898    HIGH
libssl1.1          1.1.1n-0+deb11u3         1.1.1n-0+deb11u4         CVE-2023-0286     HIGH
libssl1.1          1.1.1n-0+deb11u3         1.1.1n-0+deb11u4         CVE-2023-0215     HIGH
libssl1.1          1.1.1n-0+deb11u3         1.1.1n-0+deb11u4         CVE-2022-4450     HIGH
libtiff5           4.2.0-1+deb11u1          4.2.0-1+deb11u3          CVE-2022-3970     HIGH
libxml2            2.9.10+dfsg-6.7+deb11u2  2.9.10+dfsg-6.7+deb11u3  CVE-2022-40303    HIGH
libxml2            2.9.10+dfsg-6.7+deb11u2  2.9.10+dfsg-6.7+deb11u3  CVE-2022-40304    HIGH
libcurl4           7.74.0-1.3+deb11u3       7.74.0-1.3+deb11u7       CVE-2023-23916    HIGH
libexpat1          2.2.10-2+deb11u4         2.2.10-2+deb11u5         CVE-2022-43680    HIGH
…


Total vulnerabilities: 201 (8 Critical, 44 High, 56 Medium, 85 Low, 8 Unknown)

FATAL[2023-04-17T19:48:10Z] Scan result: The highest severity allowed by policy is HIGH but vulnerabilities
with CRITICAL severity were found
```


© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Vulnerability Scan

CI/CD

API

Chris Taylor
Administrator

Images

docker.io/library/nginx

Image Hash: f0d28f2047853cbc10732d6eaa1b57f1f4db9b017679b9fd7966b6a2f9ccc2d1
Image Tags: 1.22.0

VULNERABILITIES | IMAGE LAYERS | CIS BENCHMARK | PACKAGES & LICENSES | EXPOSURE

Active only | Acknowledged only

Image layer: Select...
Fixable only: No

Acknowledge | Refresh | Columns

FINDINGS	NAME	FIX AVAILABILITY	DESCRIPTION
9.8 critical	CVE-2022-32221	Fix available	When doing HTTP(S) transfers, libcurl might erroneously use the read callback (`CURLOPT_READFUNCTION`) to ask for data to send, even when the `CURLOPT_POSTFIELDS` option has been set, if the same handle previously was used to issue a `PUT` request which used that callback. This flaw may surprise the application and cause it to misbehave and either send off the wrong data or use memory after free or similar in the subsequent `POST` request. The problem exists in the logic for a reused handle when it is changed from a PUT to a POST.
9.1 critical	CVE-2021-46848	Fix available	GNU Libtasn1 before 4.19.0 has an ETYPE_OK off-by-one array size check that affects asn1_encode_simple_der.
8.8 high	CVE-2022-3970	Fix available	A vulnerability was found in LibTIFF. It has been classified as critical. This affects the function TIFFReadRGBATileExt of the file libtiff/tif_getimage.c. The manipulation leads to integer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The name of the patch is 227500897dfb07fb7d27f7aa570050e62617e3be. It is recommended to apply a patch to fix this issue. The identifier VDB-213549 was assigned to this vulnerability.
7.5 high	CVE-2023-2004	No fix is currently available	An integer overflow vulnerability was discovered in Freetype in tt_hvadvance_adjust() function in src/truetype/ttgxvar.c.
7.5 high	CVE-2021-33560	No fix is currently available	Libgcrypt before 1.8.8 and 1.9.x before 1.9.3 mishandles ElGamal encryption because it lacks exponent blinding to address a side-channel attack against mpi_powm, and the window size is not chosen appropriately. This, for example, affects use of ElGamal in OpenPGP.
7.5 high	CVE-2022-43680	Fix available	In libexpat through 2.4.9, there is a use-after free caused by overeager destruction of a shared DTD in XML_ExternalEntityParserCreate in out-of-memory situations.
7.8 high	CVE-2022-1304	No fix is currently available	An out-of-bounds read/write vulnerability was found in e2fsprogs 1.46.5. This issue leads to a segmentation fault and possibly arbitrary code execution via a specially crafted filesystem.
7.5 high	CVE-2023-0361	Fix available	A timing side-channel in the handling of RSA ClientKeyExchange messages was discovered in GnuTLS. This side-channel can be sufficient to recover the key encrypted in the RSA ciphertext across a network in a Bleichenbacher style attack. To achieve a successful decryption the attacker would need to send a large amount of specially crafted messages to the vulnerable server. By recovering the secret from the

PAGE 1

50 | 100 | 200 PER PAGE

CIS Benchmark Scan

CI/CD

API

Chris Taylor
Administrator

Images

docker.io/library/nginx

Image Hash: f0d28f2047853cbc10732d6eaa1b57f1f4db9b017679b9fd7966b6a2f9ccc2d1
Image Tags: 1.22.0

VULNERABILITIES | IMAGE LAYERS | CIS BENCHMARK | PACKAGES & LICENSES | EXPOSURE

Active only | Acknowledged only

Ignore | Refresh | Columns

NAME	TITLE	FINDINGS	DESCRIPTION
CIS-DI-0001	Create a user for the container	Warning	Last user should not be root
CIS-DI-0005	Enable Content trust for Docker	Info	export DOCKER_CONTENT_TRUST=1 before docker pull/build
CIS-DI-0006	Add HEALTHCHECK instruction to the container image	Info	not found HEALTHCHECK statement
CIS-DI-0008	Confirm safety of setuid/setgid files	Info	setgid file: grwxr-xr-x usr/bin/wall, setuid file: urwxr-xr-x usr/bin/chsh, setuid file: urwxr-xr-x usr/bin/passwd, setgid file: grwxr-xr-x usr/bin/chage, setuid file: urwxr-xr-x bin/mount, setuid file: urwxr-xr-x bin/su, setuid file: urwxr-xr-x usr/bin/newgrp, setuid file: urwxr-xr-x usr/bin/chfn, setuid file: urwxr-xr-x bin/umount, setgid file: grwxr-xr-x sbin/unix_chkpwd, setuid file: urwxr-xr-x usr/bin/gpasswd, setgid file: grwxr-xr-x usr/bin/expiry

PAGE 1

50 | 100 | 200 PER PAGE

ADMIN

CI/CD

API

Chris Taylor
Administrator

Images

SBOM View

docker.io/library/nginx

Image Hash: f0d28f2047853cbc10732d6eaa1b57f1f4db9b017679b9fd7966b6a2f9ccc2d1
Image Tags: 1.22.0

VULNERABILITIES | IMAGE LAYERS | CIS BENCHMARK | PACKAGES & LICENSES | EXPOSURE

Active only — Acknowledged only

NAME	LICENSES	VERSION
ncurses-base	BSD-3-Clause, X11	6.2+20201114-2
libcom-err2		1.46.2-2
debianutils	GPL-2.0-only	4.11.2
libffi7		3.3-6
libxxhash0	BSD-2-Clause, GPL-2.0-only	0.8.0-2
libpcre3		2:8.39-13
gcc-9-base	LGPL-2.1-or-later, GFDL-1.2-only, GPL-2.0-only, GPL-3.0-only	9.3.0-22
logsave	LGPL-2.0-only, GPL-2.0-only	1.46.2-2
libaudit-common	GPL-1.0-only, LGPL-2.1-only, GPL-2.0-only	1:3.0-2
libintl		0.21
libxml2	ISC	2.9.10+dfsg-6.7+deb11u2
nginx-module-xslt		1.22.0-1~bullseye
libxslt1.1		1.1.34-4+deb11u1
libpam-modules-bin		1.4.0-9+deb11u1
fontconfig-config		2.13.1-4.2
libjbig0	GPL-2.0-or-later, GPL-2.0-only	2.1-3.1+b2
tar	GPL-2.0-only, GPL-3.0-only	1.34+dfsg-1
libunistring2	LGPL-3.0-only, GPL-3.0-or-later, MIT, GPL-2.0-or-later, GFDL-1.2-only, GPL-2.0-only, GPL-3.0-only, LGPL-3.0-or-later	0.9.10-4
openssl		1.1.1n-0+deb11u3
debconf	BSD-2-Clause	1.5.77
tzdata		2021a-1+deb11u6
sensible-utils	GPL-2.0-or-later, GPL-2.0-only	0.0.14

Panoptica adds Security to CD Pipelines

- Scans deployment files (HELM, Terraform etc.) detecting potential risks prior to their deployment
- Kubernetes roles and role binding (detect overly permissive roles)
- Security Context:
  - Root, Privileged containers
  - Privileges escalations
  - Host path or sensitive volumes mount
- Exposed credentials, passwords, certifications, and tokens
- Secure App Cloud allow users to apply security policies on their deployments automatically during the CD/GitOps phase

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Secure Application Cloud scanning helm deployments

```
sh-3.2$ helm securecn --command 'install tomcat bitnami/tomcat' --access-key $ACCESS_KEY --
secret-key $SECRET_KEY --controller-secret-key $CONTROLLER_SECRET_KEY --run-security-check

Risk assessment for DEPLOYMENT tomcat:

Risk: HIGH

Category: SECURITY_CONTEXT

Reasons:

1. Allowing privileges escalation on the container, allow attacker to escalate its
privileges to privileged or root if they're not granted originally


sh-3.2$ helm list

NAME    NAMESPACE      REVISION     STATUS      CHART              APP VERSION

tomcat  tomcat         1            deployed    tomcat-10.1.15    10.0.18
```


© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Kubernetes Cluster runtime policies

Panoptica – Runtime Policies

Secure App Cloud

CI/CD Policies
- Vulnerability Level
- Dockerfile Severity

Deployment Rules
- API Policies
- Pod Sec Profile
- Vulnerability Level

Connection Rules
- API Policies
- L7 Policies
- Encryption Policies
- Vulnerability Level

Cluster Events Rules
- RBAC Controls
- Custom API Controls

Serverless Policies
- Vulnerability Level
- Accessibility

- Controls image build and K8s deployments
- Utilizes K8s Admission Controller / Validating Webhook

- Secures comm. across K8s workloads
- Uses Integrated Service Mesh

- Govern K8s control plane actions
- Utilizes K8s native RBAC controls

- Scanning serverless functions
- Define access based on risk

Filter Policies

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Panoptica – Cisco IT Curated Set of Policies

CI/CD Policies

- Vulnerable Image – Disable storage with Critical finding
- Dockerfile Scan – Issue warning on High finding

Connection Rules

- Vulnerable Pods – Connections from external env to Pod with CRITICAL finding
- Encrypt POD to POD traffic in production environment

Deployment Rules

- Unidentified workload cannot run in the environment
- Vulnerable Pods – Block pods running in specific environments
- Deploy containers from only trusted registries

Cluster Events Rules

- Prevent workload modification
- Prevent Cluster admin binding
- Prevent interactive exec
- Prevent defense evasion
- Prevent K8s secret modification

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Developer First – Policy Automation

- Programmatically build policies applicable to their applications from within Terraform, Helm Charts enabling GitOps
- Across Deployment Rules, Connection Rules, Cluster Events, API Policies…

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Integrated Service Mesh

POLICIES

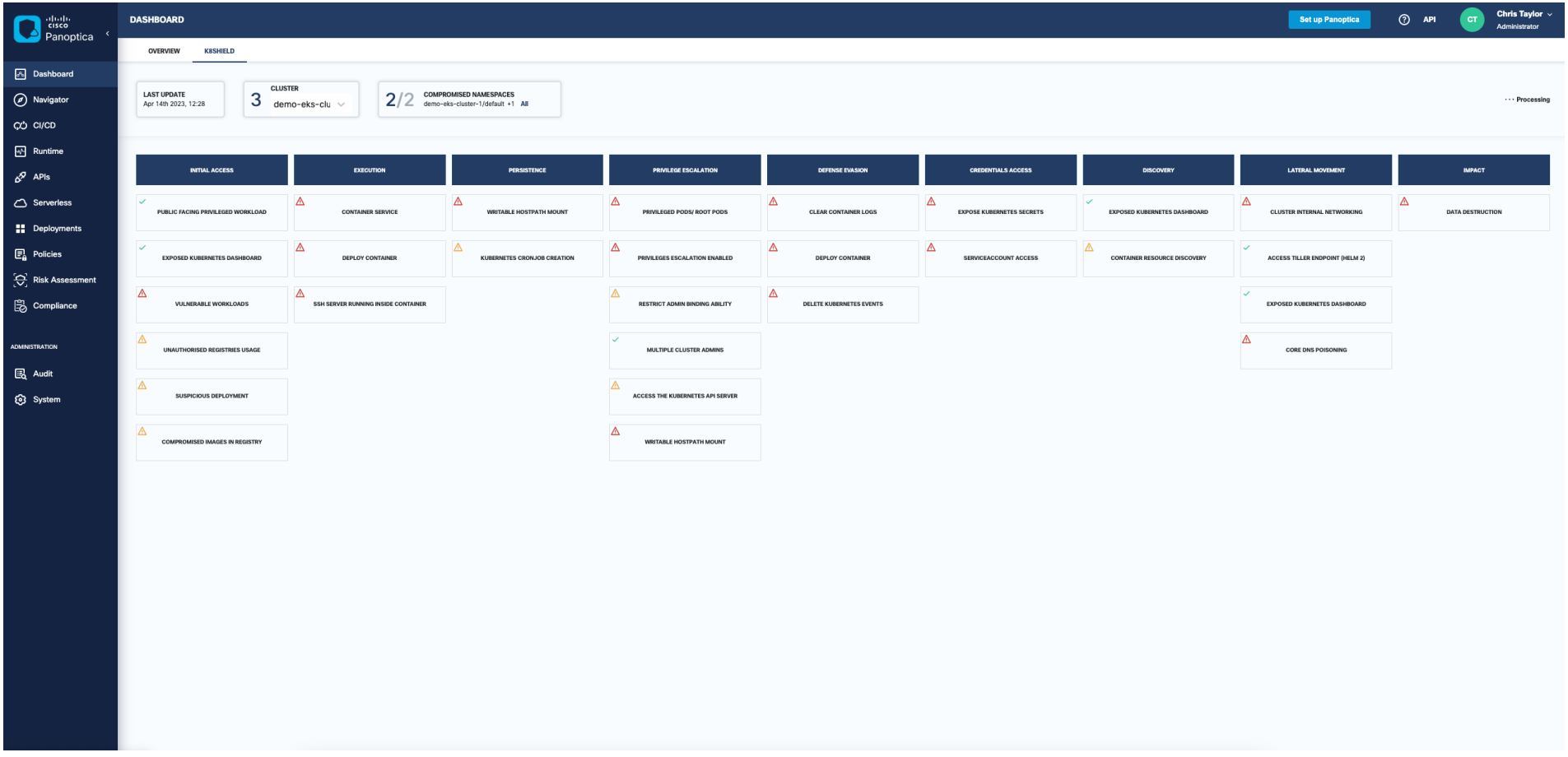
DEPLOYMENT RULES | CONNECTION RULES | CLUSTER EVENTS RULES | POD STANDARDS | CI/CD POLICY | API POLICIES

+ New Connection rule | New Encryption rule | Edit default rule | Search for Deployment/Pod | Collapse all | Expand all

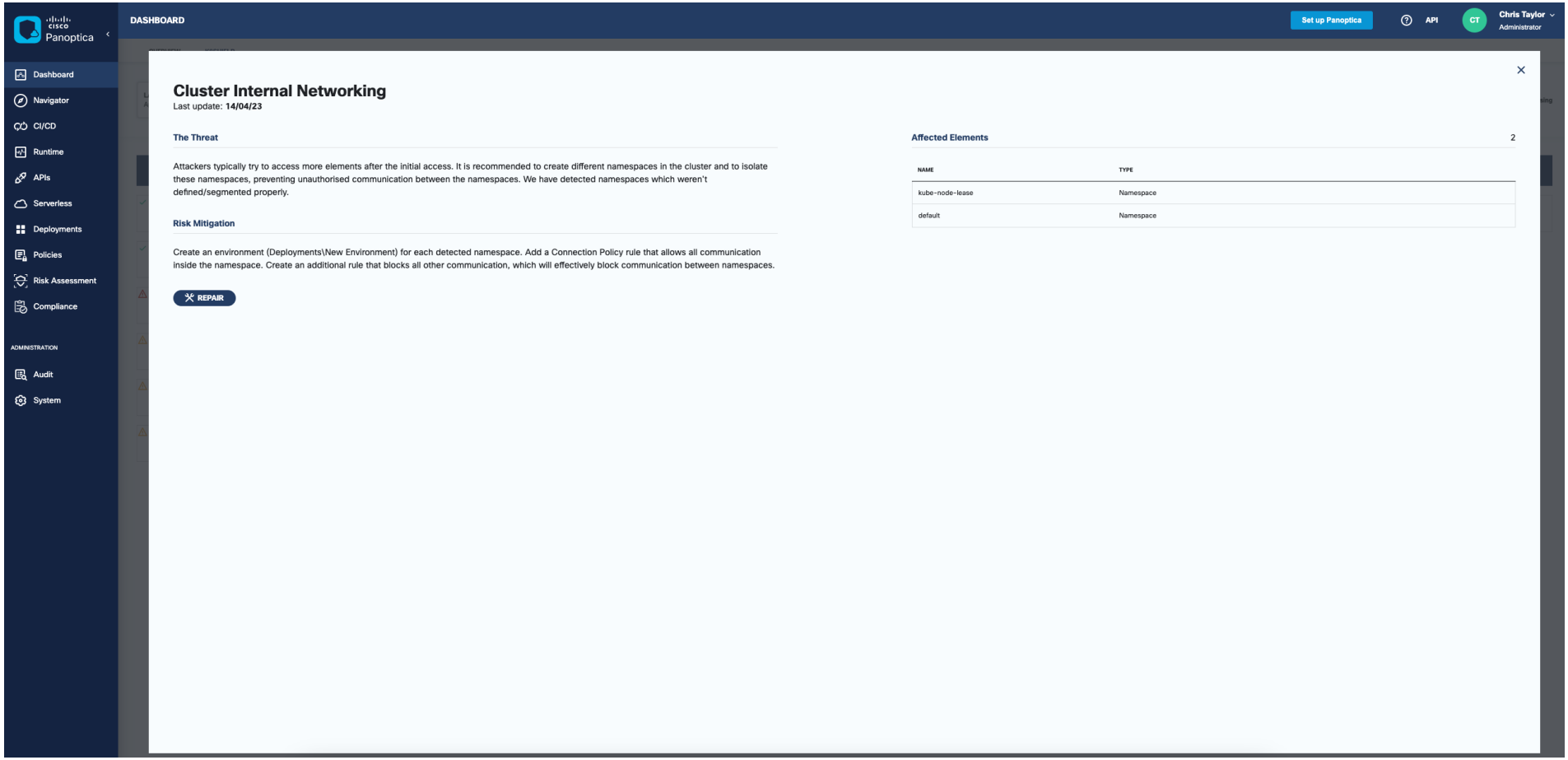
Connection to Kafka Broker	**billing pod** and **mail-sender pod** on **Prod** can communicate with Kafka brokers: **kafka**
Encrypt production	Connections from workloads that are deployed on **Prod** or **Finance** to workloads that are deployed on **Prod** or **DB** are encrypted
Detect Layer 7	**Any pod** can't communicate with **any pod** with **/application** path using **GET** and **POST** methods

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

MITRE ATT&CK® framework



MITRE ATT&CK® framework



APIs – The “glue” of modern applications.

API Security top asks

1 What internal APIs do our apps use? What external APIs do they consume from 3rd parties?

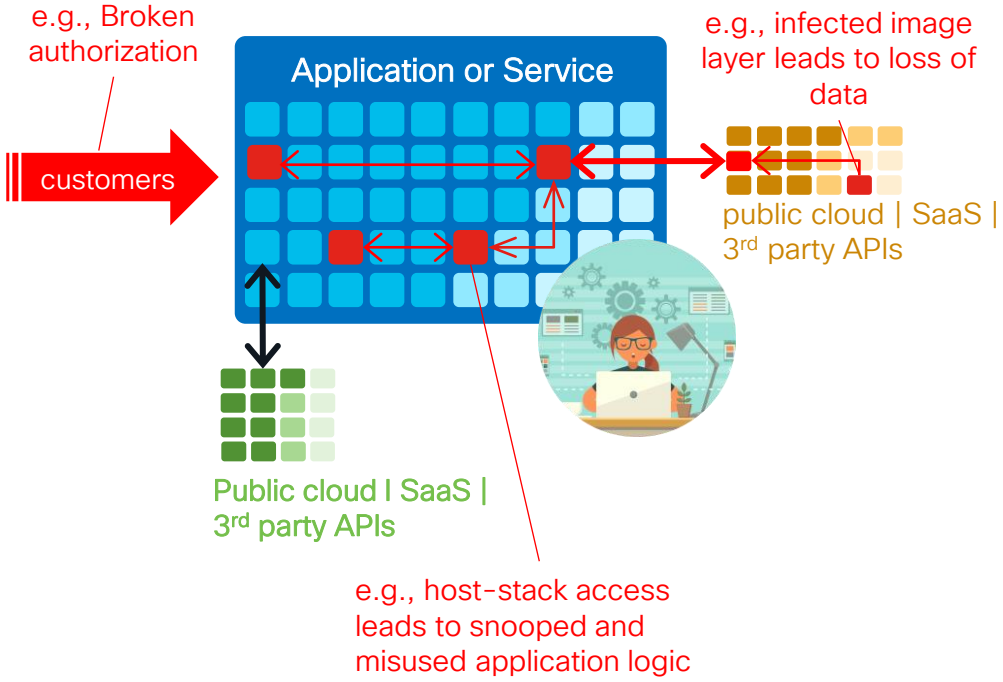
2 What are the specifications of our internal and external APIs? Are they (well) documented?

3 Is proper authentication and authorization in place?

4 Are API backend implementations compliant and secure?

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

A few examples on API security challenges



- Quality and security of services is often unknown
- Shadow and Zombie API detection
- Puts customer data and enterprise at risk when interacting with App
- Hard to detect Broken Function Level Auth (BFLA) vulnerabilities with Web App Firewall (WAF) and API Gateway

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

API Security starts from the specs…

- Captures and displays all API traffic from a service mesh or API Gateways
- Reconstructs OpenAPI specifications and allows user to review and approve them
- Allows user to provide «official» OpenAPI specifications and to compare them with those reconstructed.
- Monitor differences and track spec drift over time detecting zombie and shadow APIs

… having clarity on the APIs and their specs is just the first step!

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

API Security is extended with a set of security modules

Trace Analysis

- Discover weak authentications and insecure API practices

BFLA

- Tracks users and client pods to detect broken authorization procedures

Testing/Fuzzing

- Actively tests API endpoints to discover insecure implementations

Stats

- Tracking API performance
- Detect Anomalies

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Panoptica

APIS

Set up Panoptica | API | CT | Chris Taylor, Administrator

- Dashboard
- Navigator
- CI/CD
- Runtime
- APIs
- Serverless
- Deployments
- Policies
- Risk Assessment
- Compliance

ADMINISTRATION

- Audit
- System

DASHBOARD | RISK FINDINGS | INTERNAL APIS | THIRD PARTY APIS | TOKENS | GATEWAYS | API POLICY PROFILE

+ New API

API name: github.com

Policy compliance: Select...

Refresh | Columns

API NAME	SECURITY FINDINGS ▲	CLIENT WORKLOADS	POLICY COMPLIANCE	SPECS
github.com	Total: 68720 871 1133 570... 3655 5973		✓	✓

PAGE 1

50 100 200 PER PAGE

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Panoptica

APIS

Set up Panoptica | API | CT | Chris Taylor, Administrator

- Dashboard
- Navigator
- CI/CD
- Runtime
- APIs
- Serverless
- Deployments
- Policies
- Risk Assessment
- Compliance

ADMINISTRATION

- Audit
- System

API inventory

github.com

Last update: 9:43:47 AM Apr 17th, 2023

API DETAILS | SPECS | SECURITY POSTURE | API ENDPOINTS | Download JSON

Structure

- General
- Tags
- Components

GitHub v3 REST API 1.1.4

[BASE URL: null]

https://appsecurity.cisco.com/api/apiSecurity/openApiSpecs/.../openApiSpecSwagger.json

See on swagger | Refresh | Reset

GitHub's v3 REST API.

Terms of service

MIT

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

appsecurity.cisco.com/swagger/569346c7-7cad-4356-83a3-73b34b938ed3#/

GitHub v3 REST API 1.1.4 OAS3

https://appsecurity.cisco.com/api/apiSecurity/openApiSpecs/569346c7-7cad-4356-83a3-73b34b938ed3/openApiSpecSwagger.json

GitHub's v3 REST API.

Terms of service

Support - Website

MIT

GitHub v3 REST API

Servers

https://api.github.com

actions Endpoints to manage GitHub Actions using the REST API.

GET	/orgs/{org}/actions/cache/usage	Get GitHub Actions cache usage for an organization
GET	/orgs/{org}/actions/cache/usage-by-repository	List repositories with GitHub Actions cache usage for an organization
GET	/orgs/{org}/actions/permissions	Get GitHub Actions permissions for an organization
PUT	/orgs/{org}/actions/permissions	Set GitHub Actions permissions for an organization
GET	/orgs/{org}/actions/permissions/repositories	List selected repositories enabled for GitHub Actions in an organization

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Secure Application

APIS

API

Desh Shukla
Administrator

- Dashboard
- Navigator
- CI/CD
- Runtime
- APIs
- Deployments
- Policies
- Risk Assessment

ADMINISTRATION

- K8s Controllers
- Audit
- System

API inventory

github.com

Last update: 9:00:09 PM May 8th, 2022

API DETAILS | SPECS | SECURITY POSTURE | API ENDPOINTS

Download JSON

Categories List

email	MEDIUM
application	LOW
dns	LOW
api-specification	CRITICAL

Api api-specification risk: CRITICAL

RISK CONFIDENCE
High

RISK TREND
Stable

Number of risk findings

745 Critical risk findings

Missing global security scheme (745)

SOURCE	DESCRIPTION	MITIGATION
oas_analyser	Spec analyzer detected that the spec does not define a global security scheme. It is highly recommended that all API operations support a security scheme, which means supporting proper authentication and authorization. In principle this can be achieved without a global security scheme, by specifying a security scheme for each API operation. However it is a good practice to have a global one instead of individual ones. This makes maintenance easy and avoids that new API operations are added without any security scheme association.	Make sure all API operations have a security scheme associated and as a good practice add a global security scheme.

Conclusion

Panoptica - Cloud Native Security Coverage

Single tool to provide Comprehensive Container, API, Service Mesh and Kubernetes Security

CI

- Vulns Scan
- Docker CIS
- Image Validation

CD

- Risky RBAC
- Insecure Configurations
- Embedded Secrets

Deployment

- Secured Configurations
- RBAC monitoring

Runtime

- Deployment Scanning
- Network Policies
- Network Encryption
- Cluster Protection
- External API Scanning

Continual Security Coverage

* CI = Continuous Integration
* CD = Continuous Delivery

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Thank you

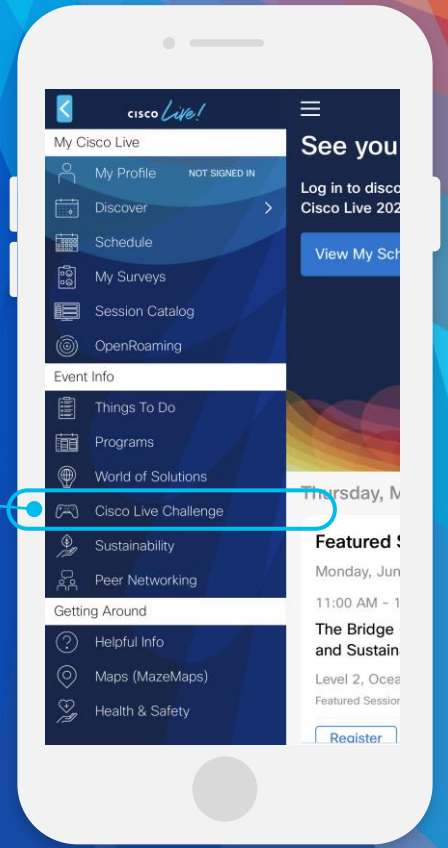
Cisco Live **Challenge**

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:



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

cisco Live!

Let's go