FORTINET

FORTINET XPERTS SUMMIT 2025

FortiCNAPP Recap & Guided CTF

Filippo Caliari

Francisco Menezes

Comprehensive Integrated Code-to-Cloud Security

360-degree cloud defense-in-depth protection against all threat and risk vectors

Secure everything from code to cloud faster with **unparalleled context and visibility with a single unified platform**.

CSPM

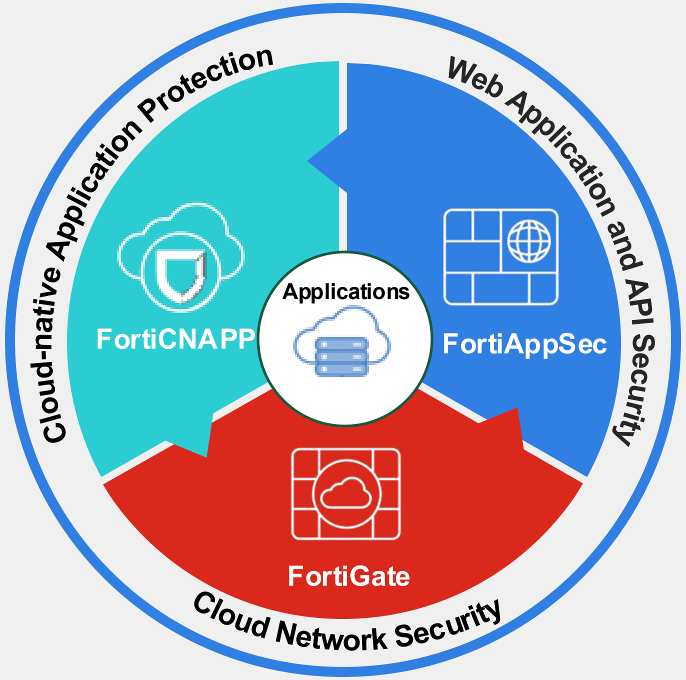
KSPM

CWP

CIEM

IaC

Code Security


Cloud-native Application Protection
Web Application and API Security
Cloud Network Security
FortiCNAPP
Applications
FortiAppSec
FortiGate

Integrated AI/ML-driven platform to protect business-critical web applications and APIs from attacks that target known and unknown vulnerabilities.

WAAP

GSLB

Bot Mitigation Management

Threat Analytics

DAST

Achieve network visibility and enforcement of **consistent security policies** across private, public, and telco clouds.

Virtual FW

Cloud-native FW

How to Address the Native Cloud Security Challenge

Identifying, Prioritizing and Resolving Risks and Threats in Cloud-native Applications

Minimize Attack Surface

Gain comprehensive visibility and proactively reduce vulnerabilities, misconfigurations and excessive privileges without slowing down development.

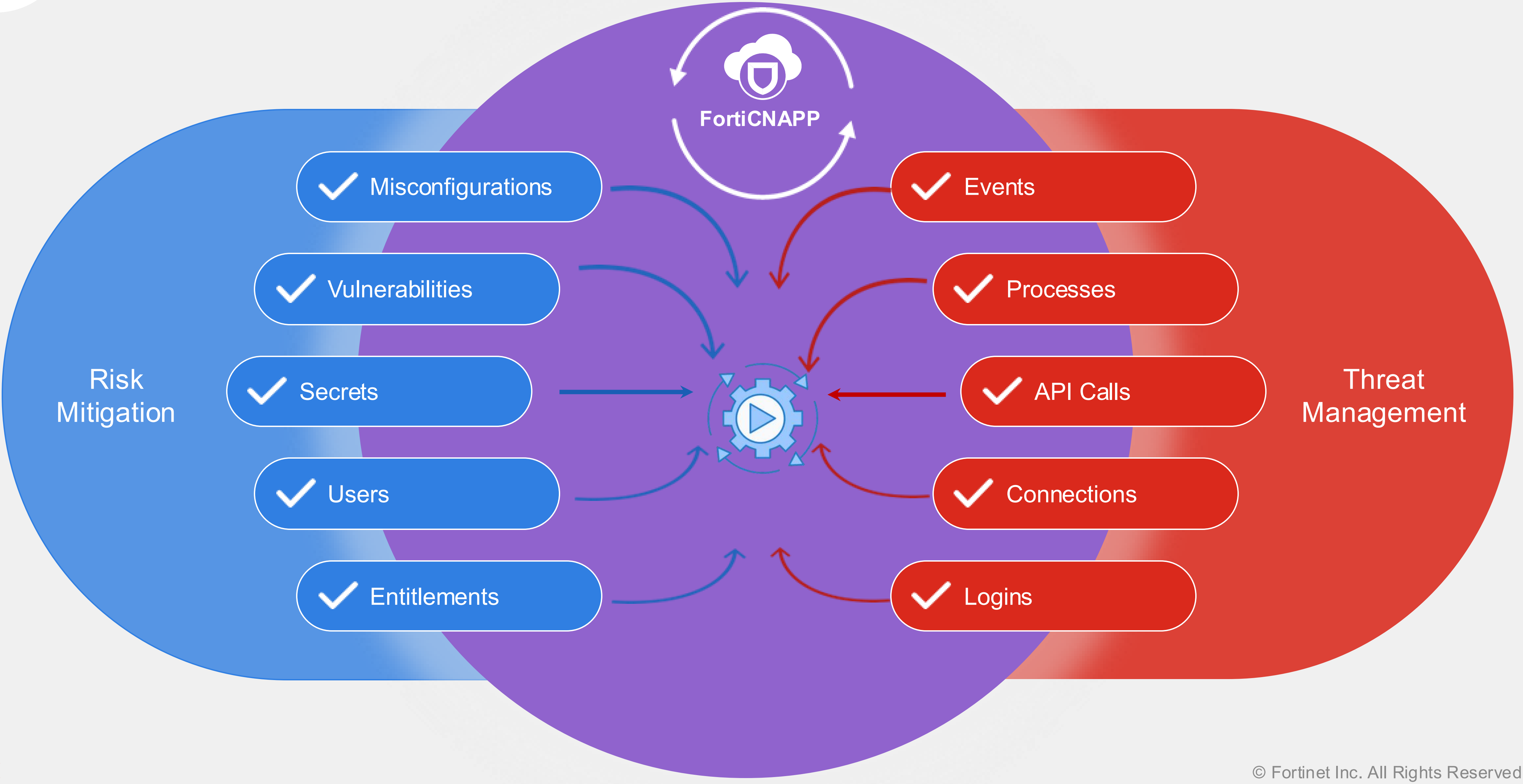
Continuously Monitor Risks

Continuously assess virtual machines, containers and Kubernetes workloads to address active risks before they are exploited.

Reduce Threat Impact

Quickly detect, investigate and respond to unusual behavior and active threats including the use of compromised credentials, cloud ransomware and cryptomining.

Prioritization Requires Combining Risk and Threat Context



FortiCNAPP Integration – Step 1:
Read only cloud environment

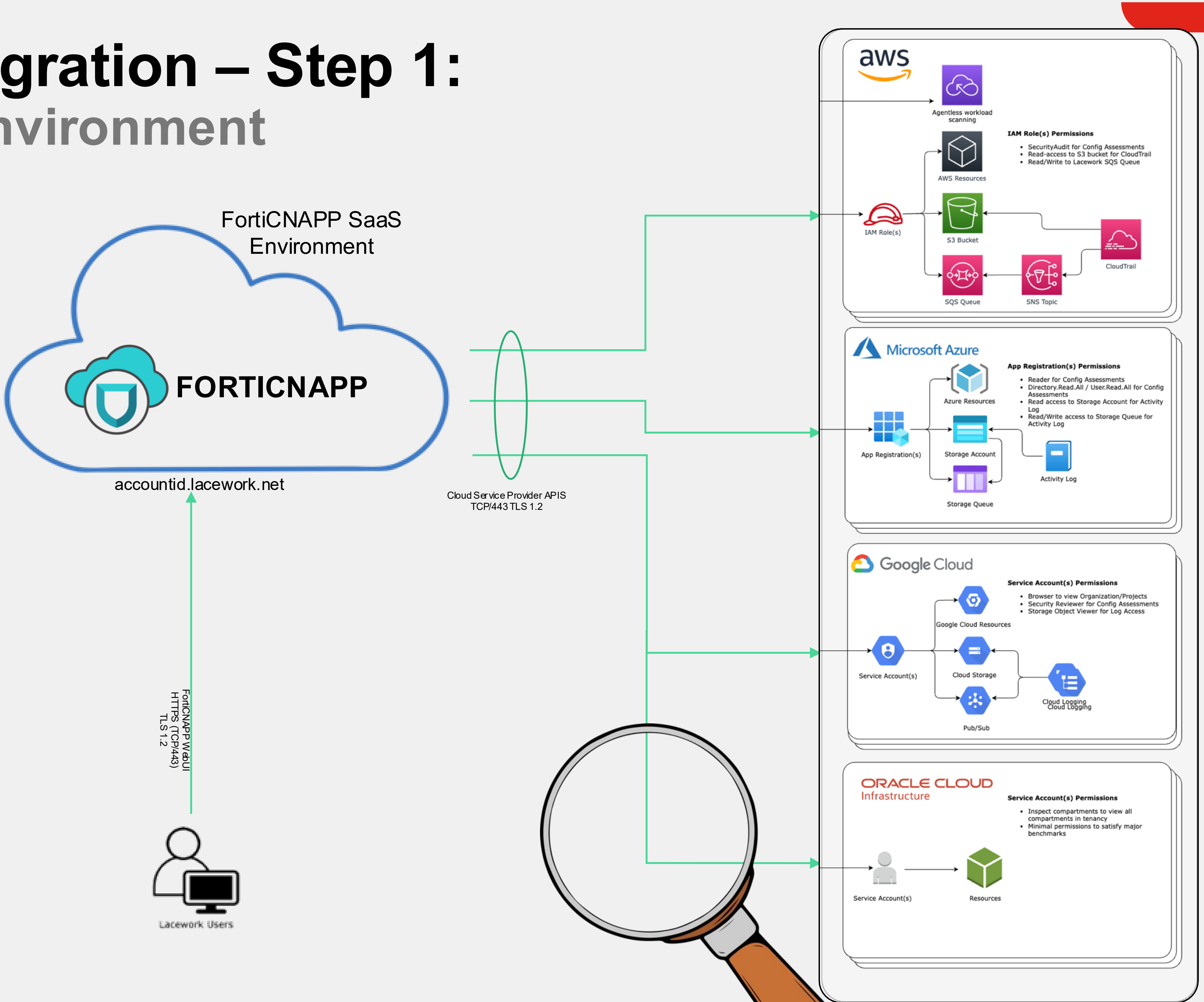
Inventory

CSPM + KSPM

CIEM

Vulnerability

CWP agentless



IAM Role(s) Permissions

- SecurityAudit for Config Assessments
- Read-access to S3 bucket for CloudTrail
- Read/Write to Lacework SQS Queue

App Registration(s) Permissions

- Reader for Config Assessments
- Directory.Read.All / User.Read.All for Config Assessments
- Read access to Storage Account for Activity Log
- Read/Write access to Storage Queue for Activity Log

Service Account(s) Permissions

- Browser to view Organization/Projects
- Security Reviewer for Config Assessments
- Storage Object Viewer for Log Access

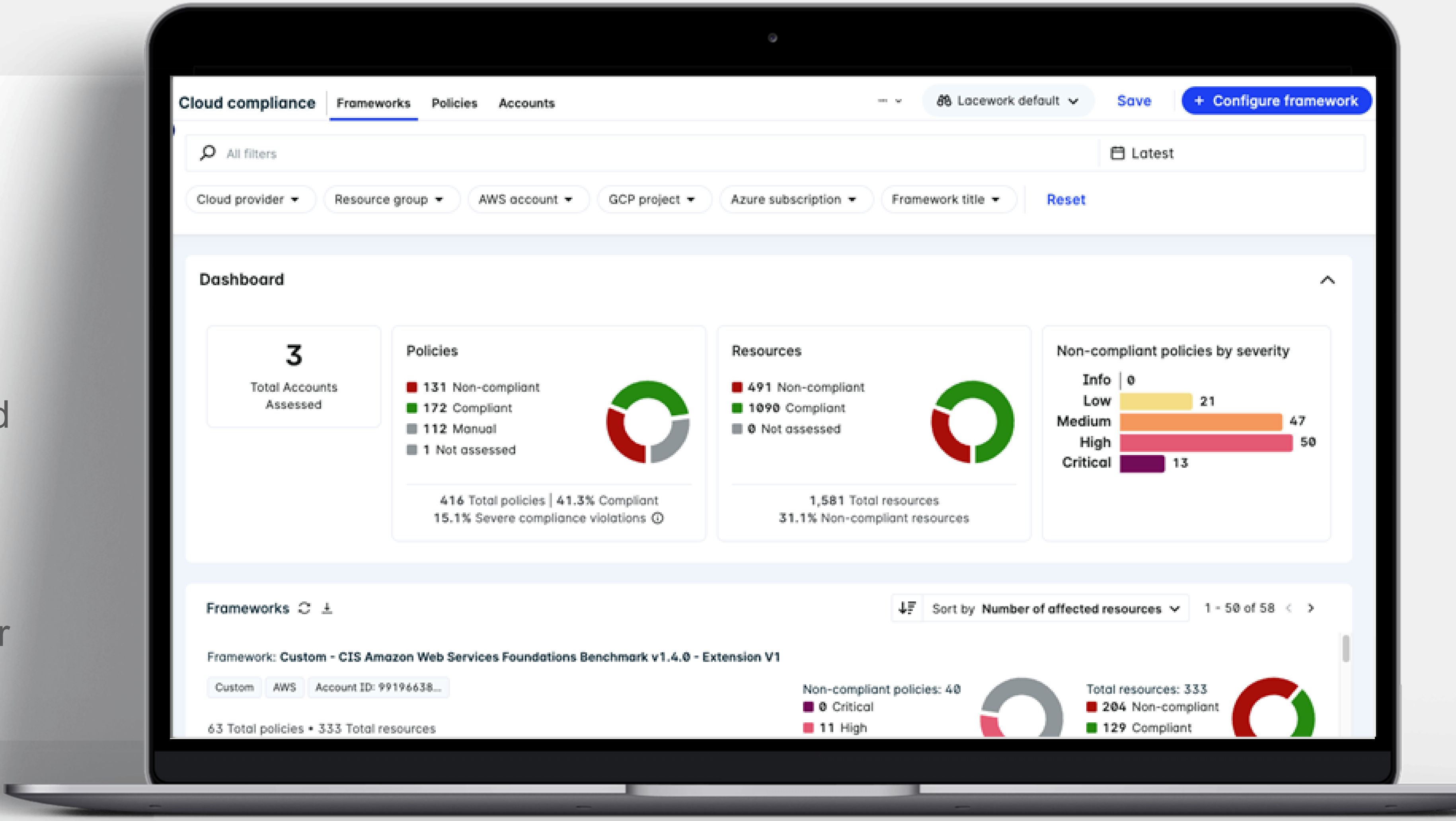
Service Account(s) Permissions

- Inspect compartments to view all compartments in tenancy
- Minimal permissions to satisfy major benchmarks

Cloud Configuration

Security Posture Management CSPM and KSPM

- Gain complete visibility of continually changing cloud resources
- Continuously monitor for misconfigurations
- Achieve compliance faster



Dashboard

3 Total Accounts Assessed

Policies

- 🟥 131 Non-compliant
- 🟩 172 Compliant
- ▨ 112 Manual
- ▨ 1 Not assessed

416 Total policies | 41.3% Compliant
15.1% Severe compliance violations

Resources

- 🟥 491 Non-compliant
- 🟩 1090 Compliant
- ▨ 0 Not assessed

1,581 Total resources
31.1% Non-compliant resources

Non-compliant policies by severity

Info	0
Low	21
Medium	47
High	50
Critical	13

Frameworks

Sort by Number of affected resources 1 - 50 of 58

Framework: **Custom - CIS Amazon Web Services Foundations Benchmark v1.4.0 - Extension V1**

Custom AWS Account ID: 99196638...

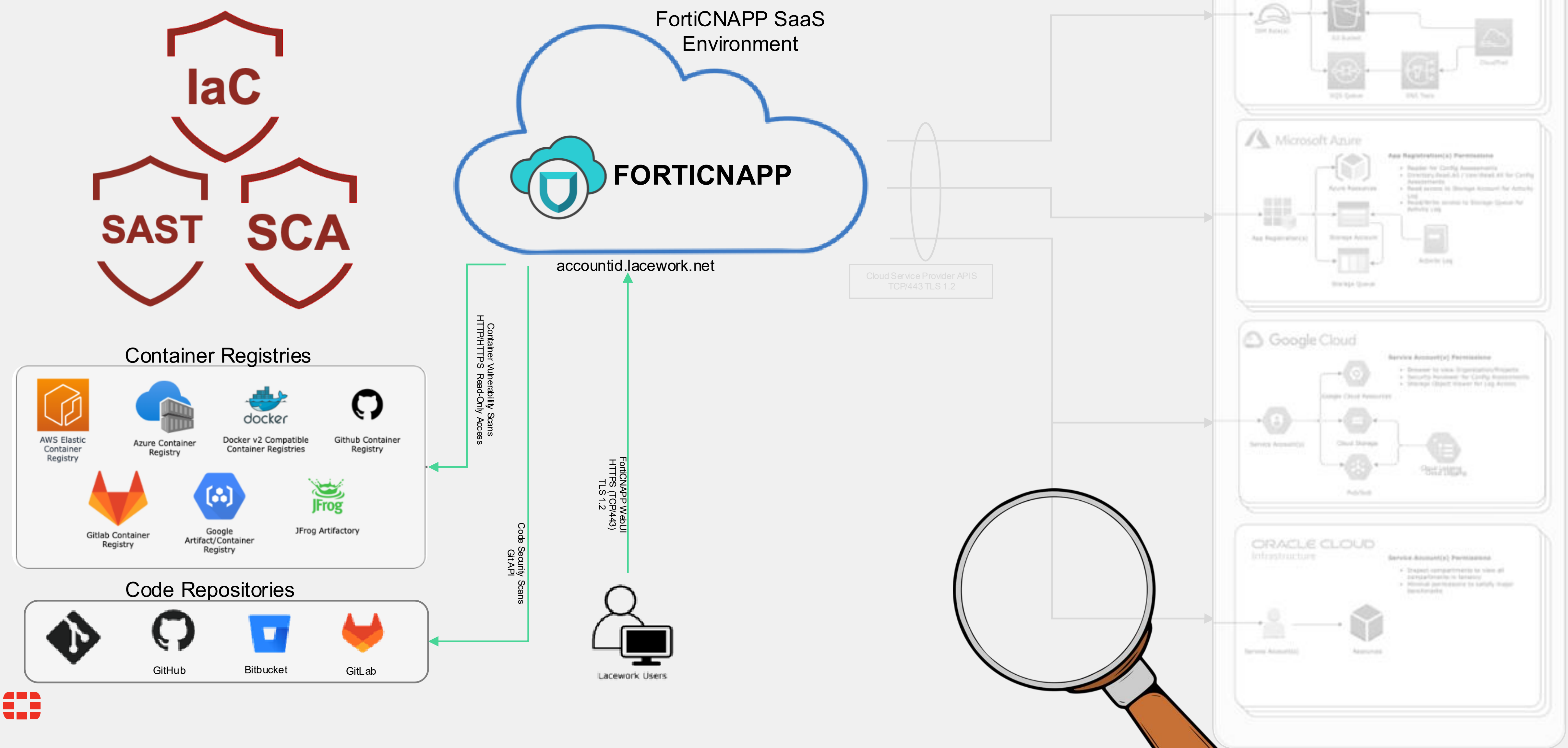
63 Total policies • 333 Total resources

Non-compliant policies: 40
- 0 Critical
- 11 High

Total resources: 333
- 🟥 204 Non-compliant
- 🟩 129 Compliant

POSSIAMO VEDERE UNA DEMO?

FortiCNAPP Integration – Step 2:
Read only repositories



IaC

SAST

SCA

FortiCNAPP SaaS Environment

FORTICNAPP

accountid.lacework.net

Container Vulnerability Scans HTTP/HTTPS Read-Only Access

Code Security Scans GitAPI

FortiCNAPP WebUI HTTPS (TCP/443) TLS 1.2

Lacework Users

Container Registries

AWS Elastic Container Registry

Azure Container Registry

Docker v2 Compatible Container Registries

Github Container Registry

Gitlab Container Registry

Google Artifact/Container Registry

JFrog Artifactory

Code Repositories

GitHub

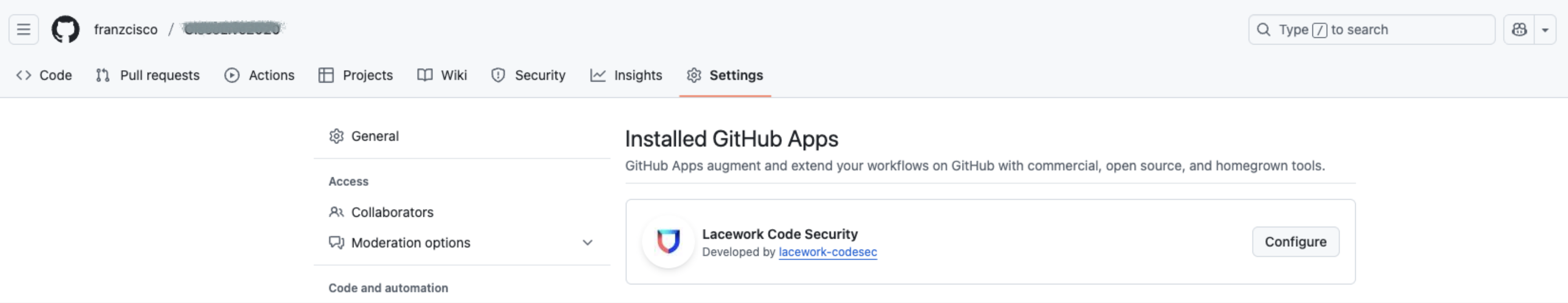
Bitbucket

GitLab

Cloud Service Provider APIS TCP/443 TLS 1.2

Code Security

FortiCNAPP registers itself as a GitHub App.
Lacework FortiCNAPP Code Security will automatically scan the default branch of all your repositories. Once the scans are completed, you will be able to see the results in the UI.



franzcisco / [redacted]

Installed GitHub Apps

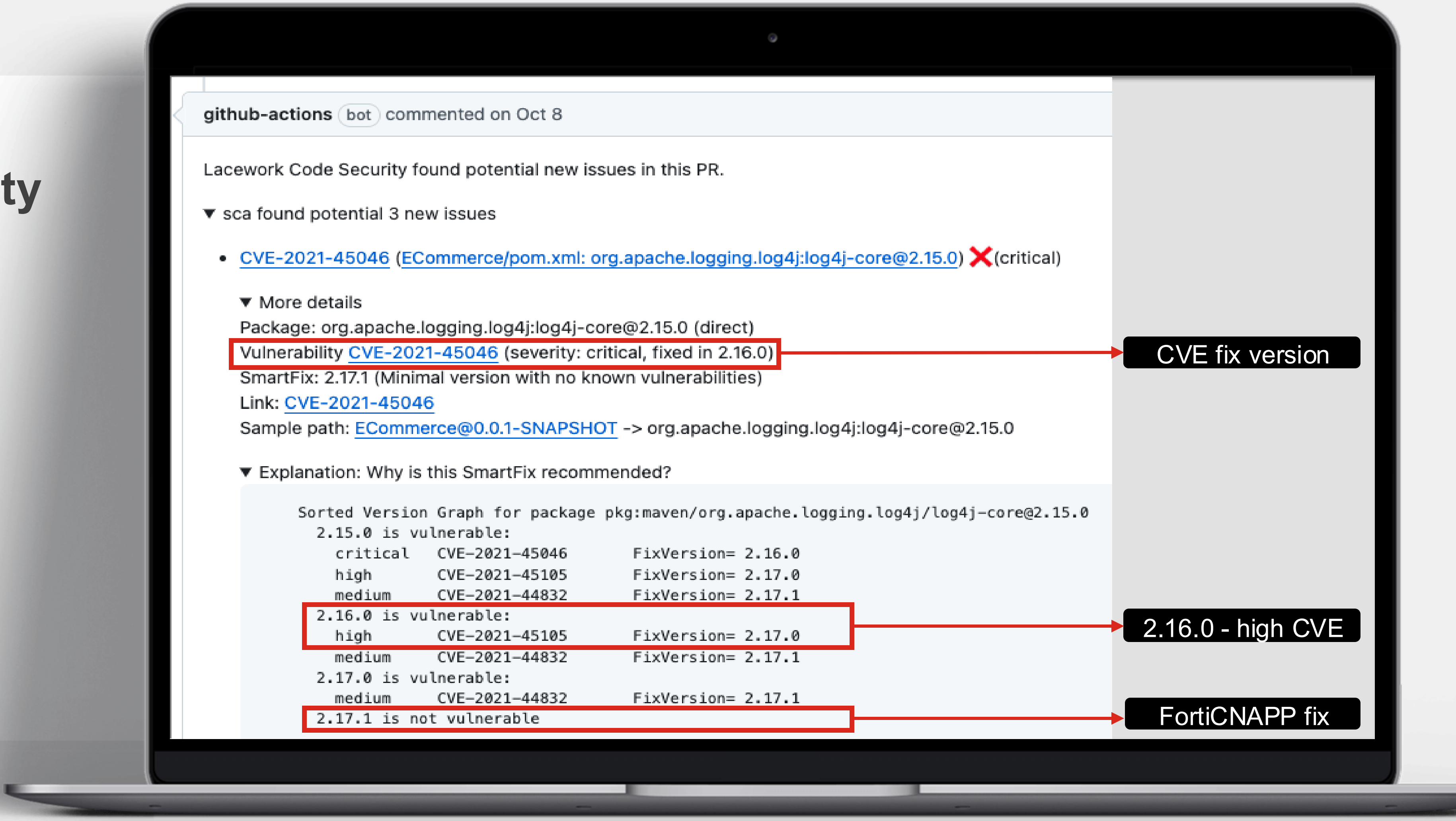
GitHub Apps augment and extend your workflows on GitHub with commercial, open source, and homegrown tools.

Lacework Code Security
Developed by lacework-codesec

Shift Security Left to Reduce Risk and Remediation Costs

Application and Infrastructure Security

- Gain visibility of software supply chain (SBOM)
- Identify third-party code CVEs (SCA)
- Detect first-party code weaknesses (SAST)
- Secrets detection
- Verify cloud infrastructure configuration (IaC)



github-actions bot commented on Oct 8

Lacework Code Security found potential new issues in this PR.

▼ sca found potential 3 new issues

- CVE-2021-45046 (ECommerce/pom.xml: org.apache.logging.log4j:log4j-core@2.15.0) ❌(critical)

▼ More details

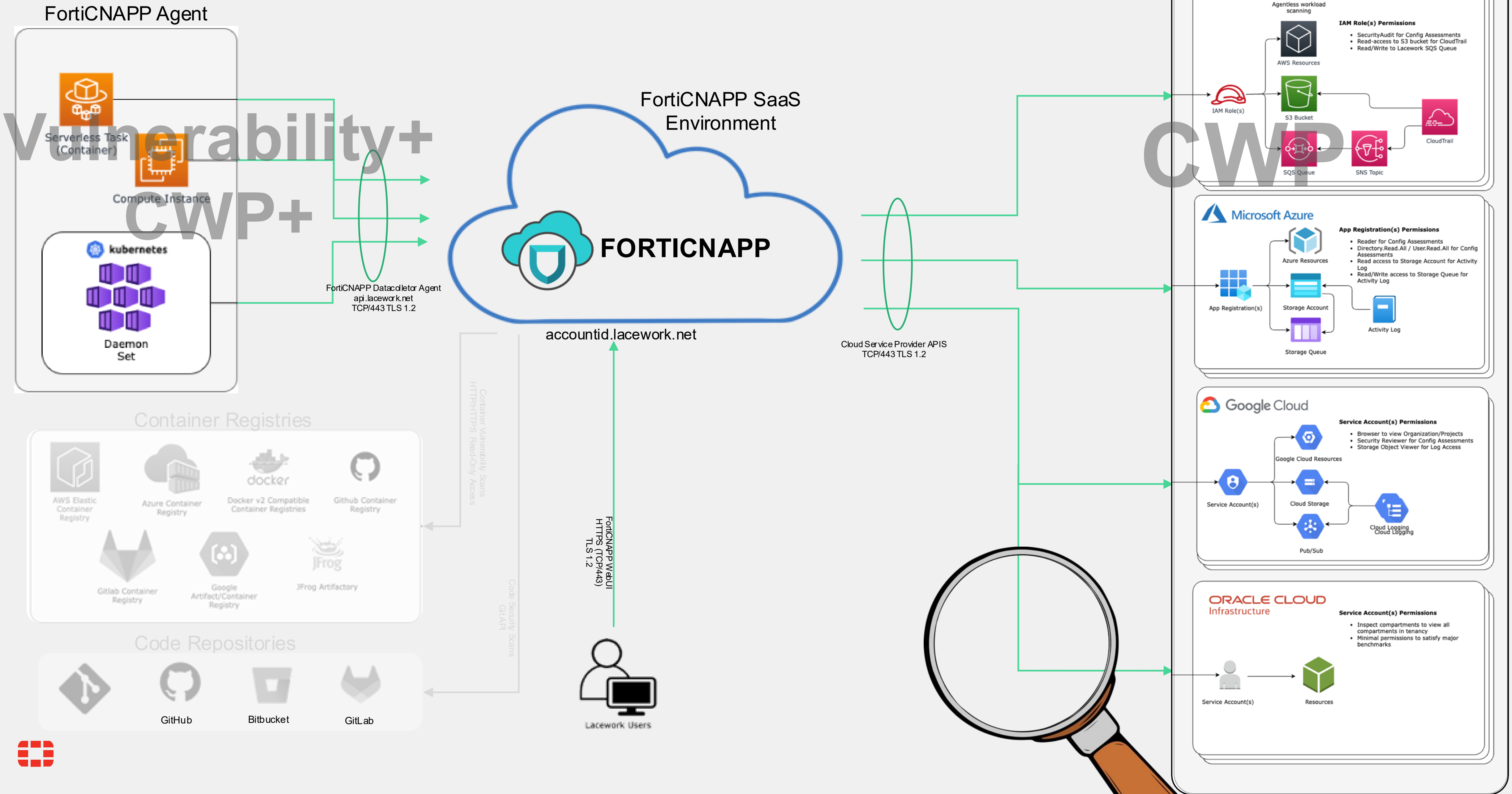
Package: org.apache.logging.log4j:log4j-core@2.15.0 (direct)
Vulnerability CVE-2021-45046 (severity: critical, fixed in 2.16.0)
SmartFix: 2.17.1 (Minimal version with no known vulnerabilities)
Link: CVE-2021-45046
Sample path: ECommerce@0.0.1-SNAPSHOT -> org.apache.logging.log4j:log4j-core@2.15.0

▼ Explanation: Why is this SmartFix recommended?

```
   Sorted Version Graph for package pkg:maven/org.apache.logging.log4j/log4j-core@2.15.0
     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
```

POSSIAMO VEDERE UNA DEMO?

FortiCNAPP Integration – Step 3: AGENT



IAM Role(s) Permissions

- SecurityAudit for Config Assessments
- Read-access to S3 bucket for CloudTrail
- Read/Write to Lacework SQS Queue

App Registration(s) Permissions

- Reader for Config Assessments
- Directory.Read.All / User.Read.All for Config Assessments
- Read access to Storage Account for Activity Log
- Read/Write access to Storage Queue for Activity Log

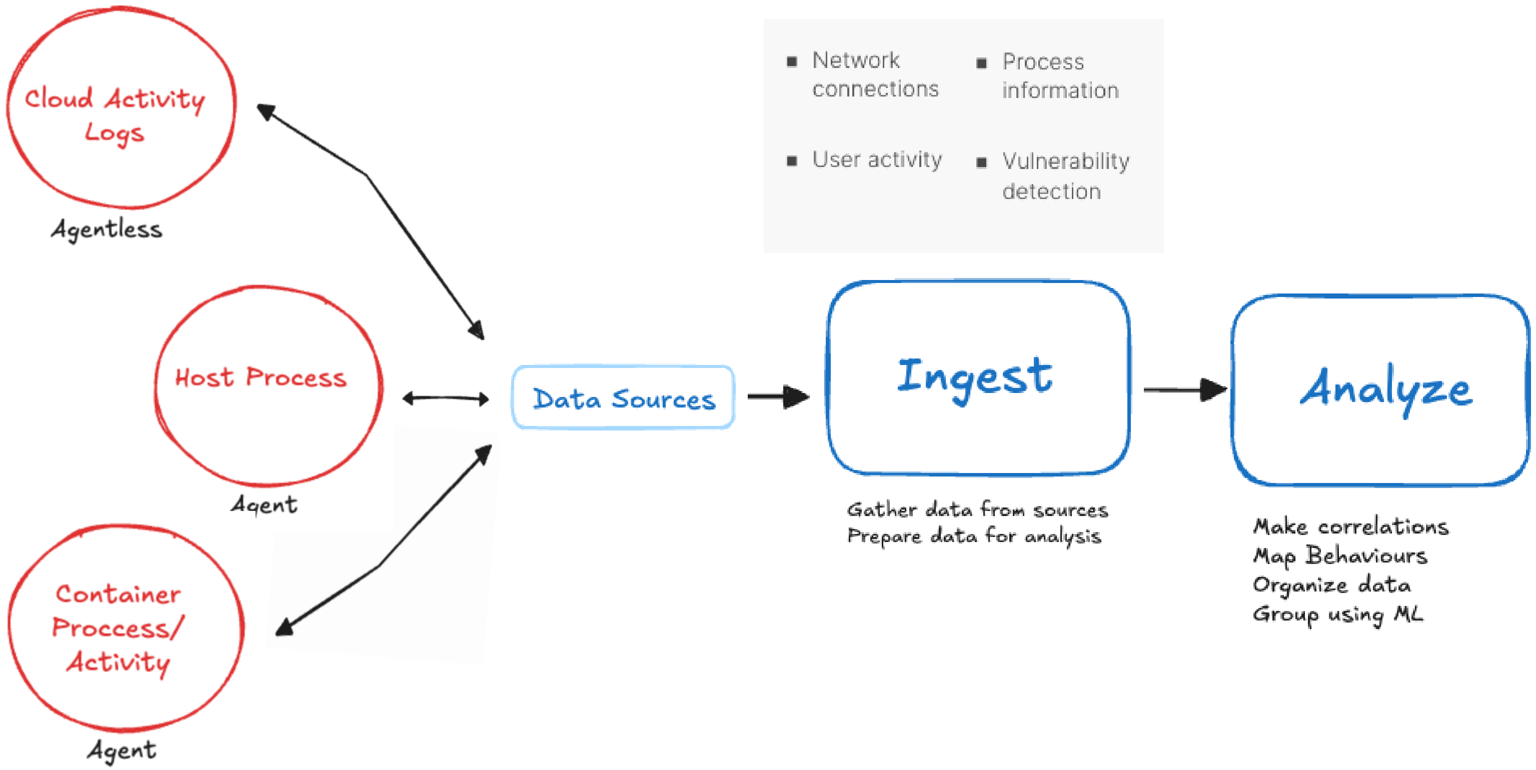
Service Account(s) Permissions

- Browser to view Organization/Projects
- Security Reviewer for Config Assessments
- Storage Object Viewer for Log Access

Service Account(s) Permissions

- Inspect compartments to view all compartments in tenancy
- Minimal permissions to satisfy major benchmarks

Runtime Protection



- Network connections
- Process information
- User activity
- Vulnerability detection

Cloud Activity Logs

Agentless

Host Process

Agent

Container Proccess/ Activity

Agent

Data Sources

Ingest

Gather data from sources
Prepare data for analysis

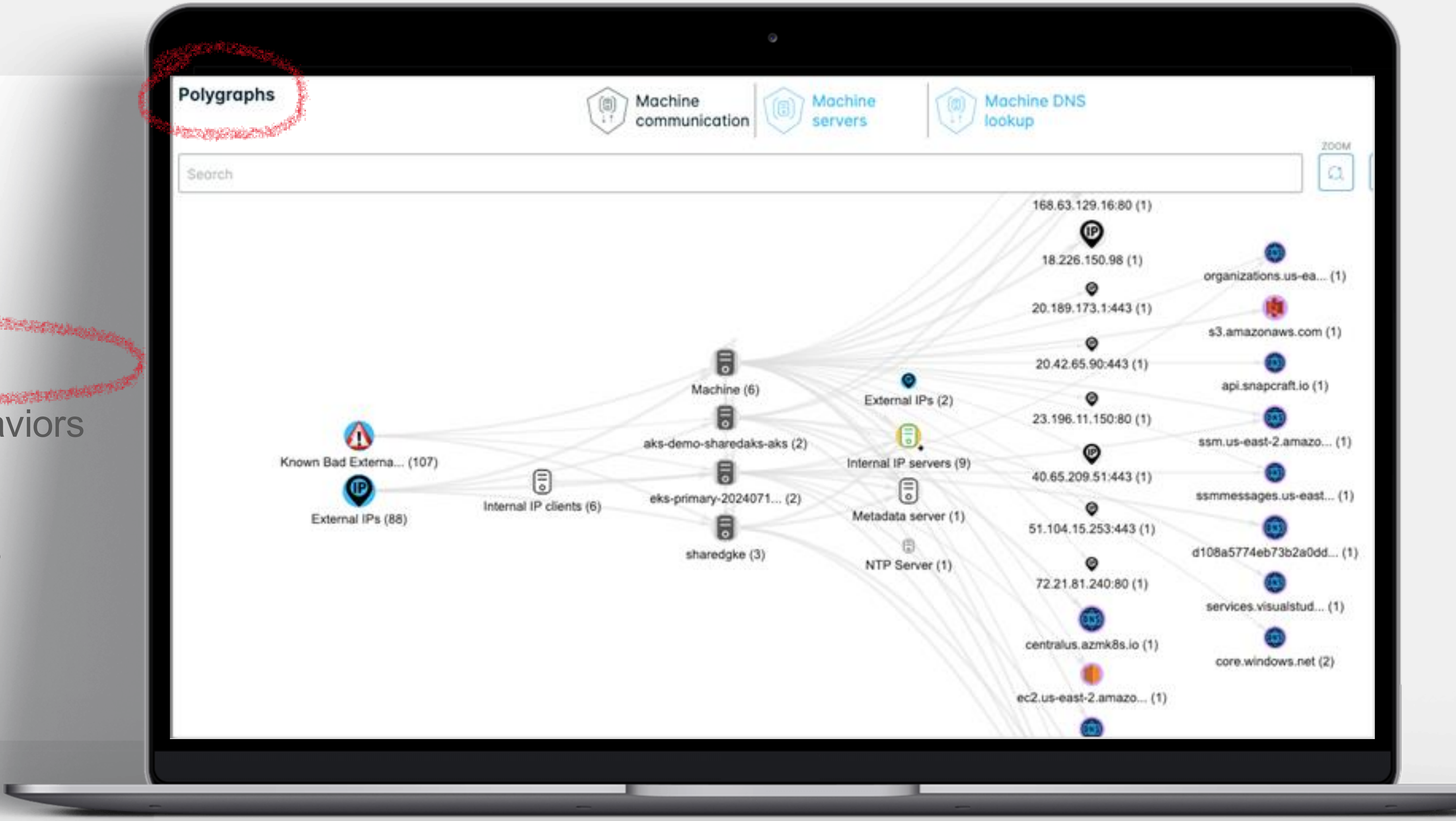
Analyze

Make correlations
Map Behaviours
Organize data
Group using ML

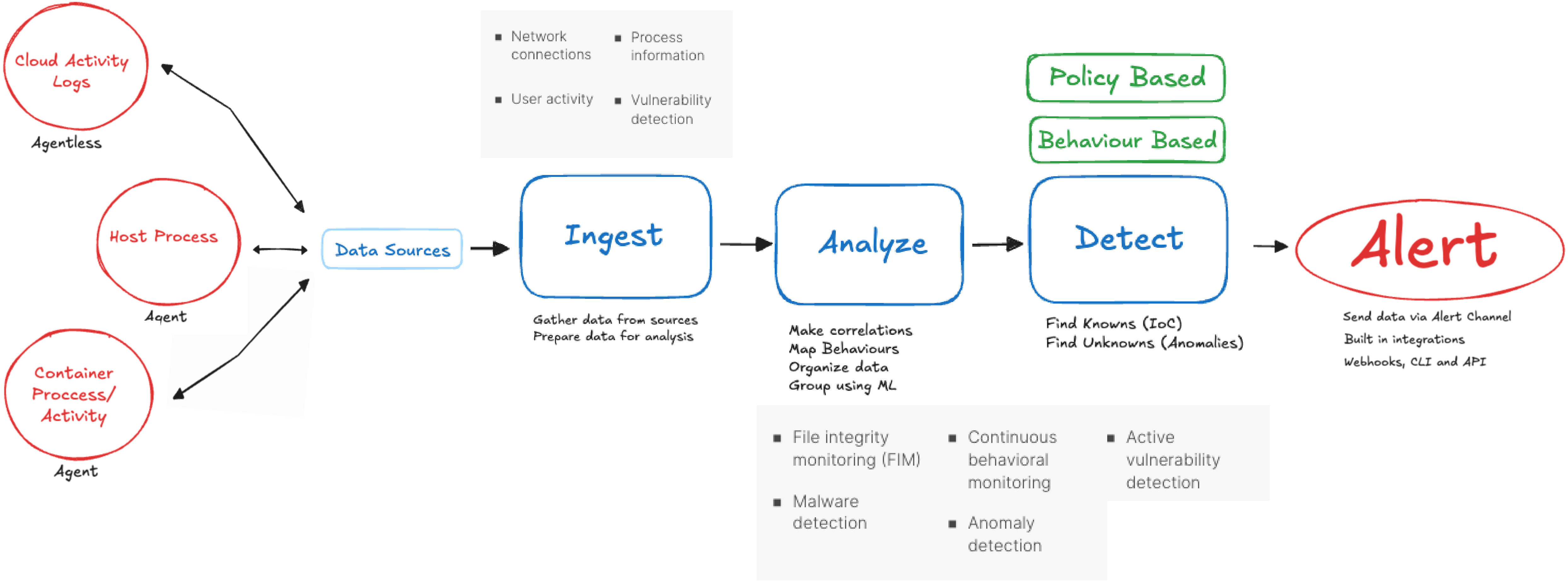
Runtime Protection

Cloud Workload Protection Platform (CWP)

- Map network connections
- Discover anomalous behaviors
- Detect in-progress threats
- Find vulnerabilities across hosts, containers and Kubernetes (K8s)



Runtime Protection



Cloud Activity Logs

Agentless

Host Process

Agent

Container Proccess/ Activity

Agent

Data Sources

- Network connections
- Process information
- User activity
- Vulnerability detection

Ingest

Gather data from sources
Prepare data for analysis

Analyze

Make correlations
Map Behaviours
Organize data
Group using ML

- File integrity monitoring (FIM)
- Malware detection
- Continuous behavioral monitoring
- Anomaly detection
- Active vulnerability detection

Policy Based

Behaviour Based

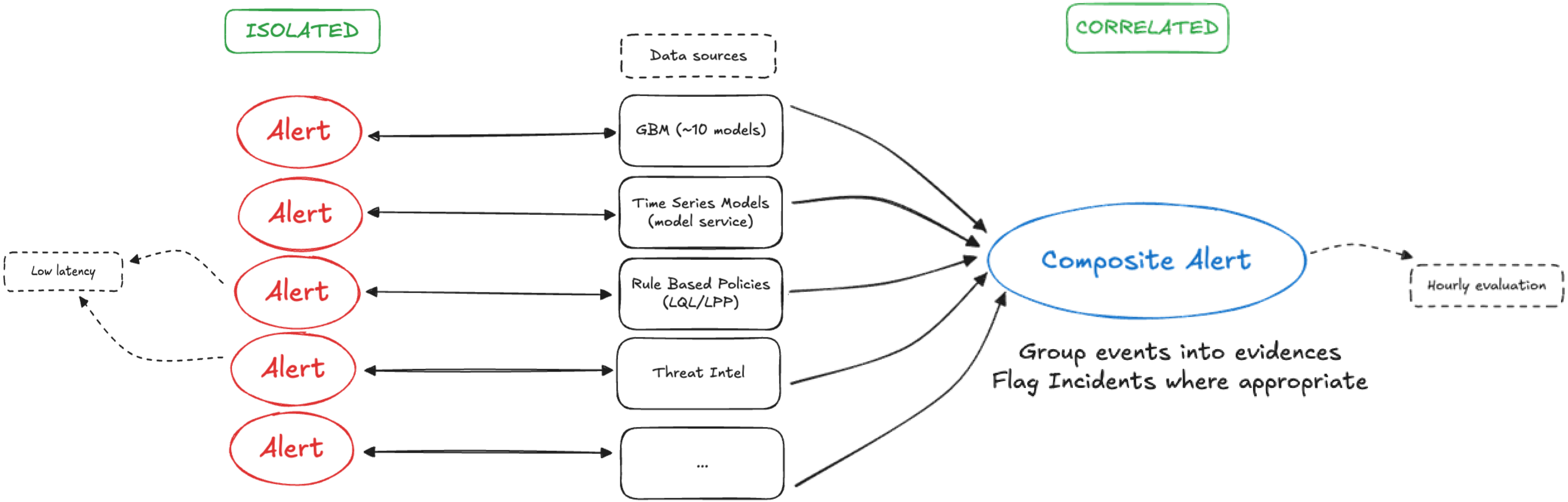
Detect

Find Knowns (IoC)
Find Unknowns (Anomalies)

Alert

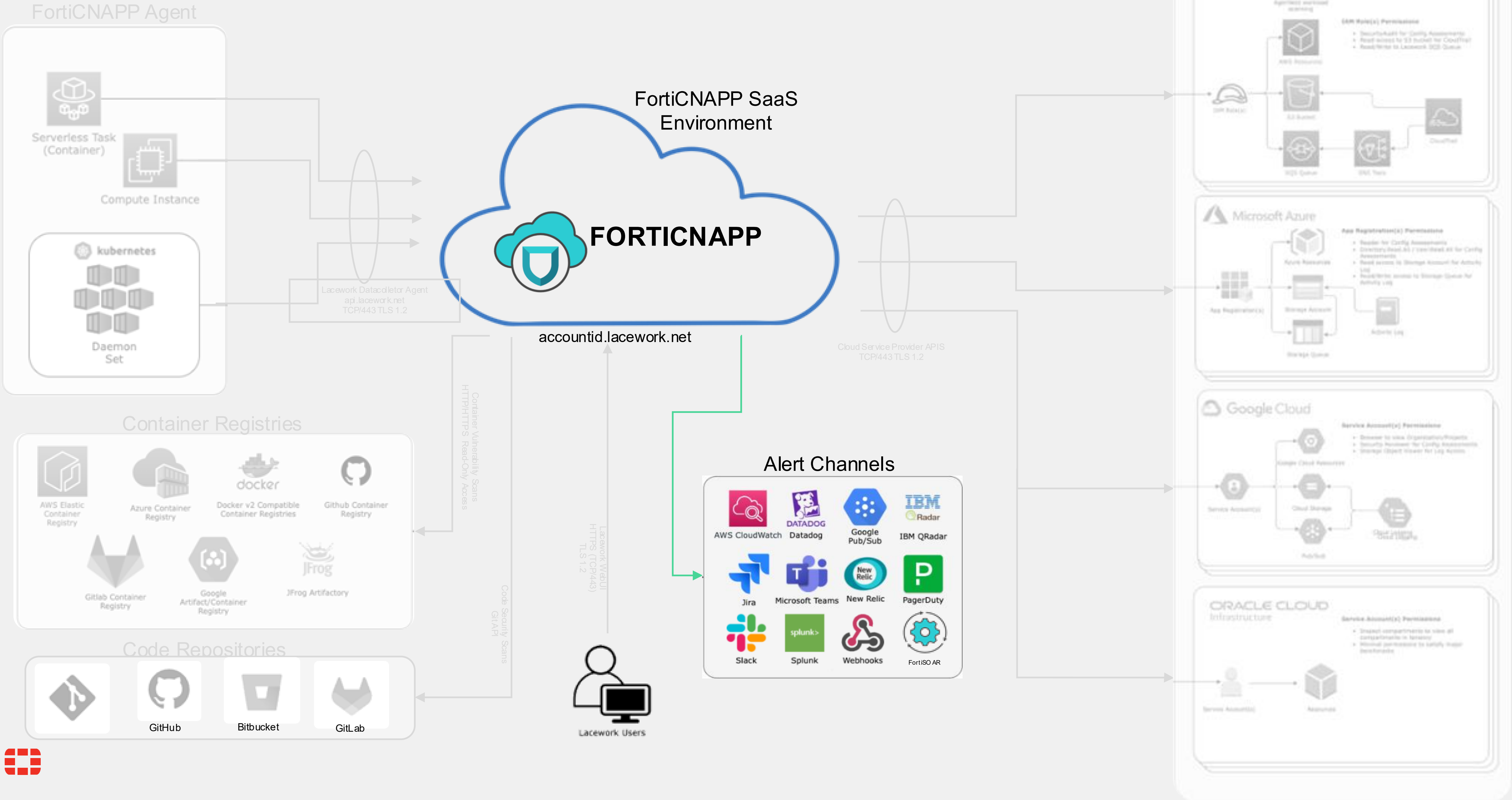
Send data via Alert Channel
Built in integrations
Webhooks, CLI and API

Alerting


ISOLATED
CORRELATED
Data sources
Alert
Alert
Alert
Alert
Alert
GBM (~10 models)
Time Series Models (model service)
Rule Based Policies (LQL/LPP)
Threat Intel
...
Low latency
Composite Alert
Hourly evaluation
Group events into evidences
Flag Incidents where appropriate

POSSIAMO VEDERE UNA DEMO?

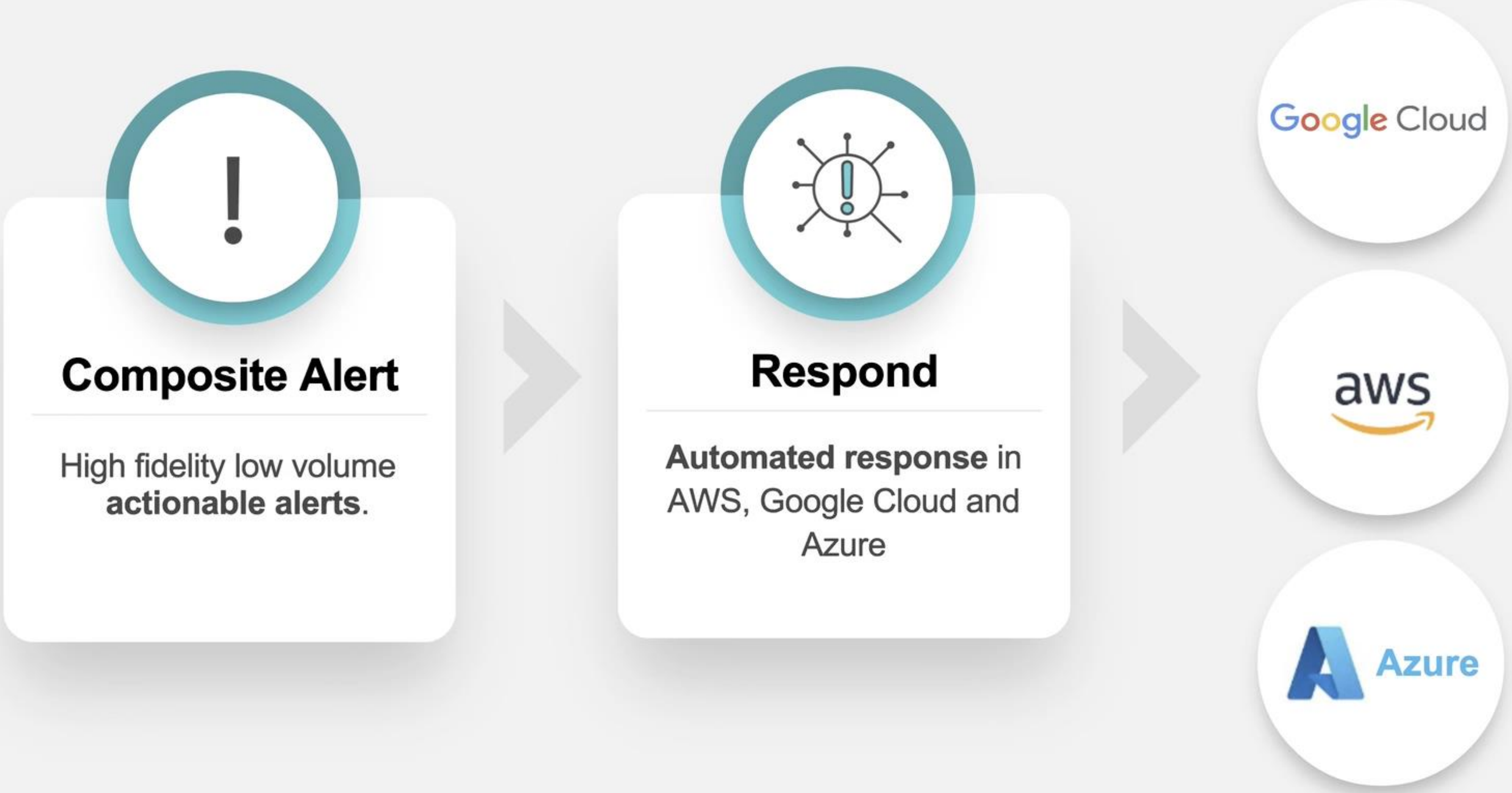
FortiCNAPP Integration – Step 4: Info sharing


FortiCNAPP Agent
Serverless Task (Container)
Compute Instance
kubernetes
Daemon Set
Lacework Datacollector Agent
api.lacework.net
TCP/443 TLS 1.2
FortiCNAPP SaaS Environment
FORTICNAPP
accountid.lacework.net
Container Registries
AWS Elastic Container Registry
Azure Container Registry
docker
Docker v2 Compatible Container Registries
Github Container Registry
Gitlab Container Registry
Google Artifact/Container Registry
JFrog
JFrog Artifactory
Container Vulnerability Scans
HTTP/HTTPS Read-Only Access
Code Repositories
GitHub
Bitbucket
GitLab
Code Security Scans
Git API
Lacework WebUI
HTTPS (TCP/443)
TLS 1.2
Lacework Users
Alert Channels
AWS CloudWatch
DATADOG
Datadog
Google Pub/Sub
IBM QRadar
IBM QRadar
Jira
Microsoft Teams
New Relic
New Relic
P
PagerDuty
Slack
splunk>
Splunk
Webhooks
FortiSOAR
Cloud Service Provider APIS
TCP/443 TLS 1.2
aws
Agentless workload scanning
IAM Role(s) Permissions
SecurityAudit for Config Assessments
Read access to S3 bucket for CloudTrail
Read/Write to Lacework SQS Queue
AWS Resources
IAM Role(s)
S3 Bucket
CloudTrail
SQS Queue
SNS Topic
Microsoft Azure
App Registration(s) Permissions
Reader for Config Assessments
Directory.Read.All / User.Read.All for Config Assessments
Read access to Storage Account for Activity Log
Read/Write access to Storage Queue for Activity Log
Azure Resources
App Registration(s)
Storage Account
Storage Queue
Activity Log
Google Cloud
Service Account(s) Permissions
Browser to view Organization/Projects
Security Reviewer for Config Assessments
Storage Object Viewer for Log Access
Google Cloud Resources
Service Account(s)
Cloud Storage
Pub/Sub
Cloud Logging
ORACLE CLOUD
Infrastructure
Service Account(s) Permissions
Inspect compartments to view all compartments in tenancy
Minimal permissions to satisfy major benchmarks
Service Account(s)
Resources

C

FortiSOAR Automated Response

Automated threat investigation and response



Composite Alert

High fidelity low volume **actionable alerts**.

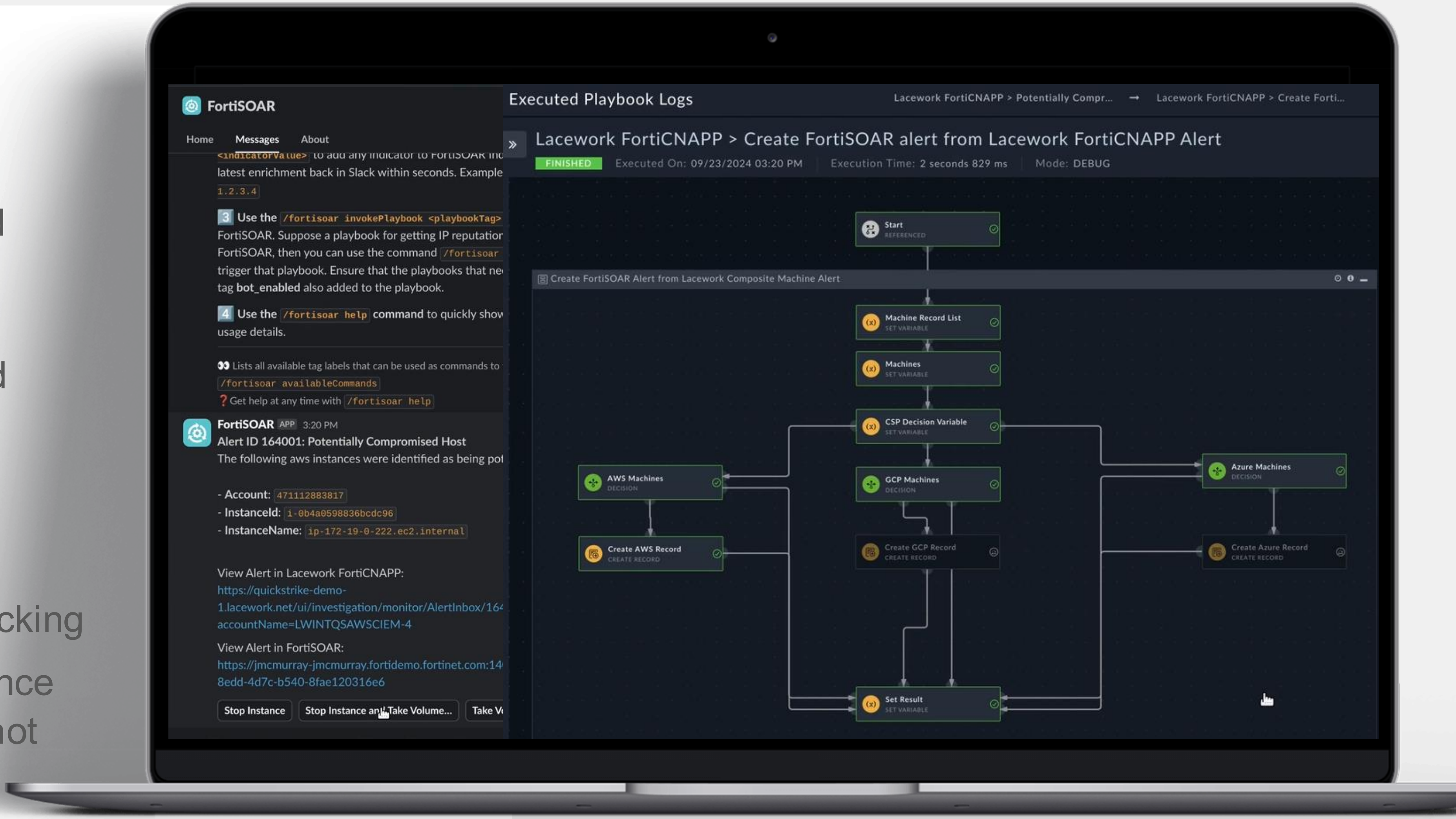
Respond

Automated response in AWS, Google Cloud and Azure

Automate Threat Response

Accelerate Alert Response Times

- Automate remediation and blocking of active runtime threats
- Easily customize and build granular playbooks for FortiCNAPP alerts
- Quickly respond to compromised credentials, ransomware and cryptojacking
- Stop Instance, Stop Instance & Snapshot, Take Snapshot



<indicatorValue> to add any indicator to FortiSOAR ind
latest enrichment back in Slack within seconds. Example
1.2.3.4

3 Use the /fortisoar invokePlaybook <playbookTag>
FortiSOAR. Suppose a playbook for getting IP reputatior
FortiSOAR, then you can use the command /fortisoar
trigger that playbook. Ensure that the playbooks that ne
tag **bot_enabled** also added to the playbook.

4 Use the /fortisoar help **command** to quickly show
usage details.

👀 Lists all available tag labels that can be used as commands to
/fortisoar availableCommands
❓Get help at any time with /fortisoar help

FortiSOAR APP 3:20 PM
Alert ID 164001: Potentially Compromised Host
The following aws instances were identified as being pot

- Account: 471112883817
- InstanceId: i-0b4a0598836bcdc96
- InstanceName: ip-172-19-0-222.ec2.internal

View Alert in Lacework FortiCNAPP:
https://quickstrike-demo-1.lacework.net/ui/investigation/monitor/AlertInbox/164
accountName=LWINTQSAWSCIEM-4

View Alert in FortiSOAR:
https://jmcmurray-jmcmurray.fortidemo.fortinet.com:14
8edd-4d7c-b540-8fae120316e6

Executed Playbook Logs

Lacework FortiCNAPP > Potentially Compr... → Lacework FortiCNAPP > Create Forti...

Lacework FortiCNAPP > Create FortiSOAR alert from Lacework FortiCNAPP Alert

FINISHED Executed On: 09/23/2024 03:20 PM | Execution Time: 2 seconds 829 ms | Mode: DEBUG

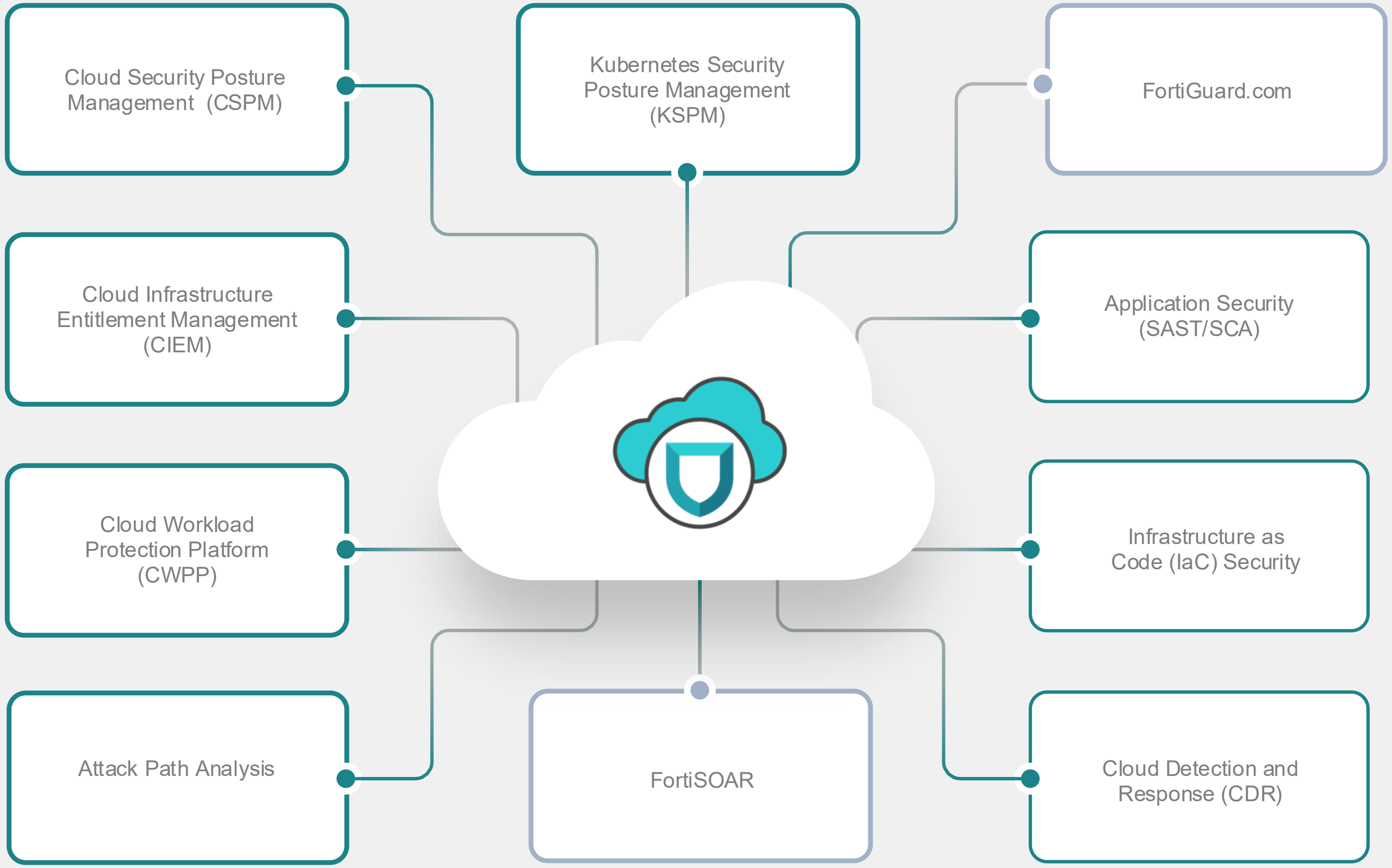
FortiCNAPP Wrap-Up

The Most Complete AI-driven Cloud-Native Application Protection Platform

Single vendor for all cloud security and secure CI/CD application development needs.

See AND protect everything from coding, deploying, and running applications across hybrid and multi-clouds.

Simplify security with AI-driven platforms.

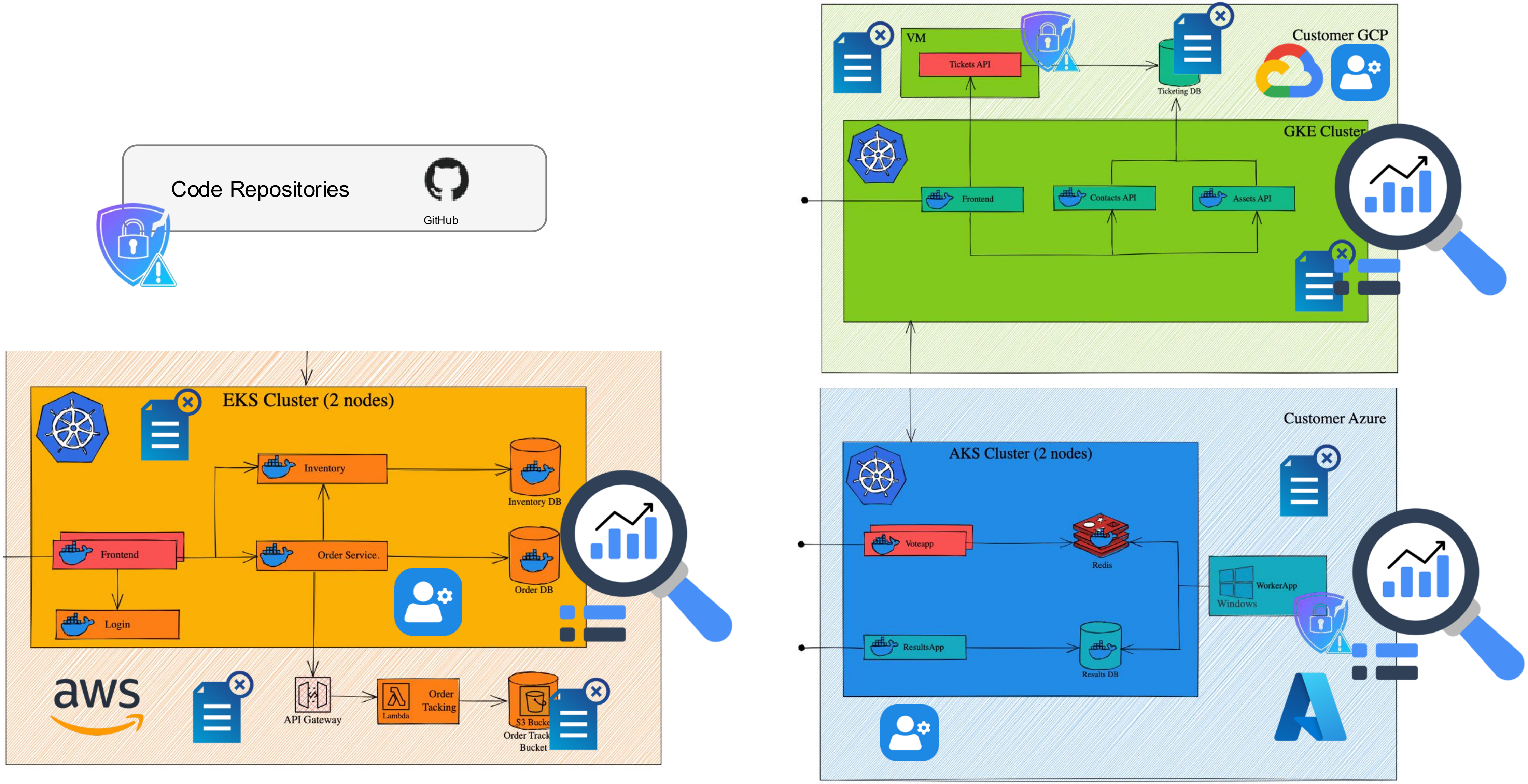


Cloud Security Posture Management (CSPM)
Kubernetes Security Posture Management (KSPM)
FortiGuard.com
Cloud Infrastructure Entitlement Management (CIEM)
Application Security (SAST/SCA)
Cloud Workload Protection Platform (CWPP)
Infrastructure as Code (IaC) Security
Attack Path Analysis
FortiSOAR
Cloud Detection and Response (CDR)

FortiCNAPP

Guided Capture the Flag

The Demo Environment



GUIDED CAPTURE THE FLAG – FortiCNAPP

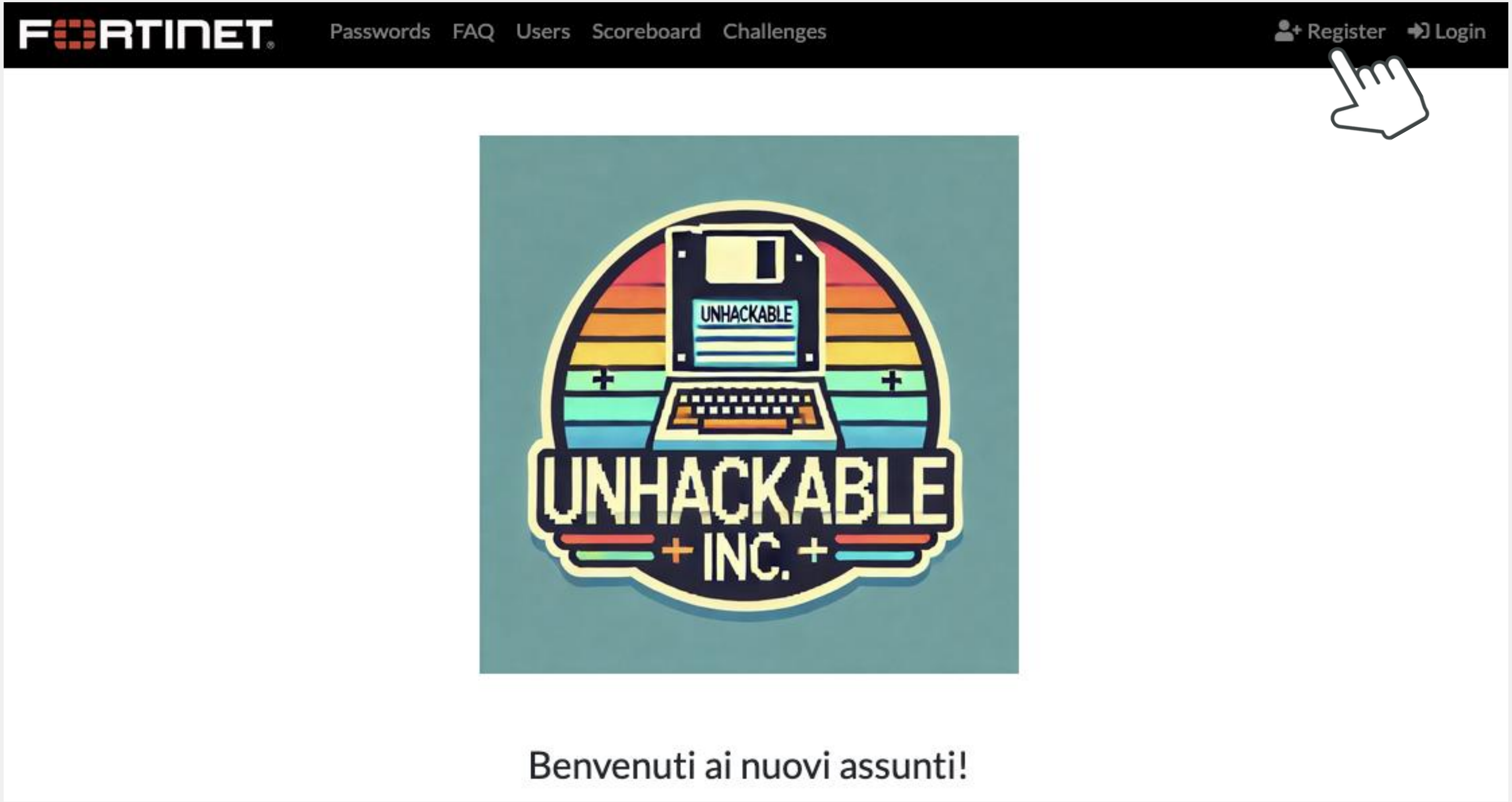
The Rules

Ambiente Demo accessibile su https://lucca25.lwctf.com/

Registration Code: LUCCA2025

GUIDED CAPTURE THE FLAG – FortiCNAPP

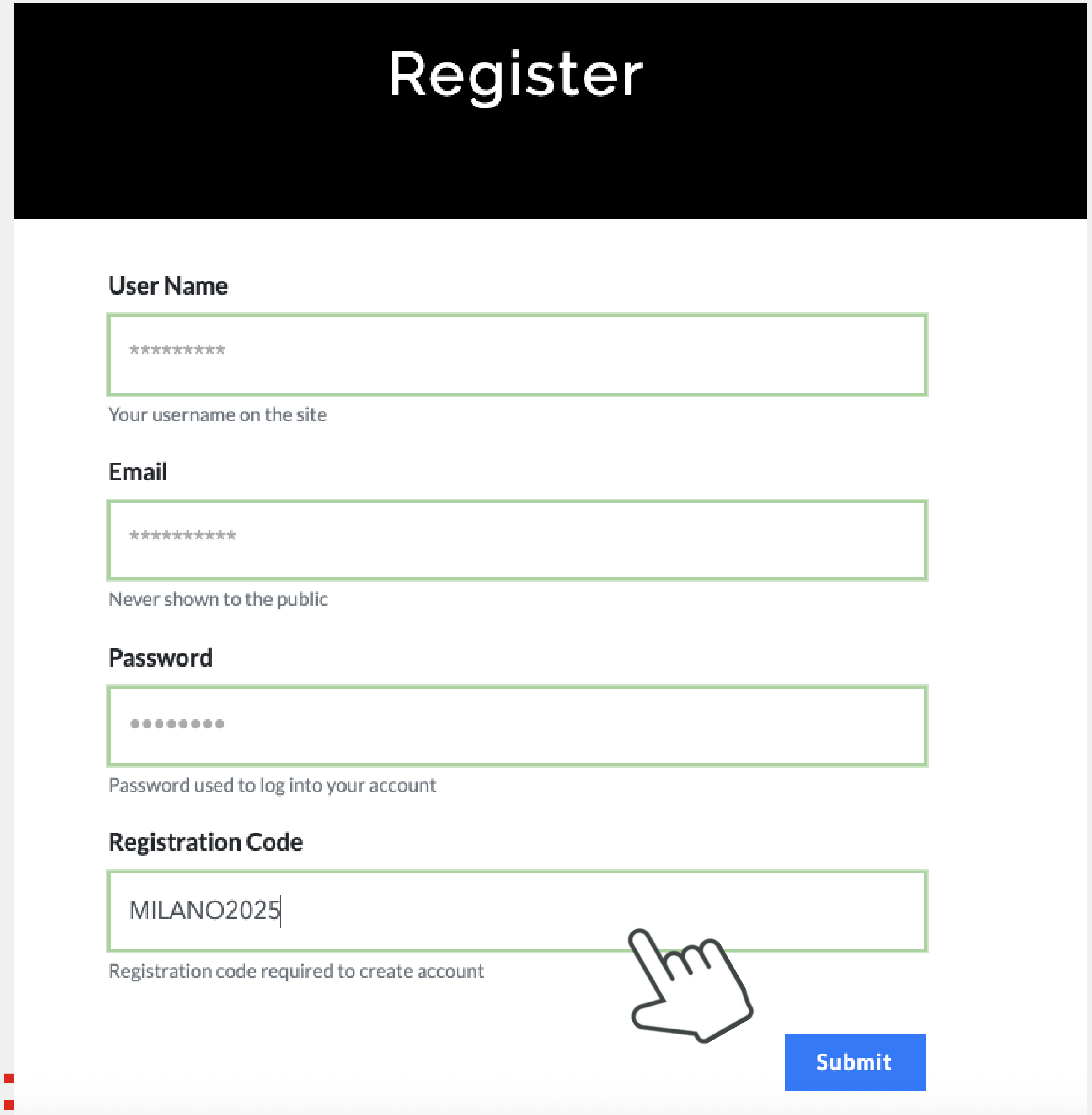
Register to the CTF site



Benvenuti ai nuovi assunti!

GUIDED CAPTURE THE FLAG – FortiCNAPP

Register to the CTF site



Register

User Name

****

Your username on the site

Email

****

Never shown to the public

Password

••••••••

Password used to log into your account

Registration Code

MILANO2025

Registration code required to create account

-> Your nickname, how you will be seen on the dashboard

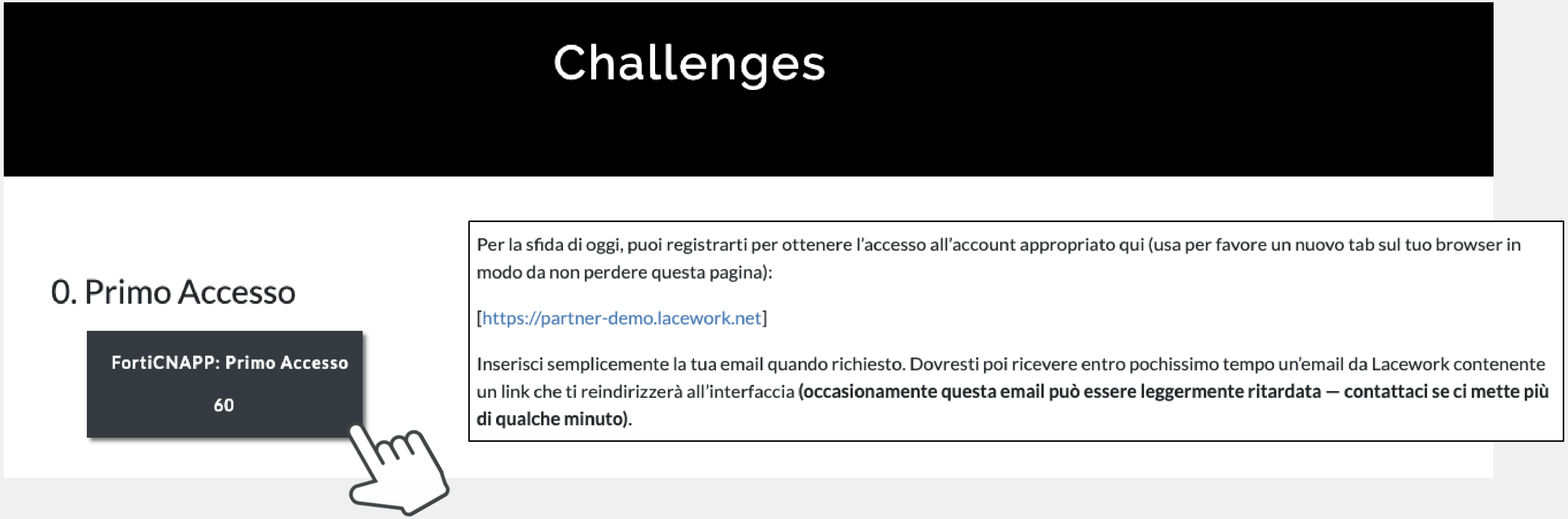
-> Your email

-> Just in case you loose your session

-> Insert «LUCCA2025»

GUIDED CAPTURE THE FLAG – FortiCNAPP

Start Capturing!



Challenges

0. Primo Accesso

FortiCNAPP: Primo Accesso

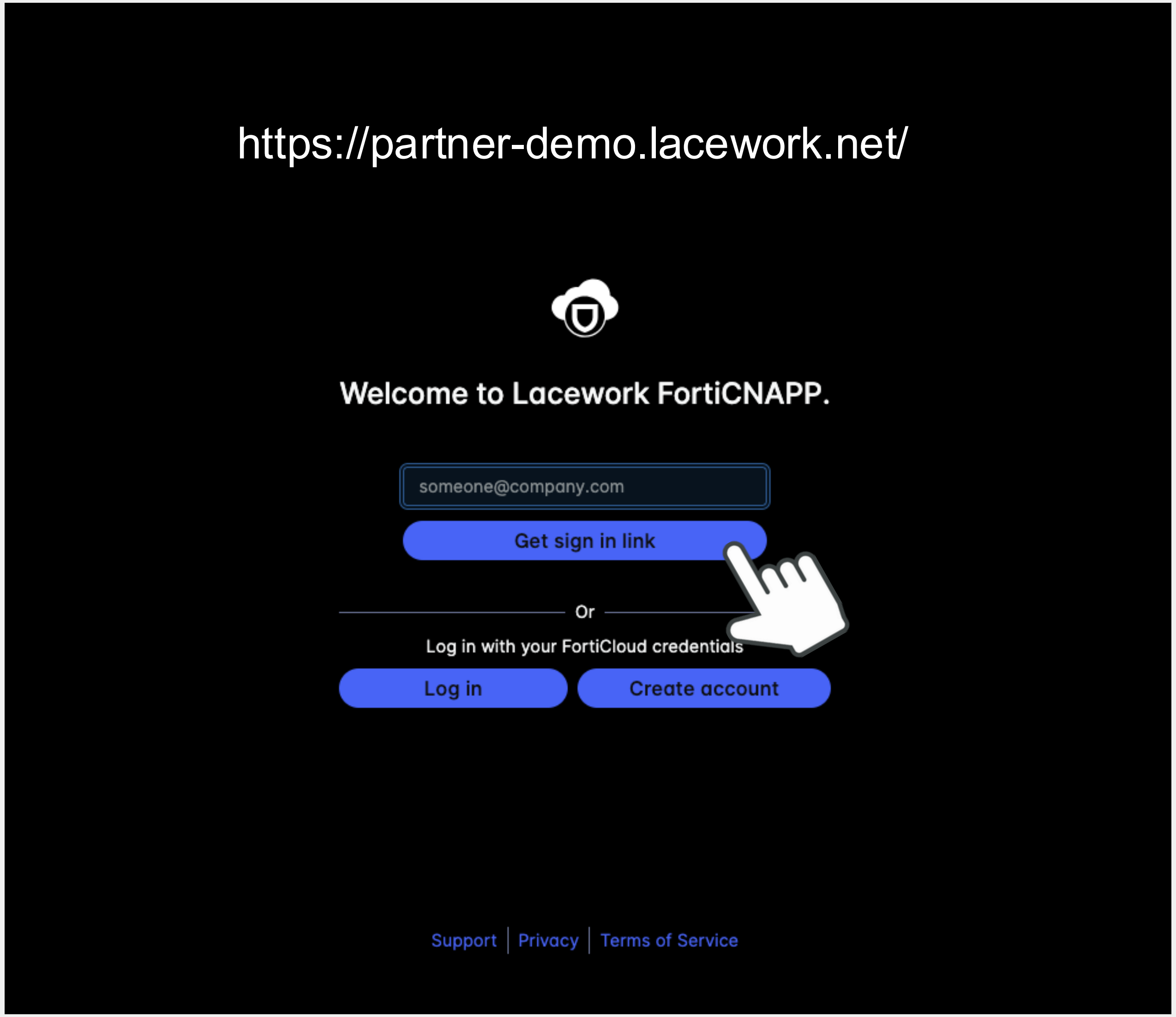
60

Per la sfida di oggi, puoi registrarti per ottenere l'accesso all'account appropriato qui (usa per favore un nuovo tab sul tuo browser in modo da non perdere questa pagina):

[https://partner-demo.lacework.net]

Inserisci semplicemente la tua email quando richiesto. Dovresti poi ricevere entro pochissimo tempo un'email da Lacework contenente un link che ti reindirizzerà all'interfaccia **(occasionamente questa email può essere leggermente ritardata — contattaci se ci mette più di qualche minuto)**.

GUIDED CAPTURE THE FLAG – FortiCNAPP

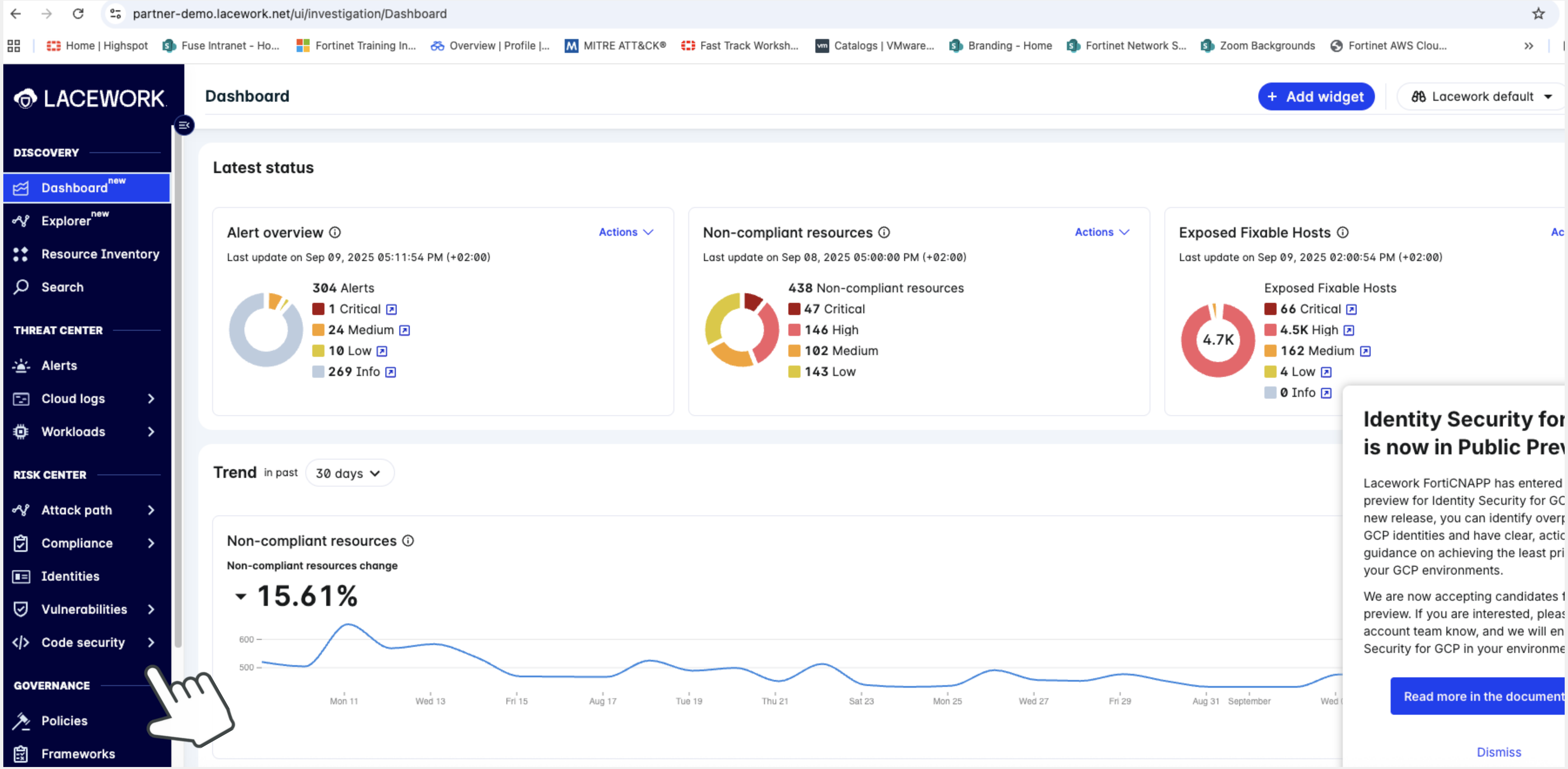


https://partner-demo.lacework.net/

Welcome to Lacework FortiCNAPP.

someone@company.com

GUIDED CAPTURE THE FLAG – FortiCNAPP



Dashboard

Latest status

Alert overview

Last update on Sep 09, 2025 05:11:54 PM (+02:00)

304 Alerts
- 🟥 1 Critical
- 🟧 24 Medium
- 🟨 10 Low
- ⬜ 269 Info

Non-compliant resources

Last update on Sep 08, 2025 05:00:00 PM (+02:00)

438 Non-compliant resources
- 🟥 47 Critical
- 🟥 146 High
- 🟧 102 Medium
- 🟨 143 Low

Exposed Fixable Hosts

Last update on Sep 09, 2025 02:00:54 PM (+02:00)

4.7K

Exposed Fixable Hosts
- 🟥 66 Critical
- 🟥 4.5K High
- 🟧 162 Medium
- 🟨 4 Low
- ⬜ 0 Info

Trend in past 30 days

Non-compliant resources

Non-compliant resources change

▾ 15.61%

Identity Security for
is now in Public Prev

Lacework FortiCNAPP has entered
preview for Identity Security for GC
new release, you can identify overp
GCP identities and have clear, actic
guidance on achieving the least pri
your GCP environments.

We are now accepting candidates f
preview. If you are interested, pleas
account team know, and we will en
Security for GCP in your environme

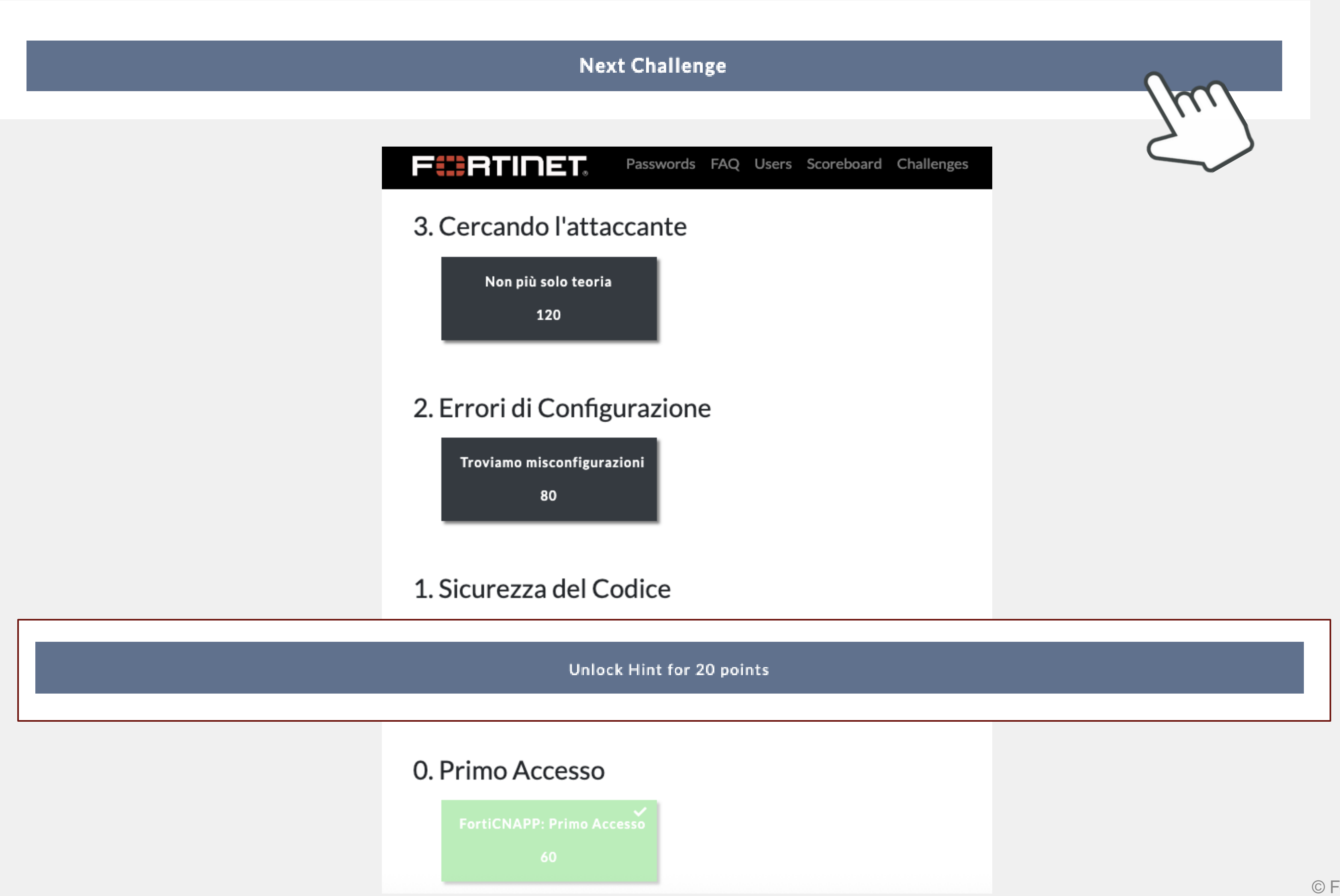
Read more in the document

Dismiss

© Fortinet Inc. All Rights Reserved.

GUIDED CAPTURE THE FLAG – FortiCNAPP

Keep Capturing Flags!



Next Challenge

FORTINET Passwords FAQ Users Scoreboard Challenges

3. Cercando l'attaccante

Non più solo teoria

120

2. Errori di Configurazione

Troviamo misconfigurazioni

80

1. Sicurezza del Codice

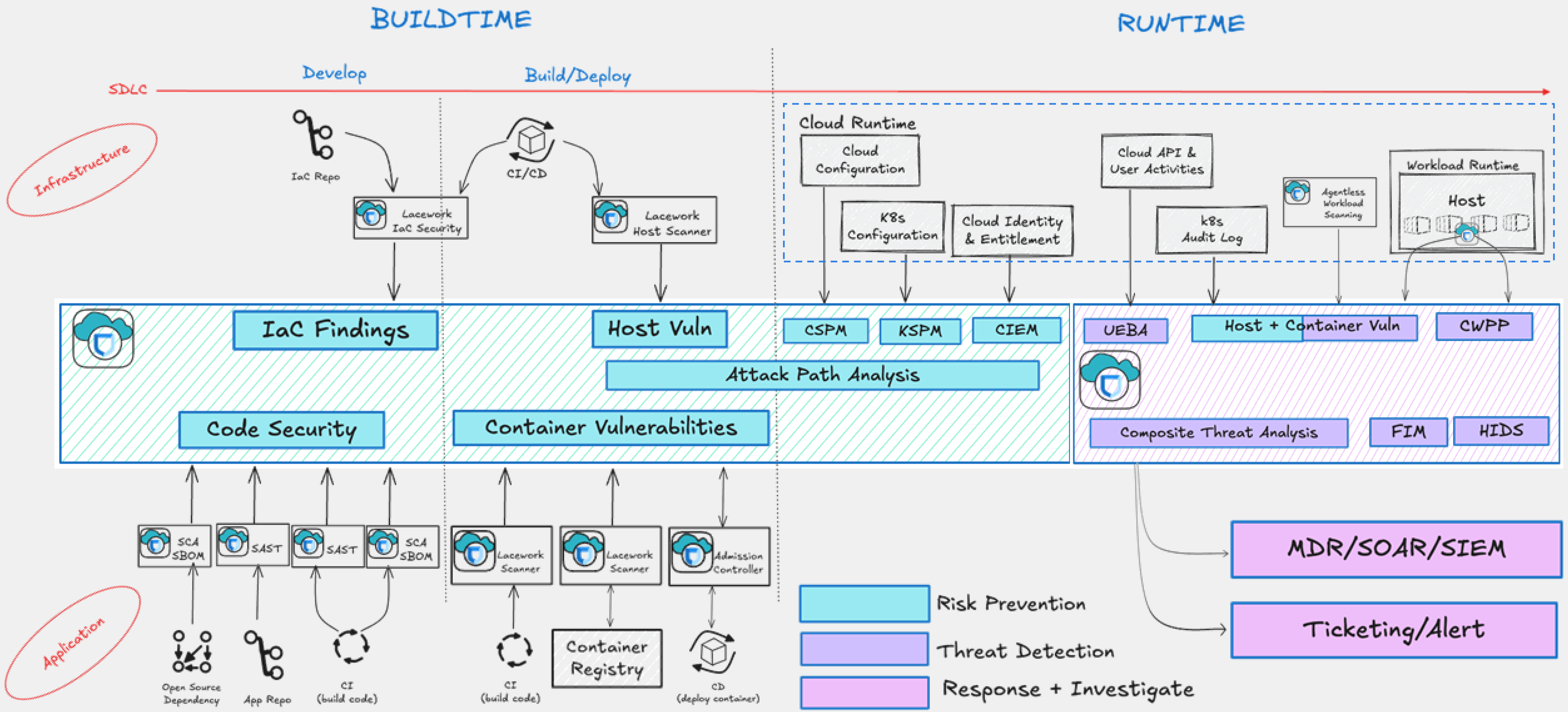
Unlock Hint for 20 points

0. Primo Accesso

FortiCNAPP: Primo Accesso ✓

60

FortiCNAPP in a nutshell



BUILDTIME

RUNTIME

Develop

Build/Deploy

SDLC

Infrastructure

Application

IaC Repo

CI/CD

Lacework IaC Security

Lacework Host Scanner

Cloud Runtime

Cloud Configuration

K8s Configuration

Cloud Identity & Entitlement

Cloud API & User Activities

k8s Audit Log

Agentless Workload Scanning

Workload Runtime

Host

IaC Findings

Host Vuln

CSPM

KSPM

CIEM

UEBA

Host + Container Vuln

CWPP

Attack Path Analysis

Code Security

Container Vulnerabilities

Composite Threat Analysis

FIM

HIDS

SCA SBOM

SAST

SAST

SCA SBOM

Lacework Scanner

Lacework Scanner

Admission Controller

Open Source Dependency

App Repo

CI (build code)

CI (build code)

Container Registry

CD (deploy container)

MDR/SOAR/SIEM

Ticketing/Alert

Risk Prevention

Threat Detection

Response + Investigate

LINK PRESENTAZIONE

https://github.com/caliaf/XPERTS2025

FORTINET