

CISCO *Live!*



#CiscoLive



The bridge to possible

Building a Scalable Open-Source IPS/IDS Platform Powered by Snort3 and Amazon Web Services

Pal Lakatos-Toth, Product Manager, Cisco

<https://www.linkedin.com/in/lakatostothpal>

Muffadal Quettawala, Solutions Architect, AWS

<https://www.linkedin.com/in/muffadal-quettawala/>

BRKSEC-2070



#CiscoLive

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 17, 2022.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2070>

About your speakers

- Name:
 - Pál Lakatos-Tóth 
 - Engineering Product Manager (Firestarter!!)
 - Cisco employee since 2016
 - 13+ Years in Security
- Free-time:
 - Family (wife, son, dog 😊), Hiking
 - Started an MSc in ML and AI (UOL)
 - No free time 😊



About your speakers

- Name:
 - Muffadal Quettawala
 - Partner Solutions Architect
 - AWS employee since 2017
 - 15+ Years in Infrastructure
- Free-time:
 - Outdoors and family!





Agenda

- Motivation and Use cases
- Solution Reference Architecture
- GitOps based CI/CD
- Amazon ECS
- AWS Gateway Load Balancer
- Snort3 Enhancements
- Solution Workflow
- Demo

Motivation and Use cases



Existing expertise and
Investments



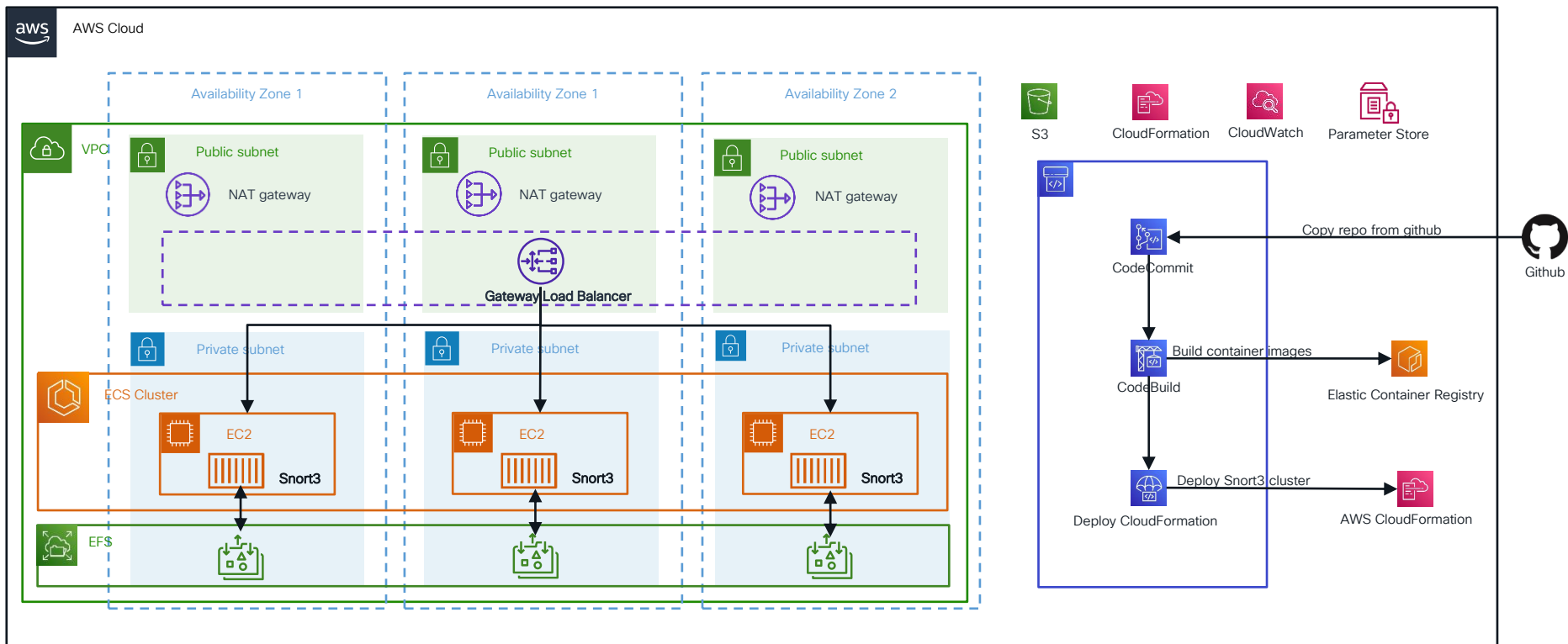
Open-Source vs.
COTS vs.
Cloud-Native



Compliance
Requirement to Inspect
East-West, Ingress and
Egress Traffic (N/S)

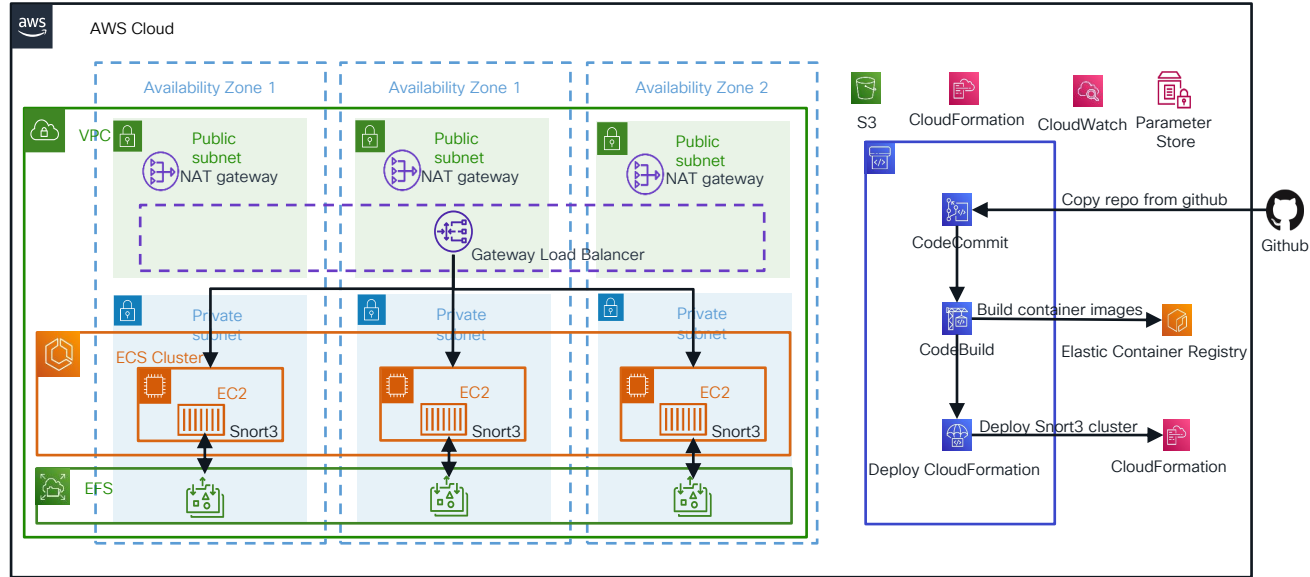
Research and Academia: DIY, Open Source, Automated and Customizable

Scalable Open-Source IPS/IDS Platform Powered by Cisco Snort3 and Amazon Web Services



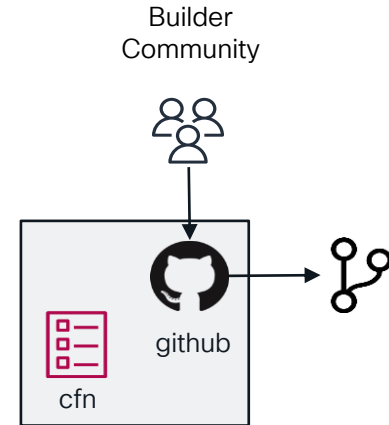
Solution Overview – Key Tenets

- GitOps based CI/CD
- Modern Application Architecture
- Cloud-Native
 - Auto-scale
 - Highly Available
 - Secure
- Logging and Monitoring



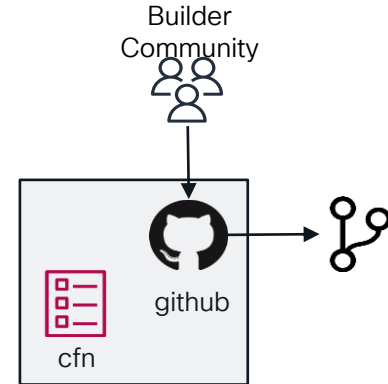
Deep Dive – GitOps based CI/CD

- Automated code compilation
- Portable
- GitOps-based code release
- Extensible



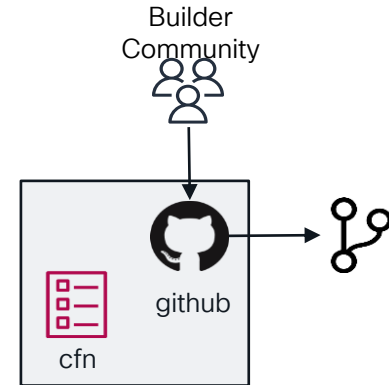
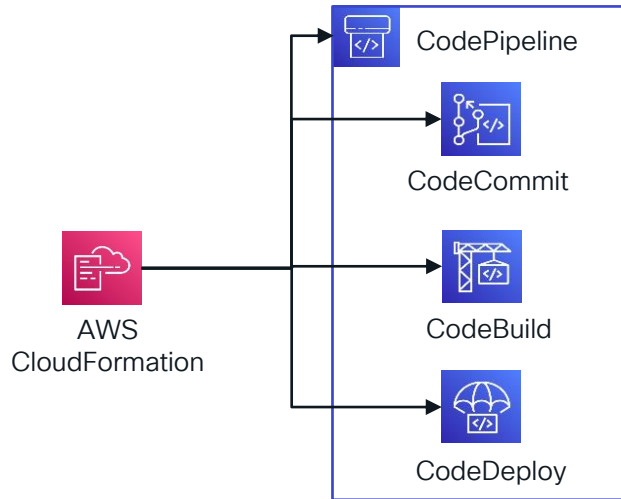
Deep Dive – GitOps based CI/CD

- Automated code compilation
- Portable
- GitOps-based code release
- Extensible



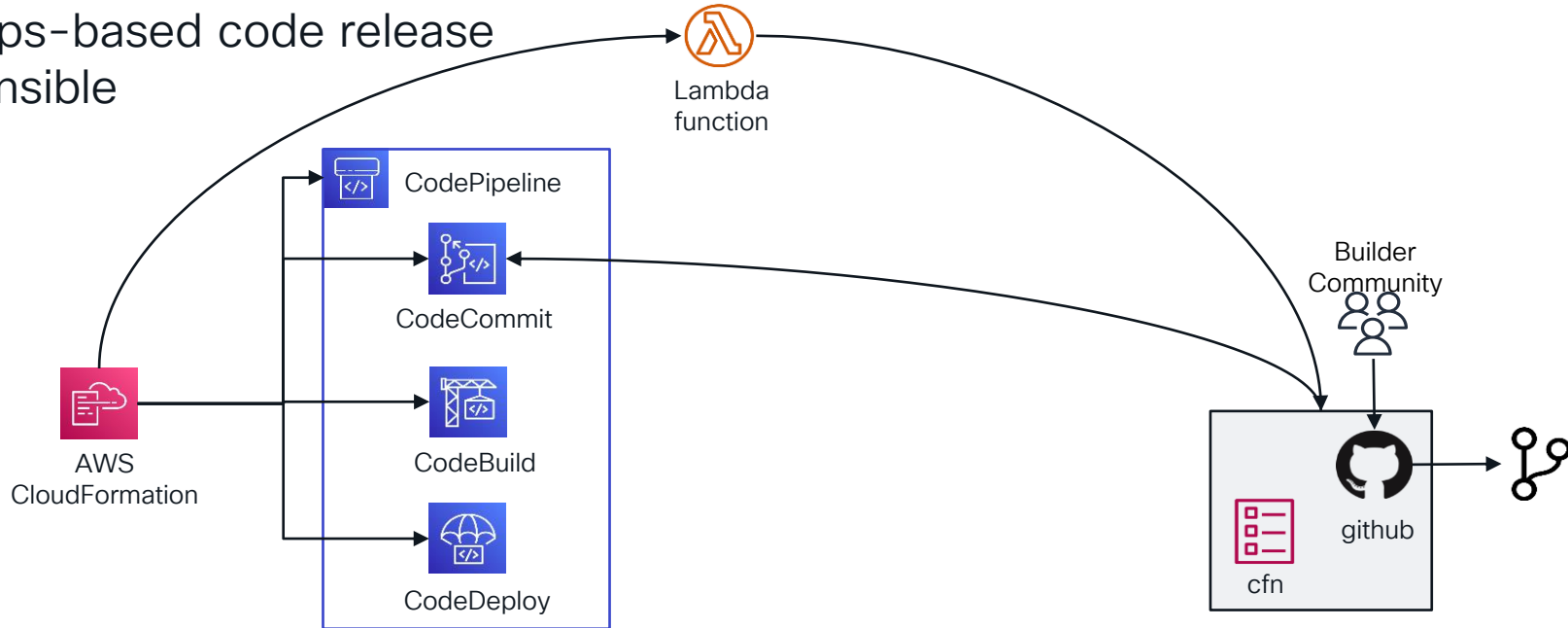
Deep Dive – GitOps based CI/CD

- Automated code compilation
- Portable
- GitOps-based code release
- Extensible



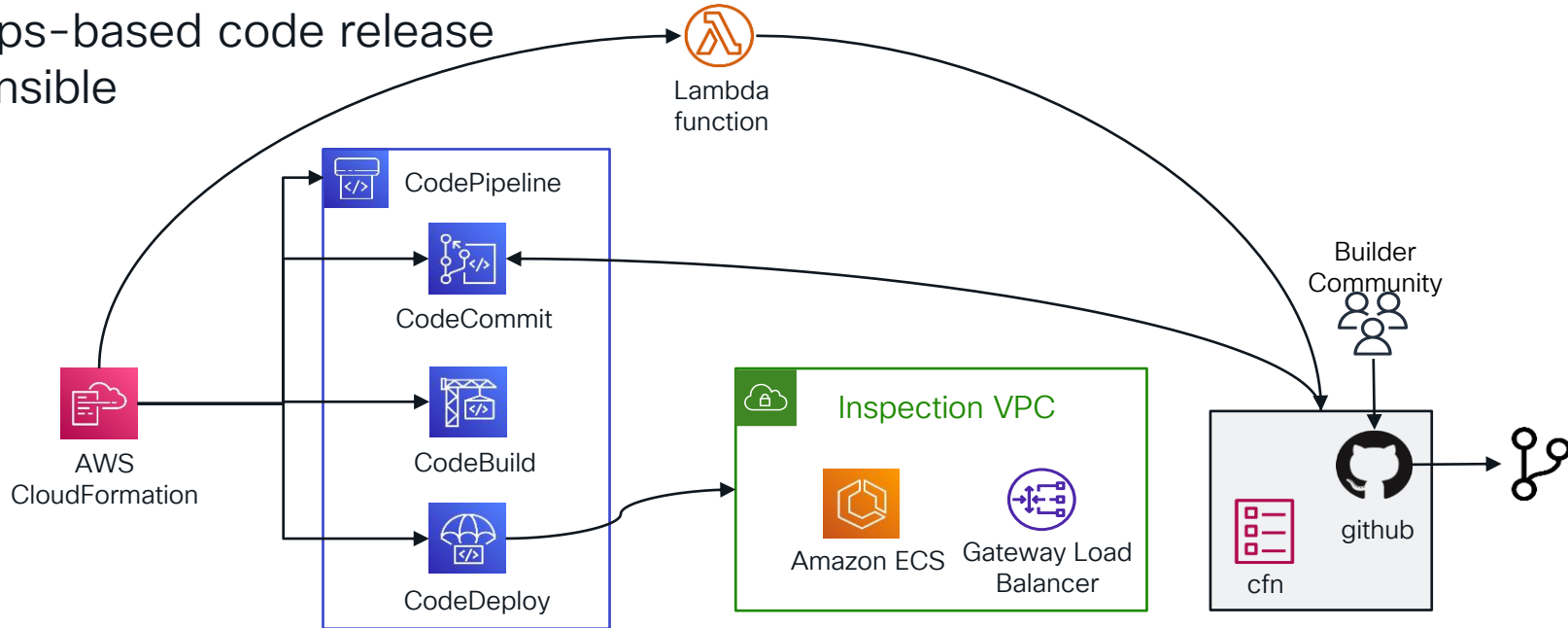
Deep Dive – GitOps based CI/CD

- Automated code compilation
- Portable
- GitOps-based code release
- Extensible



Deep Dive – GitOps based CI/CD

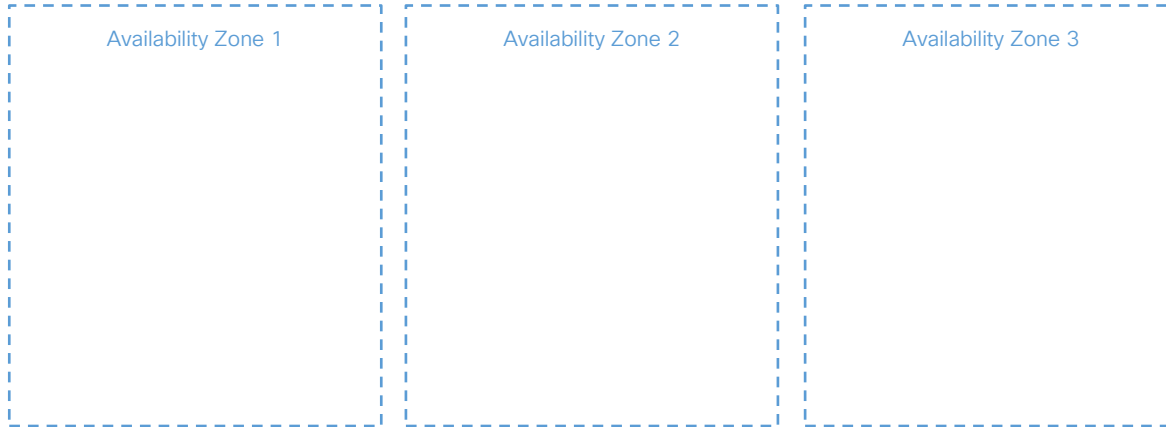
- Automated code compilation
- Portable
- GitOps-based code release
- Extensible



Deep Dive – Containerized on Amazon ECS



Inspection VPC



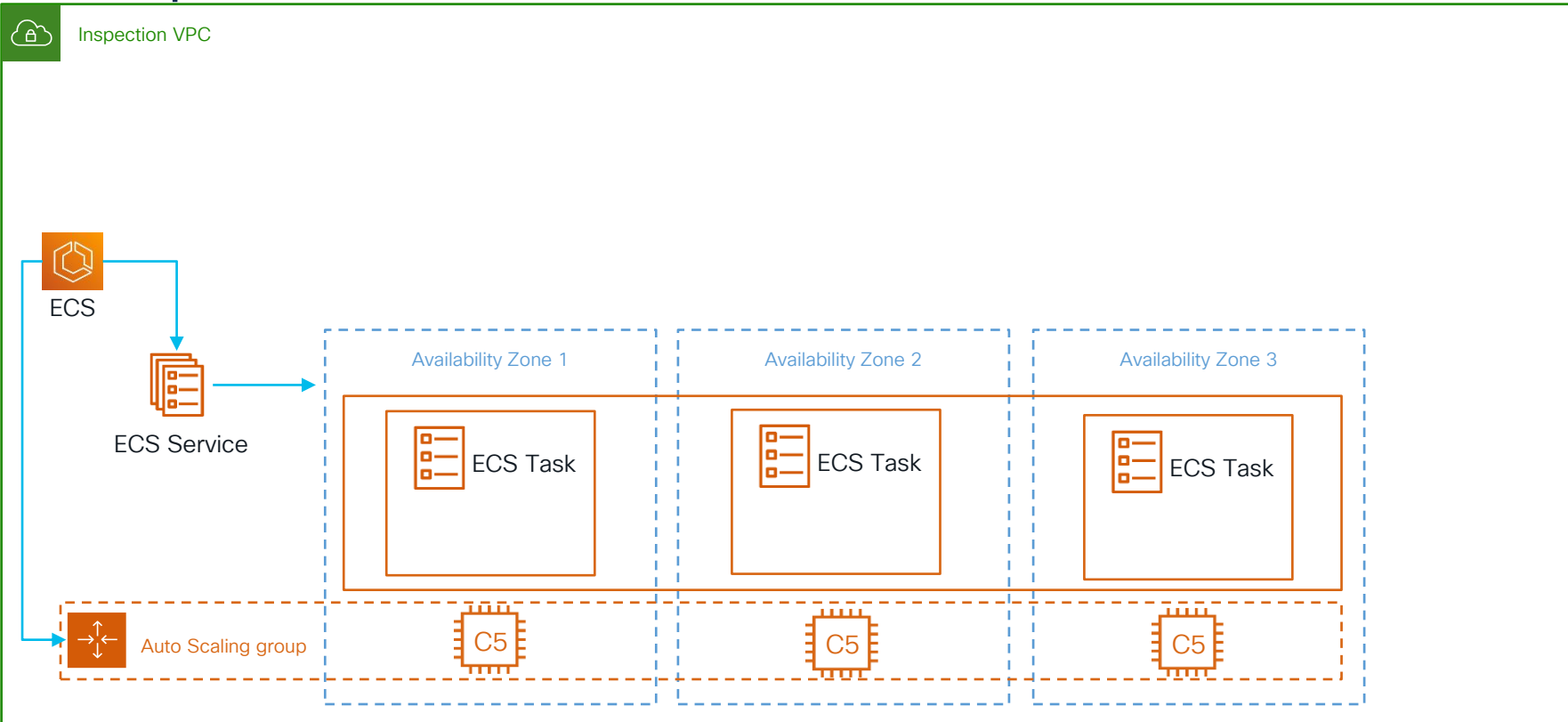
Deep Dive – Containerized on Amazon ECS



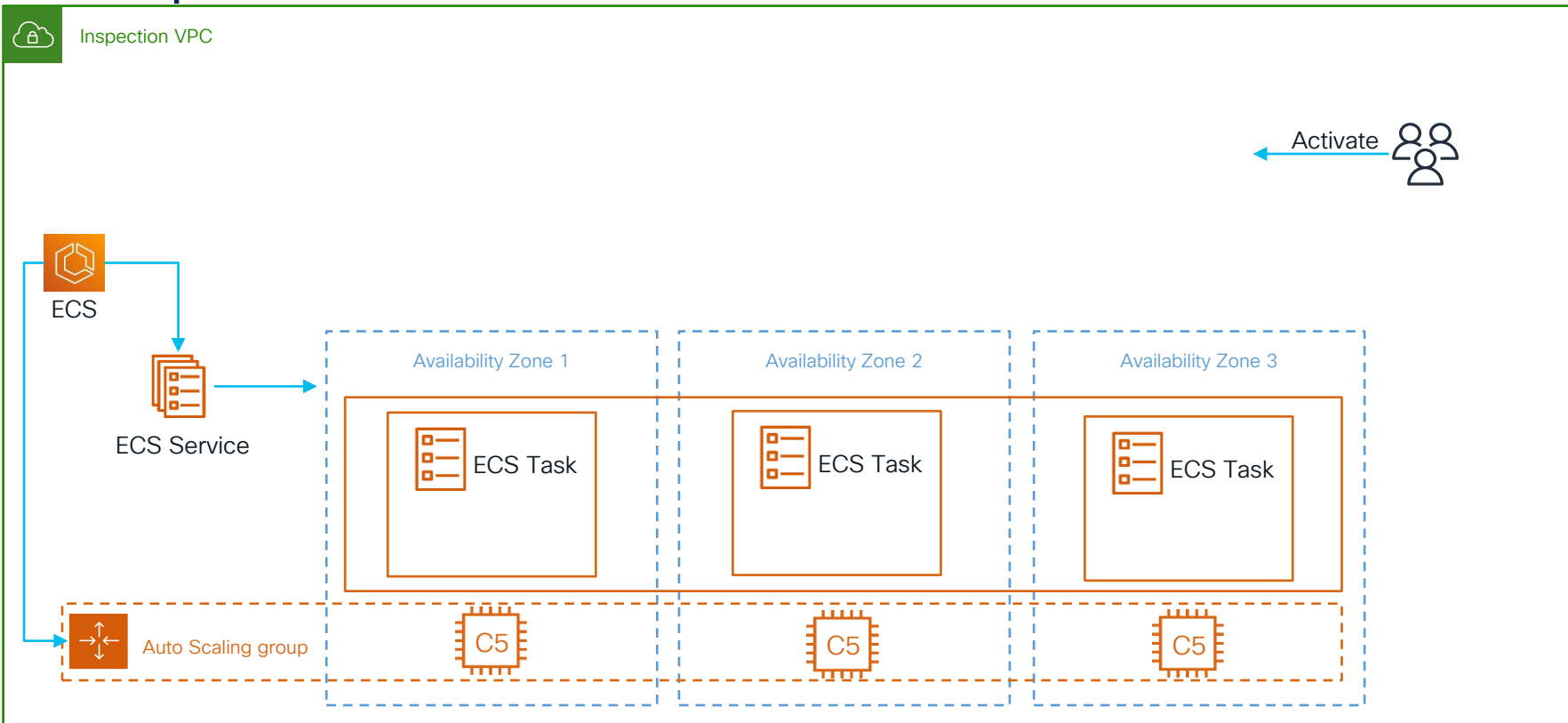
Deep Dive – Containerized on Amazon ECS



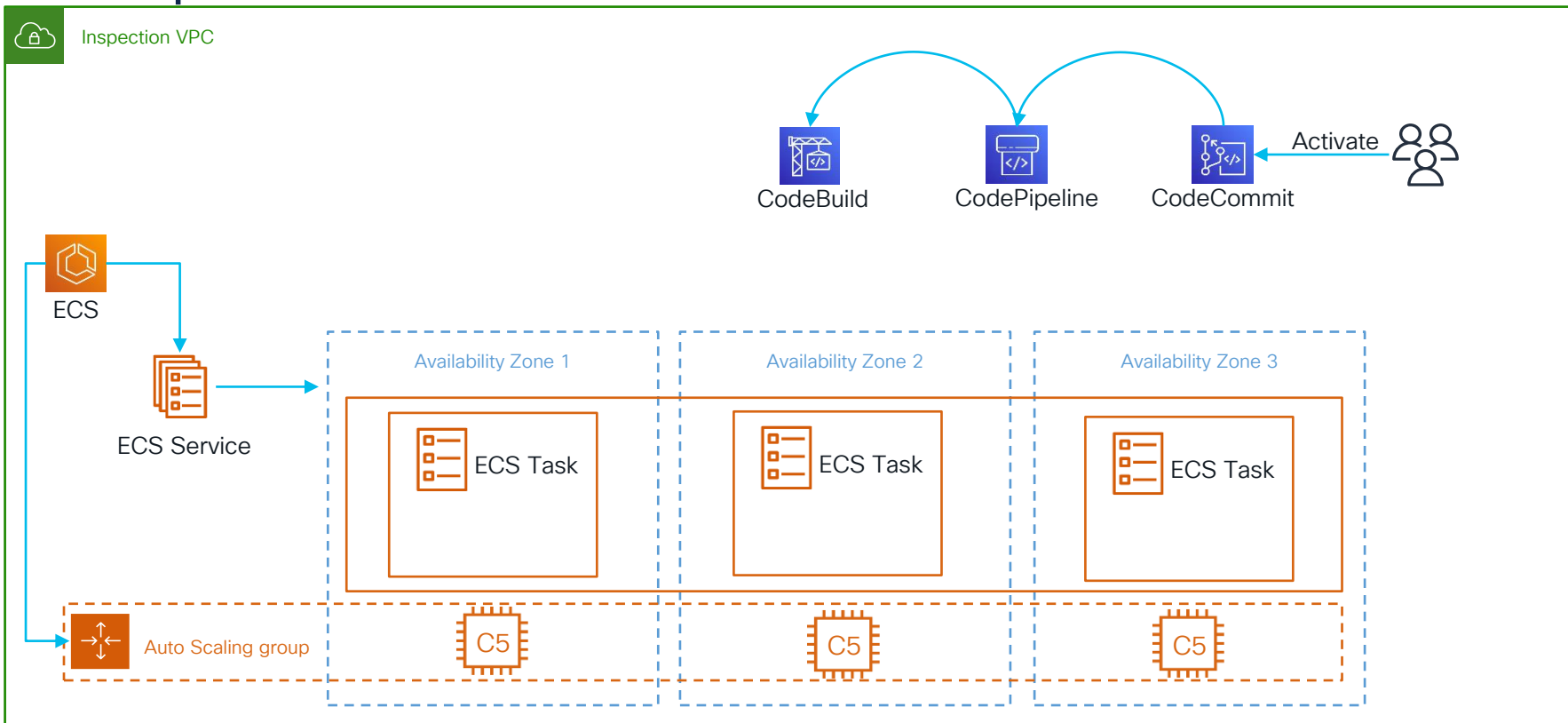
Deep Dive – Containerized on Amazon ECS



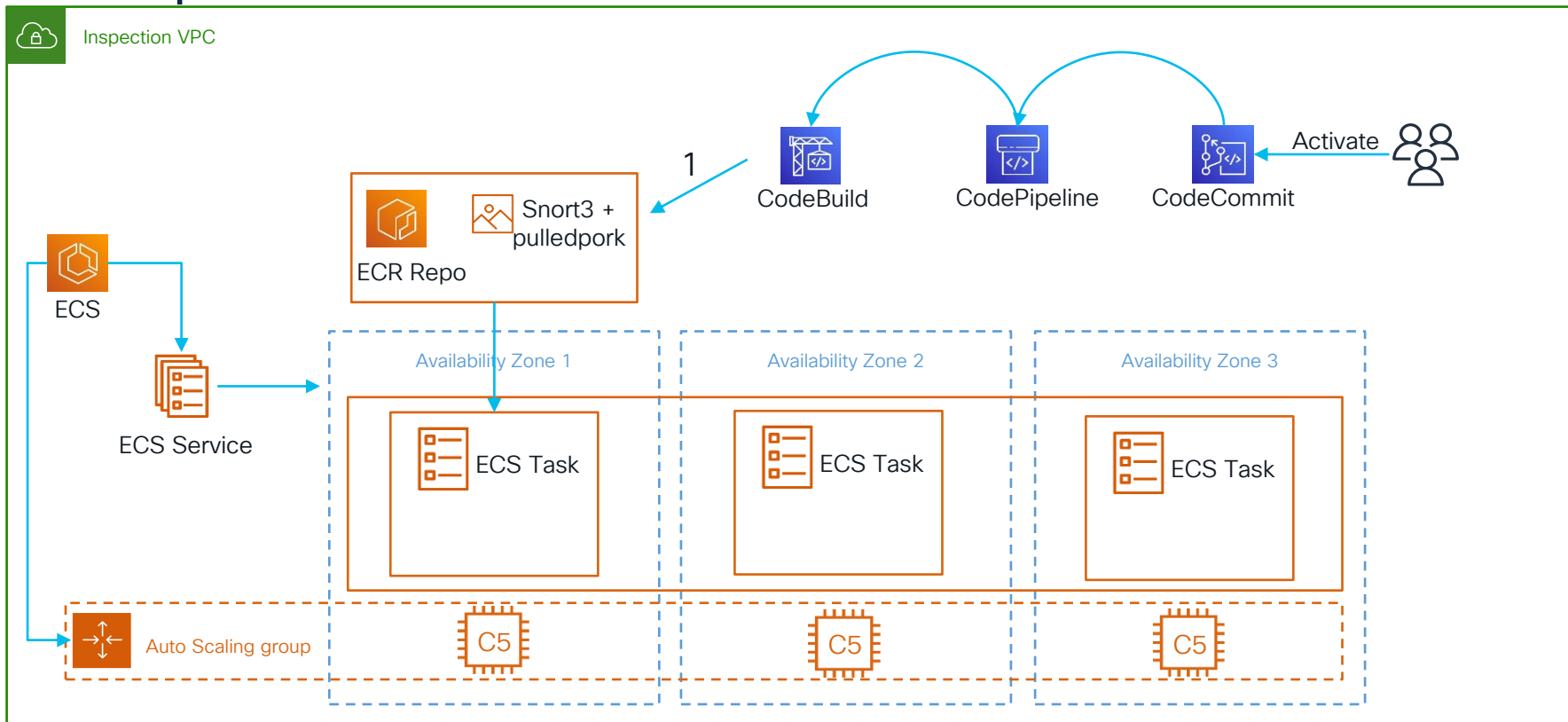
Deep Dive – Containerized on Amazon ECS



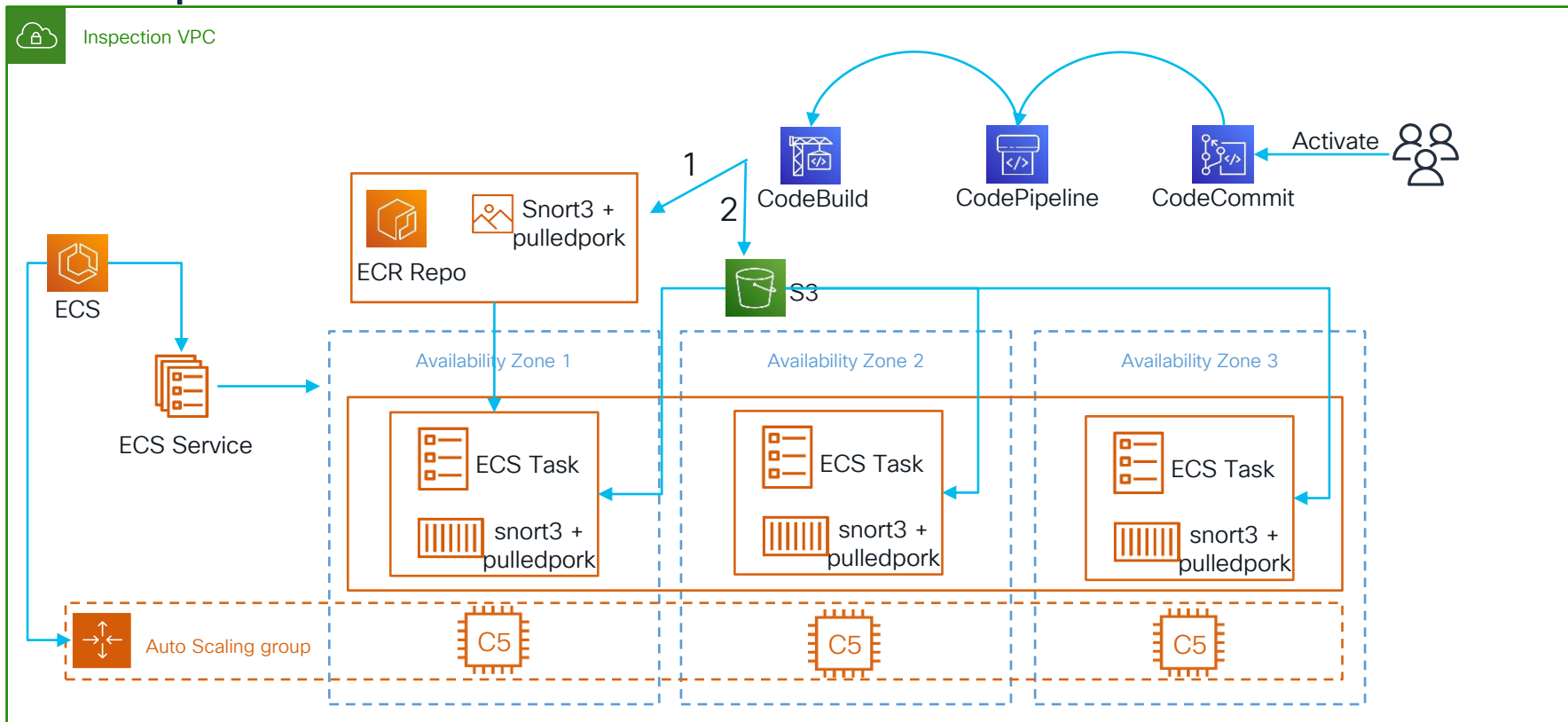
Deep Dive – Containerized on Amazon ECS



Deep Dive – Containerized on Amazon ECS



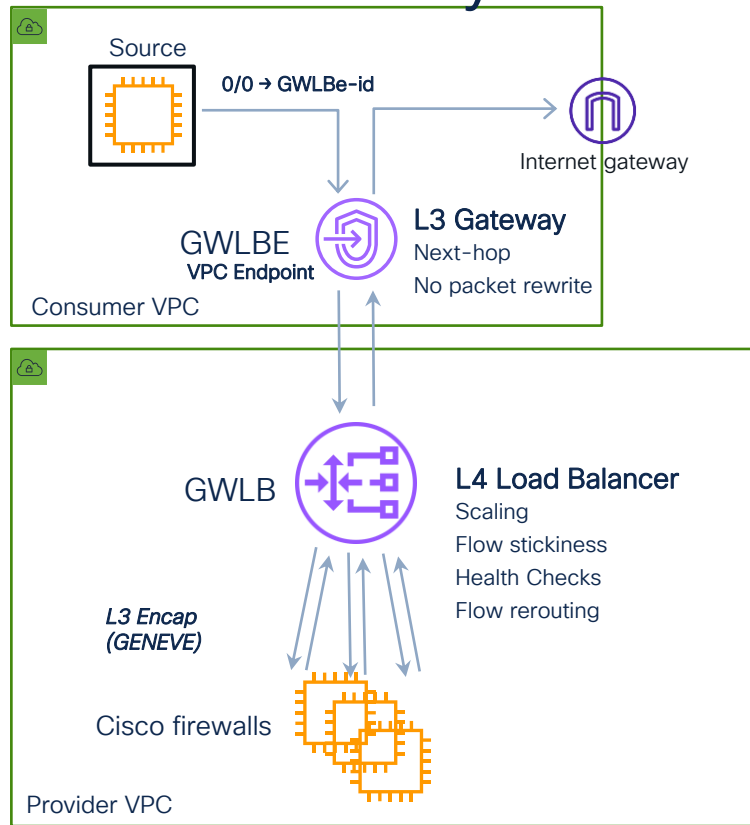
Deep Dive – Containerized on Amazon ECS



What is Geneve?

- Encapsulation Protocol
- Similar to VXLAN or GRE
- Additional Metadata Support
- AWS Gateway Load Balancer support

AWS Gateway Load Balancer



Components

- Gateway Load Balancer Endpoint (GWLBE) - A new type of VPC endpoint that can be a next-hop in a VPC route table
- Gateway Load Balancer (GWLB) - A new type of load balancer that includes L3 Gateway + L4 Load Balancer capabilities


Benefits

- Horizontal auto-scaling
- Fault tolerant (active/active)
- Transparent network insertion
- Separate security and user admin domains, share across different VPCs and AWS accounts
- Provide Appliance-as-a-Service, (e.g. Firewall-as-a-Service)

Deployment

- Create GWLB and appliance fleet and GWLBe
- Send traffic to GWLBE by updating VPC route tables

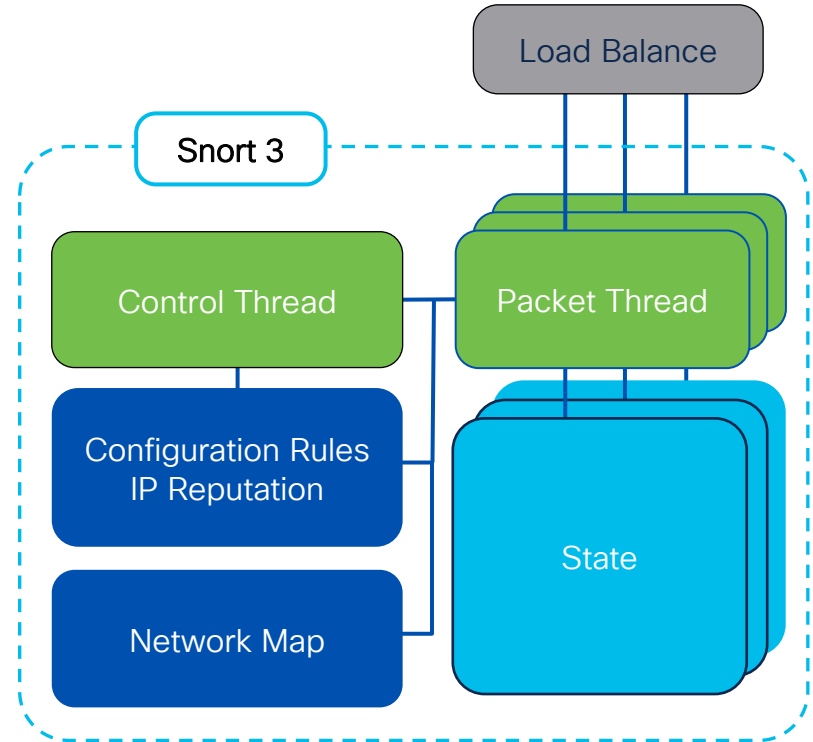
Snort Basics

- Packet Sniffer (other names: Packet Acquisition)
 - Uses Data Acquisition Module (DAQ)
 - PCAP
 - AFPacket
 - IPQ
 - NFQ
 - IPFW
 - GWLB 
 - Packet Decoder
 - Parses packet data fields (similar to tcpdump)
 - Decoded packets passed to other Snort elements



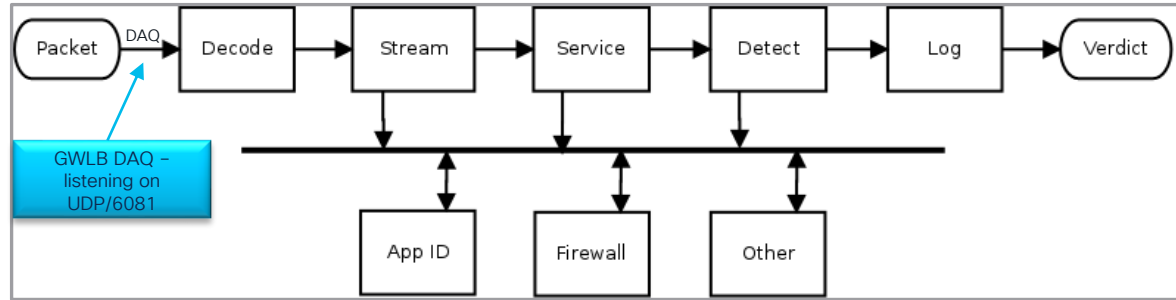
Snort 3 Architecture

- Threaded to use multiple cores:
 - 1 control thread (main)
 - N packet threads per process
 - Reloads faster (1 vs N)
- One copy of config and network map:
 - Uses less memory
 - Supports more IPS rules and larger netmap



Snort 3 Packet Processing

- Uses publish-subscribe model
- Plugin communication is event driven
- Subscribers can access the raw or normalized data as needed
- JIT buffers



High-Level Solution Architecture



How the end-to-end workflow looks like?



CloudFormation

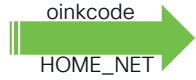


AWS CodeCommit Repo

```
snort_defaults.lua
pulledpork.conf
snort.lua
local.rules
docker-entrypoint.sh
```



CloudFormation



AWS CodeCommit Repo

```
snort_defaults.lua
pulledpork.conf
snort.lua
local.rules
docker-entrypoint.sh
```



CloudFormation



AWS CodeCommit Repo

```
snort_defaults.lua
pulledpork.conf
snort.lua
local.rules
docker-entrypoint.sh
```

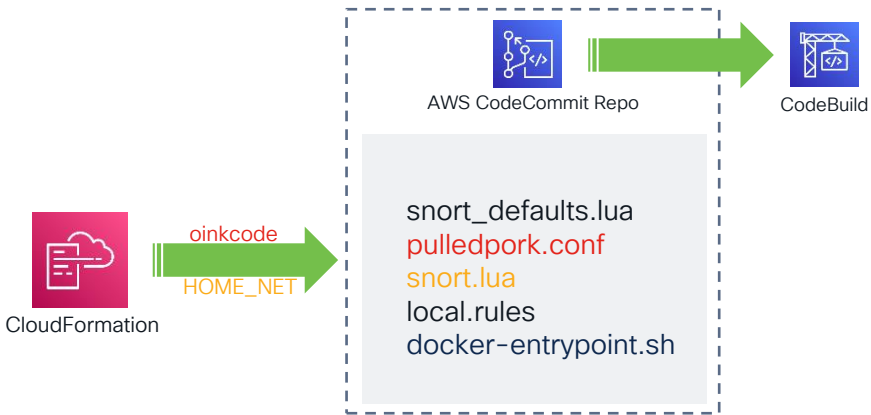


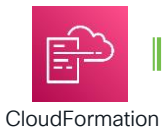

CloudFormation

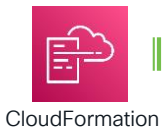


AWS CodeCommit Repo

```
snort_defaults.lua
pulledpork.conf
snort.lua
local.rules
docker-entrypoint.sh
```







oinkcode
HOME_NET



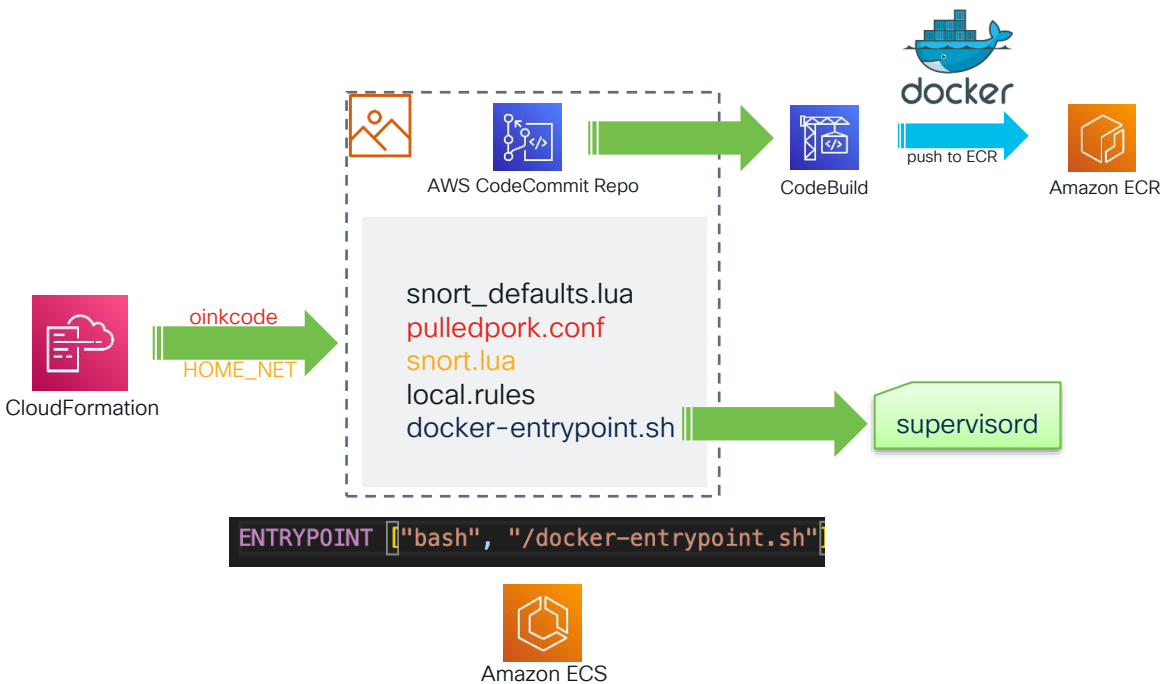
push to ECR

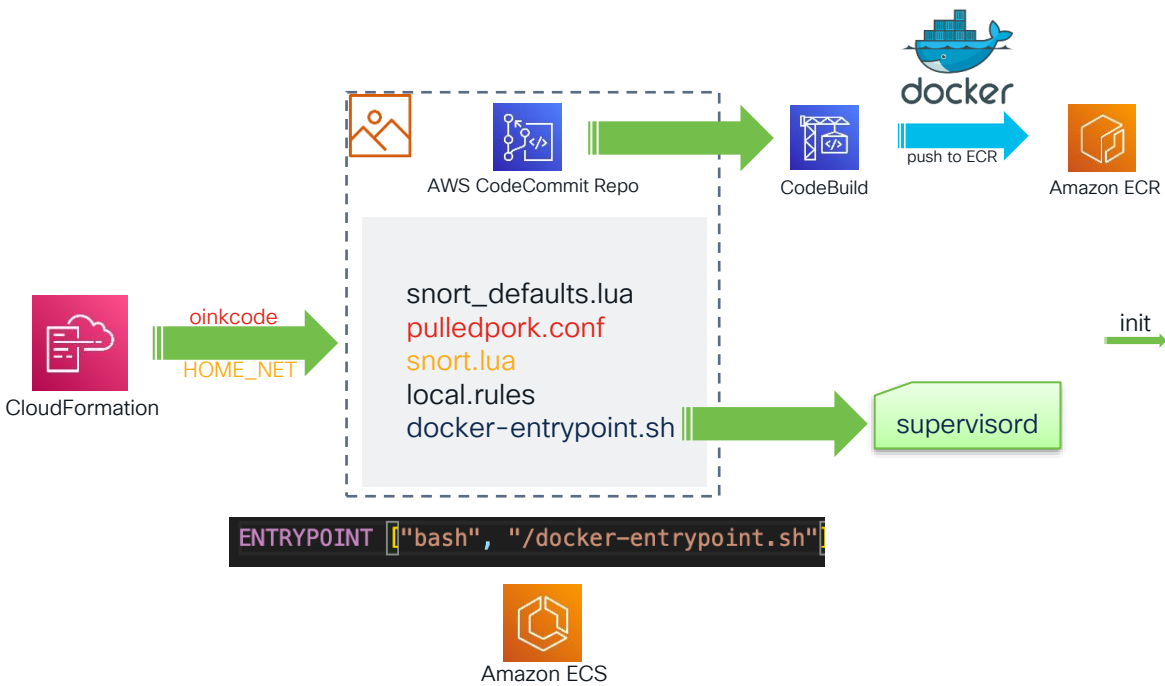


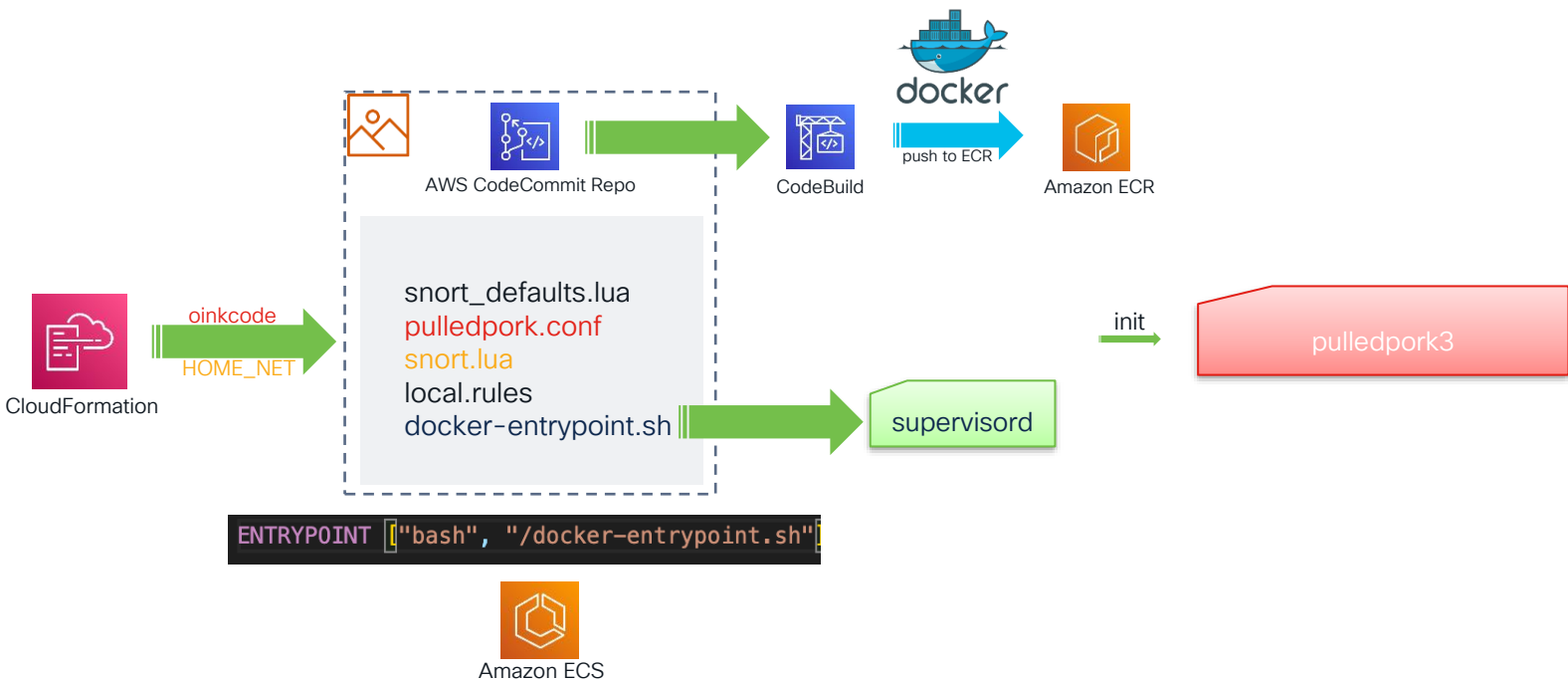
```
ENTRYPOINT ["bash", "/docker-entrypoint.sh"]
```

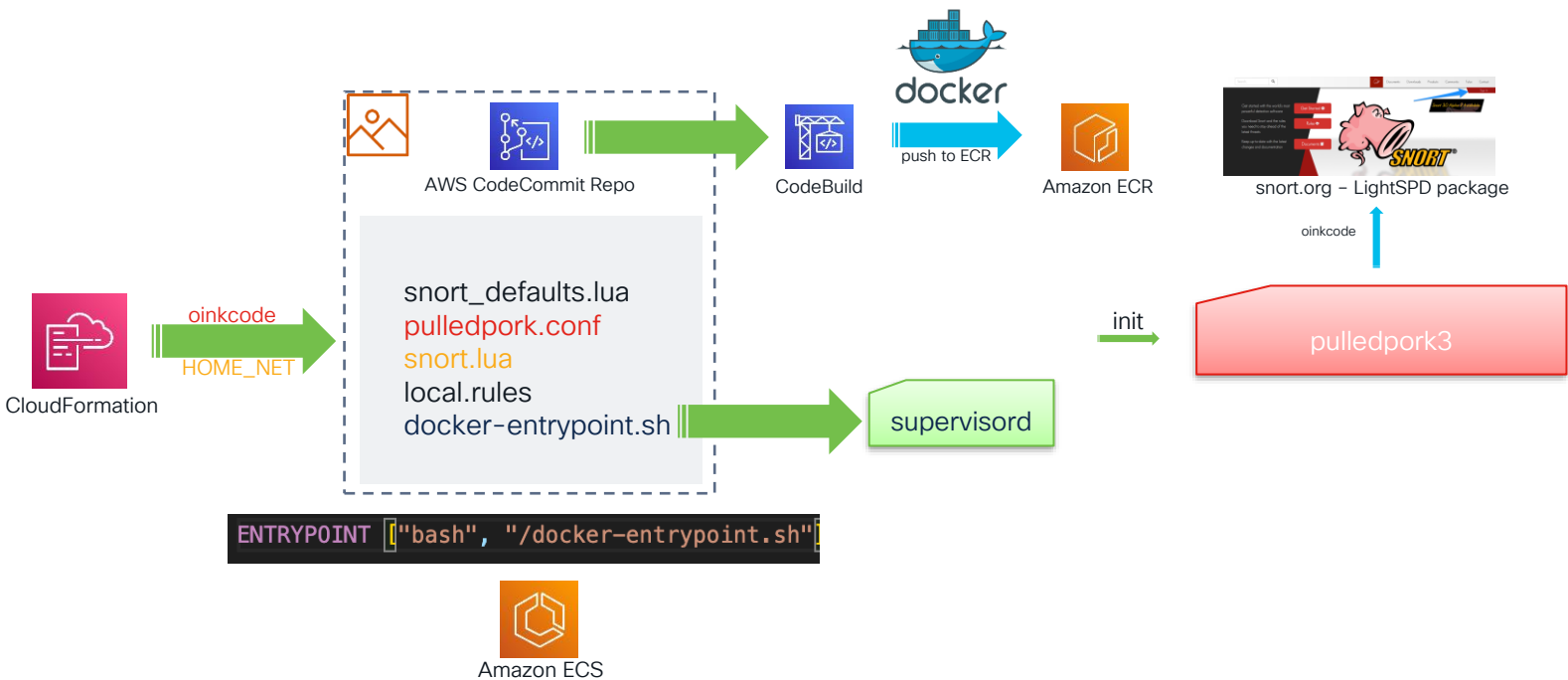


Amazon ECS



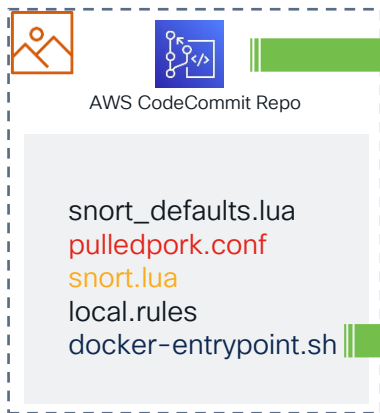








oinkcode
HOME_NET



AWS CodeCommit Repo



CodeBuild



push to ECR



Amazon ECR

init

supervisord



snort.org - LightSPD package

oinkcode

TALOS

blacklist

pulledpork3

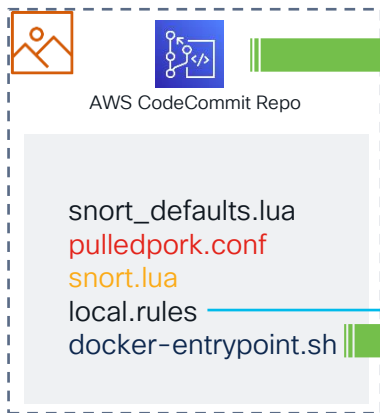
```
ENTRYPOINT ["bash", "/docker-entrypoint.sh"]
```



Amazon ECS



oinkcode
HOME_NET



custom rules

init

supervisord

pulledpork3

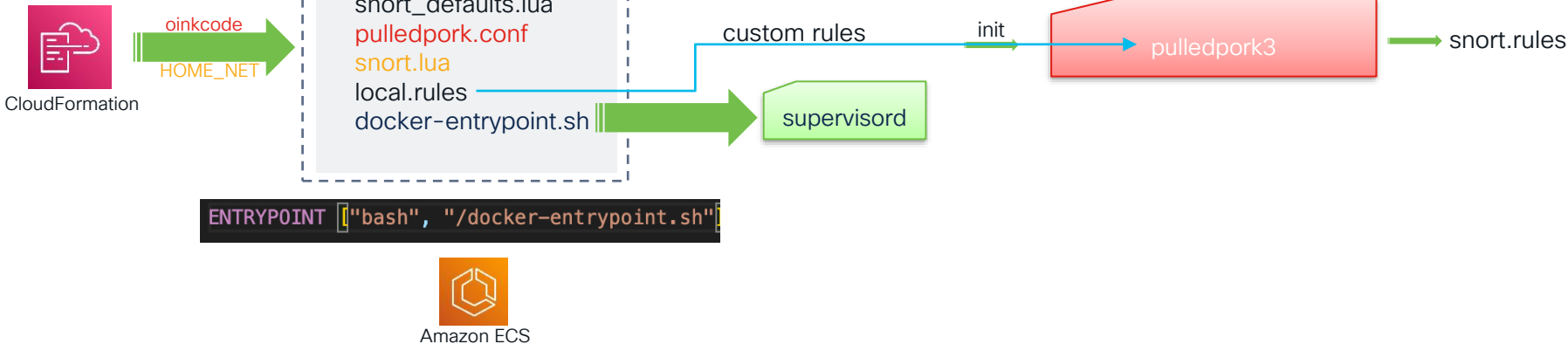
oinkcode

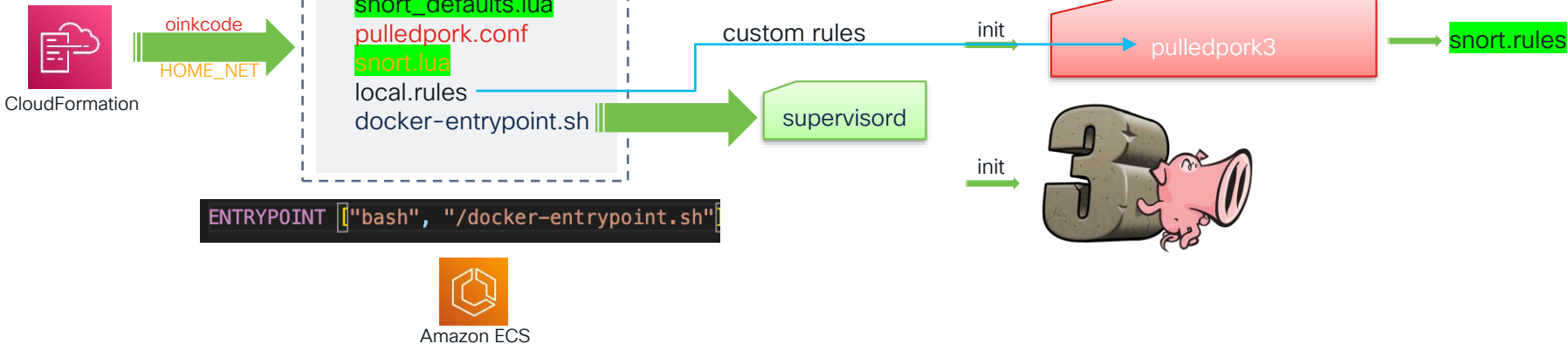


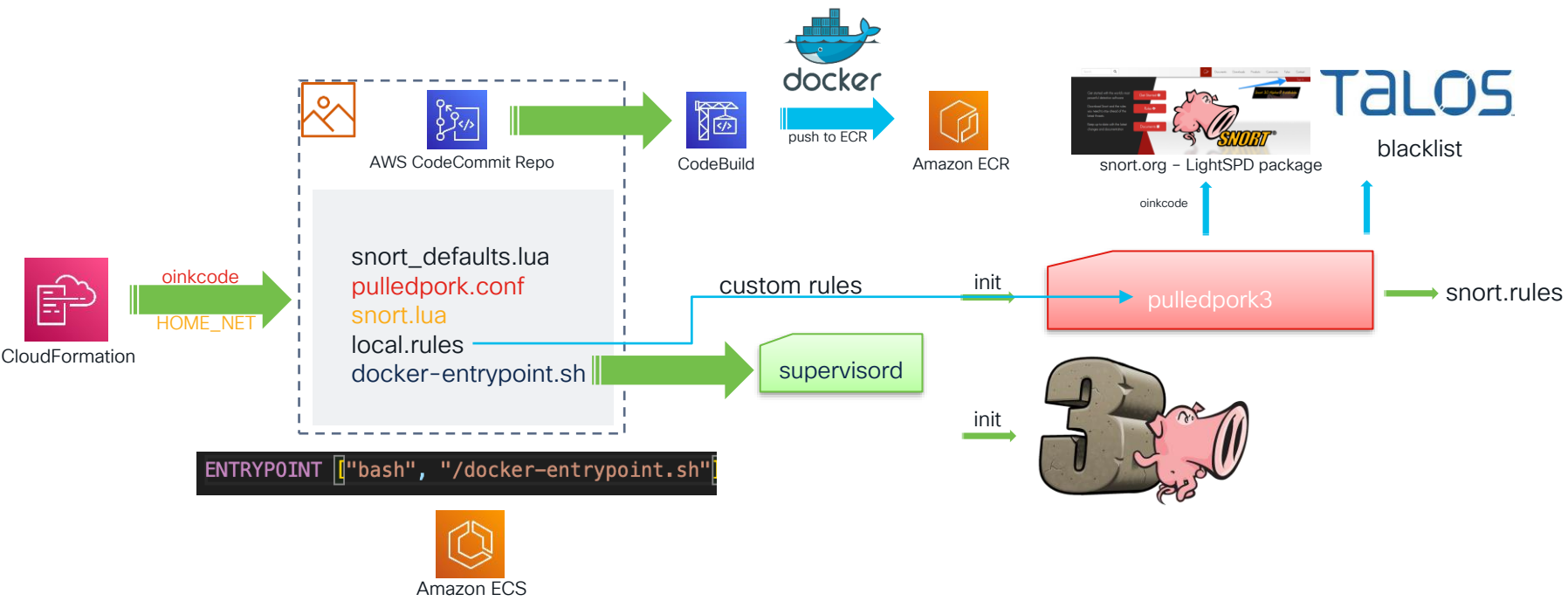
```
ENTRYPOINT ["bash", "/docker-entrypoint.sh"]
```

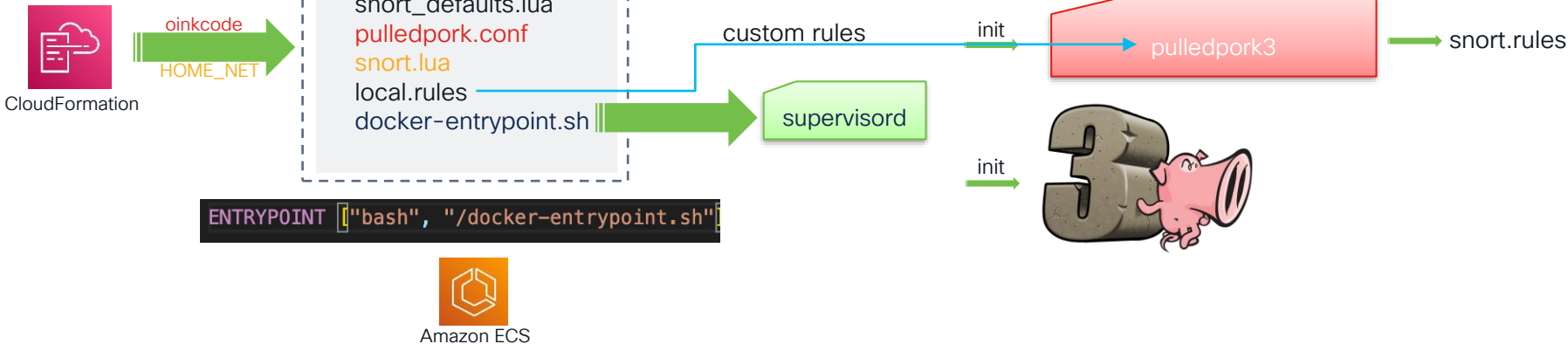


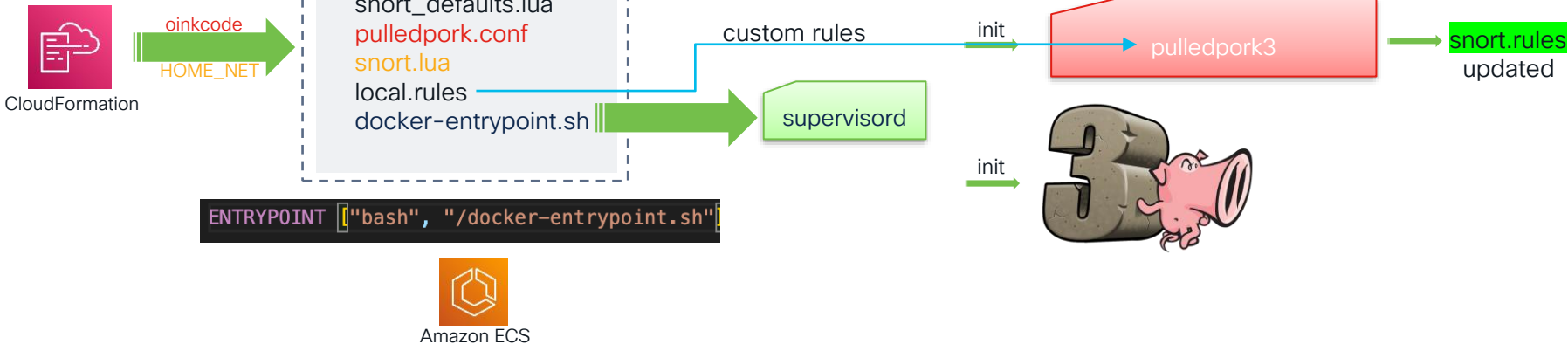
Amazon ECS

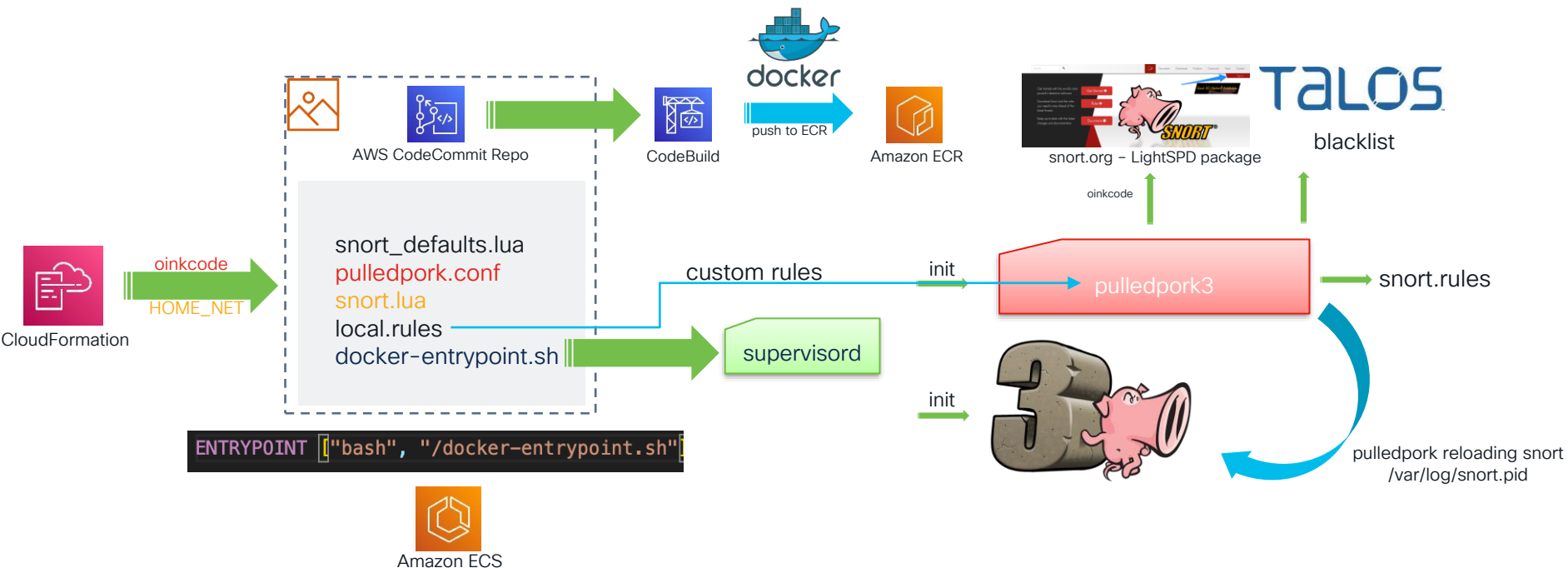


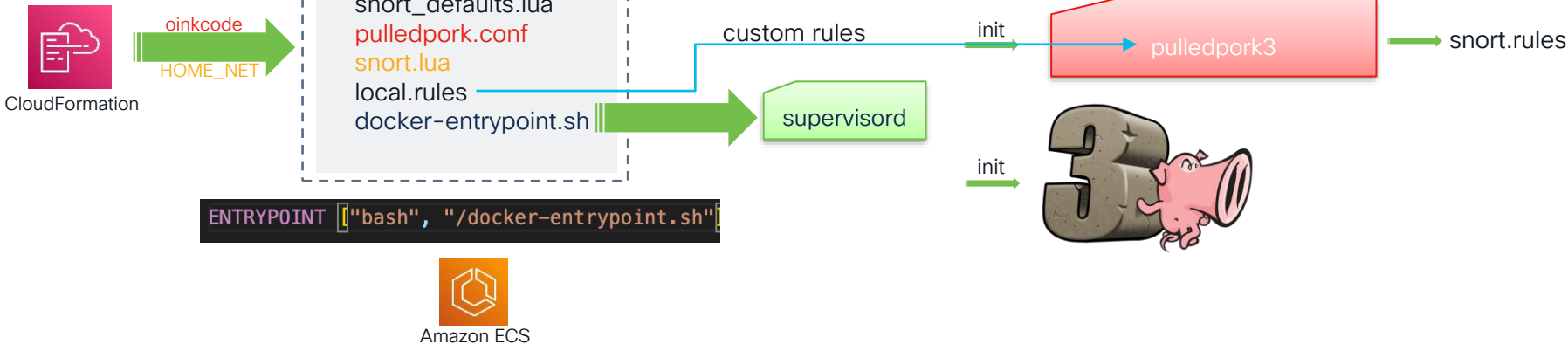




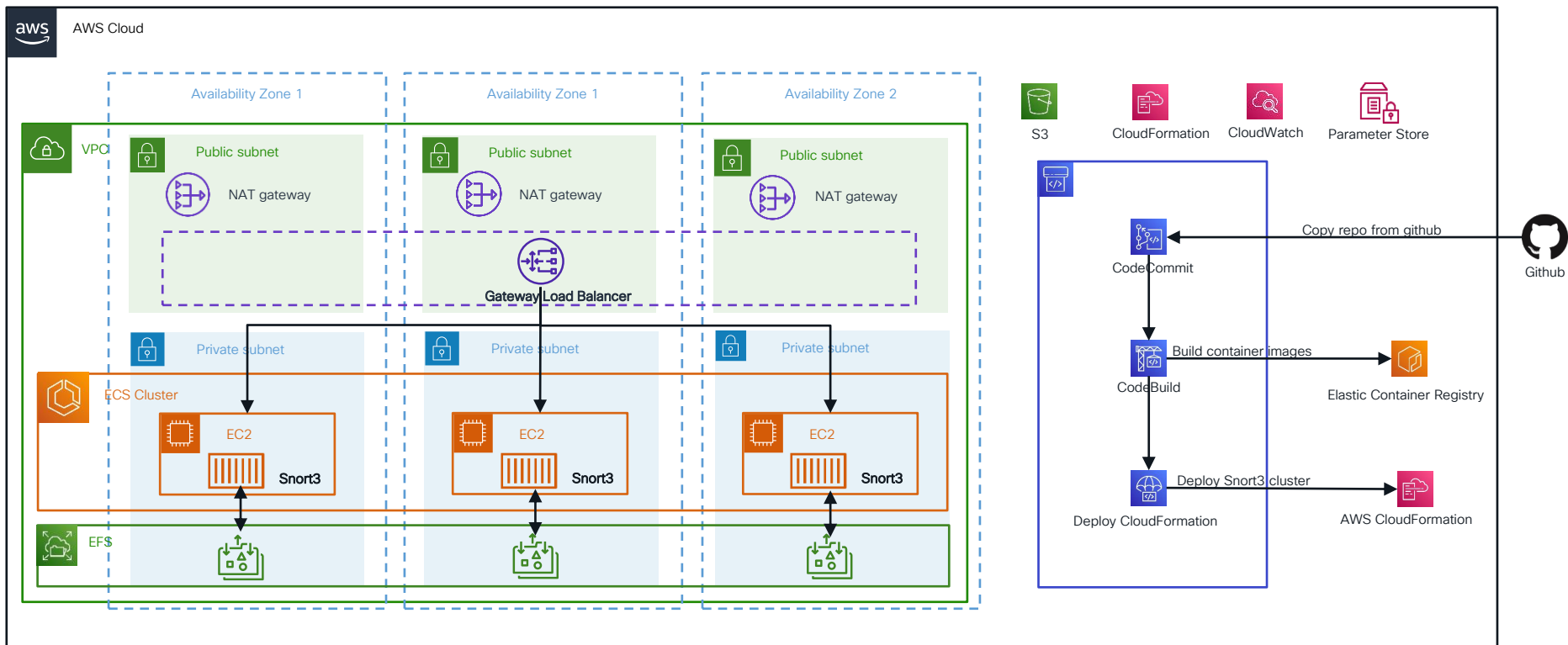








Scalable Open-Source IPS/IDS Platform Powered by Cisco Snort3 and Amazon Web Services



Demo

Special thanks:

AWS Suricata IPS/IDS Project Owners:

Adam Palmer @ AWS

Nick Coval @ AWS

Cisco Snort3 Engineering Team:

Raman Krishnan @ Cisco

Changxue Deng @ Cisco

Mike Dorsey @ Cisco

Russ Combs @ Cisco

Try It Now



<https://github.com/p4lcsi/scalable-snort-gwlb-cicd>

Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- 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.



Security Operations

SECURE X (XDR)

Managed Detection and Response Services

Security, Orchestration, Automation and Response

Incident Response and Remediation Services

Threat Visibility & Hunting

Device Insights

Kenna Vuln Mgmt

Secure Cloud Insights

3rd Party Integrations

User/Device Security

ZERO TRUST

Adaptive MFA | Passwordless | Trust

Duo Secure Access Secure E-mail

SASE/REMOTE WORKER

Unified Client | EDR | Cloud Managed



Cisco Secure Client

VPN
Posture
Telemetry
Threat
Query

ThousandEyes (Visibility)

Device Mgmt
 Meraki SM
OS, App Control

Network Security

Cloud Edge

SECURE ACCESS SERVICE EDGE (SASE)

Threat Protection | Secure Access Control | Managed Remote Access

ZERO TRUST

PRIVATE CLOUD EDGE (MSP or CUSTOMER)

Reliable | Scalable | Flexible

Umbrella/Duo

ZTNA DNS-layer security Secure web gateway L7 firewall + IPS Cloud access security broker/shadow IT
 RAaaS SSL decryption Remote browser isolation Data loss prevention Cloud malware detection

SDWAN

Cisco Meraki SDWAN SDWAN by Viptela Secure Firewall ThousandEyes Cloud DDoS, WAF

On-Premises

SASE/SDWAN

Scalable | Flexible | Visibility | Comprehensive Security

Network Edge Cisco Meraki SDWAN SDWAN by Viptela Secure Firewall ThousandEyes

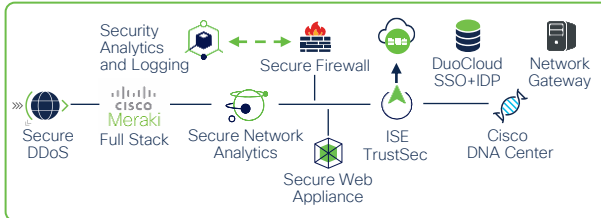
IoT/OT SECURITY

Secure Critical Infrastructure | Unified IT and OT

Industrial Router Industrial Firewall Industrial Switch/AP Cyber Vision ISE TrustSec

ZERO TRUST

Segmentation | Identity and Context | Profiling | Containment | Encrypted Visibility



Application Security

ZERO TRUST

Policy | API Security
Application Segmentation
Run-time Application Security

Application Security Stack

Cloud Native Security APIC
 Secure Workload Secure Application by AppDynamics



App Observability | Detection | Response

Hybrid Private Public Cloud
 Secure Cloud Analytics Secure Firewall
 ThousandEyes Secure DDoS, WAF/Bot

Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.



Learn

Cisco U.

IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning

Subscription-based product, technology, and certification training

Cisco Modeling Labs

Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network

Resource community portal for certifications and learning



Train

Cisco Training Bootcamps

Intensive team & individual automation and technology training programs

Cisco Learning Partner Program

Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training

Accelerated curriculum of product, technology, and certification courses



Certify

Cisco Certifications and Specialist Certifications

Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups

180-day certification prep program with learning and support

Cisco Continuing Education Program

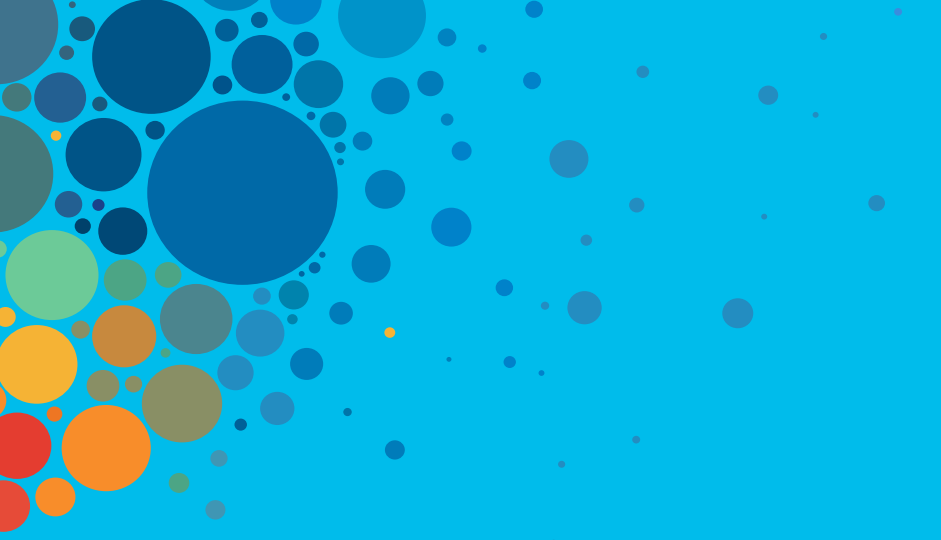
Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**



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



Continue your education

- Snort 3 with the Cisco Secure Firewall - BRKSEC-2484
- Threat Centric Network Security - BRKSEC-2480
- Secure Firewall - Threat Defense Data-Path troubleshooting (a practical hands on lab) - LTRSEC-3880
- Demystify Cloud Security using Cloud Native and Cisco Security Controls - Part 1 / 2 - TECSEC-2433a
- Simplifying migration to Cisco Secure Firewall - BRKSEC-1777
- Making Cisco Secure Firewall Threat Defense Policy Dynamic with Attribute Based Policy - BRKSEC-2127
- Cisco Secure Firewall Cloud Native on AWS - BRKSEC-3561



The bridge to possible

Thank you

CISCO *Live!*



#CiscoLive