RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: PART3-T08

Misconfigured and exposed
5 proven steps to secure your cloud

Matthew Chiodi

CSO Public Cloud
Palo Alto Networks
@mattchiodi

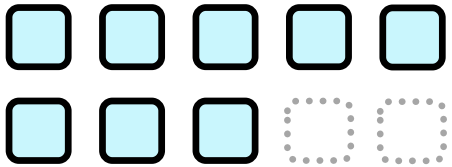
EMERGING CHALLANGES

CLOUD IS REDEFINING HOW APPLICATIONS ARE BUILT

Application Modernization

8 of **10**

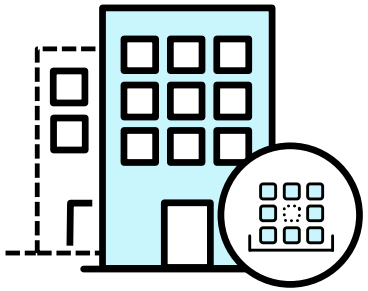
enterprise apps today are cloud-enabled/cloud-native



Containers Have Gone Mainstream

1 and **2**

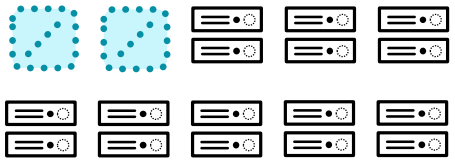
enterprises will use containers by 2021



Serverless Computing On The Rise

2 in **10**

enterprises will embrace serverless in 2021



CI/CD IS ENABLING SECURITY EARLIER IN THE LIFECYCLE

Build

Integrate vulnerability and compliance scanning into every build as part of any CI workflow

Deploy

Secure every deployment by seamlessly integrating security into continuous delivery process

Run

Reduce burden on security teams in production with minimized threat footprint

Shift Left – Ideal to implement security early in the dev lifecycle

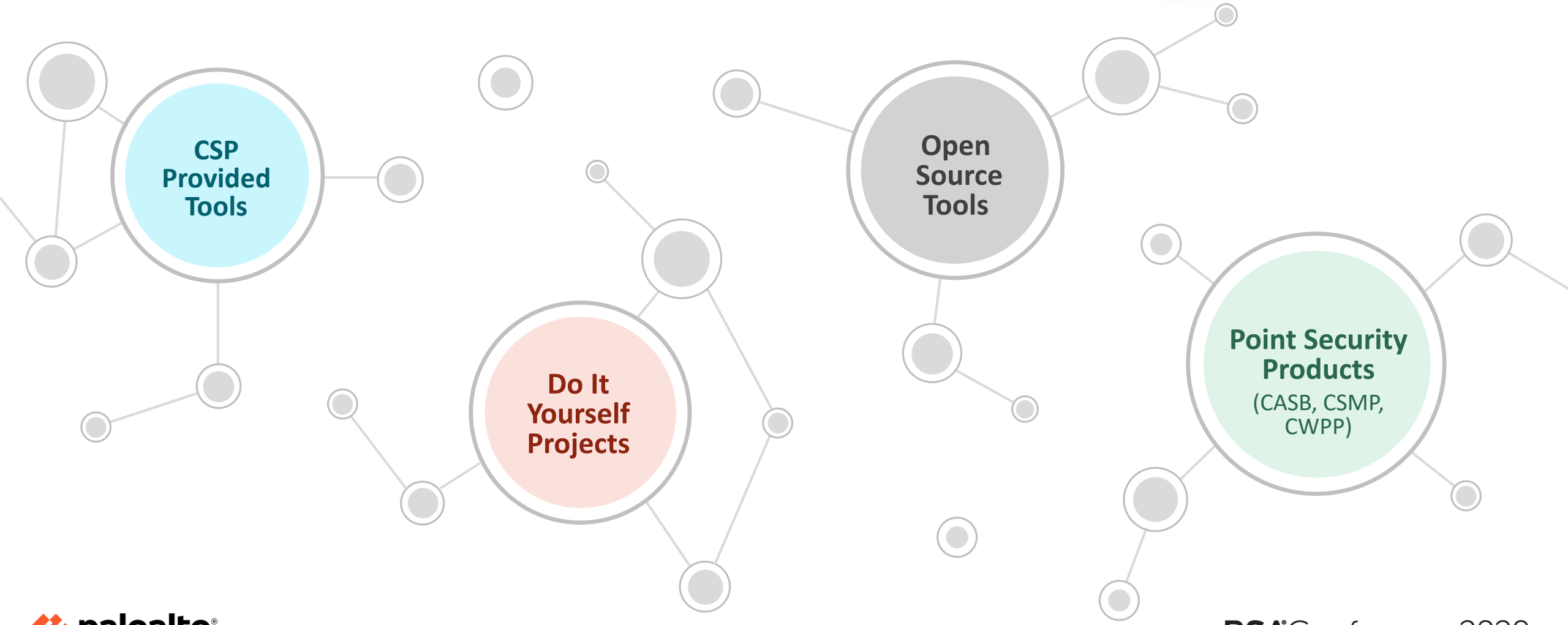
MOST ORGANIZATIONS ARE MULTI-CLOUD

81% of cloud users leverage 2 or more cloud providers

- Gartner

THE SECURITY LANDSCAPE IS FRAGMENTED

Disparate point solutions result in a lack of risk clarity and ultimately increased operational burden



RISK VECTORS ARE CHANGING | UNIT 42

Insecure Configurations

42%

of CloudFormation templates are insecure

Permissive Access

76%

of cloud workloads expose SSH (22)

Difficult Attribution

60%

of cloud storage has logging disabled

Compliance Risks

43%

of cloud databases are not encrypted

source: https://unit42.paloaltonetworks.com

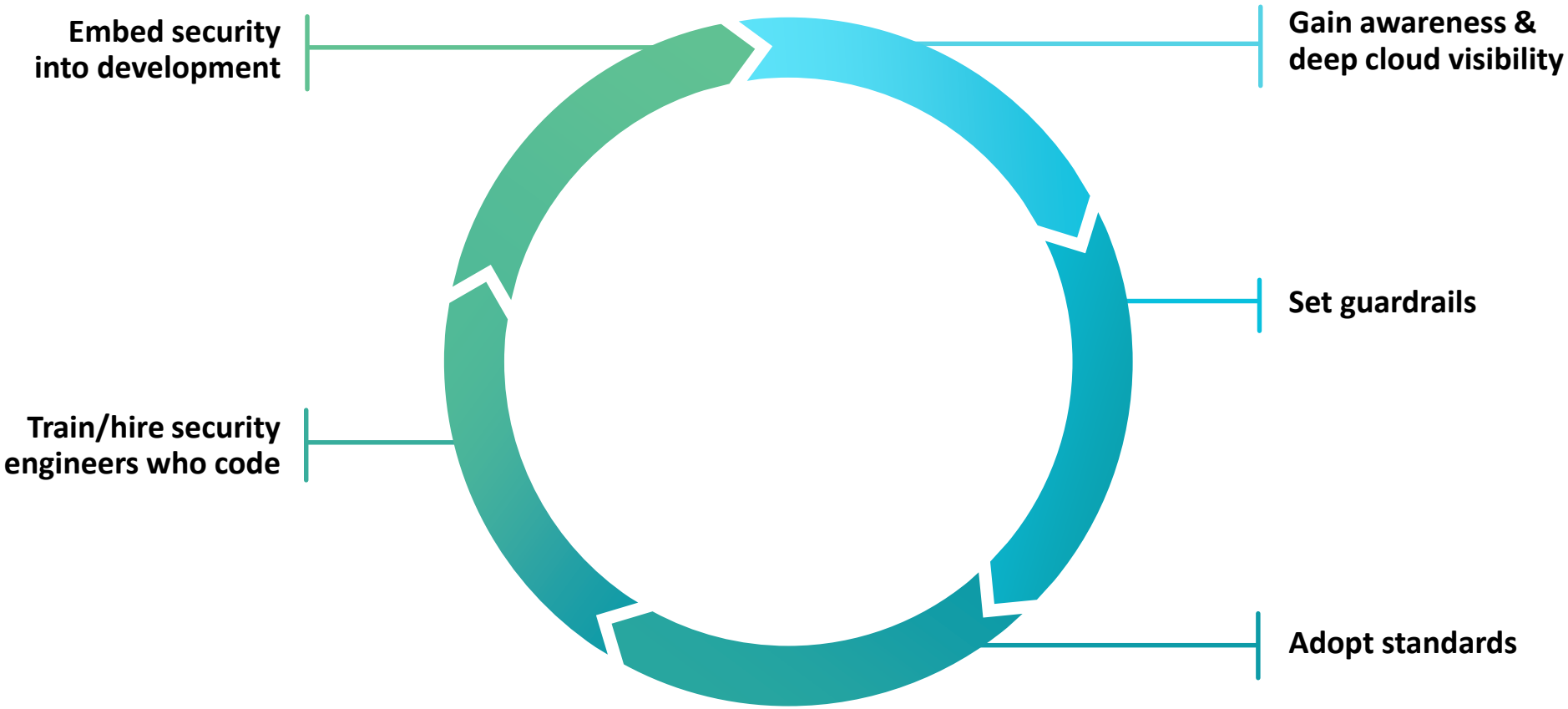
“

Security is a process, not a product.

Bruce Schneier

”

FIVE PATTERNS OF EXCELLENCE



1 Gain awareness and deep cloud visibility

Let “Shadow IT” inform cloud strategy

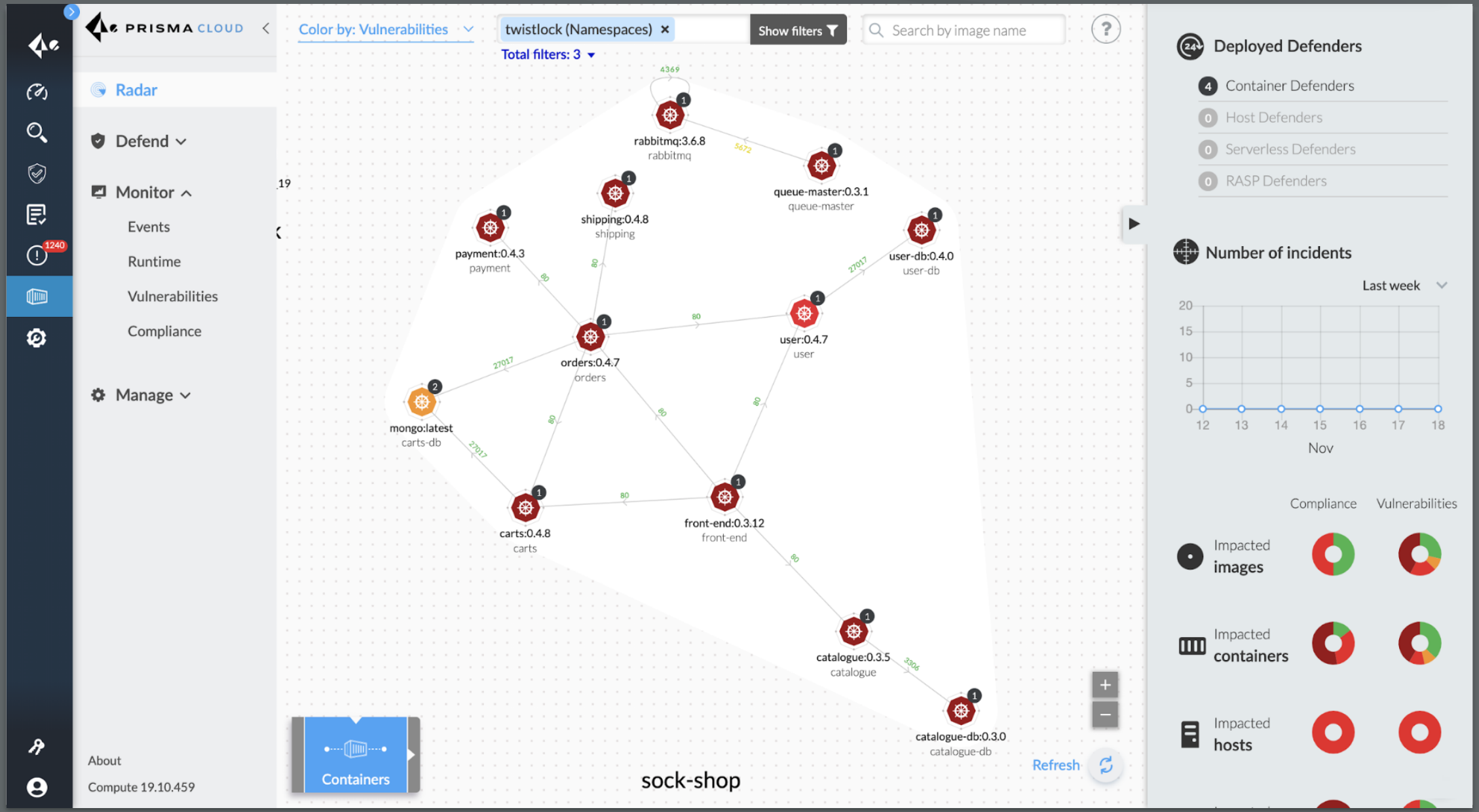
Make Shadow IT your friend by maintaining situational awareness of what’s happening

Leverage cloud provider APIs

Understand not only what apps your organization is using but utilize CSP APIs to track changes down to the workload level

Institute regular cloud usage reviews

Not a one-time event. Constantly review and monitor


PRISMA CLOUD
Radar
Defend
Monitor
Events
Runtime
Vulnerabilities
Compliance
Manage
About
Compute 19.10.459
Color by: Vulnerabilities
twistlock (Namespaces) ×
Total filters: 3
Show filters
Search by image name
rabbitmq:3.6.8
rabbitmq
queue-master:0.3.1
queue-master
shipping:0.4.8
shipping
payment:0.4.3
payment
user-db:0.4.0
user-db
user:0.4.7
user
orders:0.4.7
orders
mongo:latest
carts-db
carts:0.4.8
carts
front-end:0.3.12
front-end
catalogue:0.3.5
catalogue
catalogue-db:0.3.0
catalogue-db
Containers
sock-shop
Refresh
Deployed Defenders
4 Container Defenders
0 Host Defenders
0 Serverless Defenders
0 RASP Defenders
Number of incidents
Last week
20
15
10
5
0
12 13 14 15 16 17 18
Nov
Compliance
Vulnerabilities
Impacted images
Impacted containers
Impacted hosts

2 Set guard rails

Identify your “Dirty Dozen”

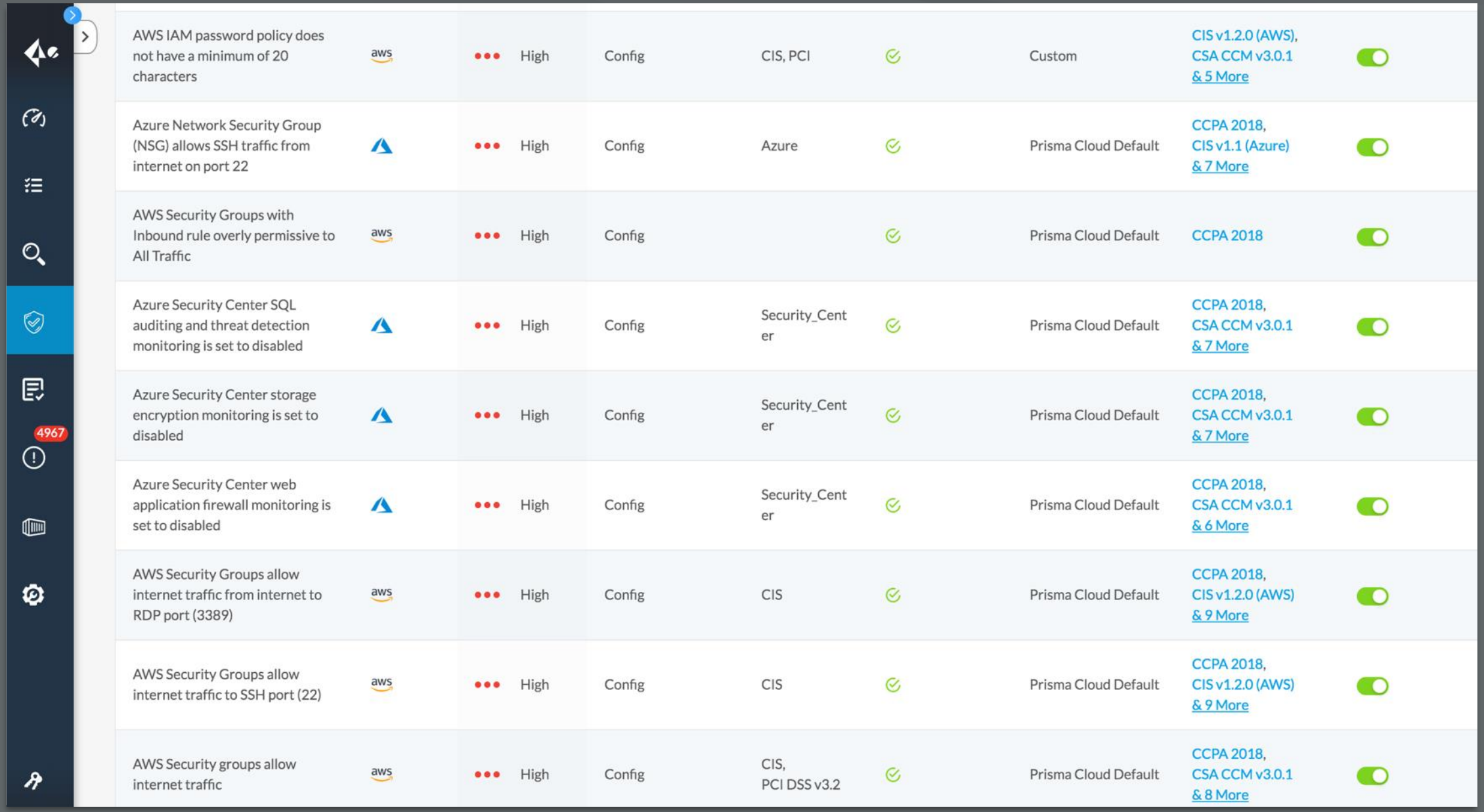
What are the configurations (anti-patterns) that should never exist in your environment?

Start small, ramp quickly

Don’t try to boil the ocean (or you’ll end up DDoS’ing yourself)

Gain buy-in from Dev

Think partnership. Not autocracy



AWS IAM password policy does not have a minimum of 20 characters	aws	•••	High	Config	CIS, PCI	✓	Custom	CIS v1.2.0 (AWS), CSA CCM v3.0.1 & 5 More
Azure Network Security Group (NSG) allows SSH traffic from internet on port 22	Azure	•••	High	Config	Azure	✓	Prisma Cloud Default	CCPA 2018, CIS v1.1 (Azure) & 7 More
AWS Security Groups with Inbound rule overly permissive to All Traffic	aws	•••	High	Config		✓	Prisma Cloud Default	CCPA 2018
Azure Security Center SQL auditing and threat detection monitoring is set to disabled	Azure	•••	High	Config	Security_Center	✓	Prisma Cloud Default	CCPA 2018, CSA CCM v3.0.1 & 7 More
Azure Security Center storage encryption monitoring is set to disabled	Azure	•••	High	Config	Security_Center	✓	Prisma Cloud Default	CCPA 2018, CSA CCM v3.0.1 & 7 More
Azure Security Center web application firewall monitoring is set to disabled	Azure	•••	High	Config	Security_Center	✓	Prisma Cloud Default	CCPA 2018, CSA CCM v3.0.1 & 6 More
AWS Security Groups allow internet traffic from internet to RDP port (3389)	aws	•••	High	Config	CIS	✓	Prisma Cloud Default	CCPA 2018, CIS v1.2.0 (AWS) & 9 More
AWS Security Groups allow internet traffic to SSH port (22)	aws	•••	High	Config	CIS	✓	Prisma Cloud Default	CCPA 2018, CIS v1.2.0 (AWS) & 9 More
AWS Security groups allow internet traffic	aws	•••	High	Config	CIS, PCI DSS v3.2	✓	Prisma Cloud Default	CCPA 2018, CSA CCM v3.0.1 & 8 More

3 Adopt standards

Leverage CIS benchmarks

Don’t start from scratch

Goal = automate 80% of benchmarks

You can’t automate what you don’t standardize

Did we mention partnering with Dev?

Don’t be the team of no

```yaml
AWSTemplateFormatVersion: '2010-09-09'
Description: ''
Resources:
    S3SharedBucket:
        Type: 'AWs::S3::Bucket'
        Properties:
            LoggingConfiguration: {}
            AccessControl: 'LogDeveryWrite'
            BucketEncryption:
                ServerSideEncryptionConfiguration
                    SSEAlgorithm: 'AES256'
            PublicAccessBlockConfiguration:
                BlockPublicAcls: 'true'
                BlockPublicPolicy: 'true'
            BucketPolicy:
                Type: 'AWS::S3::BucketPolicy'
                Properties:
                    Bucket:
                        Ref: 'S3SharedBucket'
                    PolicyDocument:
                        Version: '2012-10-17'
                        Statement
                            Principal:
                                Service:
                                    'cloudtrail.amazonaws.com'
                                    'config.amazonaws.com'
                            Action: 's3:GetBucketAcl'
                            Resource:
                                'Fn:GetAtt':
                                    'S3SharedBucket'
                                    'Arn'
                            Effect: 'Allow'
                            Condition: {}
```

4 Train/hire security engineers who code

Inventory team skills

Anyone speak Python or Ruby? Start here

Train/deputize existing developers

They already know how to code. Teach them how to do it securely. Give them stewardship - you get what you reward!

Don't have the skills in house?

Consider short-term consultants. Ensure knowledge transfer as key deliverable

5 Embed security in development << shiftLeft

Discover code movement

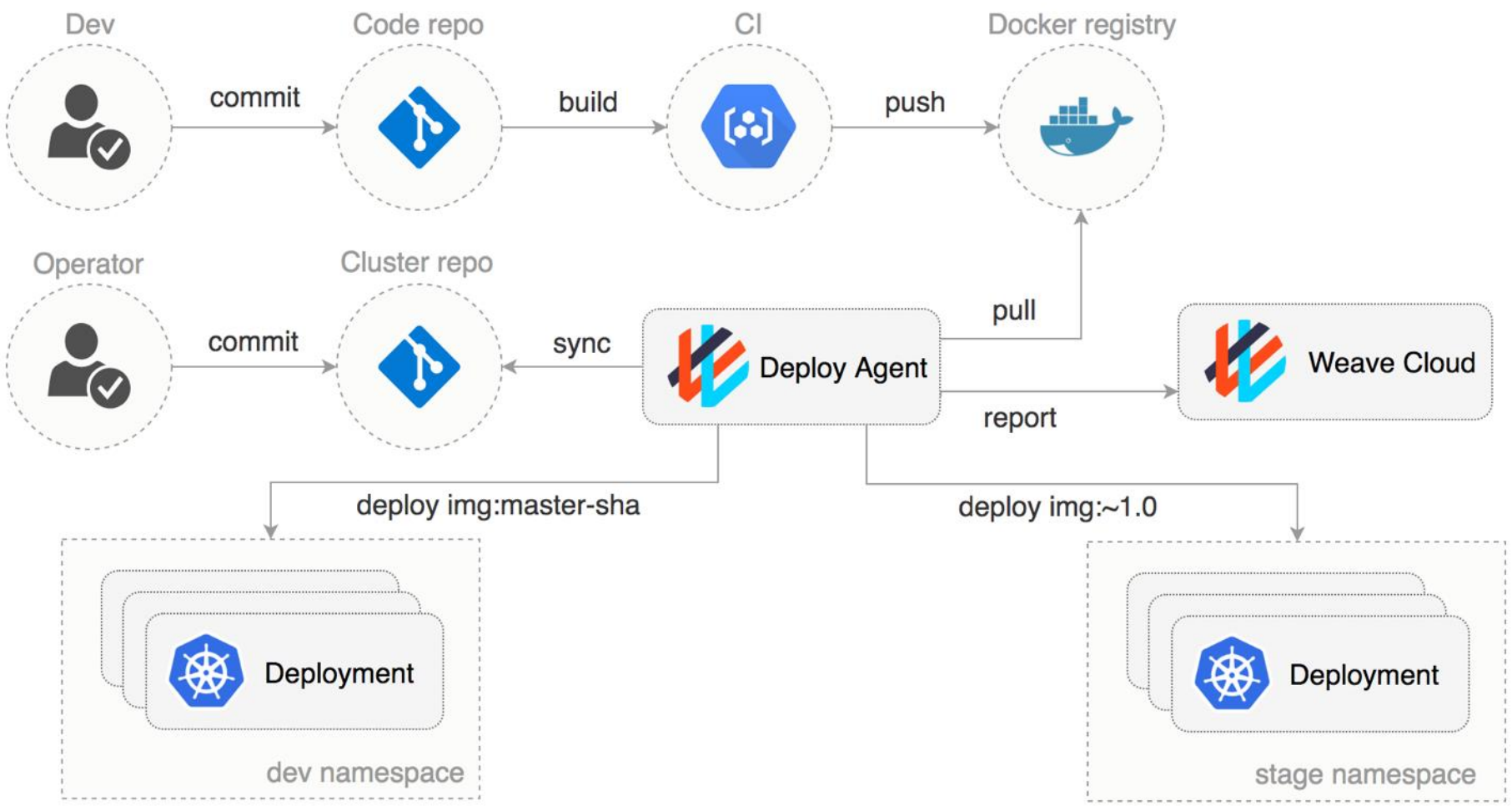
Map out who, what, when and where Code = application and infrastructure (IaC)

Develop maturity timeline minimizing human interaction

Humans = error prone and bad. Any manual changes introduce systemic risk

Identify security processes and tool insertion points

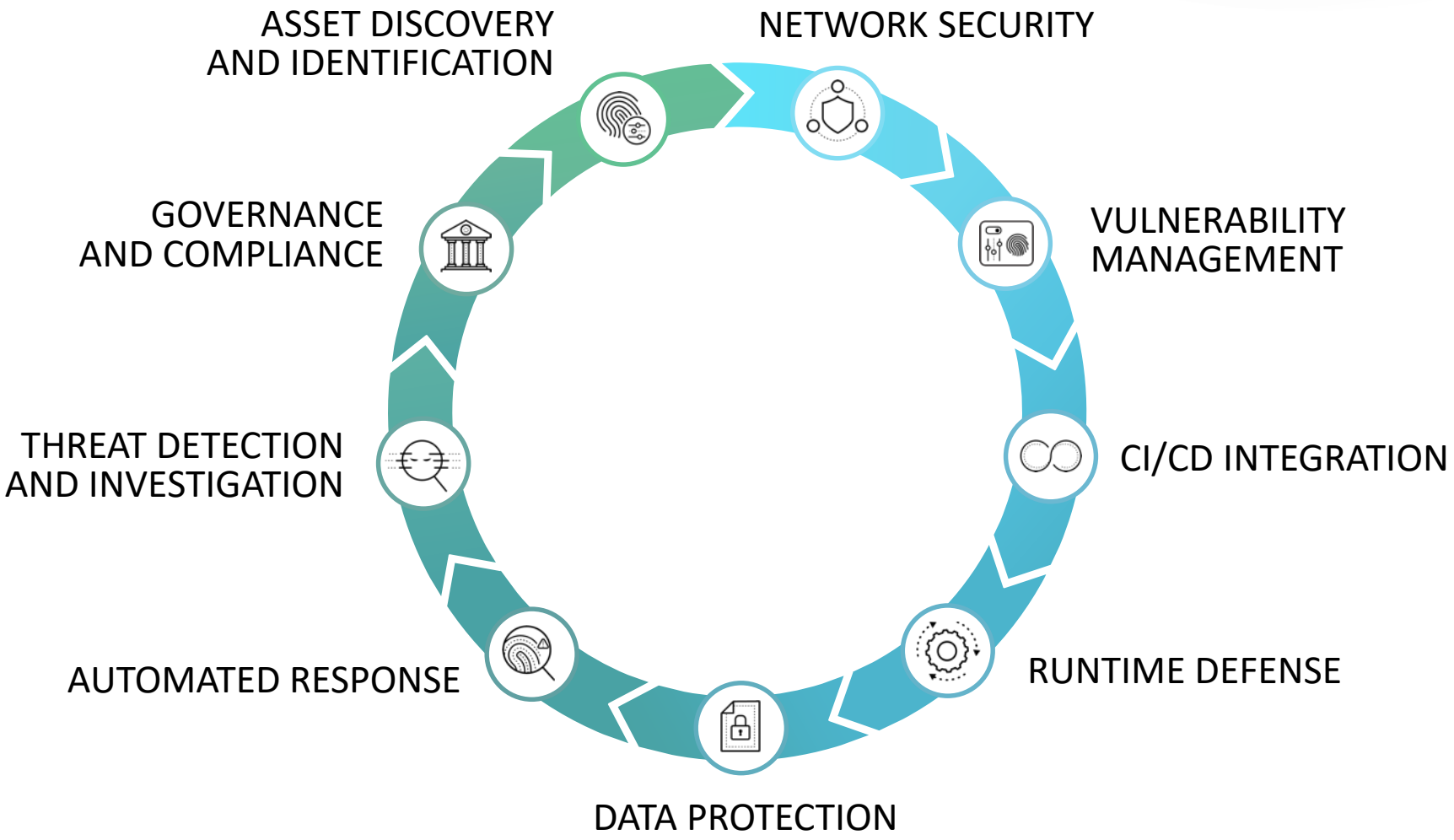
Think risk reduction through code quality control


Dev
commit
Code repo
build
CI
push
Docker registry
Operator
commit
Cluster repo
sync
Deploy Agent
pull
Weave Cloud
report
deploy img:master-sha
deploy img:~1.0
Deployment
dev namespace
Deployment
stage namespace

“Cease dependence on inspection to achieve quality. Eliminate the need for inspection on a mass basis by building quality into the product in the first place.”

W. Edwards Deming,
1982 (Father of Total Quality Management)

CLOUD NATIVE SECURITY FOCUSES ON THE ENTIRE LIFECYLCE



FIVE PATTERNS OF EXCELLENCE

Embed security into development

Map existing software/cloud development pipeline

Identify security process and tool insertion points

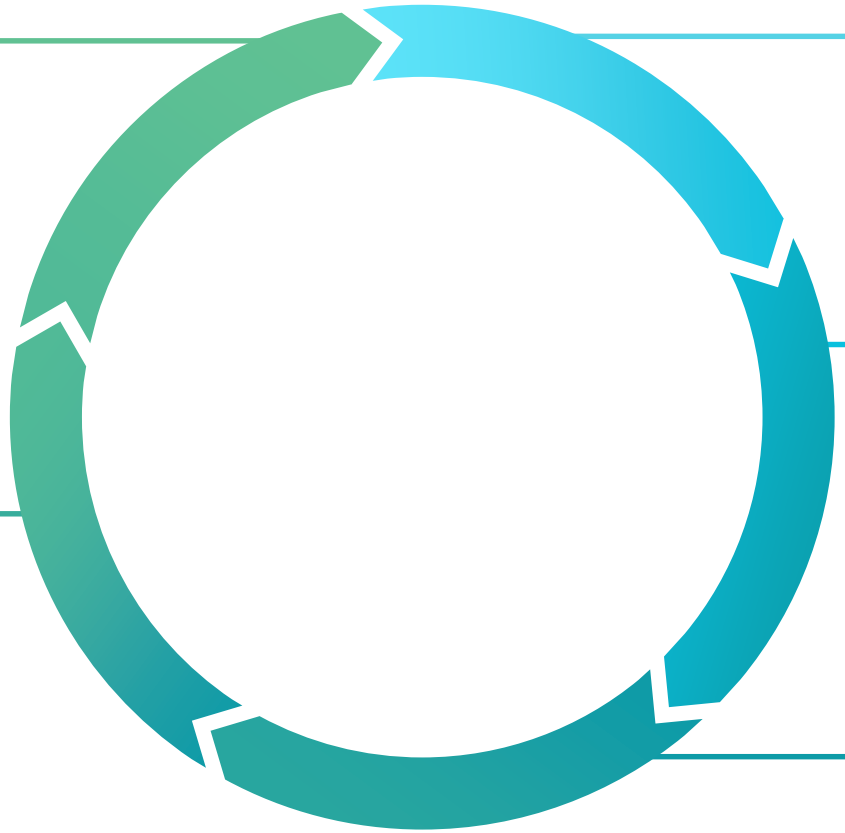
Develop maturity timeline minimizing human interaction

Train/hire security engineers who code

Inventory team skills

Incentivize learning

Train/deputize existing developers



Gain awareness & deep cloud visibility

Let ”Shadow IT” inform cloud strategy

Leverage cloud provider APIs

Institute quarterly cloud usage review

Set guardrails

Identify the Dirty Dozen

Gain buy-in from Dev

Start small, ramp quickly

Adopt standards

Leverage CIS benchmarks

Gain buy-in from Dev

Goal = automate 80% of benchmarks

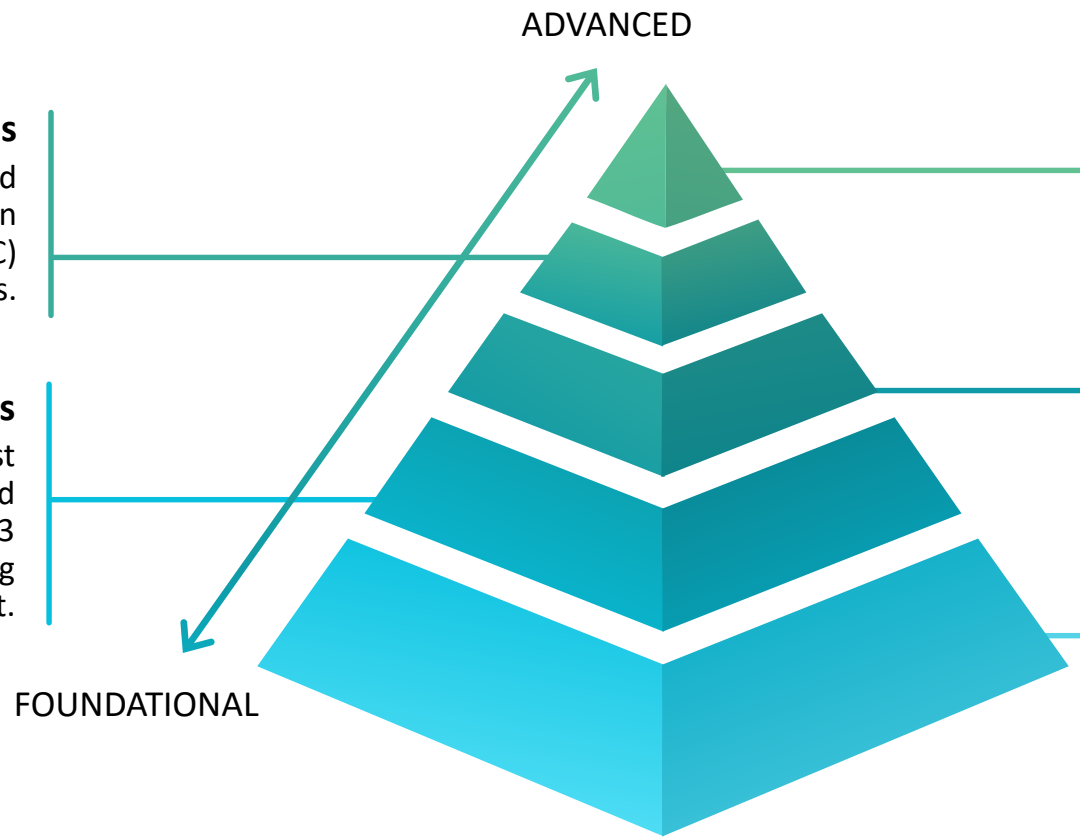
CLOUD NATIVE SECURITY MATURITY - WHERE ARE YOU TODAY?

Quality guardrails

Security standards, architecture and compliance solidified in infrastructure as Code (IaC) templates. No manual changes.

MVP guardrails

Auto-remediation of the most common cloud antipatterns and misconfiguration. E.G., public S3 buckets and databases receiving traffic directly from t the internet.



Cloud native security

CI/CD pipeline with organically embedded and centralized security, compliance, risk and cost controls across all clouds and workload types e.g., laaS, Paas, containers, serverless, VMs, and SaaS.

Code movement transparency

Who, what, when and where of development pipeline understood and agreed to by all teams. Single pipeline/ process established for all cloud changes to apps, assets, data, etc.

Deep cloud visibility

Situational awareness of multi-cloud security posture, assets, configuration, and compliance.

APPLY WHAT YOU LEARNED TODAY

Next week

- Review CIS benchmarks
- Figure out if you have centralized logging of FW & proxy logs

Next 90 days

- Determine where you are on the cloud maturity model
- Create a plan around the five steps
- Complete steps one and two

Next six months

- Set and programmatically enforce standards (step three)
- Begin the process of transforming your team into coders (step four)
- Begin step five and identify the who/where/what of your dev pipeline

RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID:

Thank you

Matthew Chiodi

CSO Public Cloud
Palo Alto Networks
@mattchiodi