The DevSecOps Approach to Cloud Security

How we can make it with Trend Micro & the Cloud

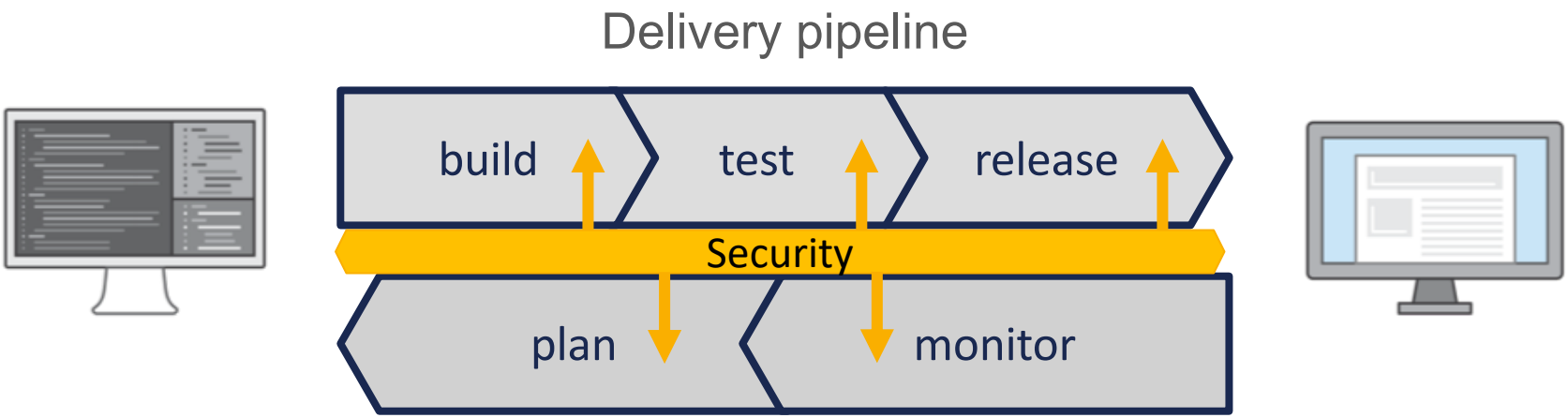
Biswajit De

Sr. Technical Consultant

What’s DevSecOps？

DevOps Model

DevOps is a way to promote software development operation to quickly and efficiently interact with customers



What is necessary for introduction of DevOps model

The introduction of DevOps is realized by having all three elements

Organization Culture

Method Practices

Tools

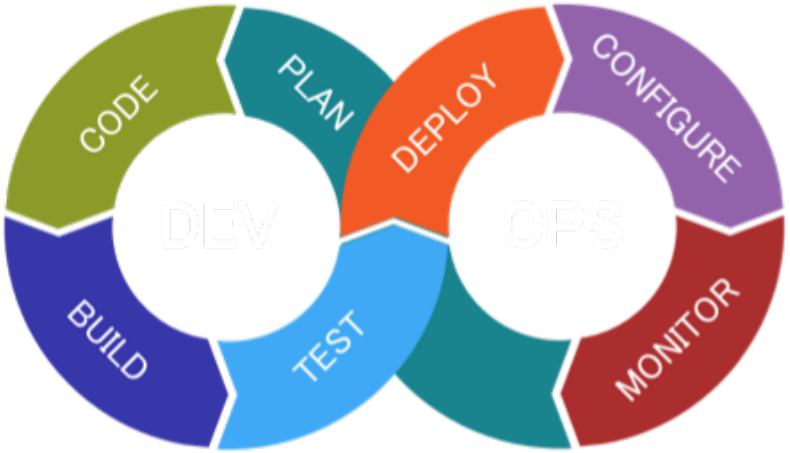
Organizational culture of DevOps (Culture)

DevOps organization is responsible for the entire lifecycle

Removal of inter-team barriers of development and operation which had been siled

Optimize both productivity of developers and reliability of operators

Improve service quality provided to customers with frequent communication



TREND MICRO

DevOps method (Practices)

Six methods to quickly and efficiently deliver services to customers

Continuous integration

Continuous delivery

Micro service

infrastructure As code

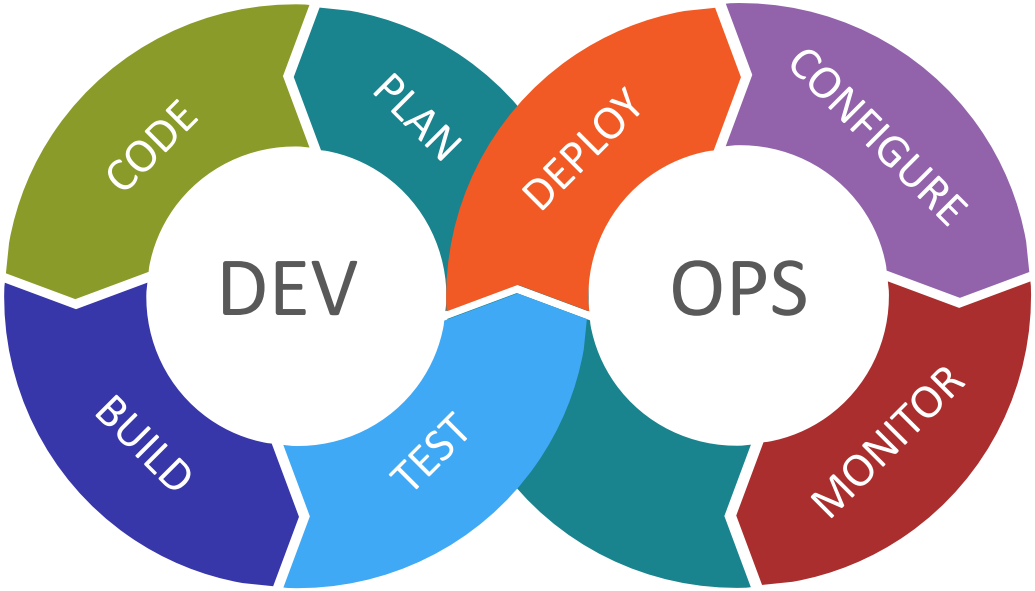
Monitoring and logging

Communication and group work

TREND MICRO

Toward realization of DevSecOps

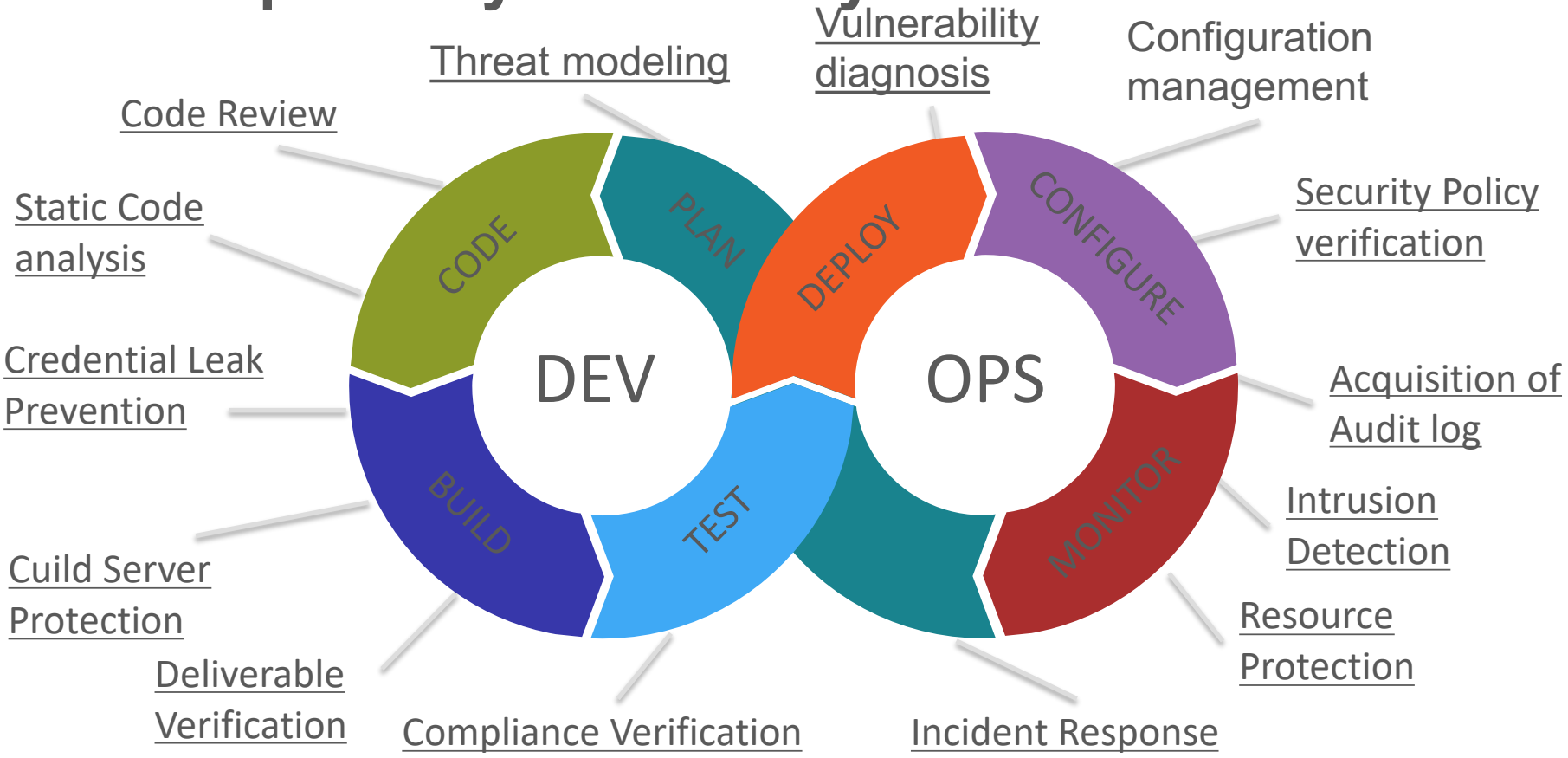
Incorporate security into the life cycle of achieving business goals



What kind of security should be applied to which stage?

TREND MICRO

DevSecOps lifecycle security

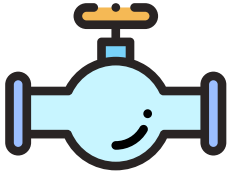


TREND MICRO

Common Concerns

Security Coverage & Visibility

Securing Server Fleets



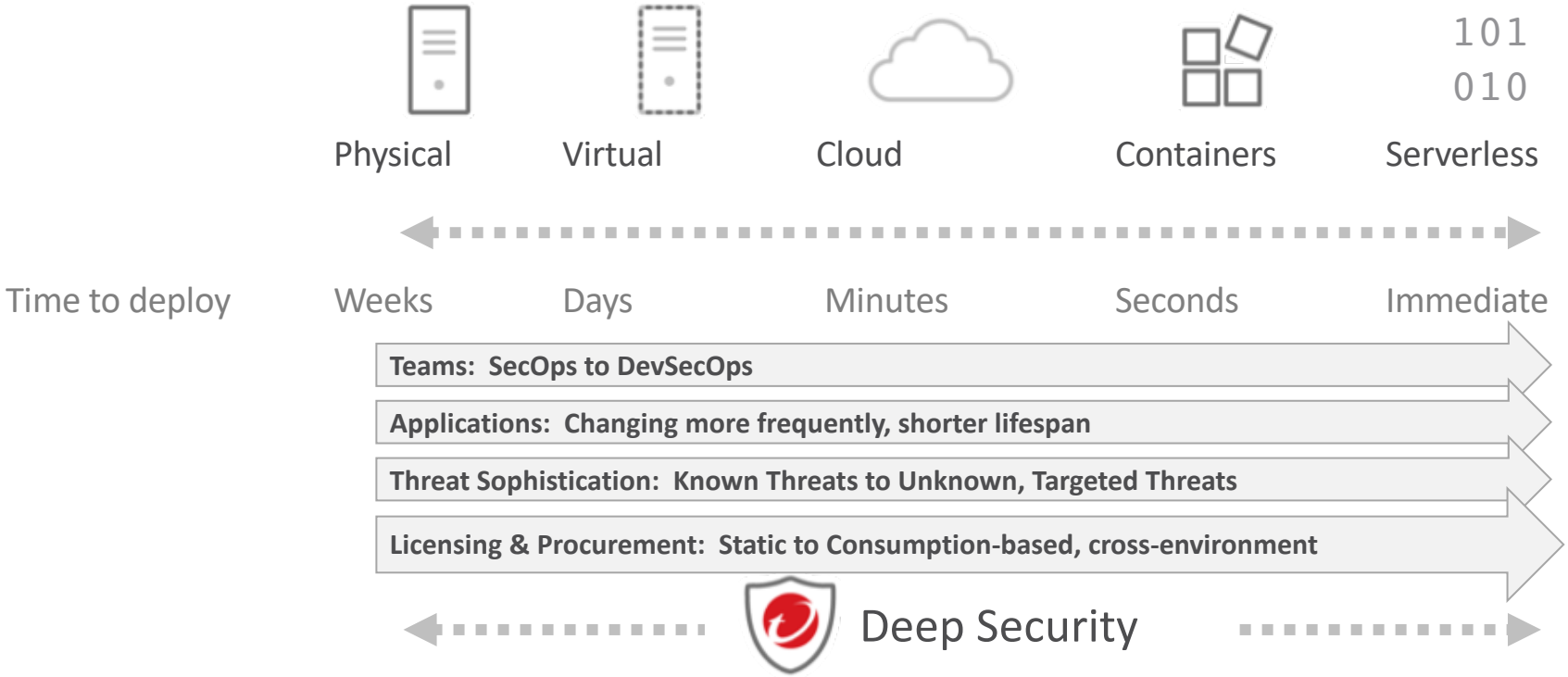
API Security Strategy

Compliance and Regulatory

Automated Security Testing

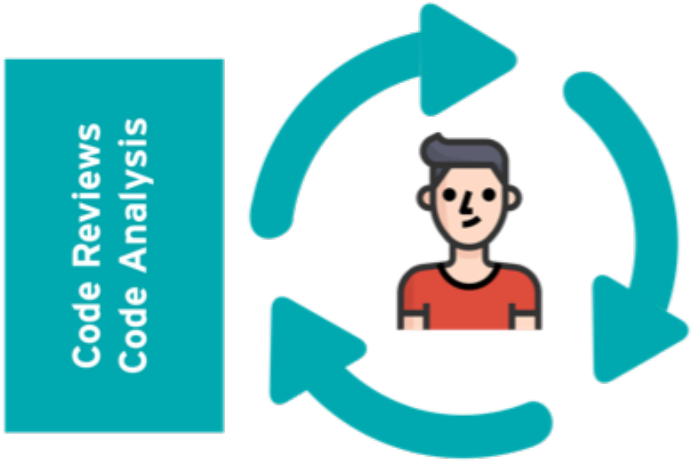
TREND MICRO

Scaling on the cloud



Protecting the server compute evolution

TREND MICRO


Code Reviews
Code Analysis

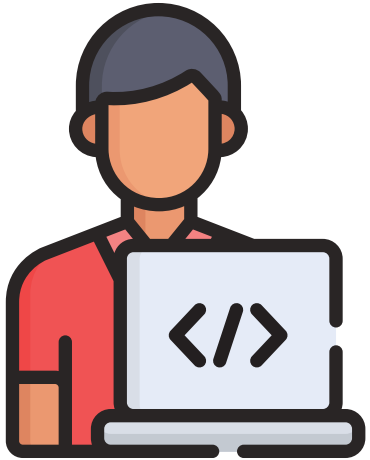
Dev

Network Security
Instance Security
Compliance

Ops

Move Fast and Secure

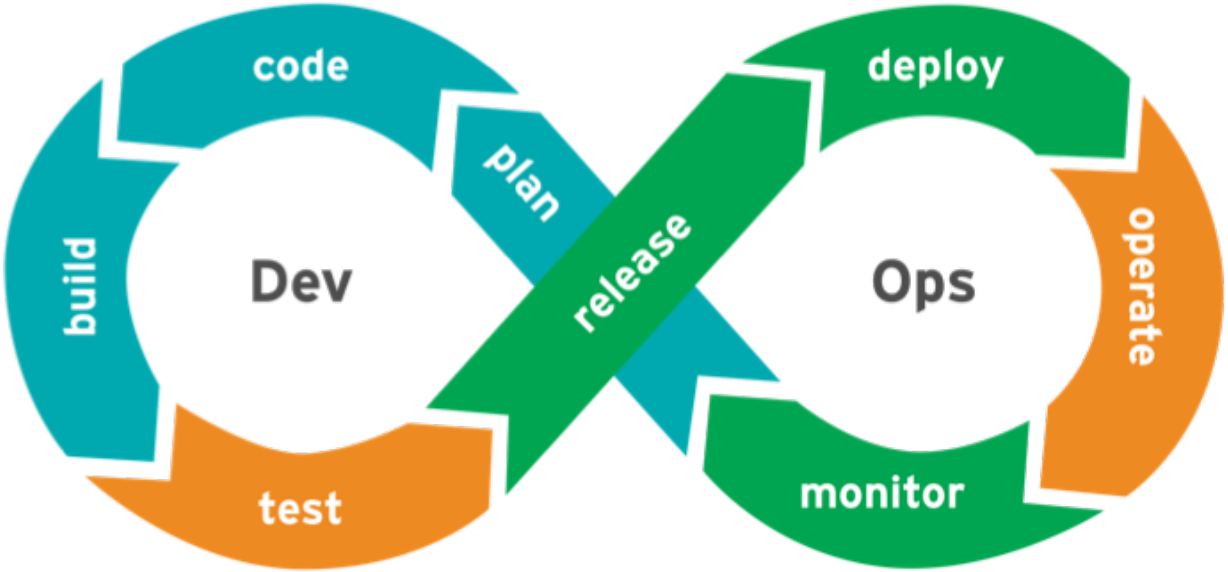
TREND MICRO

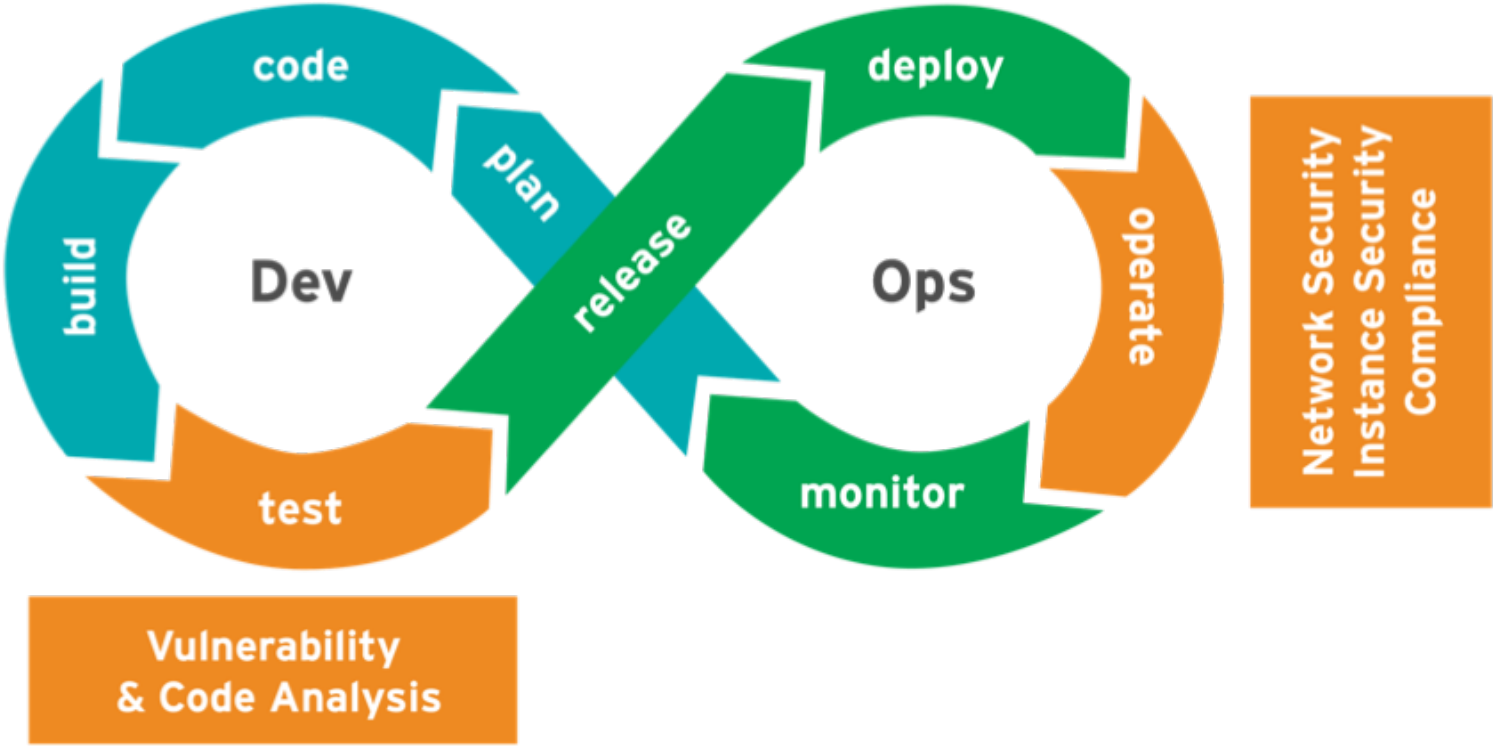


Security is Job 0

Shipping code is Job 1

TREND MICRO


code
build
test
plan
Dev
release
deploy
operate
monitor
Ops


code
plan
build
Dev
release
test
deploy
Ops
operate
monitor
Network Security
Instance Security
Compliance
Vulnerability
& Code Analysis

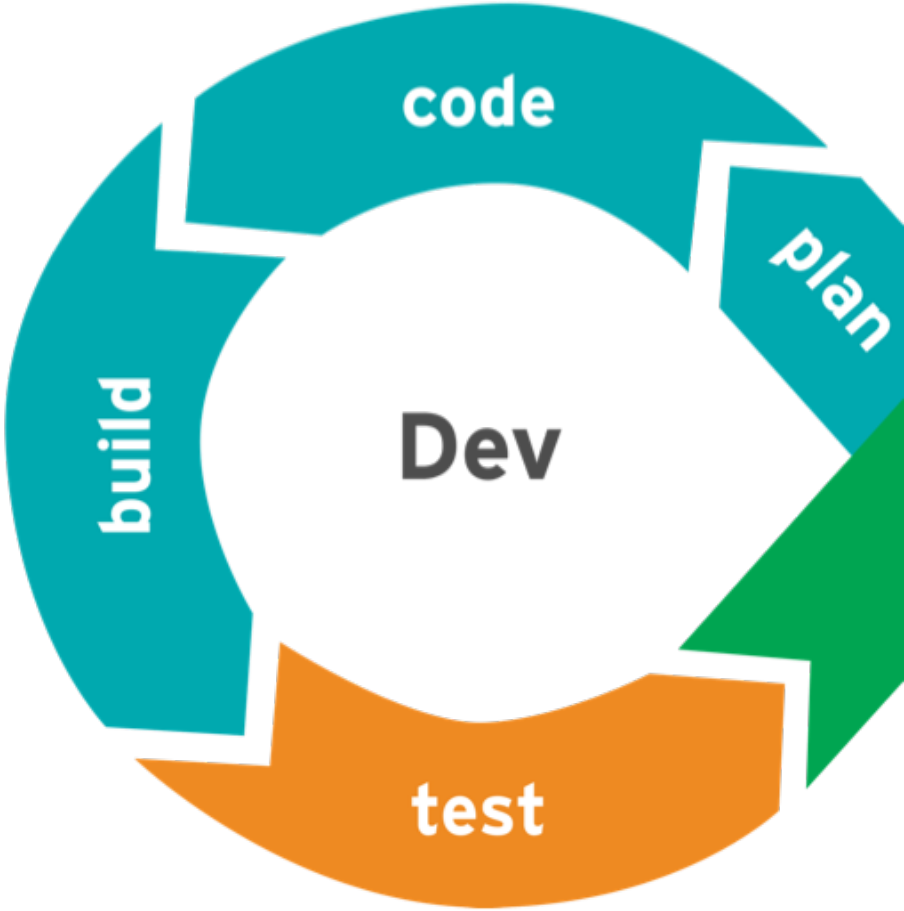
How do we add more controls in the process?

Are we using the right tools in our pipeline

How do we integrate security in the CI/CD Pipeline

How would we know the integrity of sources

How do traditional security controls keep up



Shifting Security to the Left

Your team decided to check the integrity of the images in your pipeline and you are tasked to check if your containers have any malware or vulnerabilities

TREND MICRO

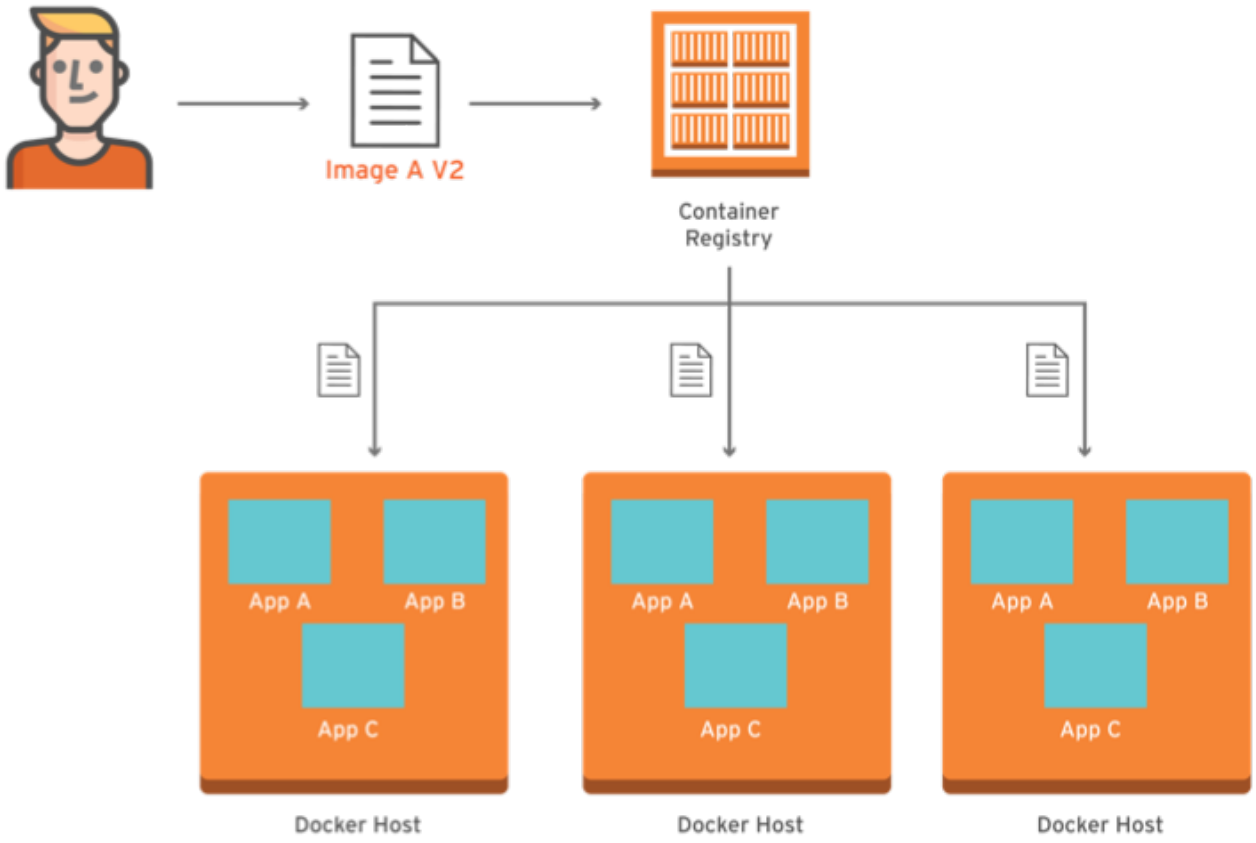
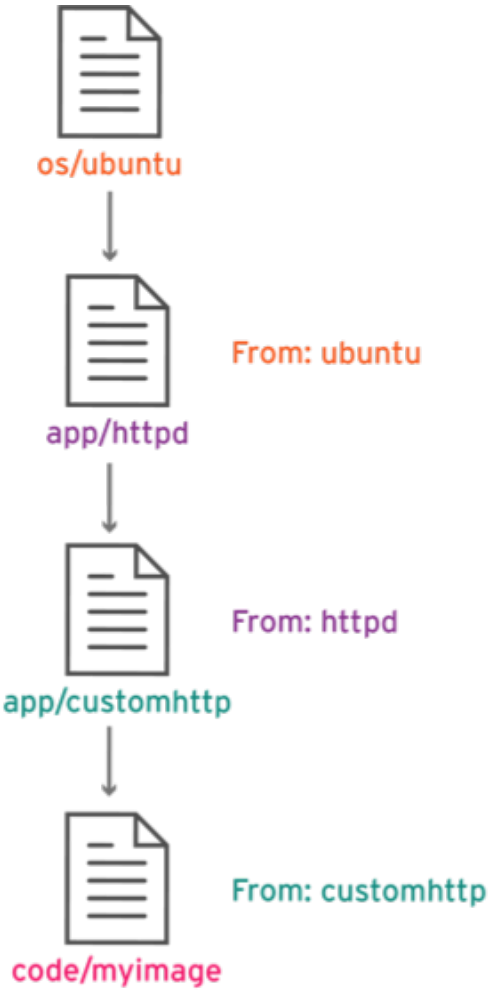
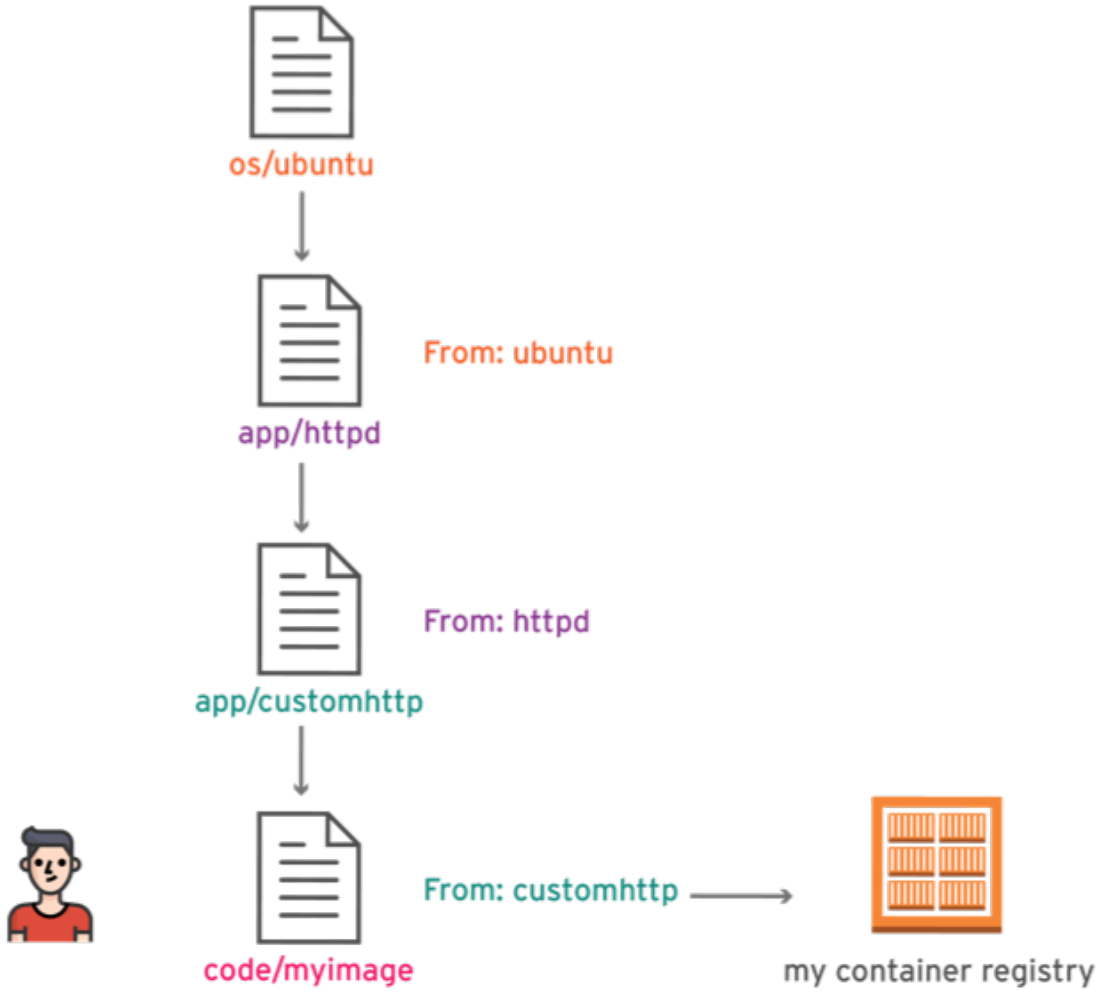


Image A V2
Container Registry
App A
App B
App C
Docker Host
App A
App B
App C
Docker Host
App A
App B
App C
Docker Host

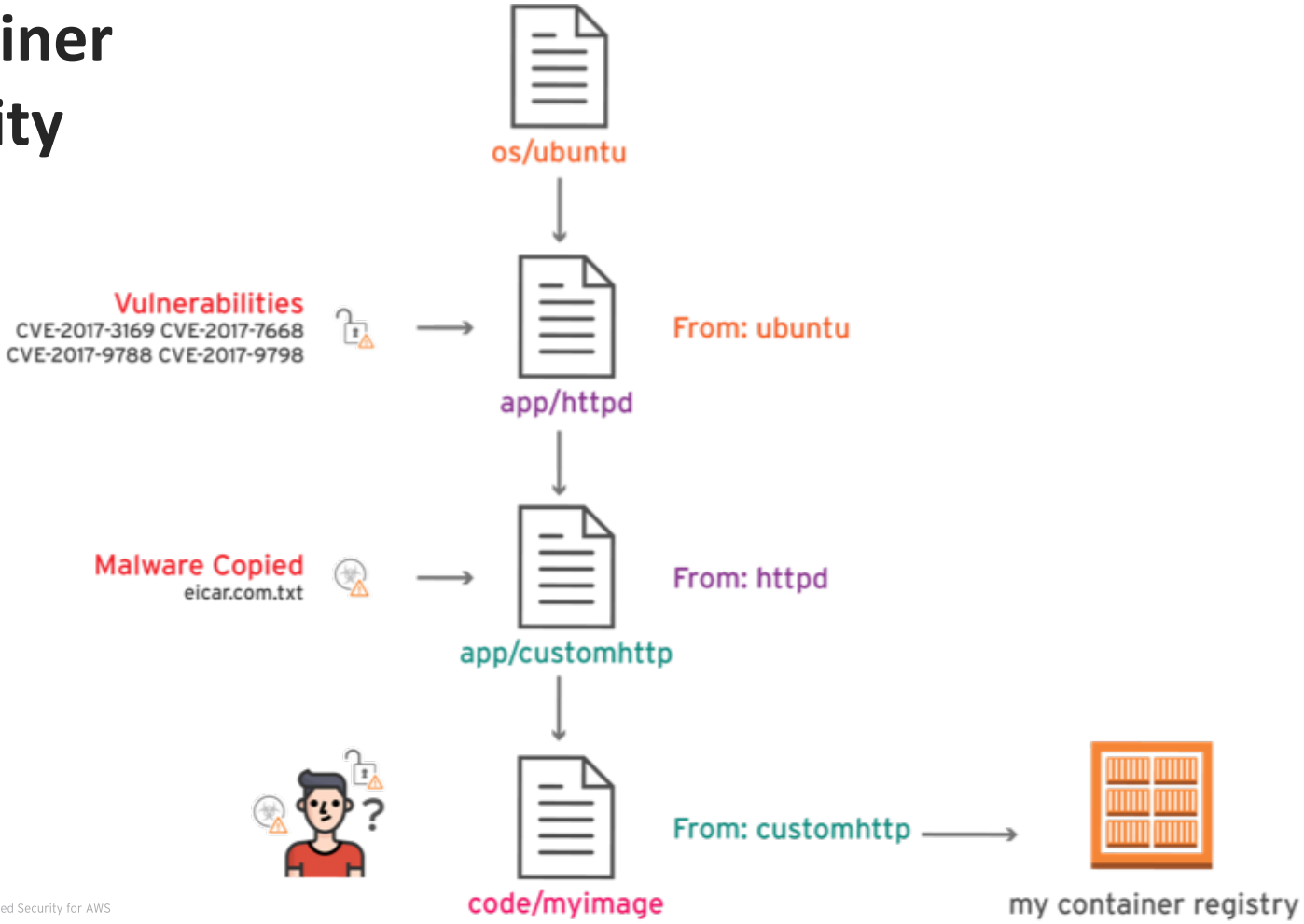
Container Security



Container Security



Container Security



Demo

Deep Security Smart Check

https://smart-check.jaws.world

Deep Security Smart Check

Summary

Scan Coverage

Scanned Not Scanned

Vulnerabilities

Critical High Medium
Low Negligible Unknown

Malware

Statistics

1 Registry

1 Repository

1 Image

1 Scan in past 24 hours

1 Scan in past 7 days

Views

View Name	Last Updated	Scan Coverage
Dvwa	2018 May 1	

Firefox File Edit View History Bookmarks Tools Window Help 99% Tue 7:50 AM

Deep Security Smart Check

https://smart-check.jaws.world/scans?registry=gcr.io&repository=bryce-178904/dvwa&tag=latest 110%

Deep Security Smart Check

Scan History

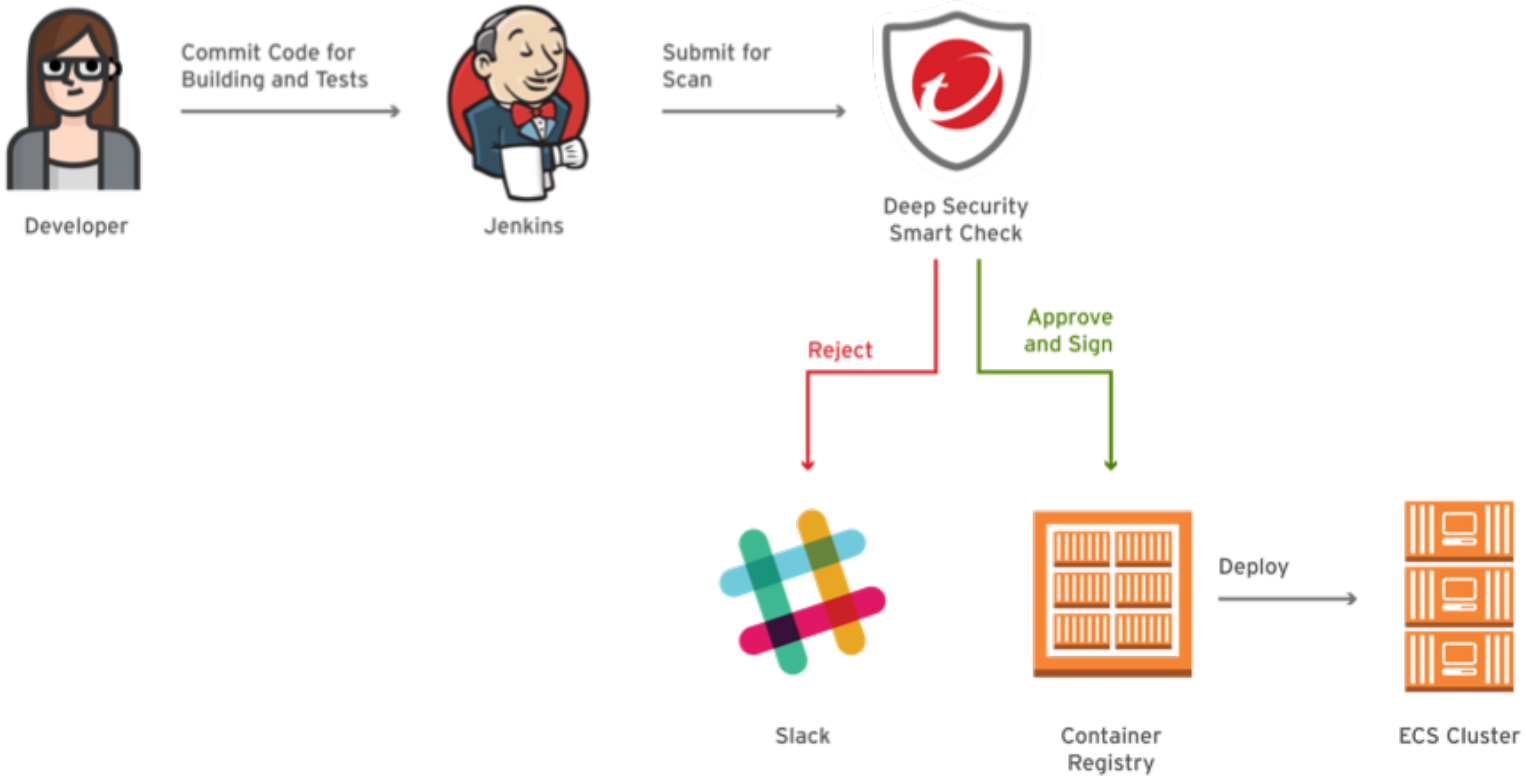
gcr.io/bryce-178904/dvwa:latest 2018-03-30 12:49
1 11 High + 765 Other

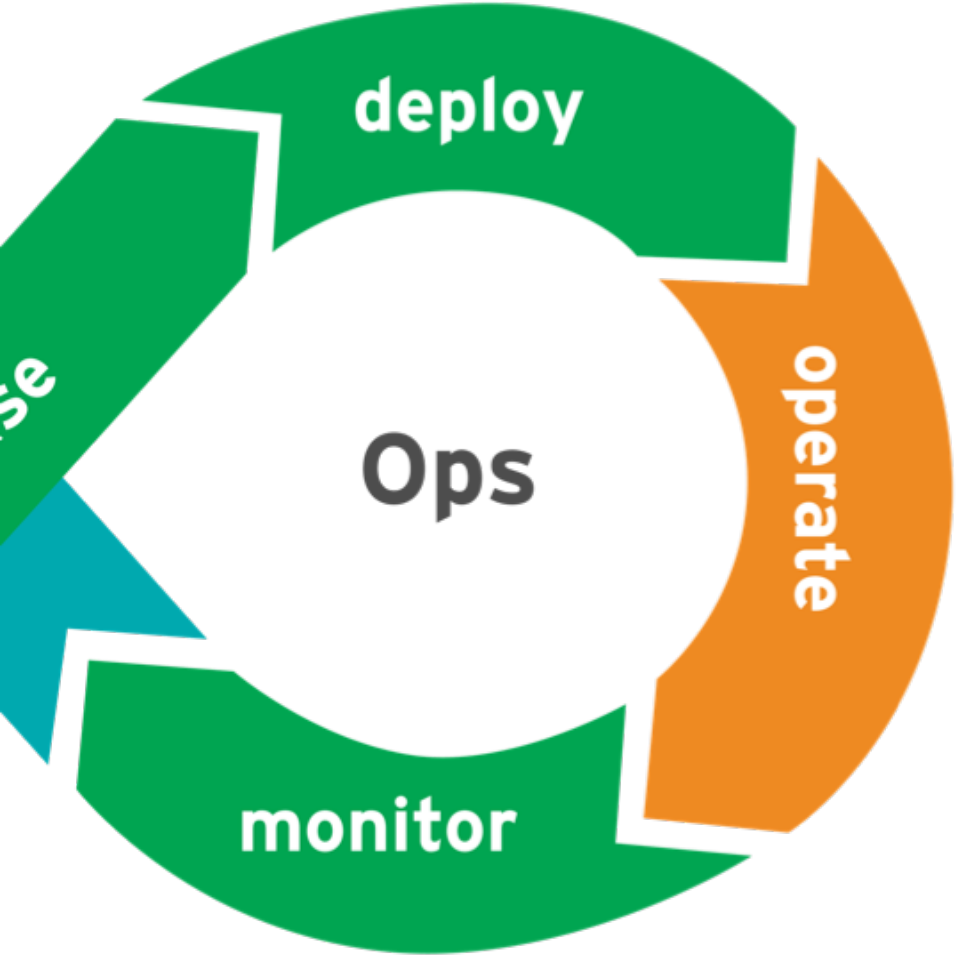
gcr.io/bryce-178904/dvwa:latest 2018-04-03 12:43
1 11 High + 765 Other

gcr.io/bryce-178904/dvwa:latest 2018-04-11 04:48
1 11 High + 769 Other

gcr.io/bryce-178904/dvwa:latest 2018-05-01 07:49

Security at build

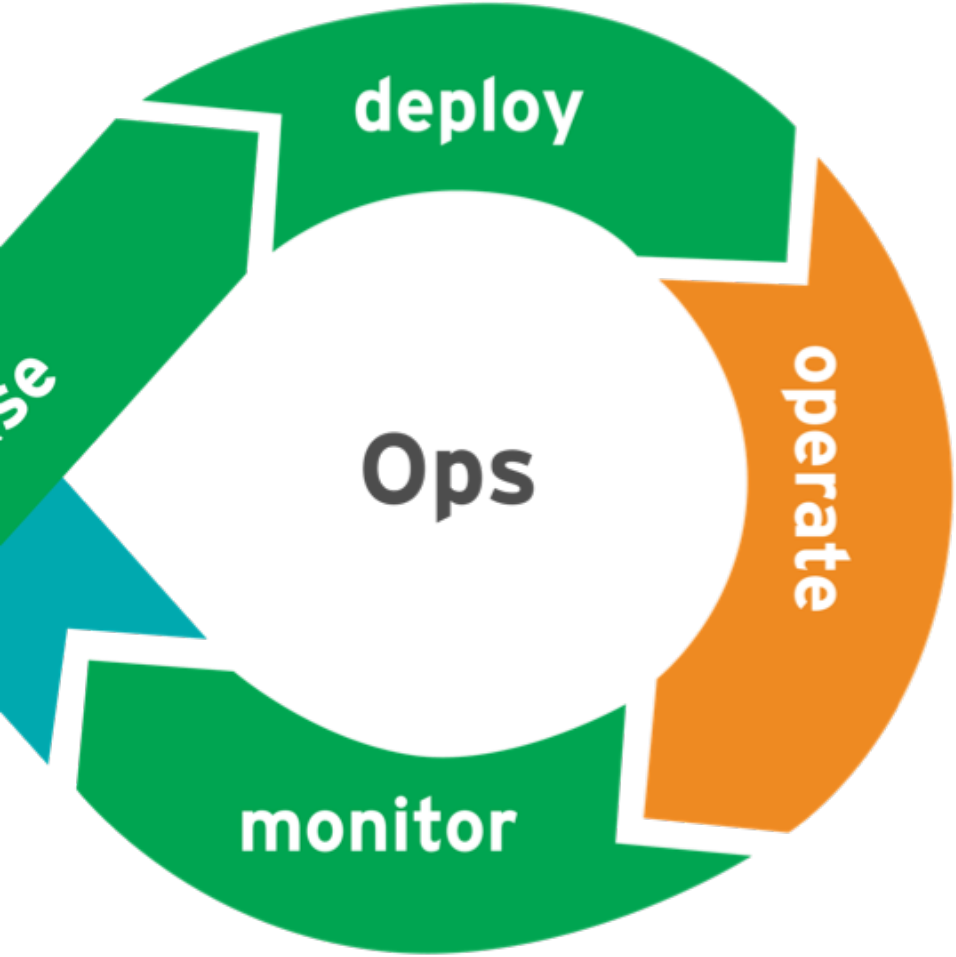




How can we quickly react when incidents occur

How can we make sense of the noise

How can I check if my configuration still secure



How can we quickly react when incidents occur

How can we make sense of the noise

How can I check if my configuration still secure

Making sense of the noise

Your Security team implemented Amazon GuardDuty, How can you ensure that your instances are protected from those attacks?

TREND MICRO

Amazon GuardDuty

Demo

AWS Management Con | GuardDuty Manageme | EC2 Management Con | Trend Micro Deep Sec | Lambda Management | EC2 Management Con | Uber halts self-driving

https://ap-southeast-1.console.aws.amazon.com/guardduty/home?region=ap-southeast-1#/findings 133%

aws Services Resource Groups sg-paul @ trendsea Singapore Support

GuardDuty

Findings
- Current
- Archived

Settings
- General
- Lists
- Accounts

Usage
- Details

Partners

Current findings

Showing 365 of 365 354 7 4

Actions

Saved filters: No saved filters

Include and exclude filter options are available on certain finding attributes in the details

	Finding	Last seen	
	Unprotected port on EC2 instance i-0d146625e41a6e1c5 is being pr...	2018-03-20 07:07:23 (18 minutes a...	4
	46.17.97.4 is performing RDP brute force attacks against i-0d146625...	2018-03-20 07:07:23 (18 minutes a...	9
	Unprotected port on EC2 instance i-04e6ba99a60c5e737 is being pr...	2018-03-20 07:03:11 (23 minutes a...	5
	46.17.97.4 is performing RDP brute force attacks against i-04e6ba99...	2018-03-20 07:03:11 (23 minutes a...	2
	Unprotected port on EC2 instance i-0ba893ce199b1217d is being pr...	2018-03-20 07:00:52 (25 minutes a...	4
	Unprotected port on EC2 instance i-0ab76630ad4878bc3 is being pr...	2018-03-20 07:00:31 (25 minutes a...	4
	Unprotected port on EC2 instance i-0ea531d86d9bcff5a is being pro...	2018-03-20 06:59:44 (26 minutes a...	4
	Unprotected port on EC2 instance i-038d52442783a61af is being pro...	2018-03-20 06:57:55 (28 minutes a...	5
	Unprotected port on EC2 instance i-029e9ce7886627c09 is being pr...	2018-03-20 06:00:28 (an hour ago)	3
	193.201.224.220 is performing RDP brute force attacks against i-0ba...	2018-03-20 04:30:45 (3 hours ago)	6

Feedback English (US)

© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Privacy Policy Terms of Use

Terminal Shell Edit View Window Help 100% Tue 8:06 AM

security — root@bryce-sg-attack-linux-krill:/home/bryce — ssh -i bryce bryce@13.228.102.57

```
[04:05] root @ bryce-sg-attack-linux-krill bryce :
```

110%

ws | Help | Support | Help Center Search

gorg-gd

STATUS	LAST COMMUNICATIO
Managed (Online)	0 Minutes Ago

Firefox File Edit View History Bookmarks Tools Window Help 100% Tue 8:40 AM

EC2 Management Console | GuardDuty Management Conso | Trend Micro Deep Security Man

https://ap-southeast-1.console.aws.amazon.com/guardduty/home?region=ap-southeast-1#/findings 120%

aws Services Resource Groups sg-paul @ trendsea Singapore Support

New feature: GuardDuty added new findings

GuardDuty added nine new finding types for unusual API usage by an IAM user in your account Learn more

Current findings

Showing **632** of **632** 620 10 2

Actions Saved filters *No saved filters*

Add filters

	Finding type	Resource	Lat...	Cc
	Recon:EC2/PortProbeUnprotecte...	Instance: i-07d63412ab69	13 min...	3634
	Recon:EC2/PortProbeUnprotecte...	Instance: i-043070a74eac	14 min...	2840
	UnauthorizedAccess:EC2/RDPBr...	Instance: i-08dca553cdfb	17 min...	49
	UnauthorizedAccess:EC2/RDPBr...	Instance: i-0690ebe96a2C	23 day...	34
	UnauthorizedAccess:EC2/RDPBr...	Instance: i-00f8ca7f76ca9	23 day...	13
	UnauthorizedAccess:EC2/RDPBr...	Instance: i-00f8ca7f76ca9	23 day...	35

Useful? Close

Recon:EC2/PortProbeUnprotectedPort

Finding ID: e2b14d413d8ce6364a1ed4ae14357f70

EC2 instance has an unprotected port which is being probed by a known malicious host.

Severity	Region	Count
Low	ap-southeast-1	3634
Account ID	**Resource ID**	**Threat list name**
650143975734	i-07d63412ab6...	ProofPoint
Created at	**Updated at**	
2018-04-06 14:...	2018-05-01 08:...	

Resource affected

Resource role	Resource type
TARGET	Instance
Instance ID	**Port**
i-07d63412ab692bcf2	5000
Port name	**Instance type**
Unknown	t2.small
Instance state	**Availability zone**

Firefox File Edit View History Bookmarks Tools Window Help 100% Tue 8:41 AM

EC2 Management Console | GuardDuty Management Conso | Trend Micro Deep Security Man

https://ap-southeast-1.console.aws.amazon.com/guardduty/home?region=ap-southeast-1#/find 120%

aws Services Resource Groups sg-paul @ trendsea Singapore Support

New feature: GuardDuty added new findings

GuardDuty added nine new finding types for unusual API usage by an IAM user in your account Learn more

Current findings

Showing **632** of **632** 620 10 2

Actions Saved filters No saved filters

Add filters

Finding type	Resource	La...	Co
Recon:EC2/PortProbeUnprotec...	Instance: i-07d63412ab6	13 min...	3634
Recon:EC2/PortProbeUnprotec...	Instance: i-043070a74ea	15 min...	2840
UnauthorizedAccess:EC2/RDP...	Instance: i-08dca553cdf	18 min...	49
UnauthorizedAccess:EC2/RDP...	Instance: i-0690ebe96a2	23 day...	34
UnauthorizedAccess:EC2/RDP...	Instance: i-00f8ca7f76ca	23 day...	13
UnauthorizedAccess:EC2/RDP...	Instance: i-00f8ca7f76ca	23 day...	35

Useful? Close

Recon:EC2/PortProbeUnprotectedPort

Finding ID: e2b14d413d8ce6364a1ed4ae14357f70

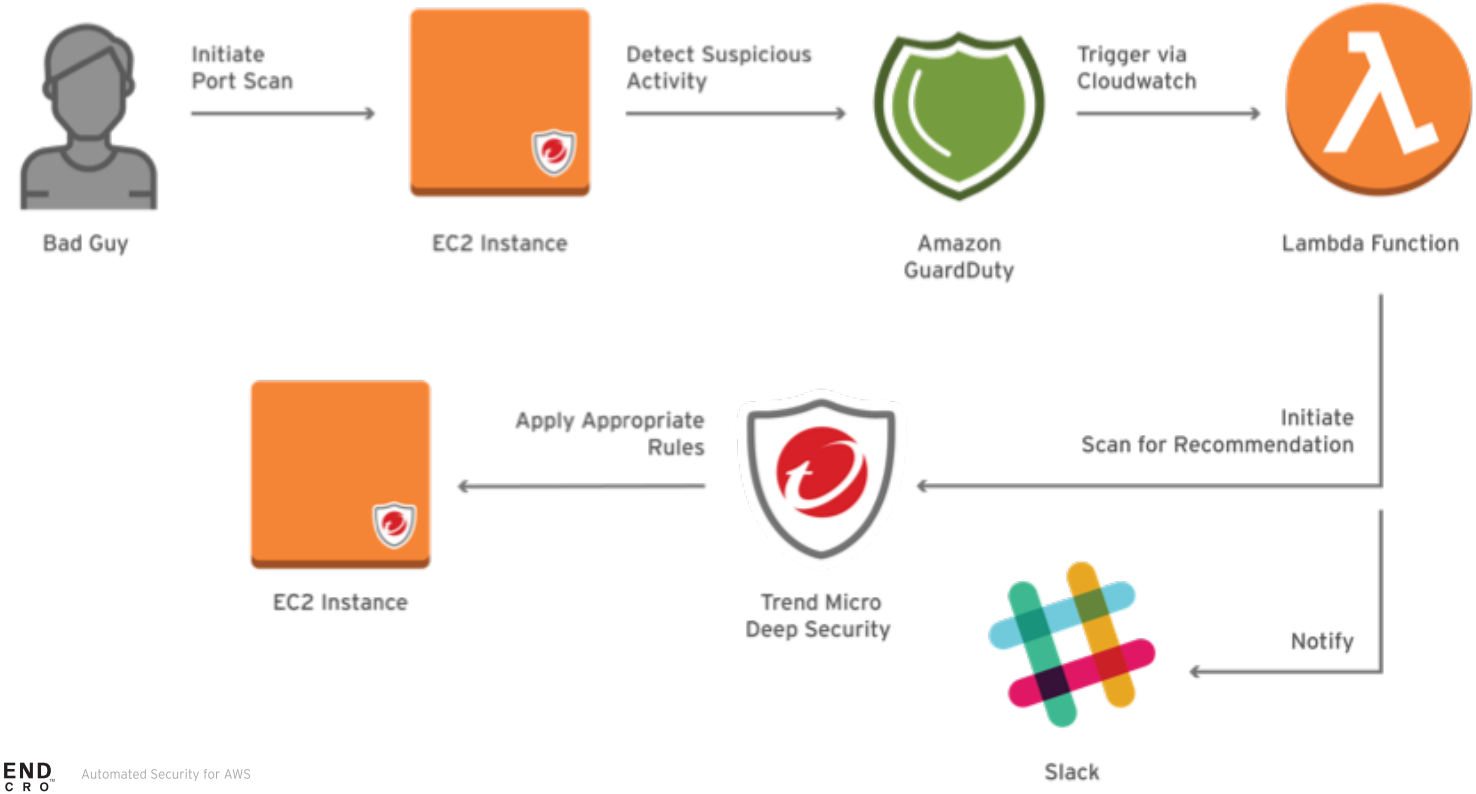
EC2 instance has an unprotected port which is being probed by a known malicious host.

Severity	Region	Count
Low	ap-southeast-1	3634
Account ID	**Resource ID**	**Threat list name**
650143975734	i-07d63412ab6...	ProofPoint
Created at	**Updated at**	
2018-04-06 14...	2018-05-01 08...	

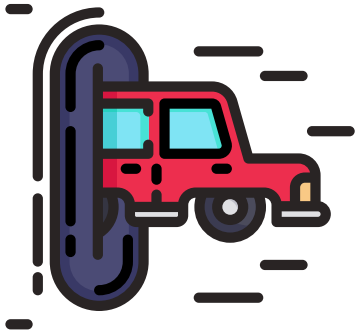
Resource affected

Resource role	Resource type
TARGET	Instance
Instance ID	**Port**
i-07d63412ab692bcf2	5000
Port name	**Instance type**
Unknown	t2.small
Instance state	**Availability zone**

Security Integration with GuardDuty



Its not hard to:



Shift security to the left

Automate incident response

TREND MICRO

Hybrid Cloud Security Solution

Network Security

Intrusion Prevention

Firewall

Vulnerability Scanning

Stop network attacks, shield vulnerable applications & servers

System Security

Application Control

Integrity Monitoring

Log Inspection

Lock down systems & detect suspicious activity

Malware Prevention

Anti-Malware

Behavioral Analysis & Machine Learning

Sandbox Analysis

Stop malware & targeted attacks

vmware

Microsoft Hyper-V

openstack CLOUD SOFTWARE

aws

Google Cloud Platform

docker

VCE

SAP

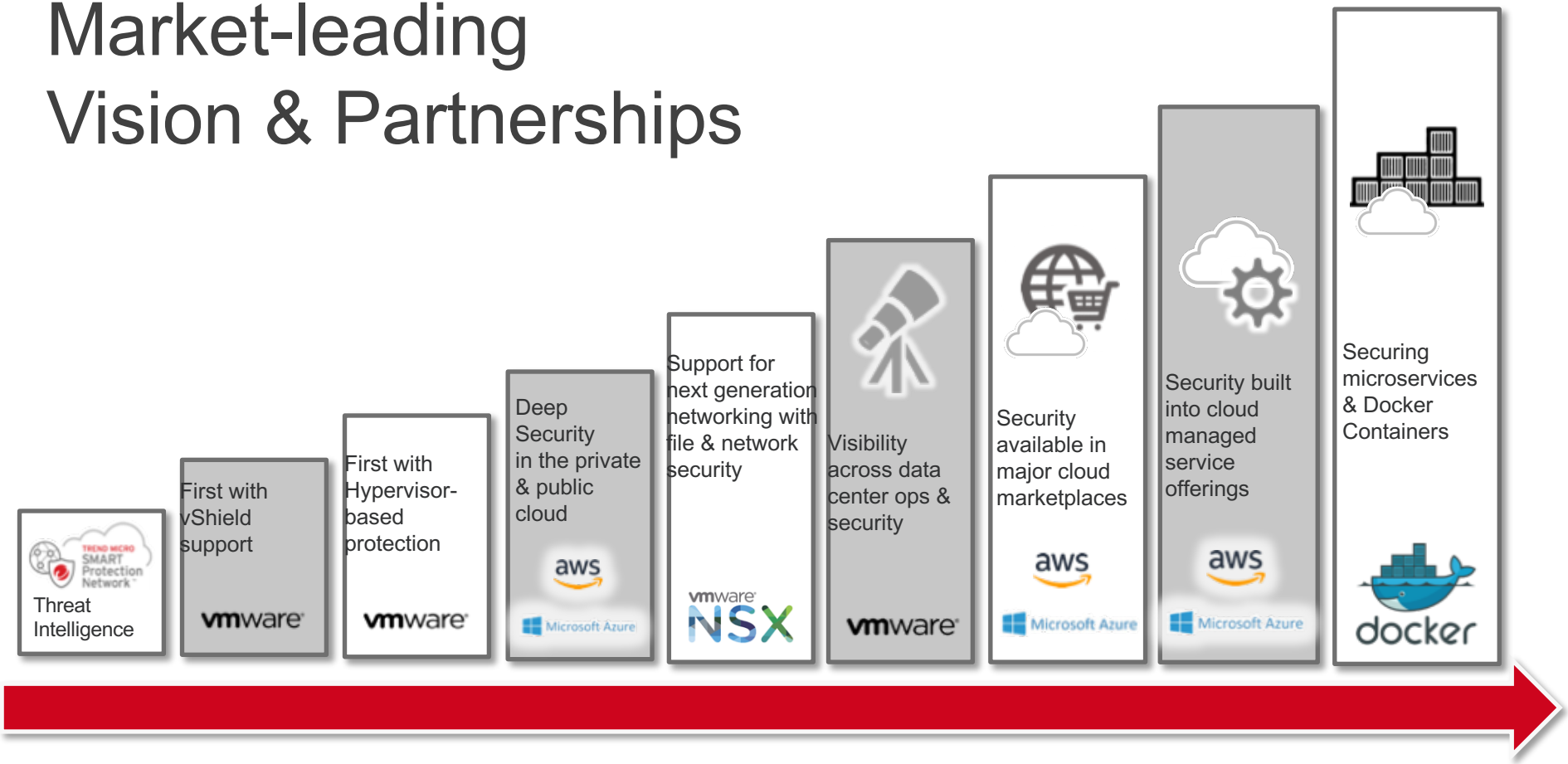
Microsoft Azure

IBM

Copyright 2018 Trend Micro Inc.

TREND MICRO

Market-leading Vision & Partnerships



Copyright 2018 Trend Micro Inc.

Thank You!

TREND MICRO