RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **PART1-R02**

Shift-left: Top 10 Most Disruptive Ideas of Modern Cloud Security

Nicolas Popp

Chief Product Officer
Tenable
https://www.linkedin.com/in/nicopopp/

DISCLAIMER

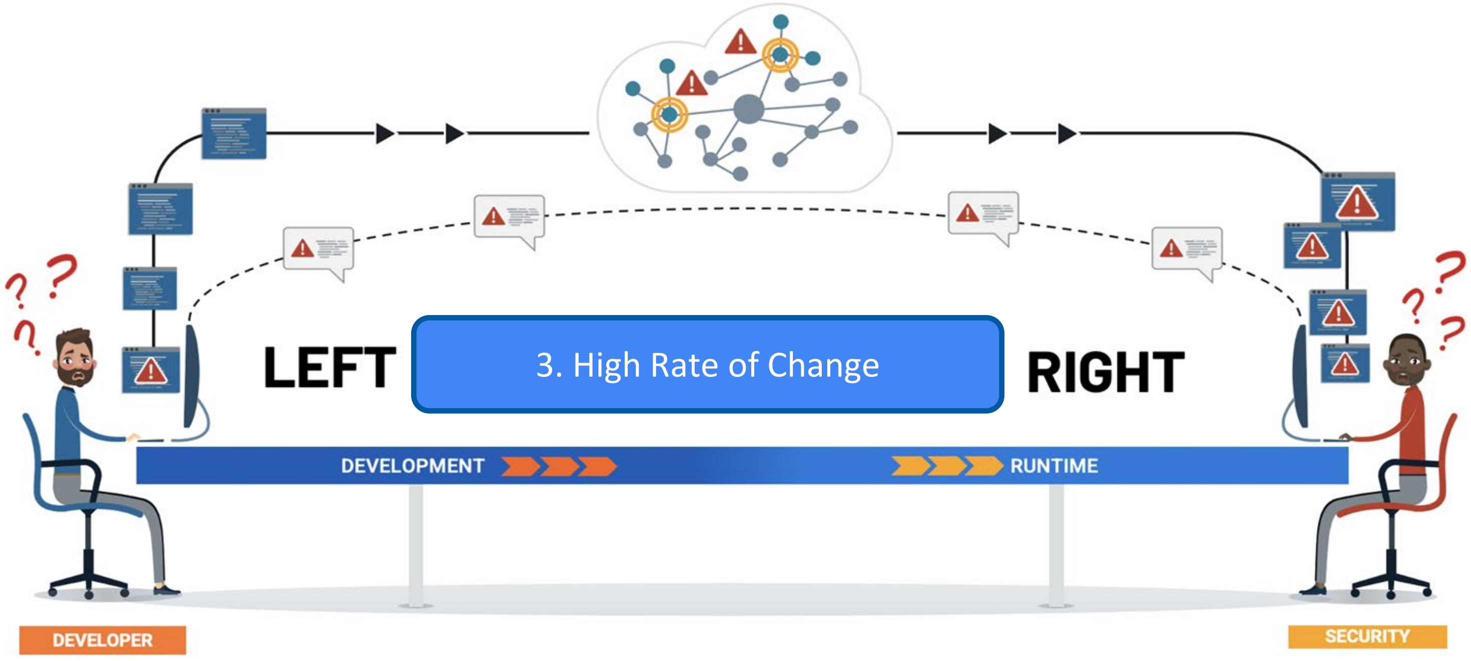
Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

#1: FROM LIFT & SHIFT TO SHIFT & LEFT

1. New Architectures

2. New Deployment Model

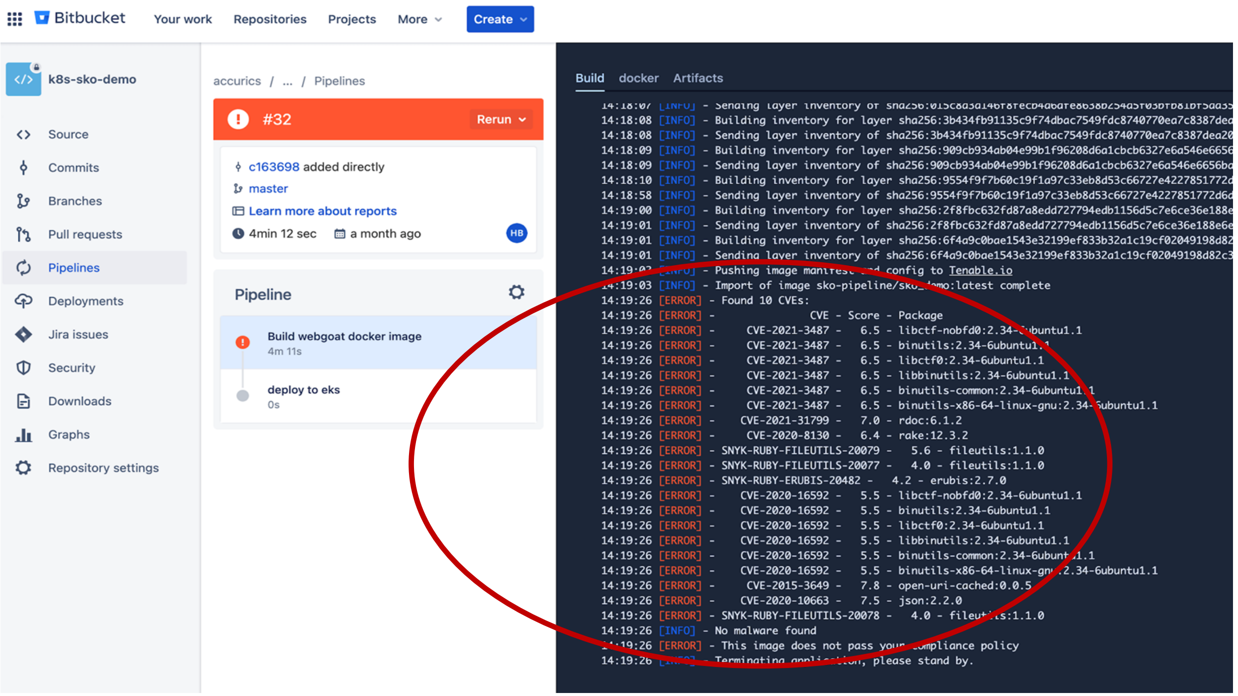


Conclusion:
New Approach to
Security Required

Shift-Left: Rethink runtime-centric approach to cloud security
(too slow, too late, lacks app context, cannot remediate)

#2: REVENGE OF THE NERDS (DEV RULES SECURITY)

PEACE LOVE CODE

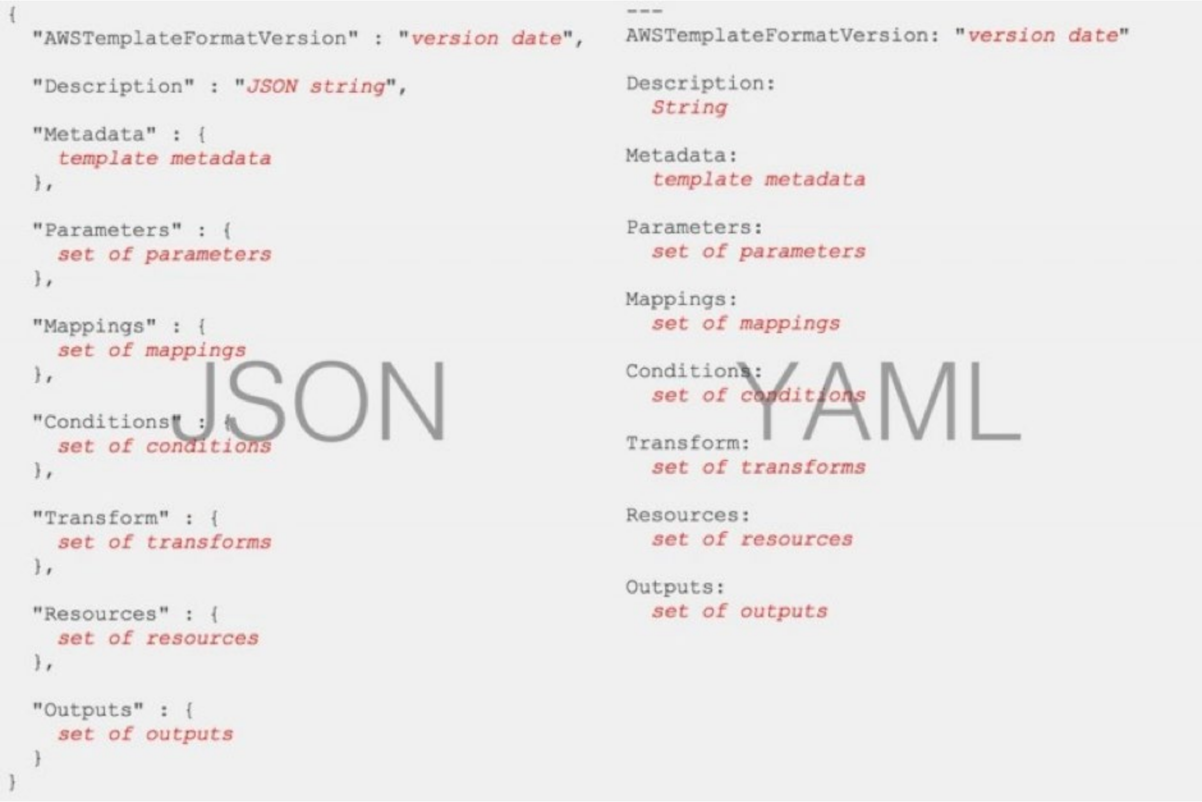


```
14:18:07 [INFO] - Sending layer inventory of sha256:015c8a3a146f8fecb4a6afe8638b254a5f05bfb81bf5aa35
14:18:08 [INFO] - Building inventory for layer sha256:3b434fb91135c9f74dbac7549fdc8740770ea7c8387dea
14:18:08 [INFO] - Sending layer inventory of sha256:3b434fb91135c9f74dbac7549fdc8740770ea7c8387dea20
14:18:09 [INFO] - Building inventory for layer sha256:909cb934ab04e99b1f96208d6a1cbcb6327e6a546e6656
14:18:09 [INFO] - Sending layer inventory of sha256:909cb934ab04e99b1f96208d6a1cbcb6327e6a546e6656ba
14:18:10 [INFO] - Building inventory for layer sha256:9554f9f7b60c19f1a97c33eb8d53c66727e4227851772d
14:18:58 [INFO] - Sending layer inventory of sha256:9554f9f7b60c19f1a97c33eb8d53c66727e4227851772d6d
14:19:00 [INFO] - Building inventory for layer sha256:2f8fbc632fd87a8edd727794edb1156d5c7e6ce36e188e
14:19:01 [INFO] - Sending layer inventory of sha256:2f8fbc632fd87a8edd727794edb1156d5c7e6ce36e188e6e
14:19:01 [INFO] - Building inventory for layer sha256:6f4a9c0bae1543e32199ef833b32a1c19cf02049198d82
14:19:01 [INFO] - Sending layer inventory of sha256:6f4a9c0bae1543e32199ef833b32a1c19cf02049198d82c3
14:19:03 [INFO] - Pushing image manifest and config to Tenable.io
14:19:03 [INFO] - Import of image sko-pipeline/sko_demo:latest complete
14:19:26 [ERROR] - Found 10 CVEs:
14:19:26 [ERROR] -                CVE - Score - Package
14:19:26 [ERROR] -      CVE-2021-3487 -   6.5 - libctf-nobfd0:2.34-6ubuntu1.1
14:19:26 [ERROR] -      CVE-2021-3487 -   6.5 - binutils:2.34-6ubuntu1.1
14:19:26 [ERROR] -      CVE-2021-3487 -   6.5 - libctf0:2.34-6ubuntu1.1
14:19:26 [ERROR] -      CVE-2021-3487 -   6.5 - libbinutils:2.34-6ubuntu1.1
14:19:26 [ERROR] -      CVE-2021-3487 -   6.5 - binutils-common:2.34-6ubuntu1.1
14:19:26 [ERROR] -      CVE-2021-3487 -   6.5 - binutils-x86-64-linux-gnu:2.34-6ubuntu1.1
14:19:26 [ERROR] -     CVE-2021-31799 -   7.0 - rdoc:6.1.2
14:19:26 [ERROR] -      CVE-2020-8130 -   6.4 - rake:12.3.2
14:19:26 [ERROR] - SNYK-RUBY-FILEUTILS-20079 -   5.6 - fileutils:1.1.0
14:19:26 [ERROR] - SNYK-RUBY-FILEUTILS-20077 -   4.0 - fileutils:1.1.0
14:19:26 [ERROR] - SNYK-RUBY-ERUBIS-20482 -   4.2 - erubis:2.7.0
14:19:26 [ERROR] -     CVE-2020-16592 -   5.5 - libctf-nobfd0:2.34-6ubuntu1.1
14:19:26 [ERROR] -     CVE-2020-16592 -   5.5 - binutils:2.34-6ubuntu1.1
14:19:26 [ERROR] -     CVE-2020-16592 -   5.5 - libctf0:2.34-6ubuntu1.1
14:19:26 [ERROR] -     CVE-2020-16592 -   5.5 - libbinutils:2.34-6ubuntu1.1
14:19:26 [ERROR] -     CVE-2020-16592 -   5.5 - binutils-common:2.34-6ubuntu1.1
14:19:26 [ERROR] -     CVE-2020-16592 -   5.5 - binutils-x86-64-linux-gnu:2.34-6ubuntu1.1
14:19:26 [ERROR] -      CVE-2015-3649 -   7.8 - open-uri-cached:0.0.5
14:19:26 [ERROR] -     CVE-2020-10663 -   7.5 - json:2.2.0
14:19:26 [ERROR] - SNYK-RUBY-FILEUTILS-20078 -   4.0 - fileutils:1.1.0
14:19:26 [INFO] - No malware found
14:19:26 [ERROR] - This image does not pass your compliance policy
14:19:26 [INFO] - Terminating application, please stand by.
```

Take a DEV-Centric Approach: Don’t take developers to security, take security to developers.
Security must integrate into developer platforms: code repos, pipelines, …
(GitHub, GitLabs. Jenkins, Jira…)

#3: HELLO, IAC SECURITY. GOOD-BYE CSPM

IaC is foundational to Cloud Native App Development



```
{
  "AWSTemplateFormatVersion" : "version date",

  "Description" : "JSON string",

  "Metadata" : {
    template metadata
  },

  "Parameters" : {
    set of parameters
  },

  "Mappings" : {
    set of mappings
  },

  "Conditions" : {
    set of conditions
  },

  "Transform" : {
    set of transforms
  },

  "Resources" : {
    set of resources
  },

  "Outputs" : {
    set of outputs
  }
}
```

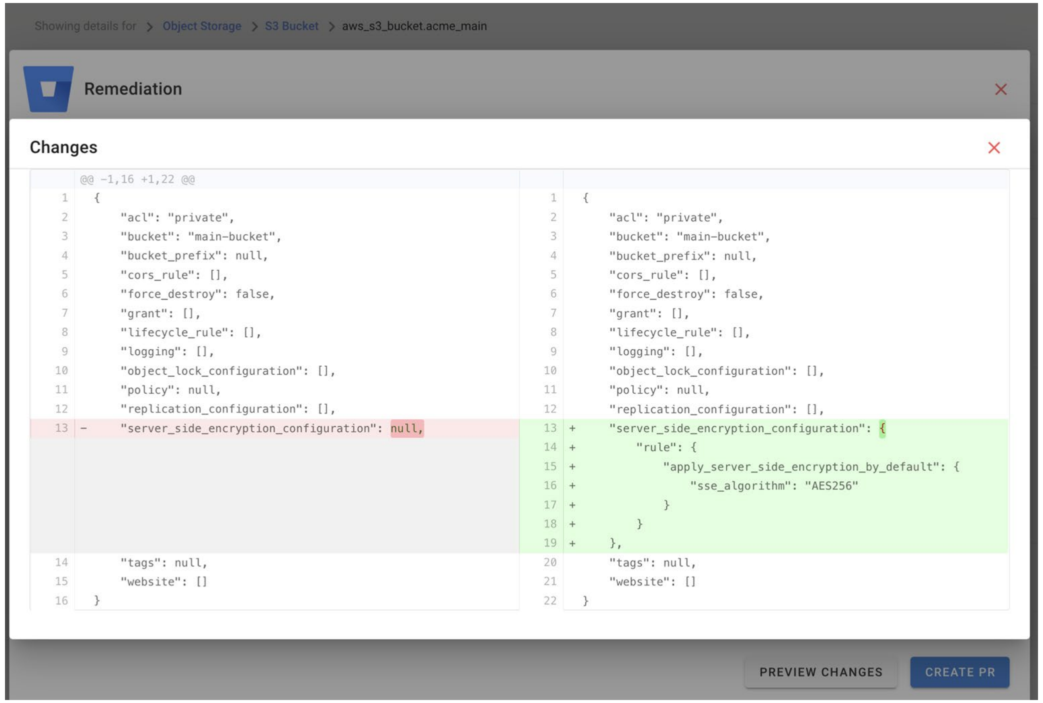
```
---
AWSTemplateFormatVersion: "version date"

Description:
  String

Metadata:
  template metadata

Parameters:
  set of parameters

Mappings:
  set of mappings

Conditions:
  set of conditions

Transform:
  set of transforms

Resources:
  set of resources

Outputs:
  set of outputs
```

IaC becomes Foundational to Cloud Native App Security

Embrace IaC Security: As your developers embrace IaC, IaC security will become a cornerstone of your cloud security (VM, CSPM, CIEM all shift-left based on IaC scanning)

#3+: PATCHING IS DEAD

Dev Side: Unencrypted S3 Bucket


Showing details for > Object Storage > S3 Bucket > aws_s3_bucket.acme_main
Remediation
Changes
PREVIEW CHANGES
CREATE PR

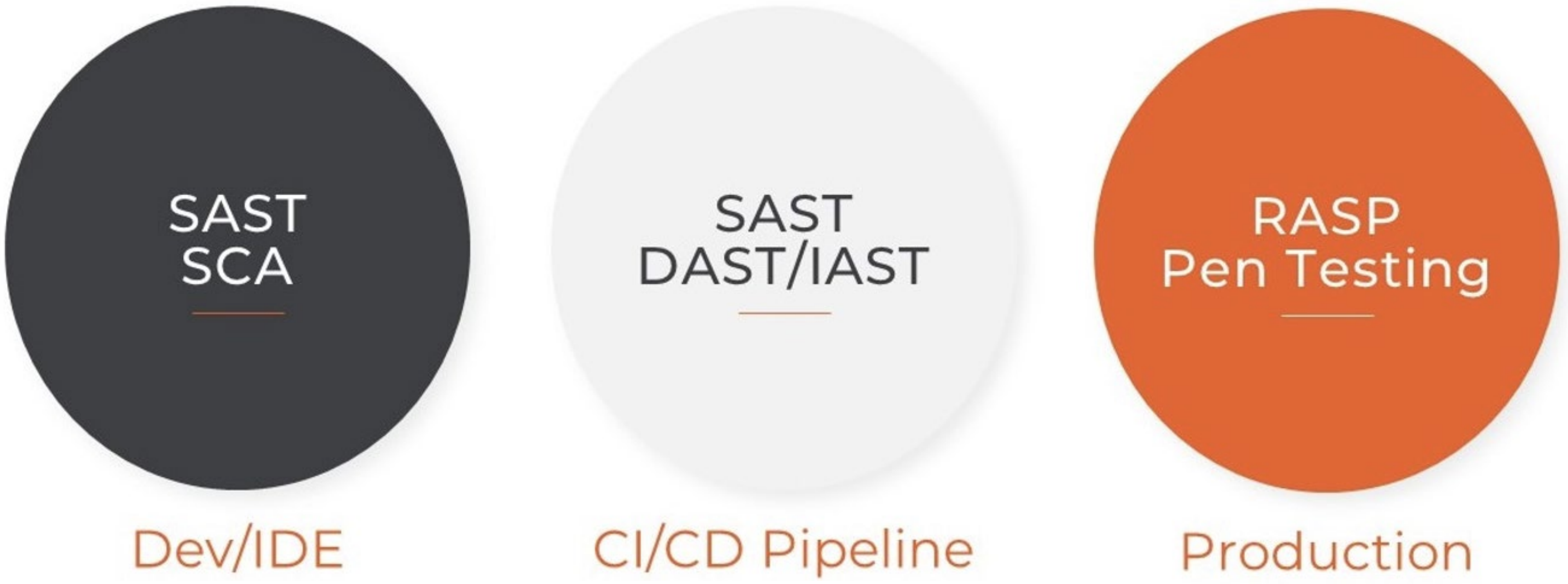
```
@@ -1,16 +1,22 @@
 {
     "acl": "private",
     "bucket": "main-bucket",
     "bucket_prefix": null,
     "cors_rule": [],
     "force_destroy": false,
     "grant": [],
     "lifecycle_rule": [],
     "logging": [],
     "object_lock_configuration": [],
     "policy": null,
     "replication_configuration": [],
-    "server_side_encryption_configuration": null,
     "tags": null,
     "website": []
 }
```

```
 {
     "acl": "private",
     "bucket": "main-bucket",
     "bucket_prefix": null,
     "cors_rule": [],
     "force_destroy": false,
     "grant": [],
     "lifecycle_rule": [],
     "logging": [],
     "object_lock_configuration": [],
     "policy": null,
     "replication_configuration": [],
+    "server_side_encryption_configuration": {
+        "rule": {
+            "apply_server_side_encryption_by_default": {
+                "sse_algorithm": "AES256"
+            }
+        }
+    },
     "tags": null,
     "website": []
 }
```

Sec Side: Auto-Generated Remediation as Code

Patching as Code: Do not patch the cloud. Embrace the immutable runtime principles and remediation as code based on IaC and pull-requests.

#4: APPSEC IS COOL AGAIN



SAST
SCA

Dev/IDE

SAST
DAST/IAST

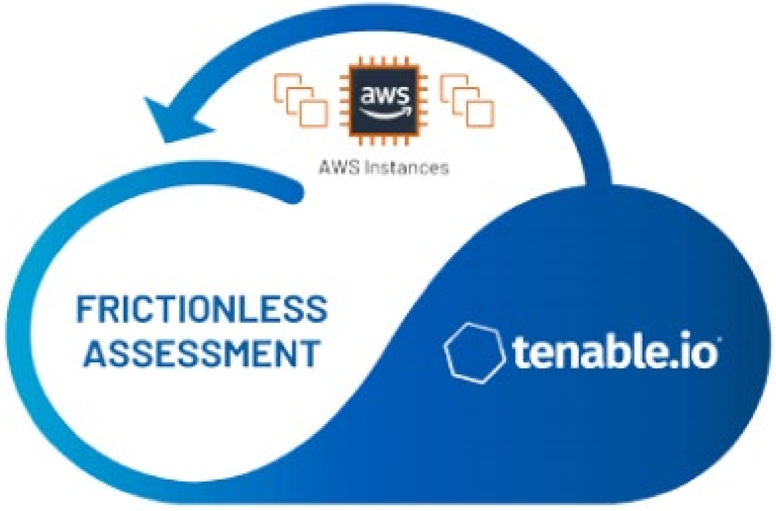
CI/CD Pipeline

RASP
Pen Testing

Production

The Return of AppSec: you can no longer ignore the AppSec discipline of SAST and SCA. They will become the left most part of your cloud security strategy

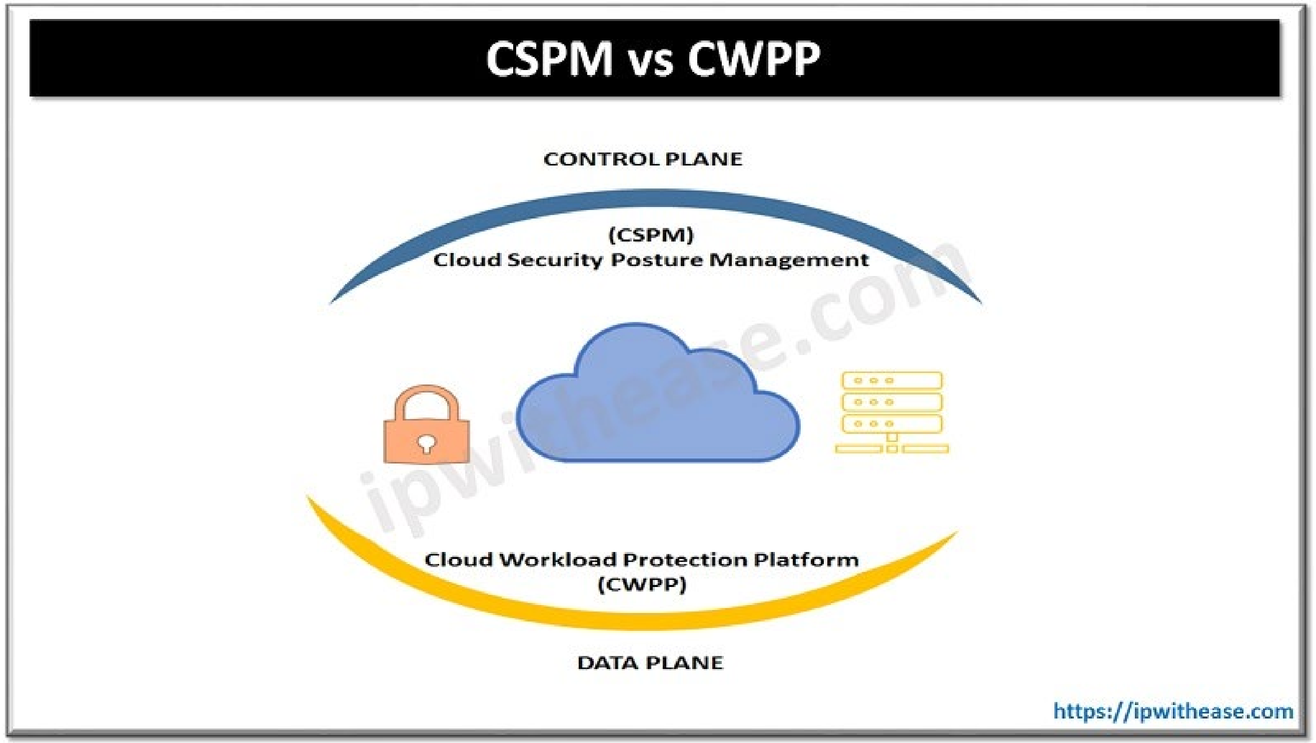
#5: THE API-BASED SECURITY REVOLUTION IS BEING TELEVISED



From Agent-Based to API-Based VM

Favor Agent-Less Approach: Cloud security vendors must leverage cloud APIs to enable **agentless** and **continuous** cloud security. The transformation of VM into API-based cloud native VM is a great example.

#6: RIGHT IS NOT WRONG (BUT IT HAS AN AGENT)



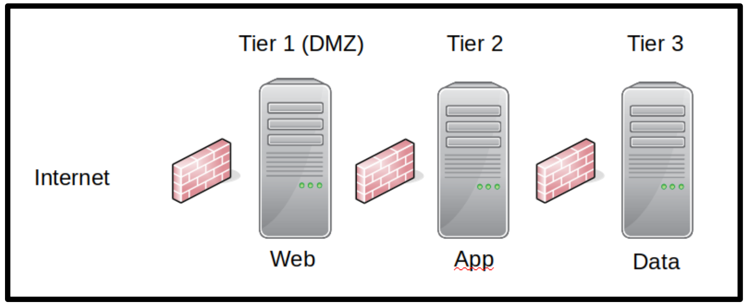
Endpoint Protection Still Matters

- Suspicious OS calls monitoring
- Abnormal process activity
- Process & file integrity
- Malicious egress traffic

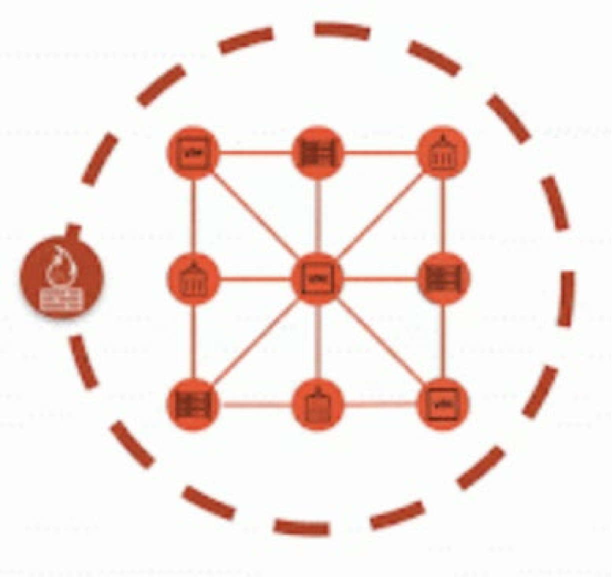
eBPF

Runtime Security Still Matters! Don’t let the cool and leftist kids (AppSec vendors) fool you. The right side security is still required, but EPP vendors must embrace cloud architecture (e.g. eBPF).

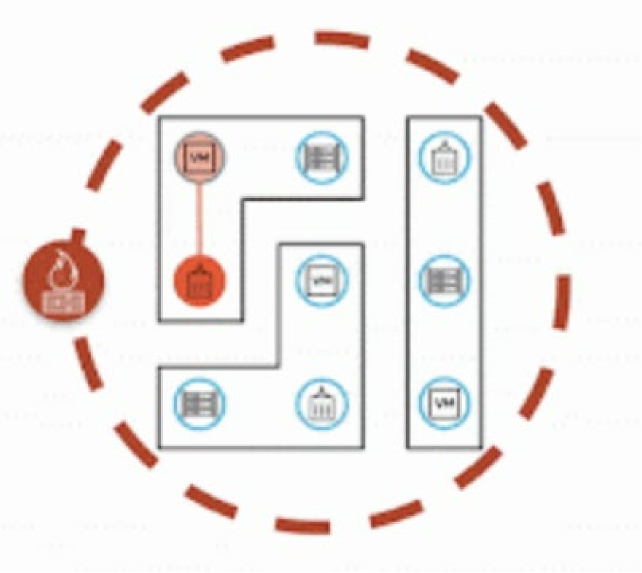
#7: IDENTITY IS THE NEW FIREWALL (MICRO-SEGMENTATION)



Segmented Three Tier App



API Mesh or Security Mess?

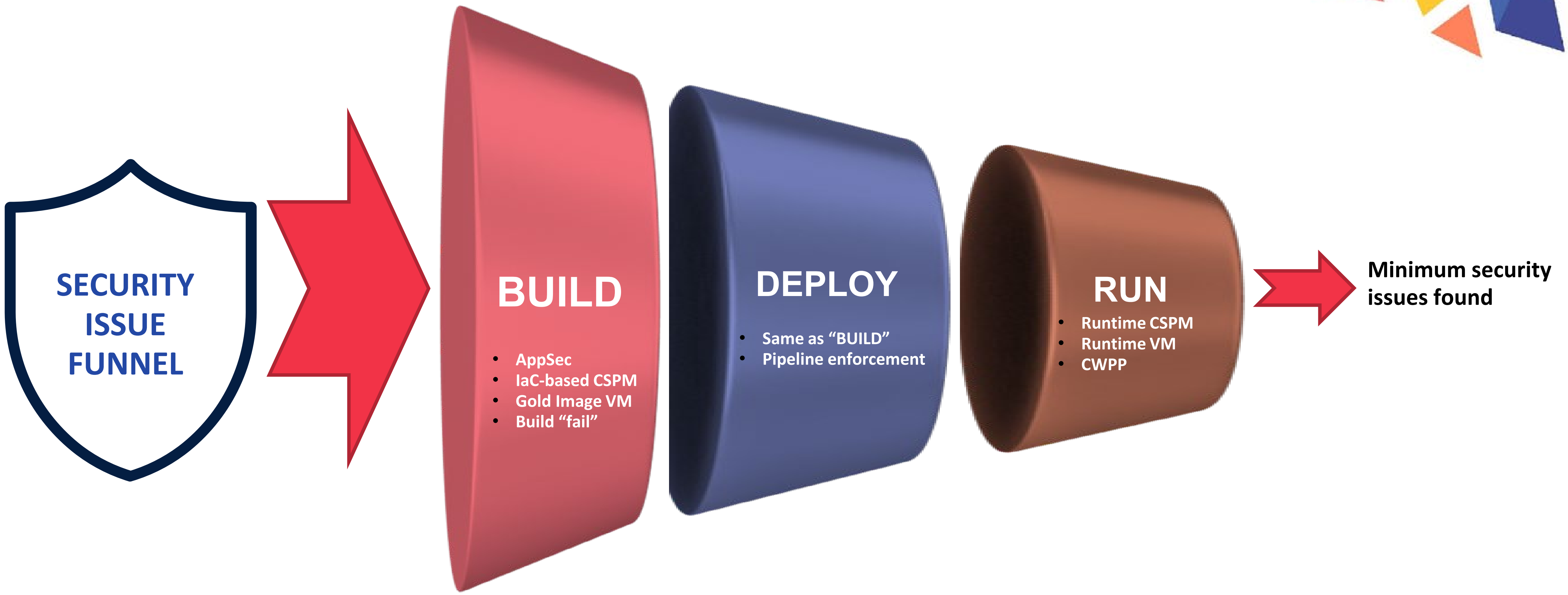


Segmented Mesh

eBPF Convergence?!

Micro-Segmentation / ZTNA Dirty Secret! Beware, IAM policies are even more complex than firewall rules! Look for automation

#8: CYBER-HEAVEN HAS GATES



BUILD
- AppSec
- IaC-based CSPM
- Gold Image VM
- Build “fail”

DEPLOY
- Same as “BUILD”
- Pipeline enforcement

RUN
- Runtime CSPM
- Runtime VM
- CWPP

Minimum security issues found

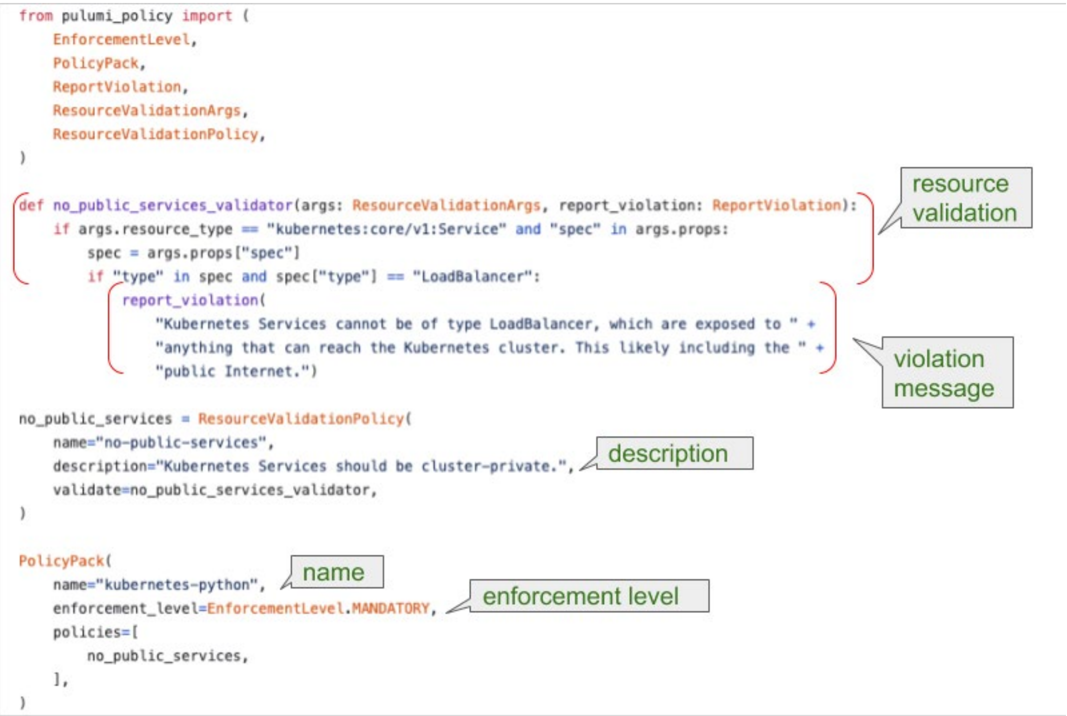
Deploy Continuous Security Gates: Cloud security should account for changes across the cloud app life-cycle to detect and eliminate less and less security flaws from build-time (gate 1), to deployment (pipeline gate 2) to runtime detection-response (SecOps gate)

#8+: THREE GATES BUT ONE POLICY AS CODE!

1. **Consistent security policy across all gates**

2. **Policy as code (Dev-Friendly)**

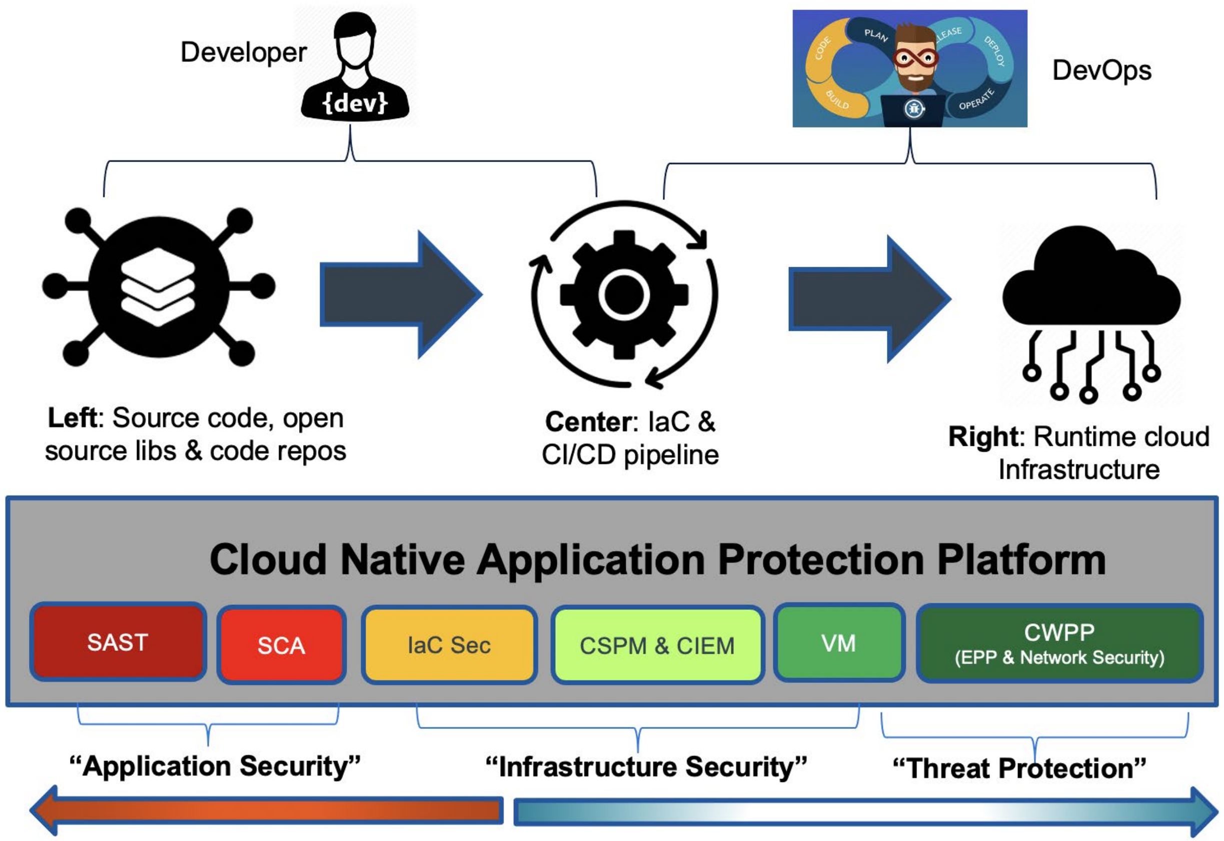
3. **Open Standard over proprietary format (OPA)**



```python
from pulumi_policy import (
    EnforcementLevel,
    PolicyPack,
    ReportViolation,
    ResourceValidationArgs,
    ResourceValidationPolicy,
)

def no_public_services_validator(args: ResourceValidationArgs, report_violation: ReportViolation):
    if args.resource_type == "kubernetes:core/v1:Service" and "spec" in args.props:
        spec = args.props["spec"]
        if "type" in spec and spec["type"] == "LoadBalancer":
            report_violation(
                "Kubernetes Services cannot be of type LoadBalancer, which are exposed to " +
                "anything that can reach the Kubernetes cluster. This likely including the " +
                "public Internet.")

no_public_services = ResourceValidationPolicy(
    name="no-public-services",
    description="Kubernetes Services should be cluster-private.",
    validate=no_public_services_validator,
)

PolicyPack(
    name="kubernetes-python",
    enforcement_level=EnforcementLevel.MANDATORY,
    policies=[
        no_public_services,
    ],
)
```

One "Policy as code" to rule them all: Unify the gates of cyber-heaven with a single policy as code. Consider open standards over vendor-centric policy languages

#9: CNAPP: THE CLOUD EMPIRE OR THE BALKANS?



Developer

DevOps

Left: Source code, open source libs & code repos

Center: IaC & CI/CD pipeline

Right: Runtime cloud Infrastructure

Cloud Native Application Protection Platform

SAST

SCA

IaC Sec

CSPM & CIEM

VM

CWPP
(EPP & Network Security)

"Application Security"

"Infrastructure Security"

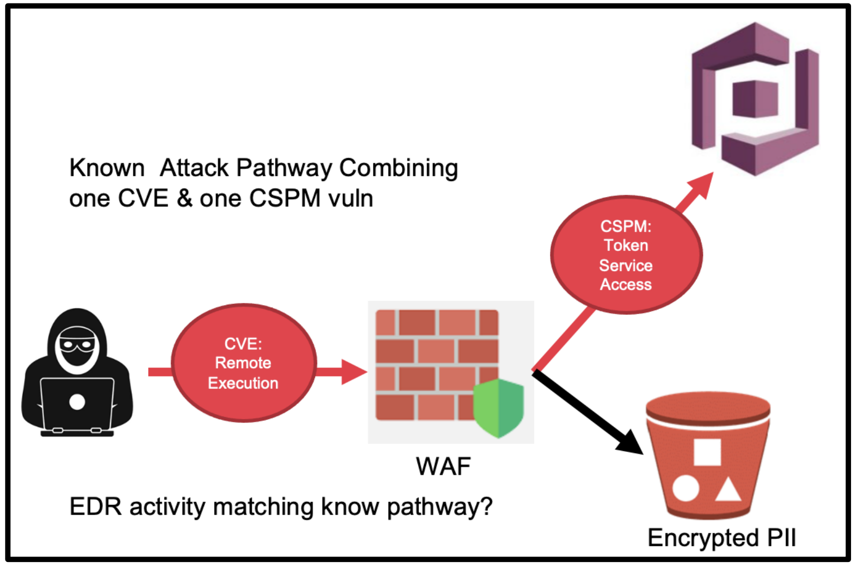
"Threat Protection"

1. **Left:** App Sec
2. **Center:** Cloud Native VM
3. **Right:** Threat Detection

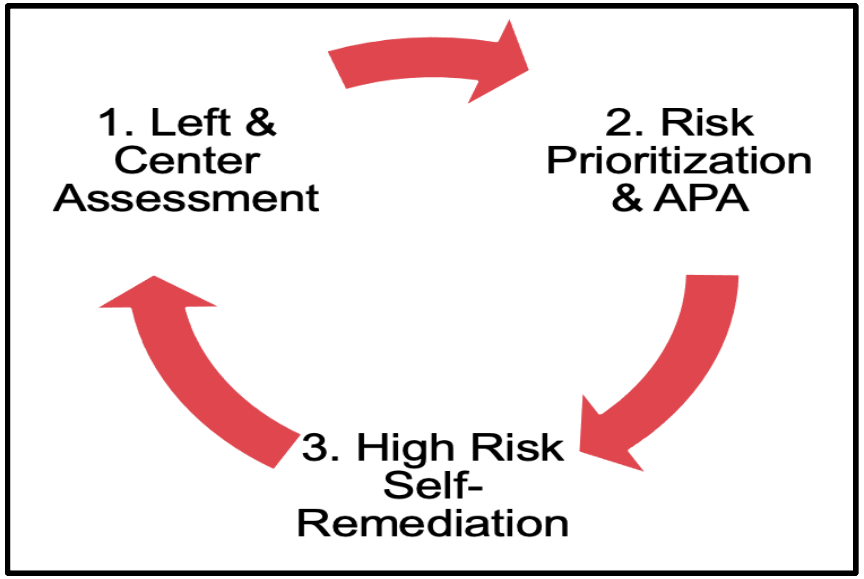
Know Yourself: large Enterprise will continue to be hybrid, thus best-of breed ("three towers, three vendors" across on-prem and cloud) while smaller 'all-cloud' enterprises will benefit from single vendor platform

#10: FUTURE: LEFT BRAIN & AUTONOMOUS SECURITY

Left-Guided CWPP


Known Attack Pathway Combining
one CVE & one CSPM vuln
CVE: Remote Execution
WAF
CSPM: Token Service Access
Encrypted PII
EDR activity matching know pathway?

Autonomous Security


1. Left & Center Assessment
2. Risk Prioritization & APA
3. High Risk Self-Remediation

Left-Side Guided Runtime security: Left side establishes context (asset relationships) and risk (prioritized findings and APA) to help prioritizing SecOps security events

NEXT STEP: SHIFT-LEFT AS EASY AS 1-2-3

1. **THIS WEEK**
   Become a “shift-left” thinker!
2. **NEXT MONTH**
   Identify one cloud-native application security project you can shift-left
3. **THIS SUMMER**
   Make it real!

Thank You & Shameless Plug!

linkedin.com/in/nicopopp

tenable.cs™

cloud security