



COLLABORATION

National Conference 2017

Murray Goldschmidt

Chief Operating Officer, Sense of Security Pty Ltd

AWS - DevOps Cyber Attack Kill Chain with Automated Security Response & Visibility

Track 1

Wednesday, October 11, 2017

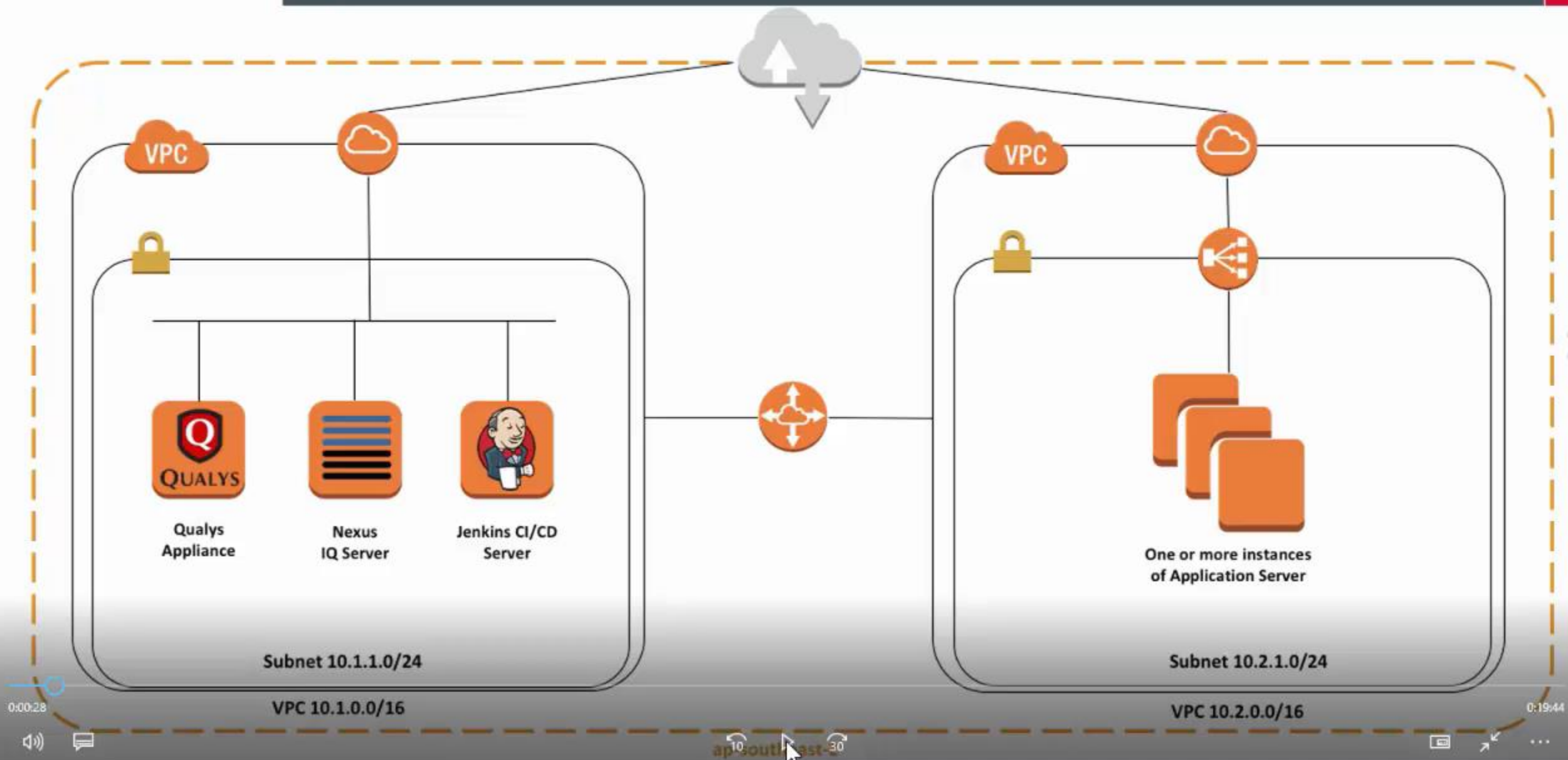
11:10 AM - 11:55 AM

Grand Ballroom 1



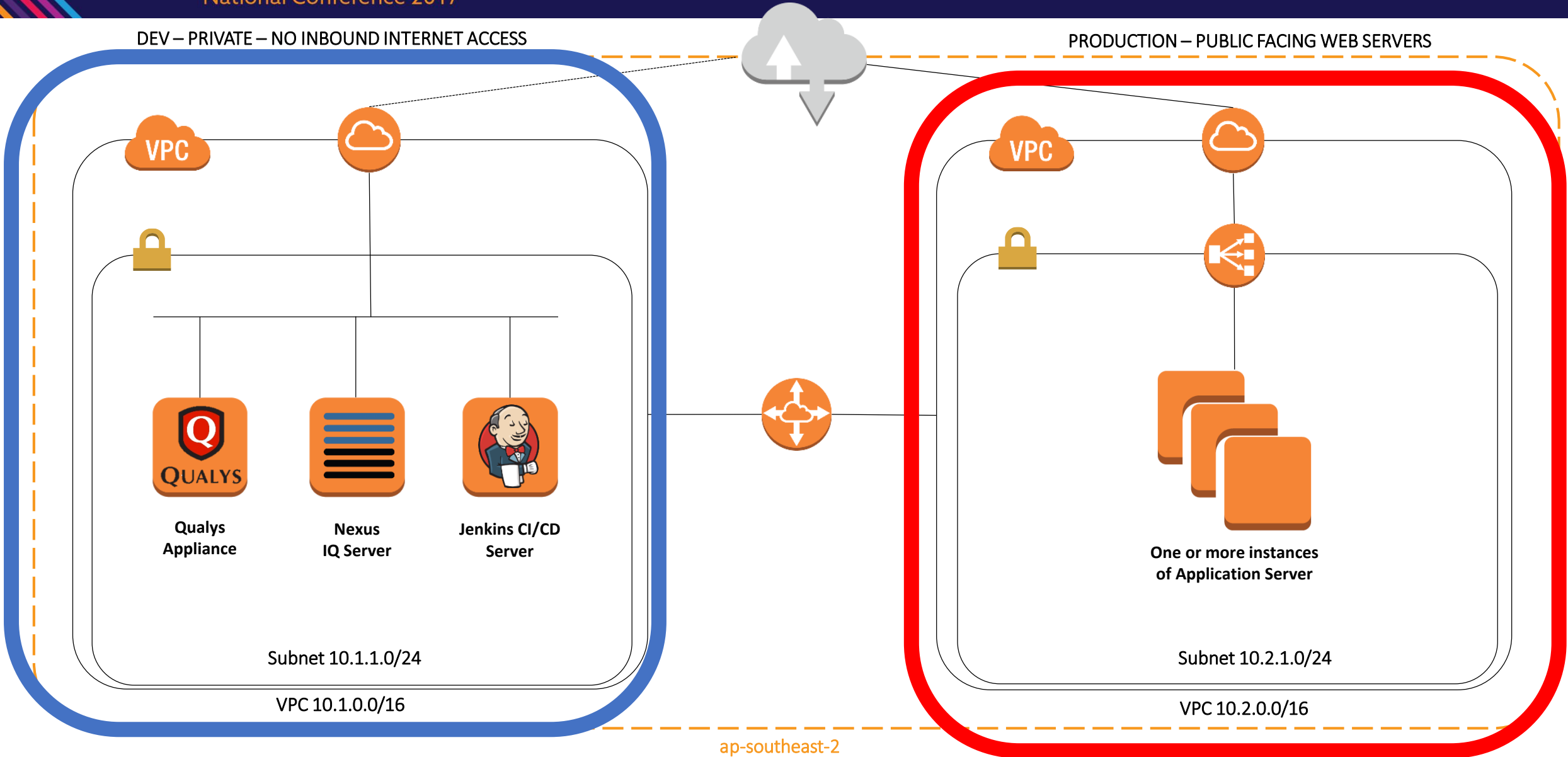
Sense of Security, DevSecOps AWS Kill Chain Demonstration

<https://www.youtube.com/watch?v=fm4CqlxqQfs>



DEV – PRIVATE – NO INBOUND INTERNET ACCESS

PRODUCTION – PUBLIC FACING WEB SERVERS



→ ↺ Secure | <https://www.wired.com/story/equifax-breach-no-excuse/>



Equifax Officially Has No Excuse

embarrassingly inadequate credentials of "admin/admin." Equifax took the platform down on Tuesday. But observers say the ongoing discoveries increasingly paint a picture of negligence—especially in Equifax's failure to protect itself against a known flaw with a ready fix.

A 'Relatively Easy' Hack

The vulnerability that attackers exploited to access Equifax's system was in the Apache Struts web-application software, a widely used enterprise platform. The Apache

SHARE



3288



Equifax blames massive data breach on Apache Struts vulnerability

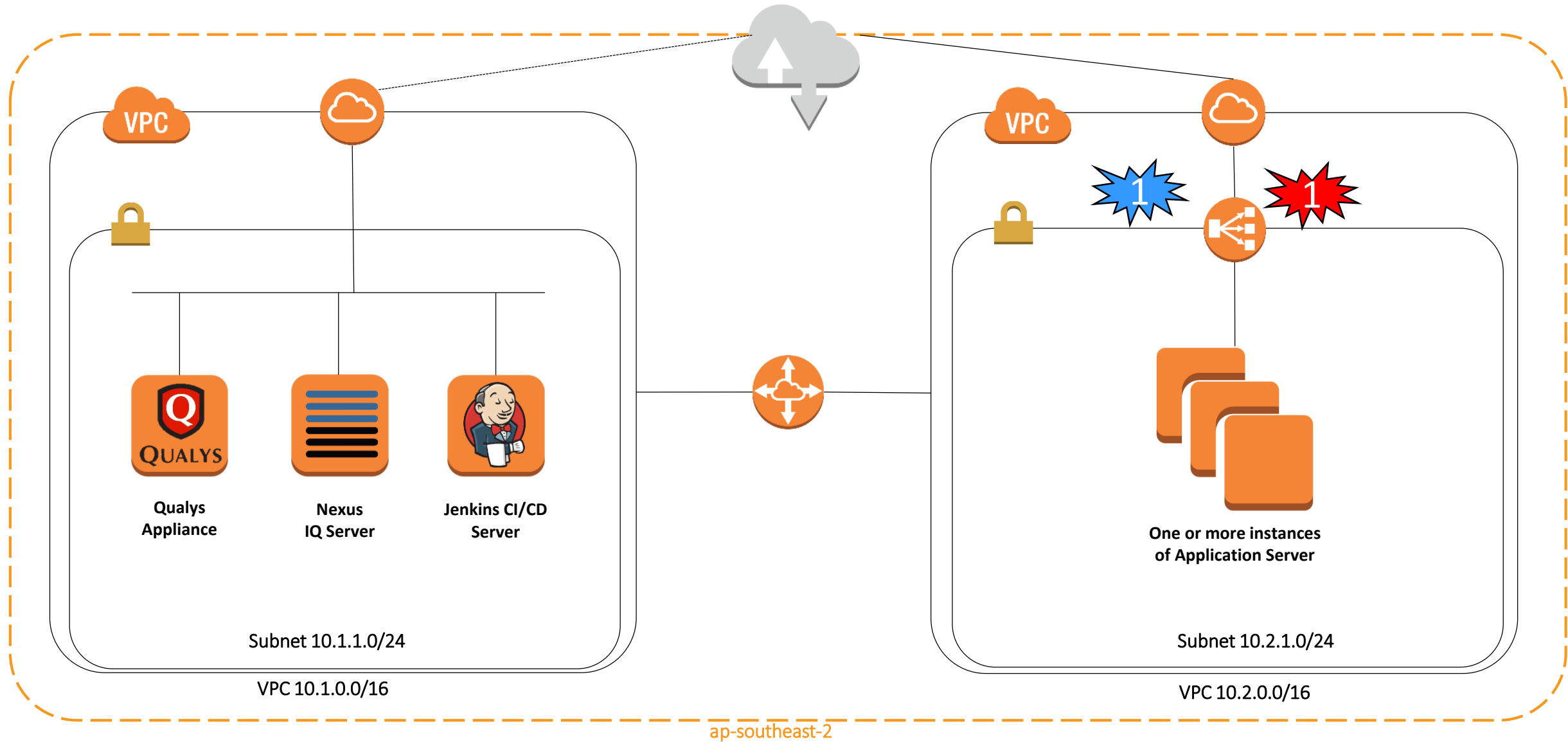
Hack compromised the personal details of as many as 143 million US consumers

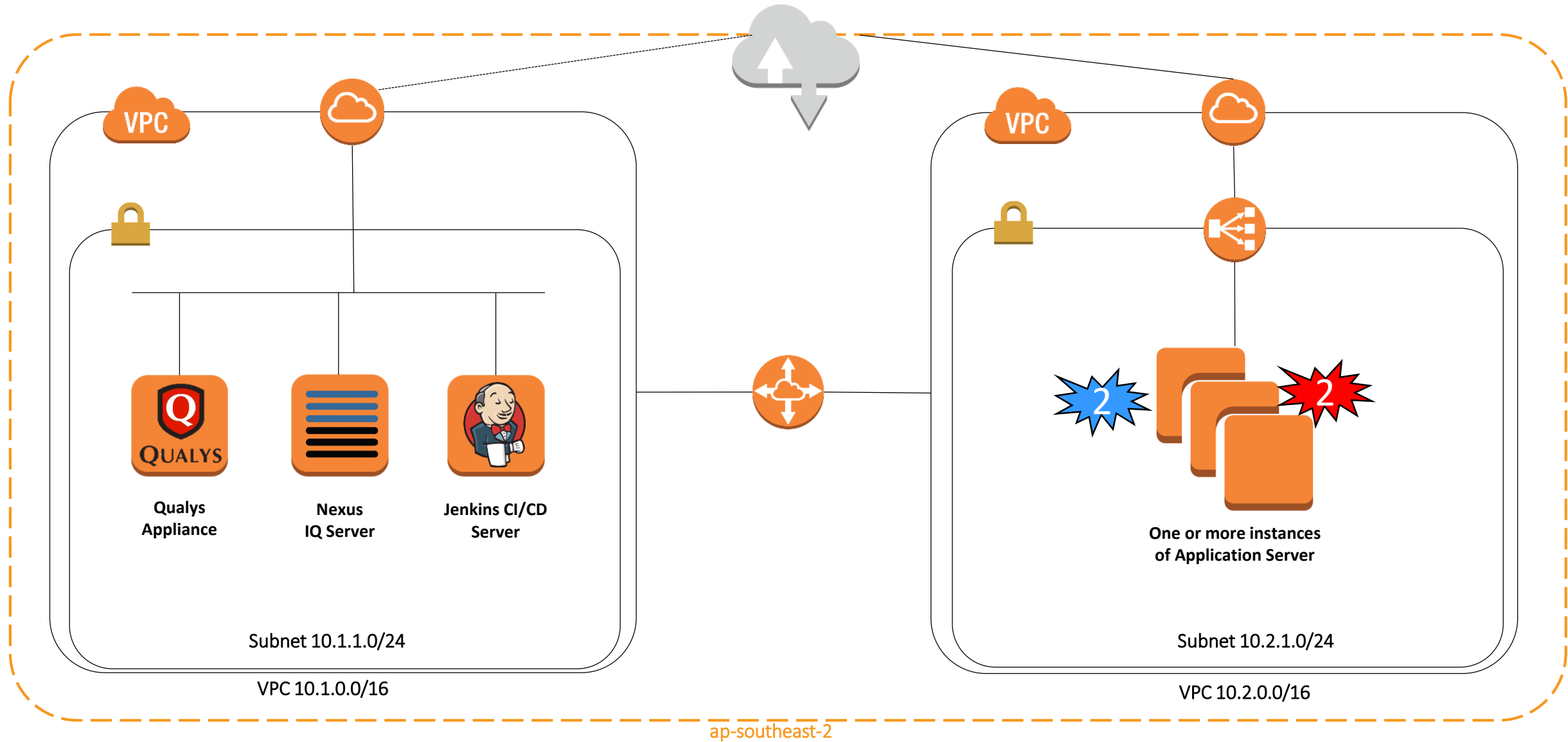


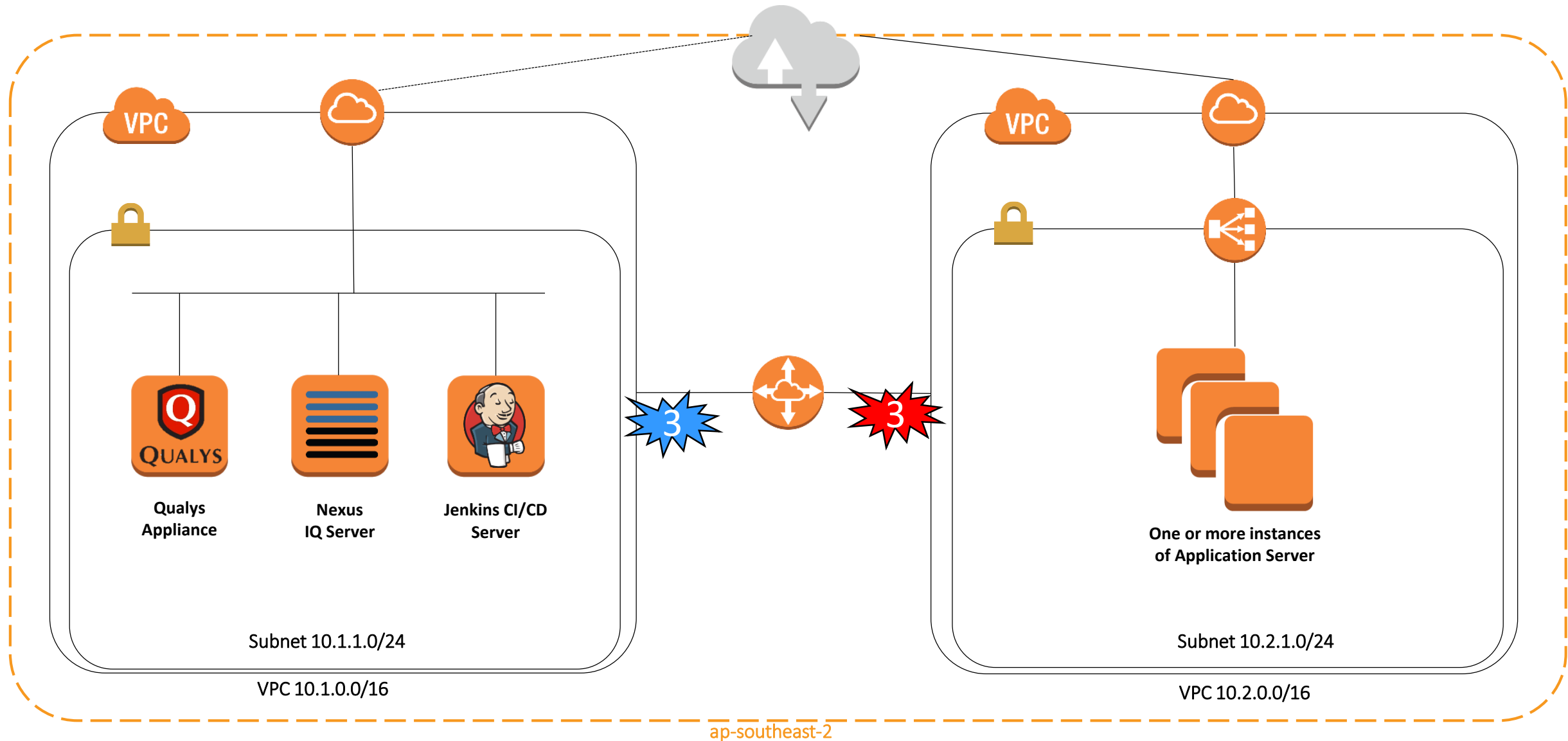
Reuters
(ARN)

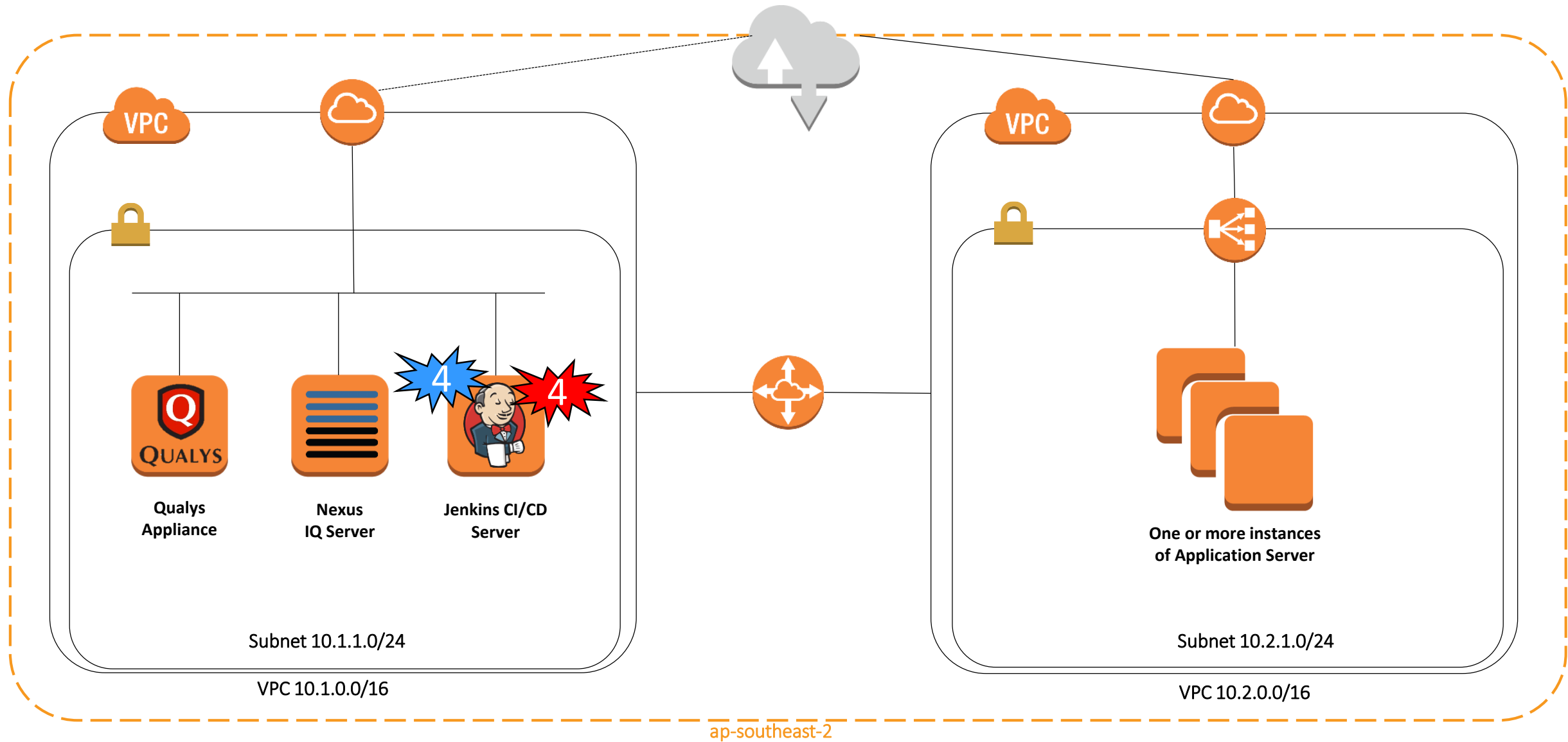
14 September, 2017 15:23

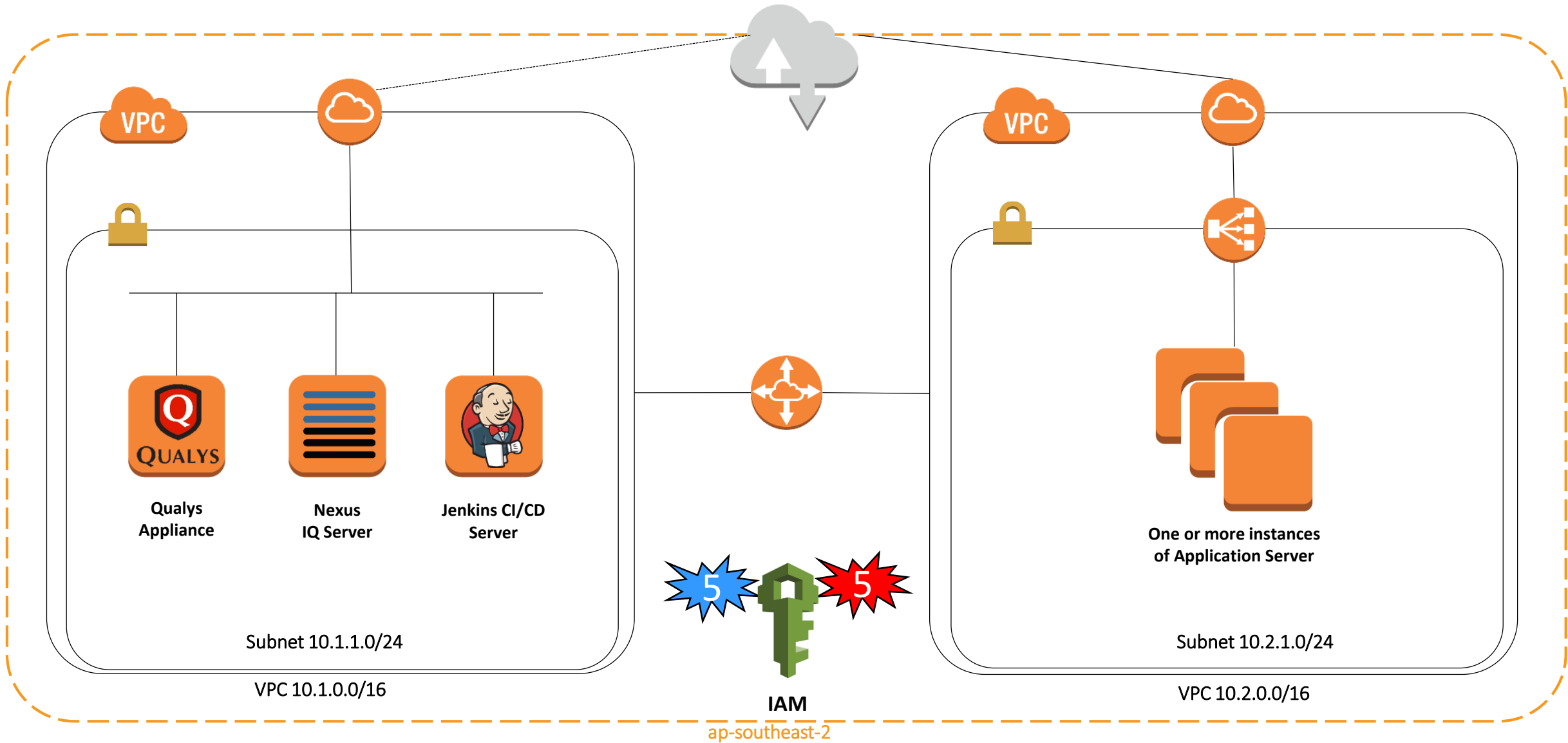
RECAP











The defaults, including what would at face(palm) value appear to be innocuous settings, cause a litany of problems ...



PREVENTION

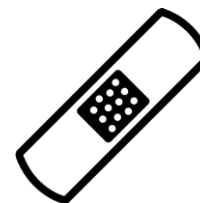
through

CONFIGURATION MGT

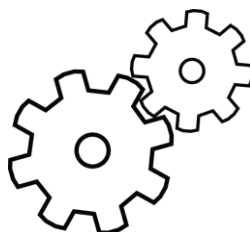
OPERATIONAL MGT (PATCH/VULN)

CONTINUOUS MONITORING

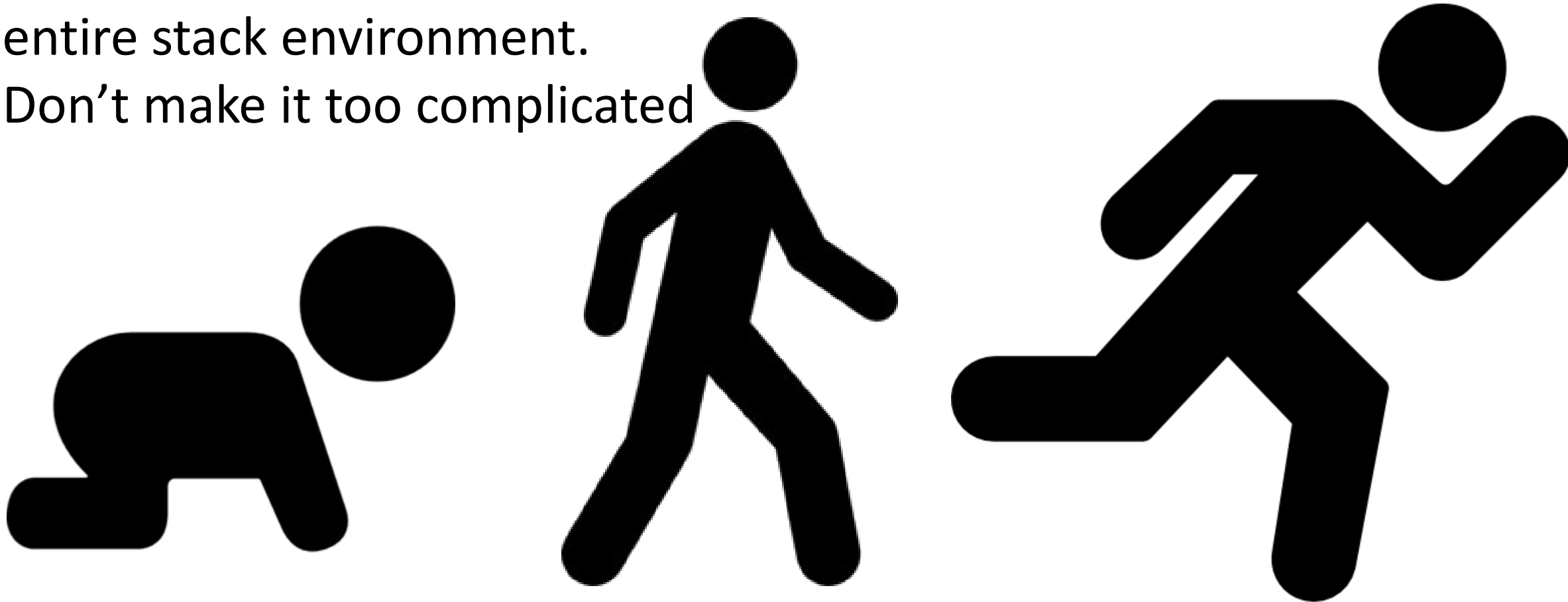
SELF HEALING

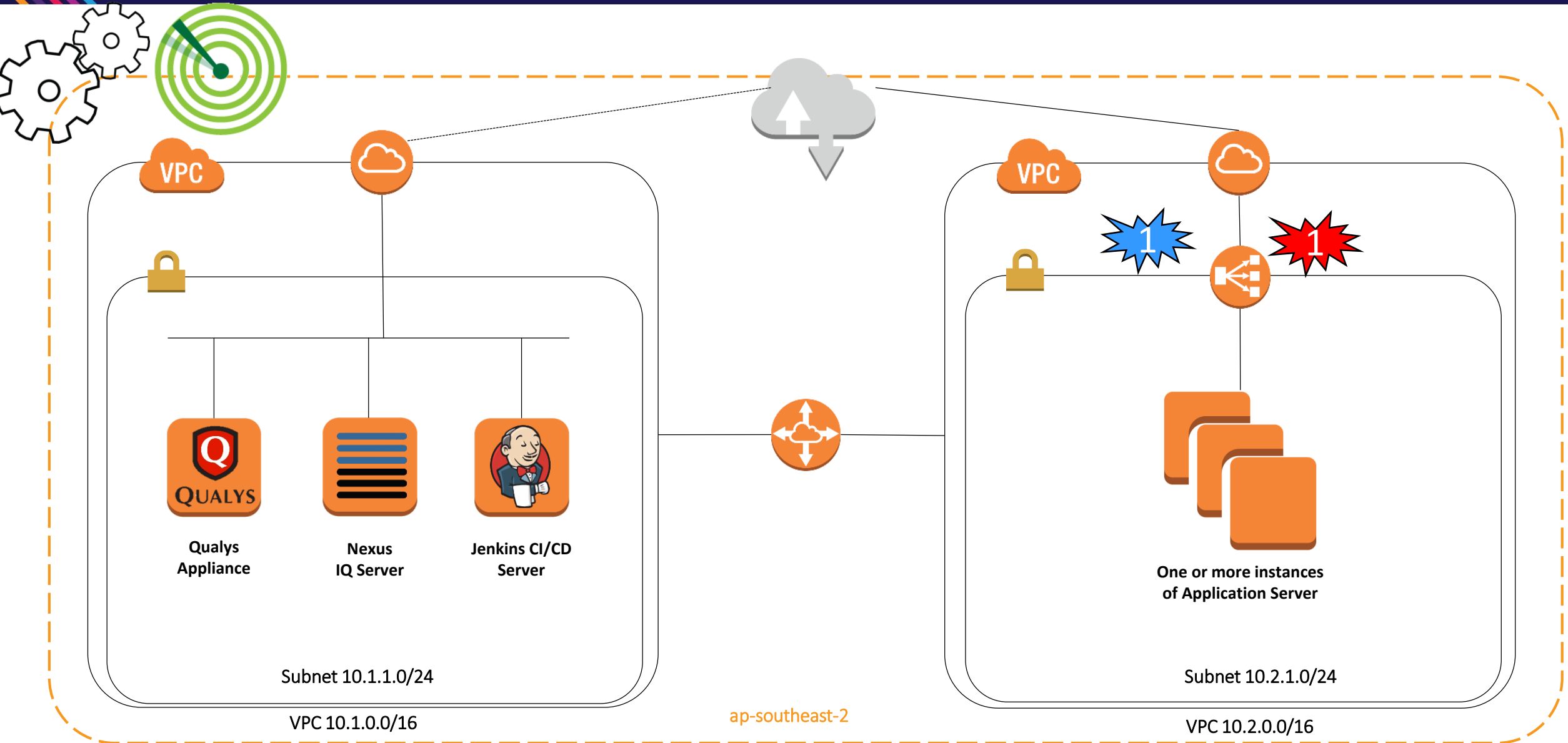


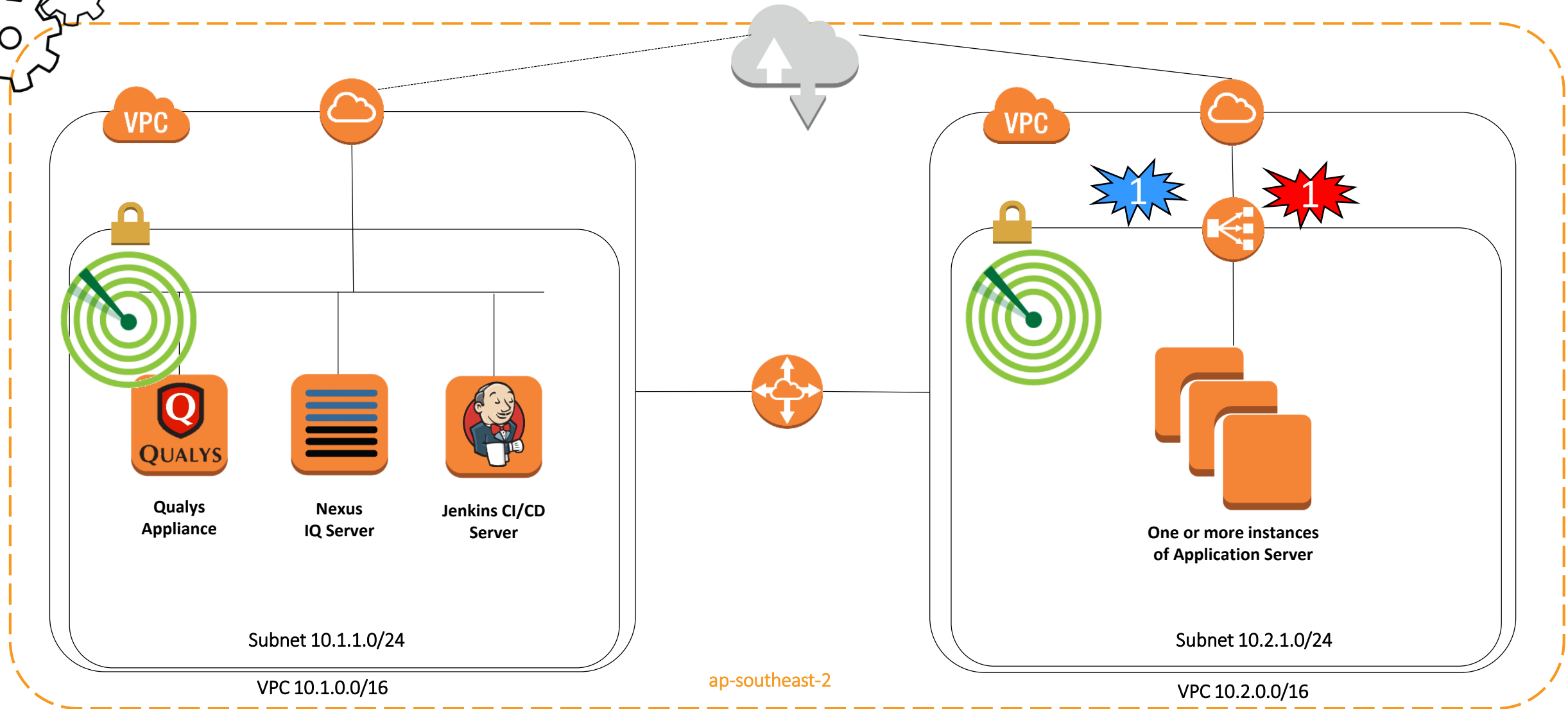
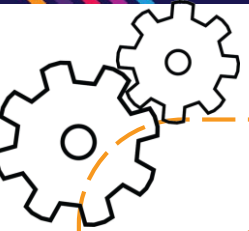
AUTOMATION

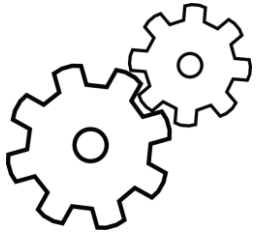


- Automation can dramatically improve security
- Make the application build success rely on the security state of the entire stack environment.
- Don't make it too complicated

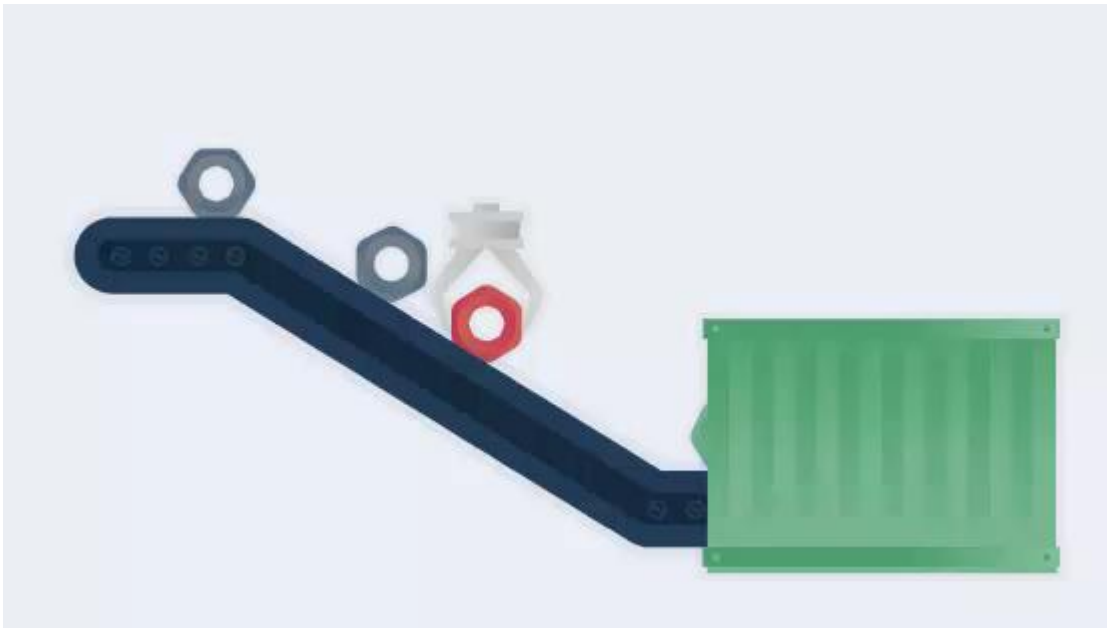




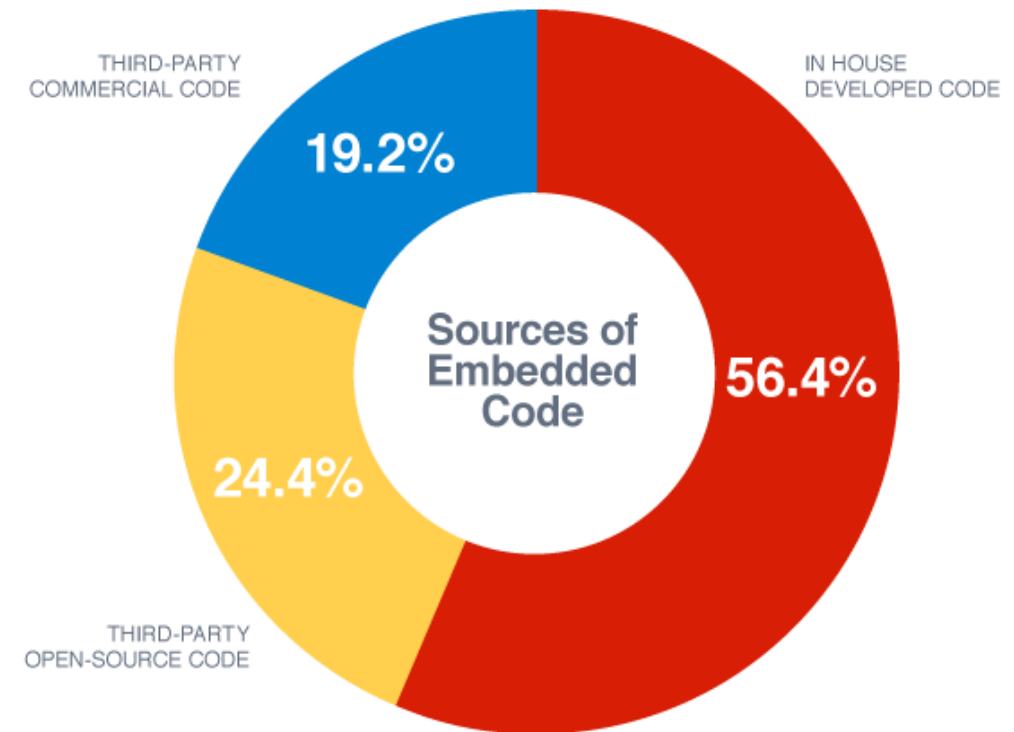




Supply Chain Security: Identify Vulnerable Third Party Components. Automatically strengthen and secure software supply chains everywhere, and at scale



Source: <https://www.sonatype.com>



Source: <https://www.grammatech.com/>

Benefits of Continuous Monitoring

Real-time, Continuous Monitoring Platform

- ✓ **Immediate discovery of assets** including mobile, cloud, and virtual systems
- ✓ **Continuous, real-time** vulnerability assessment
- ✓ **Integrated threat detection** and advanced malware analysis, isolation of attack paths
- ✓ **Real-time network monitoring** and anomaly detection
- ✓ **Integrated logging, forensics,** and threat investigation & response
- ✓ **Proactive compliance reporting** and patch auditing

Continuous Monitoring



Malware Detection



Network Behavioral Analysis



Vulnerability Management



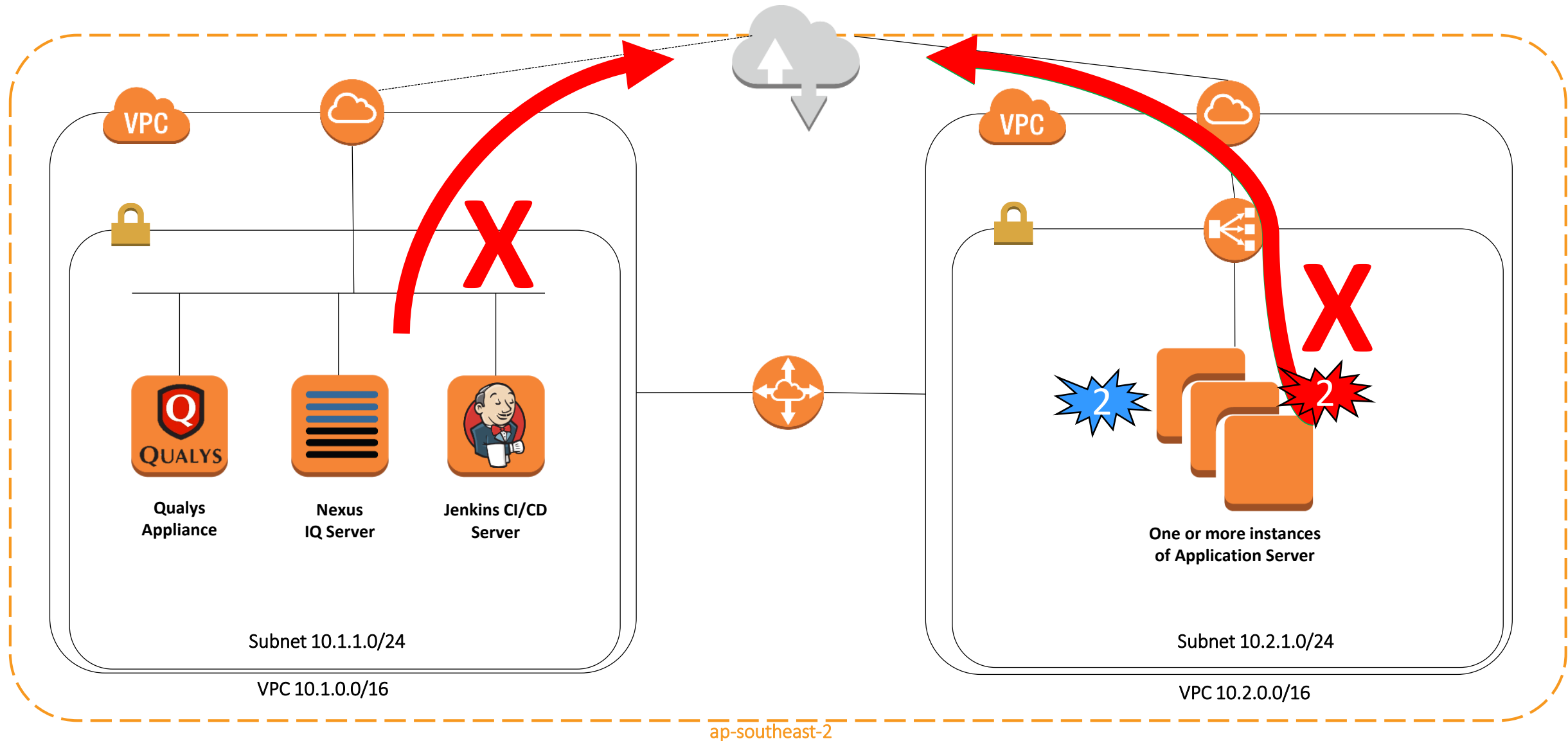
Compliance & Patch Monitoring



Log Collection & Analysis



<https://www.slideshare.net/FrostandSullivan/cutting-edge-approaches-to-vulnerability-management>



<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html#vpc-security-groups>

Security Group Rules

The rules of a security group control the inbound traffic that's allowed to reach the instances that are associated with the security group and the outbound traffic that's allowed to leave them.

The following are the characteristics of security group rules:

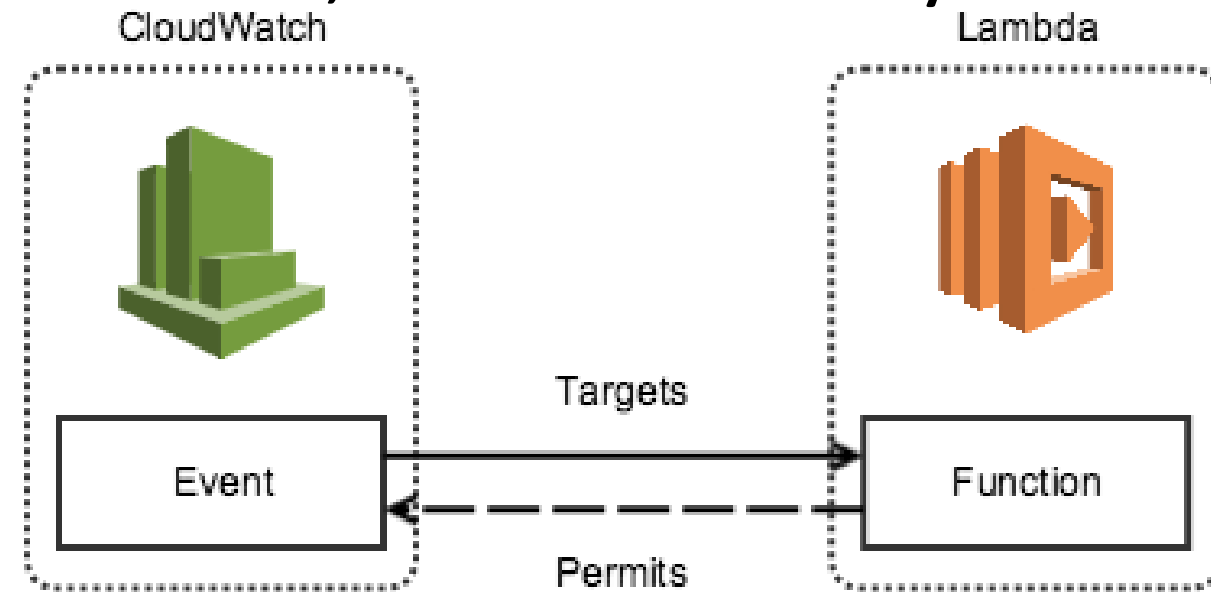
- By default, security groups allow all outbound traffic.



Self Healing

- Lambda Trigger on CloudWatch Event, Re-Set Security Group Rule.

1. Setup your CloudWatch event
2. Setup your Lambda function
3. Give the alert permissions to Lambda
4. Make the rule target the function



- Commercial Tools – e.g. Dome9, TamperProofing Security Groups.

<https://dome9.com/wp-content/uploads/2015/08/Dome9-Securing-AWS-Network-Best-Practices-Webinar-Mar-2015.pdf>

Run Time Defence - WAF

Capability	Requirements
WAF's "could" mitigate this attack through Whitelisting *	If the rules are set to whitelist valid content types or blacklist Object Graph Navigation Library (OGNL) expressions.
WAF's "could" mitigate this attack through Custom Rules **	Custom rule reqd to block requests that contain invalid Content-Type header values for a specific URL that accepts multipart requests conditions: request.path EQUAL "/struts2-showcase/index.action" request.header "Content-Type" NOT.EQUAL "multipart/form-data"
More Advanced WAFs "could" mitigate this attack through Zero Day Protections ***	Payload analysis on form submissions & API calls.

Run Time Defence - WAF

Capability	Requirements
More Advanced Application Firewalling – RASP ****	<ul style="list-style-type: none">• Runtime application self-protection (RASP)<ul style="list-style-type: none">• Built into an application• Detect and prevent real-time application attacks.• “self-protecting” or reconfiguring automatically without human intervention (on conditions of threats, faults, etc.).

* <https://blog.blackducksoftware.com/cve-2017-5638-anatomy-apache-struts-vulnerability>

** <https://blog.qualys.com/technology/2017/03/09/qualys-waf-2-0-protects-against-critical-apache-struts2-vulnerability-cve-2017-5638>

*** <https://www.imperva.com/blog/2017/09/apache-struts-rce-and-managing-app-risk/>

**** <https://www.veracode.com/security/runtime-application-self-protection-rasp> , <https://www.waratek.com/runtime-application-self-protection-rasp/>

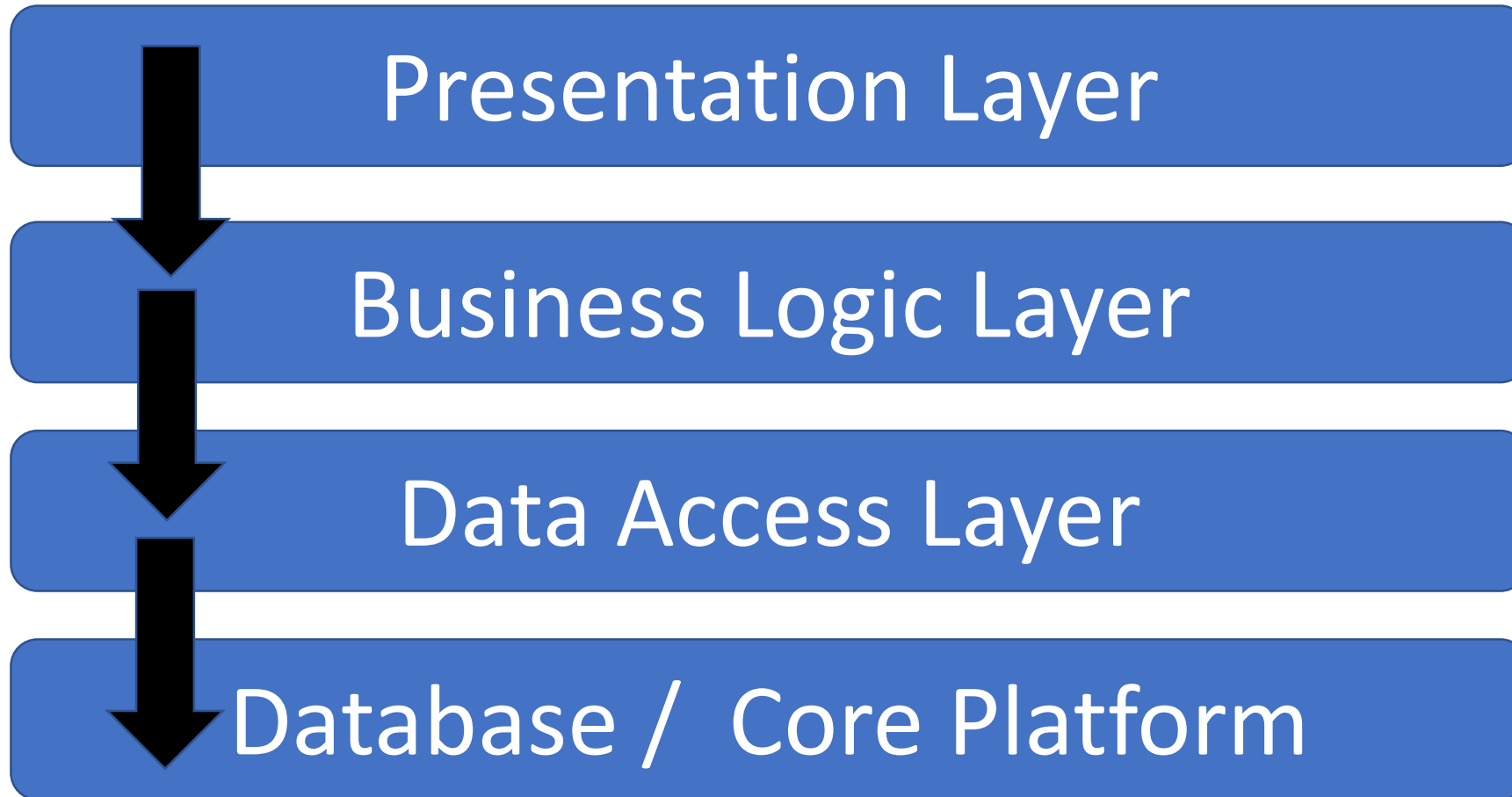
When attackers hack web apps/servers, they want to:

- Get access to sensitive data
- Remain persistent
- Access additional internal resources –
Horizontal Attack



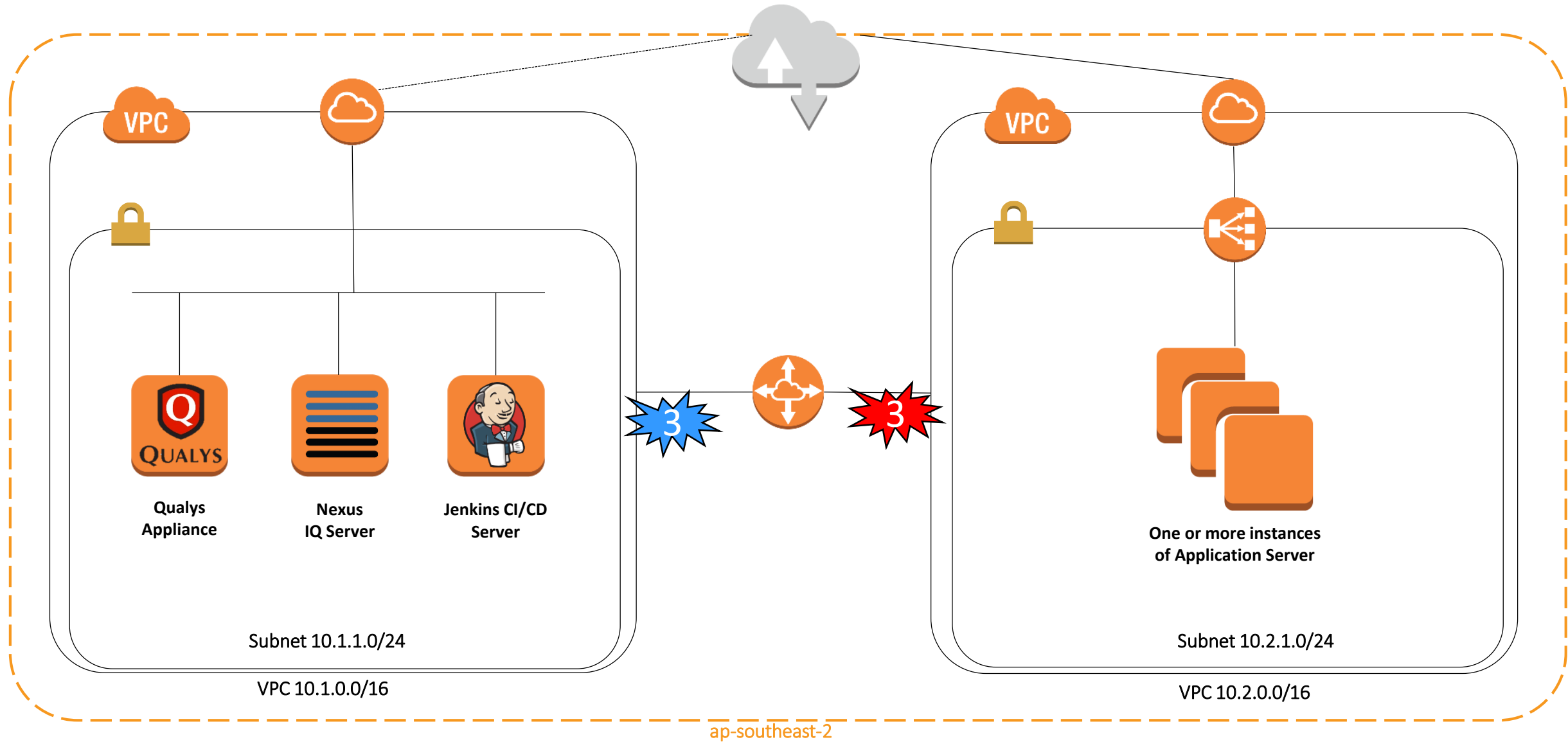
Pre Run Time Defence – Containers

Container Attribute	Defence in Depth
TTL - Containers Don't Live as Long as servers	Affects Persistence of Attack
Isolated from the underlying machine, and from other containers	Increasing difficulty for lateral movement and Pivot Attack
Fewer privileges than regular processes	Escape from a container usually involves kernel exploitation (difficult).
Container images can be scanned (before deployment) for known vulns.	Quality at Source. <i>Prevent</i> images with a vulnerability from being deployed.
Supports microservice architecture	Patch, update, redeploy



Run Time Defence – Container Firewalls

Attribute	Defence in Depth
Attack Window	<ul style="list-style-type: none"> • before a vulnerability is published, • before a patched is available • before you can implement a corrective action.
Additional Controls <ul style="list-style-type: none"> • Container Firewall 	<ul style="list-style-type: none"> • application segmentation • whitelist of allowed container connections • policy for internal applications (web servers), prevent connections to external networks • prohibit direct connections to database/core



<http://docs.aws.amazon.com/AmazonVPC/latest/PeeringGuide/vpc-peering-basics.html>

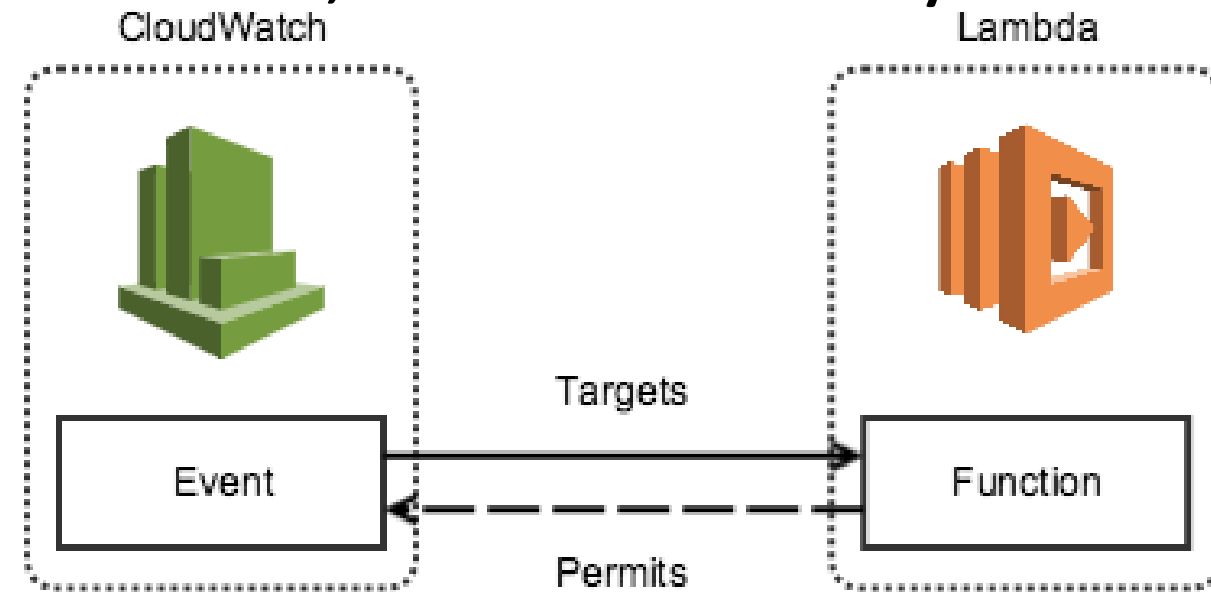
4. If required, update the security group rules that are associated with your instance to ensure that traffic to and from the peer VPC is not restricted. You can reference a security group from the peer VPC as a source or destination for ingress or egress rules in your security group rules.



Self Healing

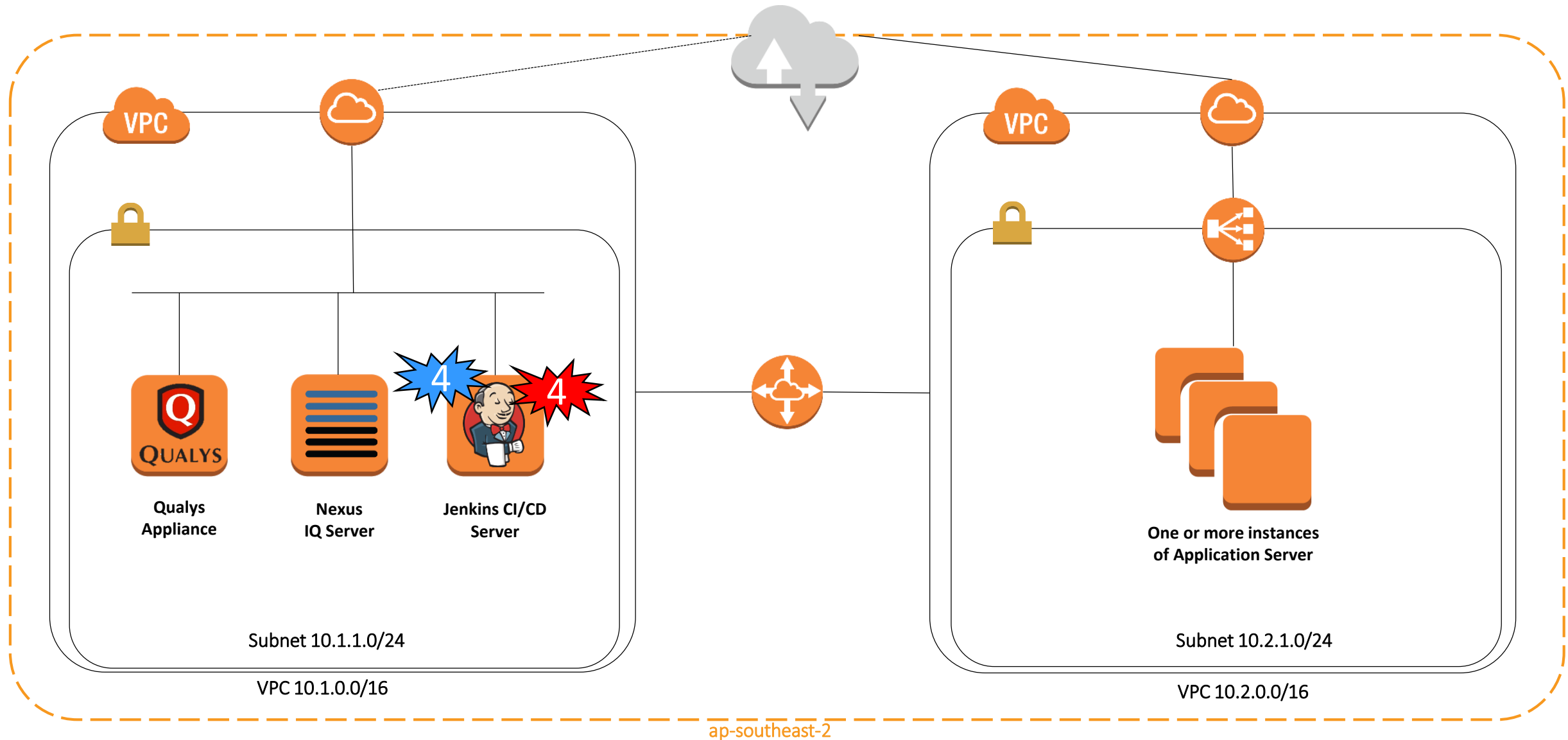
- Lambda Trigger on CloudWatch Event, Re-Set Security Group Rule.

1. Setup your CloudWatch event
2. Setup your Lambda function
3. Give the alert permissions to Lambda
4. Make the rule target the function



- Commercial Tools – e.g. Dome9, TamperProofing Security Groups.

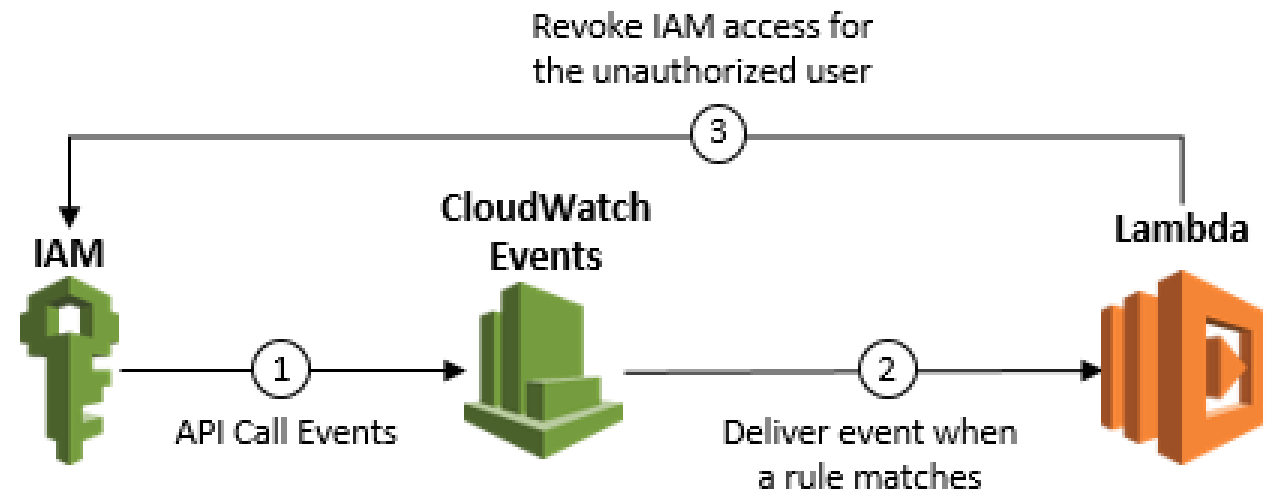
<https://dome9.com/wp-content/uploads/2015/08/Dome9-Securing-AWS-Network-Best-Practices-Webinar-Mar-2015.pdf>



Self Healing

- Lambda Trigger on CloudWatch Event, Revoke IAM Privileges.

1. Setup your CloudWatch event
2. Setup your Lambda function
3. Give the alert permissions to Lambda
4. Make the rule target the function



<https://aws.amazon.com/blogs/security/how-to-detect-and-automatically-revoke-unintended-iam-access-with-amazon-cloudwatch-events/>

- Commercial Tools – e.g. Dome9, TamperProofing IAM.

https://go.dome9.com/Whitepaper_RichardStiennon.html

Improved DevOps Architecture Principles

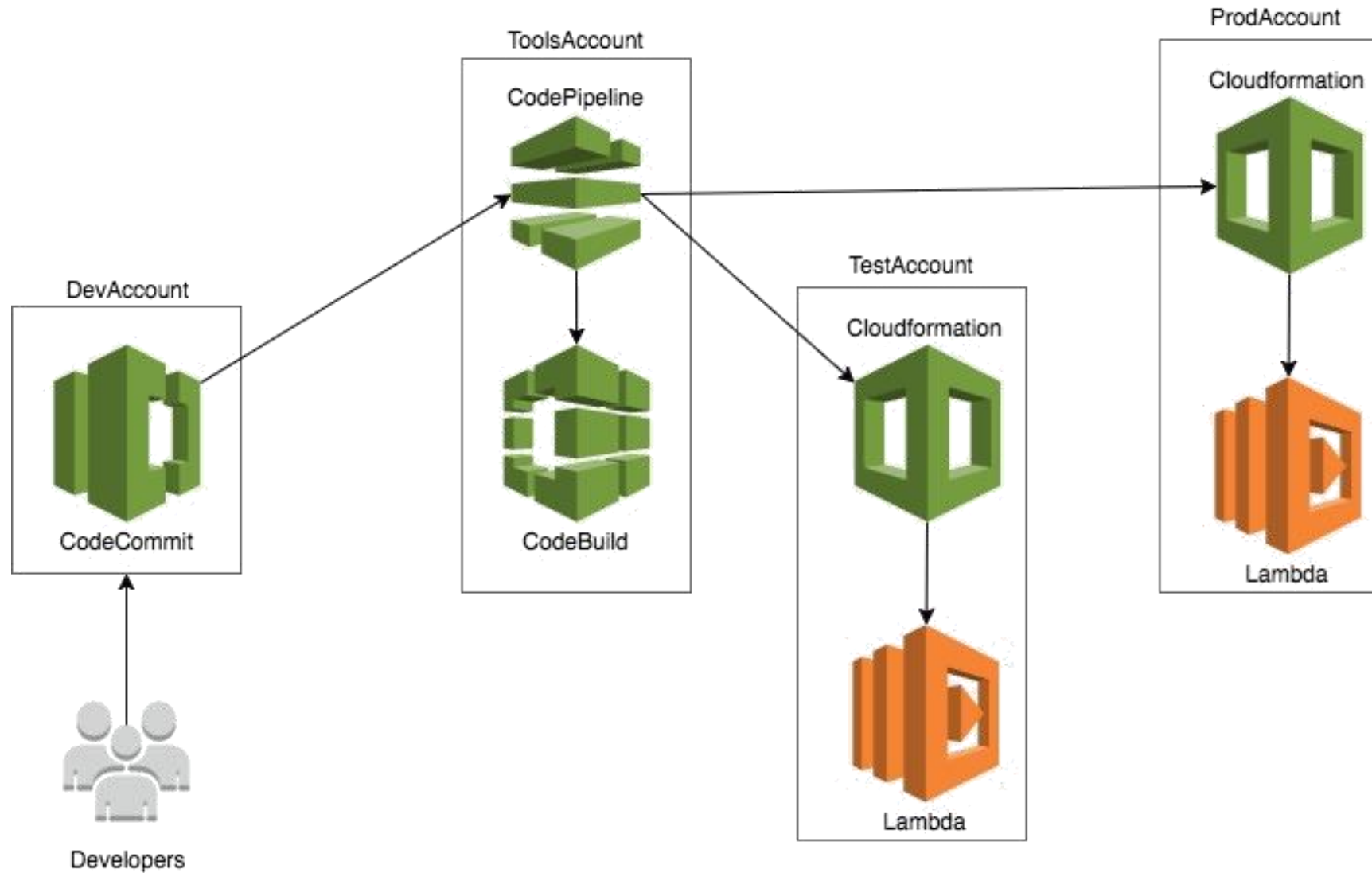
Isolation for Development,

Testing,

Deployment etc

Use Multiple Accounts

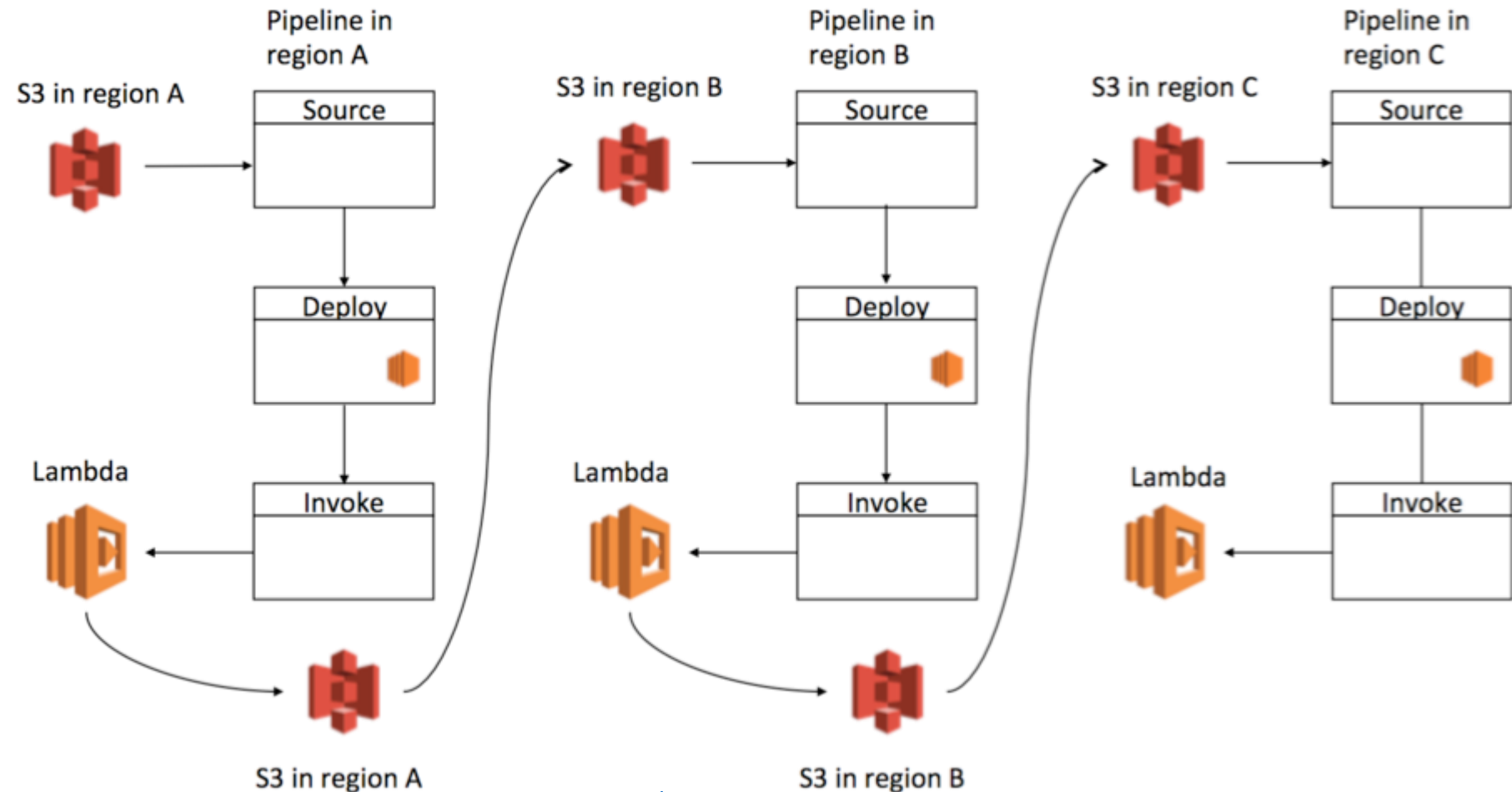
Account	RBAC
DevAccount	<ul style="list-style-type: none"> • Developers check the code into repo. • Store all the repositories as a single source of truth for application code. • Developers have full control over this account. • Used as a sandbox for developers.
ToolsAccount	<ul style="list-style-type: none"> • Central location for all the tools related to the org, incl CI/CD services. • Developers have limited/read -only access in this account. • Operations team has more control.
TestAccount	<ul style="list-style-type: none"> • Applications using the CI/CD orchestration for test purposes deployed from this account. • Developers & Ops team have limited/read only access in this account.
ProdAccount	<ul style="list-style-type: none"> • Applications using the CI/CD orchestration tested in the ToolsAccount deployed to production from this account. • Developers & Ops team have limited/read only access in this account.



<https://aws.amazon.com/blogs/devops/aws-building-a-secure-cross-account-continuous-delivery-pipeline/>

https://d0.awsstatic.com/aws-answers/AWS_Multi_Account_Security_Strategy.pdf

A successful processing of source code in all of its AWS CodePipeline stages will invoke a Lambda function as a custom action, which will copy the source code into an S3 bucket in Region B. After the source code is copied into this bucket, it will trigger a similar chain of processes into the different AWS CodePipeline stages in Region B. See the following diagram.



<https://aws.amazon.com/blogs/devops/building-a-cross-regioncross-account-code-deployment-solution-on-aws/>

Conclusions

- Cloud introduces some (new) challenges
- Common Sense & Reasonable Security Measures Prevail!
- Active Defence and Self-Healing is possible
- Continuous Monitoring can be achieved thru automation
- Common attacks can be defeated with Low/No Cost!
- Crawl, Walk, Run
- Start with the basics, improve configurable settings
- Strive towards more advanced DevOps Deployments with integrated security

Sense of Security

www.senseofsecurity.com.au

+61 2 9290 4444

info@senseofsecurity.com.au