NSC42

CSA UK cloud security alliance SM
UNITED KINGDOM Chapter

Cloud Transformation Challenges

Chartered Institute of Information Security

ISP North Chapter

About The founder

Francesco Cipollone

Founder – NSC42 LTD

I'm a CISO and a CISO Advisor, Cybersecurity Cloud Expert. Speaker, Researcher and Chair of Cloud security Alliance UK, Researcher and associate to ISC2.

I've been helping organizations define and implement cybersecurity strategies and protect their organizations against cybersecurity attacks

@FrankSec42 Fracipo Linkein Email Website Articles NSC42 LinkedIn

Cloud is just someone else computer

Security is everyone else job and needs to be aligned to business needs

Our Agenda

About the author and company

Setting the context

The Challenges

- Regulation
- Shared Responsibilities
- Identities and Access controls
- Patterns
- Processes review

Caveat/Pitfalls

Take Away

Q&A

Cloud Evolution

2005 Datacentre Land

2006

2007

2008

2010

2011

2012

2013

2014 Cloud Adoption

amazon.com web services
Google app engi
vmware
rackspace HOSTING
Microsoft Azure
IBM Cloud
IBMSmartCloud
Google Compute Engine

Major Breaches

Why security is everybody’s responsibility?

Because we all get affected by it…

2009/ 2010
Heartland
US Military
Aol
TJMax

2012
Sony PSN
NHS
Betfair
Steam

2012
Dropbox
Lastfm
Blizzard

2013
Yahoo(orignal)
US Retailers
Adobe
UbiSoft
Court Ventures

2014
JP Morgan
Home Depo
Ebay

2015
Deep Root
IRS
Anthem

2016
Linkedin
Friend Finder
Dailymotion
Mossack Fonseca

2017
Myspace
Twitter
Yahoo

2018
Marriot
Twitter
MyHeritage
Uber
Quora..

2019
…

Cloud Security Breaches

Capital One (2019)

Misconfiguration of WAF (web application Firewalls)

Accenture (2017)

4 S3 buckets available over the web

Verizon (2018)

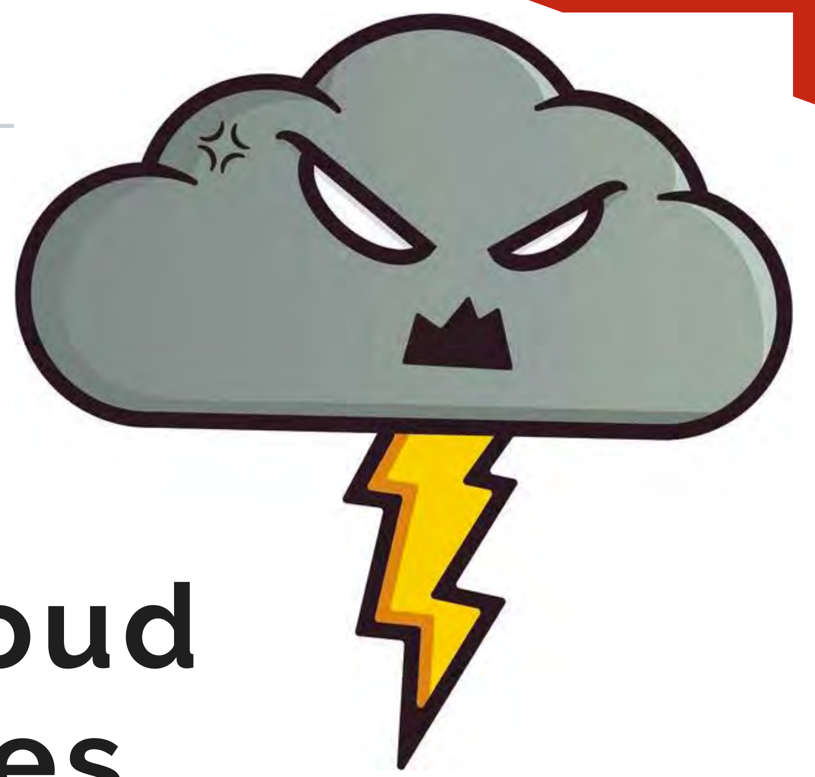
3rd party vendor committed config on a public S3 bucket

Exactos (2018)

Open Elasticsearch Database

IMPERVA

Web application firewall was compromised



Most Recent Cloud Security Breaches

The common theme around all those breaches are

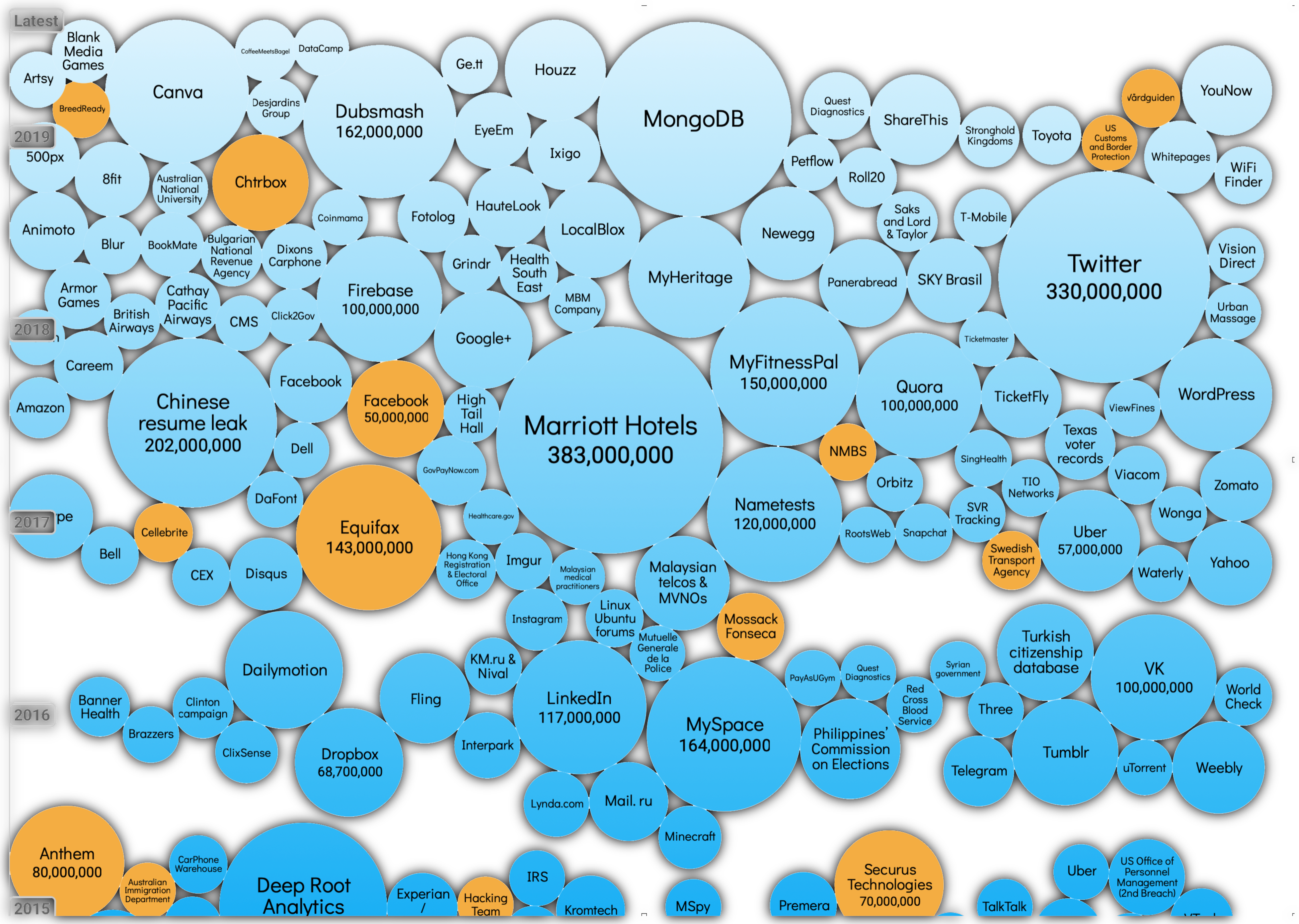
1. **Misconfiguration**
2. **Public Storage**
3. **Easy to guess credentials No MFA on critical accounts**
4. **No segmentations/Blast radius reduction**

Why security?

Data breaches exposed 4.1 billion records in the first half of 2019.

Data breaches are the new norm. They threaten the viability of every business as they’re now larger in number and impact.

it takes only one misconfiguration to get a you in front of the newspaper



Source: www.informationisbeautiful.net

Why Cloud and Why Security

Total cost of cloud breaches

5 trillion $ / 4 trillion GBP

Adversaries don't need many misconfiguration ONE is all it takes.

Is your business equipped with the right tool and trusted partner to address it?

Every min

62K record disclosed

Record per minute disclosed

N. Of Vuln records

33 billion

Disclosed records over 1 year

Data breaches

80% due to misconfiguration

Cloud misconfiguration is dominat

Av. Cost per record

150$ per record

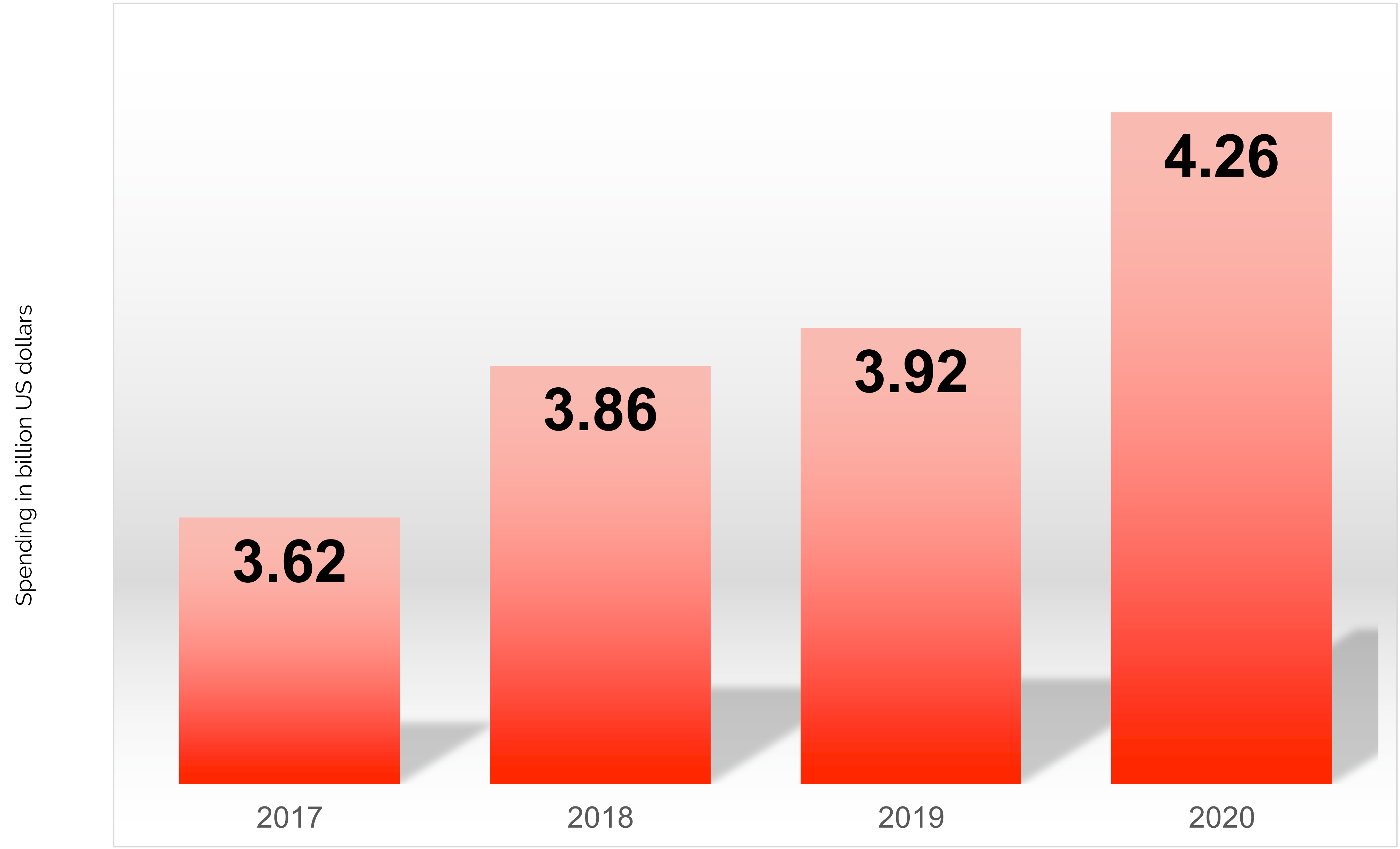
Average cost per loss record

The Cybersecurity Sector in Numbers

Av Cost of data Breach
3.03 m

The number of data breaches reported since 2017 to regulators has increased 480%.

71% of breaches in 2019 were financially motivated



Source Gartner Report 2018

AVERAGE COST OF DATA BREACH IN MILLION OF DOLLARS

Company	Net Loss ($US)	Settlement/ Regulatory Fine	No. of Customer Affected
eBay	2.33 billion, $1.82/share	$650million	147million
Equifax	$555.9 million	$700million	147million
Capital One	$150million	TBD	106million
Travelex	£4.6m ransom + 30 days inactivity	TBD	
Average	the average total cost of a breach now stands at £3.03m		

Top Cyber Security Risks – CSA Report

1. Data Breaches

Credential Loss & detection

e.g. Sony

2. Misconfiguration & Change Control

Assets Configured incorrectly e.g. S3 Bucket Open

3. Lack of Cloud Security Arch

Contextual View could leave door open e.g. Use of public Storage for private data

4. Broken Access Control

Understanding IAM Roles.

Keys not in Code

5. Account Hijack

Access to Cloud master account

6. Insider Threat

Rogue Admin,

Rogue Collaborators inside

Bribable individuals

7. Insecure API

CSA Api secure,

Key to access the API must be secured

8. Weak Control Plane

Multi Cloud

Control for data migration (CI/CD)

9. CSP API Usage

Immature CSP don't provide mechanism to access services via API

10. Poor Cloud Usage Visibility

Lack of monitoring means inability of detection of misuse

11. Abuse of Cloud Services

Increase of usage

Usage in unmonitored regions

Top Threats to Cloud Computing

The Egregious 11

Regulation

Understand Regulation and how will it impact the transformation:

- Out of date regulation
- Roles and responsibilities
- Adapt the mandated control to the cloud
- Refer to existing patterns/control set (e.g. CSA CCM…)
- Refer to cloud based regulation (ISO27017/18, CSA CCM…)

GDPR

DPA

HIPPA

FIPS/NIST

FIPS/NIST

GLBA

SOX

Common Challenges

Setting the context and challenges:

- Skills shortages/Upskilling
- Security as part of the cloud journey/Foundation
- Assessment and continuous compliance

- Bringing Management on the journey
- Disruption and strategy
- Architecture patterns:
  - don’t reinvent the wheel
  - don’t take on-premises into the cloud

…Considerations

In a cloud transformation, consider the following key elements:

- Shared responsibility model
- Regulation incompatibility
- Identities and Access management
- New work methodologies (DevOPS and Microservices)
- Exposure on something new
- Continuous compliance and new tools

Fix the problem with technology

People – Process – Technology is the mantra of cybersecurity
Why starting from the latter?

Solutions

1. **Cloud Responsibility Matrix**
Division of responsibility

2. **Cloud Foundation**
New programme of work

3. **Cloud Patterns**
Building blocks to go at pace

4. **Design Security**
Design Security components

5. **Security by Design**
Integrate security in design

6. **Dev & Shift Left**
Integration of security in DEV practices

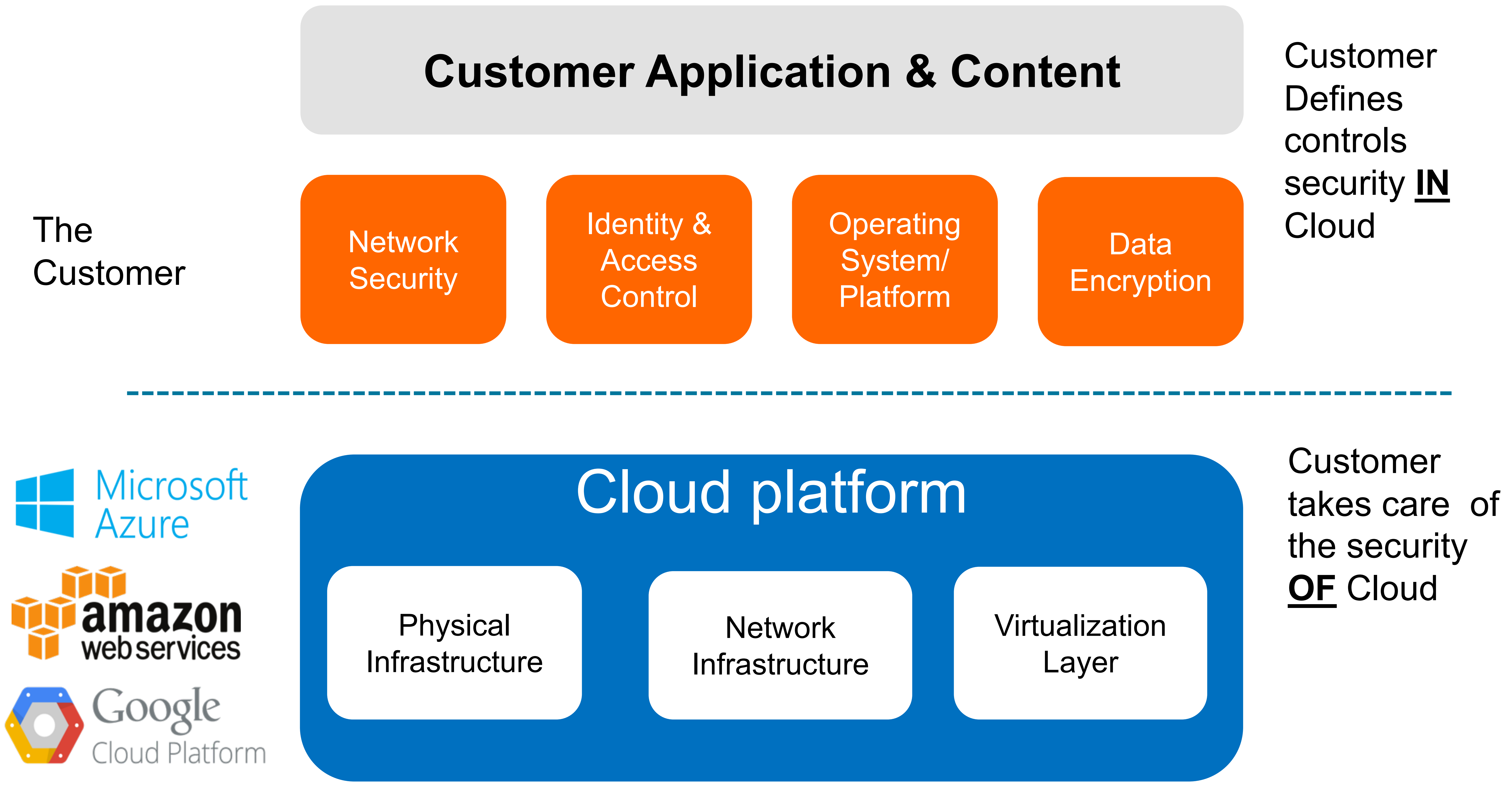
7. **Security Testing**
Continuous testing

8. **DevSECops**
Security as part of the lifecycle

Step 1 - Cloud Responsibilities

Consider what are you are getting yourself into in a cloud migration. Cloud is not natively secure or insecure

“Understand Shared Responsibility model Delegation and you’ll master cloud”



Customer Application & Content

The Customer

Network Security

Identity & Access Control

Operating System/ Platform

Data Encryption

Customer Defines controls security **IN** Cloud

Microsoft Azure

amazon web services

Google Cloud Platform

Cloud platform

Physical Infrastructure

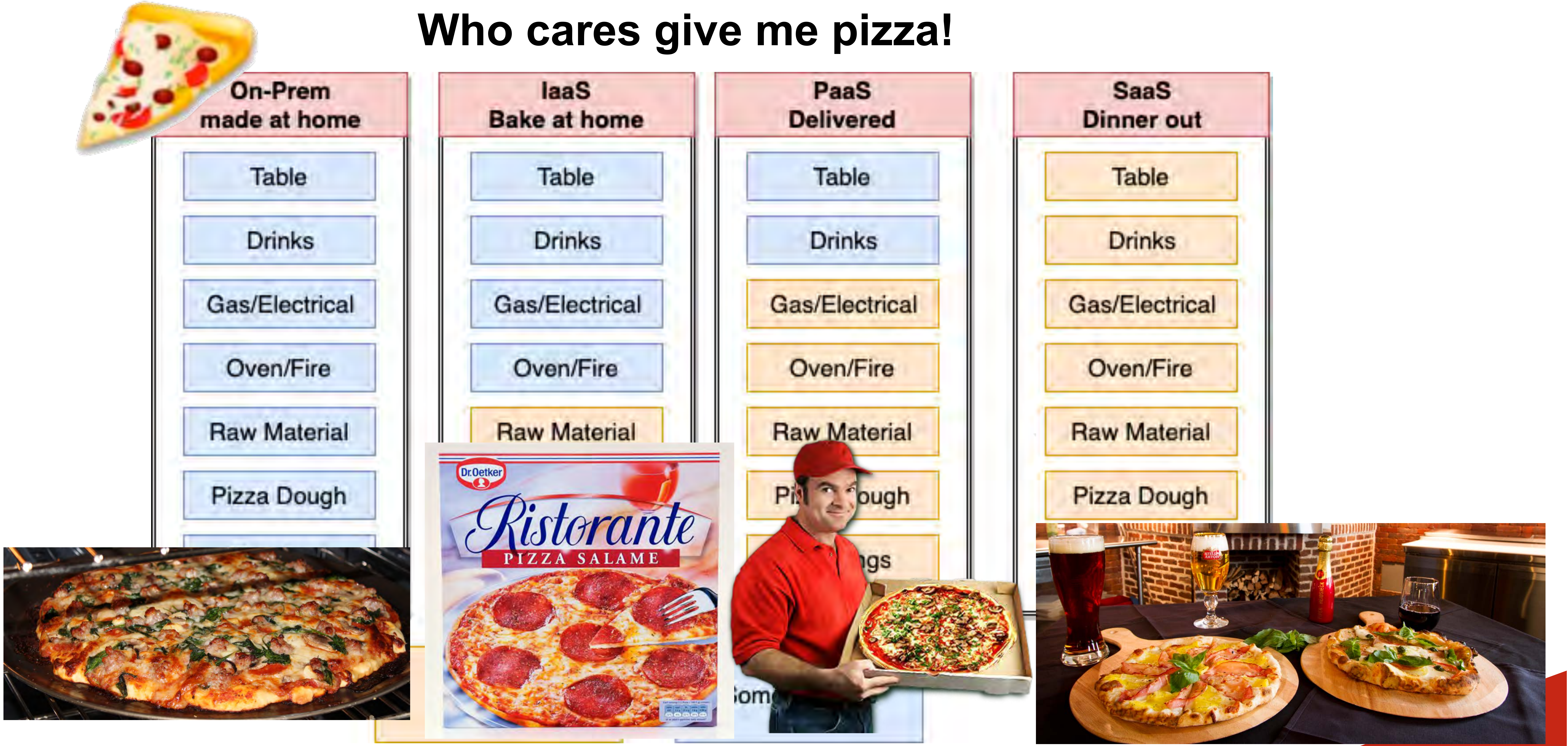
Network Infrastructure

Virtualization Layer

Customer takes care of the security **OF** Cloud

Step 1 - Cloud Pizza

IaaS, PaaS, SaaS, …
Who cares give me pizza!


Dr.Oetker
Ristorante
PIZZA SALAME

On-Prem made at home	IaaS Bake at home	PaaS Delivered	SaaS Dinner out
Table	Table	Table	Table
Drinks	Drinks	Drinks	Drinks
Gas/Electrical	Gas/Electrical	Gas/Electrical	Gas/Electrical
Oven/Fire	Oven/Fire	Oven/Fire	Oven/Fire
Raw Material	Raw Material	Raw Material	Raw Material
Pizza Dough		Pi ough	Pizza Dough
		ngs	
		om	

Step 2 – Foundation

How do you build a solid house?

You don't skip the foundation!

How do you build a solid cloud?

You don't skip the foundation!

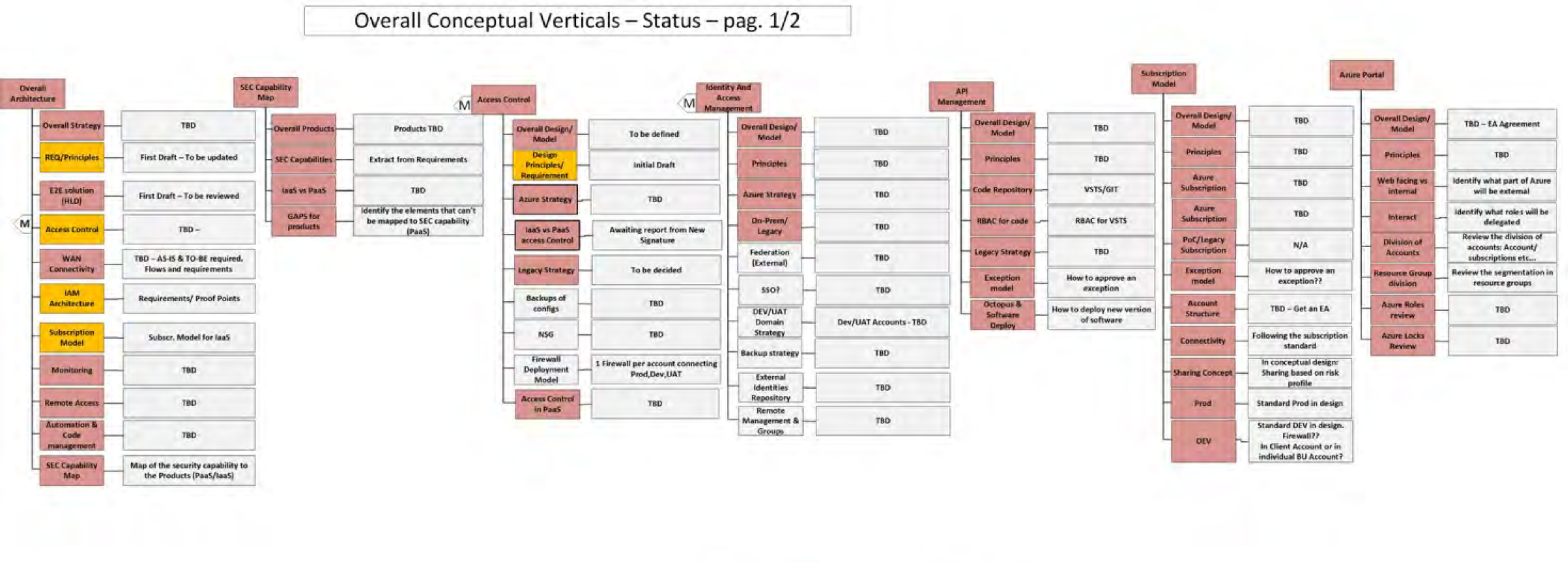
How do you build a solid cloud (security) foundation?

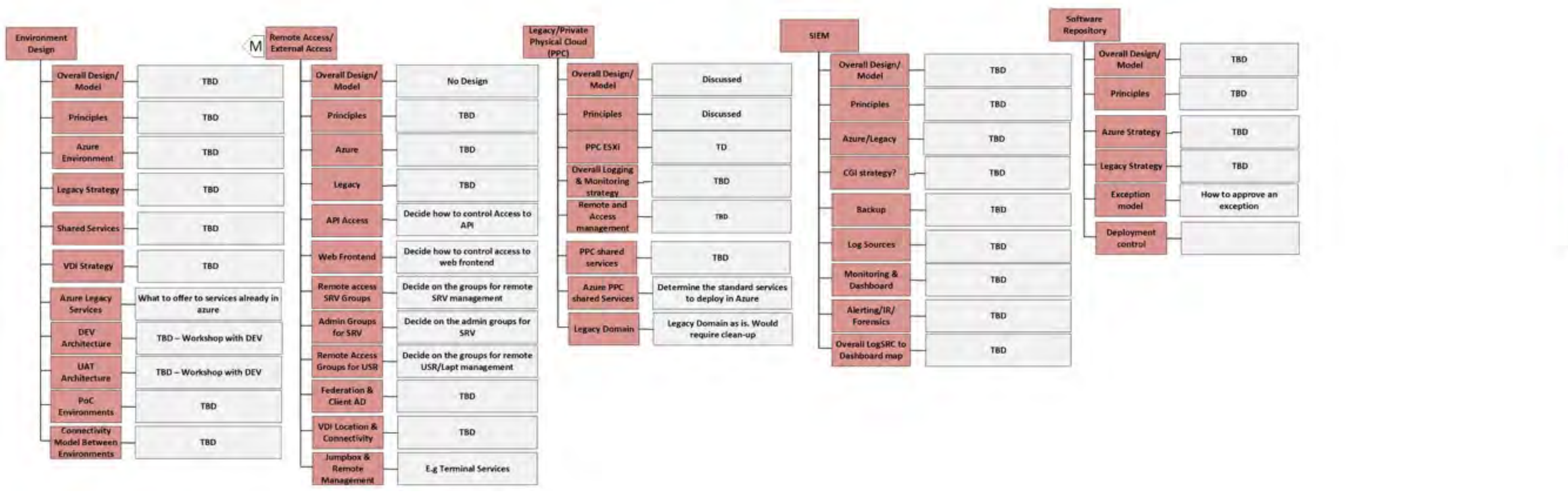
Cultural, Management support and skills

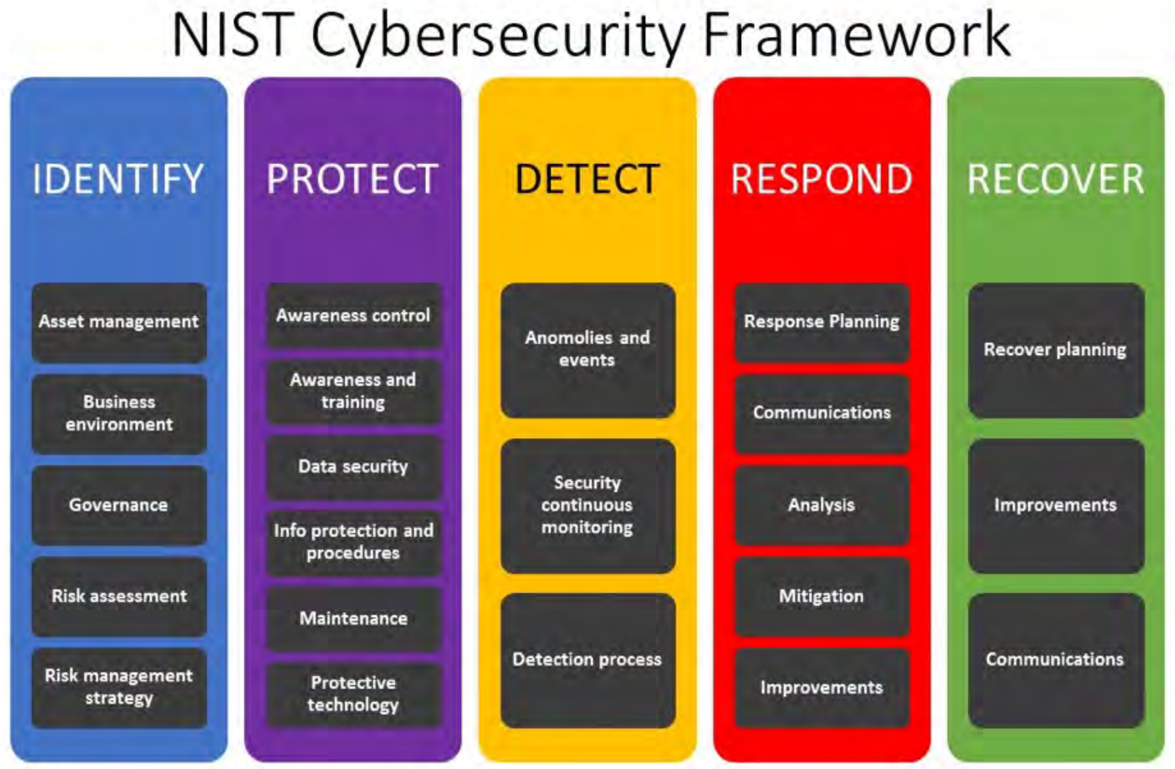
1. Management Support
2. Disruption and strategy
3. **Security as part of the cloud journey**
4. Skills shortages
5. Architecture patterns & Re-use

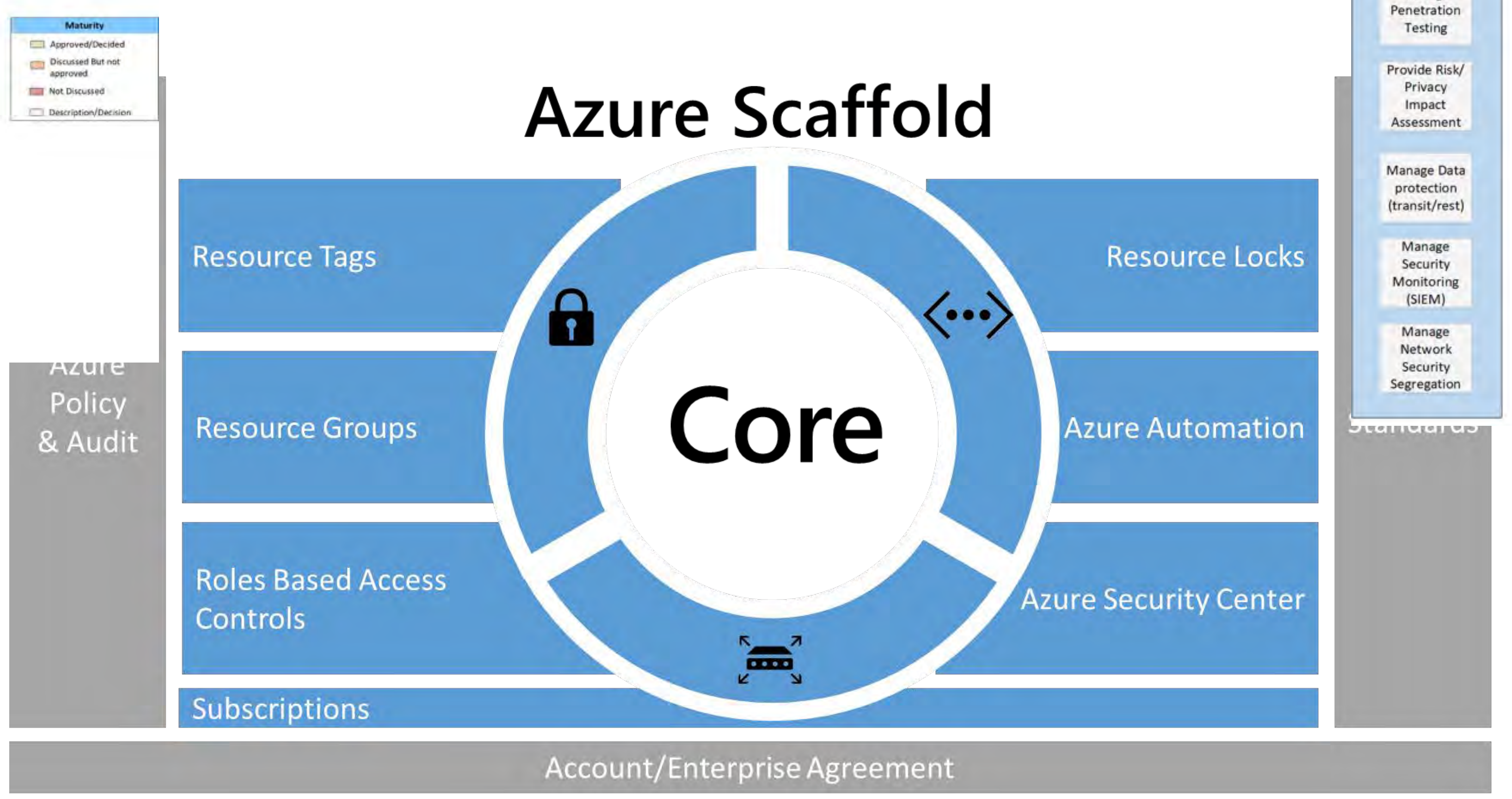
Step 2 – Foundation

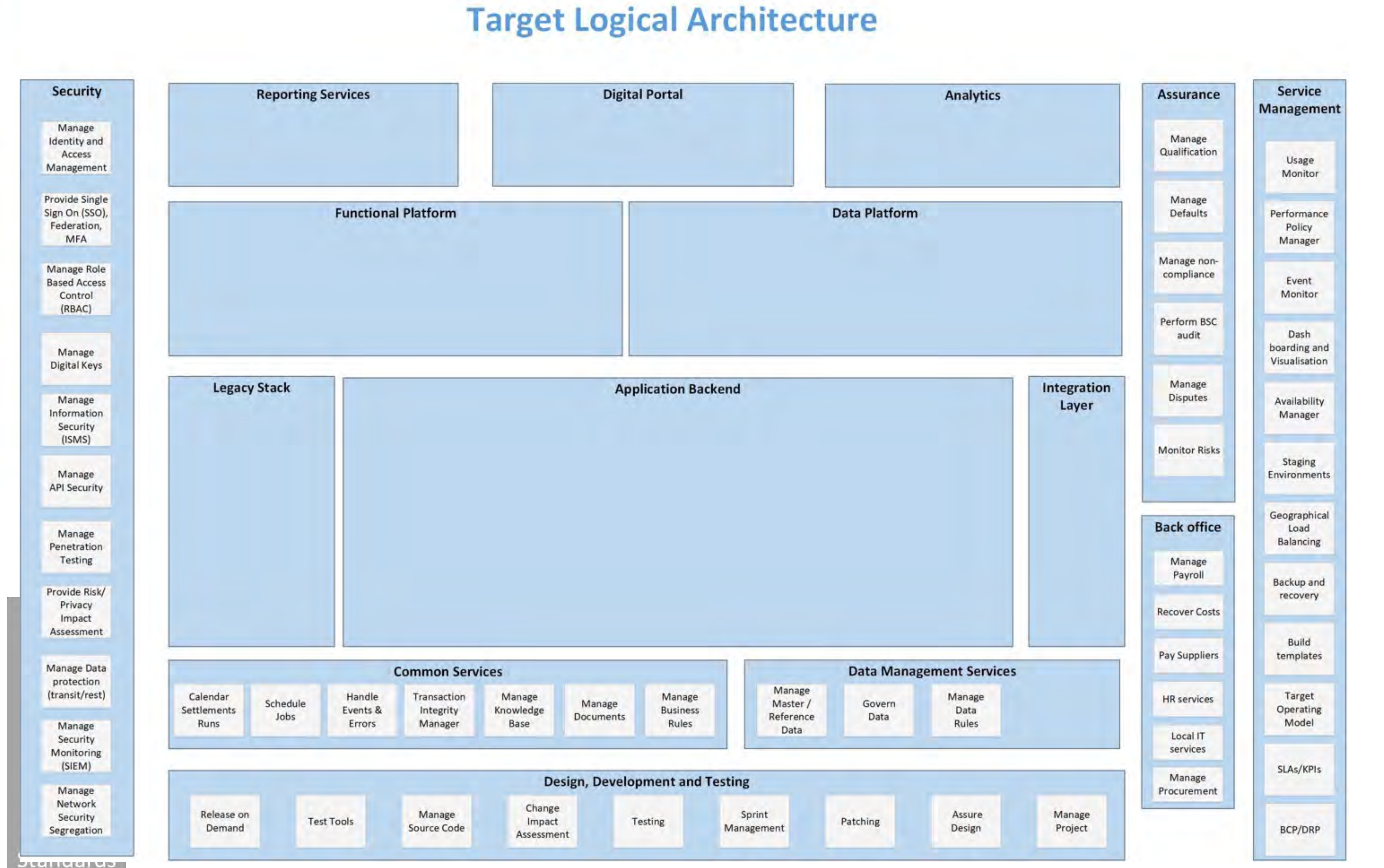
What Tools do you use for the solid cloud (Security) Foundation?


Overall Conceptual Verticals – Status – pag. 1/2




NIST Cybersecurity Framework


Azure Scaffold

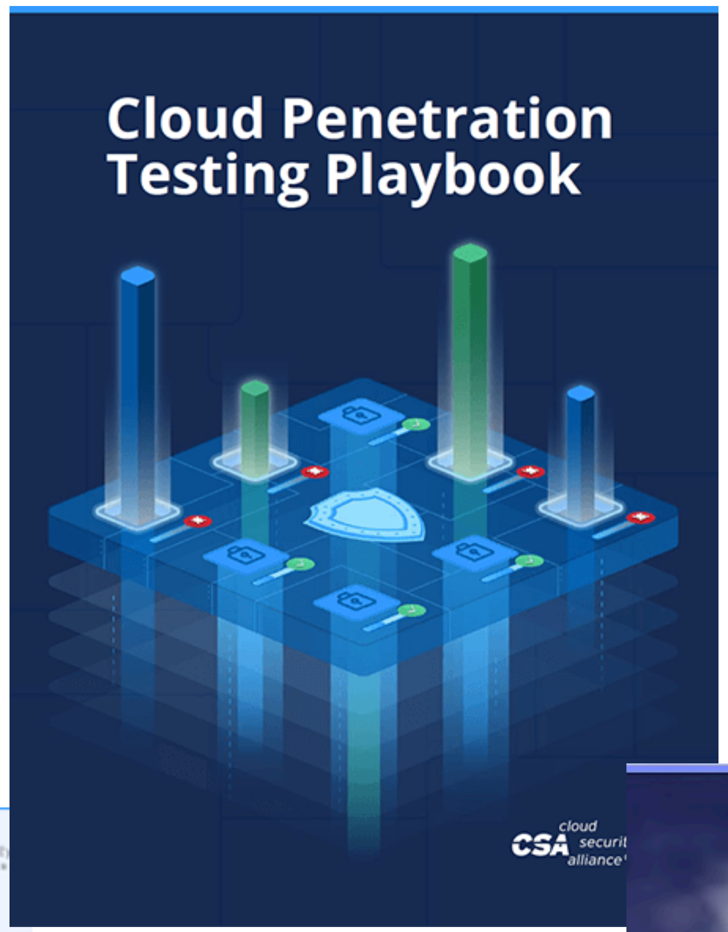

Target Logical Architecture

Step 2 – Foundation

Other Tools for foundation

The Six Pillars of DevSecOps
Achieving Reflexive Security Through Integration of Security, Development and Operations

Top Threats to Cloud Computing
The Egregious 11

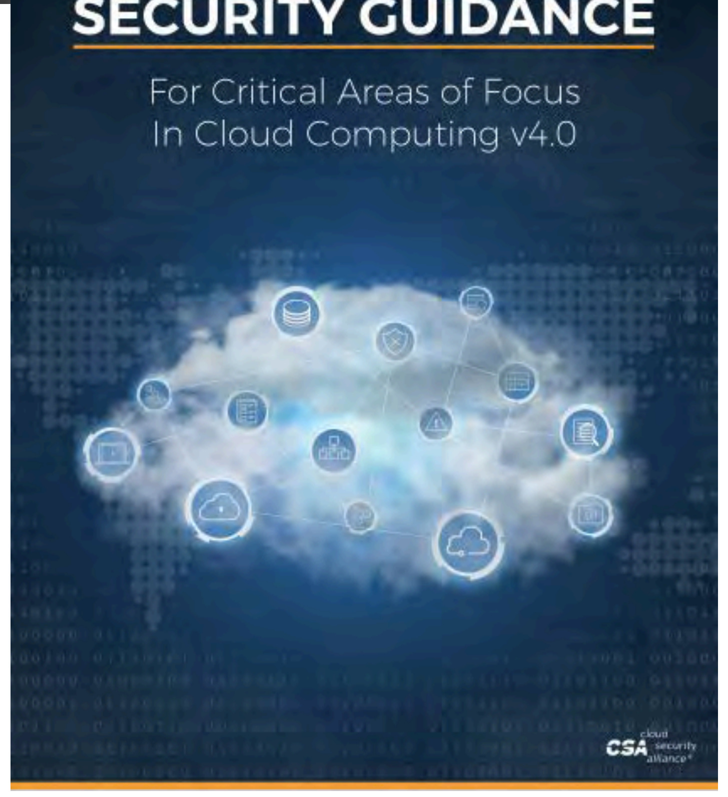

Cloud Penetration Testing Playbook

Guideline on Effectively Managing Security Service in the Cloud

Top Threats to Cloud Computing: Deep Dive
A case study analysis for 'The Treacherous 12: Top Threats to Cloud Computing' and a relative security industry breach analysis

Best Practices for Implementing a Secure Application Container Architecture
Integrating Application Container Security Considerations into the Engineering of Trustworthy Secure Systems

The 12 Most Critical Risks for Serverless Applications 2019


SECURITY GUIDANCE
For Critical Areas of Focus In Cloud Computing v4.0

https://cloudsecurityalliance.org/research/artifacts

Step 3 – Cloud Patterns

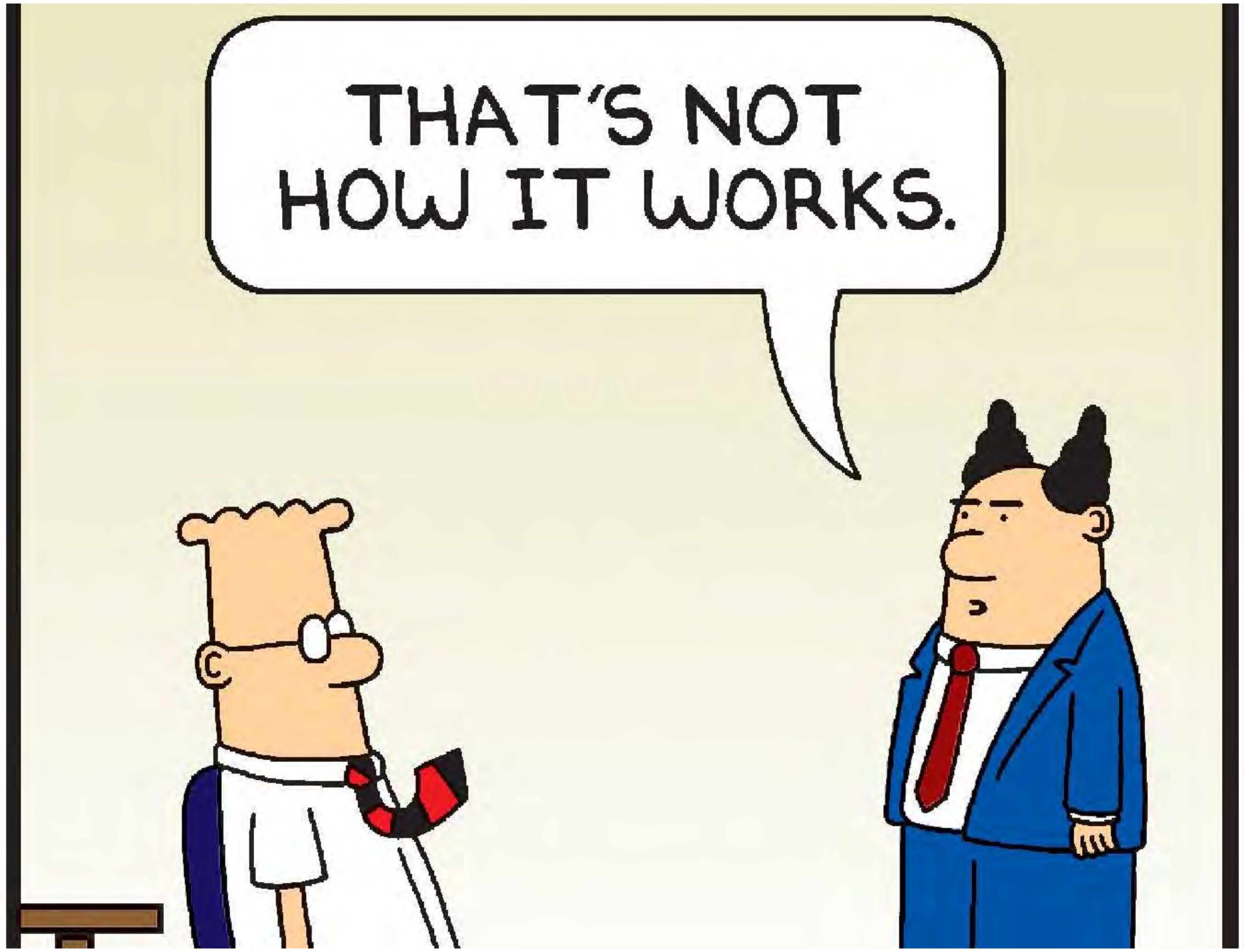
**“There is no such a thing as free lunch…
but leverage on patterns as starting point”**

- Account Isolation
- Controls Traditional vs cloud
- Logging and monitoring
- Identity and access management
- Key Management

Step 4 – Design Security

“How would expand the security team without expanding the team?”

Train Software Engineers on security and you’ll have ‘extended security team’”

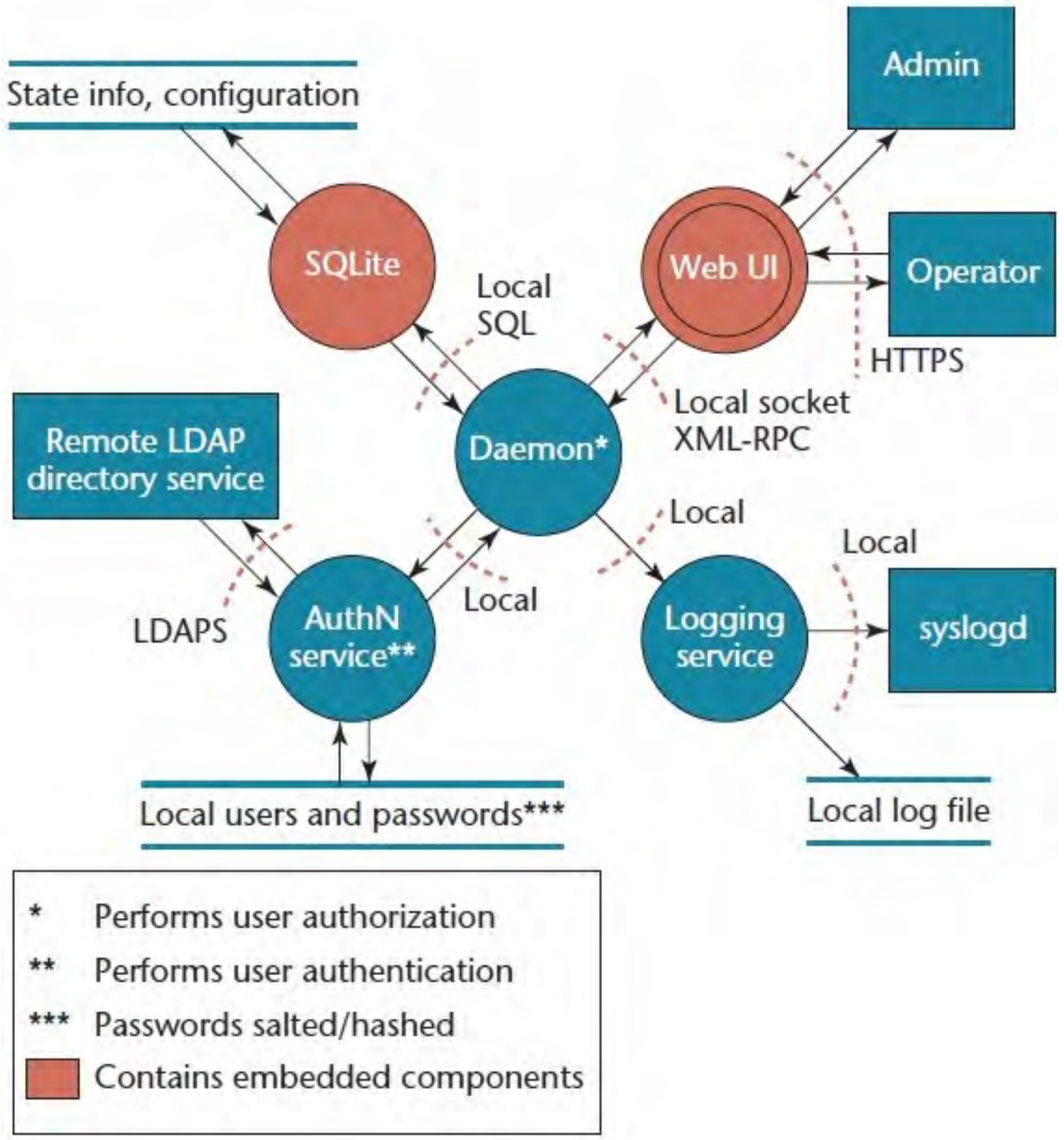


Step 5 – Security by Design

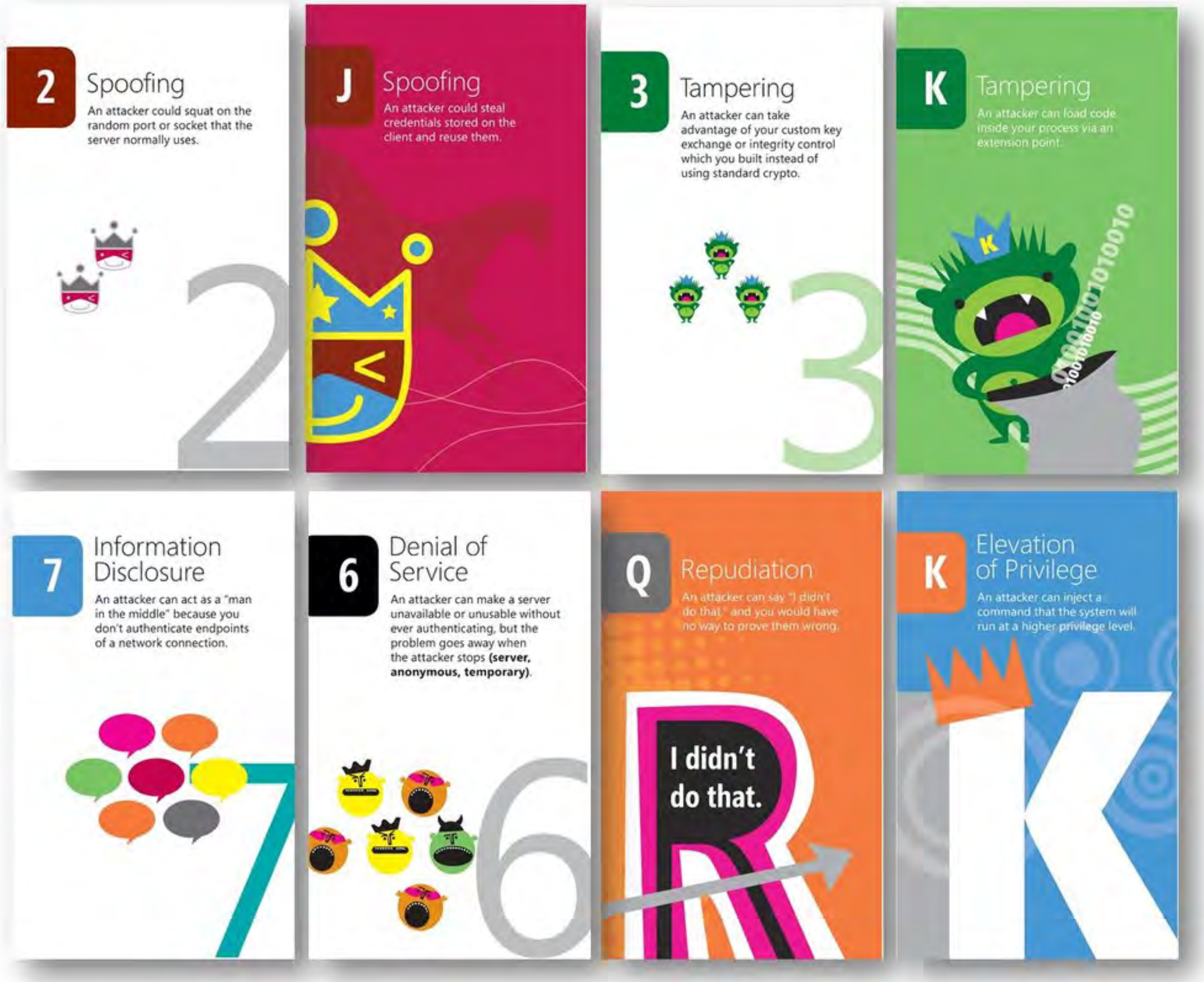
“So what would the software engineer do with the security hat on?”

How do we make threat security fun?”

“gamification…remember to have fun when doing your job”



* Performs user authorization
** Performs user authentication
*** Passwords salted/hashed
🟥 Contains embedded components



2 Spoofing
An attacker could squat on the random port or socket that the server normally uses.

J Spoofing
An attacker could steal credentials stored on the client and reuse them.

3 Tampering
An attacker can take advantage of your custom key exchange or integrity control which you built instead of using standard crypto.

K Tampering
An attacker can load code inside your process via an extension point.

7 Information Disclosure
An attacker can act as a “man in the middle” because you don’t authenticate endpoints of a network connection.

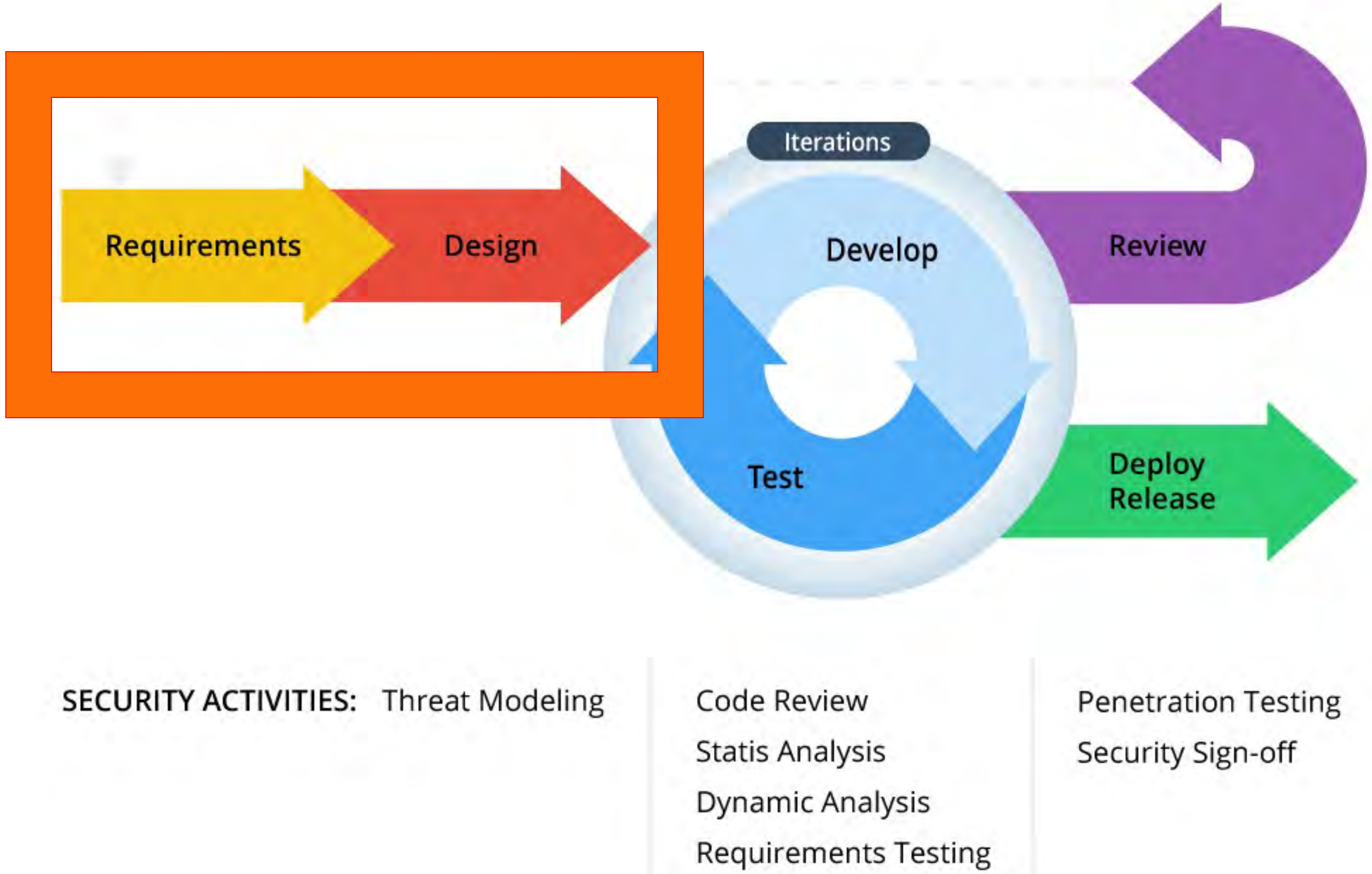
6 Denial of Service
An attacker can make a server unavailable or unusable without ever authenticating, but the problem goes away when the attacker stops **(server, anonymous, temporary)**.

Q Repudiation
An attacker can say “I didn’t do that,” and you would have no way to prove them wrong.

K Elevation of Privilege
An attacker can inject a command that the system will run at a higher privilege level.

Step 6 – Shift left in DEV

“Security as early as possible: Integrate security in the software development pipeline”



SECURITY ACTIVITIES: Threat Modeling

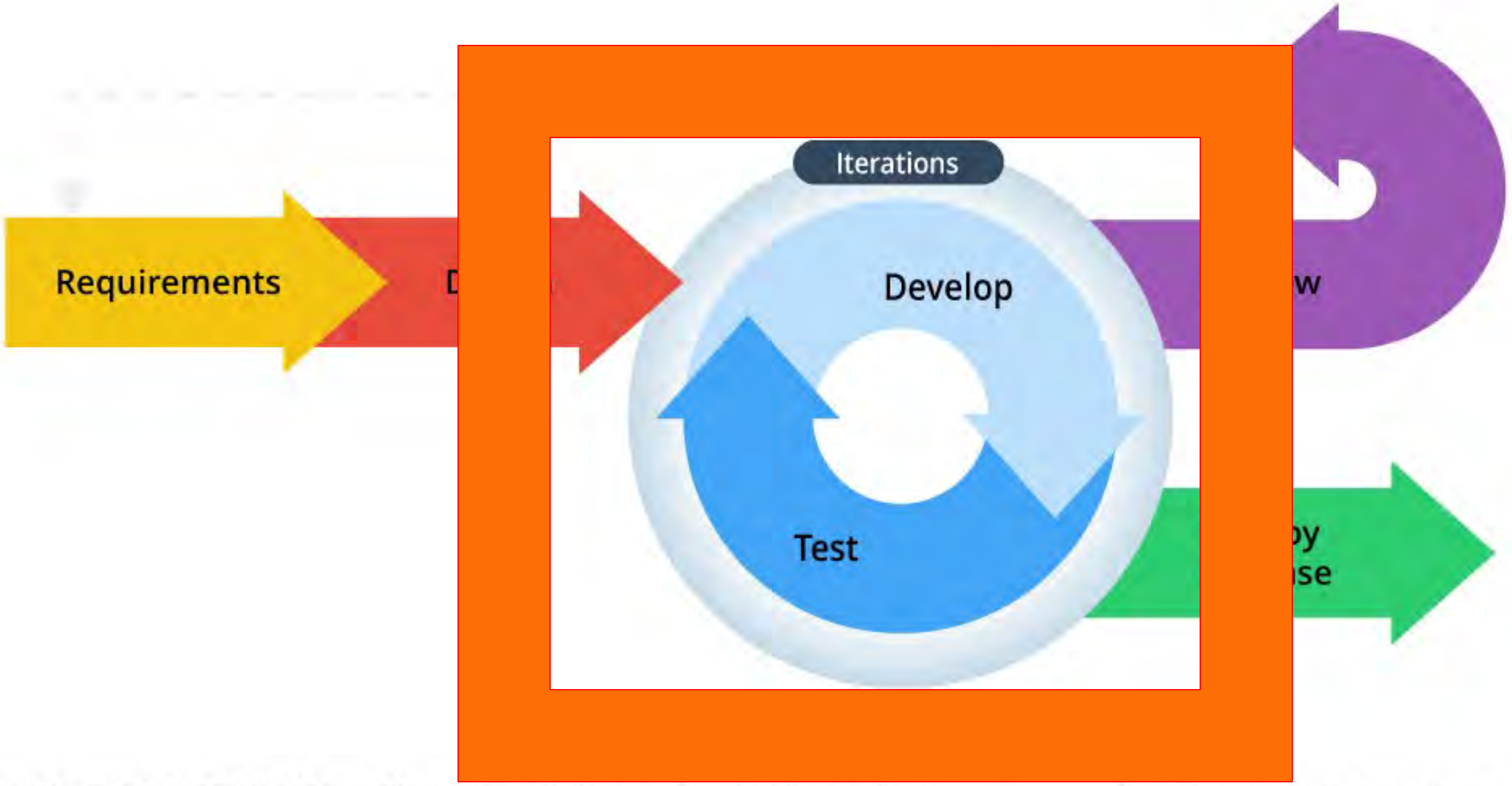
Code Review
Statis Analysis
Dynamic Analysis
Requirements Testing

Penetration Testing
Security Sign-off

Keep Threat or fraud model exercise concise and fun! Don’t overcomplicate

Step 7 – Security in Test

“Security (Testing) as early as possible”



SECURITY ACTIVITIES: Threat Modeling

Code Review
Statis Analysis
Dynamic Analysis
Requirements Testing

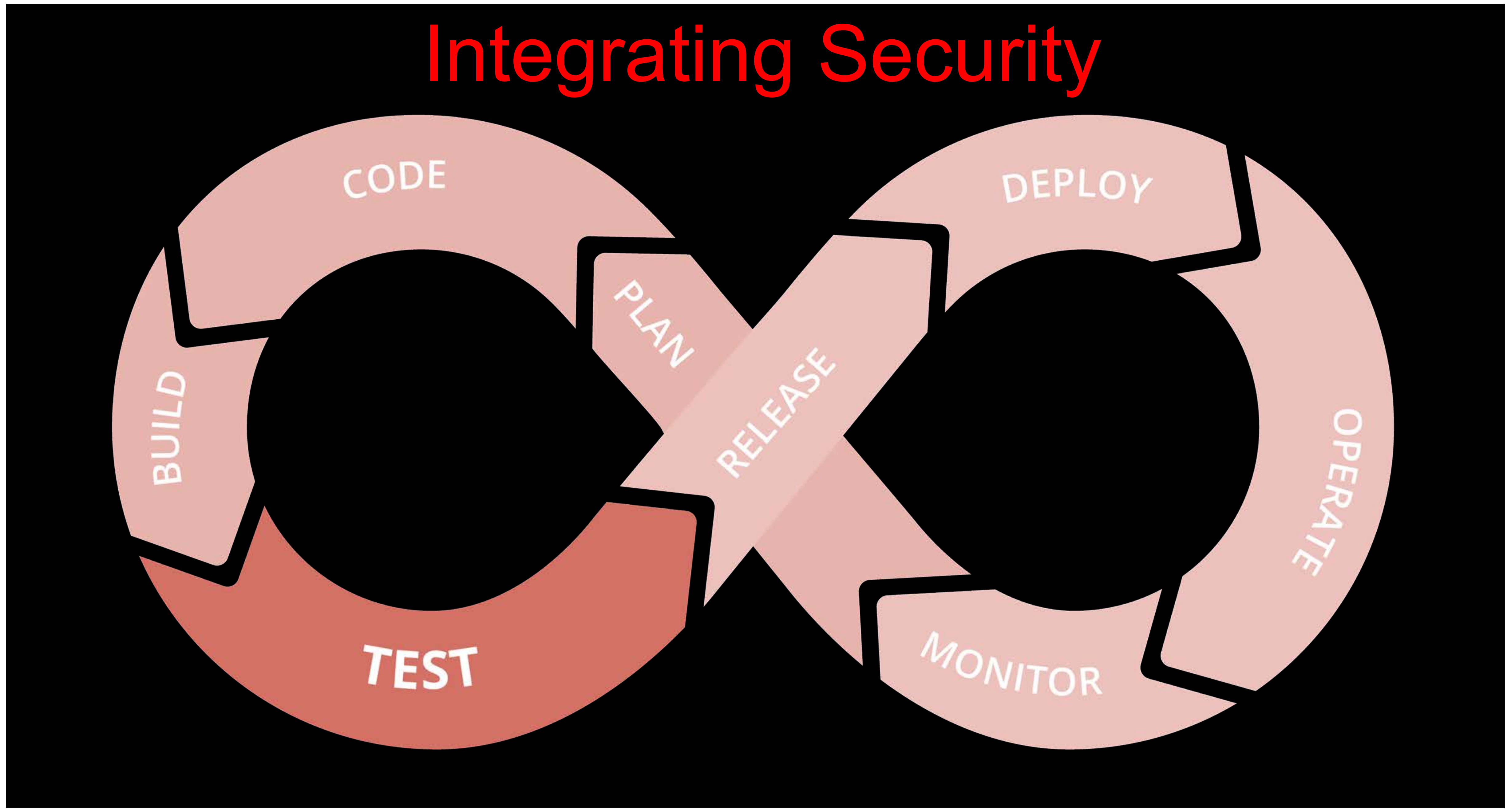
Penetration Testing
Security Sign-off

Security testing as bug bounty program! Make it fun and rewarding

Step 8 - DEV–SEC–OPS(BIZ)

What kind of animal is the DEV-SEC-OPS?

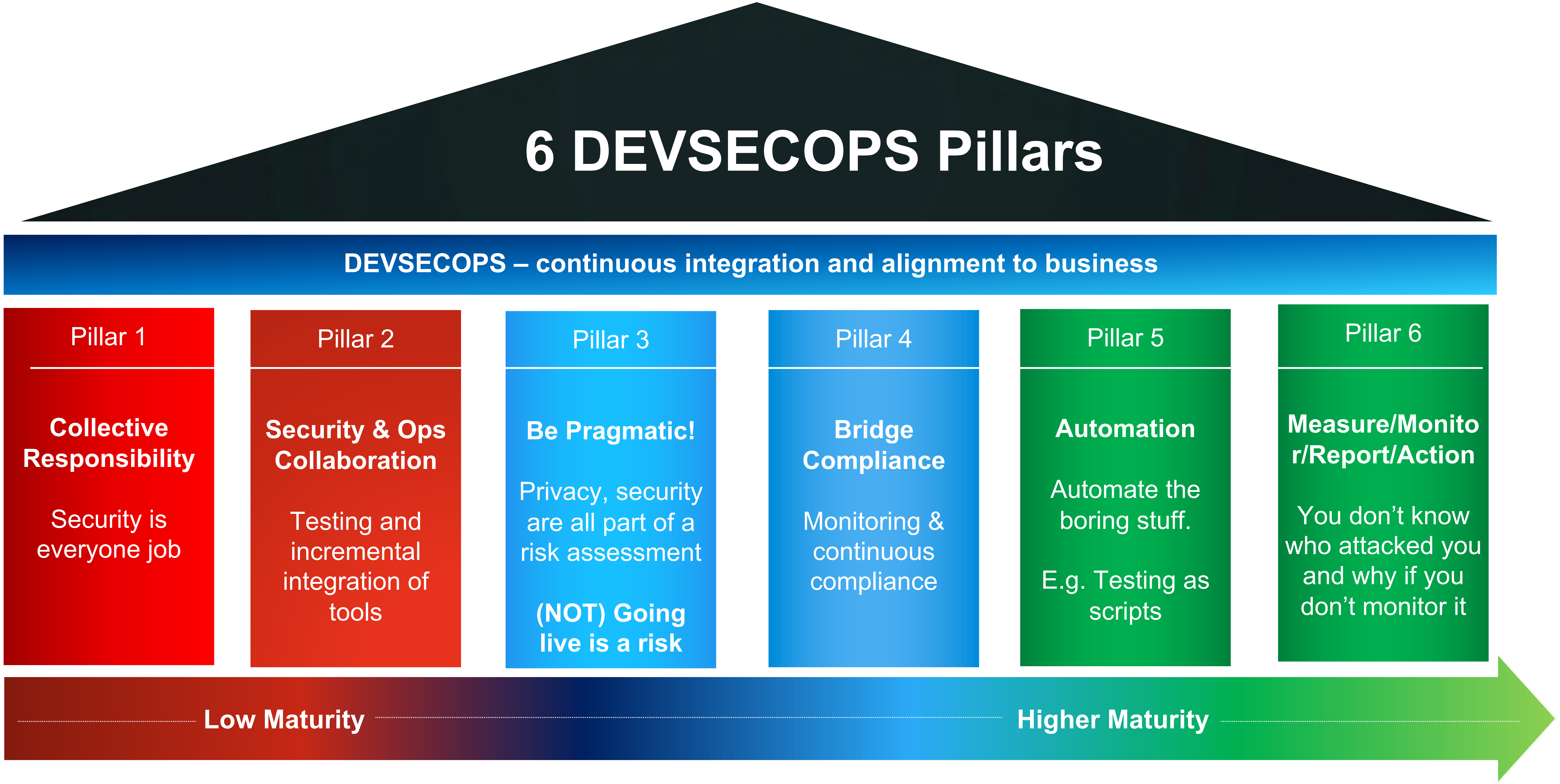
Integrate security into the OPS team (and add a spark of BIZ)



Security is everybody responsibility.

Reward security effort with -> Low cost High Impact

Step 8 - DEV–SEC–OPS(BIZ)



6 DEVSECOPS Pillars

DEVSECOPS – continuous integration and alignment to business

Pillar 1

Collective Responsibility

Security is everyone job

Pillar 2

Security & Ops Collaboration

Testing and incremental integration of tools

Pillar 3

Be Pragmatic!

Privacy, security are all part of a risk assessment

(NOT) Going live is a risk

Pillar 4

Bridge Compliance

Monitoring & continuous compliance

Pillar 5

Automation

Automate the boring stuff.

E.g. Testing as scripts

Pillar 6

Measure/Monitor/Report/Action

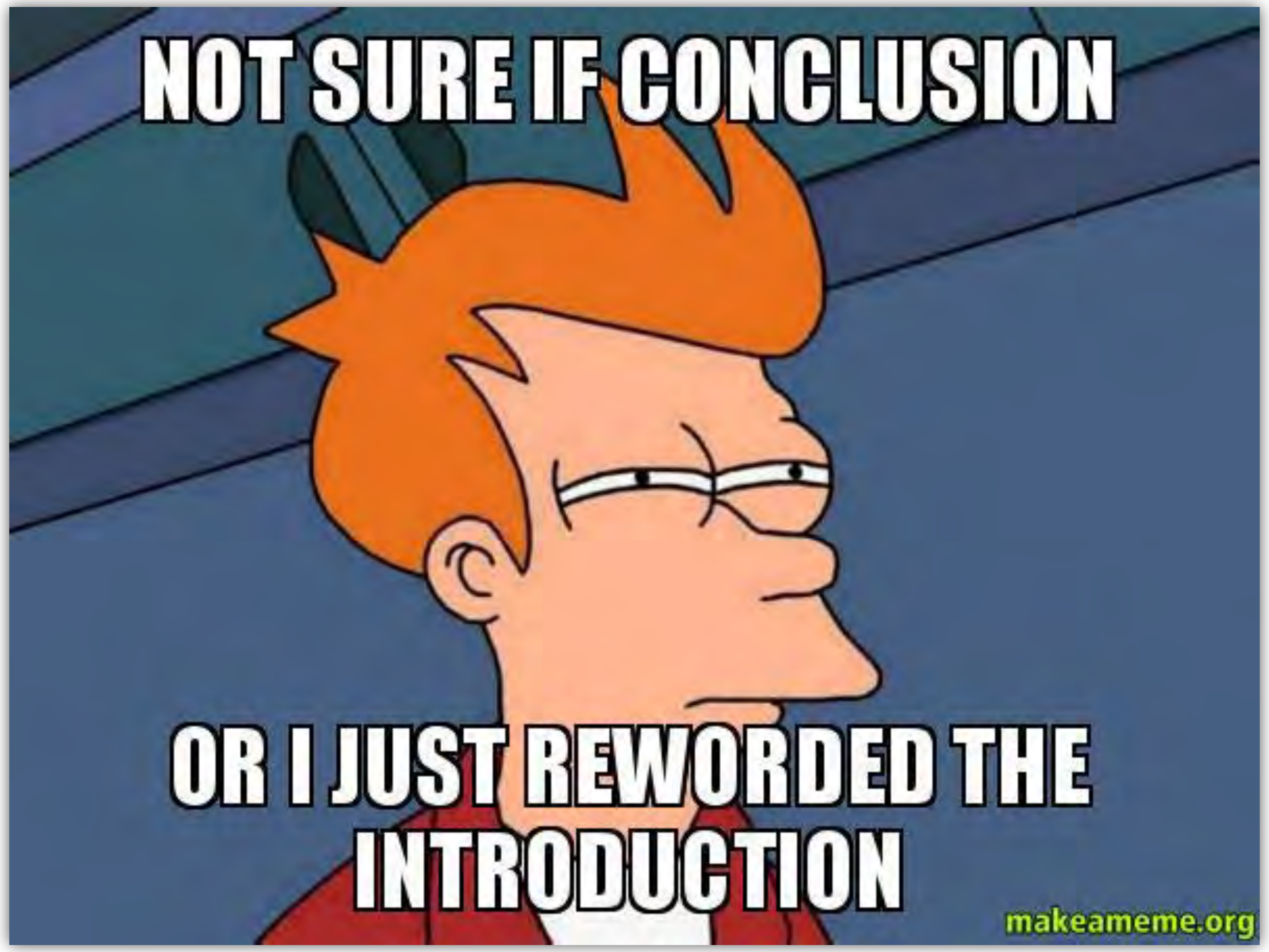
You don't know who attacked you and why if you don't monitor it

Low Maturity **Higher Maturity**

Conclusions

Wrapping up, we've discussed

- Cloud transformations planning
- Challenges and how to address them
- New Architecture/methodologies



Conclusions conslusions conclusions

Caveats/Pitfalls

Cloud transformations can be a treacherous journey especially for security professionals. Watch out for the common pitfalls

- Security imposed to cloud transformation with just policies/standards and antiquated patterns.

- Security team would require upskilling to understand how to best make use of the cloud fabric

- Transformation team can aggregate cloud transformation with other resulting in increased pressure on the security team.

Cloud is just someone else's PC ☺

Take Away

Cloud transformations can be a treacherous journey especially for security professionals:

- Decisions & Strategy
- Foundation (Security)
- Security by design
- Native tool! Use them
- Skill shortage: be prepared to learn
- Automation

Q&A

Question and Answers

Contacts

Thank you

Get in touch:

in https://uk.linkedin.com/in/fracipo

Francesco.cipollone (at) nsc42.co.uk

www.nsc42.co.uk

Problem with vendor only solution

Too many vendors

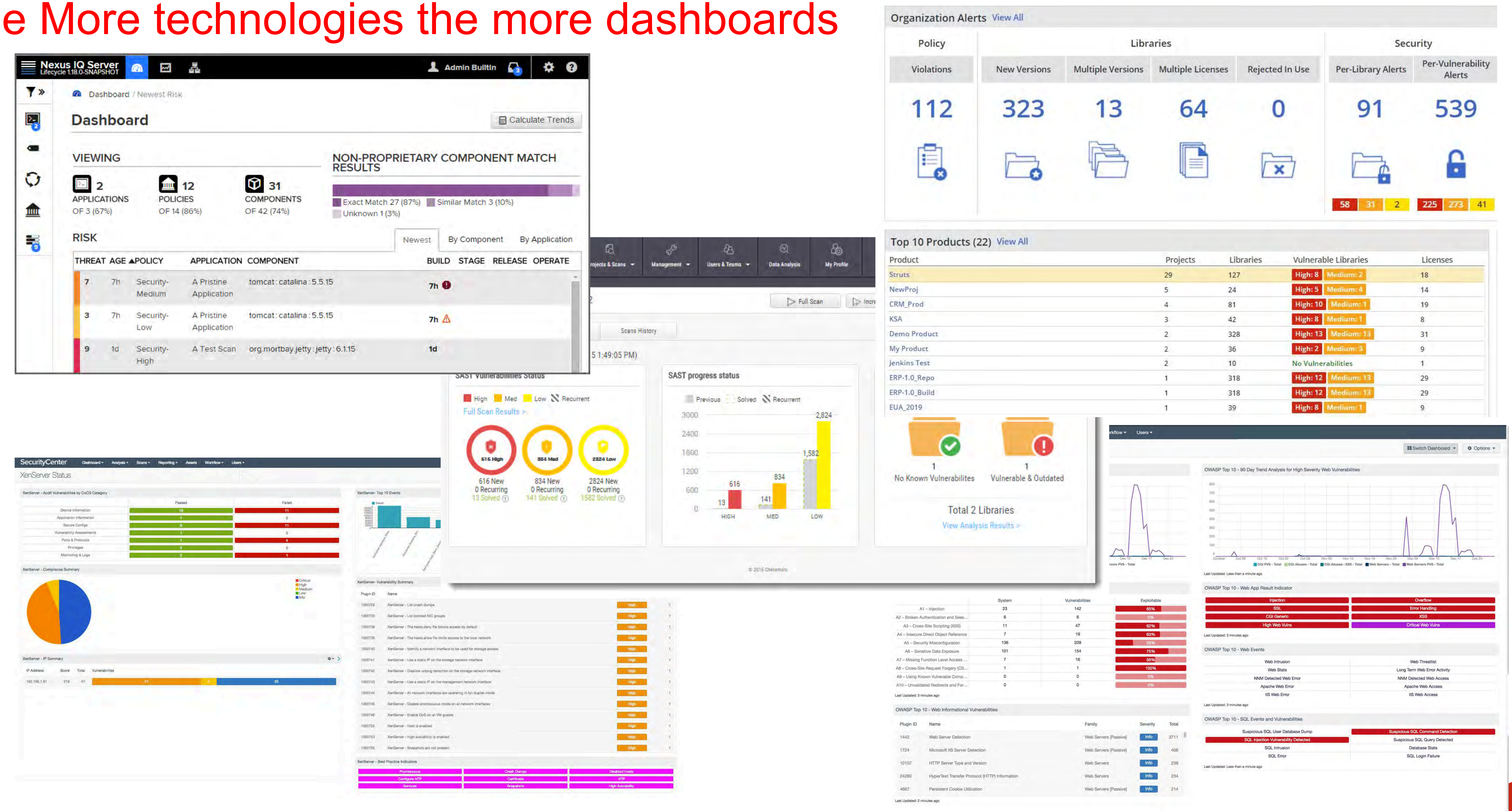
Too many alerts & dashboards

Not enough skilled expertise

Not enough time

Fix the problem with technology

The More technologies the more dashboards



Nexus IQ Server
Lifecycle 1.18.0-SNAPSHOT

Admin BuiltIn

Dashboard / Newest Risk

Dashboard

Calculate Trends

VIEWING

2 APPLICATIONS	12 POLICIES	31 COMPONENTS
OF 3 (67%)	OF 14 (86%)	OF 42 (74%)

NON-PROPRIETARY COMPONENT MATCH RESULTS

Exact Match 27 (87%) Similar Match 3 (10%) Unknown 1 (3%)

RISK

Newest | By Component | By Application

THREAT	AGE	▲POLICY	APPLICATION	COMPONENT	BUILD	STAGE	RELEASE	OPERATE
7	7h	Security-Medium	A Pristine Application	tomcat : catalina : 5.5.15	7h ❗			
3	7h	Security-Low	A Pristine Application	tomcat : catalina : 5.5.15	7h ⚠			
9	1d	Security-High	A Test Scan	org.mortbay.jetty : jetty : 6.1.15	1d			

Organization Alerts View All

Policy	Libraries				Security	
Violations	New Versions	Multiple Versions	Multiple Licenses	Rejected In Use	Per-Library Alerts	Per-Vulnerability Alerts
112	323	13	64	0	91	539
					58 31 2	225 273 41

Top 10 Products (22) View All

Product	Projects	Libraries	Vulnerable Libraries	Licenses
Struts	29	127	High: 8 Medium: 2	18
NewProj	5	24	High: 5 Medium: 4	14
CRM_Prod	4	81	High: 10 Medium: 1	19
KSA	3	42	High: 8 Medium: 1	8
Demo Product	2	328	High: 13 Medium: 13	31
My Product	2	36	High: 2 Medium: 3	9
Jenkins Test	2	10	No Vulnerabilities	1
ERP-1.0_Repo	1	318	High: 12 Medium: 13	29
ERP-1.0_Build	1	318	High: 12 Medium: 13	29
EUA_2019	1	39	High: 8 Medium: 1	9

1 No Known Vulnerabilites

1 Vulnerable & Outdated

Total 2 Libraries

View Analysis Results >

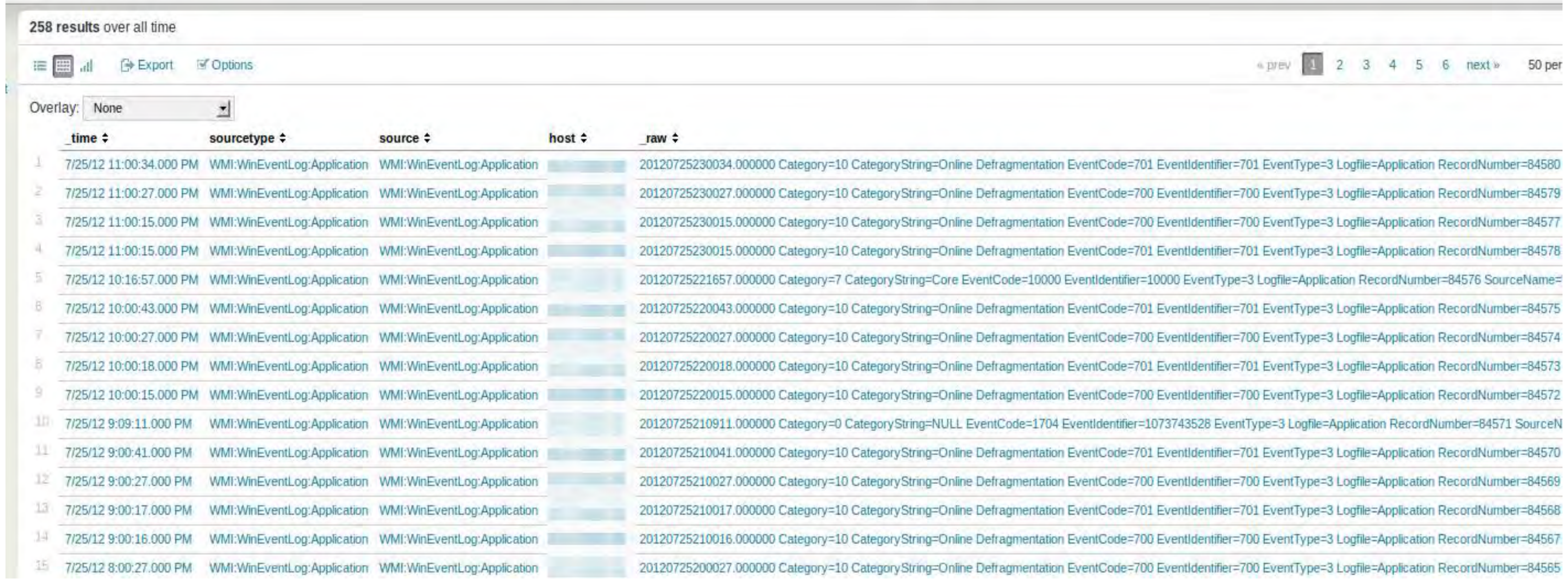
SecurityCenter
XenServer Status
XenServer - Audit Vulnerabilities by CoCS Category
XenServer - Top 10 Events
XenServer - Compliance Summary
XenServer - Vulnerability Summary
XenServer - IP Summary
XenServer - Best Practice Indicators
Workflow
Users
Switch Dashboard
Options
OWASP Top 10 - 90 Day Trend Analysis for High Severity Web Vulnerabilities
OWASP Top 10 - Web App Result Indicator
OWASP Top 10 - Web Events
OWASP Top 10 - SQL Events and Vulnerabilities
OWASP Top 10 - Web Informational Vulnerabilities

Fix the problem with technology

Too many alert
Too little time
Who can you trust?

Total cost of cloud breaches
5 trillion $
4 trillion GBP

Every min
62K record disclosed
Record per minute disclosed

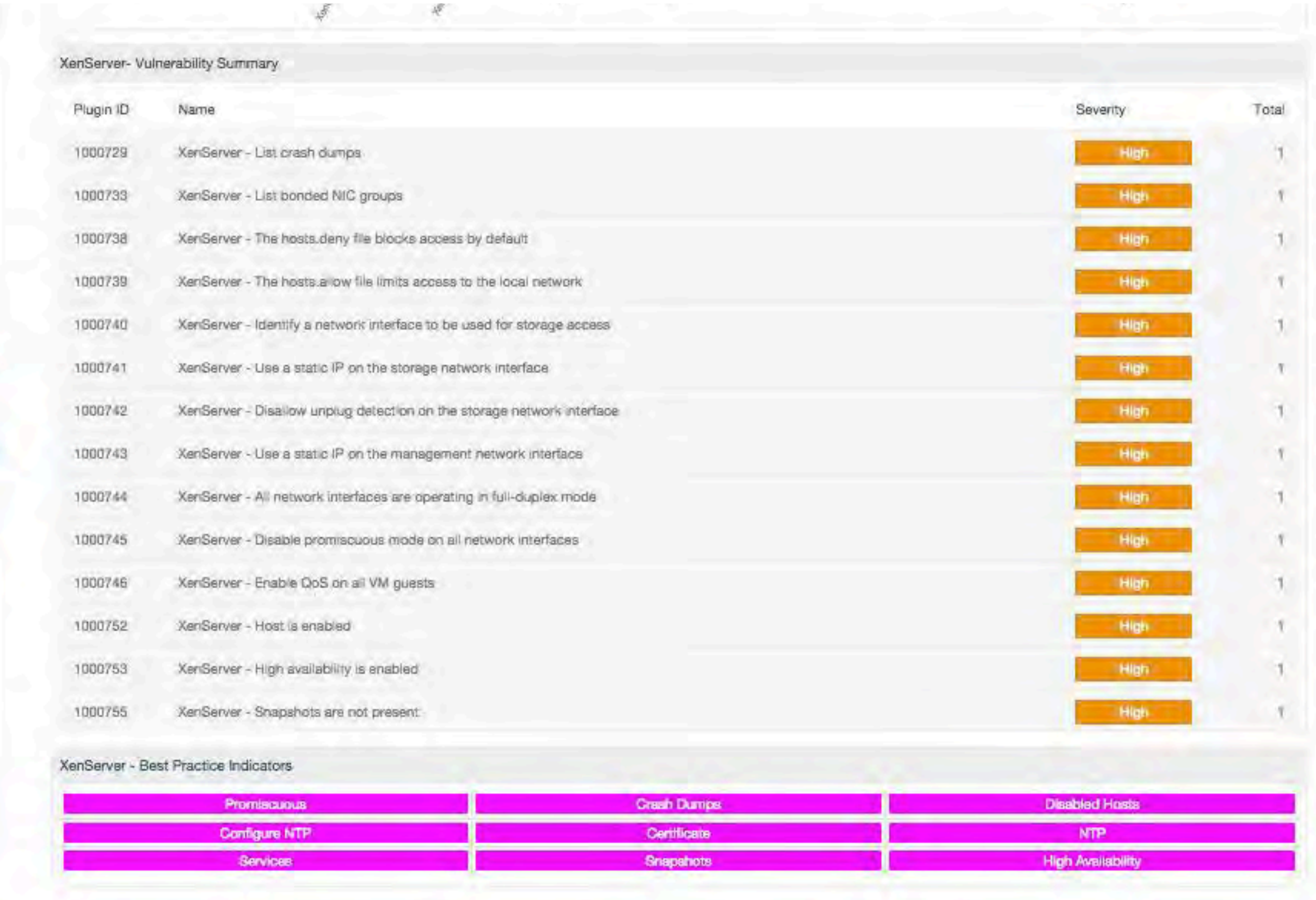


258 results over all time

Export Options « prev 1 2 3 4 5 6 next » 50 per

Overlay: None

	_time	sourcetype	source	host	_raw
1	7/25/12 11:00:34.000 PM	WMI:WinEventLog:Application	WMI:WinEventLog:Application	[redacted]	20120725230034.000000 Category=10 CategoryString=Online Defragmentation EventCode=701 EventIdentifier=701 EventType=3 Logfile=Application RecordNumber=84580
2	7/25/12 11:00:27.000 PM	WMI:WinEventLog:Application	WMI:WinEventLog:Application	[redacted]	20120725230027.000000 Category=10 CategoryString=Online Defragmentation EventCode=700 EventIdentifier=700 EventType=3 Logfile=Application RecordNumber=84579
3	7/25/12 11:00:15.000 PM	WMI:WinEventLog:Application	WMI:WinEventLog:Application	[redacted]	20120725230015.000000 Category=10 CategoryString=Online Defragmentation EventCode=700 EventIdentifier=700 EventType=3 Logfile=Application RecordNumber=84577
4	7/25/12 11:00:15.000 PM	WMI:WinEventLog:Application	WMI:WinEventLog:Application	[redacted]	20120725230015.000000 Category=10 CategoryString=Online Defragmentation EventCode=701 EventIdentifier=701 EventType=3 Logfile=Application RecordNumber=84578
5	7/25/12 10:16:57.000 PM	WMI:WinEventLog:Application	WMI:WinEventLog:Application	[redacted]	20120725221657.000000 Category=7 CategoryString=Core EventCode=10000 EventIdentifier=10000 EventType=3 Logfile=Application RecordNumber=84576 SourceName=
6	7/25/12 10:00:43.000 PM	WMI:WinEventLog:Application	WMI:WinEventLog:Application	[redacted]	20120725220043.000000 Category=10 CategoryString=Online Defragmentation EventCode=701 EventIdentifier=701 EventType=3 Logfile=Application RecordNumber=84575
7	7/25/12 10:00:27.000 PM	WMI:WinEventLog:Application	WMI:WinEventLog:Application	[redacted]	20120725220027.000000 Category=10 CategoryString=Online Defragmentation EventCode=700 EventIdentifier=700 EventType=3 Logfile=Application RecordNumber=84574
8	7/25/12 10:00:18.000 PM	WMI:WinEventLog:Application	WMI:WinEventLog:Application	[redacted]	20120725220018.000000 Category=10 CategoryString=Online Defragmentation EventCode=701 EventIdentifier=701 EventType=3 Logfile=Application RecordNumber=84573
9	7/25/12 10:00:15.000 PM	WMI:WinEventLog:Application	WMI:WinEventLog:Application	[redacted]	20120725220015.000000 Category=10 CategoryString=Online Defragmentation EventCode=700 EventIdentifier=700 EventType=3 Logfile=Application RecordNumber=84572
10	7/25/12 9:09:11.000 PM	WMI:WinEventLog:Application	WMI:WinEventLog:Application	[redacted]	20120725210911.000000 Category=0 CategoryString=NULL EventCode=1704 EventIdentifier=1073743528 EventType=3 Logfile=Application RecordNumber=84571 SourceN
11	7/25/12 9:00:41.000 PM	WMI:WinEventLog:Application	WMI:WinEventLog:Application	[redacted]	20120725210041.000000 Category=10 CategoryString=Online Defragmentation EventCode=701 EventIdentifier=701 EventType=3 Logfile=Application RecordNumber=84570
12	7/25/12 9:00:27.000 PM	WMI:WinEventLog:Application	WMI:WinEventLog:Application	[redacted]	20120725210027.000000 Category=10 CategoryString=Online Defragmentation EventCode=700 EventIdentifier=700 EventType=3 Logfile=Application RecordNumber=84569
13	7/25/12 9:00:17.000 PM	WMI:WinEventLog:Application	WMI:WinEventLog:Application	[redacted]	20120725210017.000000 Category=10 CategoryString=Online Defragmentation EventCode=701 EventIdentifier=701 EventType=3 Logfile=Application RecordNumber=84568
14	7/25/12 9:00:16.000 PM	WMI:WinEventLog:Application	WMI:WinEventLog:Application	[redacted]	20120725210016.000000 Category=10 CategoryString=Online Defragmentation EventCode=700 EventIdentifier=700 EventType=3 Logfile=Application RecordNumber=84567
15	7/25/12 8:00:27.000 PM	WMI:WinEventLog:Application	WMI:WinEventLog:Application	[redacted]	20120725200027.000000 Category=10 CategoryString=Online Defragmentation EventCode=700 EventIdentifier=700 EventType=3 Logfile=Application RecordNumber=84565

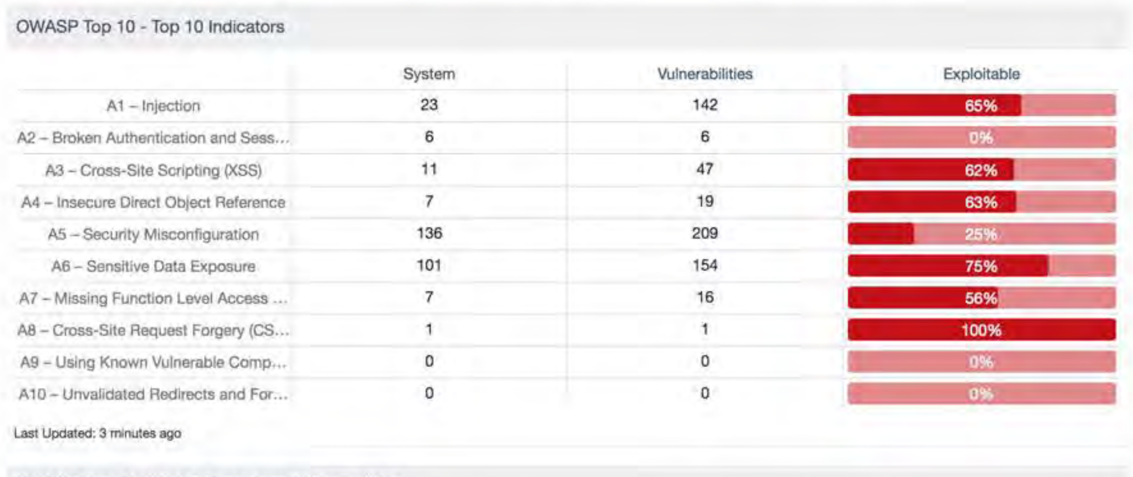


XenServer- Vulnerability Summary

Plugin ID	Name	Severity	Total
1000729	XenServer - List crash dumps	High	1
1000733	XenServer - List bonded NIC groups	High	1
1000738	XenServer - The hosts.deny file blocks access by default	High	1
1000739	XenServer - The hosts.allow file limits access to the local network	High	1
1000740	XenServer - Identify a network interface to be used for storage access	High	1
1000741	XenServer - Use a static IP on the storage network interface	High	1
1000742	XenServer - Disallow unplug detection on the storage network interface	High	1
1000743	XenServer - Use a static IP on the management network interface	High	1
1000744	XenServer - All network interfaces are operating in full-duplex mode	High	1
1000745	XenServer - Disable promiscuous mode on all network interfaces	High	1
1000746	XenServer - Enable QoS on all VM guests	High	1
1000752	XenServer - Host is enabled	High	1
1000753	XenServer - High availability is enabled	High	1
1000755	XenServer - Snapshots are not present	High	1

XenServer - Best Practice Indicators

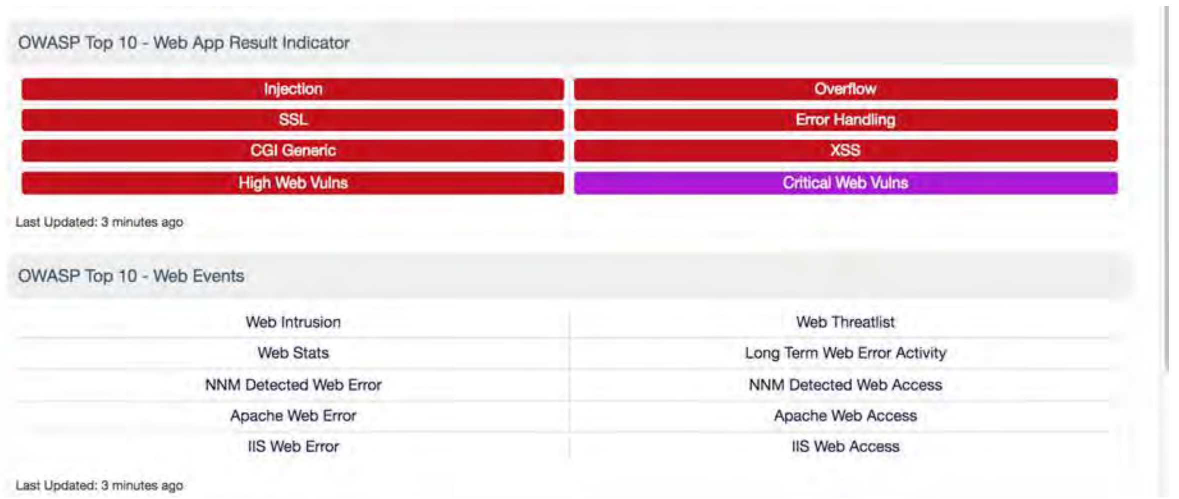
Promiscuous	Crash Dumps	Disabled Hosts
Configure NTP	Certificate	NTP
Services	Snapshots	High Availability



OWASP Top 10 - Top 10 Indicators

	System	Vulnerabilities	Exploitable
A1 – Injection	23	142	65%
A2 – Broken Authentication and Sess…	6	6	0%
A3 – Cross-Site Scripting (XSS)	11	47	62%
A4 – Insecure Direct Object Reference	7	19	63%
A5 – Security Misconfiguration	136	209	25%
A6 – Sensitive Data Exposure	101	154	75%
A7 – Missing Function Level Access …	7	16	56%
A8 – Cross-Site Request Forgery (CS…	1	1	100%
A9 – Using Known Vulnerable Comp…	0	0	0%
A10 – Unvalidated Redirects and For…	0	0	0%

Last Updated: 3 minutes ago



OWASP Top 10 - Web App Result Indicator

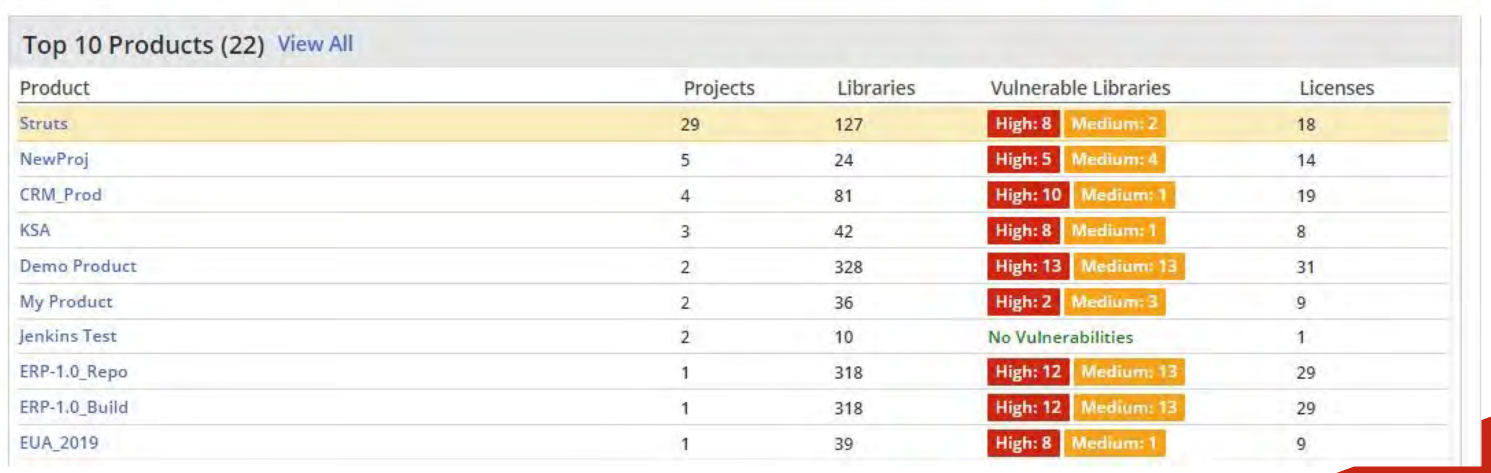
Injection	Overflow
SSL	Error Handling
CGI Generic	XSS
High Web Vulns	Critical Web Vulns

Last Updated: 3 minutes ago

OWASP Top 10 - Web Events

Web Intrusion	Web Threatlist
Web Stats	Long Term Web Error Activity
NNM Detected Web Error	NNM Detected Web Access
Apache Web Error	Apache Web Access
IIS Web Error	IIS Web Access

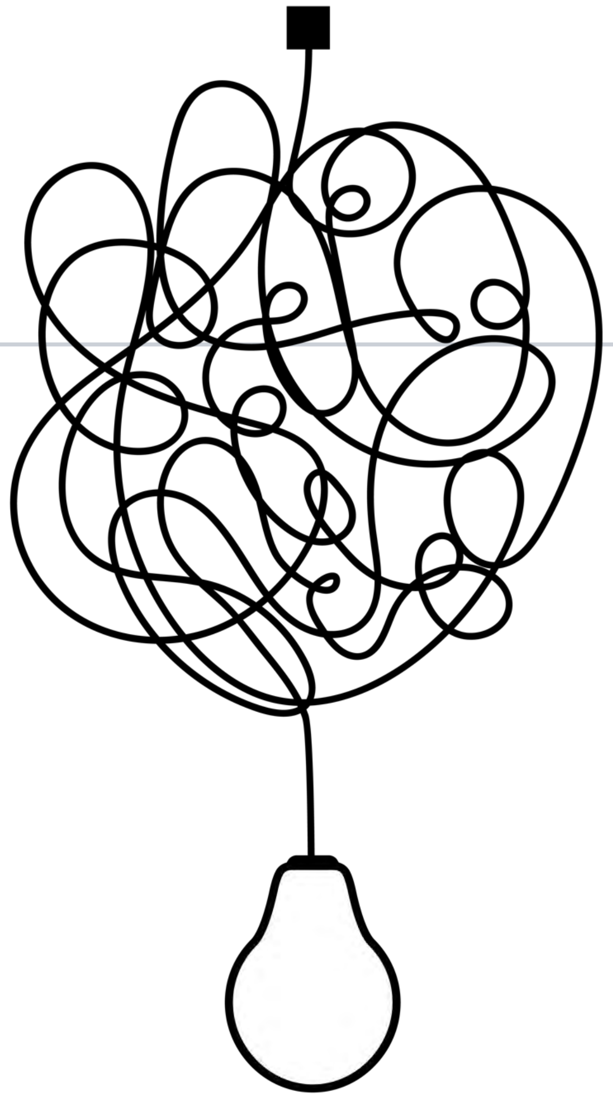
Last Updated: 3 minutes ago



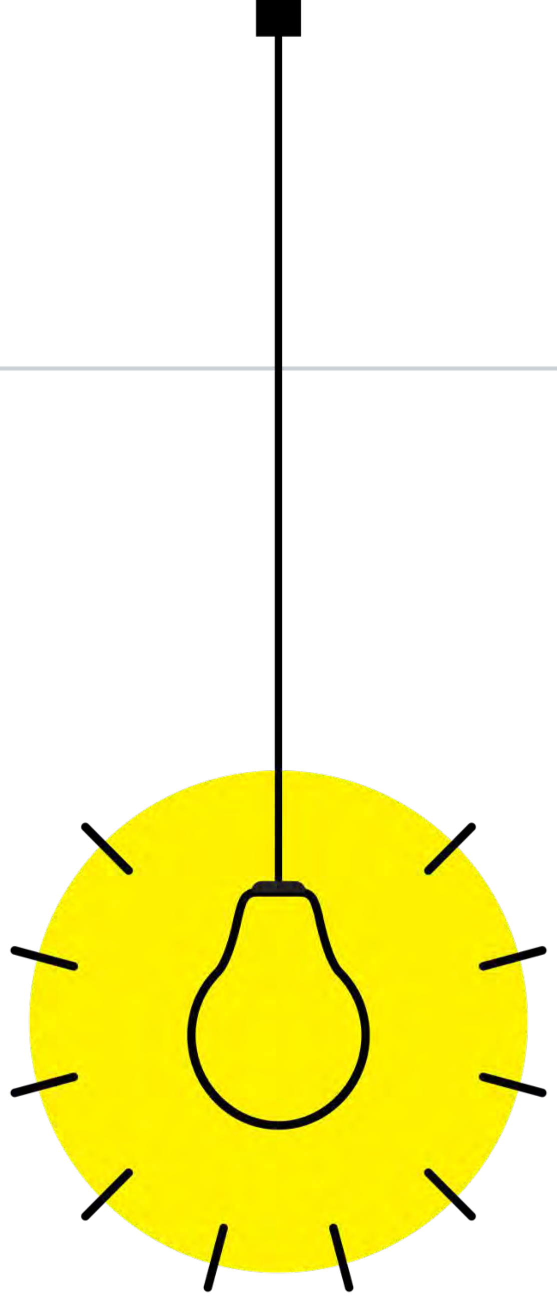
Top 10 Products (22) View All

Product	Projects	Libraries	Vulnerable Libraries	Licenses
Struts	29	127	High: 8 Medium: 2	18
NewProj	5	24	High: 5 Medium: 4	14
CRM_Prod	4	81	High: 10 Medium: 1	19
KSA	3	42	High: 8 Medium: 1	8
Demo Product	2	328	High: 13 Medium: 13	31
My Product	2	36	High: 2 Medium: 3	9
Jenkins Test	2	10	No Vulnerabilities	1
ERP-1.0_Repo	1	318	High: 12 Medium: 13	29
ERP-1.0_Build	1	318	High: 12 Medium: 13	29
EUA_2019	1	39	High: 8 Medium: 1	9

Our Solution



Trust & Clarity



Too many vendors

Too many alerts & dashboards

Too much confusion & overwhelm

Not enough skilled expertise

Single view and report

Report and vulnerabilities explained by experts

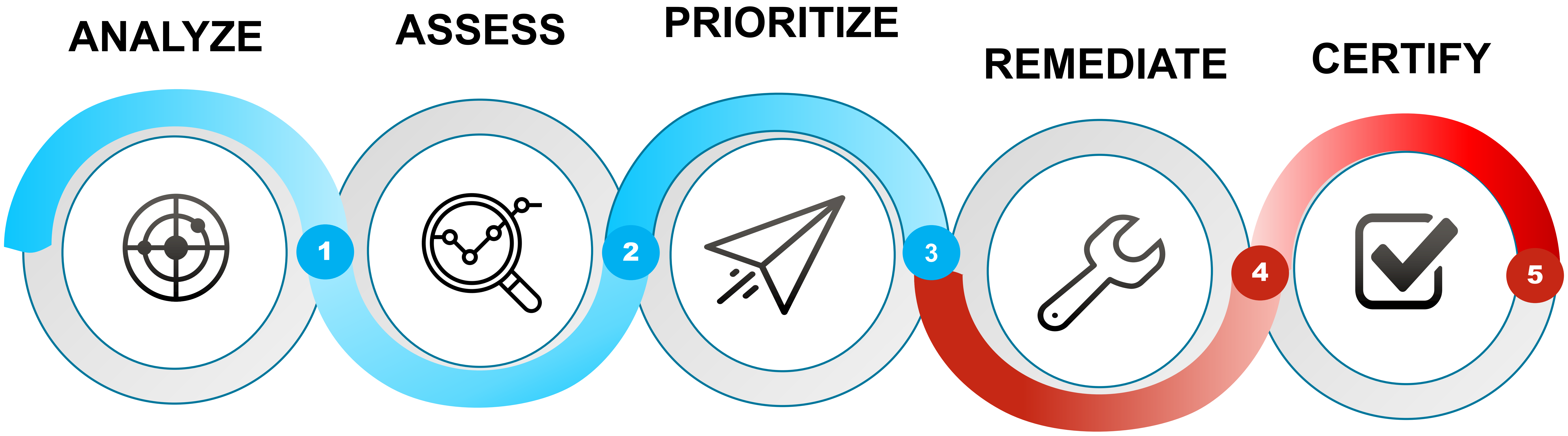
Consultancy from recognized cyber experts

Training and consultancy

A validated methodology across our services

Your Protection is Our Success

OUR METHOD: AAP-RC



Analyze the posture & highlight the problems

Recommend remediation path

Agree Scope, Prioritize

Execute the agreed remediation steps

Review & Certify

Customer Journey – Cloud Security Assessments

Initial Assessment

Unknown Security Posture

Initial Call

Size of Assessment

Bronze

Base Assessment

Service Tier

Silver

Silver

Bronze +

Cloud Assessment Actioned & Resolved

Agree on Vulnerabilities to be resolved

Cloud Assessment Walkthrough

Gold (MSSP)

Gold (MSSP)

AD-HOC

Agree on services to be secured (MSSP)

Onboard Client on the security Platform

Agree on the

Managed Services

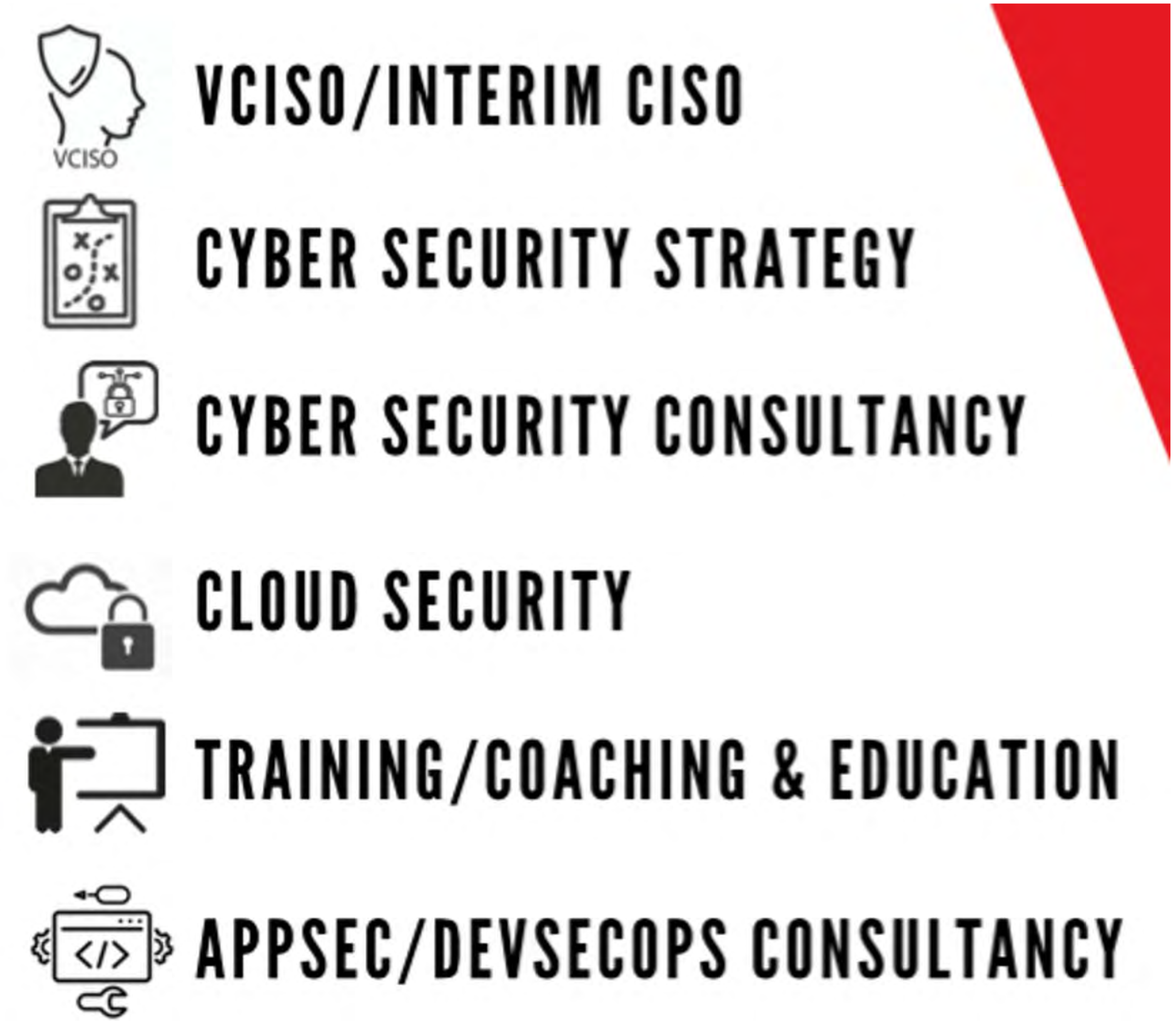
Our Other Services

We believe in an all rounded set of services built on the need of our clients over the years and recognized by the Cloud Security Alliance.

What differentiates our company from other consultancies is that we do what we love and are customer focused.

Our company goes the extra mile in order to deliver solutions that are fit for purpose, effective and cost-effective for your organization's risks appetite.

We offer a range of products within cybersecurity.



VCISO/INTERIM CISO

CYBER SECURITY STRATEGY

CYBER SECURITY CONSULTANCY

CLOUD SECURITY

TRAINING/COACHING & EDUCATION

APPSEC/DEVSECOPS CONSULTANCY

Chartered Institute of Information Security

NSC42

When **you** are **Cybersafe**
We are **Cyberhappy**

Contacts

NSC42

WHEN YOU ARE CYBERSAFE WE ARE CYBERHAPPY

Thank you

Get in touch:

https://www.linkedin.com/company/nsc42-limited

Communications@nsc42.co.uk

www.nsc42.co.uk