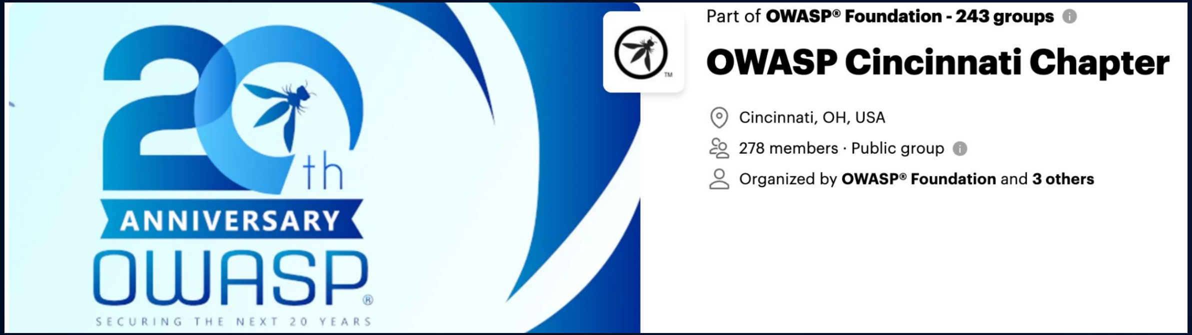
Stand Up Straight
-
Security Posture And You



Part of **OWASP® Foundation - 243 groups**

OWASP Cincinnati Chapter

Cincinnati, OH, USA

278 members · Public group

Organized by **OWASP® Foundation** and **3 others**

@mcdwayne

@mcdwayne

Please Join Me For A Stretch

- Standing is optional
- Always take care of yourself
- Always remember to breathe

"Juvenile Burrowing Owl stretching"
https://www.onthewingphotography.com/wings/portfolio-items/juvenile-burrowing-owl-stretching/

@mcdwayne

Hi. I’m Dwayne.

Dwayne McDaniel

- I live in Chicago
- I’ve been a Developer Advocate since 2016
- Co-host of [The Security Repo Podcast]
- On Twitter @mcdwayne
- mcdwayne@mastodon.social
- LinkedIn @dwaynemcdaniel
- Happy to chat about anything, hit me up
- Outside of tech, I love improv, karaoke and going to rock and roll shows!

@mcdwayne

About GitGuardian

GitGuardian is the code security platform for the DevOps generation.

We help enterprises answer the issue of "Where are my hardcoded secrets and have they been leaked?"

@mcdwayne

@mcdwayne

Poll

Who here works on a security team?

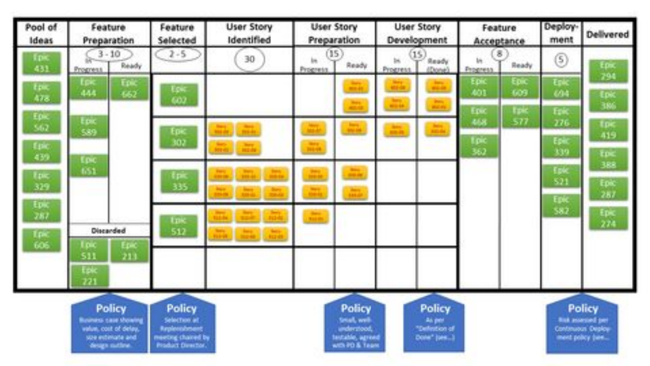
Poll

How many people here work to improve security inside your code, deployments, and organization?

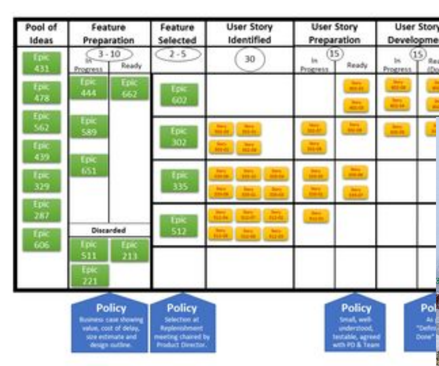
Poll

Who knows exactly what you should work on next to improve security the most?

What Should I do Next?



What Should I do Next?



Pool of Ideas	Feature Preparation	Feature Selected	User Story Identified	User Story Preparation	User Story Development	Feature Acceptance	Deploy-ment	Delivered
	3 - 10 In Progress / Ready	2 - 5	30	15 In Progress / Ready	15 In Progress / Ready (Done)	8 In Progress / Ready	5	
Epic 431 Epic 478 Epic 562 Epic 439 Epic 329 Epic 287 Epic 606	In Progress: Epic 444 Epic 589 Epic 651 Ready: Epic 662 Discarded Epic 511 Epic 213 Epic 221	Epic 602 Epic 302 Epic 335 Epic 512				Epic 401 Epic 609 Epic Epic	Epic 694 Epic	Epic 294 Epic 386

Policy
Business case showing value, cost of delay, size estimate and design outline.

Policy
Selection at Replenishment meeting chaired by Product Director.

Policy
Small, well-understood, testable, agreed with PD & Team

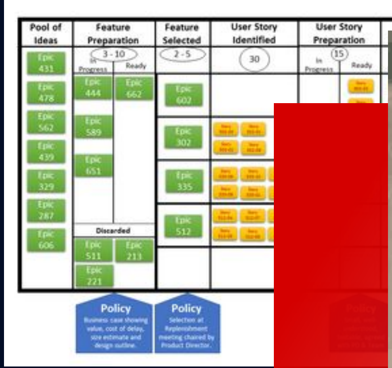
Pol
As
"Defin
Done"

What Should I do Next?

Pool of Ideas
Feature Preparation
Feature Selected
User Story Identified
User Story Preparation
User Story Development
Feature Acceptance
Deploy-ment
Delivered
3 - 10
In Progress
Ready
2 - 5
30
15
15
Ready (Done)
8
5
Epic 431
Epic 478
Epic 562
Epic 439
Epic 329
Epic 287
Epic 606
Epic 444
Epic 662
Epic 589
Epic 651
Discarded
Epic 511
Epic 213
Epic 221
Epic 602
Epic 302
Epic 335
Epic 512
Epic 401
Epic 609
Epic 694
Epic 294
Epic 386
Policy
Business case showing value, cost of delay, size estimate and design outline.
Policy
Selection at Replenishment meeting chaired by Product Director.
Policy
Small, well-understood, testable, agreed with PO & Team

What Should I do Next?

What Should I do Next?



Security Posture Management Can Help You Answer "What Should I Do Next?"

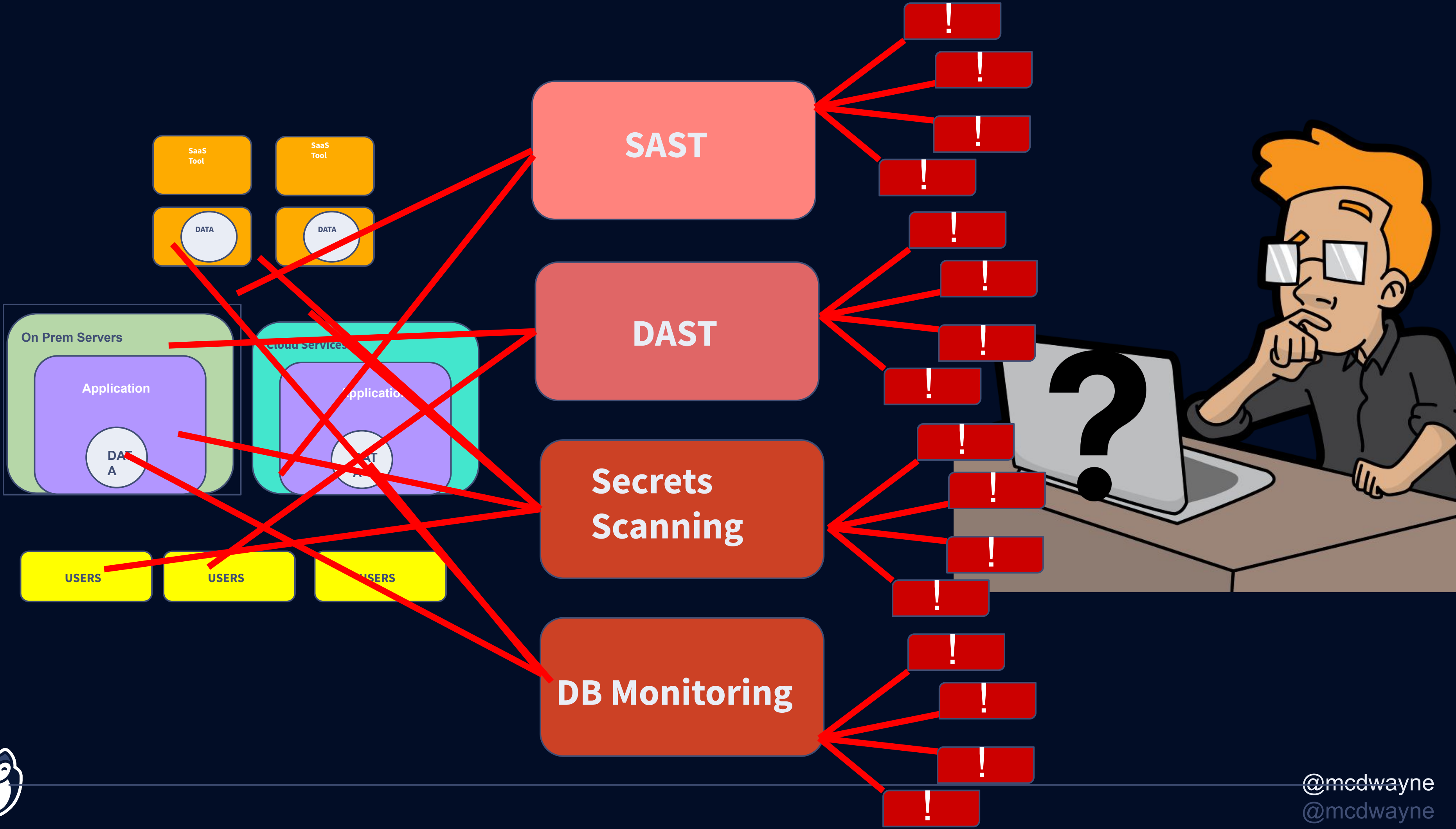
Fog of war

@mcdwayne

Security Posture Management

- Priorities - What should I work on next?
- Risk - Which incidents would be the most expensive?
- In-Context Data - How do I know I need to fix that?
- Remediation - How should I fix it?

@mcdwayne



SAST

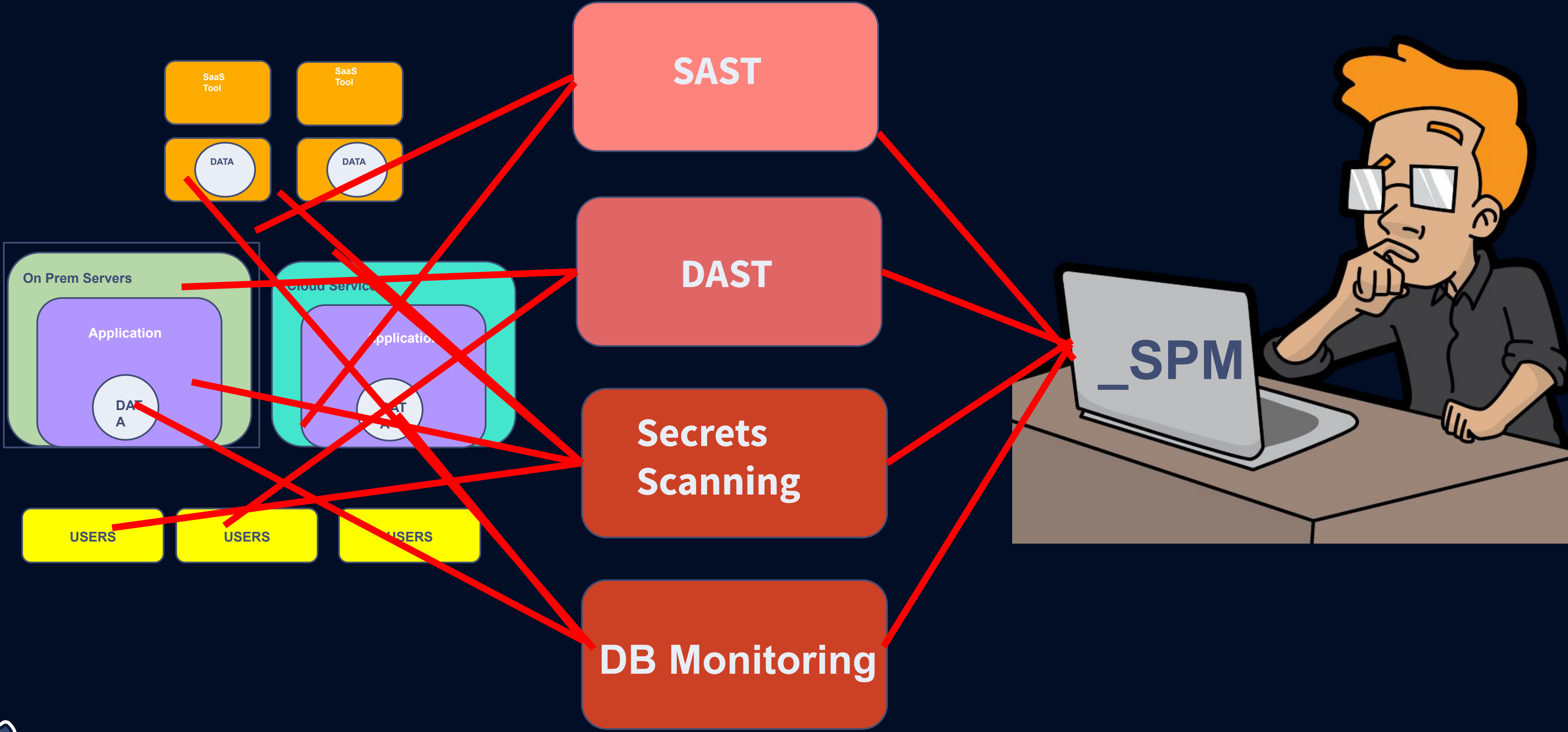
DAST

Secrets Scanning

DB Monitoring

@mcdwayne

@mcdwayne



SaaS Tool

SaaS Tool

DATA

DATA

On Prem Servers

Application

DATA

Cloud Services

Application

DATA

USERS

USERS

USERS

SAST

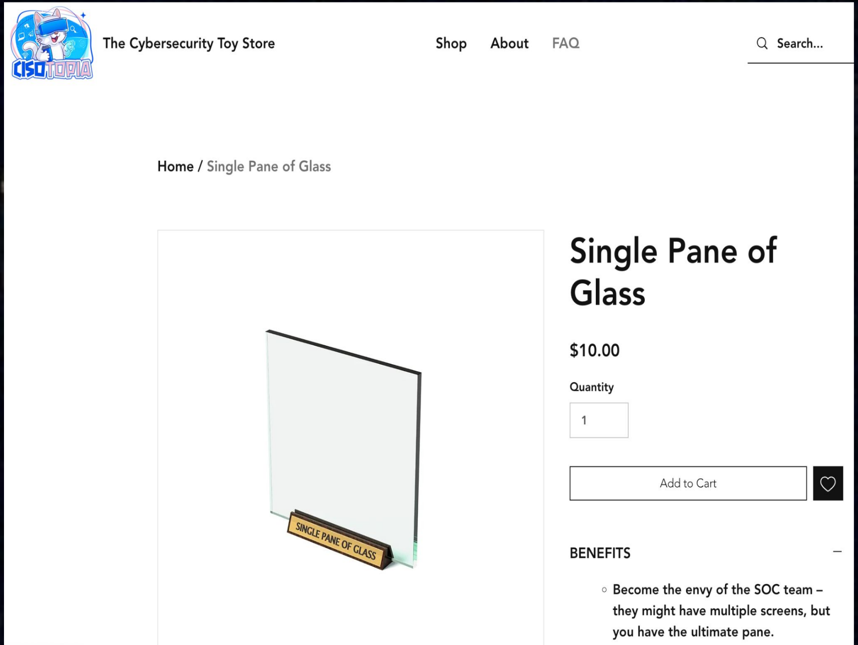
DAST

Secrets Scanning

DB Monitoring

@mcdwayne

@mcdwayne



The Cybersecurity Toy Store

Shop About FAQ

Search...

Home / Single Pane of Glass

Single Pane of Glass

$10.00

Quantity

1

Add to Cart

BENEFITS

- Become the envy of the SOC team – they might have multiple screens, but you have the ultimate pane.

www.cisotopia.com/product-page/single-pane-of-glass

The Big 4 SPM Categories

(According to Gartner)

CSPM = Cloud

SSPM = SaaS

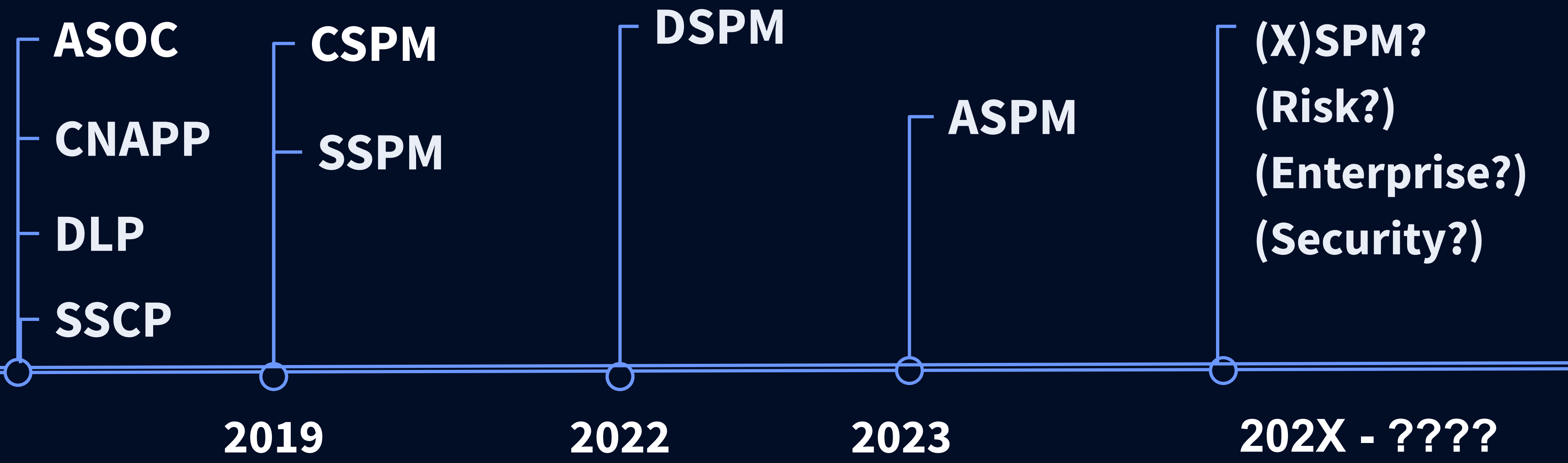
DSPM = Data

ASPM = Application

@mcdwayne

History of the Posture Management World

(According to Gartner)



ASOC

CNAPP

DLP

SSCP

2019

CSPM

SSPM

2022

DSPM

2023

ASPM

202X - ????

(X)SPM?

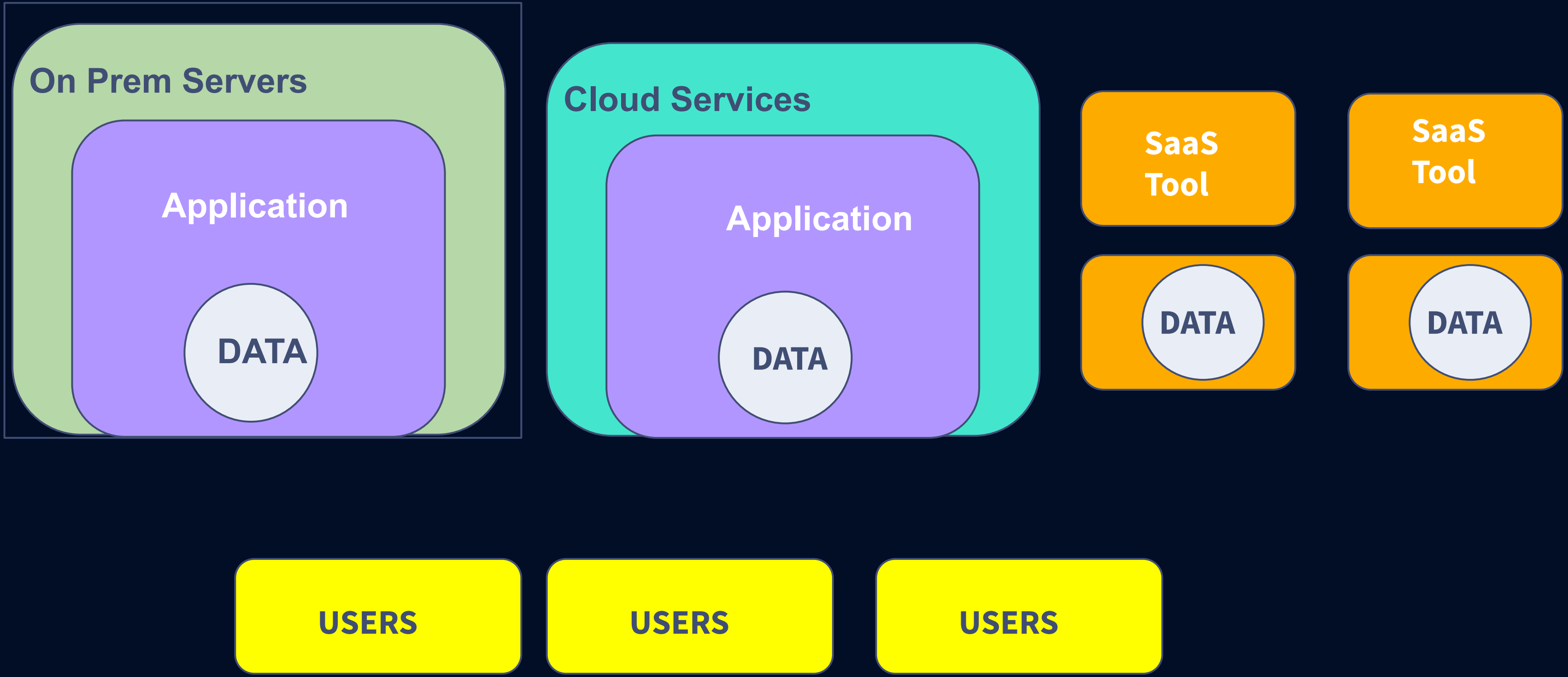
(Risk?)

(Enterprise?)

(Security?)

@mcdwayne

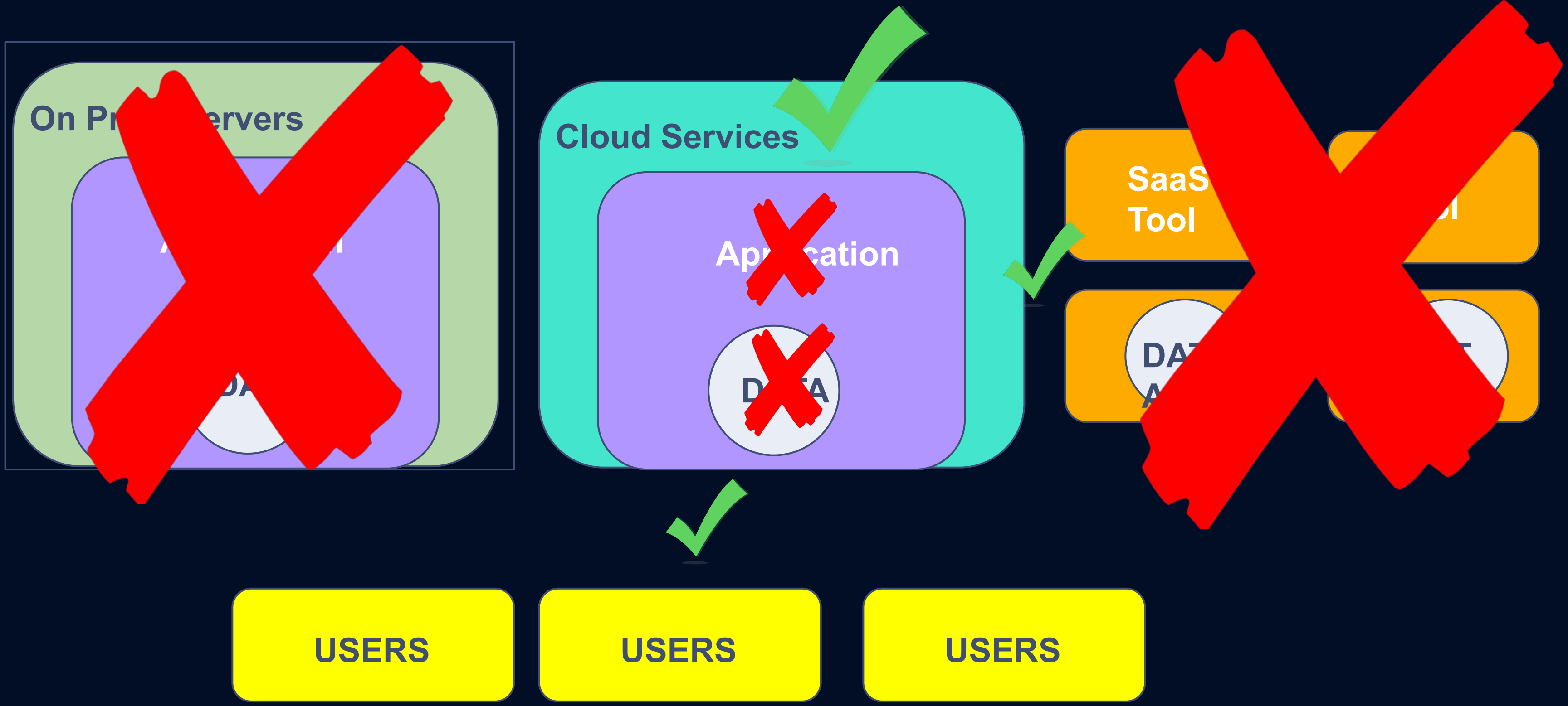
Areas Of Concern



@mcdwayne

@mcdwayne

CSPM = Cloud



@mcdwayne

@mcdwayne

CSPM

Cloud Security Posture Management

Cares about:

Anomalous clients/traffic

Unencrypted S3 buckets

Suspicious OS processes

Cloud Misconfigurations

OS Vulnerabilities

IAM/ROLE/Permission changes

Cloud API/Service usage

On services like:

AWS :
EC2
RDS
S3
Lambda
CloudFront

Or Azure:
Azure VMs
SQL DB
Blob Storage
Functions

Note: I am lumping Kubernetes Security Posture Management (KSPM) in with CSPM

@mcdwayne

CSPM

Cloud Security Posture Management

Example Vendors:

PRISMA®
BY PALO ALTO NETWORKS

CROWDSTRIKE

WIZ

Sysdig

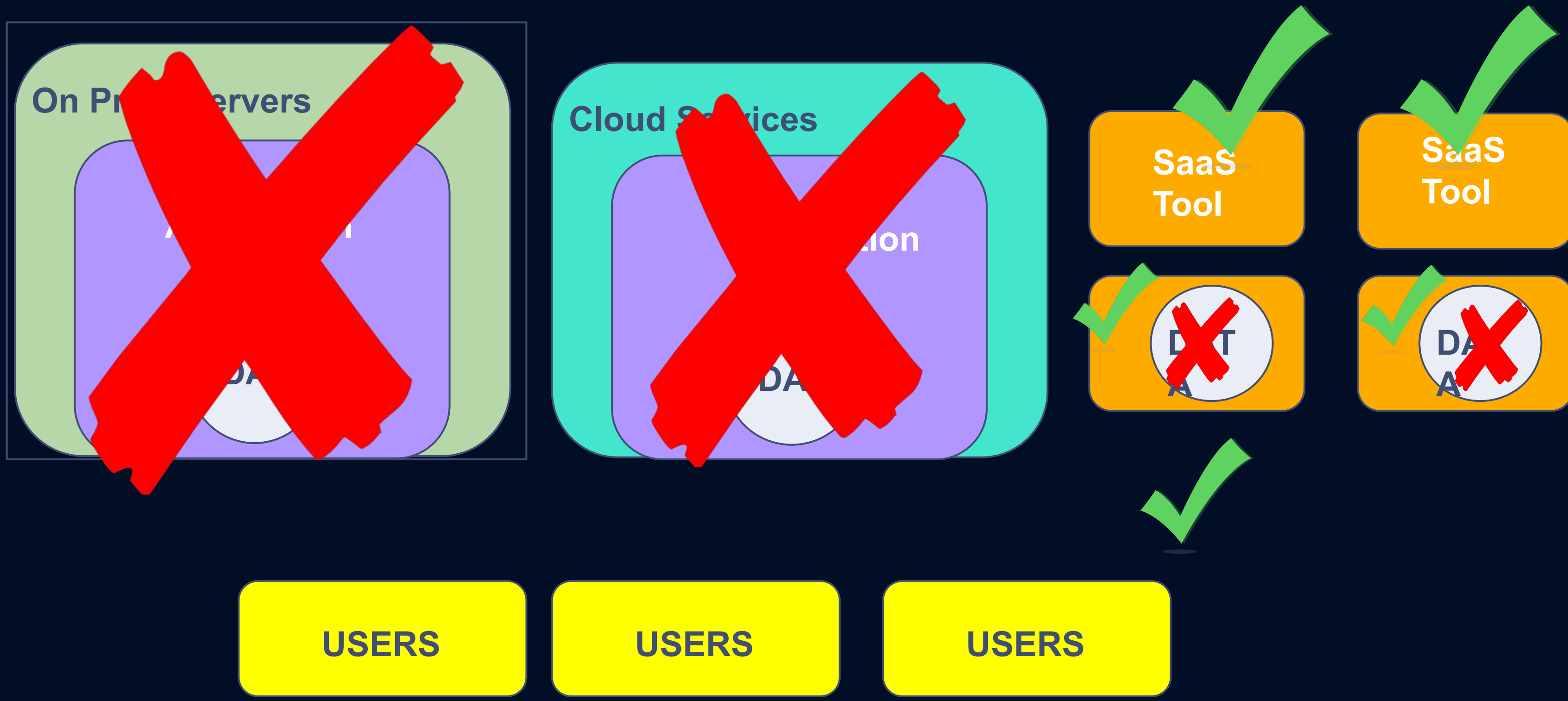
zscaler™

PingSafe

orca
security

@mcdwayne

SSPM = SaaS



@mcdwayne

SSPM

SaaS Security Posture Management

Cares about:

SaaS Misconfigurations
Anomalous clients/traffic
User Devices
User Permissions
Third party access
Saas to SaaS connections
IAM changes
Cloud API/Service usage
SaaS vulns

On services like:

Salesforce
Hubspot
Figma
Canva
Google Suite
Office365
Confluence
Jira
Box
Slack
Asana
Trello

@mcdwayne

SSPM

Example Vendors:

SaaS
Security
Posture
Management

Obsidian

netskope

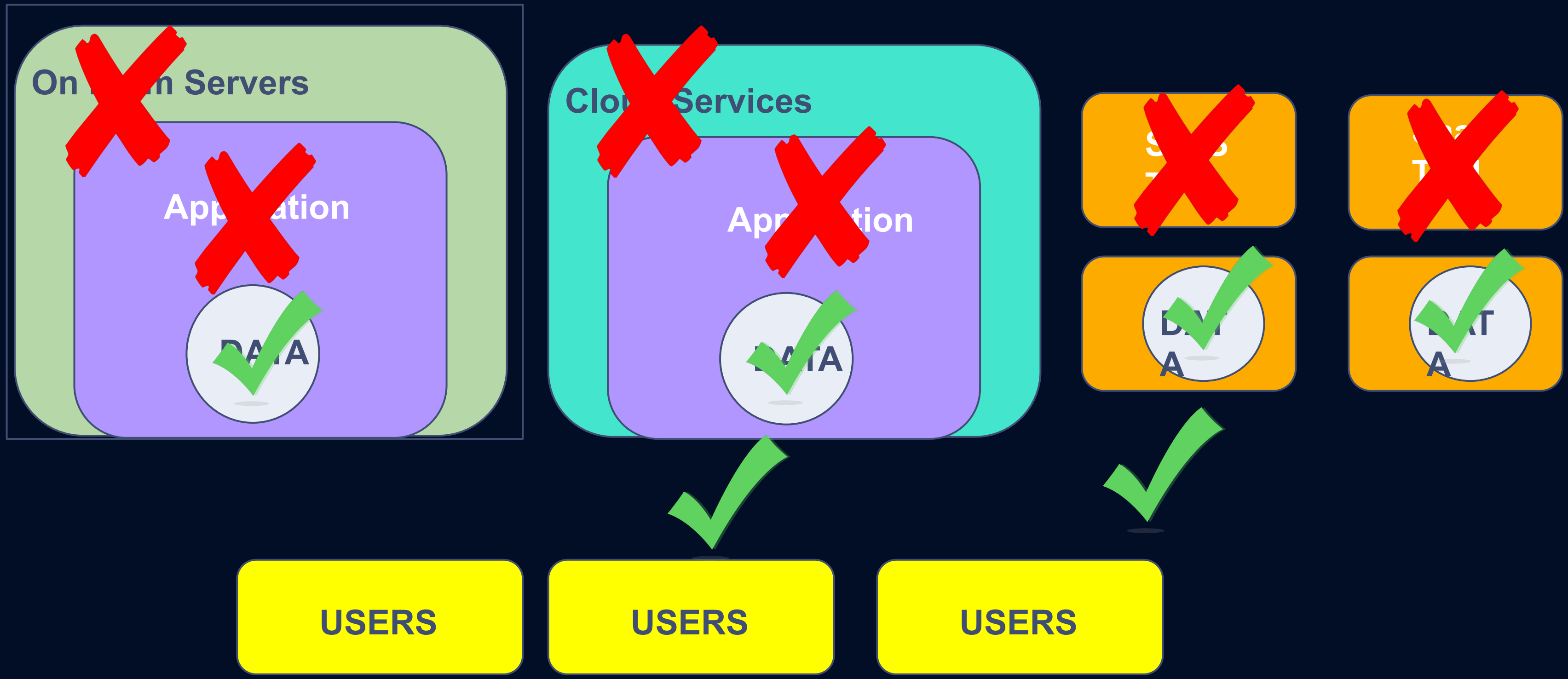
cynet

ADAPTIVE SHIELD

AppOmni

@mcdwayne

DSPM = Data



@mcdwayne

DSPM

Data Security Posture Management

Cares about:

- Data Discovery
- Visibility of Data
- Data movement
- Saas to SaaS connections
- Regulatory Compliance
- Wrong type of data
- Too much data shared
- Third party access
- MFA
- Device access

On services like:

- NAS
- Local DBs
- Private cloud
- AWS
- GCP
- Azure
- Salesforce
- Hubspot
- Google Suite
- Office365
- Confluence
- Jira
- Slack
- Asana

DSPM

Example Vendors:

Data Security Posture Management

VARONIS

SYMMETRY SYSTEMS

securiti

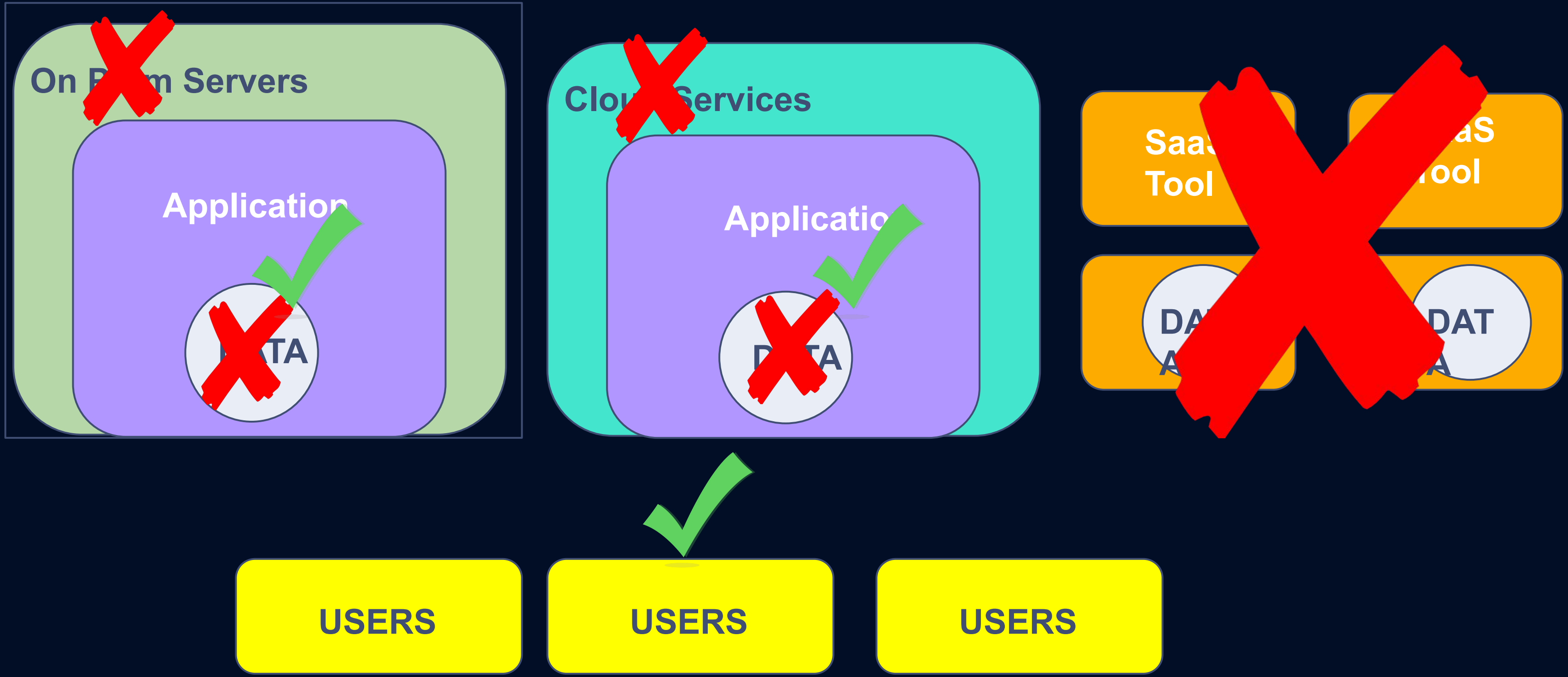
Laminar

Dig Security BY PRISMA CLOUD

CYERA

@mcdwayne

ASPM = SaaS



@mcdwayne

@mcdwayne

ASPM

Application Security Posture Management

Cares about:

Hardcoded secrets

Unauthed APIs

Unencrypted data flows

App Misconfig

App CVEs

PII Data Leakage

OSS/Code Vulns

On services like:

WebApps
DBs
Message brokers
Directory services
3rd party apps
NAS

@mcdwayne

ASPM

Example Vendors:

Application Security Posture Management

DEFECTDOJO

ArmorCode

BIONIC
A CrowdStrike Company

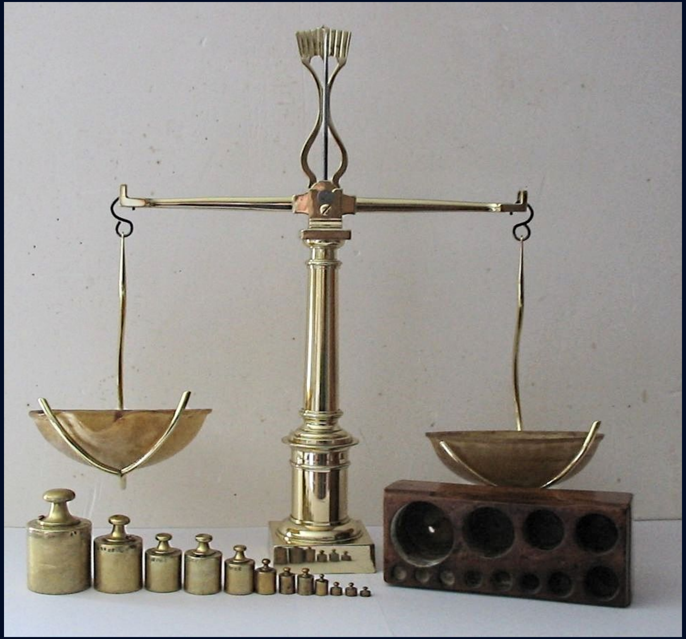
[arnica]

PHOENIX SECURITY

kondukto

@mcdwayne

How to measure your security posture?



Measuring Security == Measuring Risk

@mcdwayne

@mcdwayne

Measuring Risk

Risks are NOT threats.
Risks are NOT vulns.
Risks are NOT exploits.

Risks are what you are set to lose if things go bad.

– Walt Powell - Field CISO, CDW

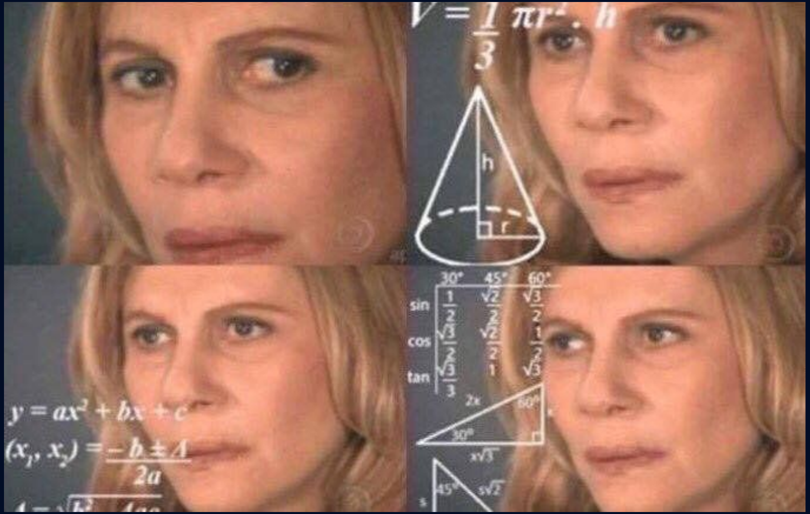
@mcdwayne

Measuring Risk

Security Risk = Threat ❎ Exploitability ❎

Criticality

- Where am I vulnerable?
- What is the likelihood of a successful attack?
- What would it cost the company or you?

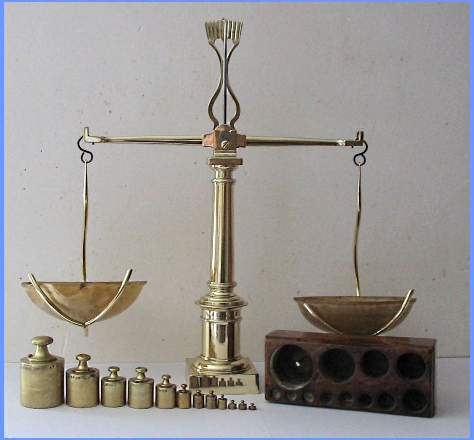


@mcdwayne

Measuring Risk

"Risk" means very different things to different parts of the organization. Beyond just security risk, business face:

- Business risk
- Compliance risk
- Operational risk
- Financial risk



- Investor risk
- Strategic risk
- Human risk
- Legal risk

@mcdwayne

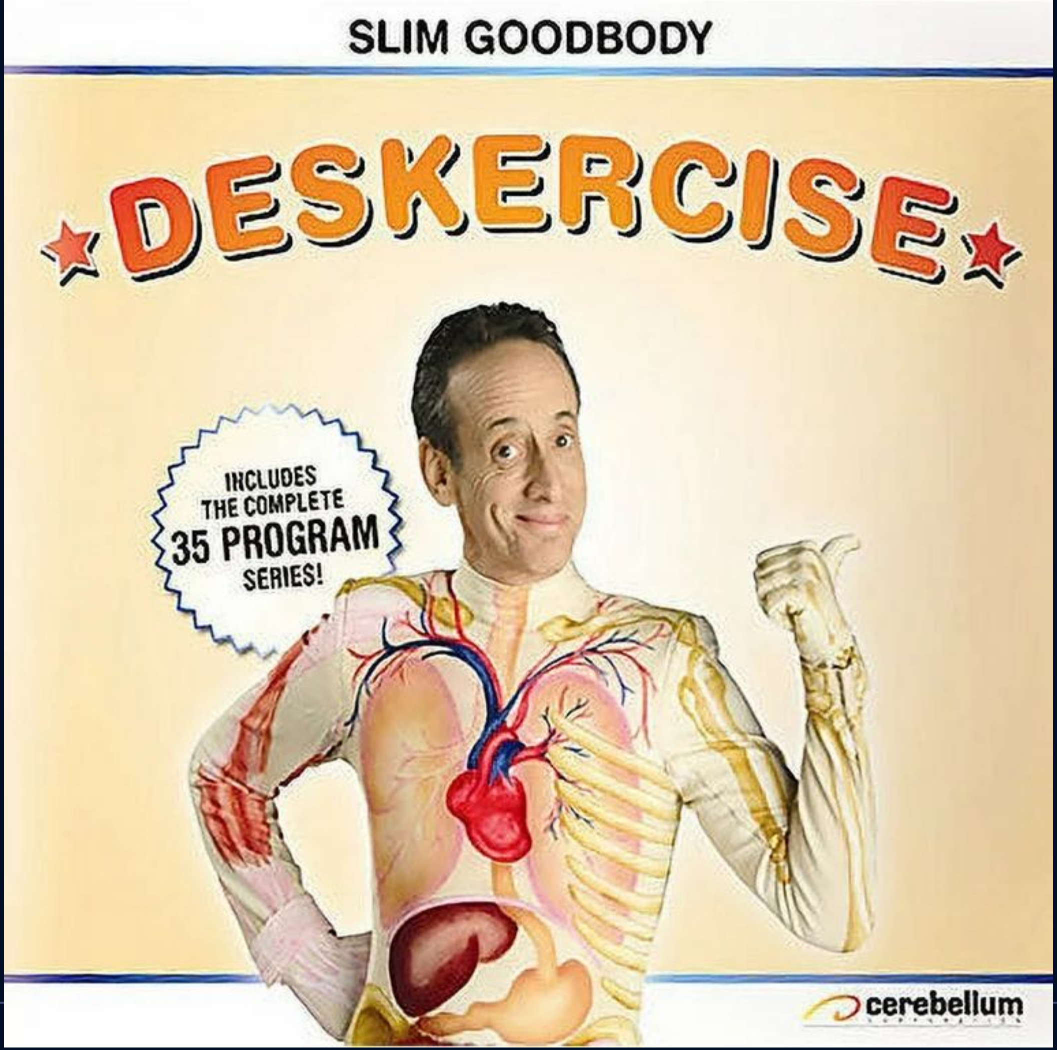
Business Risks != Technical Risk

"The Board does not know or care what a CVE is.
They care that something is going to make them lose money.

Period."

– again, thank you to Walt Powell - Field CISO, CDW

@mcdwayne


SLIM GOODBODY
DESKERCISE
INCLUDES THE COMPLETE 35 PROGRAM SERIES!
cerebellum

@mcdwayne

Which holds the largest risk for your company?

1. Your cloud hosted logging platform has been compromised.

2. New OpenSSL vulnerability announced, high severity m ironically only affects latest patched version.

3. Your endpoint security product is suffering an outage can only be mitigated by disabling the security product for some time.

4. A security researcher disclosed finding Jenkins credentials for your testing environments in a pastebin dump.

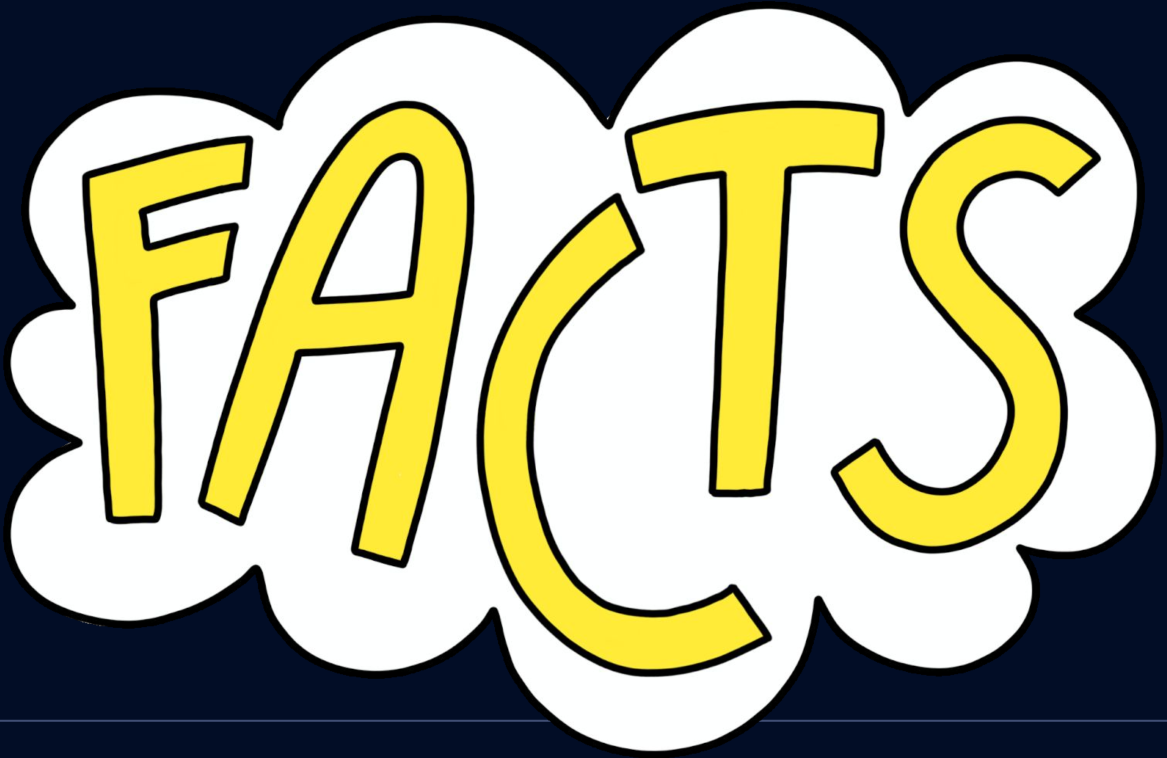
@mcdwayne

Risk Impact Analysis

Comparing known risks to determine priority of remediation efforts.

@mcdwayne

Risk Impact Analysis
Are Based On:



@mcdwayne

SPM Tools Aggregate:

- SAST
- DAST
- SCA
- IAST
- Secrets Scanning

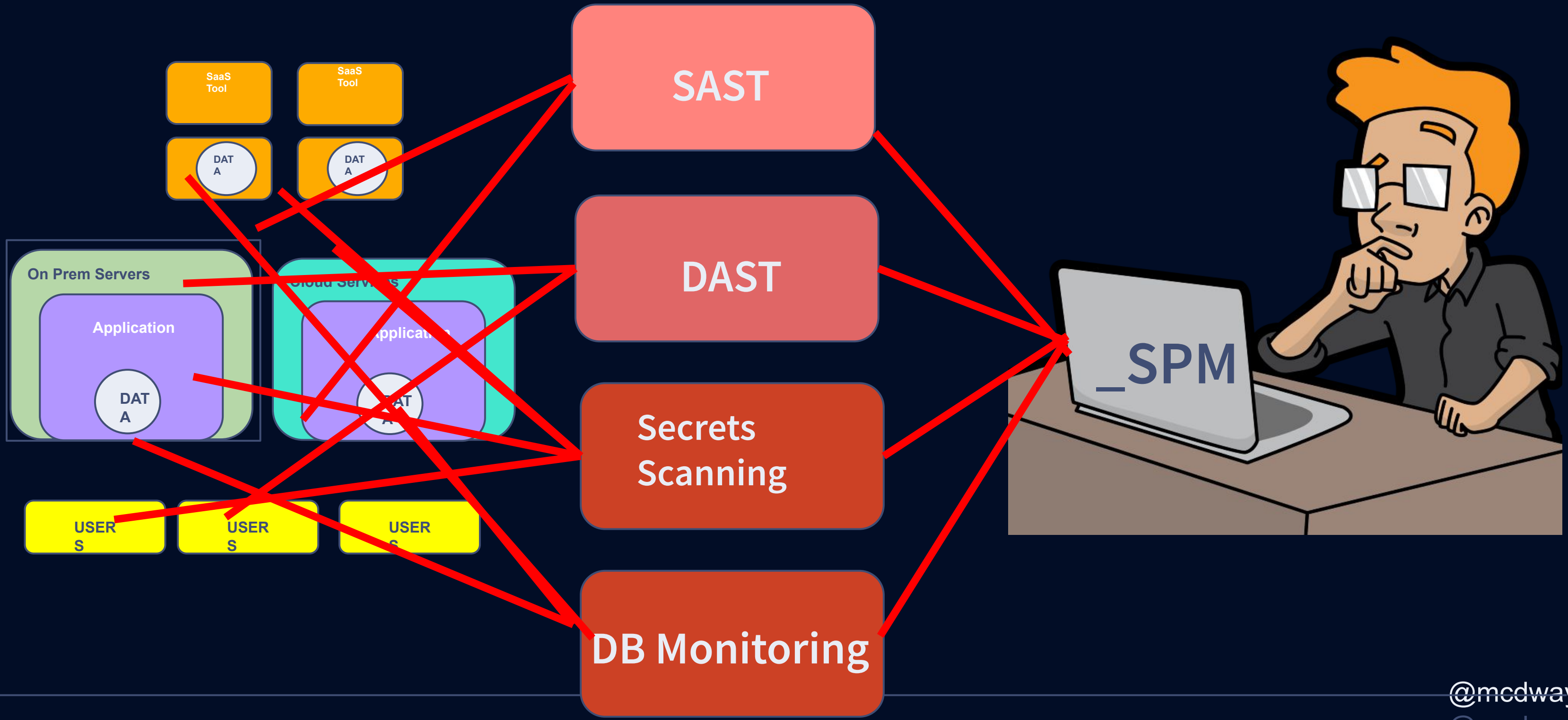
- IaC Scanning
- Network Monitoring
- Endpoint Security
- Test-Coverage Analyzers
- And more…depending on the solution

@mcdwayne

Scanners: Two Schools Of Thought

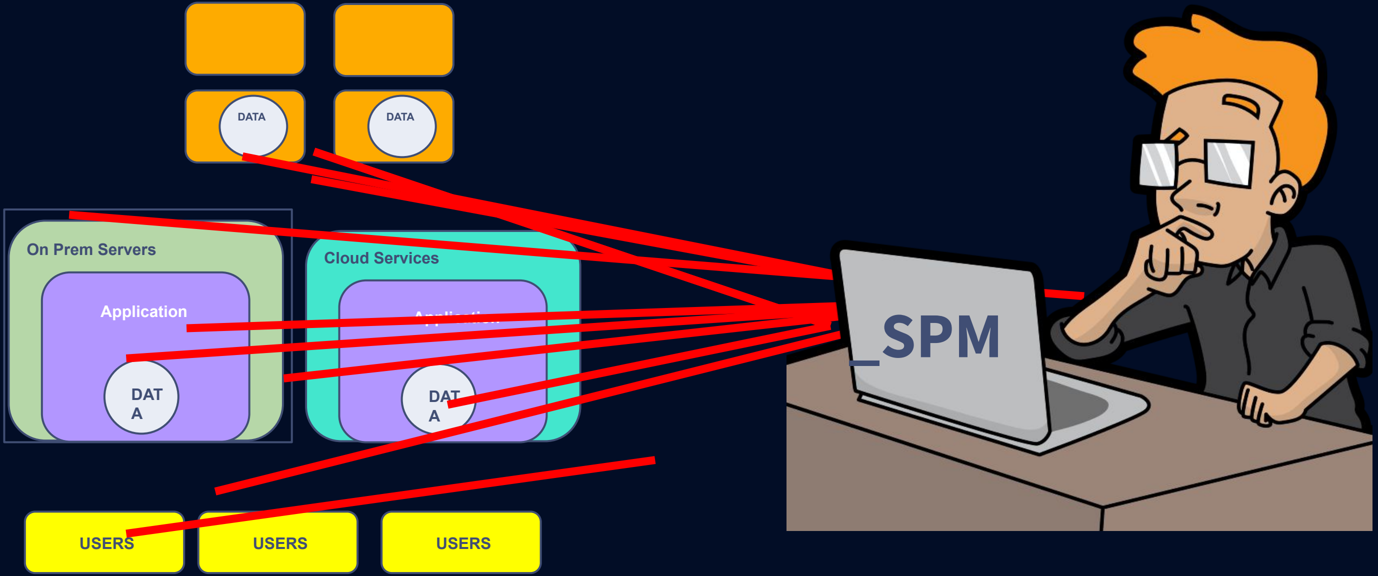
@mcdwayne

Option 1:
Use the scanners you already use



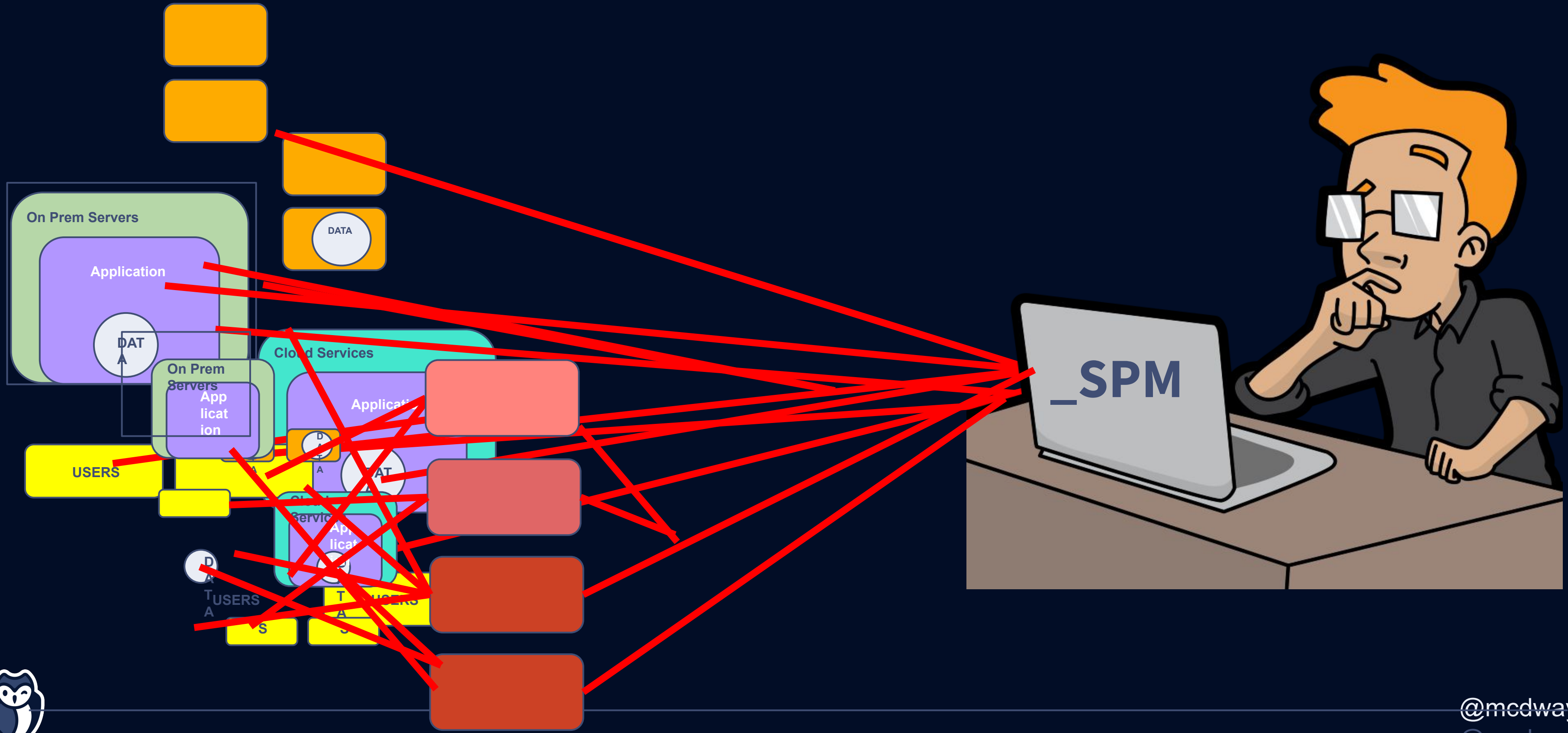
@mcdwayne

Option 2:
Use scanners built into your SPM tool



@mcdwayne

Option 3:



@mcdwayne

@mcdwayne

Bad Data = A Bad Time

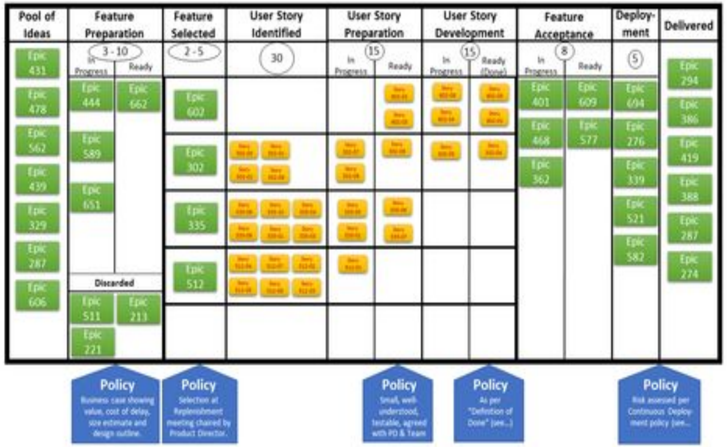
- False Positives
- False Negatives
- "Too many hops"
- Alert overload
- Looking for the wrong things

YOU FRENCH FRY WHEN YOU SHOULD PIZZA,
INSTRUCTOR
YOU'RE GONNA HAVE A BAD TIME!

@mcdwayne

Remediation Effort
❎
Risk
=
Likelihood Of Fixing

@mcdwayne



Pool of Ideas	Feature Preparation		Feature Selected	User Story Identified	User Story Preparation		User Story Development		Feature Acceptance		Deploy-ment	Delivered
	3 - 10		2 - 5	30	15		15		8		5	
	In Progress	Ready			In Progress	Ready	In Progress	Ready (Done)	In Progress	Ready		
Epic 431 Epic 478 Epic 562 Epic 439 Epic 329 Epic 287 Epic 606	Epic 444 Epic 589 Epic 651	Epic 662	Epic 602 Epic 302 Epic 335 Epic 512						Epic 401 Epic 468 Epic 362	Epic 609 Epic 577	Epic 694 Epic 276 Epic 339 Epic 521 Epic 582	Epic 294 Epic 386 Epic 419 Epic 388 Epic 287 Epic 274
	Discarded											
	Epic 511 Epic 221	Epic 213										

Policy
Business case showing value, cost of delay, size estimate and design outline.

Policy
Selection at Replenishment meeting chaired by Product Director.

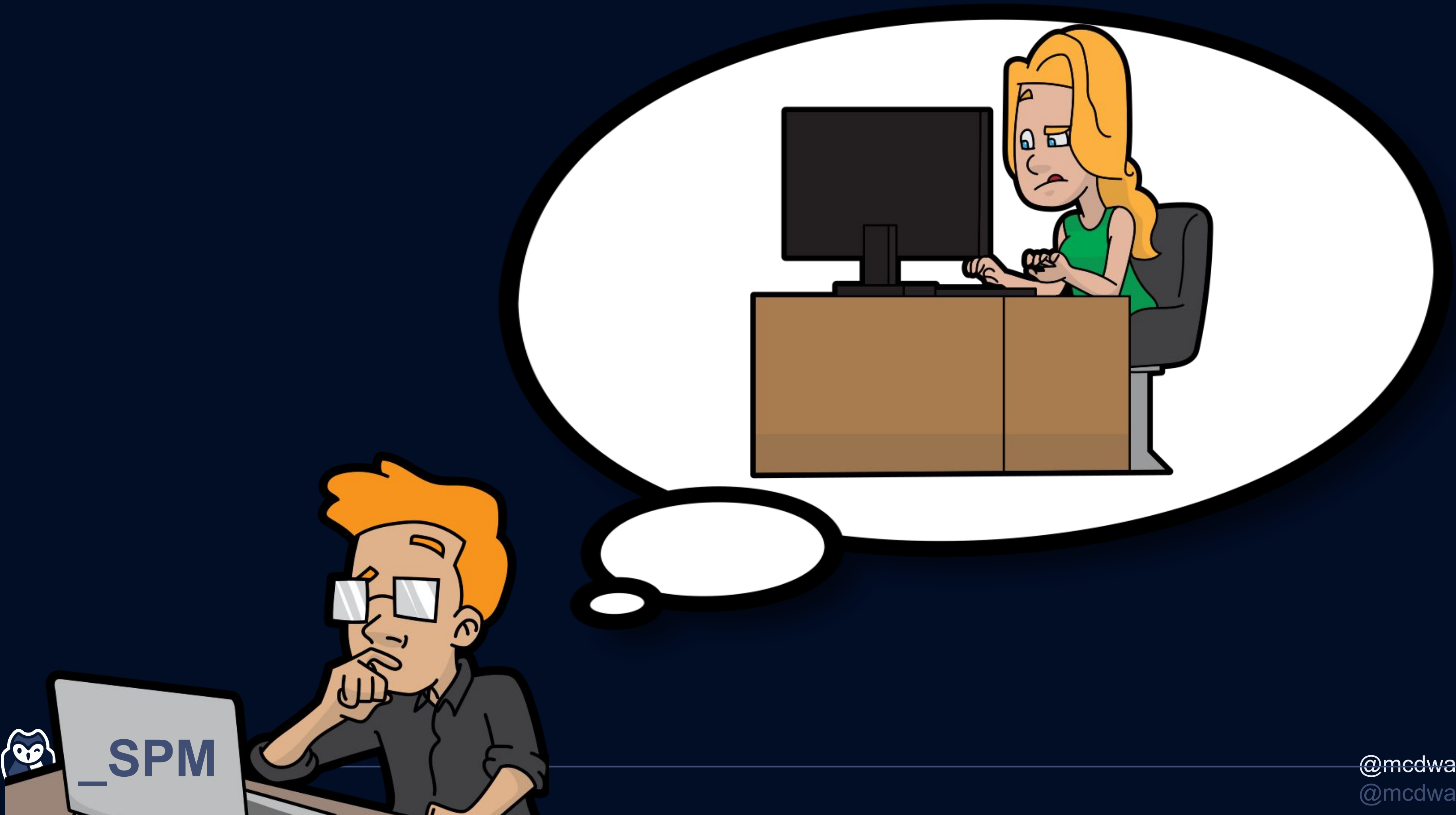
Policy
Small, well-understood, testable, agreed with PO & Team

Policy
As per "Definition of Done" (see...)

Policy
Risk assessed per Continuous Deployment policy (see...

@mcdwayne

@mcdwayne



@mcdwayne

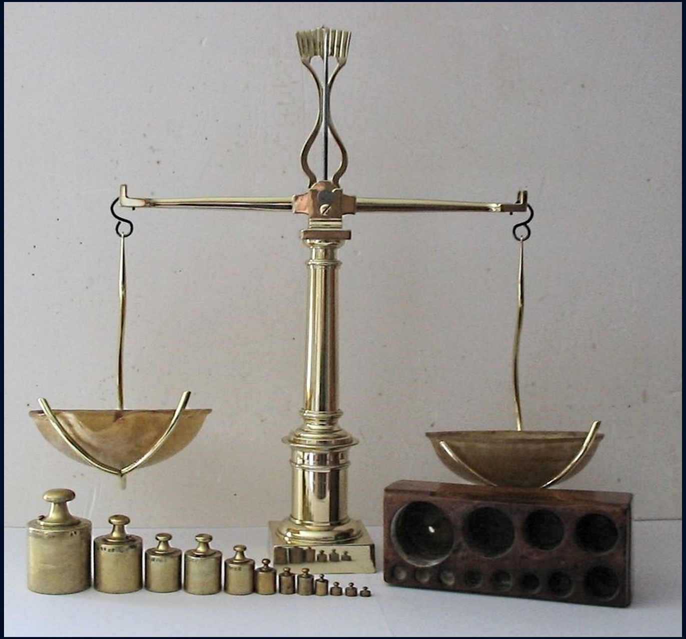
@mcdwayne

What is the best posture?

It depends…

@mcdwayne

Measuring Security == Measuring Risk



Risks are what you are set to lose if things go bad.

@mcdwayne

Security Posture Management

- Priorities - What should I work on next?
- Risk - Which incidents would be the most expensive?
- In-Context Data - How do I know I need to fix that?
- Remediation - How should I fix it?

@mcdwayne

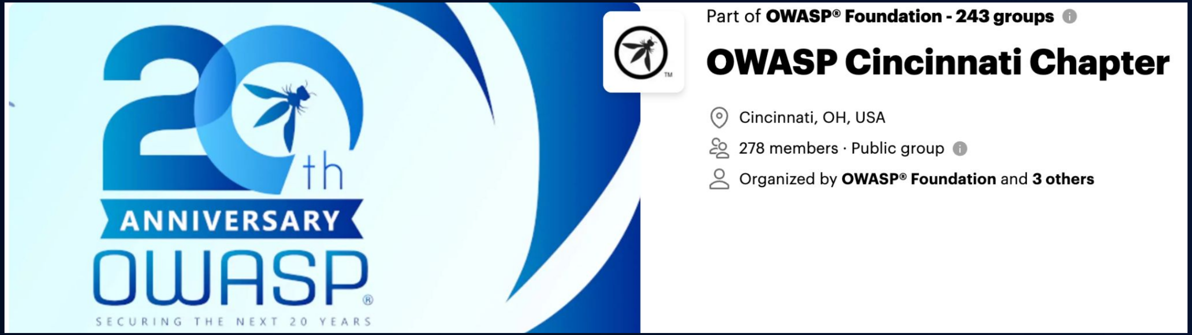
Hi. I’m Dwayne.

Dwayne McDaniel

- I live in Chicago
- I’ve been a Developer Advocate since 2016
- Co-host of The Security Repo Podcast
- On Twitter @mcdwayne
- mcdwayne@mastodon.social
- LinkedIn @dwaynemcdaniel
- Happy to chat about anything, hit me up
- Outside of tech, I love improv, karaoke and going to rock and roll shows!

@mcdwayne

Stand Up Straight
-
Security Posture And You



Part of **OWASP® Foundation - 243 groups**

OWASP Cincinnati Chapter

Cincinnati, OH, USA

278 members · Public group

Organized by **OWASP® Foundation** and **3 others**

@mcdwayne

@mcdwayne