RSA®Conference2022

Building a Security Program

(A Look in Four Dimensions)

Andy Ellis

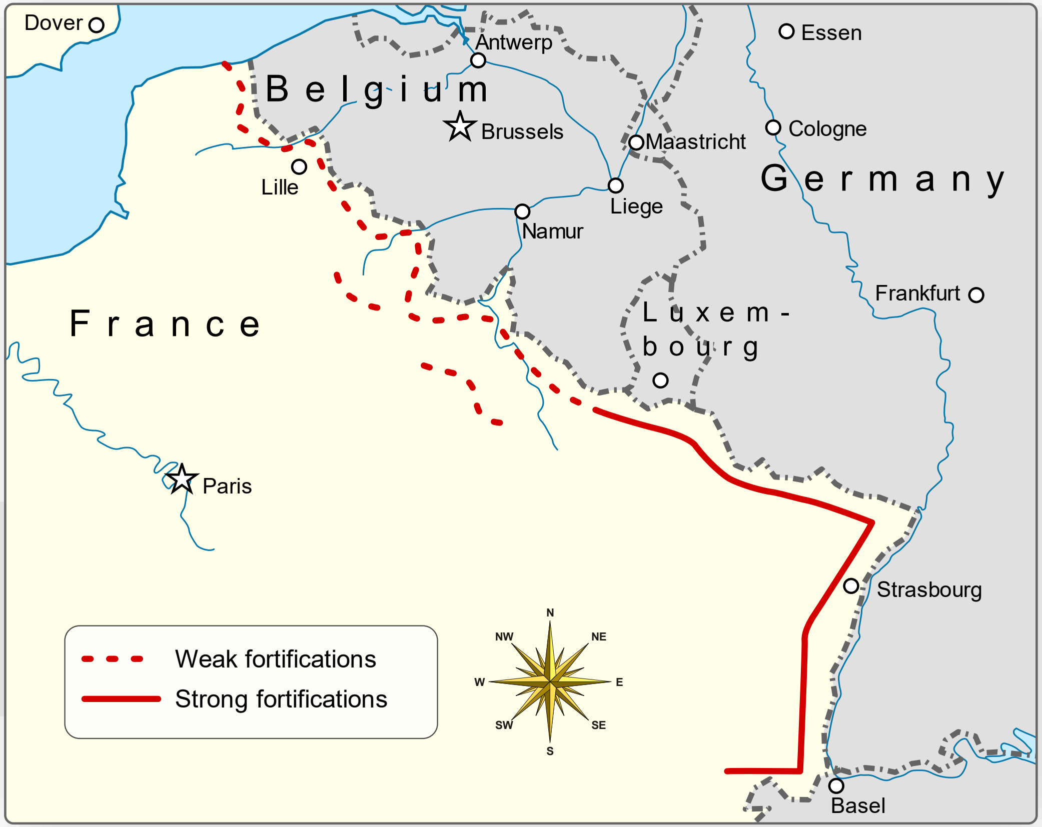
Advisory CISO, Orca Security

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.

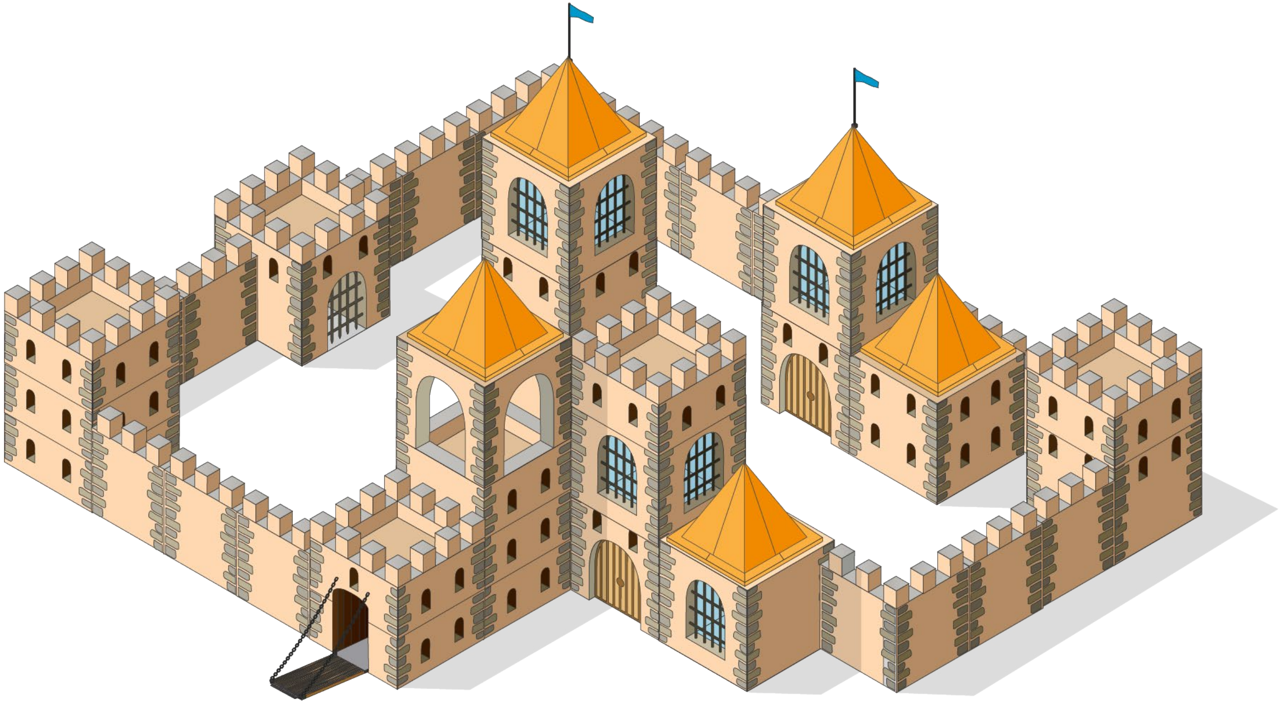
Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

“Defense in Depth”

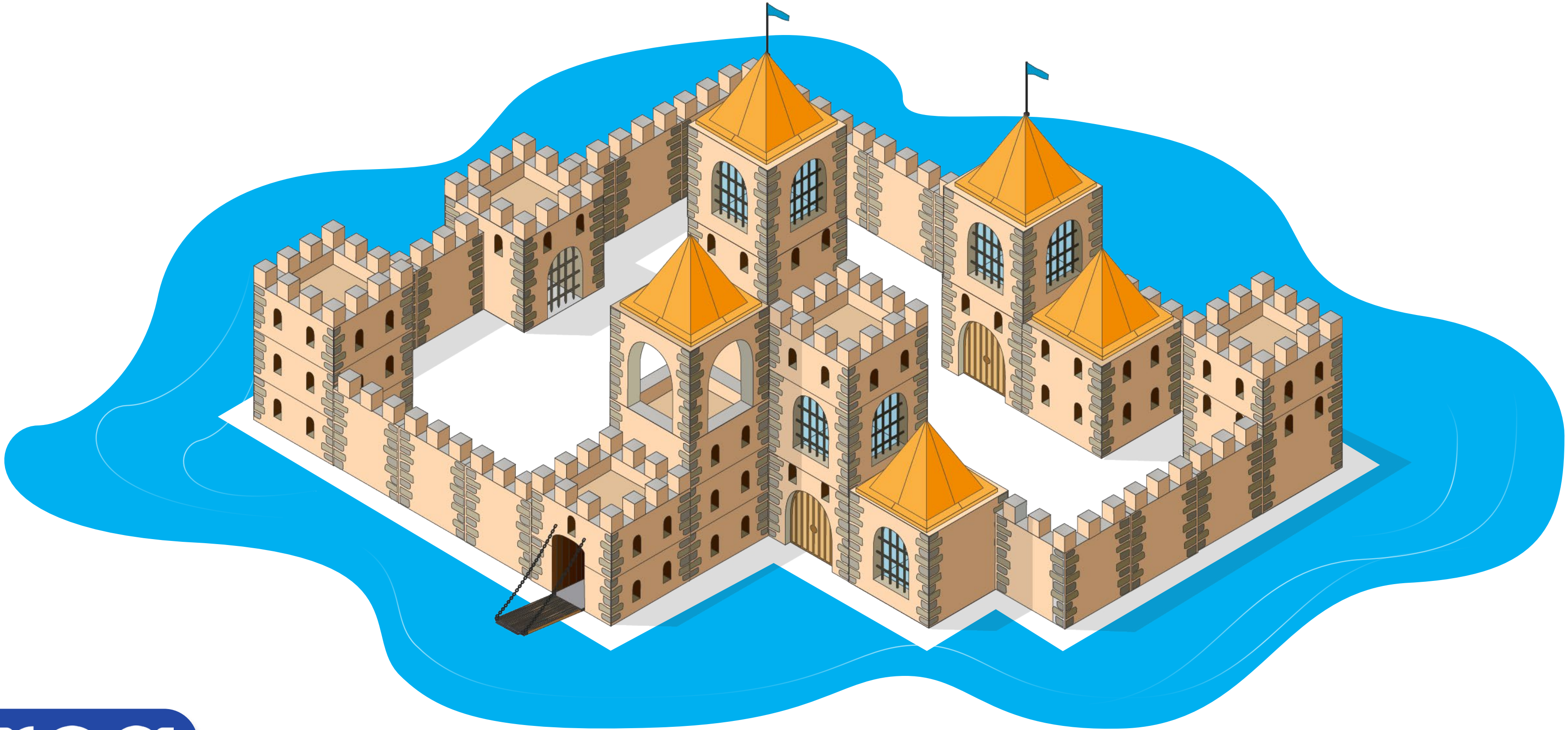


Maginot Line, CC BY-SA 4.0 Goran tek-en

The Perimeter

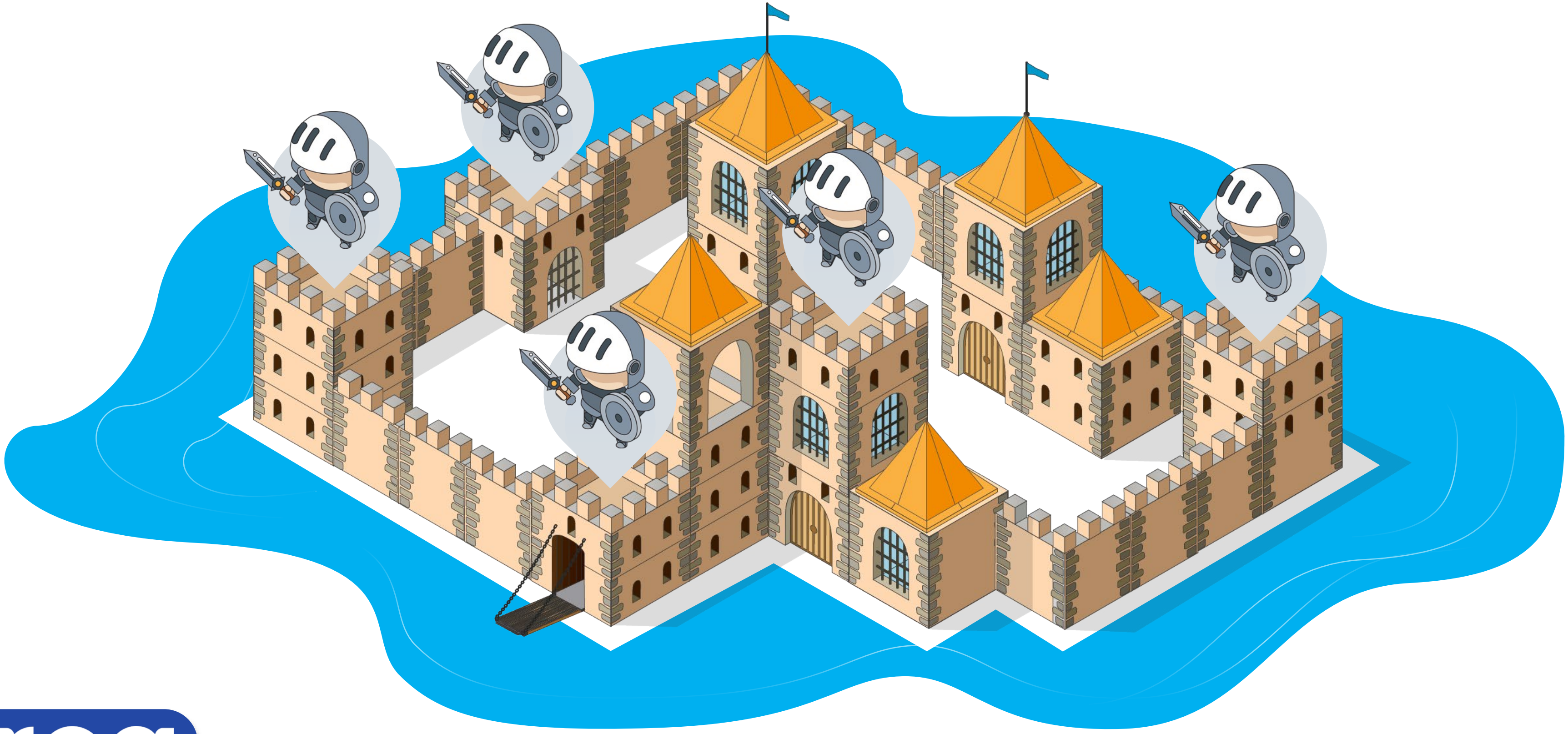


The Moat



Andy Ellis
@csoandy

Defenders



Andy Ellis
@csoandy

Even in “meatspace,” defense isn’t linear

Andy Ellis
@csoandy

APPLY!

#RSAC

Apply: Vulnerability Management

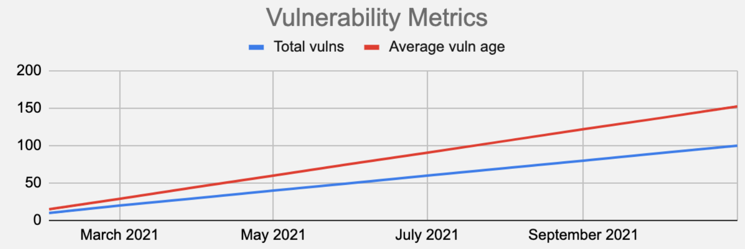
Review the current metric

Step 1: Challenge the Definition

- What systems aren't covered?
- What vulnerabilities aren't counted?
- What less relevant vulnerabilities are counted?

Patching Vulnerabilities

- **Average Age of Open Vulnerabilities**



- **Definition:** Defect measurement: How long have current vulnerabilities been unpatched

Charts from: https://www.csoonline.com/article/3648997/vulnerabilities-dont-count.html

orca security

Andy Ellis
@csoandy

APPLY!

#RSAC

Apply: Vulnerability Management

Review the current metric

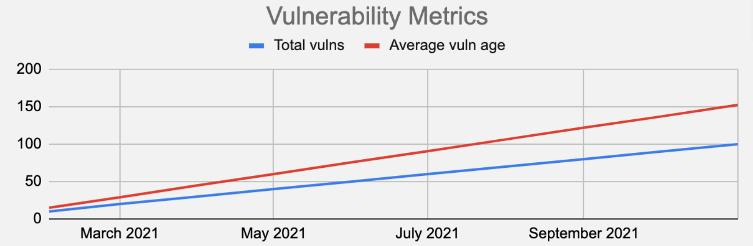
Step 1: Challenge the Definition

- What systems aren’t covered?
- What vulnerabilities aren’t counted?
- What less relevant vulnerabilities are counted?

Charts from: https://www.csoonline.com/article/3648997/vulnerabilities-dont-count.html

Patching Vulnerabilities

- **Average Age of Open Vulnerabilities**



- **Definition:** Defect measurement: How long have current vulnerabilities been unpatched

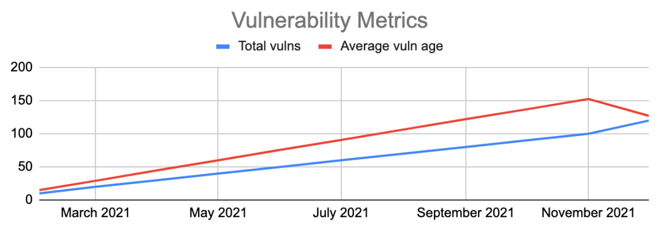
Andy Ellis
@csoandy

Apply: Vulnerability Management

Break the current metric

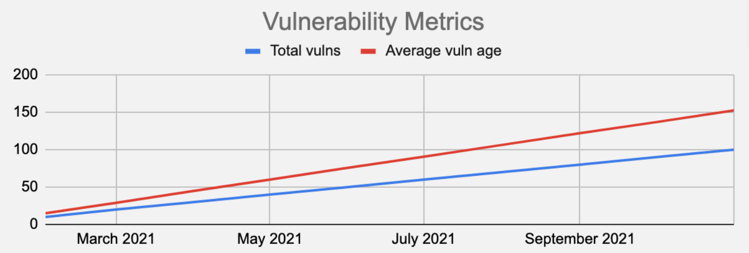
Step 1: Challenge the Definition

Step 2: Roundtable: What If?



Patching Vulnerabilities

Average Age of Open Vulnerabilities



Definition: Defect measurement: How long have current vulnerabilities been unpatched

What if we don't patch log4j?

APPLY!

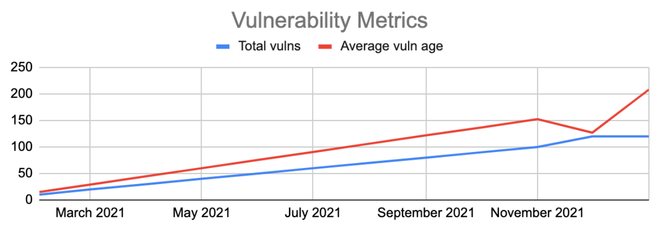
#RSAC

Apply: Vulnerability Management

Break the current metric

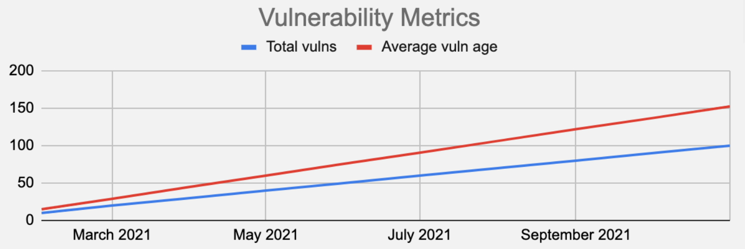
Step 1: Challenge the Definition

Step 2: Roundtable: What If?



Patching Vulnerabilities

Average Age of Open Vulnerabilities



Definition: Defect measurement: How long have current vulnerabilities been unpatched

What if we patch log4j after a month?

orca security

Andy Ellis
@csoandy

RSAConference2022

APPLY!

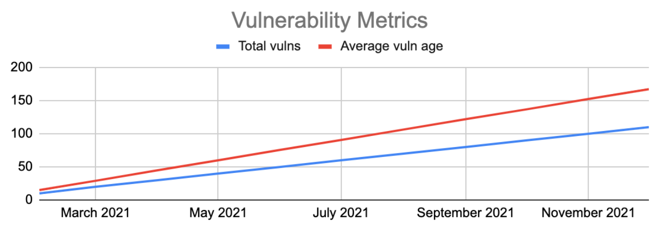
#RSAC

Apply: Vulnerability Management

Break the current metric

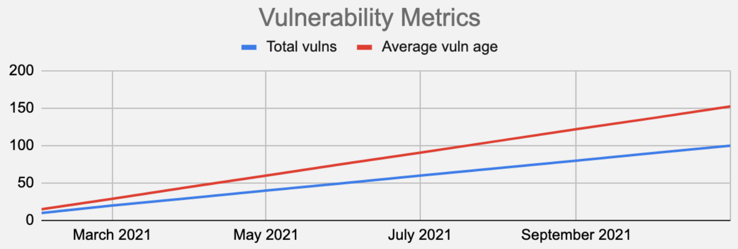
Step 1: Challenge the Definition

Step 2: Roundtable: What If?



Patching Vulnerabilities

Average Age of Open Vulnerabilities



Definition: Defect measurement:
How long have current
vulnerabilities been unpatched

What if we patch log4j between reporting intervals?

orca security

Andy Ellis
@csoandy

Apply: Vulnerability Management

Consider new metric

Step 1: Challenge the Definition

Step 2: Roundtable: What If?

Step 3: Ask what you're trying to measure

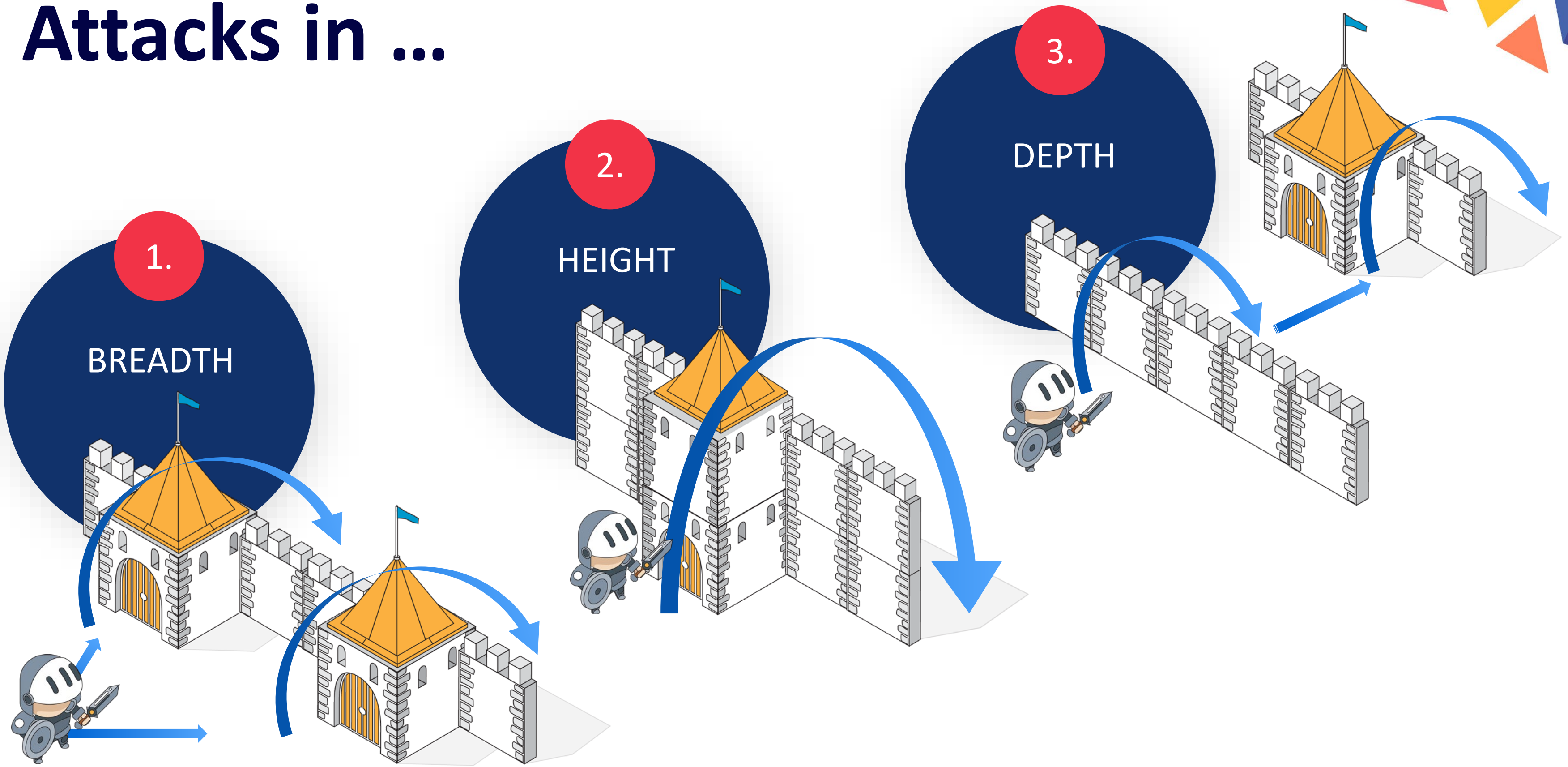
Vulnerabilities

Patch SLA measurement

Critical	High	Medium	Low
7 days	30 days	90 days	180 days
85%	70%	50%	40%

Definition: How many vulnerabilities are patched within expected window?

Attacks in …



Defenses need to meet attackers…

Building a security program without considering how an adversary will try to penetrate it?

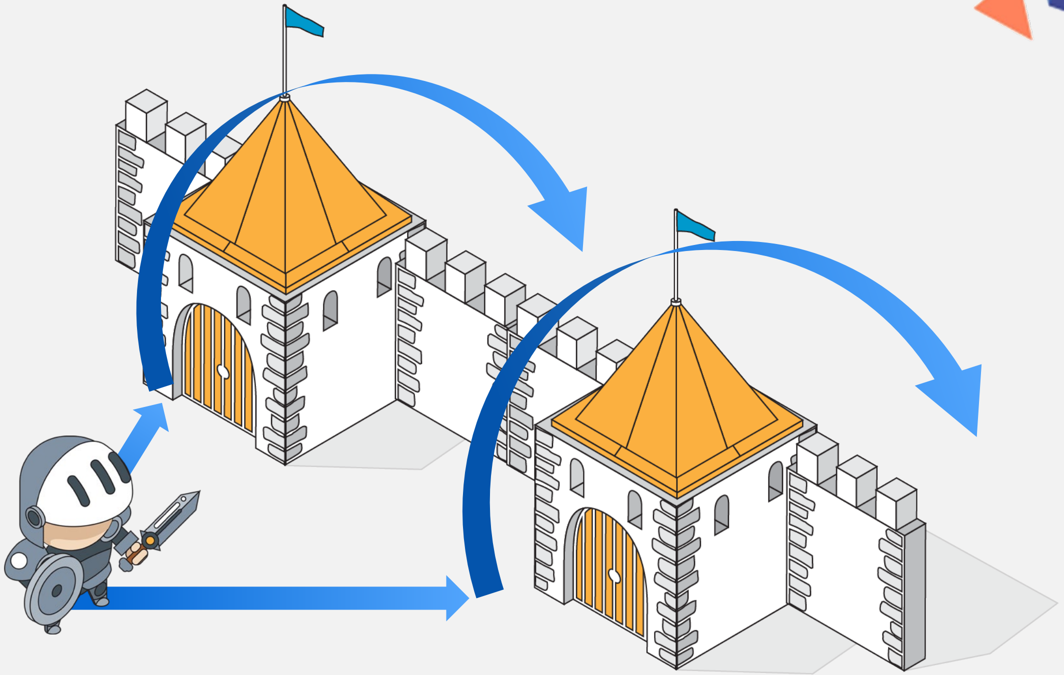
That's just a Cyber Maginot Line.

So how do we approach this challenge?

Dimension 1: Breadth / Width

Since the adversary can choose their point of entry:

Defenders must have complete *coverage* of all of their assets, *especially* if they aren't well maintained.



APPLY!

Coverage: Asset Classes

- Step 1: **List types of Assets**
- Step 2: **Count your Assets**
- Step 3: **Document ease of data collection**

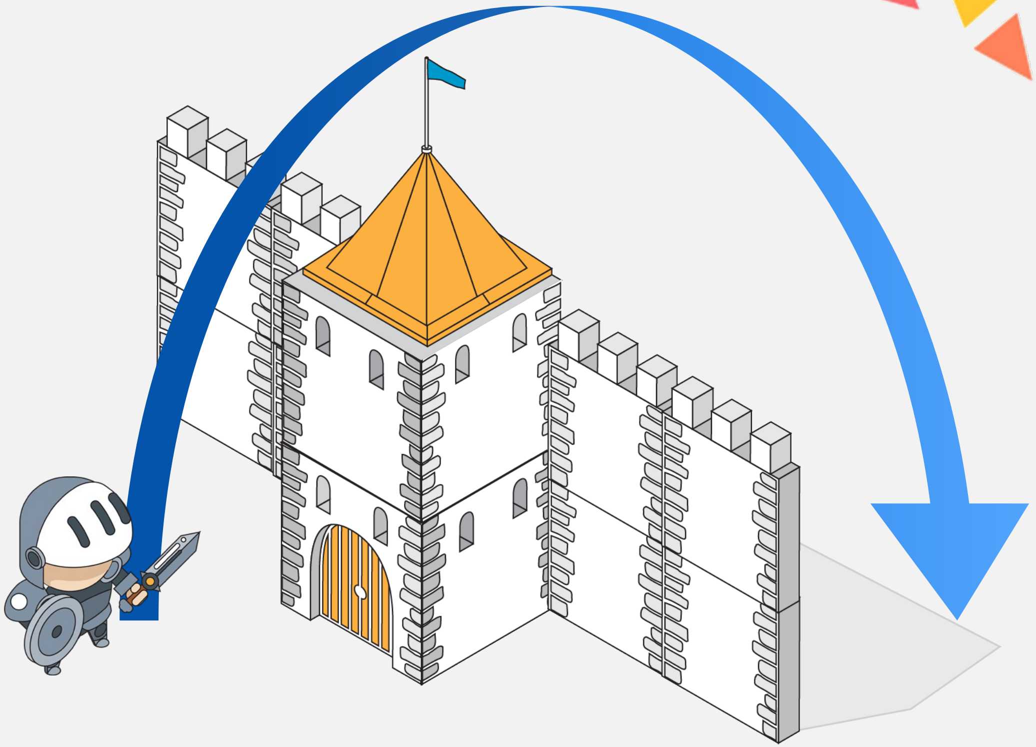
○: Easy, automated
◐: Some manual effort
●: Lots of human effort

Public Cloud	**152,435**	○
Production Servers	**3,000**	◐
Dev/Build Servers	**????**	●
Enterprise Endpoints	**9,267**	◐
Enterprise Servers	**352**	○
SaaS Services	**500+**	●

Dimension 2: Height

Since the adversary can quickly jump through security systems:

Defenders must know how *comprehensive* their defenses are, and how they "stack."



Andy Ellis
@csoandy

APPLY!

Comprehensive: Defenses

For each asset:

- Step 1: **Define Controls**
- Step 2: **Define process measurements**
- Step 3: **Document process maturity**

○: No executive required
◐: Some executive oversight
●: No process

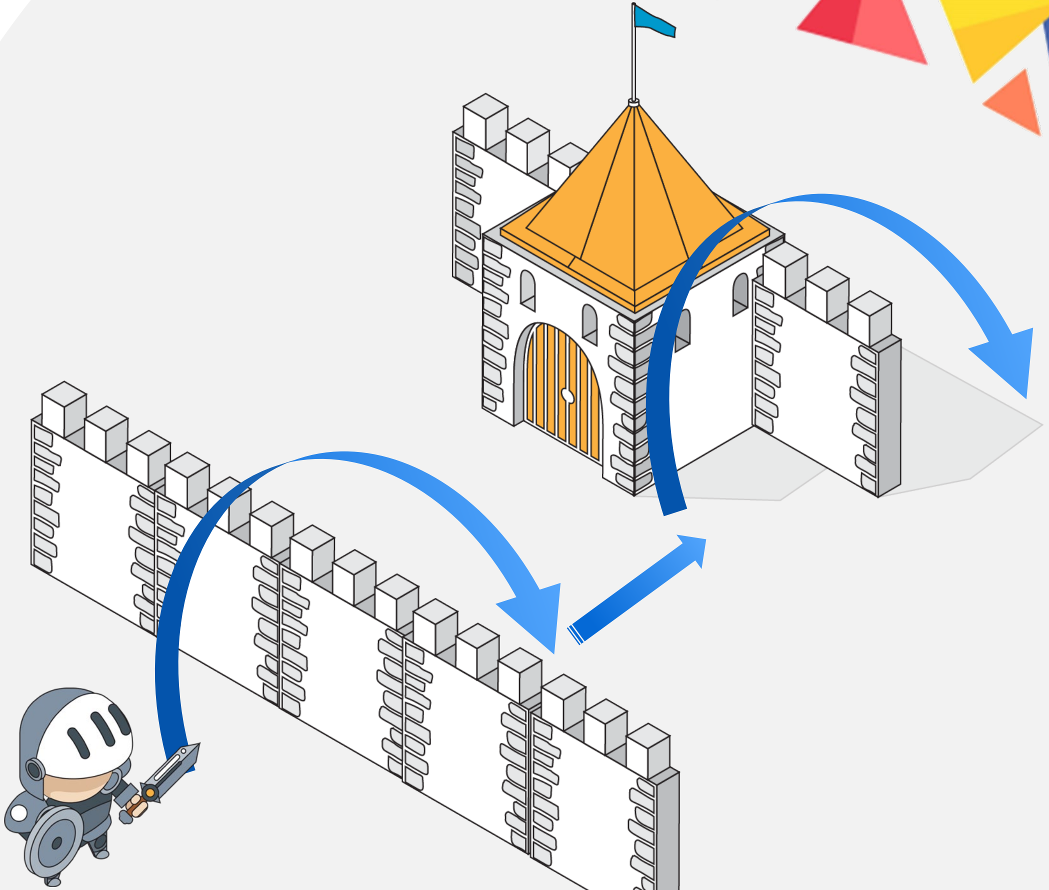
Public Cloud

Inventory	**152,435**	○
Vulnerability Mgmt	**@SLA 10%** **H/M/L: 7/30/90 days**	●
Config Hygiene	**High: 0** **Med: 50** **Low: 18,889**	◐
Authentication	**User MFA: 100%** **Machine IDs: 50%**	◐
Access Control	**Grants utilized: 82%**	○
Exploit Monitoring	**Dwell Time: 82 days**	●
Data Protection	**????**	

Dimension 3: Depth

Since the adversary will laterally move in your environment:

Defenders need the *context* of what is accessible to your front-end systems.



Andy Ellis
@csoandy

Context: Attack Scenarios

For any attack type:

Step 1: Define effective defenses

Step 2: Define incident response needs

Step 3: Narrate existing controls in this context

Ransomware

Stopped by:

- MFA
- Removal of lateral admin privileges

Mitigated by:

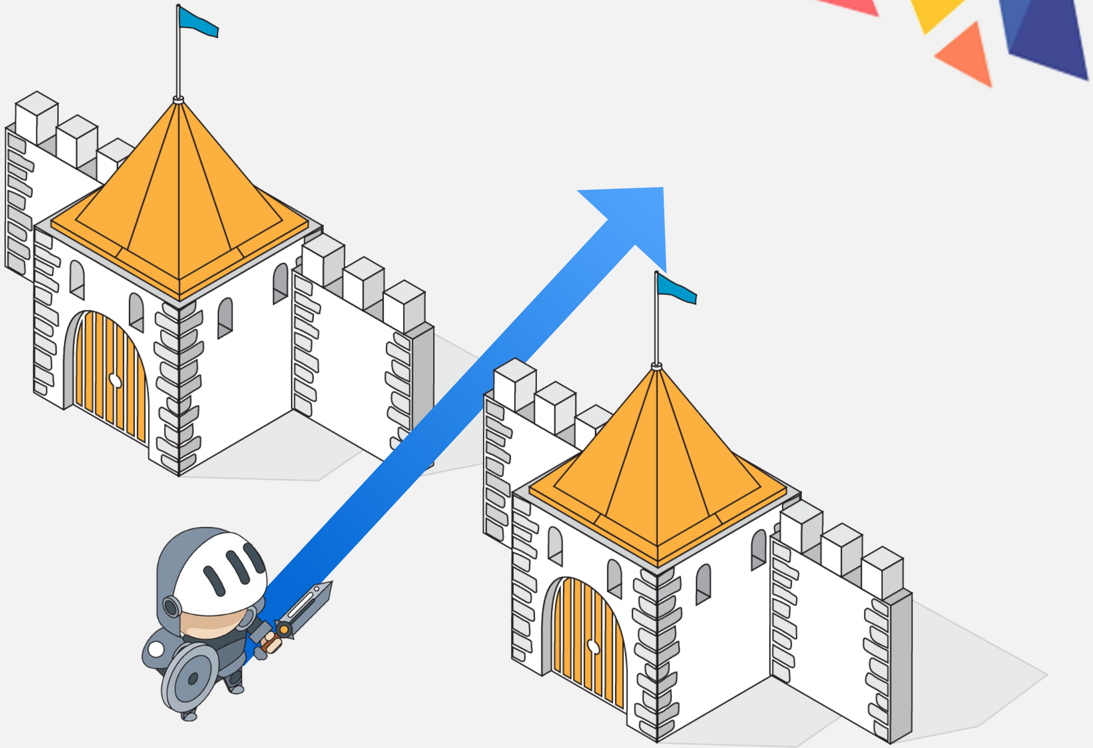
- Data backups

"We use FIDO-MFA, we've implemented three-tiered AD administration, and we've eliminated central jump servers."

Dimension 4: Time

Since the adversary can wait until you aren’t watching:

Defenders need to ensure the *continuity* of all defensive controls.



APPLY!

Continuity: Do your processes mature?

For any security control:

Step 1: Define and measure over-time efficacy

Step 2: Define improvement “missions” to mature the controls

Step 3: Track responsiveness to deviations from norms

Vulnerability

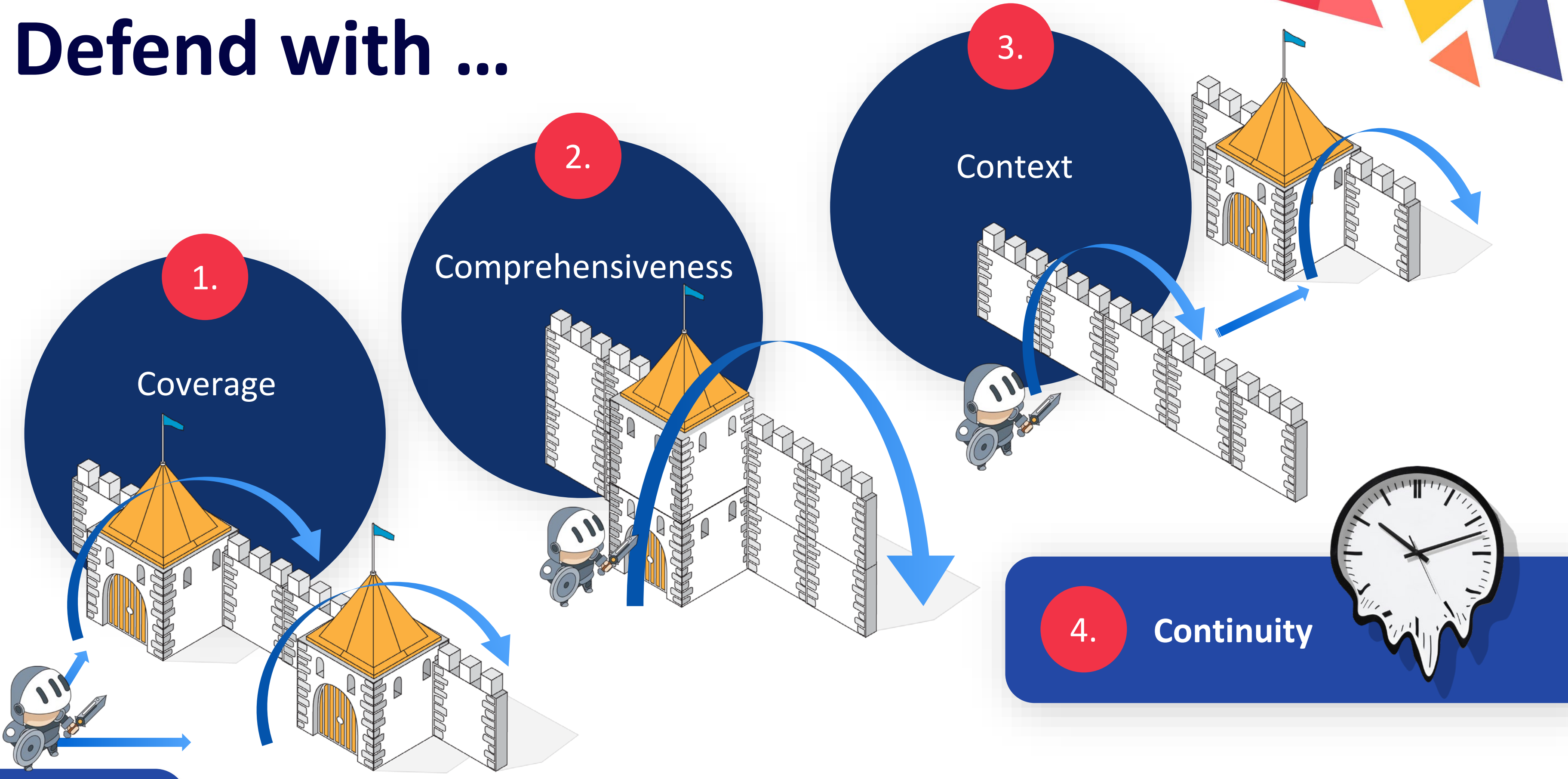
- **Patch SLAs:**

Critical	High	Medium	Low
7 days	30 days	90 days	180 days
85%	70%	50%	40%

- **Mission:** Improve build process to reduce software rollout latency by 5 days.

How many SLA violations were escalated before SLA was broken?

Defend with ...



1. Coverage

2. Comprehensiveness

3. Context

4. Continuity

APPLY!

Apply: Assess your metrics

Stop measuring activity, and start measuring *effectiveness over time*

Identify the assets that your metrics don't apply to!

Find the "unimportant" assets connected to important assets

#RSAC

RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **STR-W01**

Building a Security Program
(A Look in Four Dimensions)

Andy Ellis

Advisory CISO,
Orca Security