How to CISO in the Cloud

Andy Ellis

Advisory CISO, Orca Security

CHALLENGE: Securing Everything you Have in the Cloud

Cloud Security Posture Management

• Asset Inventory • Compliance Reporting • Continuous Cloud Configuration Assessment

Cloud Infrastructure Entitlement Management

• Entitlement Risk Management & Permissions Analysis • IAM Policies • IDP Integrations

Cloud Workload Protection

• Vulnerability Management • Workload Compliance • Log Inspection • Malware Analysis

Kubernetes Security Posture Management

• K8s Benchmarks and Compliance • K8s Control Plane Assessment

Shift Left Security

• Container Image Scanning • IaC Scanning • CI/CD Integrations

Cloud Data Security

• PII Analysis • Exposure Scanning • Asset Inventory

Cloud Detection & Response

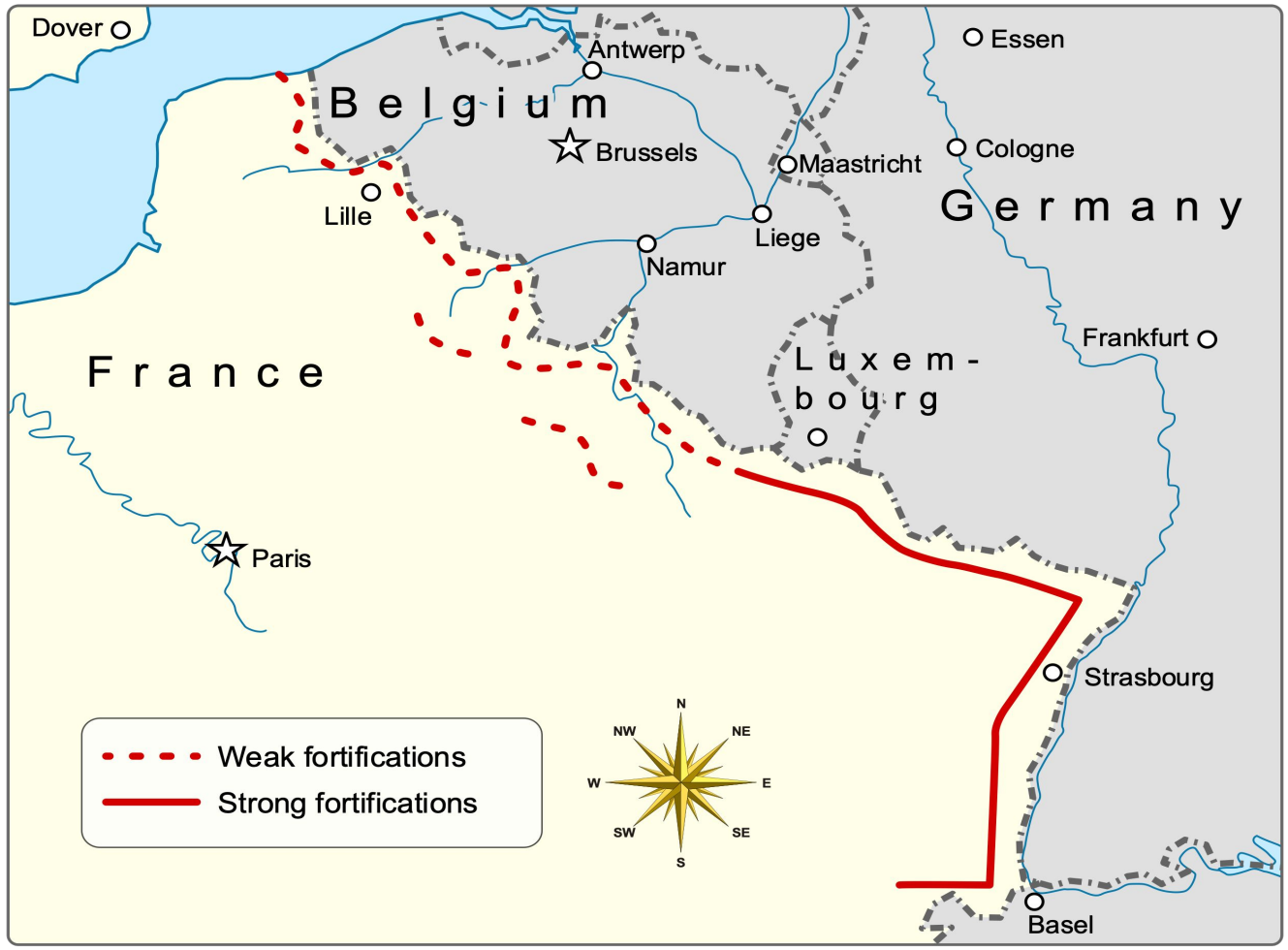
• Attack Path Analysis • Agentless Breach Detection

API Security

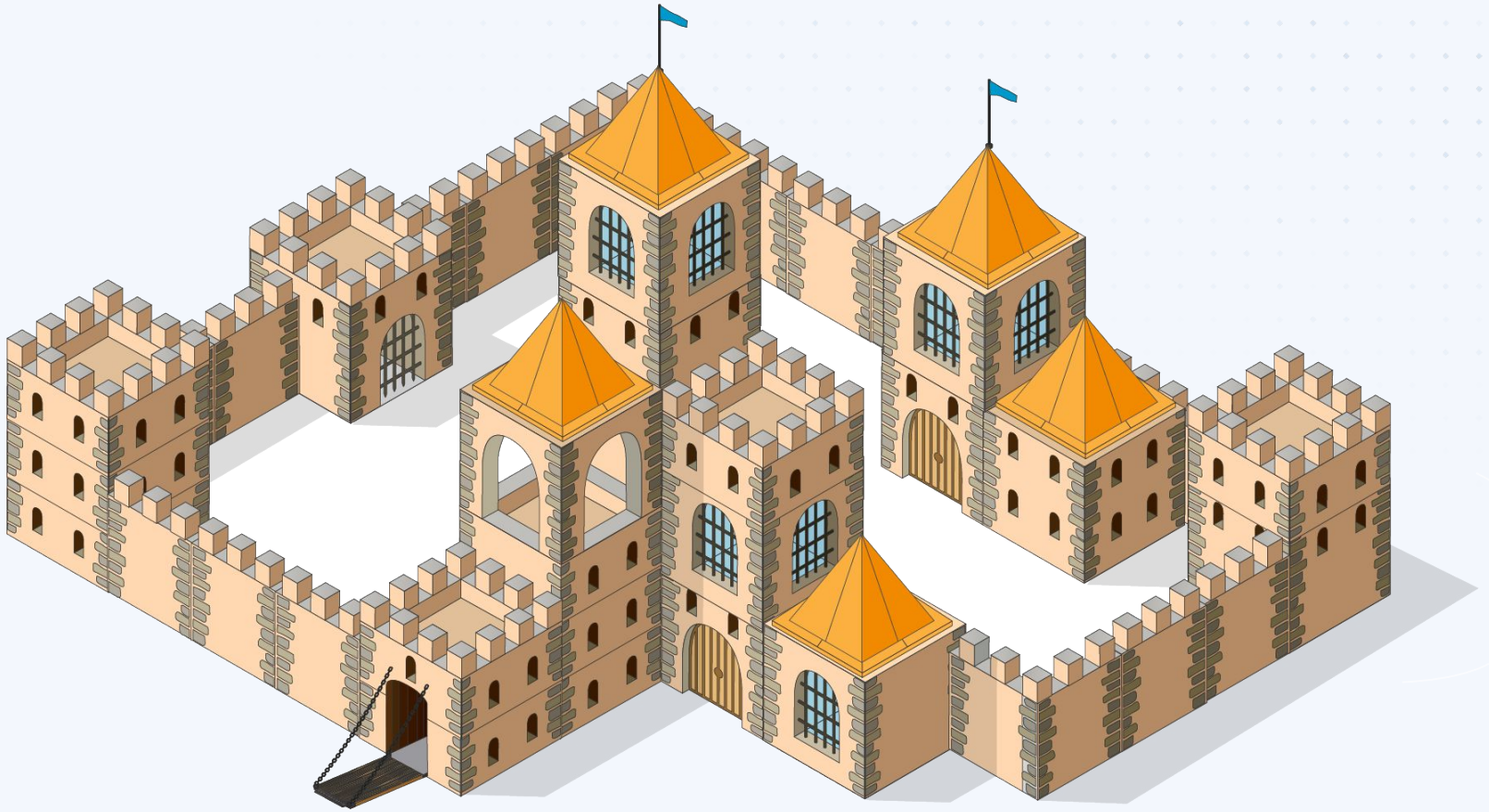
• API Inventory • Exposure Identification & Risk Analysis

“Defense in Depth”

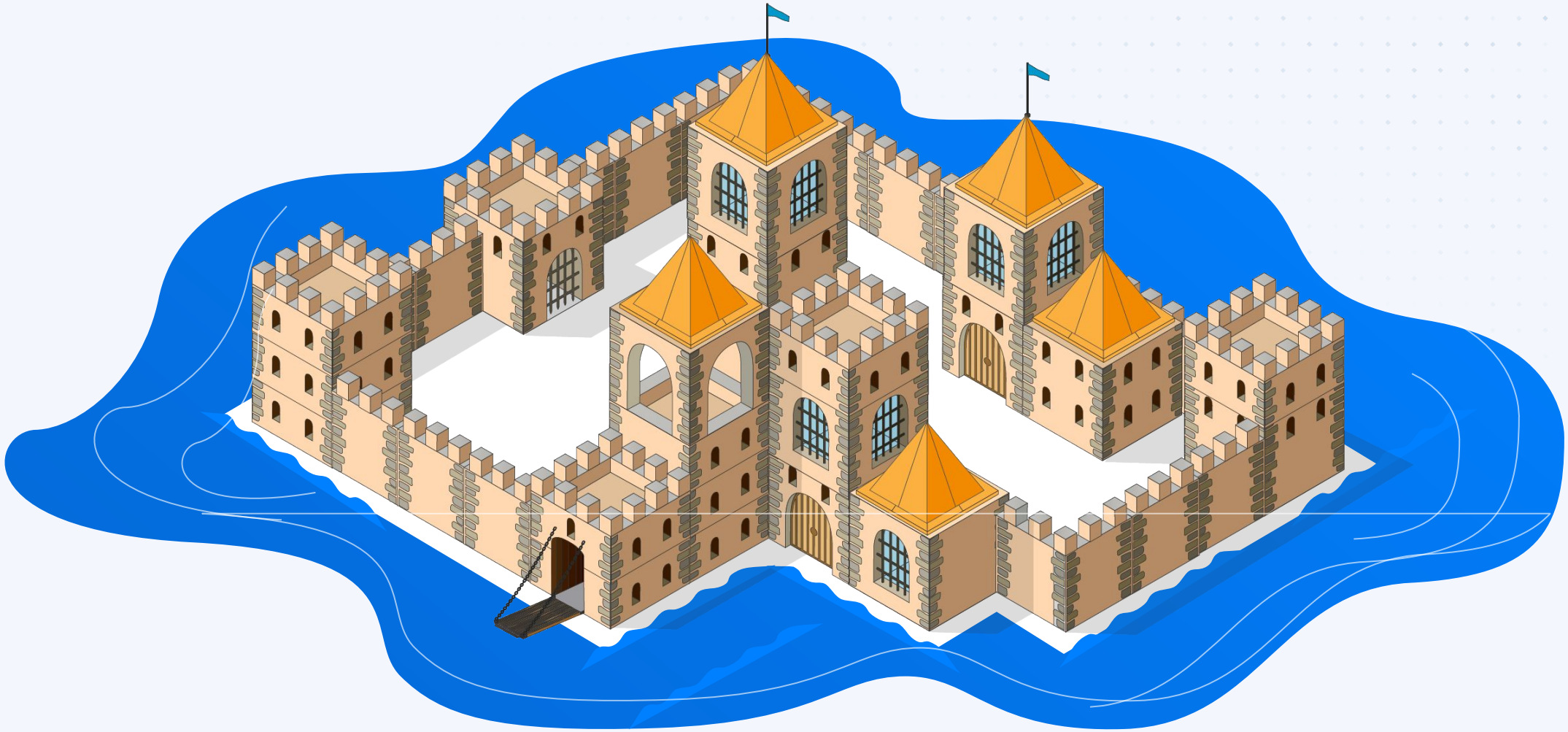
Maginot Line, CC BY-SA 4.0 Goran tek-en



The Perimeter



The Moat



Defenders

Metric Exploration: Vulnerability Management

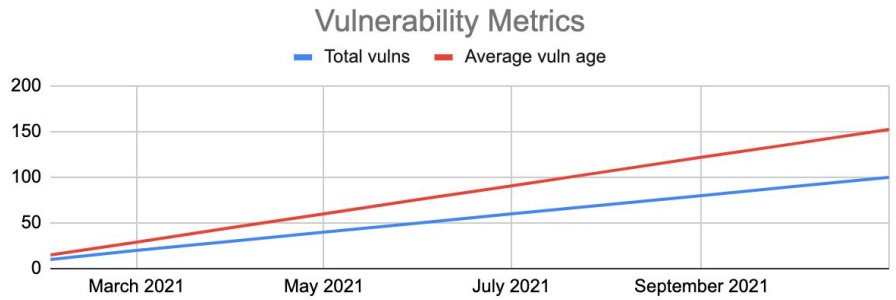
REVIEW THE CURRENT METRIC

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?

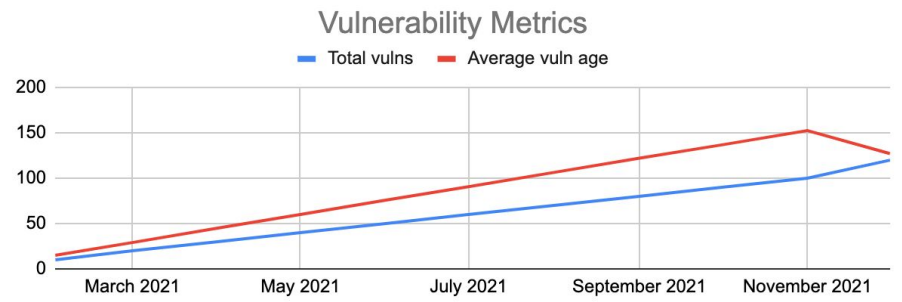
Charts from: https://www.csoonline.com/article/3648997/vulnerabilities-dont-count.html

Metric Exploration: Vulnerability Management

BREAK THE CURRENT METRIC

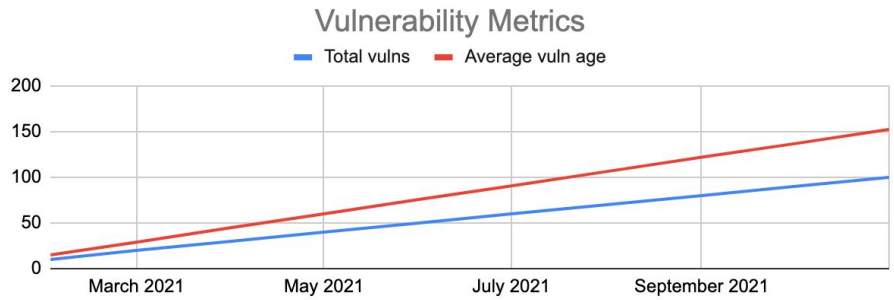
Step 1: Challenge the Definition

Step 2: Roundtable: What If?



PATCHING VULNERABILITIES

- Average Age of Open Vulnerabilities



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

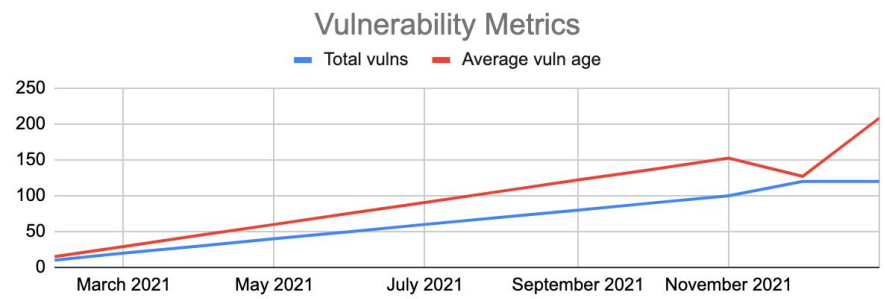
What if we don't patch at all?

Metric Exploration: Vulnerability Management

BREAK THE CURRENT METRIC

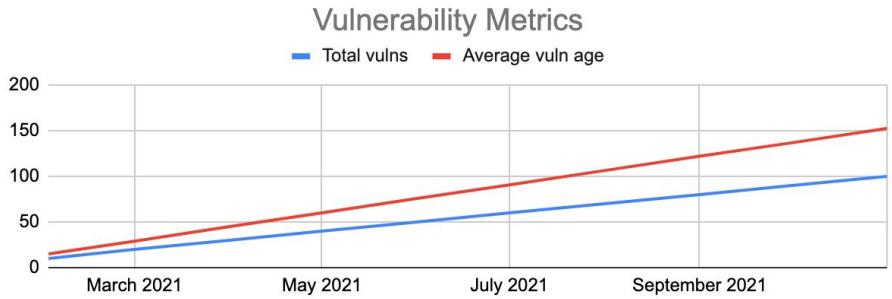
Step 1: Challenge the Definition

Step 2: Roundtable: What If?



PATCHING VULNERABILITIES

- Average Age of Open Vulnerabilities



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

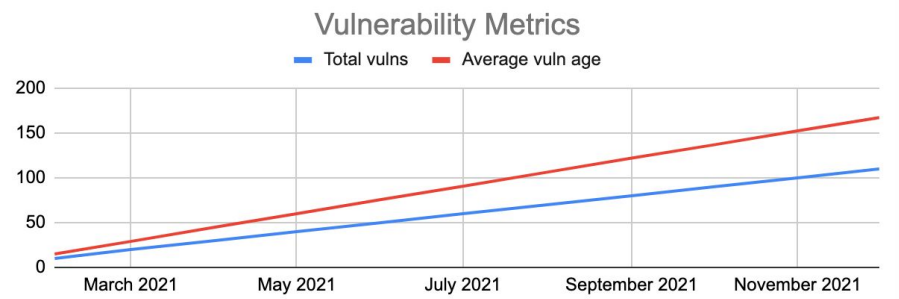
What if we patch after a month?

Metric Exploration: Vulnerability Management

BREAK THE CURRENT METRIC

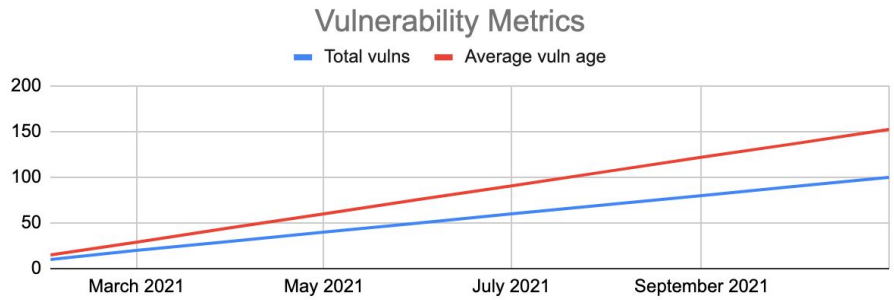
Step 1: Challenge the Definition

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 patched between reporting windows?

Metric Exploration: 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?

To defend your business, understand it

Physical Goods

- Manufacturing
- Electronic Hardware

Customer-Focused Services

- Health Care
- Financial Services
- Education

Software

- Packaged Software
- SaaS

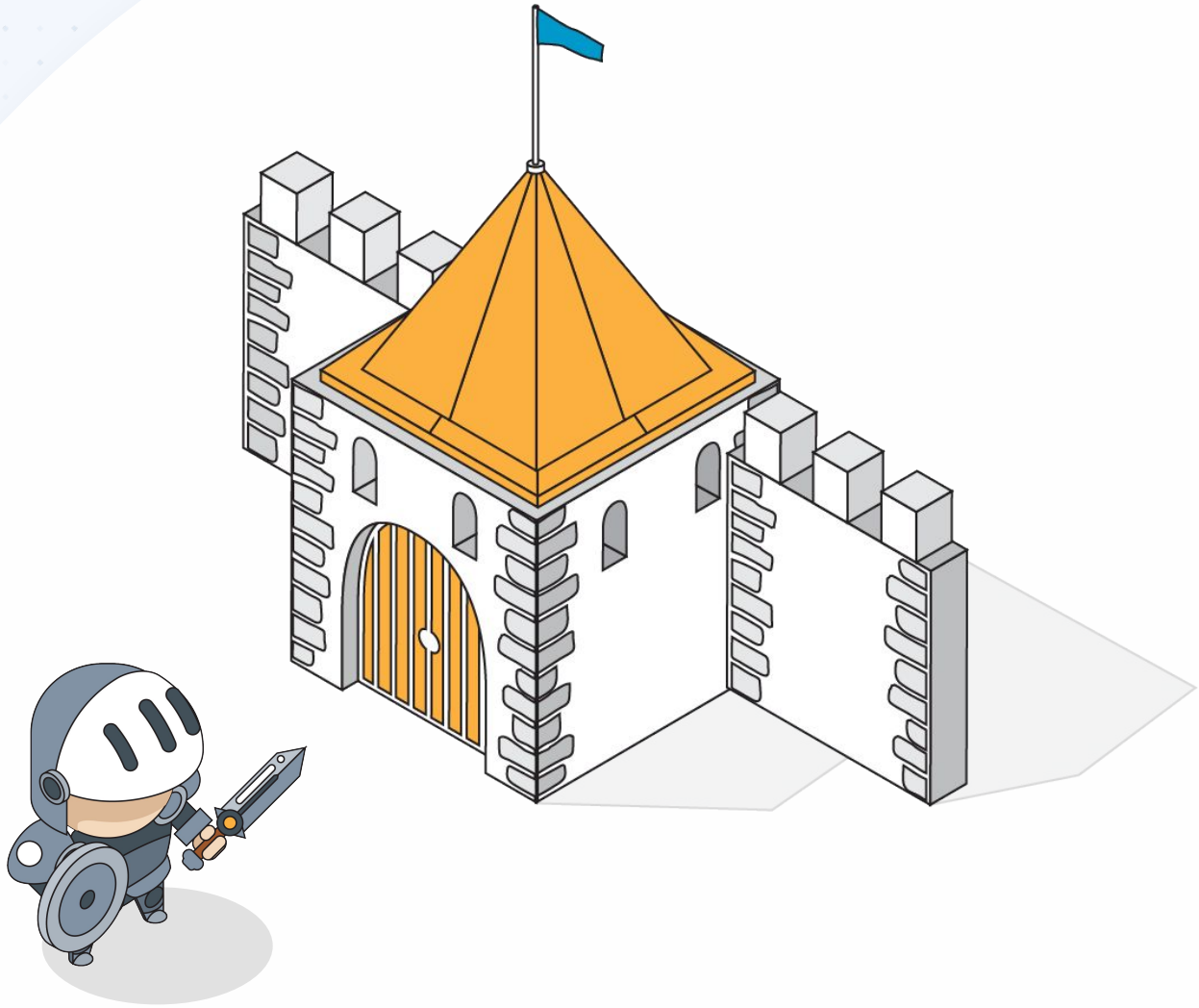
Retail

- Internet Sales
- Stores

Professional Services

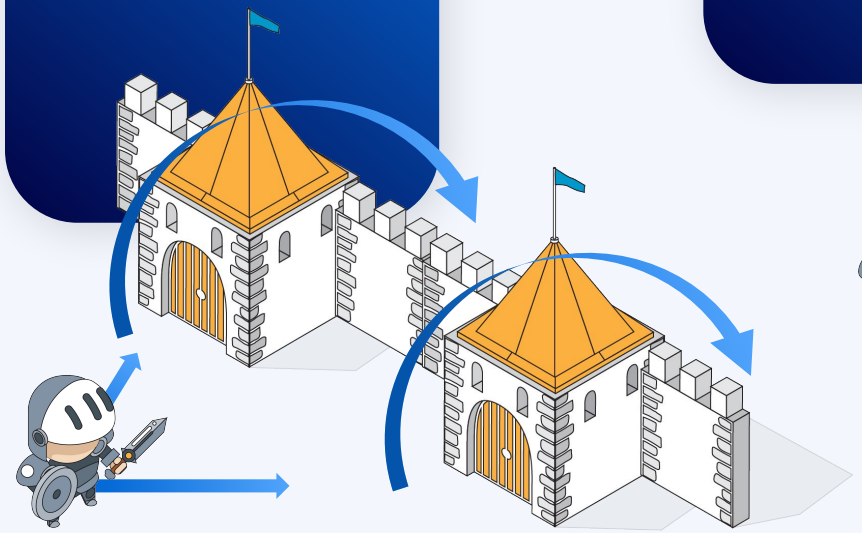
- In-person
- Managed Services

Even in “meatspace,” defense isn’t linear

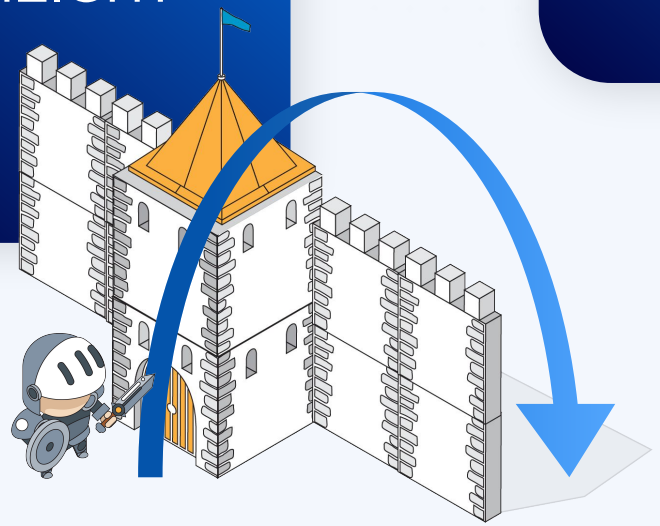


Attacks in …

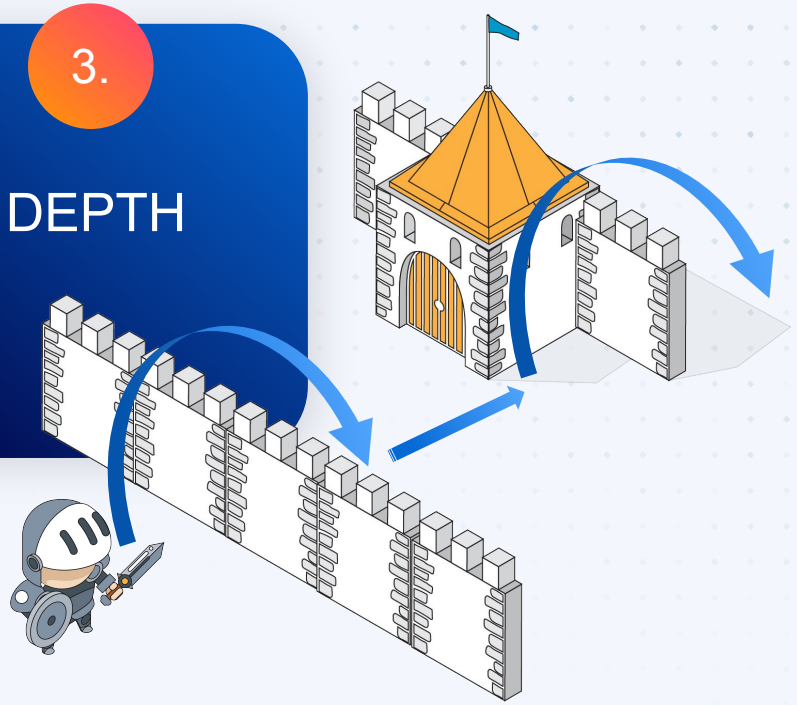
1. BREADTH



2. HEIGHT



3. DEPTH



Defenses need to meet attackers…

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

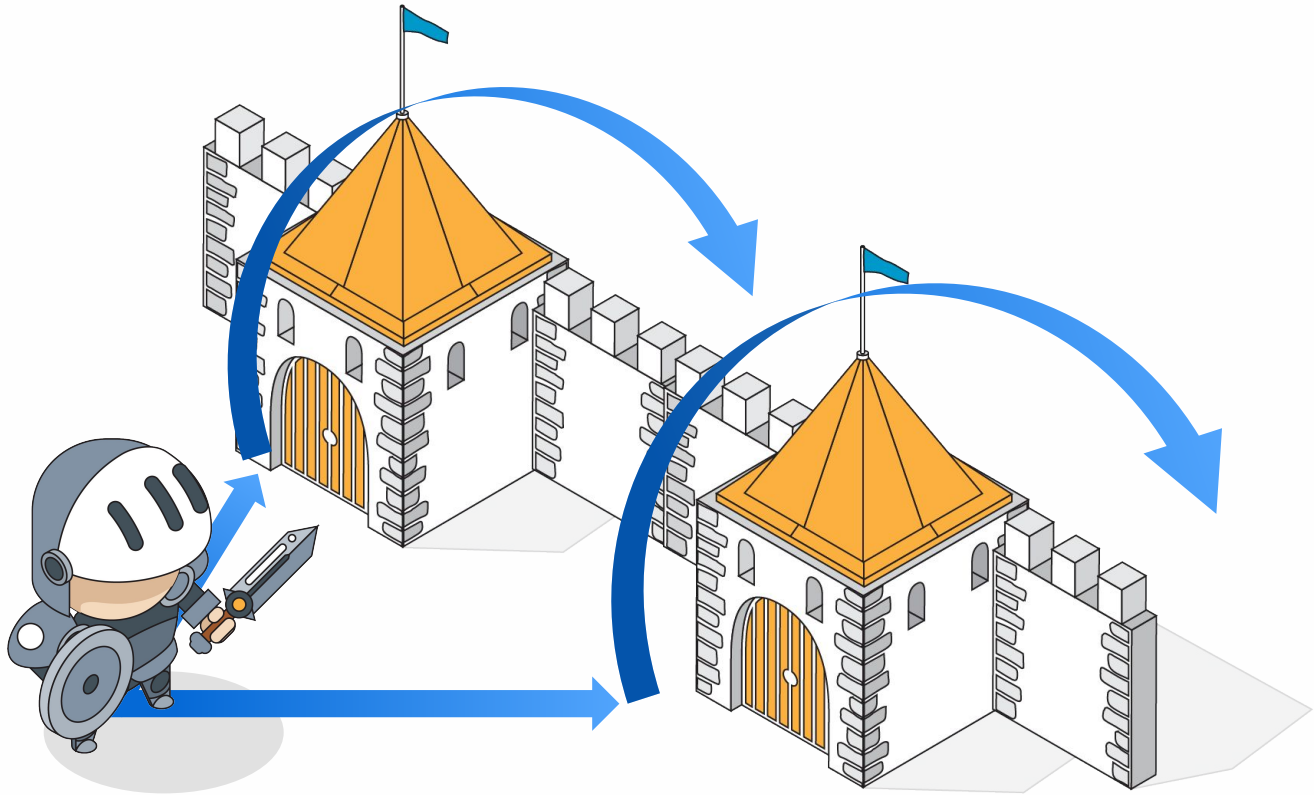
That's just a Cyber Maginot Line.

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.



Coverage: Asset Classes

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

Public Cloud	152,435	🌕
Production Servers	3,000	🌗
Dev/Build Servers	????	🌑
Enterprise Endpoints	9,267	🌗
Enterprise Servers	352	🌕
SaaS Services	500+	🌑

🌕: Easy, automated
🌗: Some manual effort
🌑: Lots of human effort

Cloud Data Sources

Cloud Control Plane

CI/CD Scans

SideScanning

Network Probing

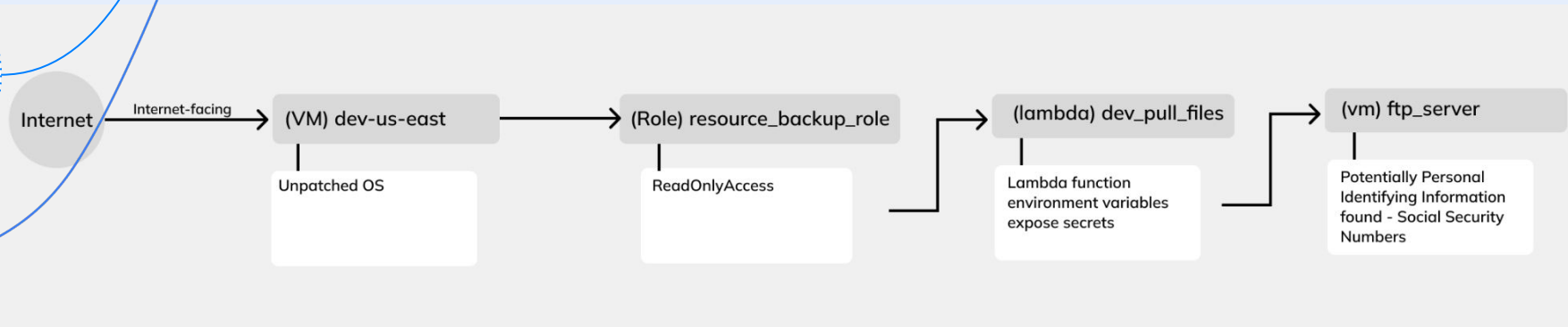
AuthN

okta

Cloud Events & Audit Logs

Unified Data Model

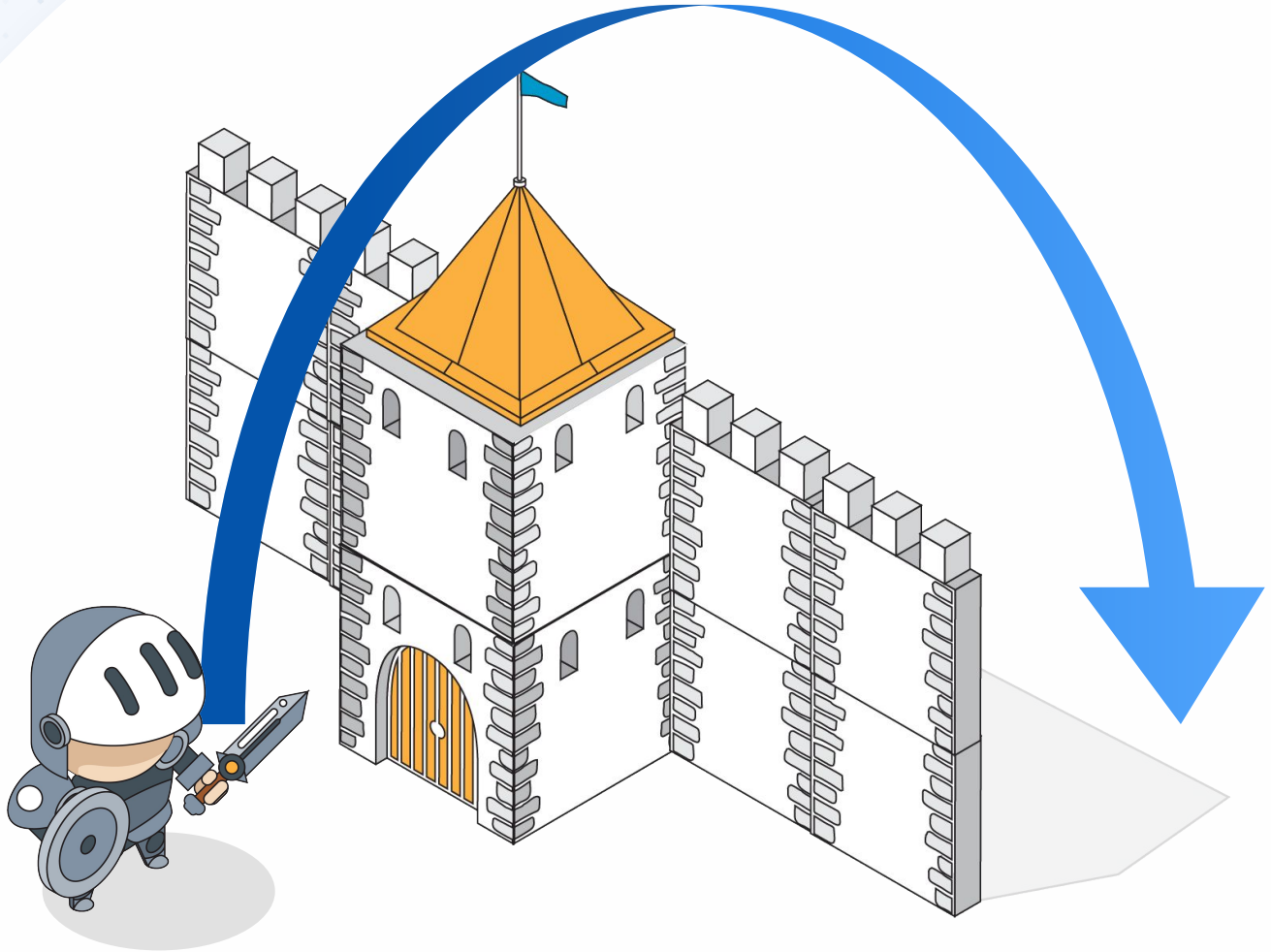
Contextualizing all data sources to unify the intelligence collected from deep inside the workload with cloud configuration data, identities, and more.



Dimension 2: Height

Since the adversary can quickly jump through security systems:

- Defenders must know how **comprehensive** their defenses are, and how they “stack.”



Comprehensive: Defenses

FOR EACH ASSET:

Step 1: Define Controls

Step 2: Define process measurements

Step 3: Document process maturity

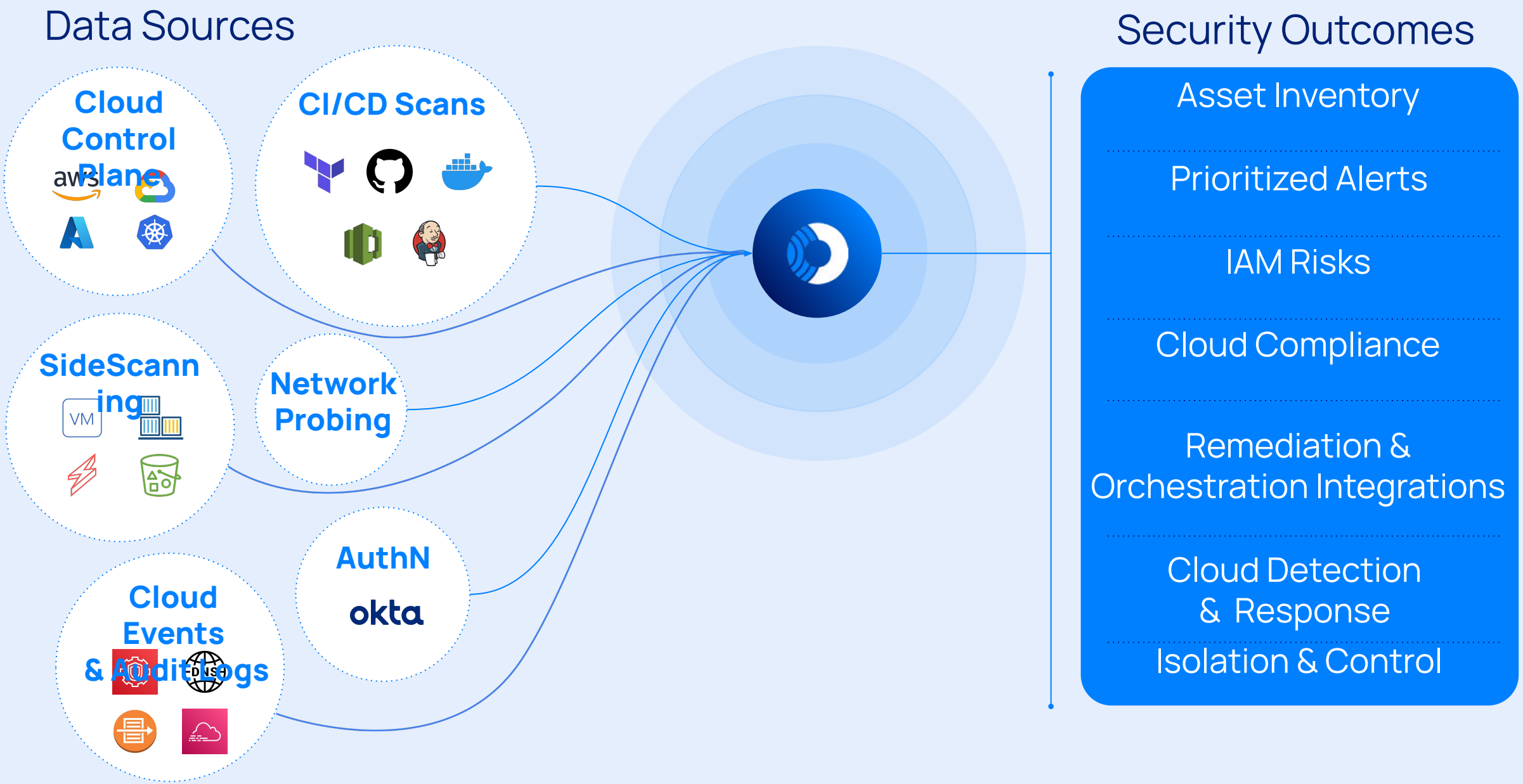
PUBLIC CLOUD

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	🌑

🌕: No executive required

🌗: Some executive oversight

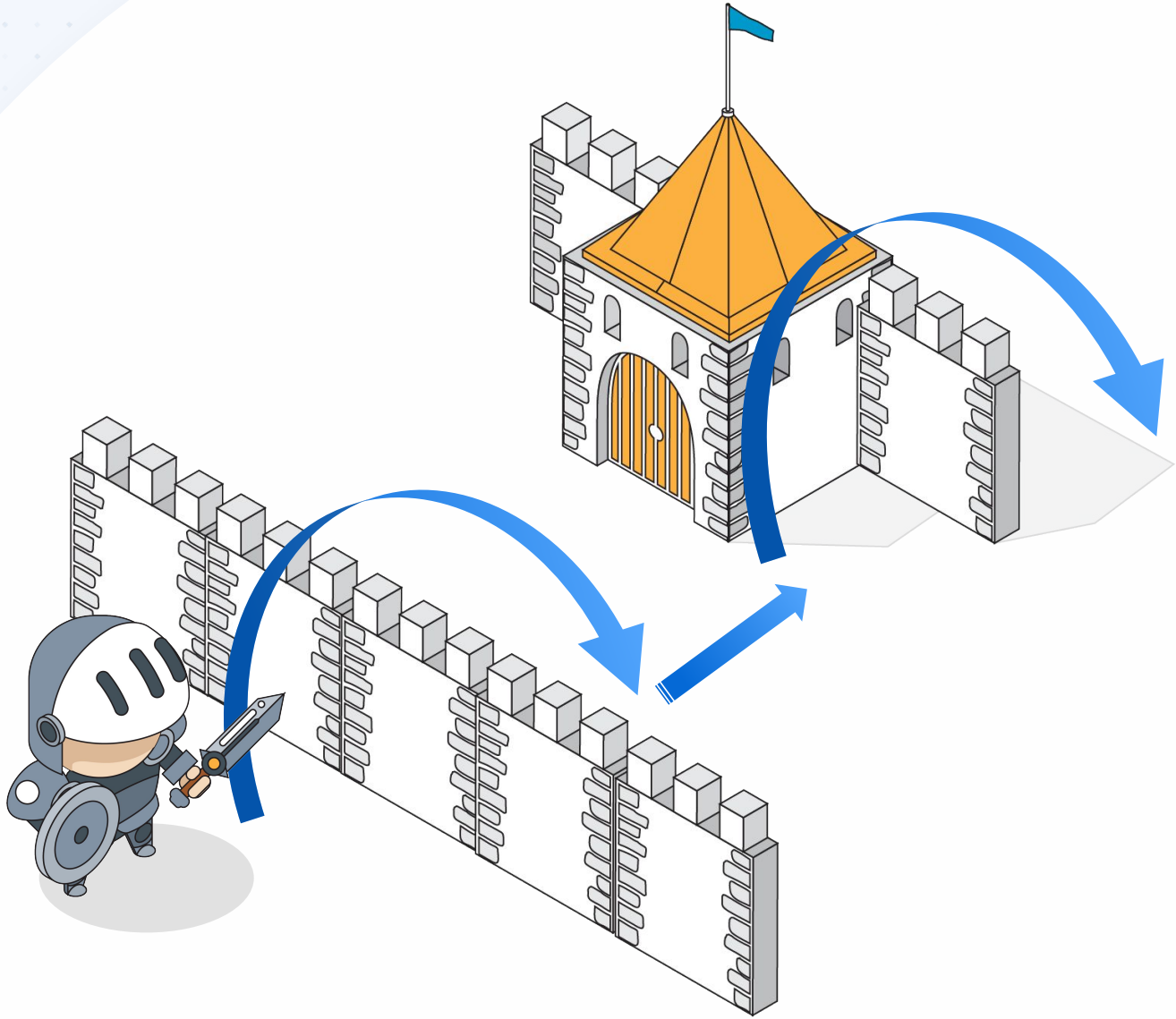
🌑: No process



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.



Context: Attack Scenarios

FOR ANY ATTACK TYPE:

Step 1: Tell the attack story

Step 2: Define effective defenses

Step 3: Narrate existing controls in this context

RANSOMWARE

An adversary gets malware to run on a (phishing, account takeover). That malware moves laterally by exploiting credentials available on that system (or exploiting known vulnerabilities), propagating across our environment, and stealing the data it finds, while leaving behind an encrypted copy. The adversary may offer to sell us the decryption key to recover.

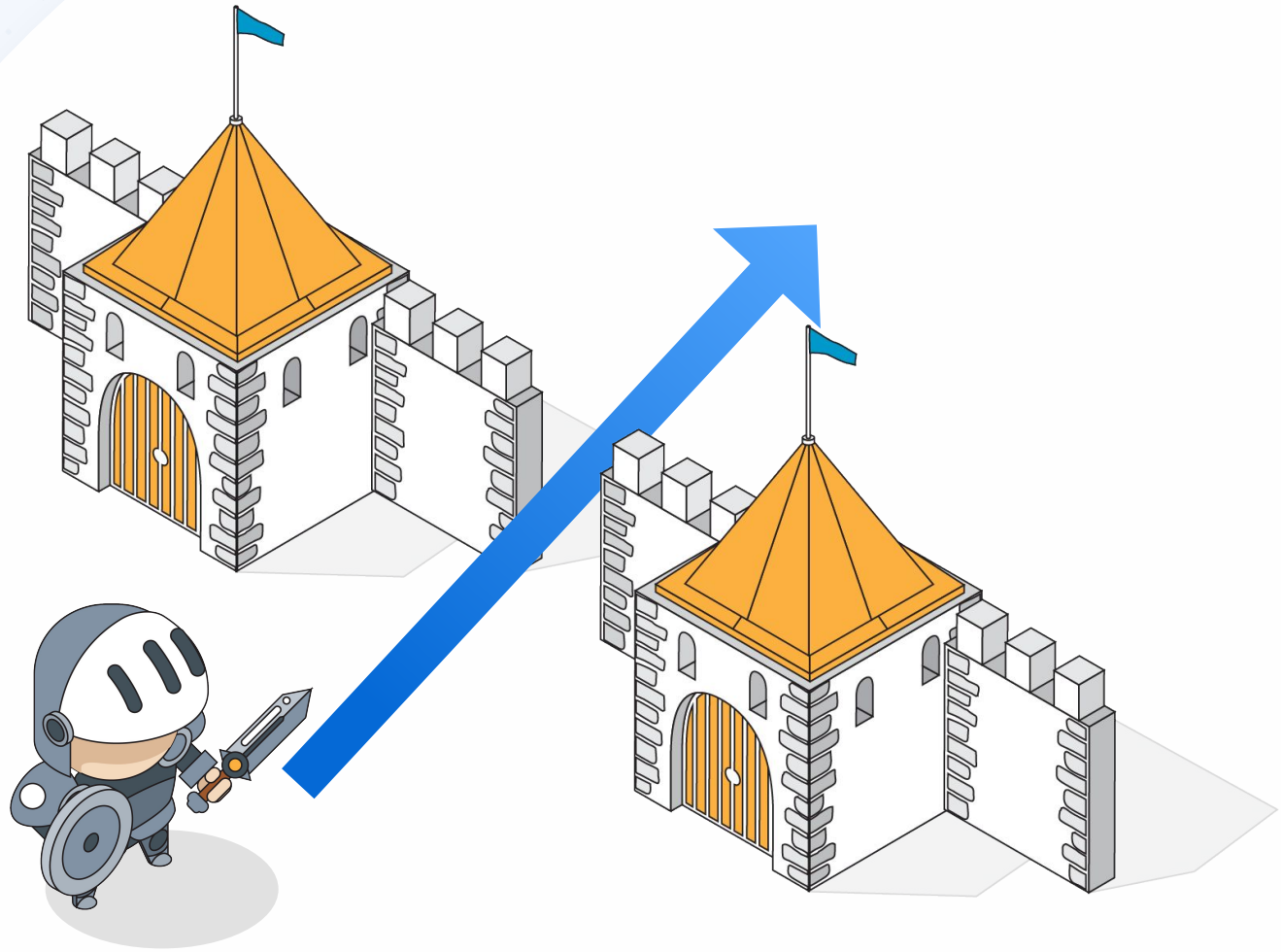
- Stopped by:
  - MFA
  - Removal of lateral admin privileges
- Mitigated by:
  - Data backups

"We use FIDO-MFA, we've implemented three-tiered AD administration, and we've eliminated central jump servers. All of our files are stored in the cloud."

Dimension 4: Time

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

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



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:

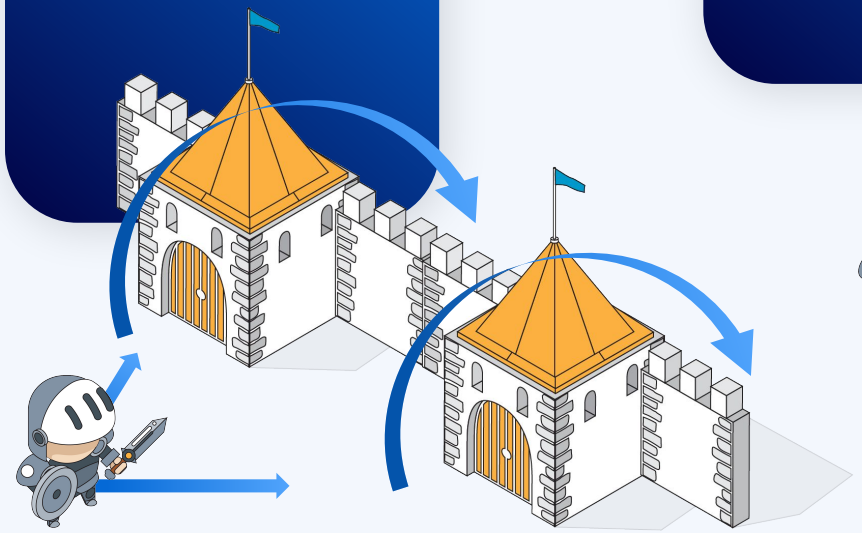
Critical	High	Medium	Low
7 days	30 days	90 days	180 days
85%	70%	50%	40%

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

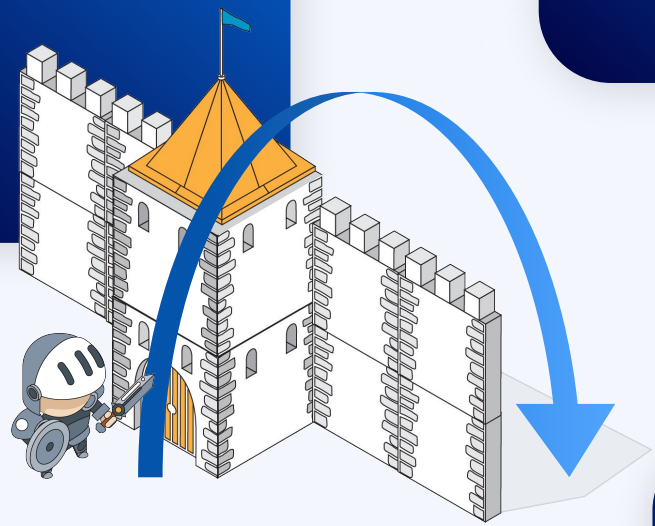
How many SLA violations were escalated before SLA was broken?

Defend with …

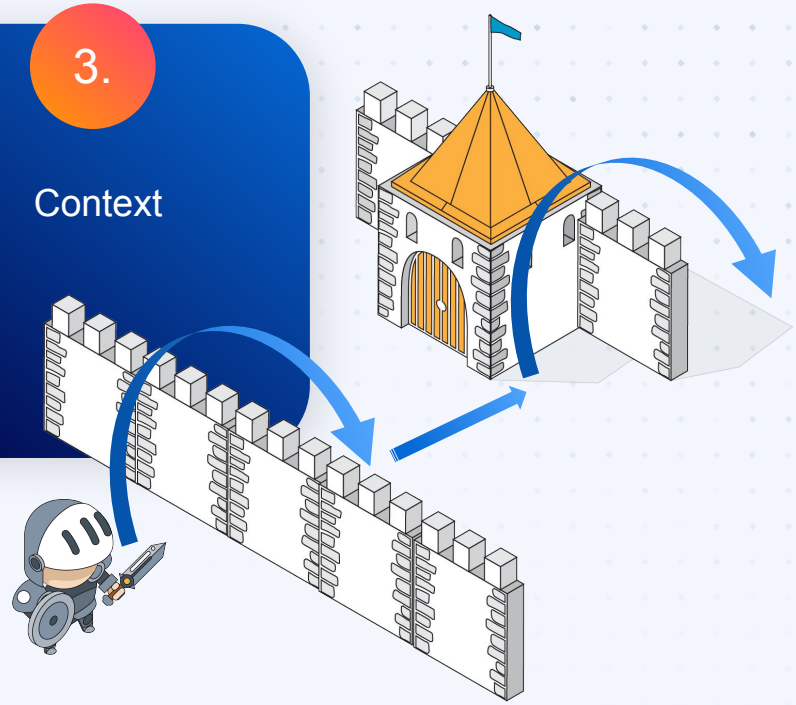
1. Coverage



2. Comprehensiveness



3. Context



4. Continuity

How to CISO in the Cloud

Andy Ellis

Advisory CISO, Orca Security