Conquering Castle Envy

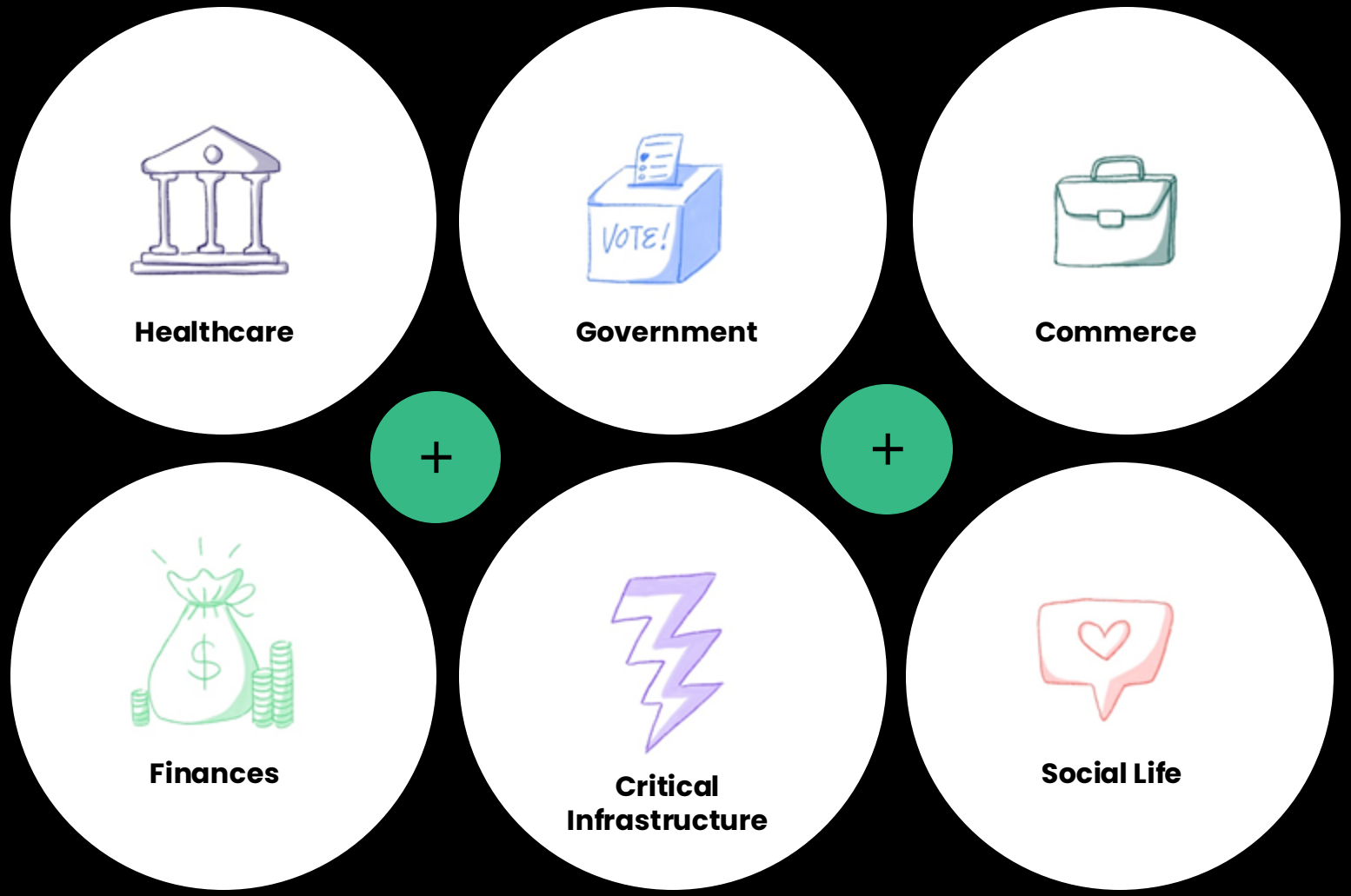
The Flawed Mindset That's Holding Application Security Back

Jeff Williams
Founder and CTO

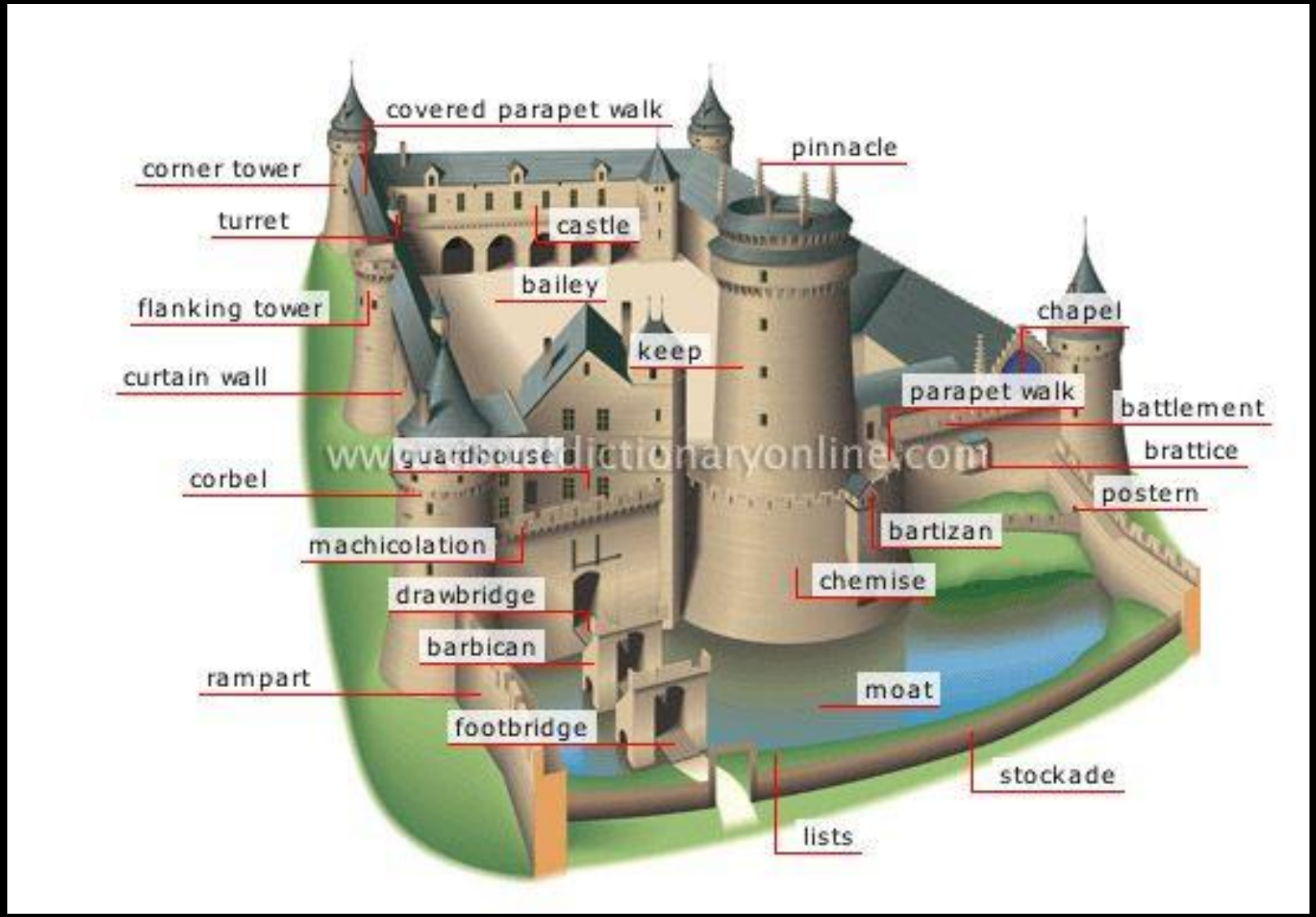
CONTRAST

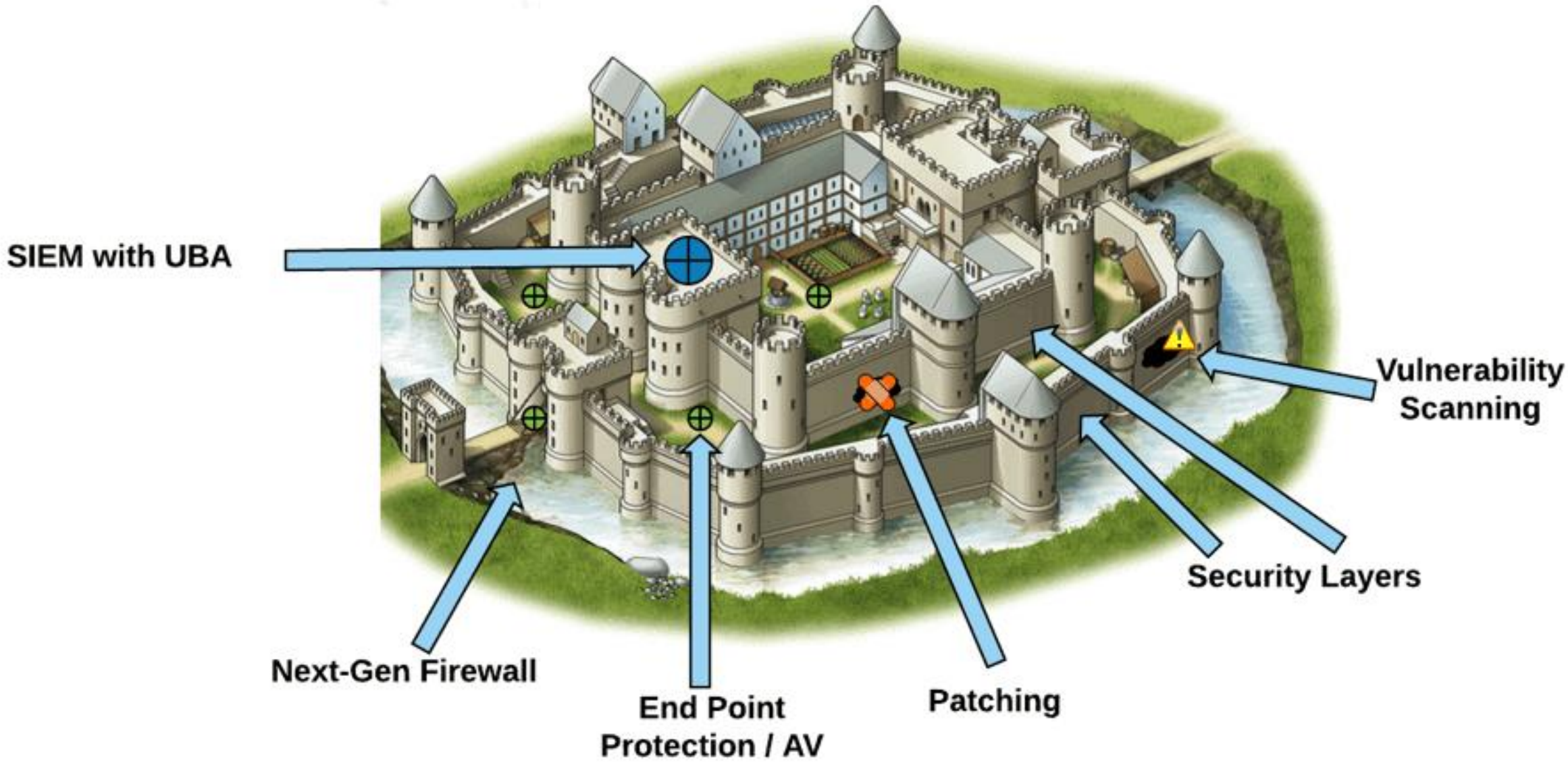
Music Credit: MC 900 Ft. Jesus

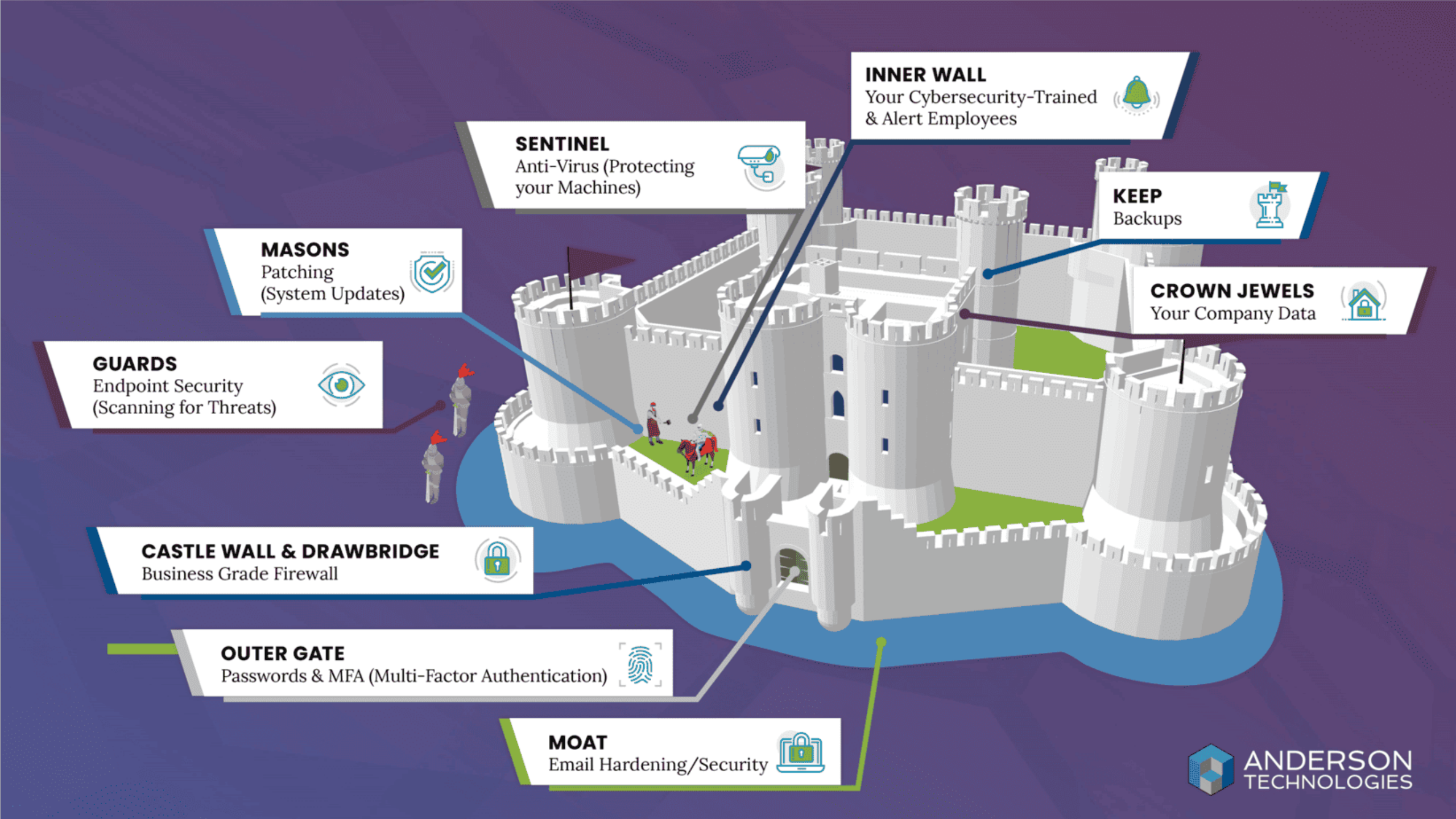
We blindly trust software with everything important in life...



We “know” how to build secure castles…




SIEM with UBA
Vulnerability Scanning
Security Layers
Next-Gen Firewall
End Point Protection / AV
Patching


INNER WALL
Your Cybersecurity-Trained & Alert Employees
SENTINEL
Anti-Virus (Protecting your Machines)
KEEP
Backups
MASONS
Patching (System Updates)
CROWN JEWELS
Your Company Data
GUARDS
Endpoint Security (Scanning for Threats)
CASTLE WALL & DRAWBRIDGE
Business Grade Firewall
OUTER GATE
Passwords & MFA (Multi-Factor Authentication)
MOAT
Email Hardening/Security
ANDERSON TECHNOLOGIES

ES&S LAYERS OF SECURITY

1

Physical Controls
Physical Security of the voting system is paramount.
The Electionware PCs should be kept in a controlled environment that limits physical access to the system. All voting equipment should be outfitted with wire and paper seals.

2

System Hardening
Hardening of the Electionware PC. Among other things, the hardening process locks down what applications can be run and loaded on the PC and establishes user login credentials and roles. It essentially turns the PC into a single use device, dedicated to the sole purpose of creating and operating elections.

3

User Authentication
No matter the device, all election PC's and voting equipment require login credentials before operation can commence.
All failed login attempts are logged.

4

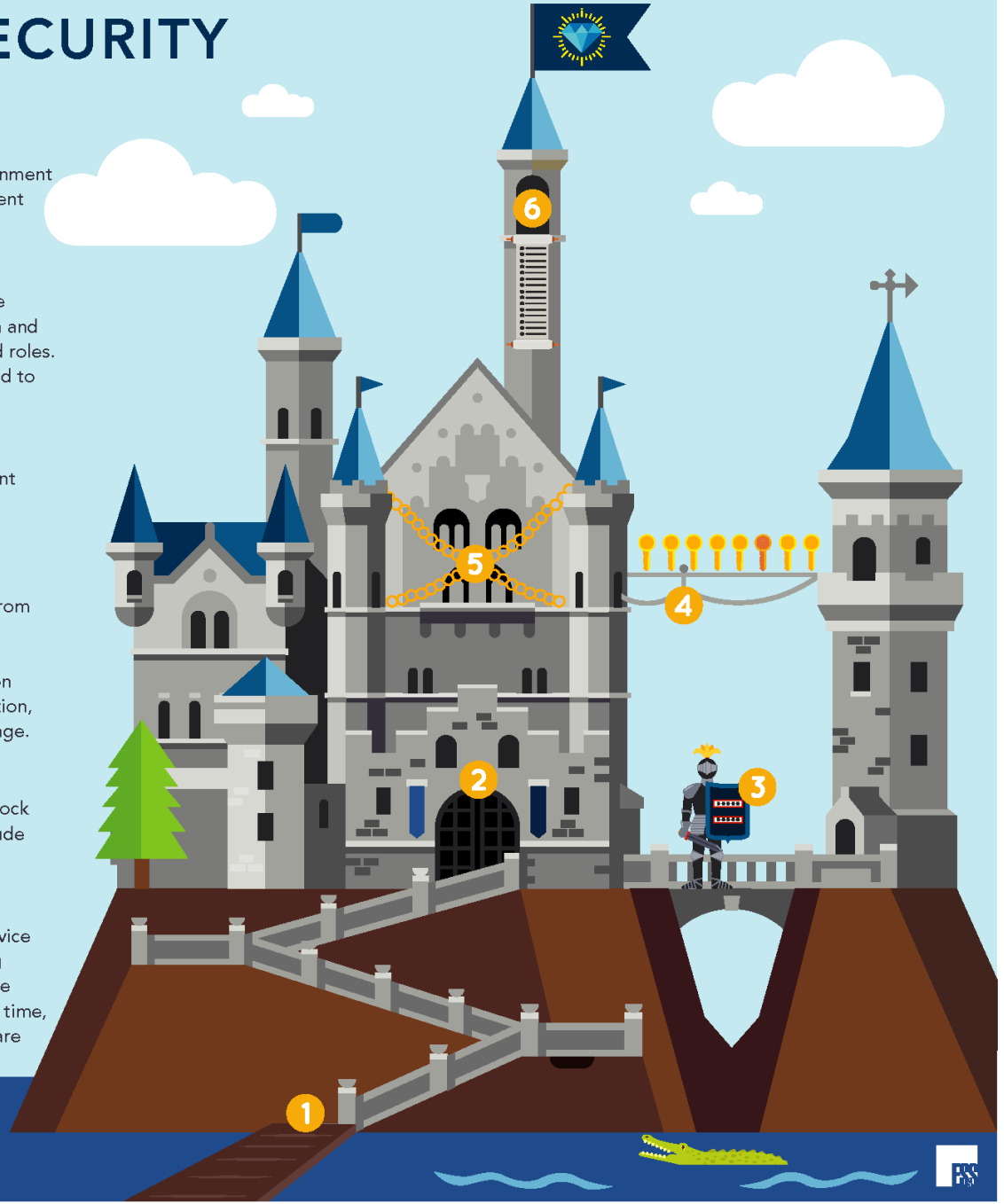
Encryption
All data in motion – such as election media that is moving from the Electionware PC to a voting device – is encrypted.
The encryption key is different for each election and is transferred to the voting device separately from the election media. In other words, a different key is used for each election, and the key and the padlock never travel in the same package.

5

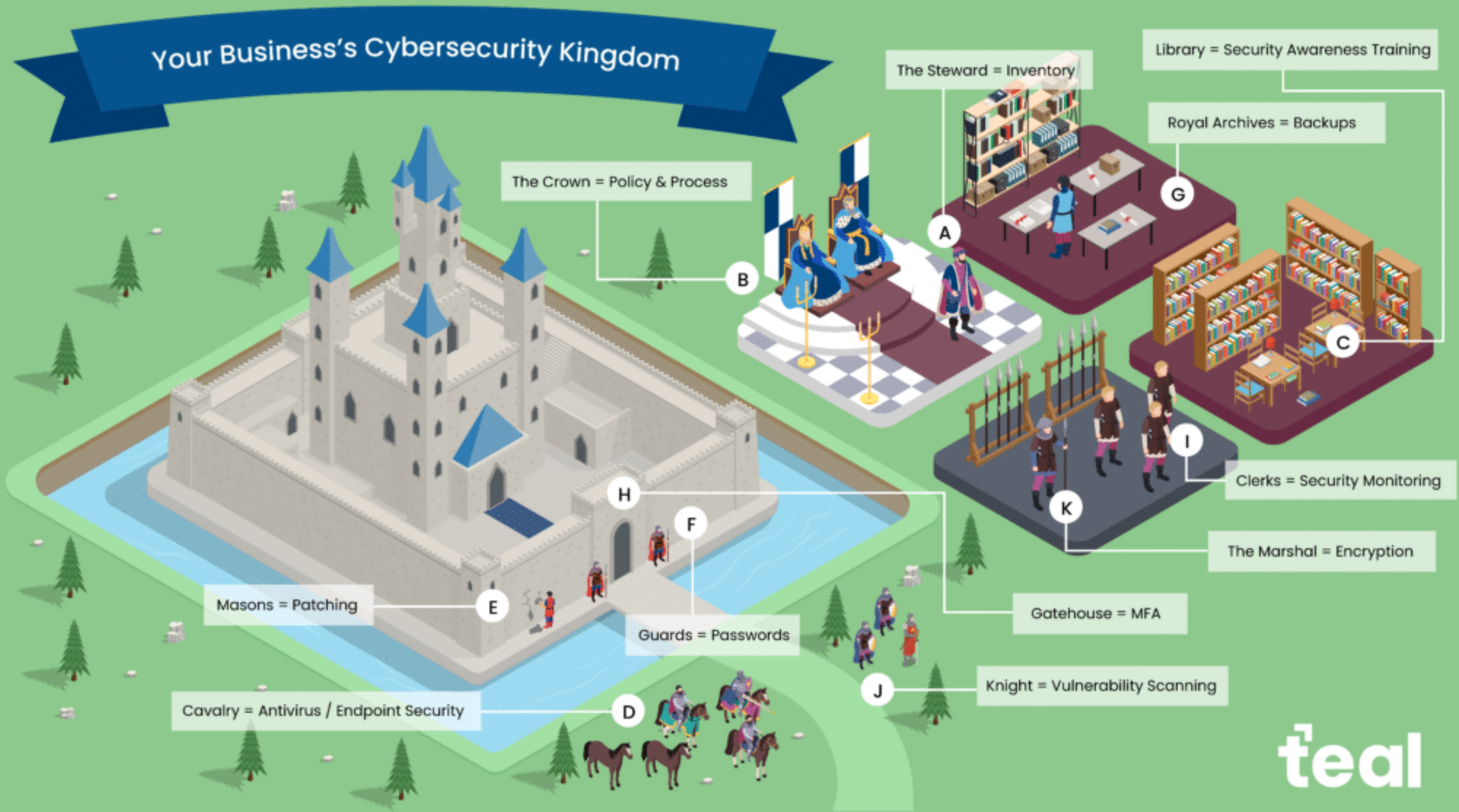
Data Integrity Validation
A number of checks are performed when attempting to unlock election media that is loaded in a voting device. These include digital signatures and hash checks to ensure data integrity.

6

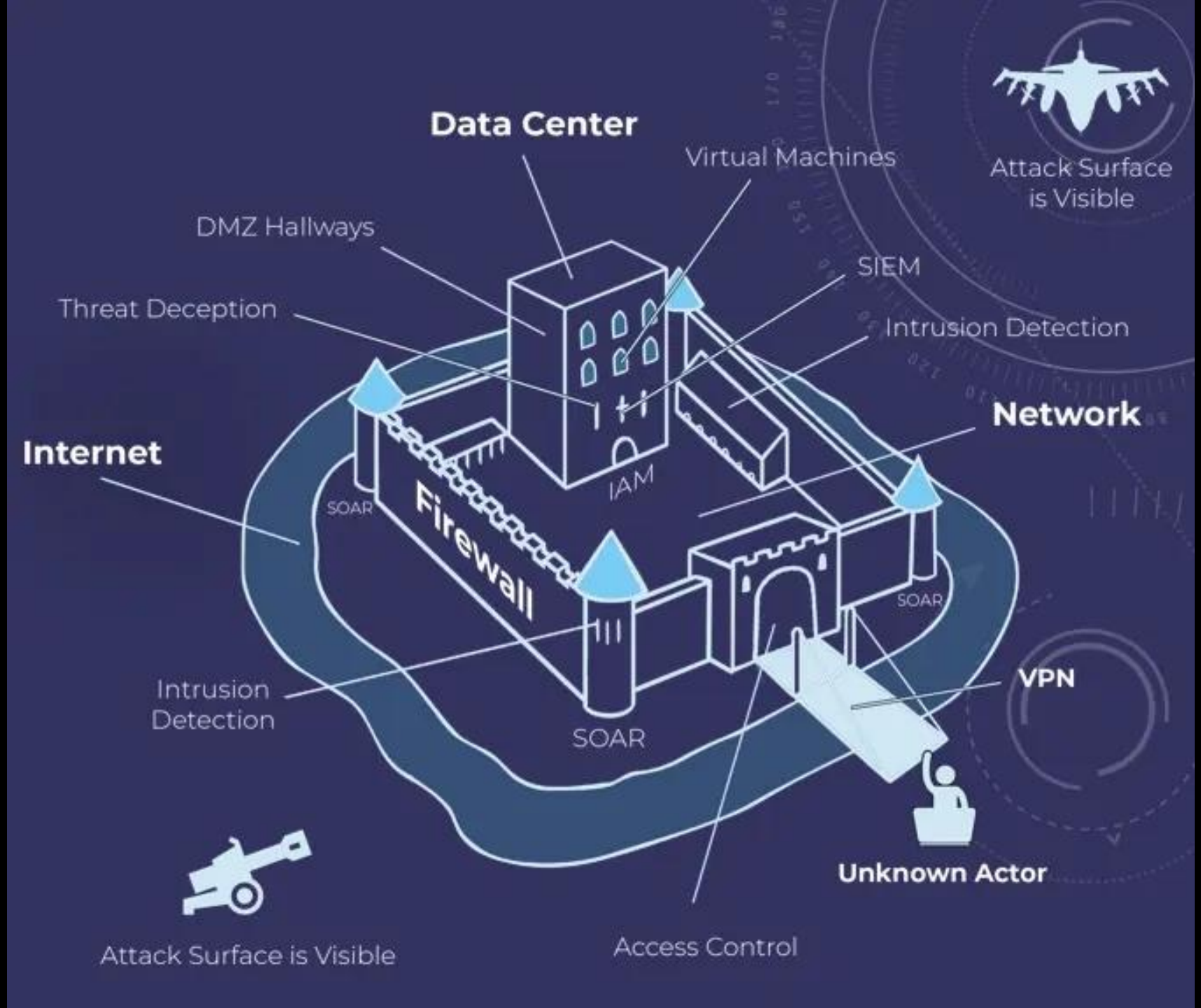
Audit Logs & Trails
All actions performed in the election – regardless of the device being used – are logged in detail. All audit logs from voting devices in the field are combined in a single database on the Electionware PC. This database can be searched by device, time, and type of action. All actions performed on the Electionware PC are also logged by user.



Your Business's Cybersecurity Kingdom



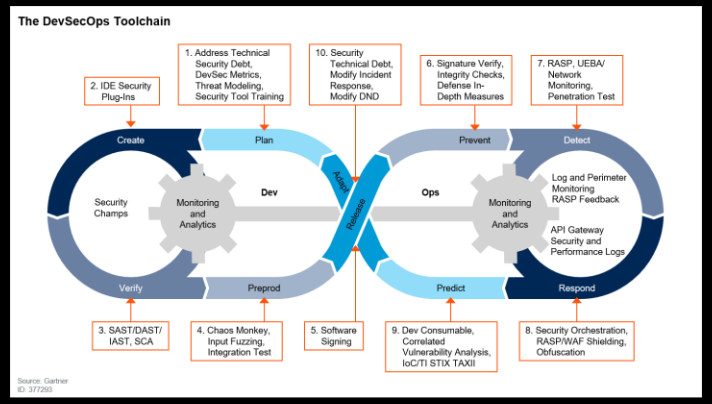
teal


Data Center
Virtual Machines
Attack Surface is Visible
DMZ Hallways
SIEM
Threat Deception
Intrusion Detection
Network
Internet
IAM
SOAR
Firewall
SOAR
VPN
Intrusion Detection
SOAR
Unknown Actor
Attack Surface is Visible
Access Control

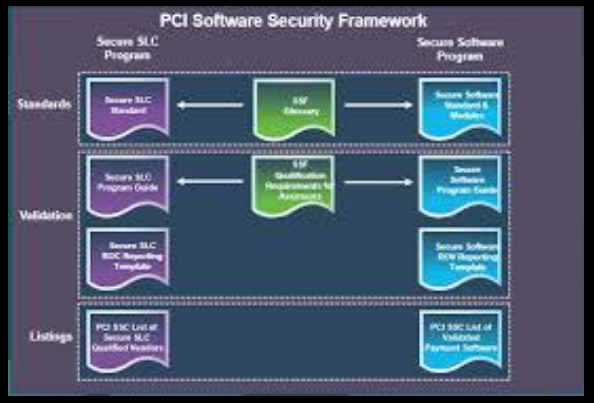
We “know” how to build secure software…

Rainbow Series

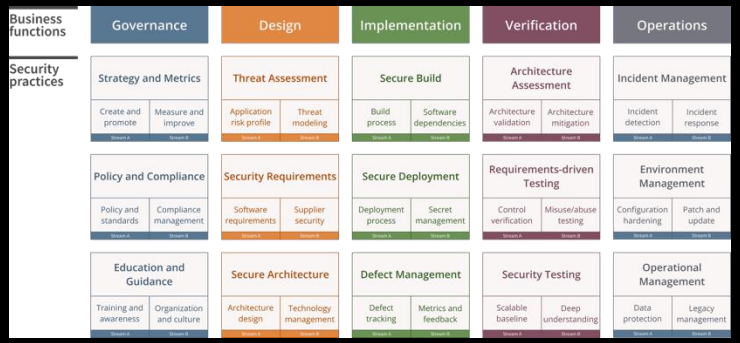
Gartner DevSecOps



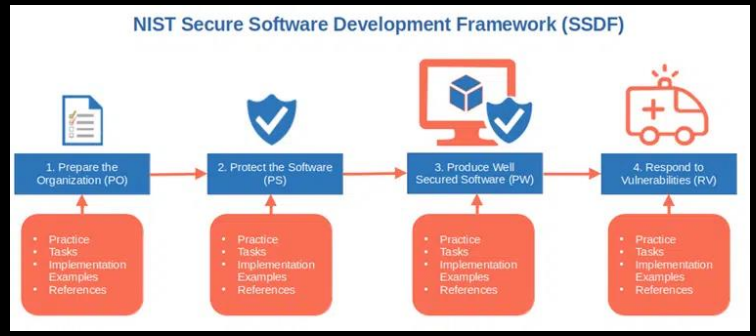
PCI SSF



2000 2010 2020



OWASP OpenSAMM

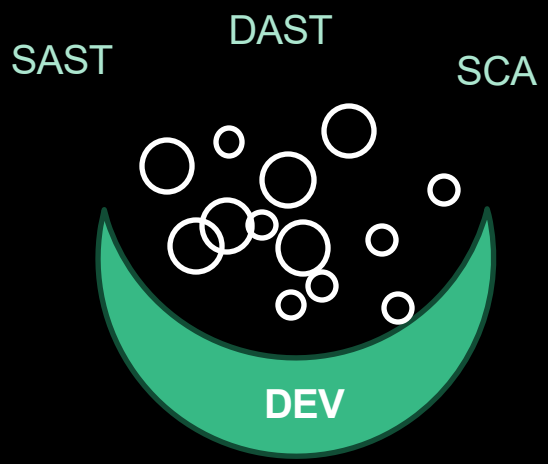


NIST SSDF

The castle approach isn't working very well

Development….

- Huge backlog
- Only 5% exploitable
- 19% of developer time
- Scans slow down pipelines



Security…

- Poor developer relationship
- Isolated from operations
- No visibility into attacks

Operations…

- App/API attacks ignored
- Focus on network and cloud
- Already overwhelmed
- 2nd leading cause of breaches (DBIR)

Your application layer is more like a city than a castle

- Way too big and complex to analyze
- Constantly under construction
- Highly interconnected
- Virtually unlimited attack surface
- Always under attack
- Relied on by people, business, government

Which one of these is true?

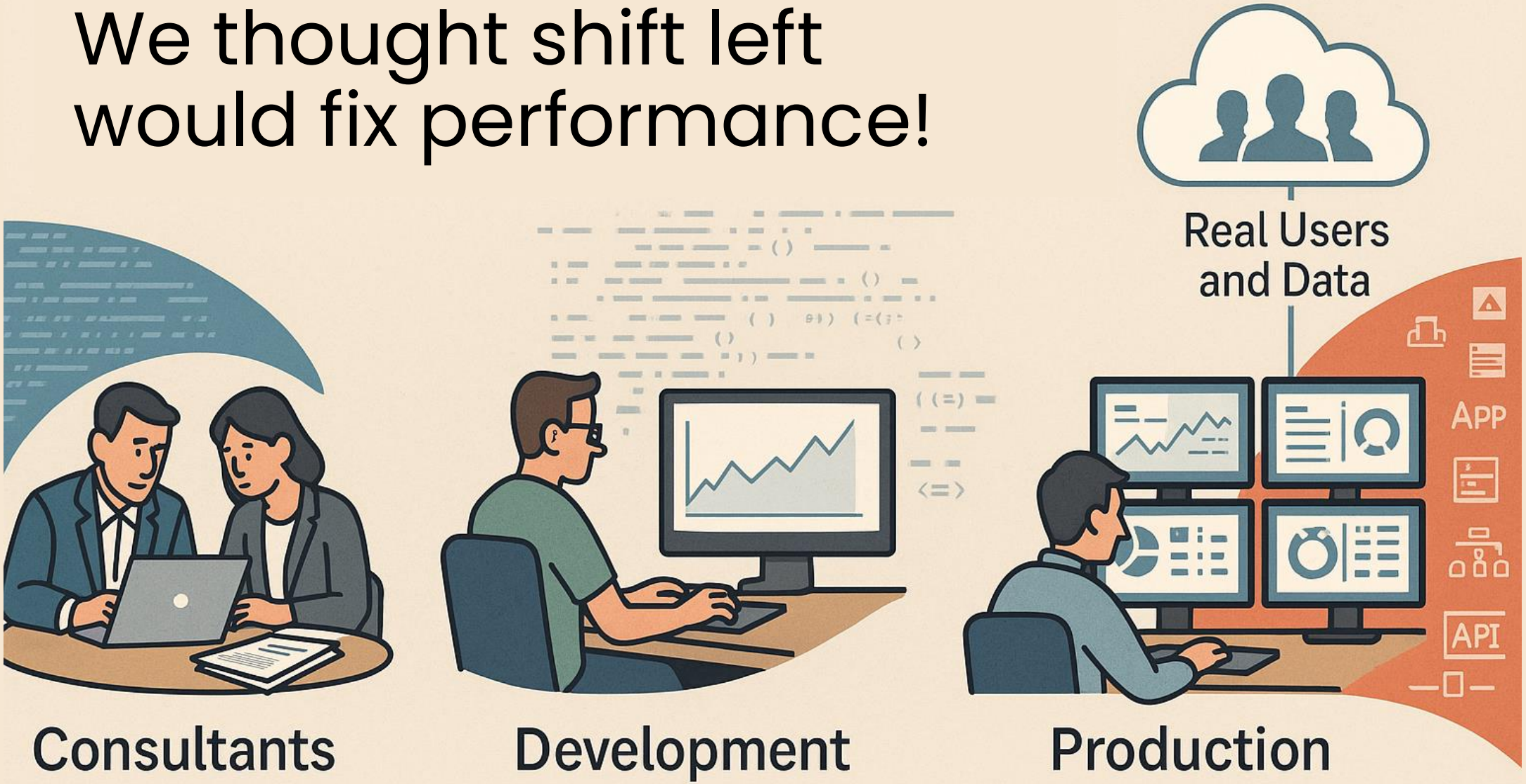
A. Earth is the center of the universe

B. Life spontaneously generates from inanimate matter

C. Your personality can be determined from bumps on your head

D. Shifting security activities left improves outcomes

We thought shift left would fix performance!



Stone Age | 2000s | 2010s

Aaron Lord · 1st
Senior Director Analyst - Software Engineering Security
1d ·

Happy to share my latest piece of #Gartner research. As I have discussed here before, shifting security left is dead. It has been misused to push more security responsibility onto software engineering, leading to increased cognitive load. In my research, I explain how we should be shifting security down, not left to scale DevSecOps.

Software engineering leaders should pivot away from "shifting left" approaches. Instead, they should shift down application security and improve collaboration across teams.

Thanks to to my co-author Jason Gross, Jim Scheibmeir, Ph.D. for your guidance, and Manjunath (Manju) Bhat for your inspiration.

Link to research in the comments.

Anton Chuvakin and 43 others 24 comments · 6 reposts

"Shifting security left is dead"

-- Aaron Lord, Senior Director Analyst at Gartner

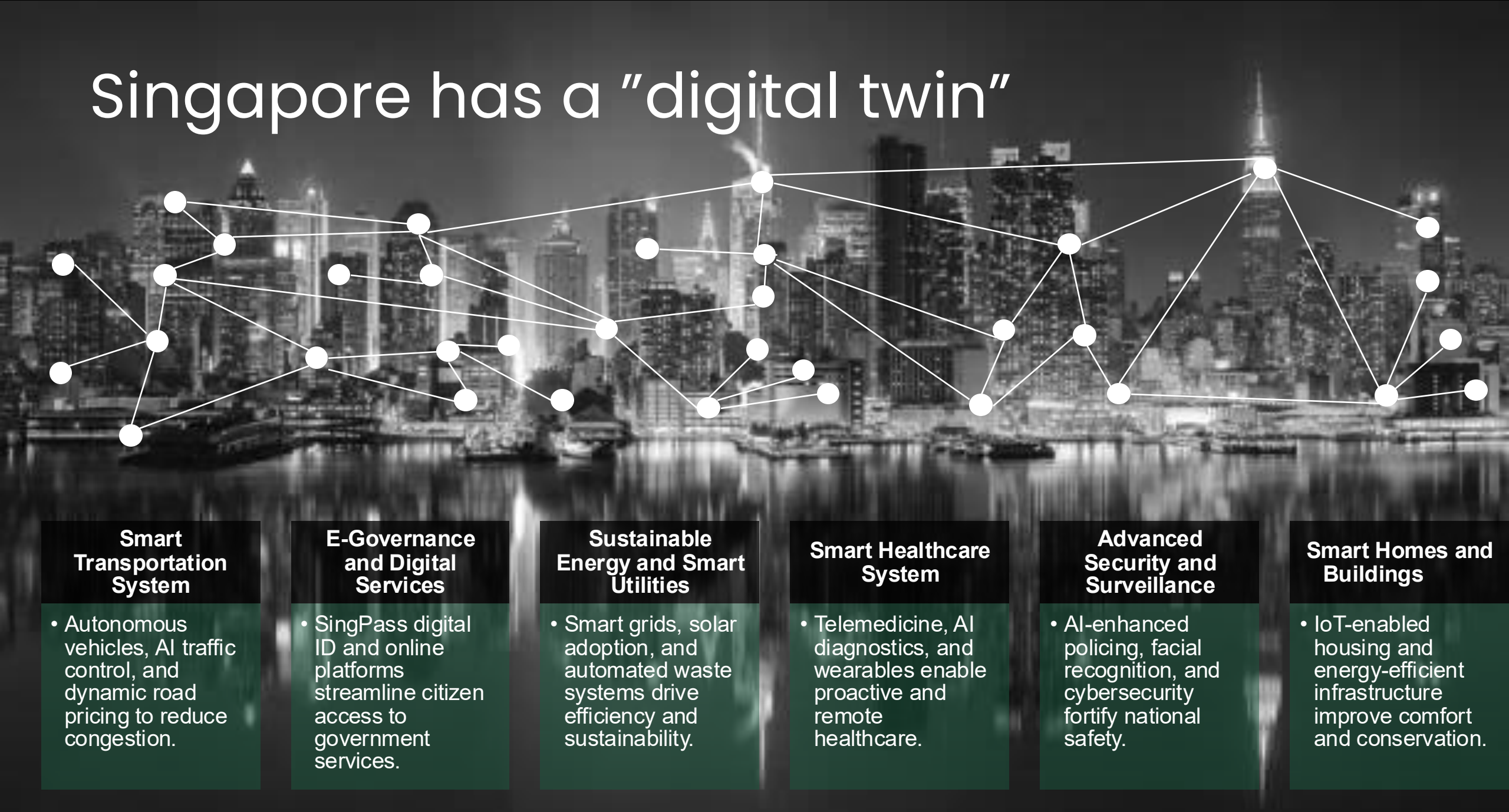
https://www.gartner.com/en/documents/6871666

And now the game has changed!

AI Powered Developers

AI Powered Attackers

Singapore has a "digital twin"



Smart Transportation System	E-Governance and Digital Services	Sustainable Energy and Smart Utilities	Smart Healthcare System	Advanced Security and Surveillance	Smart Homes and Buildings
• Autonomous vehicles, AI traffic control, and dynamic road pricing to reduce congestion.	• SingPass digital ID and online platforms streamline citizen access to government services.	• Smart grids, solar adoption, and automated waste systems drive efficiency and sustainability.	• Telemedicine, AI diagnostics, and wearables enable proactive and remote healthcare.	• AI-enhanced policing, facial recognition, and cybersecurity fortify national safety.	• IoT-enabled housing and energy-efficient infrastructure improve comfort and conservation.

Just like APM – AppSec has to get REAL

You need:

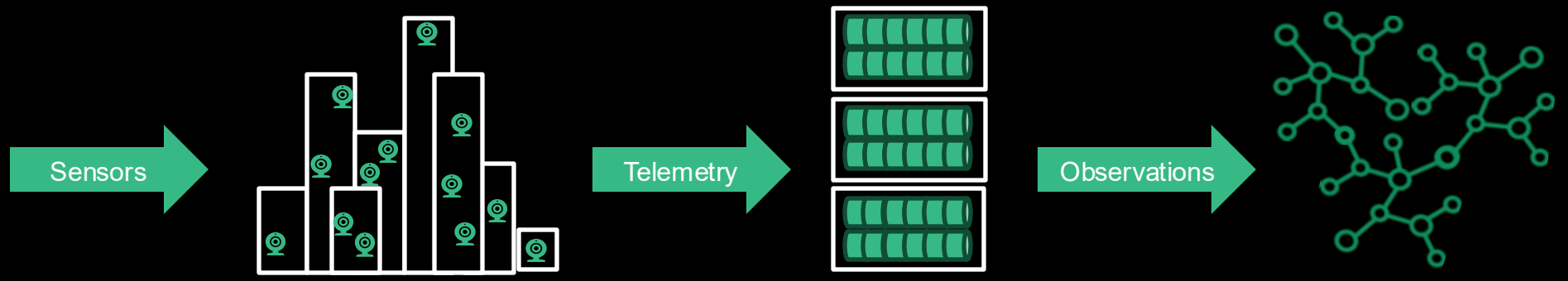
- Real fully-assembled software
- Real connections
- Real data
- Real users
- Real threats
- Real scale

Imagine a live contextual knowledge graph (CKG) of your entire application layer!

SAST
DAST
SCA
WAF

ADR
IAST
RSCA

CNAPP
CMDB
APM

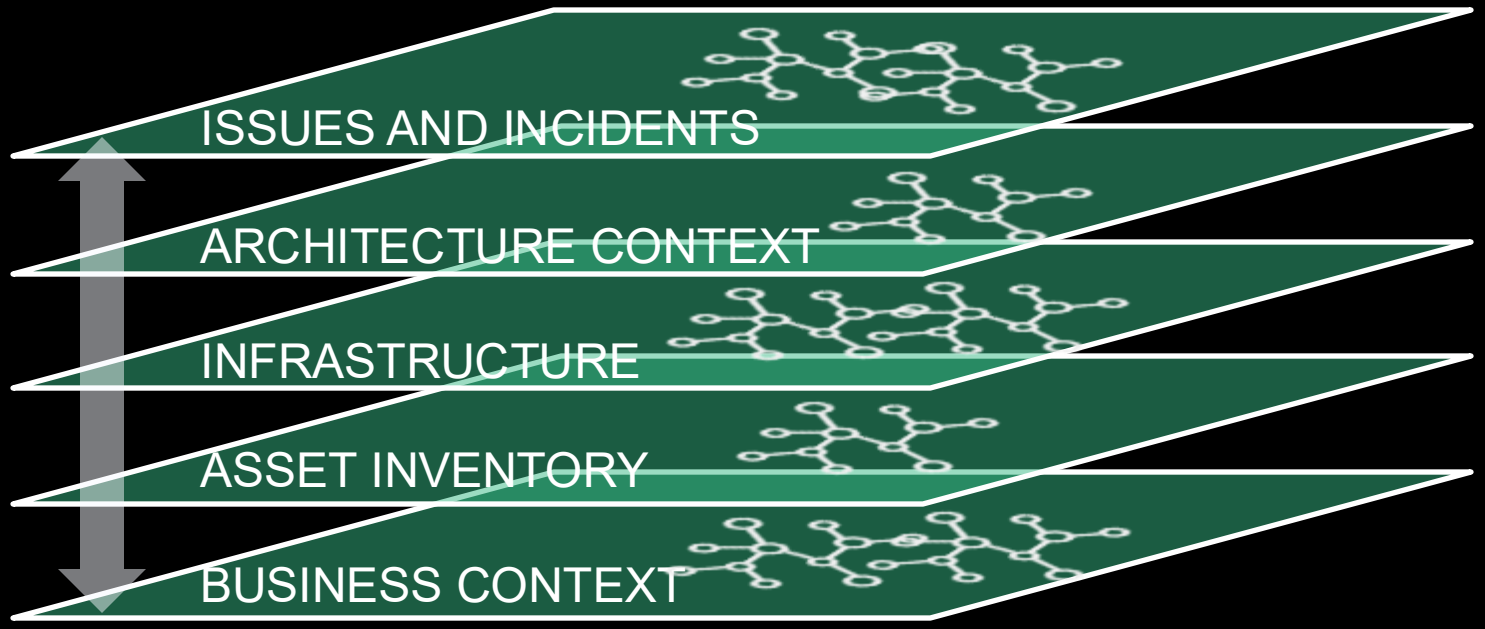


Instrument Your App Layer

Streaming Data Architecture

Update Contextual Knowledge Graph

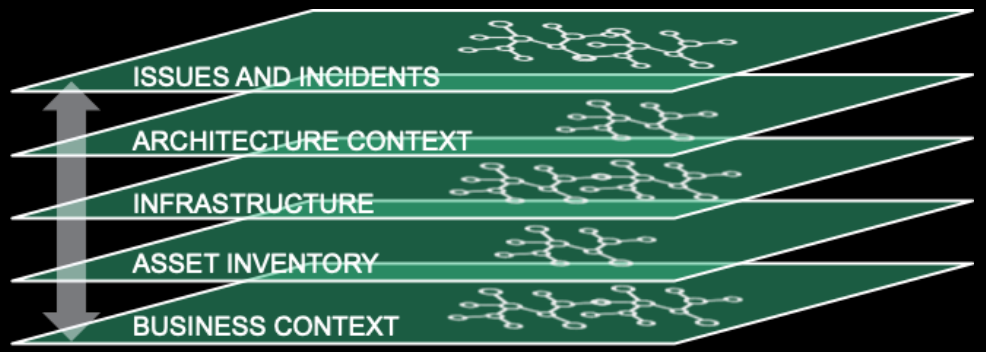
Contextual Knowledge Graph (CKG)



- ☐ Apps/APIs
- ☐ Servers
- ☐ Assets
- ☐ Attack Surface
- ☐ Attacks
- ☐ Blast Radius
- ☐ Cloud
- ☐ Connections
- ☐ Containers
- ☐ Control Flow
- ☐ Criticality
- ☐ CVEs
- ☐ Data Flow
- ☐ Defenses
- ☐ Incidents
- ☐ Libraries
- ☐ Probes
- ☐ Queues
- ☐ Repos
- ☐ Risky Functions
- ☐ Routes
- ☐ Services
- ☐ Teams
- ☐ Threat Intel
- ☐ Vulnerabilities

CKG is the perfect substrate for taking advantage of AI

Example: Streamlining threat modeling



Answers

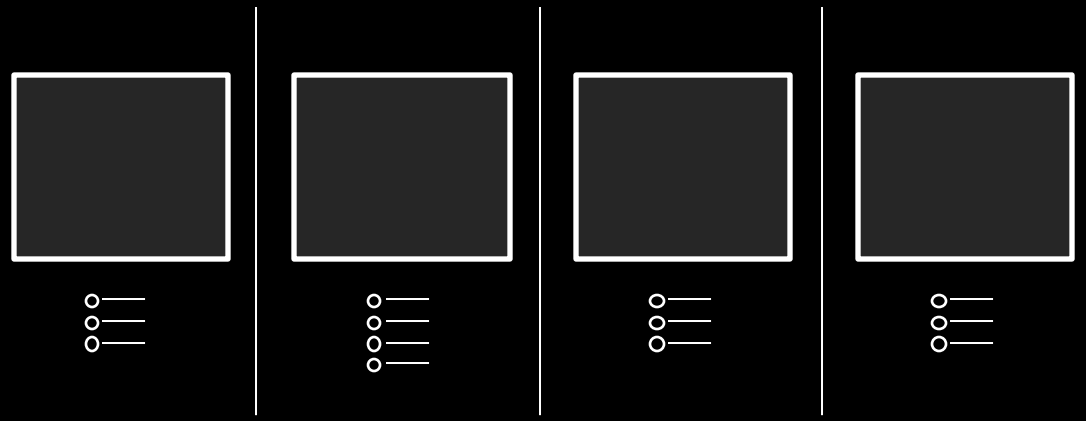
- **Show me which routes require authentication**
- **Show me what roles are required for each route**
- **Show me which routes process untrusted data**
- **Show me which routes connect to backend systems**
- **Show me which routes consume serialized objects**
- **Show me all encryption algorithms in use**
- **Show me protocols for all backend connections**
- **Show me the blast radius for this application**
- **Show me…**

Example: Better risk prioritization

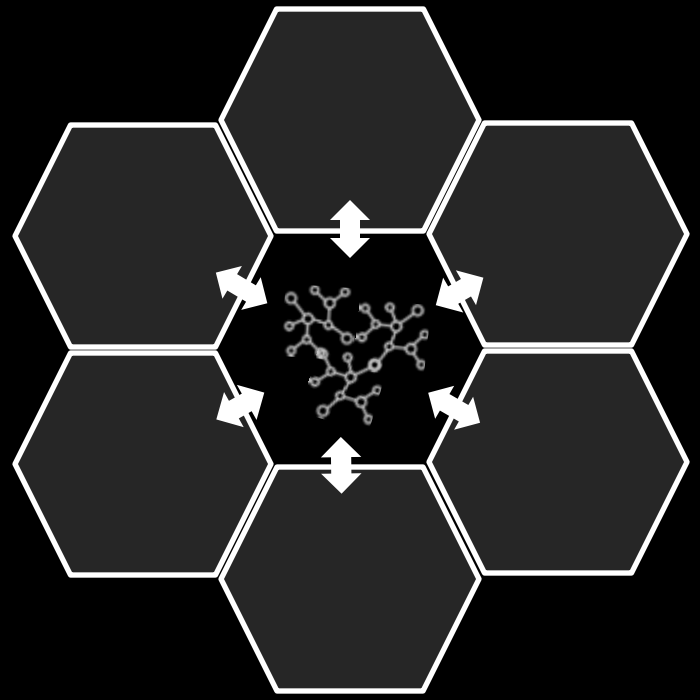
```
============================================================
CVSS V4 ISOLATED FACTOR TEST RESULTS (1000 vectors per test)
============================================================
Factor Descriptions:
 - not_attacked:    Sets E:U (no attacks known) vs X (Not Defined)
 - not_critical:    Sets CR:L/IR:L/AR:L (lowest requirements) vs X (Not Defined)
 - has_controls:    Sets MAC:H (high modified complexity) vs X (Not Defined)
 - no_blast_radius: Sets MSC:N/MSI:N/MSA:N (no subsequent impact) vs X (Not Defined)

Test Name                    |   Low   |  Medium |   High  | Critical| Avg Score | Change
-----------------------------+---------+---------+---------+---------+-----------+-----------
Baseline (No Factors)        |   14.2% |   55.2% |   28.1% |    2.5% |      5.69 |
Factor: not_attacked         |   75.8% |   22.5% |    1.7% |    0.0% |      2.51 | -3.18 (-55.9%)
Factor: not_critical         |   34.6% |   54.9% |   10.5% |    0.0% |      4.52 | -1.16 (-20.4%)
Factor: has_controls         |   18.4% |   55.4% |   24.6% |    1.6% |      5.33 | -0.35 (-6.2%)
Factor: no_blast_radius      |   23.1% |   62.5% |   10.9% |    0.3% |      4.51 | -1.17 (-20.6%)
All Factors                  |   96.5% |    0.3% |    0.0% |    0.0% |      0.58 | -5.10 (-89.7%)
```

Your CKG streamlines all your appsec workflows

Traditional Siloed AppSec Workflows with Separate Data



Streamlined AppSec Workflows with Shared CKG

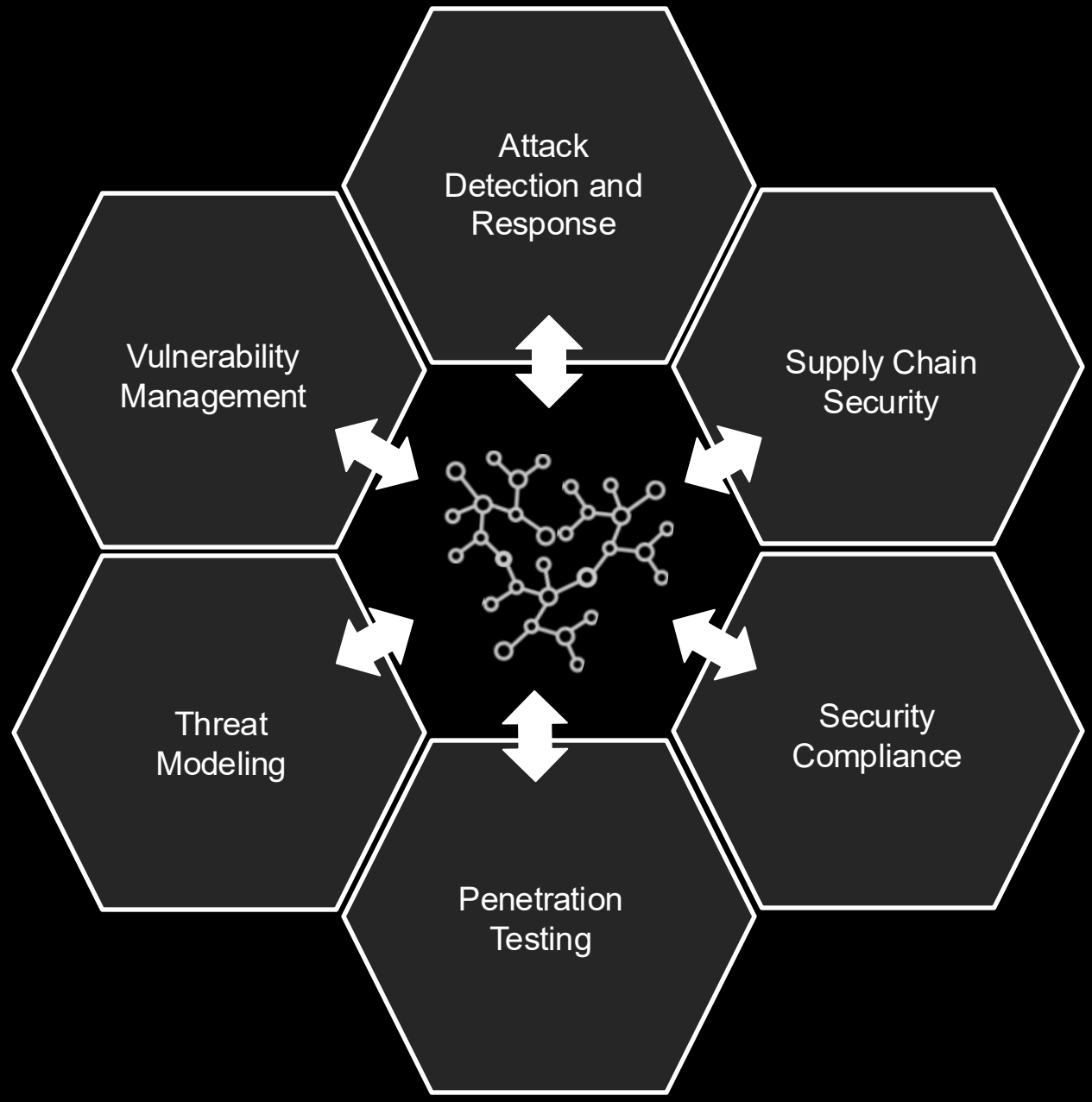


Real Benefits

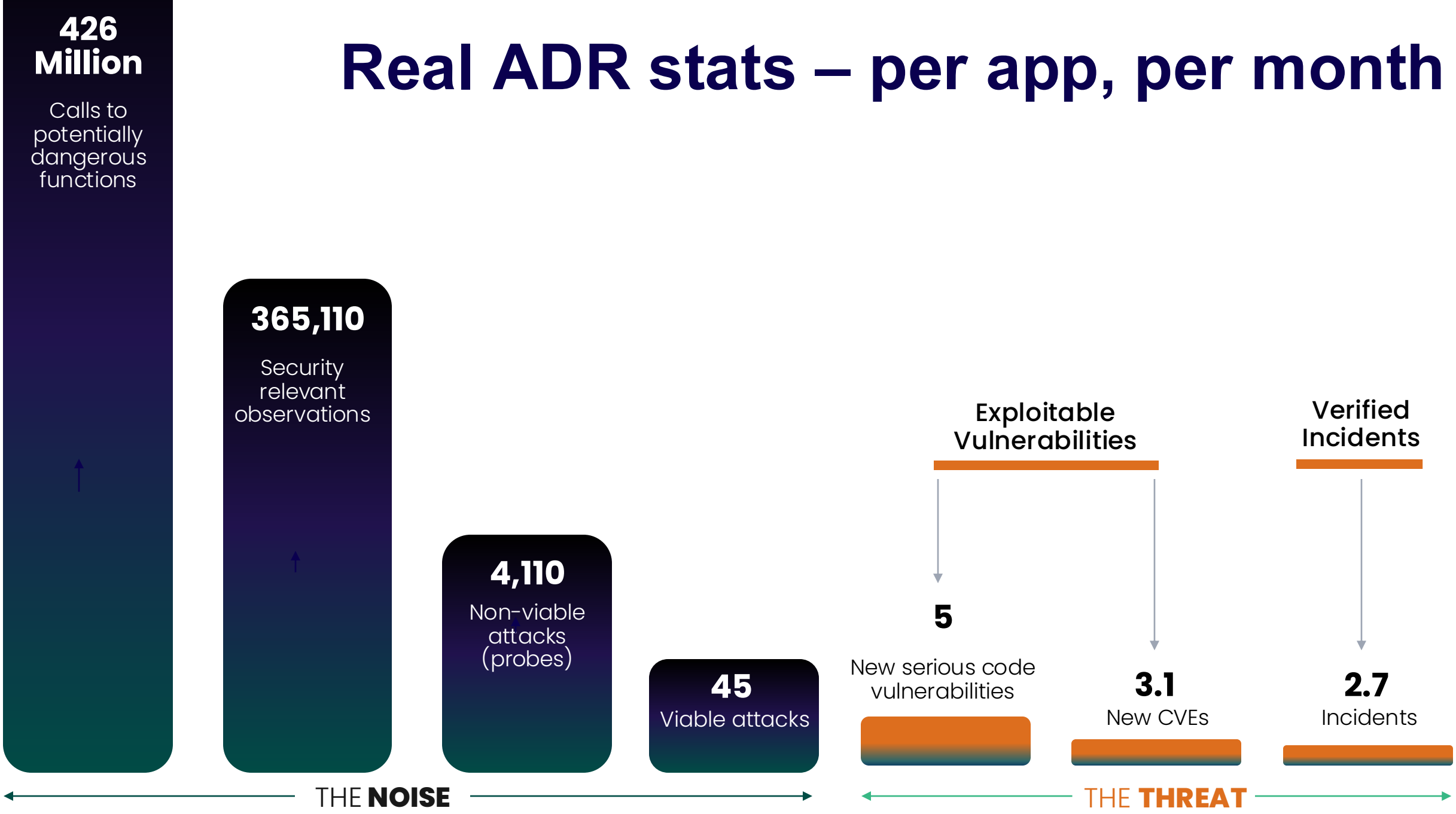
- Faster and easier
- More accurate
- More contextual
- Better prioritization
- Better collaboration
- Better culture

Reduce at least 50% of the work involved with appsec workflows.

Scale to cover more of application estate.



Real ADR stats – per app, per month



https://www.contrastsecurity.com/software-under-siege-2025-application-layer-threats-exposed-by-contrast-security

Castles are for fairy tales

It’s time for appsec to grow up, leave the castle, and move to the city.

Pick up a shovel, instrument your city, leave the theoretical world behind, and become relevant.

EMBRACE YOUR CITY

Ask me anything…

Castle Envy: the Flawed Mindset That's Holding Application Security Back

Jeff Williams
Founder and CTO
Contrast Security