Many thanks to our sponsors and partners!

Powered by orange

PLATINUM SPONSORS

BIT SENTINEL

D3 CYBER

CYBER LIFE HACKS

HACKING VILLAGE PARTNERS

cyber EDU

electron

HACKOUT Portalul Atacurilor Cibernetice

SILVER SPONSORS

efect

PFG FINANCE

wantsome the friendly IT academy

MOBILITY PARTNER

TOYOTA Cluj-Napoca prin Profi Auto

COMMUNITY & MEDIA PARTNERS

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

CLUJ IT

UNIVERSITATEA BABEȘ-BOLYAI
BABEȘ-BOLYAI TUDOMÁNYEGYETEM
BABEȘ-BOLYAI UNIVERSITÄT
BABEȘ-BOLYAI UNIVERSITY
TRADITIO ET EXCELLENTIA

BRCC British Romanian Chamber of Commerce

ISACA Trust in, and value from, information systems Romania Chapter

(ISC)² CHAPTER ROMANIA

CLOUD SECURITY ALLIANCE OFFICIAL CHAPTER Romania Chapter CSA

CARTEA DALIEI

x86 GENERATION

WOMEN 4CYBER EUROPEAN CYBER SECURITY ORGANISATION ROMANIA

ȘCOALA INFORMALĂ DE IT®

TSM TODAY SOFTWARE MAGAZINE

DevExperience

ITCAMP

MOBZINE.RO

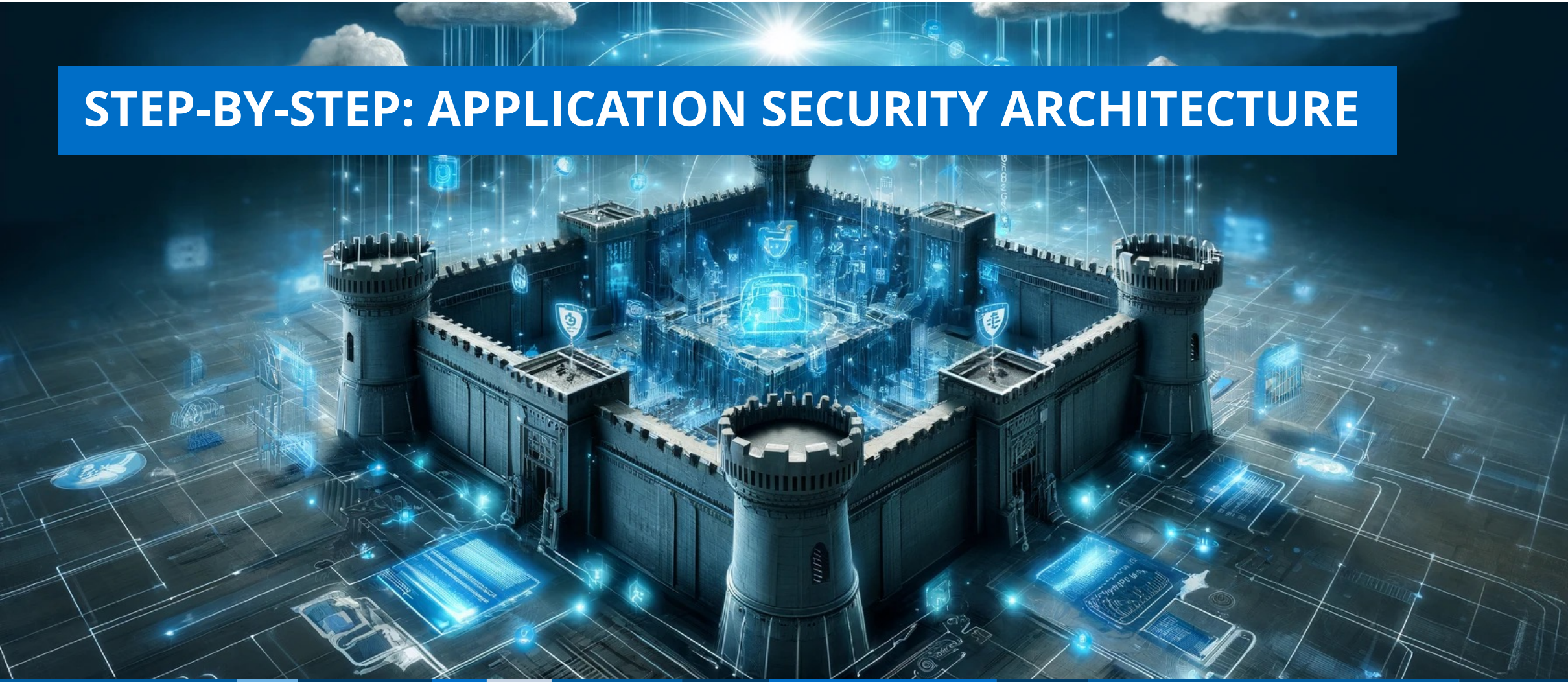
SecurityPatch

ROTSA The Highway of Romanian Tech Startups

techcelerator

4/29/24 | Rico Komenda

STEP-BY-STEP: APPLICATION SECURITY ARCHITECTURE



Rico Komenda

Who?

- **Husband and father**

- **Senior Security Consultant @ adesso SE**
- **International trainer and speaker**
- **Consulting**
  - AppSec, CloudSec, OffSec, AISec

<u>Mission statement:</u>
Securing the digital world, one byte at a time

EFFECTS OF CYBER ATTACKS

CYBERCRIME

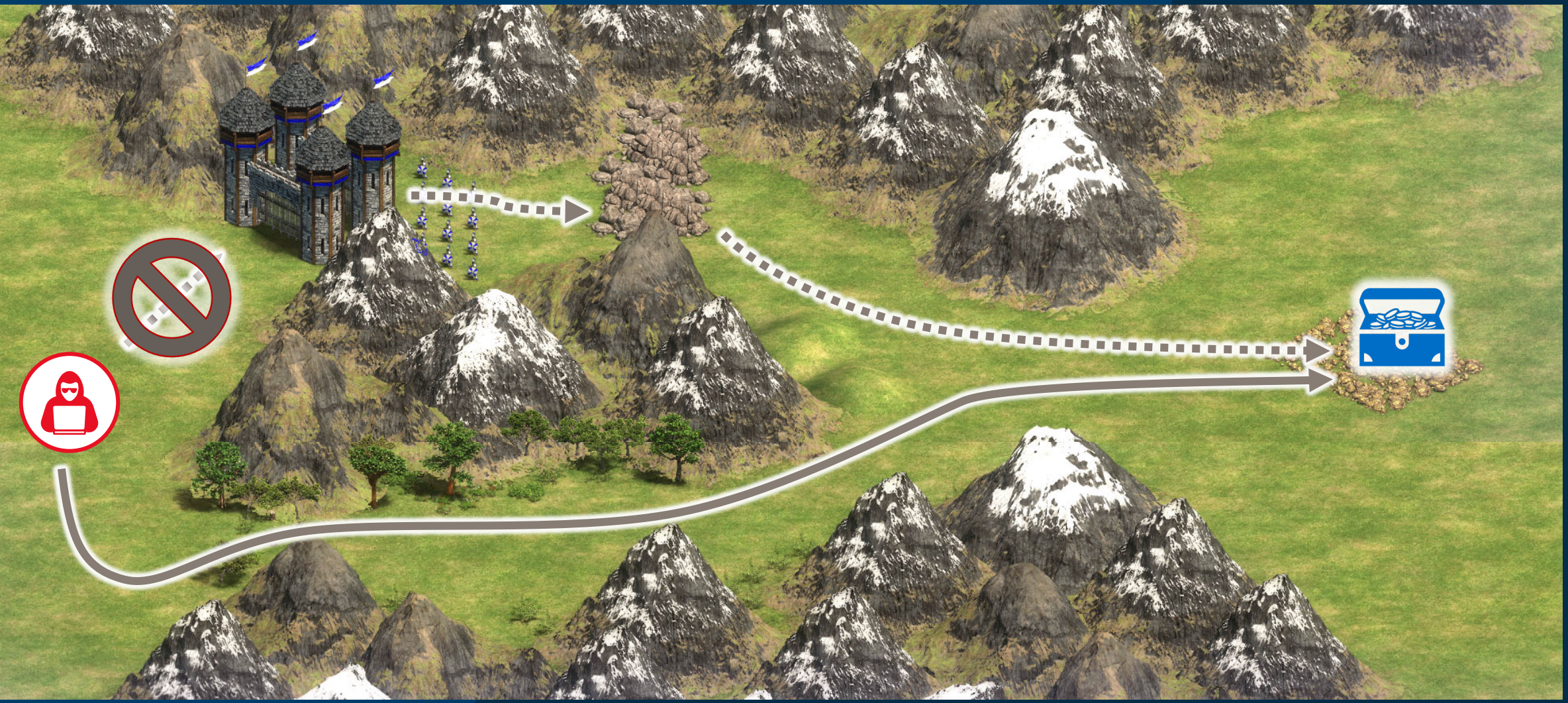
2022: around 136,000 registered cybercrime offences in DE
Increase of +3% compared to the previous year

How does it happen?

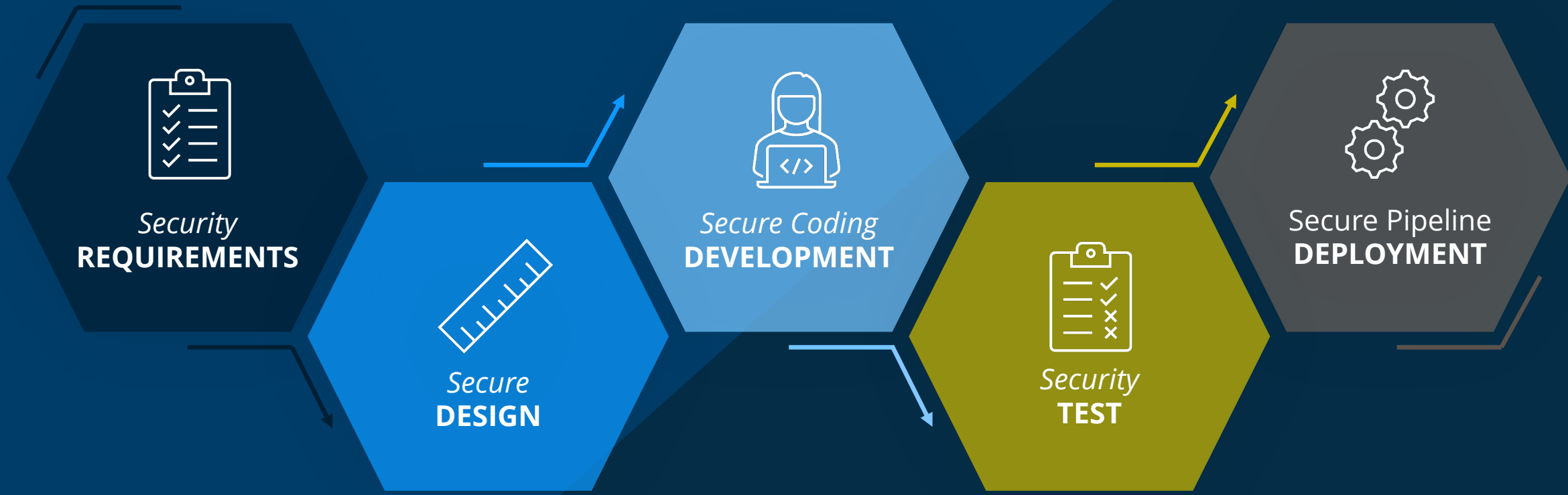
- Strongly advancing digitalization
- Increasing professionalization of perpetrators
- Low barriers to entry through CaaS (Cybercrime-as-a-Service)

Cybercrime: professional business

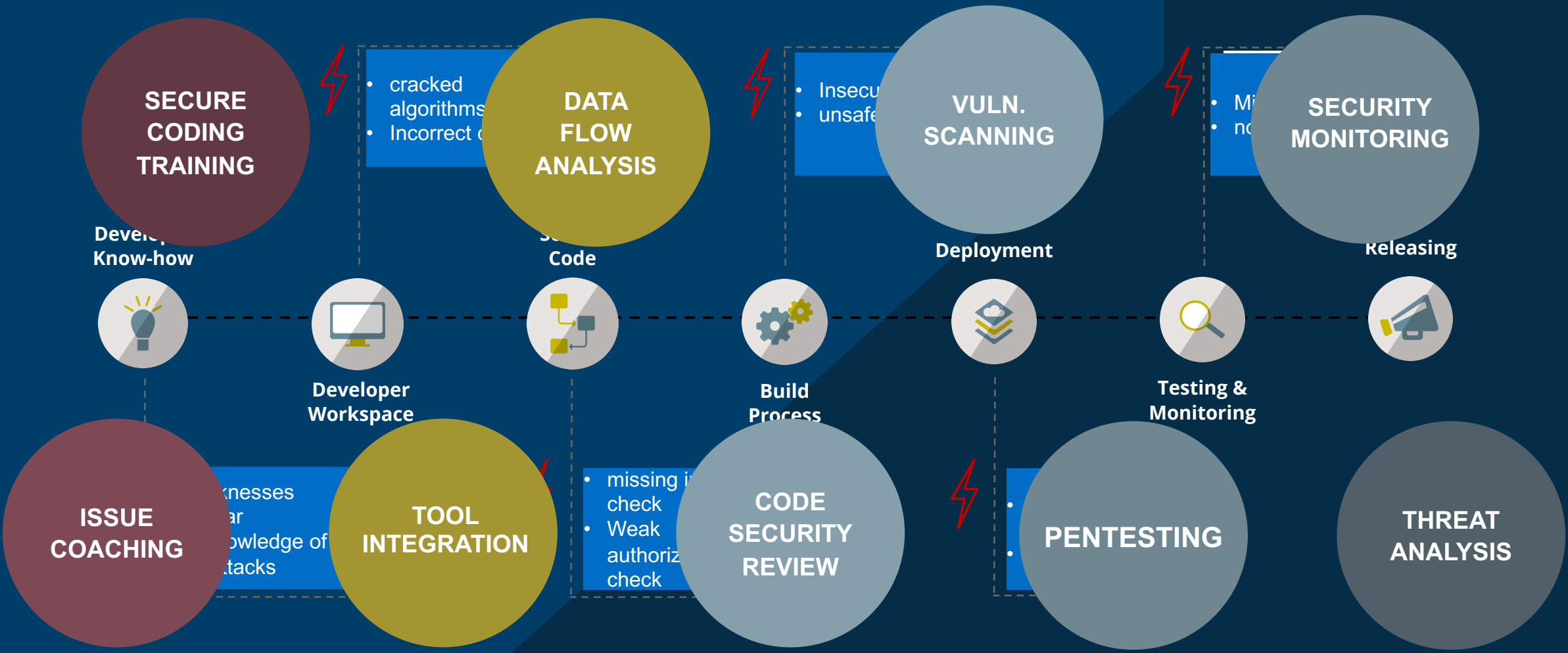
PATH OF LEAST COST/RESISTANCE



SECURITY IS A PROCESS

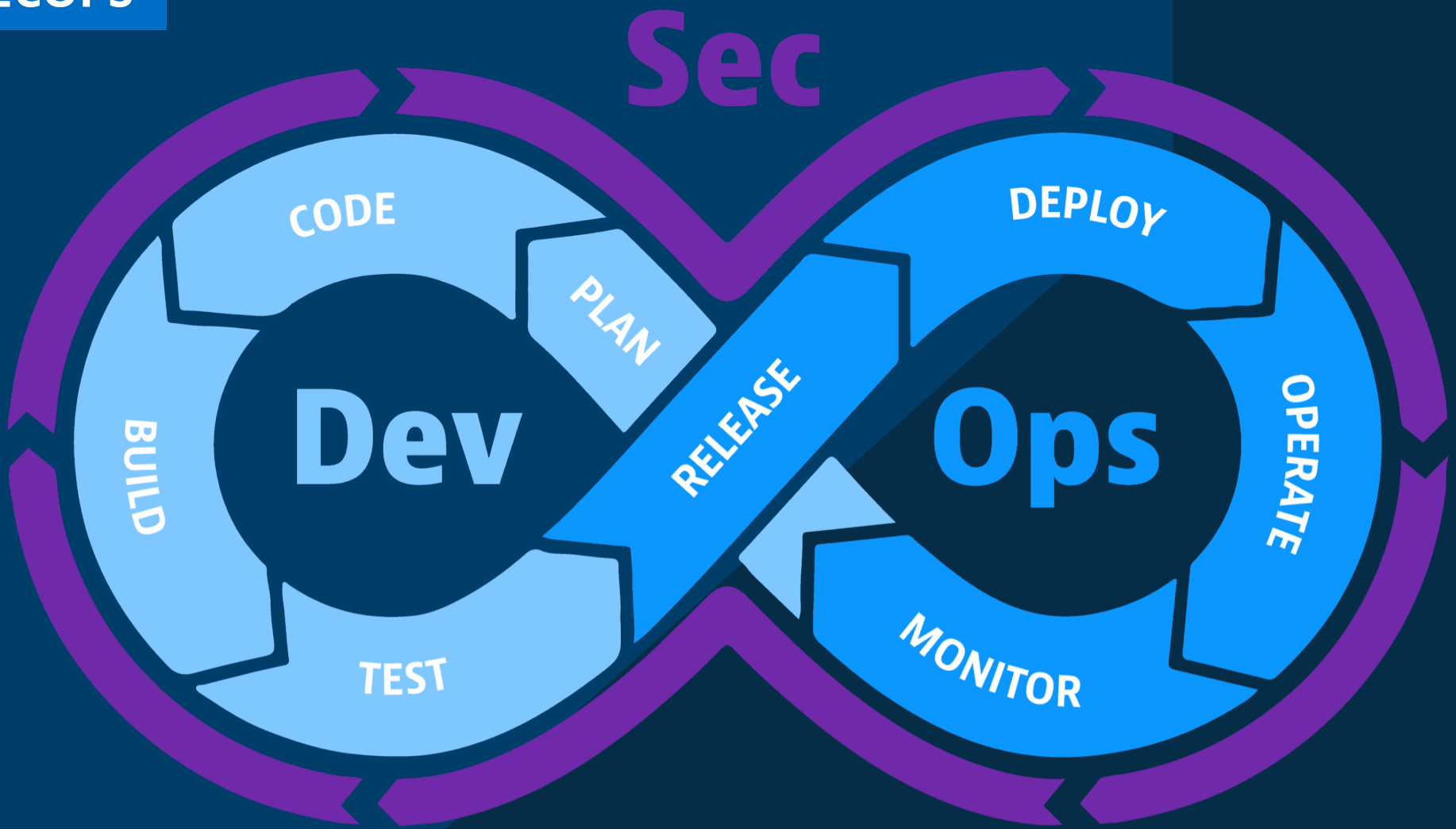


SOFTWARE DEVELOPMENT LIFECYCLE

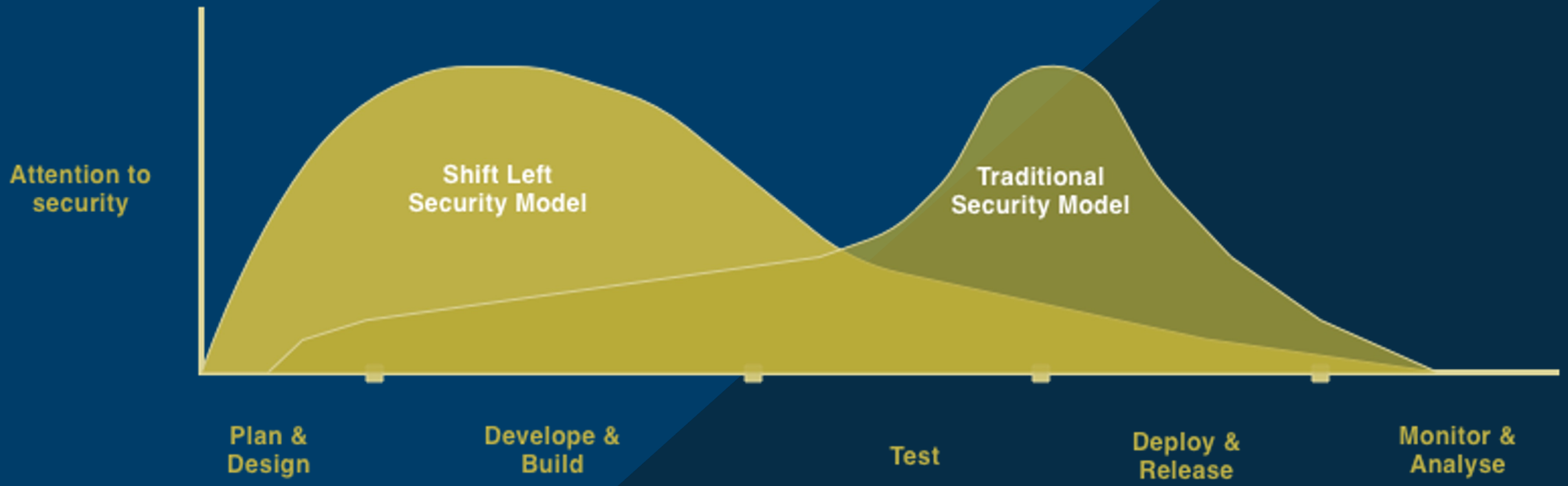


DEVOPS CYCLE

DEVSECOPS


Sec
CODE
PLAN
BUILD
TEST
RELEASE
DEPLOY
OPERATE
MONITOR
Dev
Ops

SECDEVOPS & SHIFT-LEFT



SECURITY CONCEPTS

1. Assume Breach & Zero Trust
2. Defense in Depth
3. Principle of least privilege
4. Principle of failing securely
5. Supply Chain Security
6. Security by Obscurity
7. Attack Surface Reduction
8. Useable Security

ASSUME BREACH
&
ZERO TRUST

ASSUME BREACH

Design as you though you have already been, or will be, brached.

React as though you have been breached

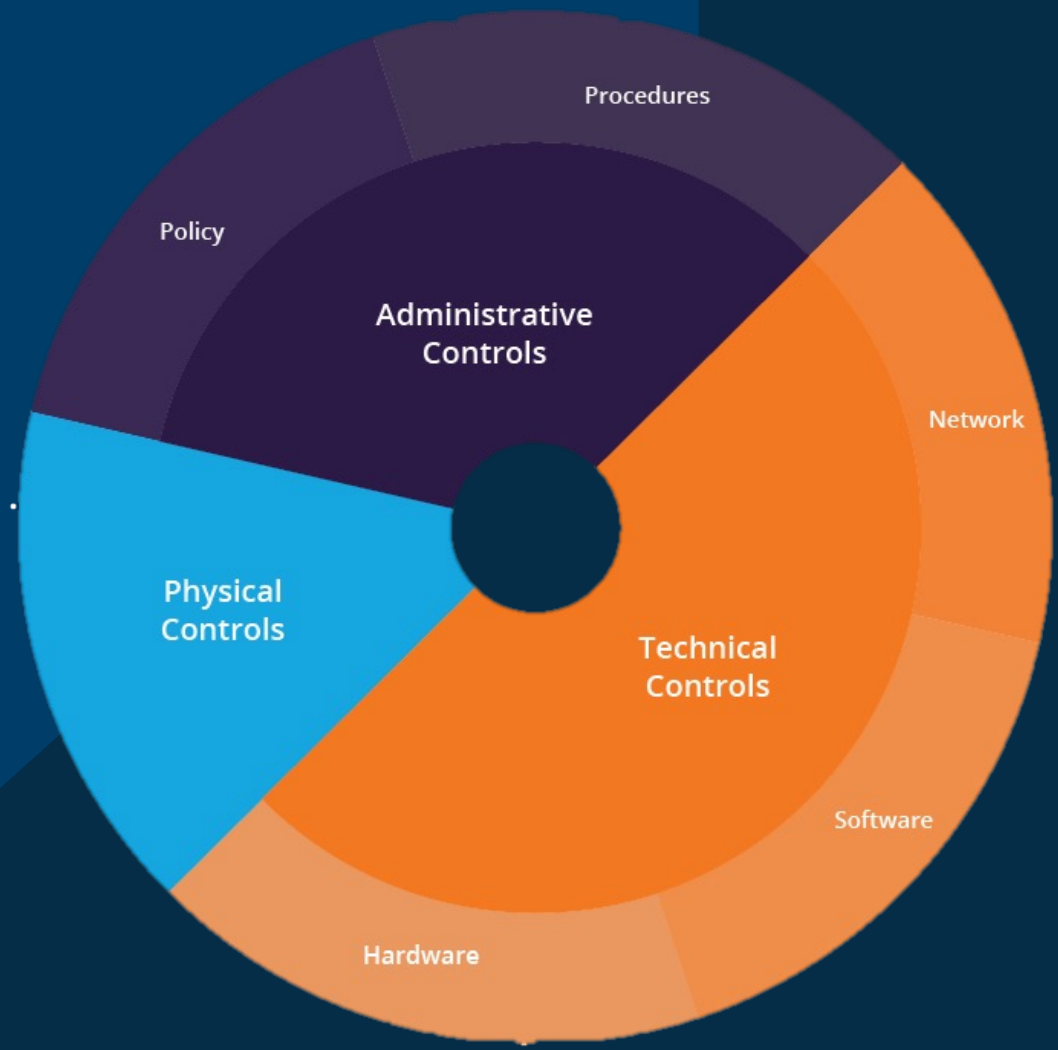
ZERO TRUST

No implicit trust between components, apps, network, system, users, ...

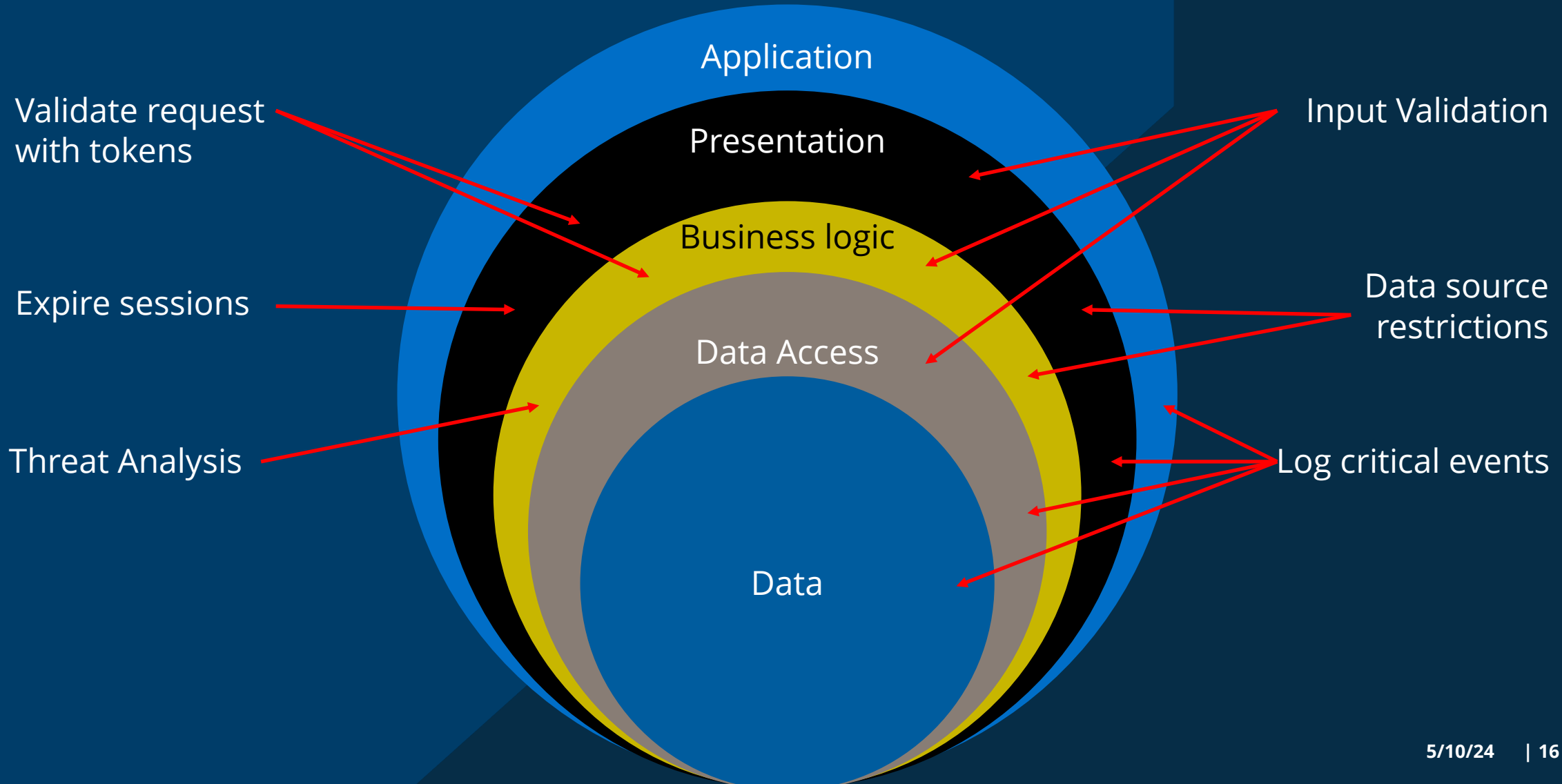
DEFENSE IN DEPTH

LAYERED DEFENSE IN DEPTH

- **Layers of security, instead of only one defense, use several**
- **In case on layer fails, another will protect your system**



DEFENSE IN DEPTH IN THE SOFTWARE LAYER

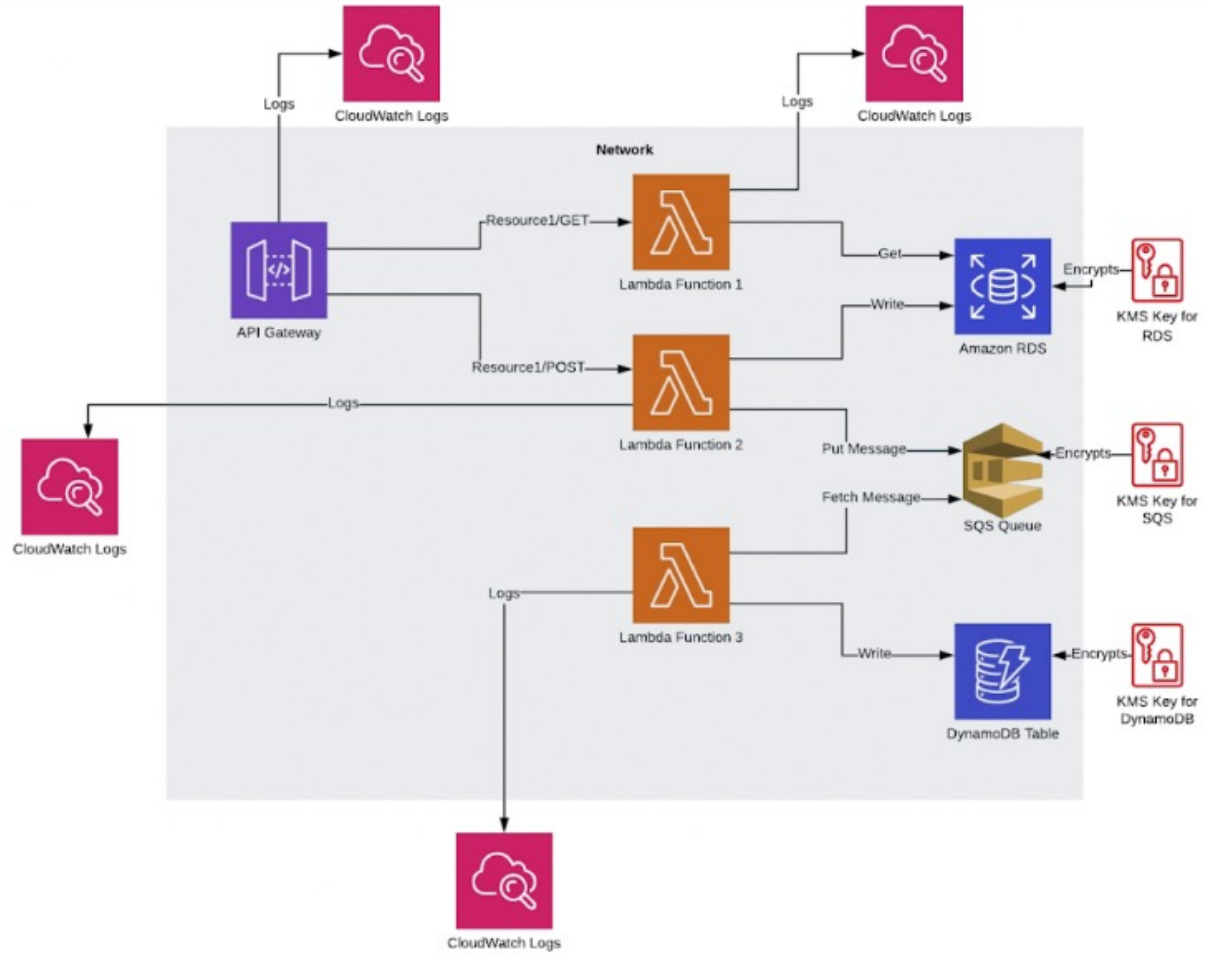


PRINCIPLE OF LEAST PRIVILEGE

PRINCIPLE OF LEAST PRIVILEGE

- **Providing only the amount of access and permission required to perform a specific function and nothing more**

EXAMPLE: AWS DYNAMODB



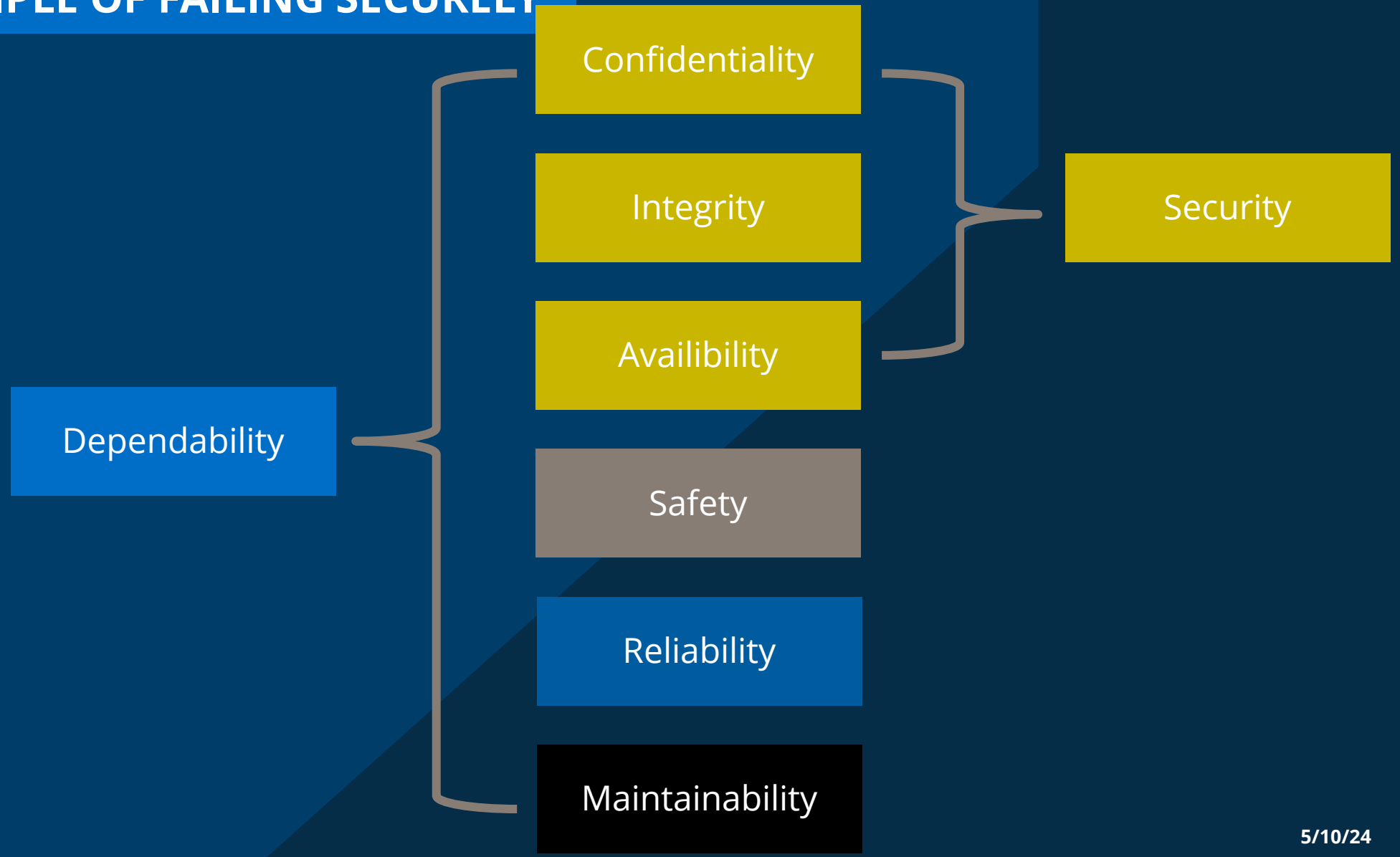
Permissions Sets:

- API
  - Resource Policy
- Lambda Functions 1, 2, 3
  - IAM Role + Policies
  - Resource Policy
- RDS Datastore
  - Security Group/s
- Message Queue
  - Access Policy
- NoSQL (DynamoDB) Database
- KMS Keys
  - Key Policy

PRINCIPLE OF FAILING SECURELY

REAL-LIFE EXAMPLE: DOOR-LOCK FAILING OPEN VS. SECURELY

PRINCIPLE OF FAILING SECURELY



SECURITY CHAOS ENGINEERING @ CLOUD

ID	Cloud Resource	Chaos Action	Description
AP1	User	create	create random user
AP2	User	delete	delete existing user
AP3	User	modify	change user configuration e.g. privileges, role or group
AP4	Policy	create	create new policies with random ACLs and attach to cloud resource(s)
AP4	Policy	modify	modify existing policy e.g. change ACL to deny original owner access to the resource
AP6	Policy	delete	detach policy from a resource, delete the policy
AP7	Role	create	create a new role
AP8	Bucket	make public	alter private configuration to public
AP9	Bucket	disable logging	stop logging API calls against bucket
AP10	Bucket	make unavailable	simulate bucket unavailability e.g. by changing bucket ACL from ALLOW to DENY

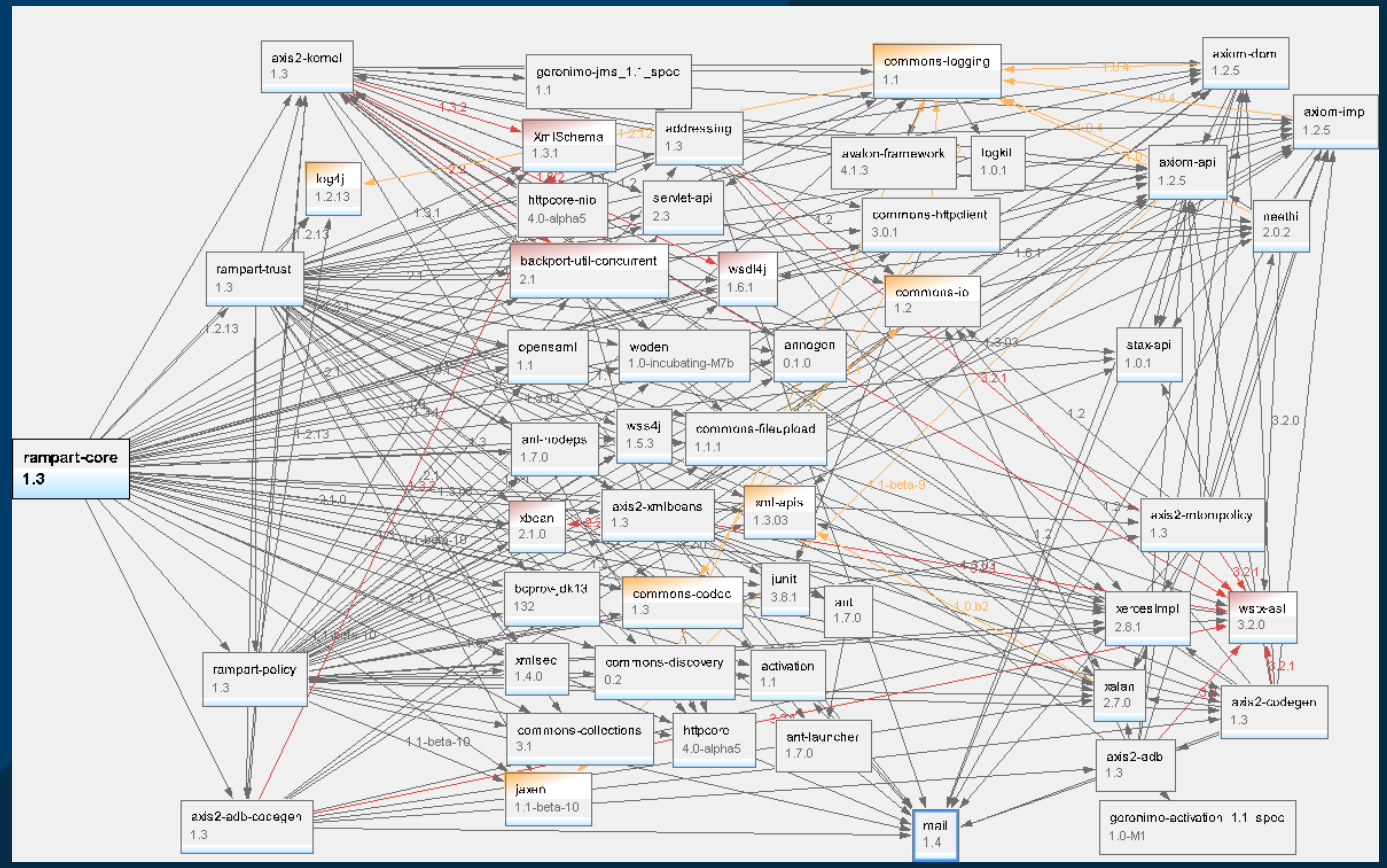
SECURITY ENGINEERING TOOLS

ChaosToolkit

SUPPLY CHAIN SECURITY

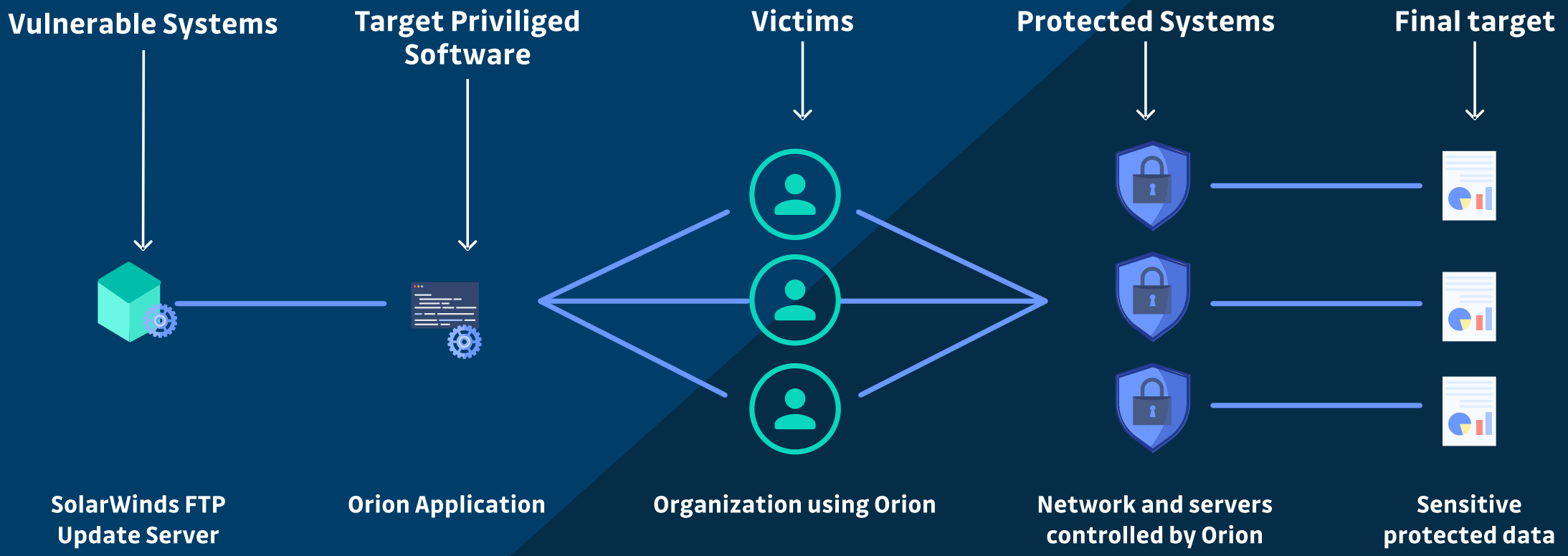
SUPPLY CHAIN SECURITY

- All of the components, libraries, frameworks and any other code you did not write, that you put in your app make up your supply chain
- Each dependency needs to be secure



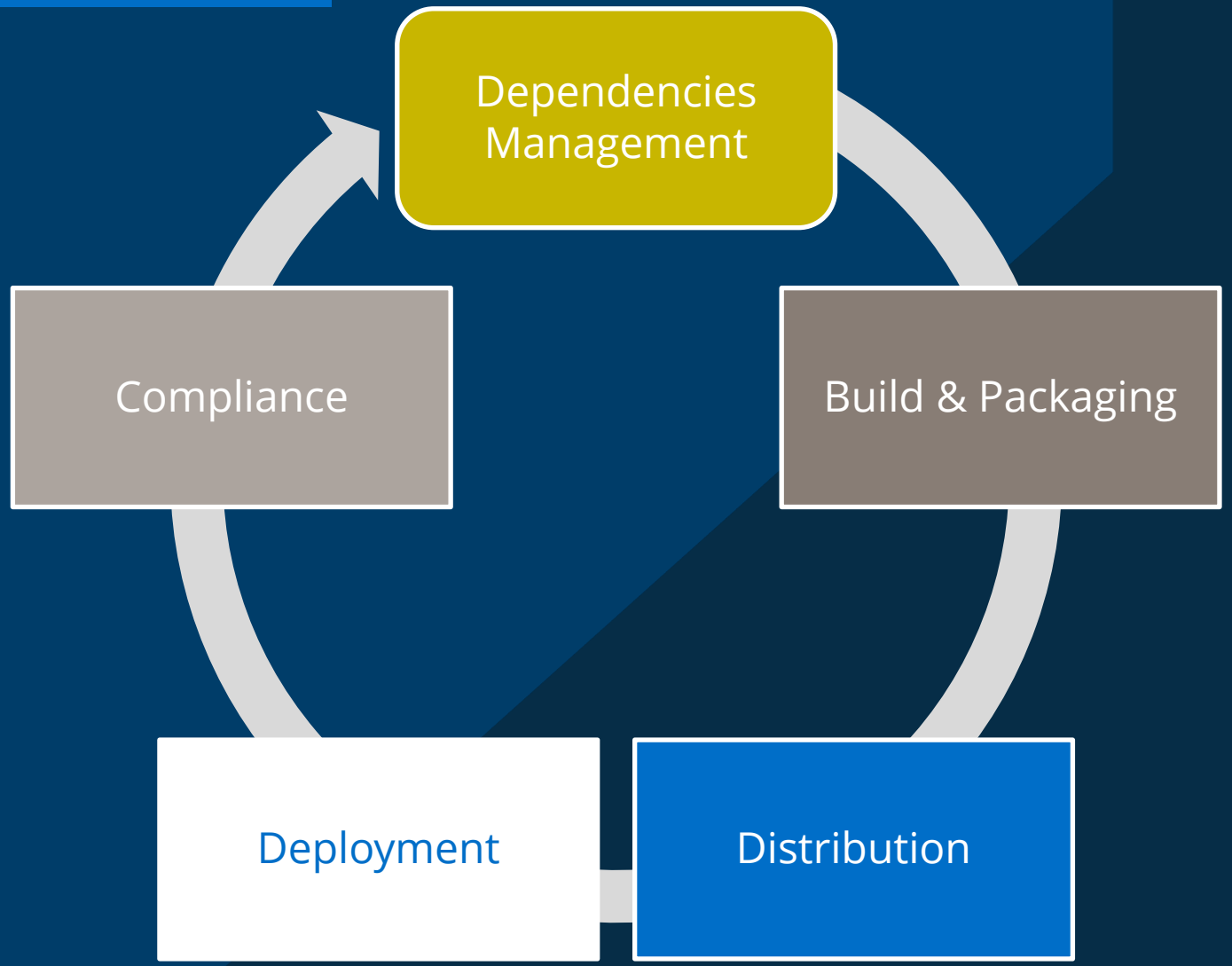
SUPPLY CHAIN SECURITY

SolarWinds - Attack through a trusted system with privileged access



SUPPLY CHAIN SECURITY

SUPPLY CHAIN SECURITY

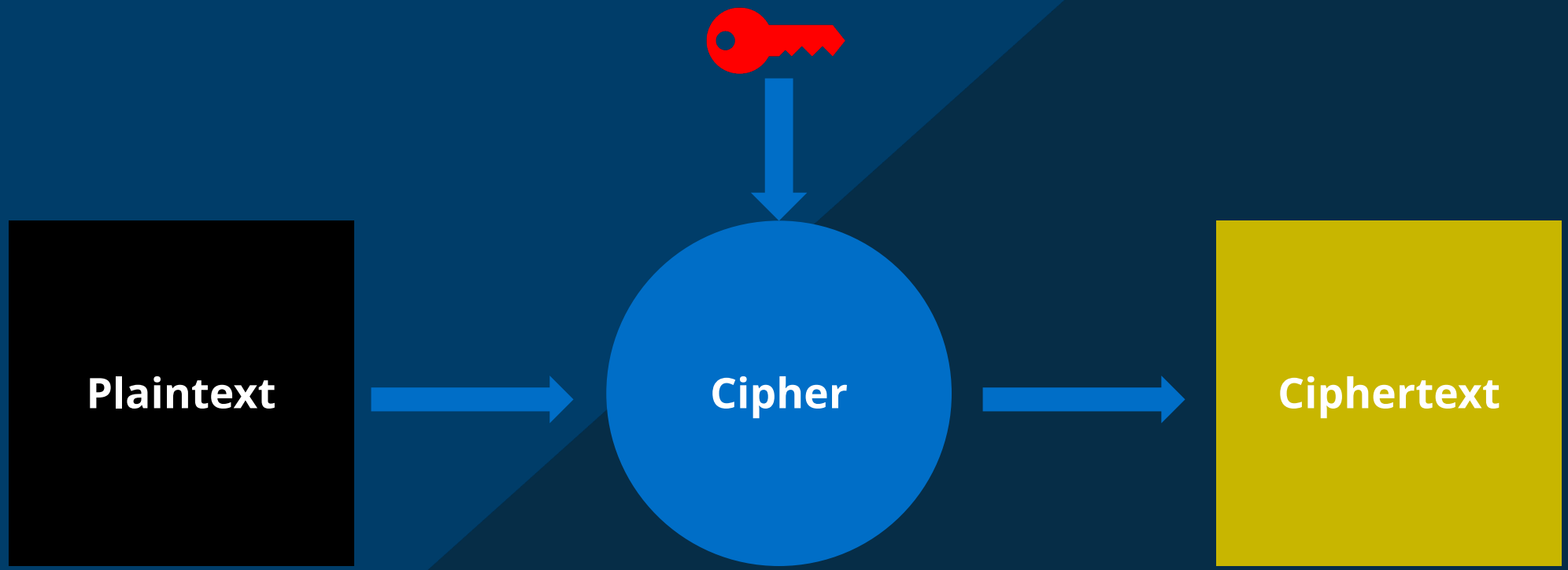


SECURITY BY OBSCURITY


HE WAS PREACHING
SECURITY-BY-OBSCURITY

The Kerchoff Principle

A cryptographic system should be secure even if everything about the system, except the key, is public knowledge



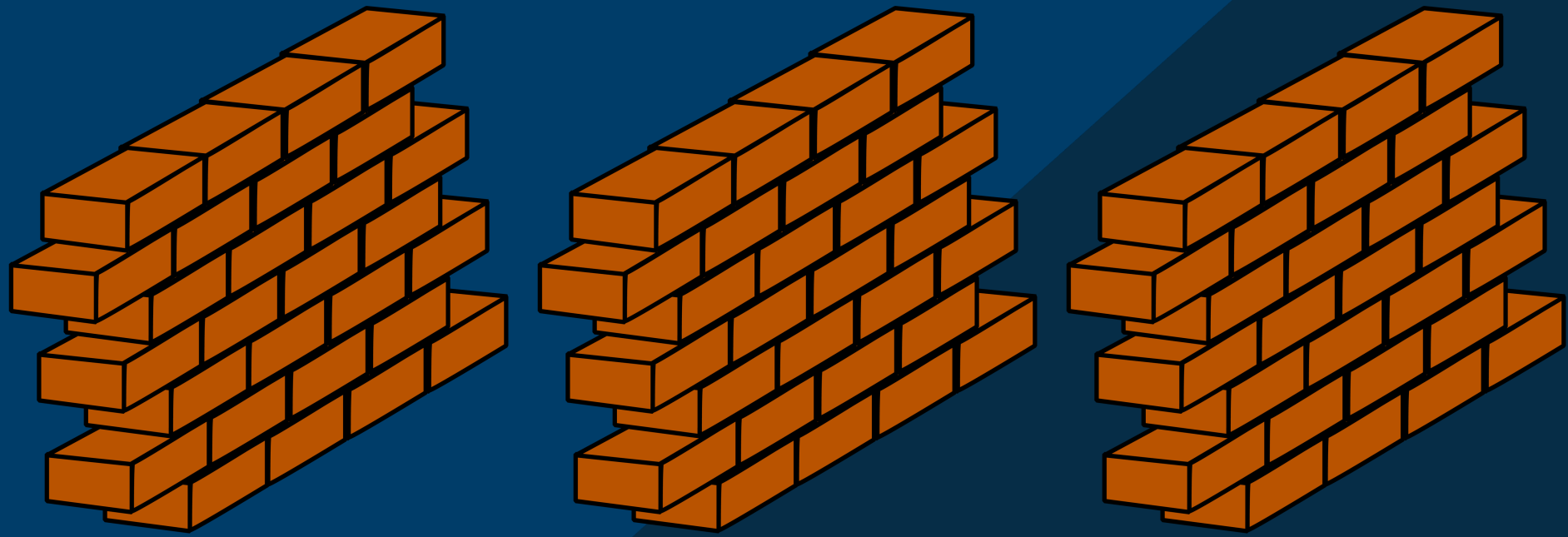
REAL-LIFE EXAMPLE: PASSWORD ON PAPER UNDER THE KEYBOARD

SECURITY BY OBSCURITY

PROS

CONS

SECURITY BY OBSCURITY



ATTACK SURFACE REDUCTION

REMOVE ANY UNUSED PARTS OF YOUR CODE

EVERY PART OF YOUR APPS AND SYSTEM IS PART OF YOUR ATTACK SURFACE

THE LESS YOU HAVE, THE LESS THERE IS TO ATTACK

USEABLE SECURITY

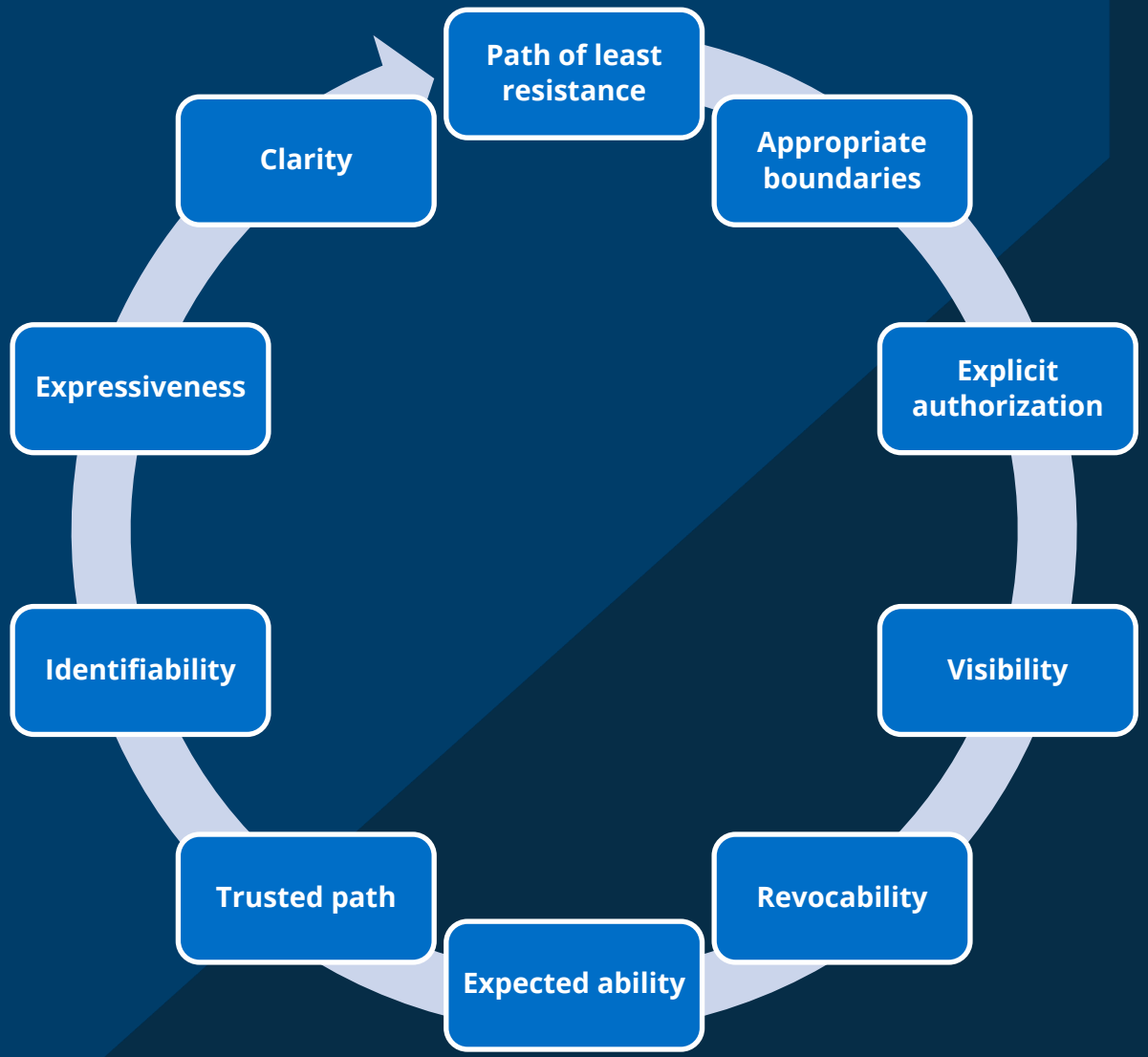
USEABLE SECURITY

USEABLE SECURITY

IF SECURITY FEATURES CAUSE USER PROBLEMS, THEY'LL FIND WAYS AROUND THEM

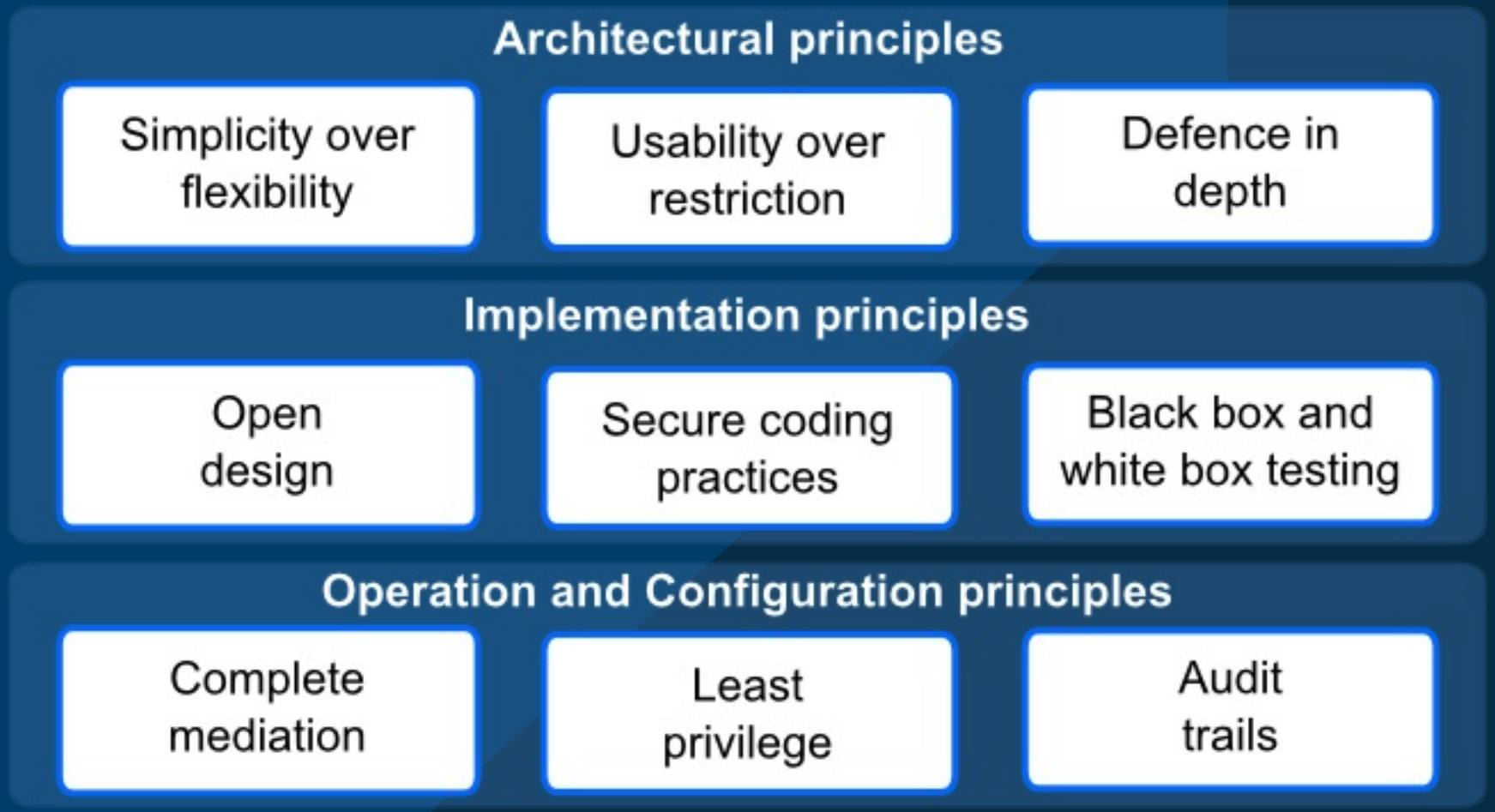
COMPROMISES AND CREATIVE SOLUTIONS CAN LEAD TO CUSTOMER DELIGHT AND BETTER COMPLIANCE

DESIGN PRINICPLES, KAI- PING YEE

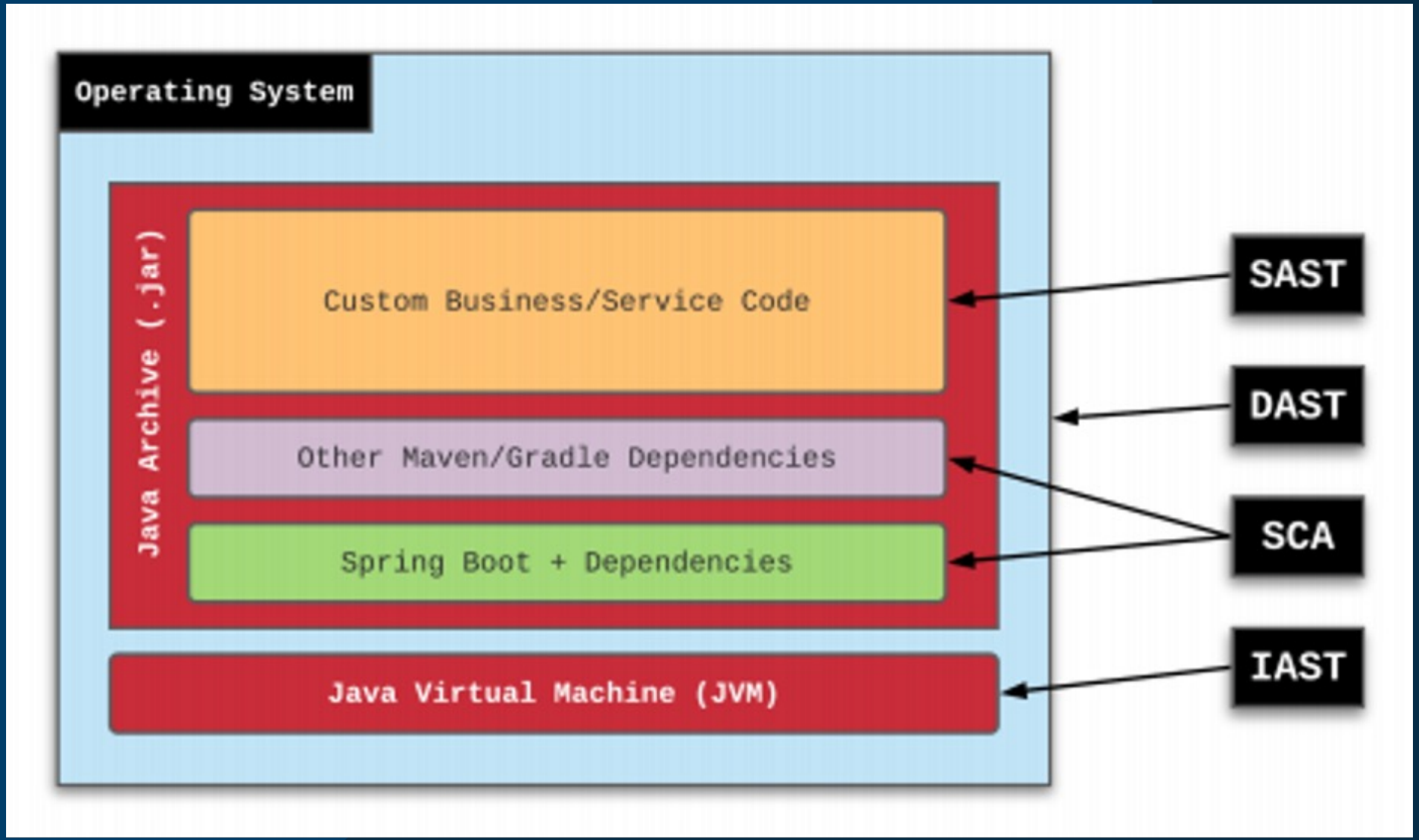


SOME TYPICAL APPSEC STUFF

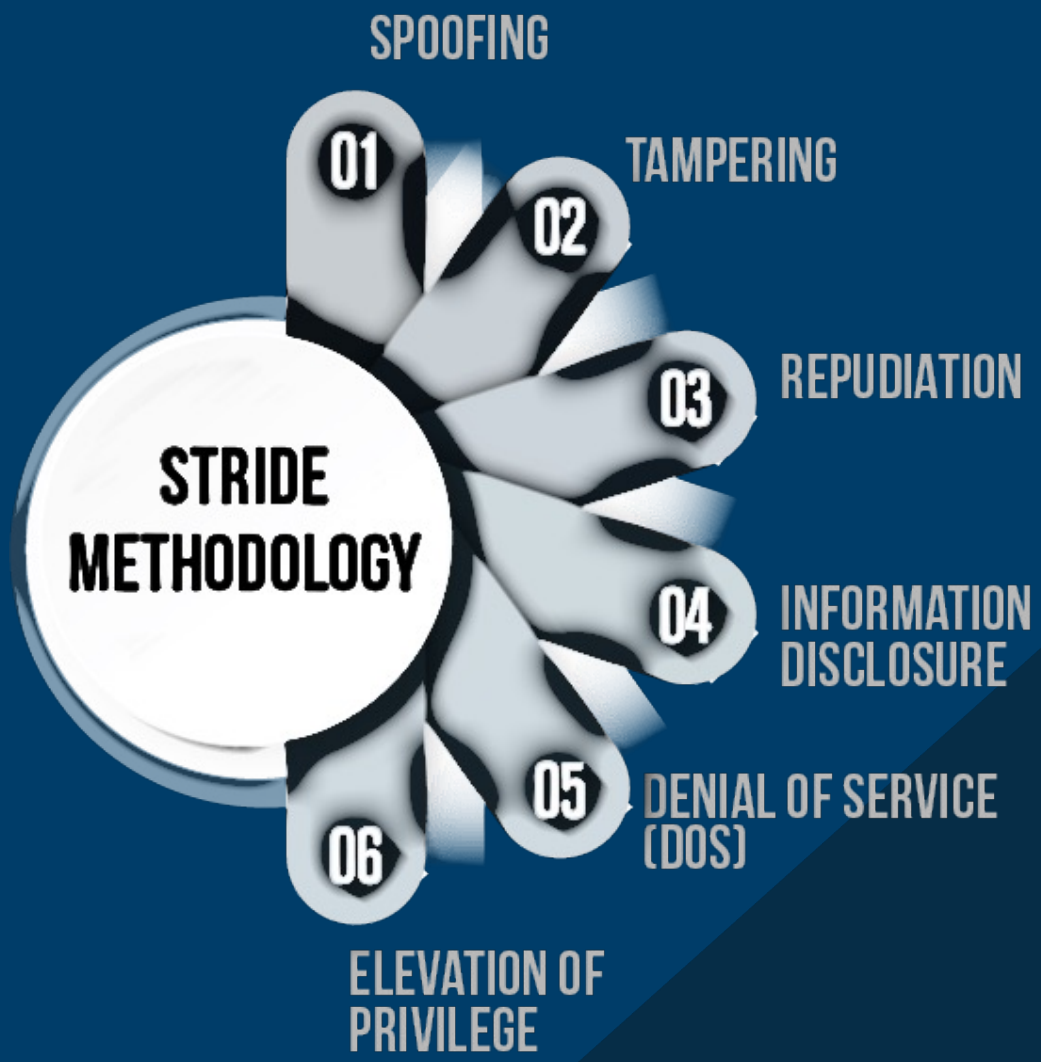
OPEN SECURITY ARCHITECTURE



APPLICATION SECURITY TESTING



THREAT MODELLING



OWASP ASVS

OWASP Application Security Verification Standard 4.0.2

The OWASP Application Security Verification Standard (ASVS) Project provides a basis for testing web application technical security controls and also provides developers with a list of requirements for secure development.

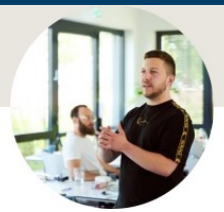
	Applicability	Building			Building, Configuration, Deployment Assurance and Verification			Assurance and Verification	
Level 1	All apps		Secure Coding	Standards and checklists	Secure & Peer Code Review	DevSecOps	Unit and Integration Tests	Penetration Testing	DAST
Level 2	All apps	Security Architecture and Reviews	Secure Coding	Standards and checklists	Secure & Peer Code Review	DevSecOps	Unit and Integration Tests	Hybrid Reviews	SAST
Level 3	High Assurance	Security Architecture and Reviews	Secure Coding	Standards and checklists	Secure & Peer Code Review	DevSecOps	Unit and Integration Tests	Hybrid Reviews	SAST

Legend	Acceptable	Suitable

OUR RESULT AT THE END

QUESTIONS?

THANK YOU!



Rico Komenda

⚡ IT-Security Ambassador ⚡ Securing the Digital World, One Byte at a Time