EVOLVE DEVSECOPS TO MANAGE BOTH SPEED AND RISK

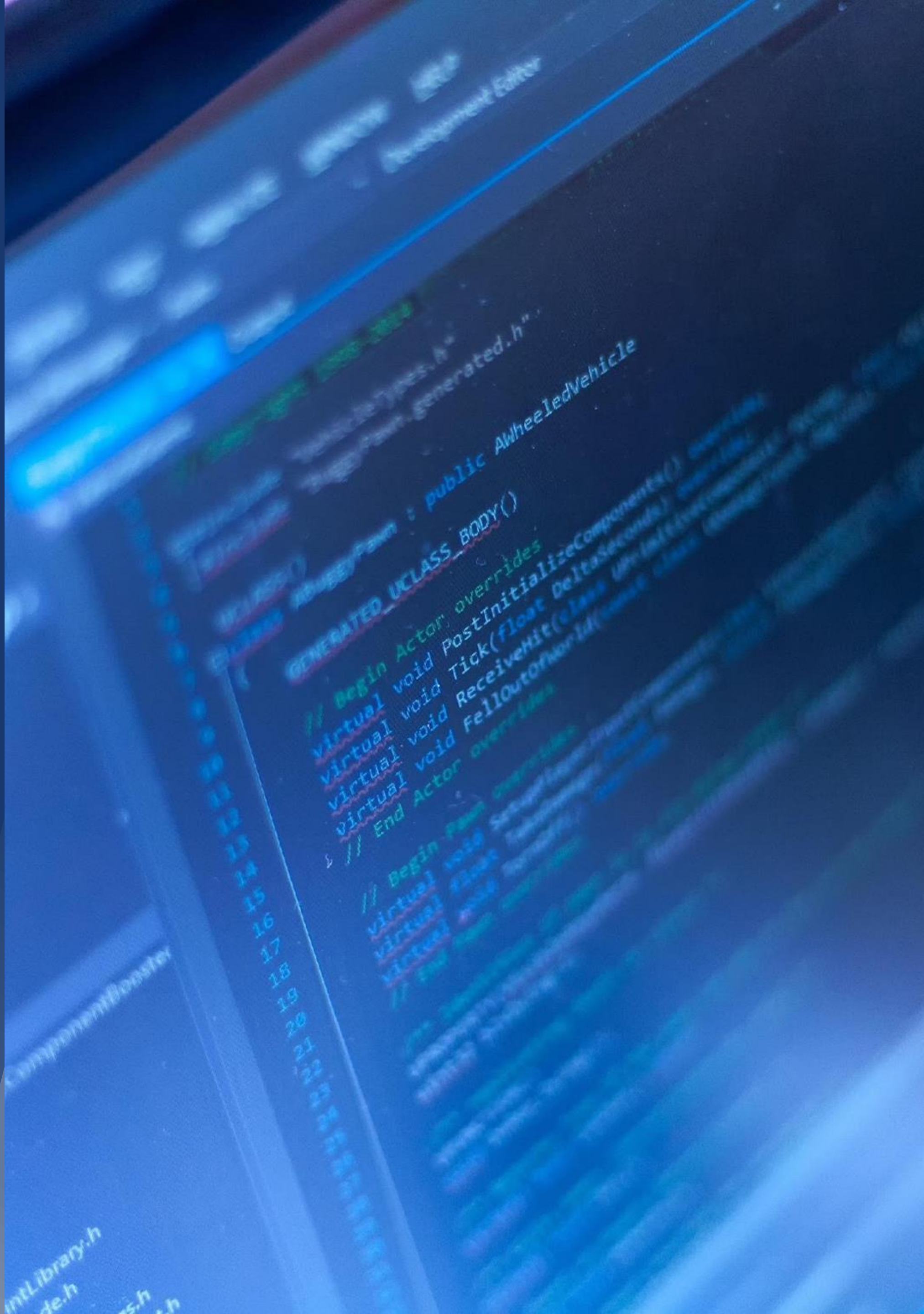
Security Compass

AGENDA

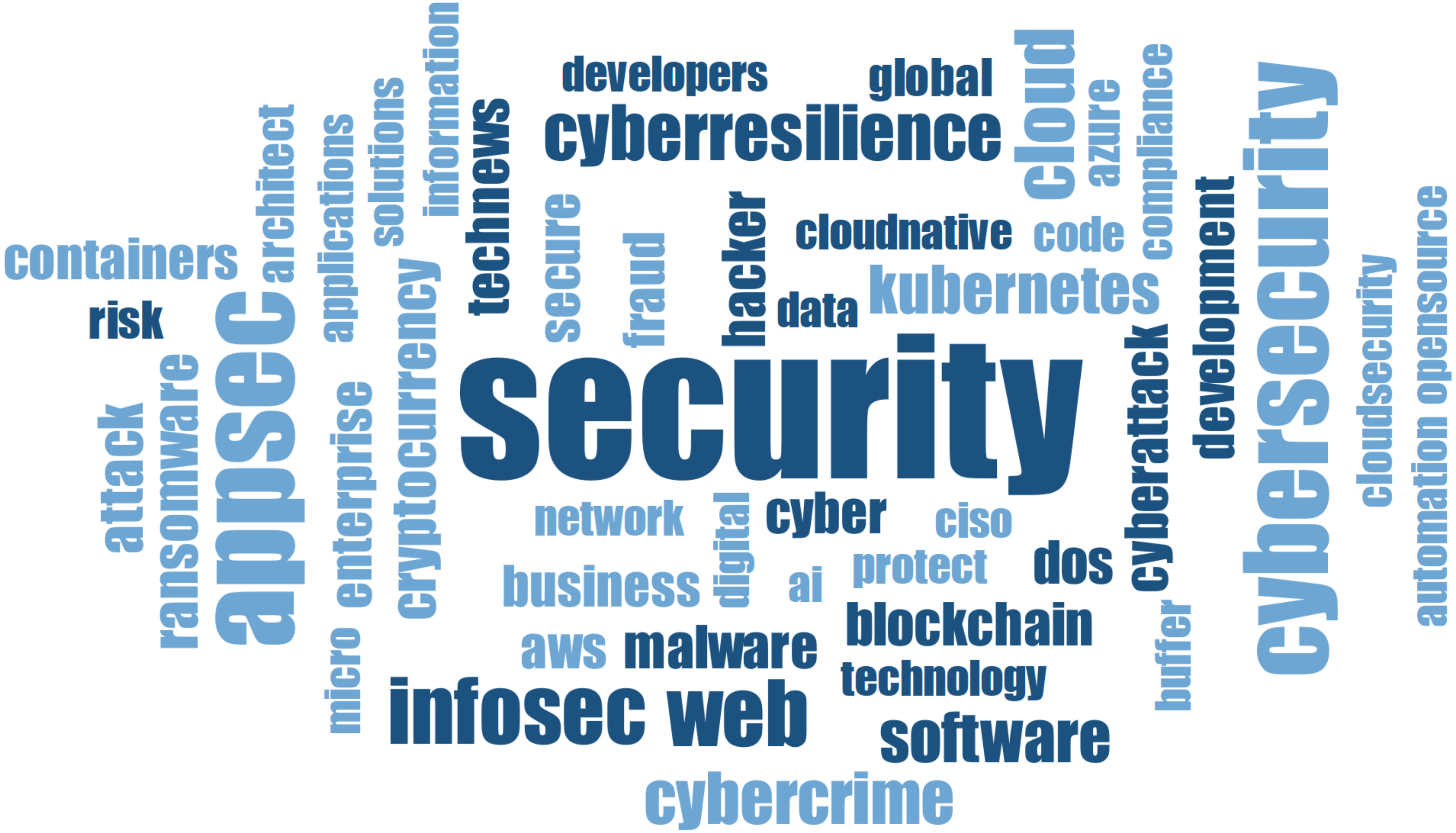
1. DevSecOps in the Context of Speed
2. DevSecOps in the Context of Risk
3. DevSecOps for Both Speed and Risk

SecurityCompass

DSO & SPEED

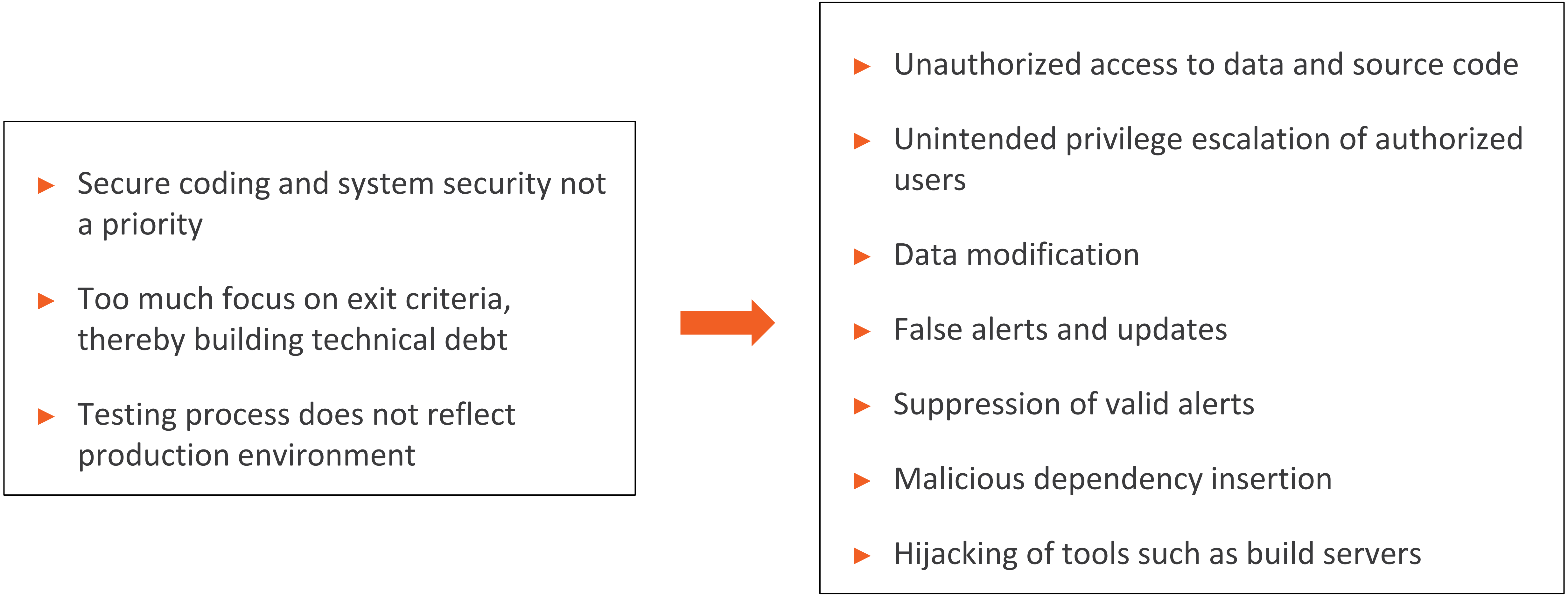


What is the DevSecOps Community Talking About?



Source: Twitter (#DevSecOps), 2020.

DevSecOps Challenges



- Secure coding and system security not a priority
- Too much focus on exit criteria, thereby building technical debt
- Testing process does not reflect production environment

- Unauthorized access to data and source code
- Unintended privilege escalation of authorized users
- Data modification
- False alerts and updates
- Suppression of valid alerts
- Malicious dependency insertion
- Hijacking of tools such as build servers

Source: Morales et al. "Security Impacts of Sub-Optimal DevSecOps Implementations in a Highly Regulated Environment", 2020.

DevSecOps Challenges

- We inherit a technology mess often not of our own making
- Organizations move into DevOps culture without addressing security
- No process or documentation for security reviews
- Haphazard security bolted on IT systems
- Cannot test all security requirements
- Adversary changes the environment

Source: D. Blum, Rational Cybersecurity for Business, *https://doi.org/10.1007/978-1-4842-5952*

Yet we still need to keep moving fast…

Security Competencies

SECURELY PROVISION (SP)

- Risk Management (RSK)
- Software Development (DEV)
- Systems Architecture (ARC)
- Technology R&D (TRD)
- Test and Evaluation (TST)
- Systems Development (SYS)

OPERATE AND MAINTAIN (OM)

- Data Administration (DTA)
- Knowledge Management (KMG)
- Customer Service and Technical Support (STS)
- Systems Administration (ADM)
- Network Services (NET)
- Systems Analysis (ANA)

OVERSEE AND GOVERN (OV)

- Exec Cyber Leadership (EXL)
- Training, Education, and Awareness (TEA)
- Program/Project Mgt (PMA) and Acquisition
- Strategic Planning & Policy (SPP)
- Legal Advice and Advocacy (LGA)
- Cybersecurity Management (MGT)

PROTECT AND DEFEND (PR)

- Cyber Defense Analysis (CDA)
- Cyber Defense Infra. Support (INF)
- Incident Response (CIR)
- Vulnerability Assessment & Management (VAM)

ANALYZE (AN)

- Threat Analysis (TWA)
- Exploitation Analysis (EXP)
- All-Source Analysis (ASA)
- Targets (TGT)
- Language Analysis (LNG)

COLLECT AND OPERATE (CO)

- Collection Operations (CLO)
- Cyber Operational Planning (OPL)
- Cyber Operations (OPS)

INVESTIGATE (IN)

- Cyber Investigation (INV)
- Digital Forensics (FOR)

Source: Adapted from NIST, “National Initiative for Cybersecurity Education (NICE): Cybersecurity Workforce Framework”, 2017.

Security Competencies

GOVERNANCE

Strategy & Metrics

- Identify gate locations, gather necessary artifacts
- Enforce gates with measurements and track exceptions
- Require a security sign off

Compliance & Policy

- Unify regulatory pressures
- Create policy
- Identify PII data inventory
- Implement and track controls for compliance
- Include software security SLA in all vendor contracts
- Impose policy on vendors

Training

- Provide awareness training

INTELLIGENCE

Attack Models

- Create a data classification scheme
- Identify potential attackers
- Gather and use attack intelligence
- Build attack patterns and abuse cases
- Create technology specific attack patterns
- Build an internal forum to discuss attacks

Security Features & Design

- Build and publish security features
- Build secure-by-design middleware frameworks and common libraries

Standards & Requirements

- Translate compliance constraints to requirements
- Identify open source
- Control open source risk

SSDL TOUCHPOINTS

Architecture Analysis

- Perform security feature review
- Define and use AA process
- Make the Software Security Group available as an AA resource or mentor

Code Review

- Use automated tools along with manual review
- Make code review mandatory for all projects
- Use centralized reporting to close the knowledge loop and drive training
- Use automated tools with tailored rules
- Use a top N bugs list

Security Testing

- Drive tests with security requirements
- Share security results with QA
- Include security tests in QA automation
- Drive tests with risk analysis results
- Begin to build and apply adversarial security tests (abuse cases)

DEPLOYMENT

Penetration Testing

- Feed results to defect management and mitigation system
- Use penetration testing tools internally

Software Environment

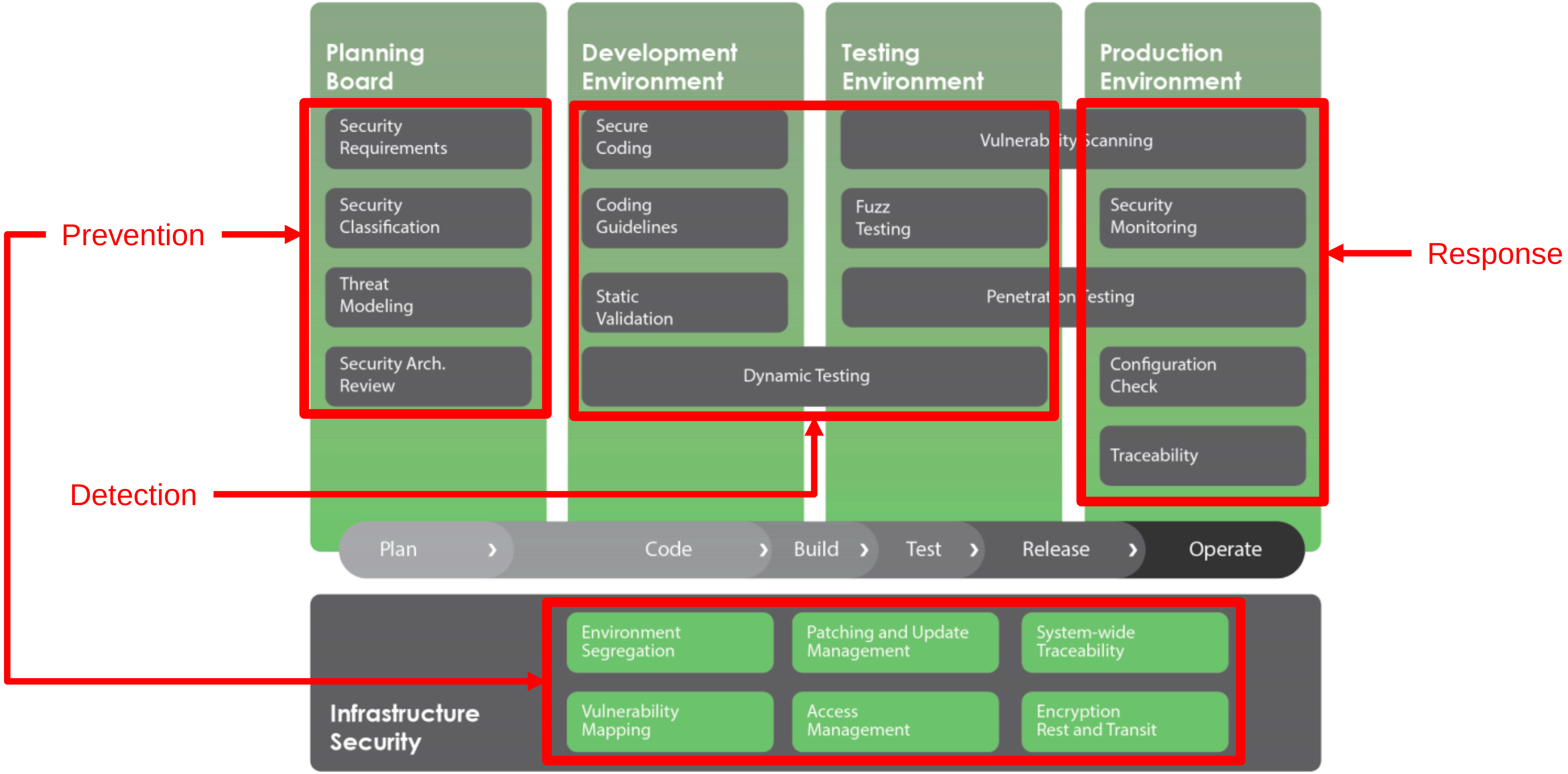
- Use application input monitoring
- Ensure host and network security
- Use application behavior monitoring and diagnostics
- Use application containers
- Use orchestration for containers and virtualized environments
- Enhance application inventory with operations BOM
- Ensure cloud security metrics

Configuration Management & Vulnerability Management

- Create or interface with incident response
- Identify software defects found in operations monitoring and feed them back to development
- Have emergency codebase response
- Track software bugs found in operations through the fix process
- Develop an operations inventory of applications
- Simulate software crises

Source: Koskinen. "DevSecOps: Building Security Into the Core of DevOps", 2020.

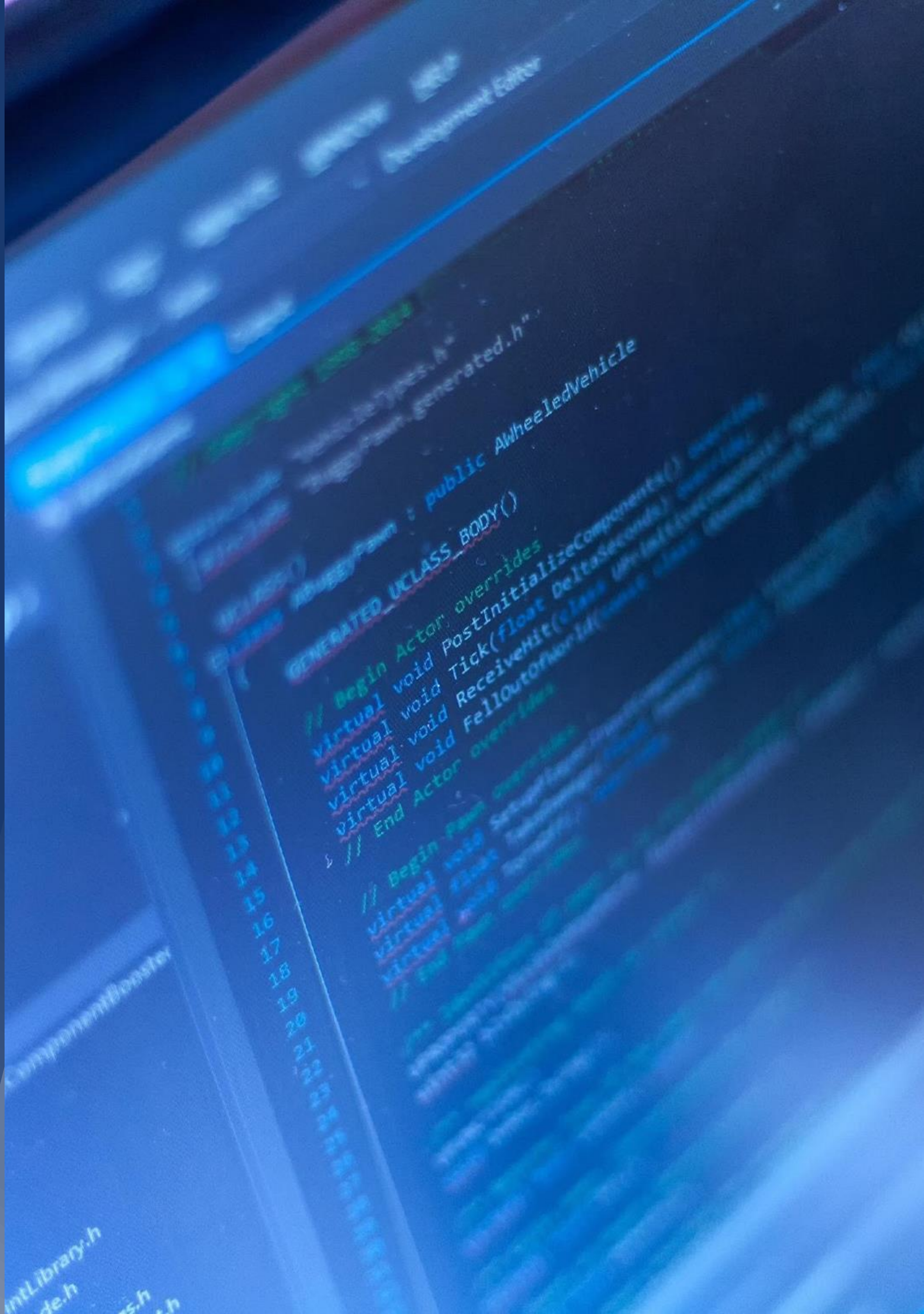
Security Best Practices



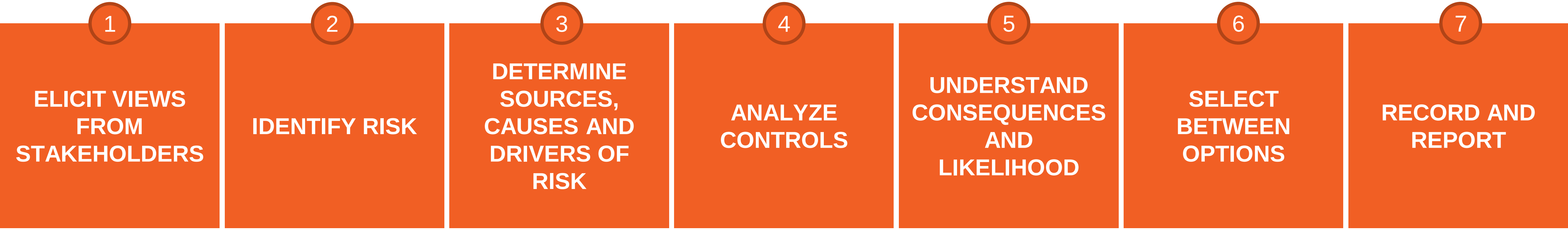
Source: Ahmed. "DevSecOps: Enabling Security by Design in Rapid Software Development", 2019.

Security Compass

DSO & RISK



The Risk Assessment Process



1 ELICIT VIEWS FROM STAKEHOLDERS

- Brainstorming
- Delphi technique
- Interview
- Survey

2 IDENTIFY RISK

- Checklist
- Taxonomy
- Classification
- Scenario

3 DETERMINE SOURCES, CAUSES AND DRIVERS OF RISK

- Ishikawa

4 ANALYZE CONTROLS

- Bow Tie Analysis

5 UNDERSTAND CONSEQUENCES AND LIKELIHOOD

- Business Impact Analysis
- Privacy Impact Analysis

6 SELECT BETWEEN OPTIONS

- Cost/Benefit Analysis

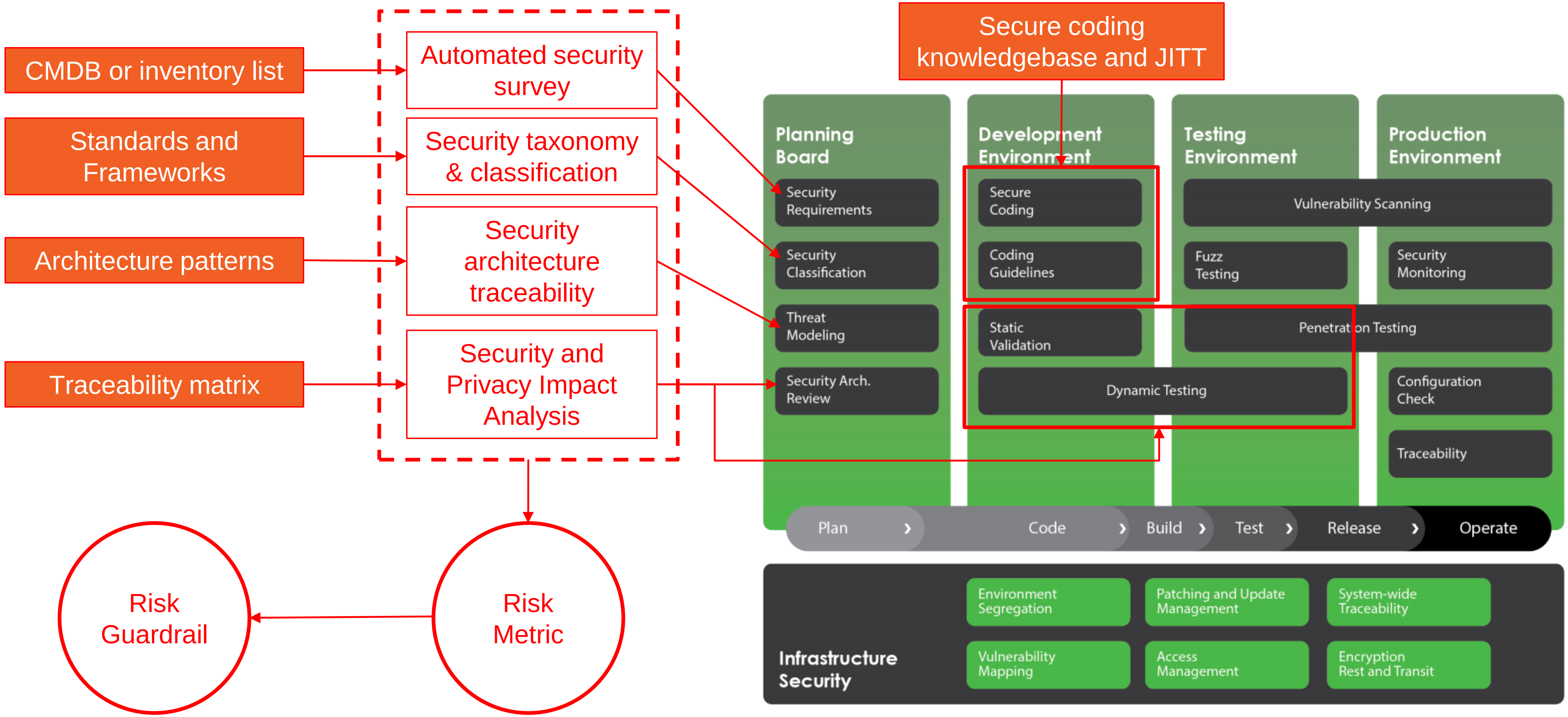
7 RECORD AND REPORT

- Risk Register

Source: ISO. “ISO 31010: Risk Management – Risk assessment techniques”, 2019.

How do we integrate this with DevSecOps?

Combining Speed and Risk



CMDB or inventory list

Standards and Frameworks

Architecture patterns

Traceability matrix

Automated security survey

Security taxonomy & classification

Security architecture traceability

Security and Privacy Impact Analysis

Risk Metric

Risk Guardrail

Secure coding knowledgebase and JITT

Planning Board

Security Requirements

Security Classification

Threat Modeling

Security Arch. Review

Development Environment

Secure Coding

Coding Guidelines

Static Validation

Dynamic Testing

Testing Environment

Vulnerability Scanning

Fuzz Testing

Penetration Testing

Production Environment

Security Monitoring

Configuration Check

Traceability

Plan › Code › Build › Test › Release › Operate

Infrastructure Security

Environment Segregation

Patching and Update Management

System-wide Traceability

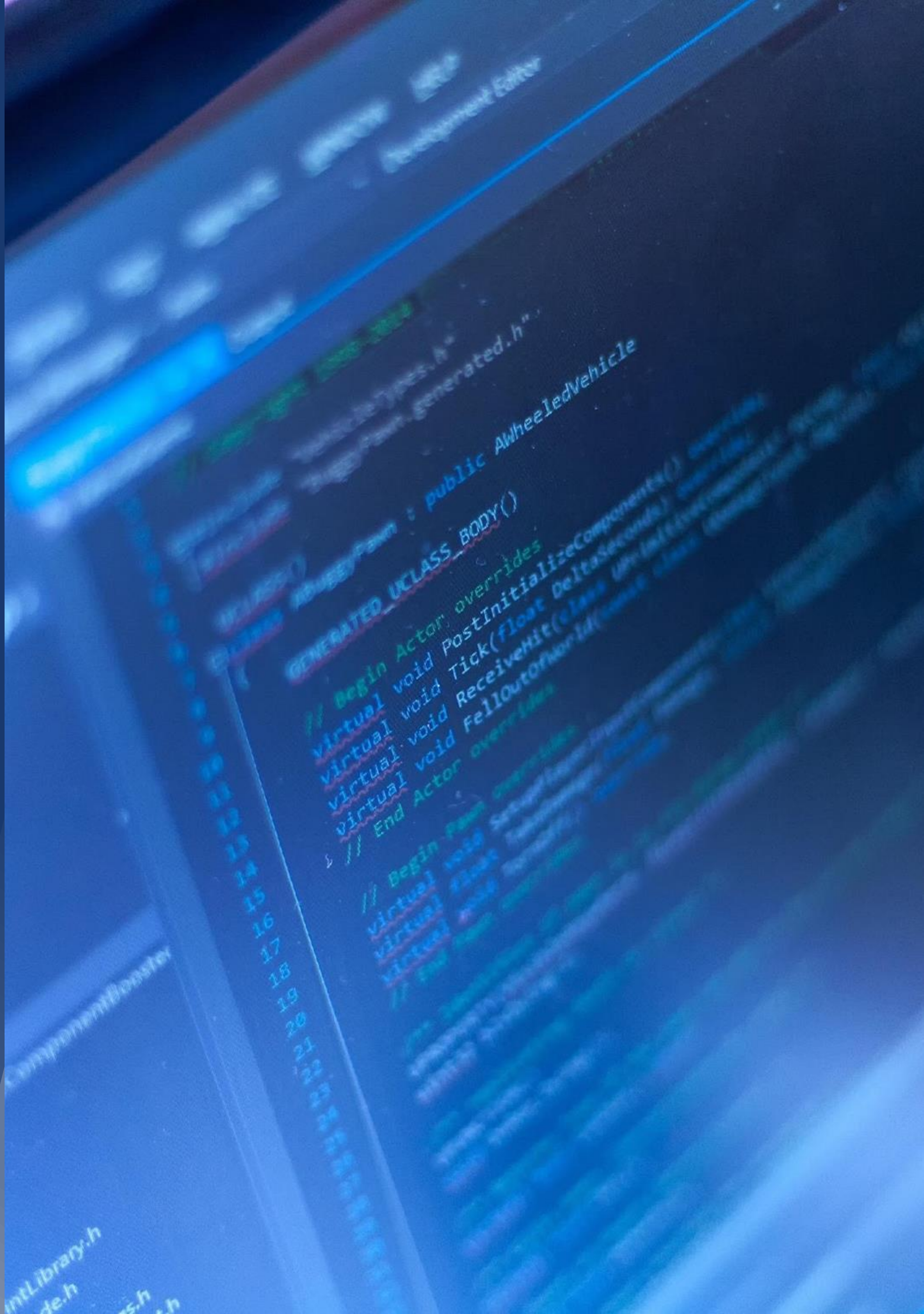
Vulnerability Mapping

Access Management

Encryption Rest and Transit

Security Compass

NEXT STEPS



Next Steps

Shorter Term

- Look for areas where good practices are missing and advocate for implementing those as part of an existing security roadmap
- Demonstrate and teach good practices such as risk assessments and threat modeling
- Influence the business toward reducing complexity and following good practices
- Be aware that you may not have all the scenarios and answers available

Longer Term

- Align with existing IT strategy
- Look through the lens of risk across all systems, even legacy systems
- Build relationships with people outside IT and Security

Security Compass

THANK YOU