OPEN SECURITY SUMMIT

Team Topologies for Cyber Security

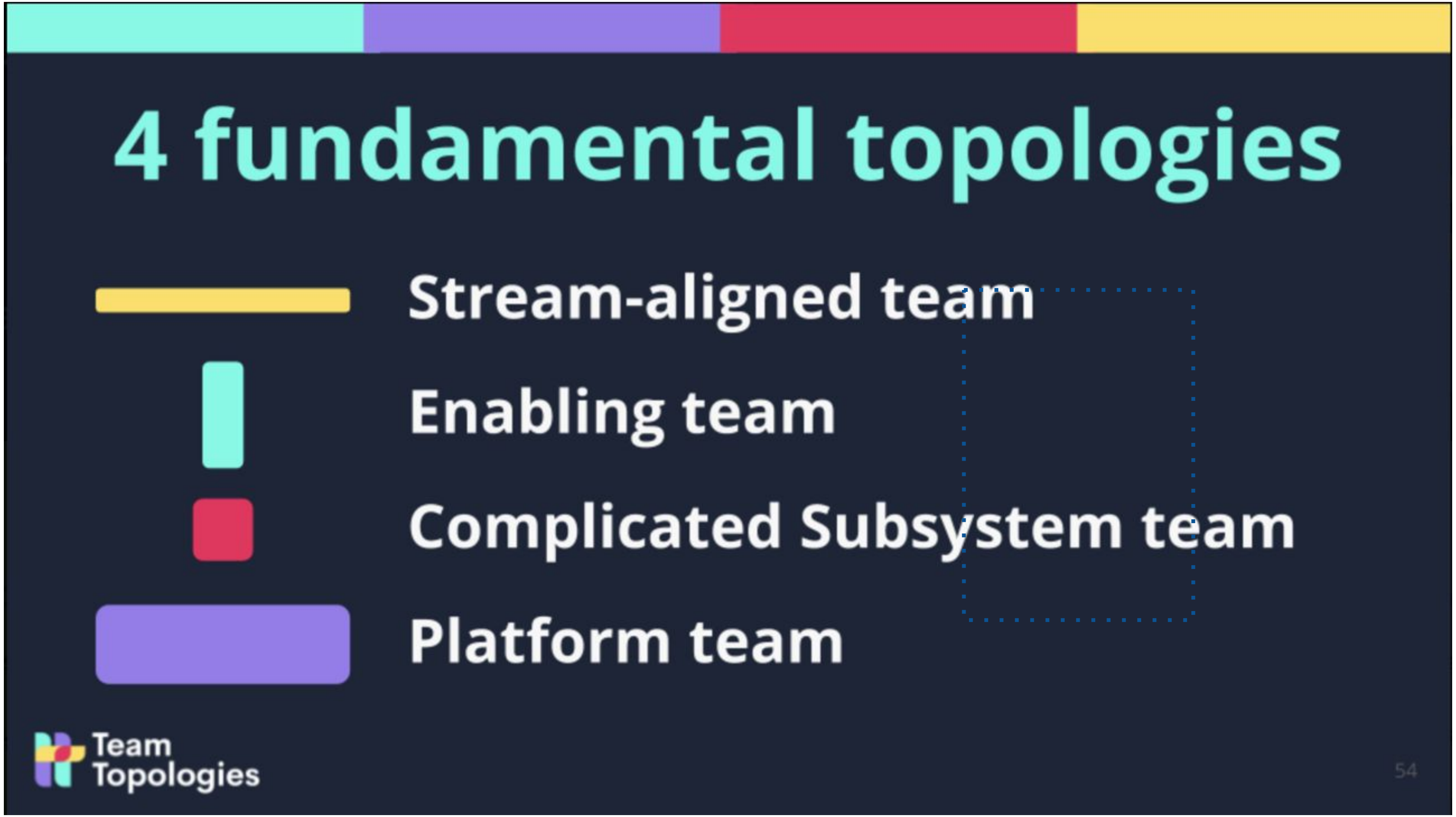
https://open-security-summit.org/

Template Structure

- Team Topologies Concepts
- Security Functions
- Security Functions in Detail
- Team Patterns (not all are developed)
  - CISO function only
  - Infosec with Security Engineering
  - Infosec with Security Engineering + QA
  - Infosec with Security Engineering + SRE
  - Infosec + QA
  - Infosec + SRE
  - Risk and Compliance as Complicated-subsystem (highly regulated industries)

Team Topologies Basics

Fundamental Topologies



4 fundamental topologies

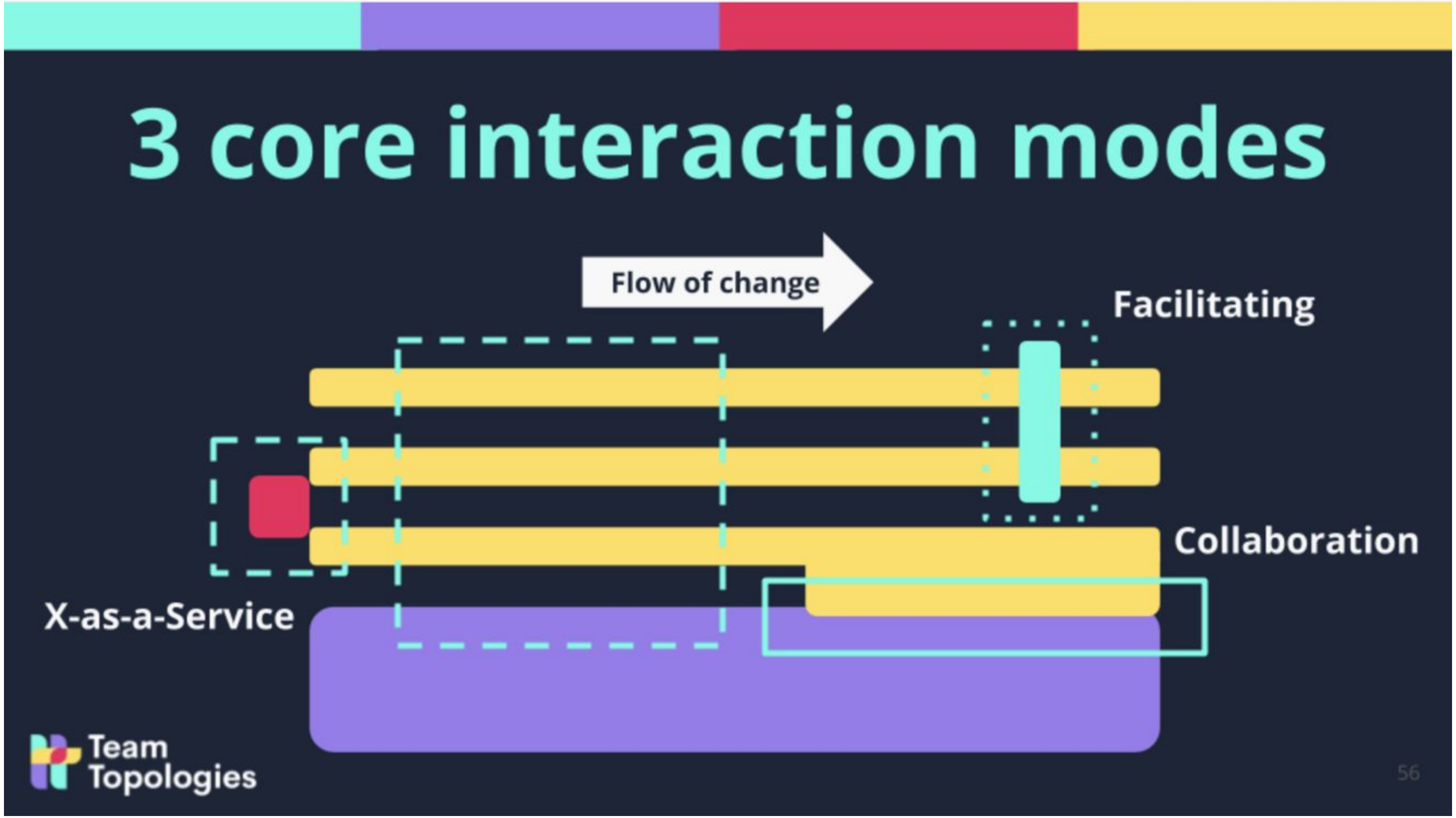
- Stream-aligned team
- Enabling team
- Complicated Subsystem team
- Platform team

Team Topologies

54

https://teamtopologies.com/key-concepts

Fundamental Topologies



https://teamtopologies.com/key-concepts

CISO Functions

Security Functions

- Coordination
- Information Risk
- Operational Security
- Security Architecture
- AppSec / Security Engineering
- Security Testing
- Audit & Assurance
- Security Culture

Security Functions in Detail

Coordination

- Metrics tracking
- Plan of action and milestones
- Security Project Management

Information Risk

- Risk assessment and analysis
- Risk Reporting
- Cyber Insurance
- 3rd Party Vendor Risk Management

Security Functions in Detail

Operational Security

- Logging & Monitoring
- Vulnerability assessment
- Incident Response
- Forensic analysis
- Threat intelligence
- Security Analytics
- Insider Threat

Security Architecture

- Security Architecture
- Business Continuity and Disaster Recovery
- Program Management

Security Functions in Detail

Application Security

- Systems security plan
- Security control assessment
- Identity and Access Management
- Security baseline Configuration
- CI / CD integrated tests
- Targeted awareness

Security Testing

- Internal and External Penetration testing
- CI / CD integrated tests ?

Security Functions in Detail

Audit & Assurance

- Security Policy
- Security Control assessment
- Control Framework Compliance
- Audit liaison

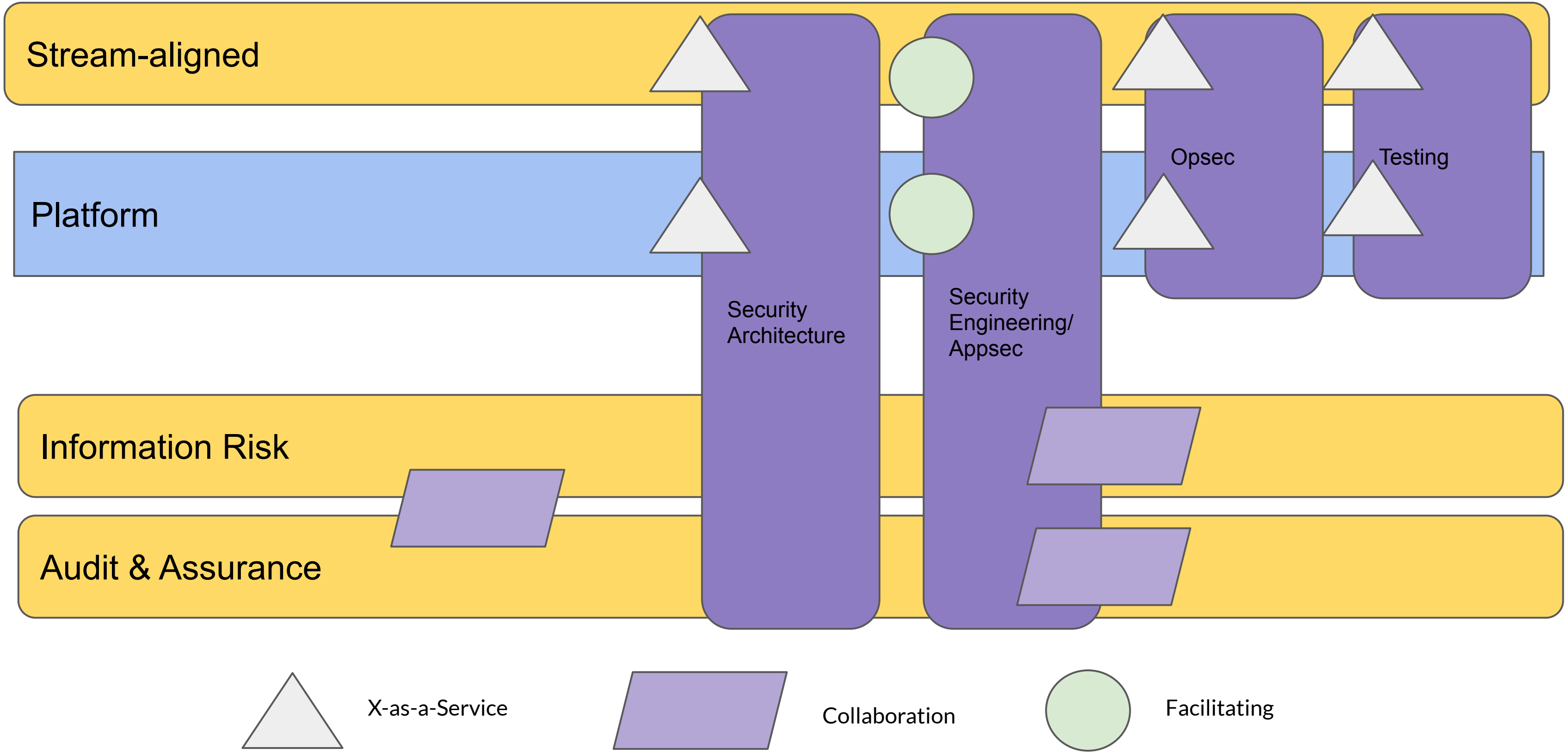
Security Culture

- End user security awareness
- Intranet Site and Policy Publication
- Phishing programs
- Exec/Board Education
- Advanced Reporting

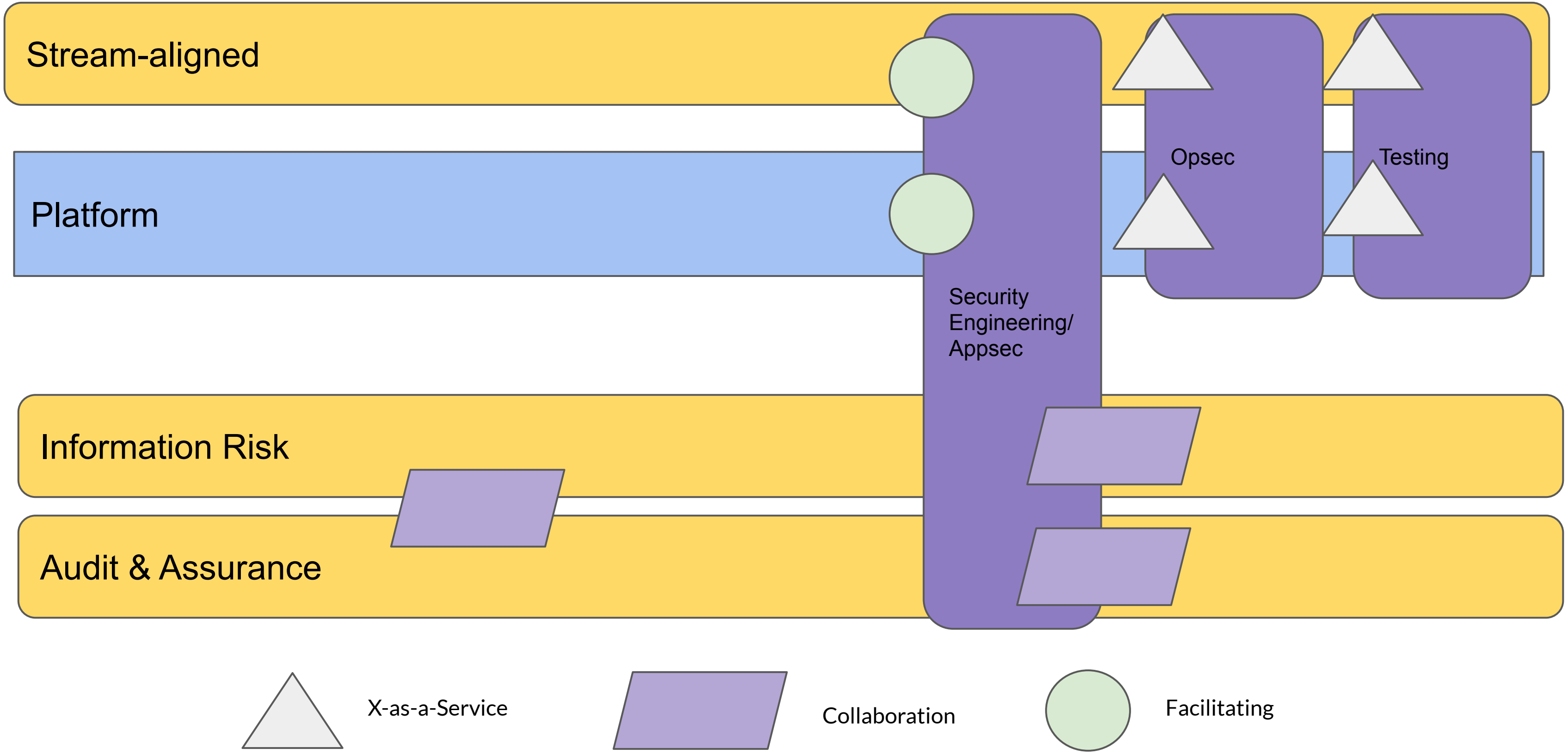
Team Patterns

CISO Functions with Security Engineering

Sample Topology - CISO Functions with Sec Eng



Sample Topology - CISO Functions with Sec Eng



Assessment

Pros

- Security Engineering provides Facilitation and boundary spanning between technical domains and other Governance teams
- Opsec and Testing provide services reducing cognitive load on Stream-aligned/Platform teams
- Audit and Risk teams don't typically engage with Value-stream/Platform teams as they operate in different timespans (Sprints with specifications vs multi-year cycles with uncertainty) which leads to misinterpretations

Cons

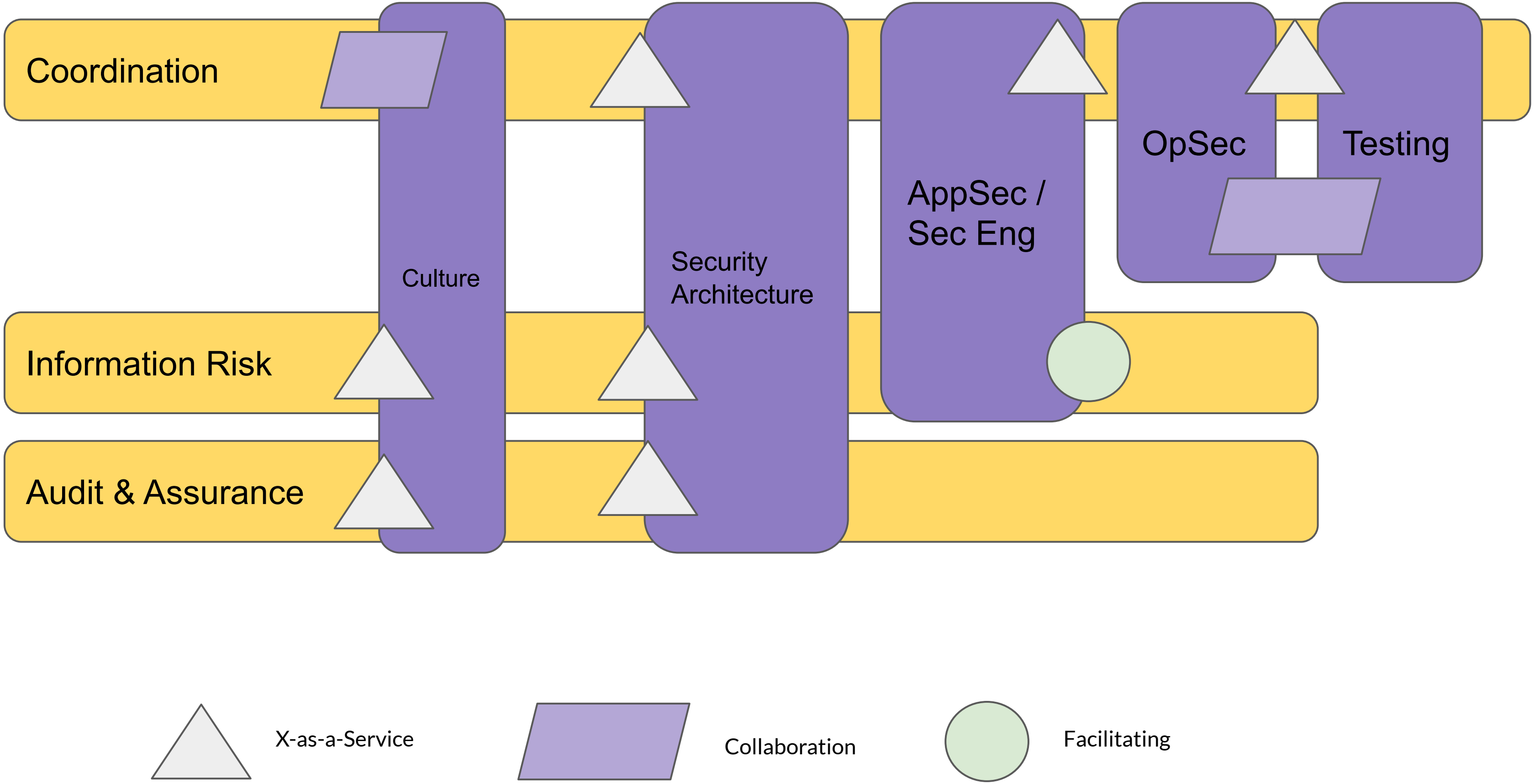
- AppSec/Security Engineering need to have clear understanding of Risk Management and Audit requirements
- OpSec may work on assumptions about the Value-stream/Platform domains which aren't often validated
- Audit and Risk may become further disconnected from the Operational realities and impact their approaches have on the organisation
- Requires clear alignment between Risk analysis and Threat modelling

Heuristics

- Appsec/Security Eng need to have people who are skilled at Technical Risk Management and Process assurance
- Culture and Awareness team need to party to forums between Risk, Audit and Security Engineering as a hedge to consider impact on culture from initiatives and provide stronger practical/pragmatic voice to transformation efforts
- Security Engineering should front requirements for Opsec and Testing (potentially checklist oriented)

CISO Functions only

Sample Topology - CISO Functions



Assessment

Pros

- Security Engineering provide facilitation to Risk and Audit, ensuring they're up to date with resilient design patterns and development practices
- Security Architecture is considered holistically through all other functions
- OpSec and Testing collaborate closely to identify weaknesses and create detections for them

Cons

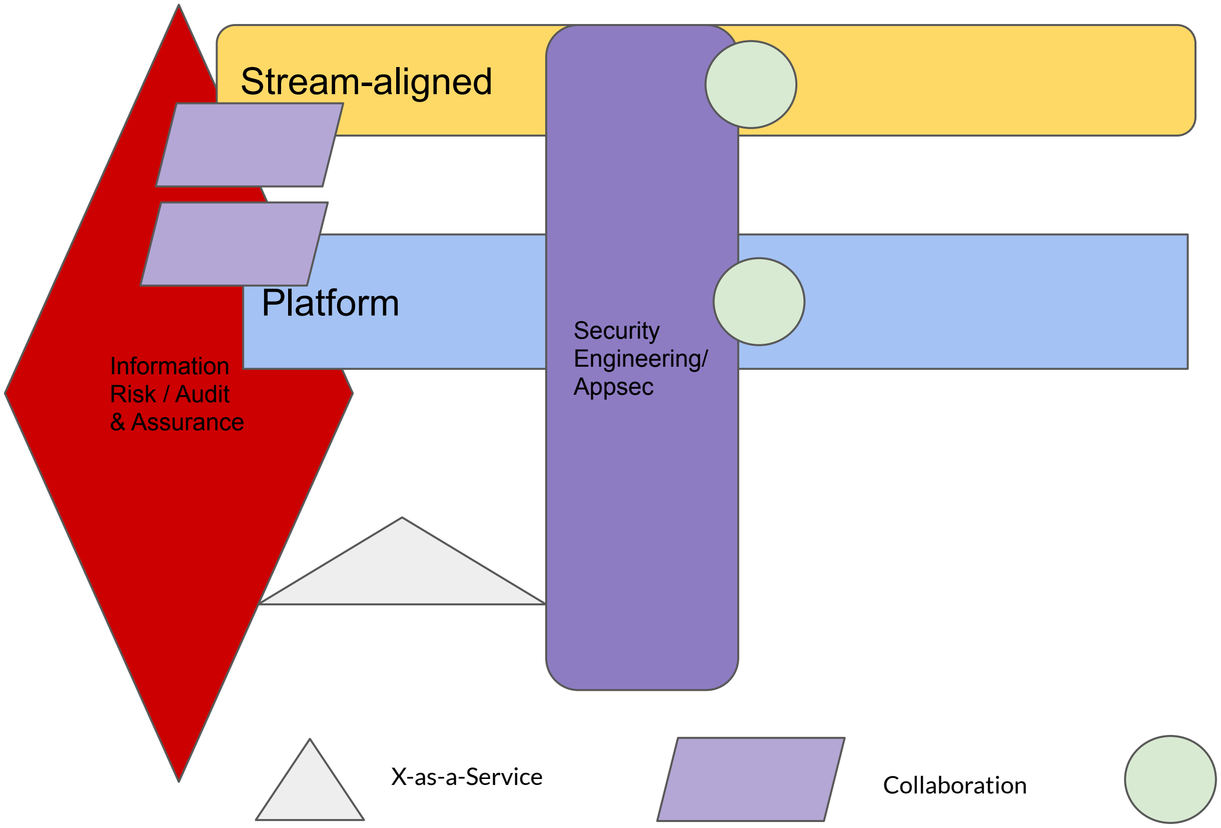
- Risk and Audit may become the sole dictators of security, if authority isn't truly shared
- Coordination, if not lightweight, will tend to overhaul security initiatives reducing autonomy and agency which in long term will impact effectiveness of team

Heuristics

- Teams transitioning from styles of Command and Control may find this model as good transition to more Agile ways of working and when not yet ready for teams owning their backlogs
- Culture team needs to work dynamically with other security and business teams to help frame their needs

Risk and Compliance as Complicated subsystem (Highly-regulated industries)

Sample Topology - CISO Functions



Assessment

Pros

- A multi-skilled team team is brought together with skills on Audit, Risk and also QA/Sofware development creating artefacts that other teams can use to ensure continuous compliance
- Reduced cognitive load by all other teams that have a stake
- Simpler team structure with holistic skills and clearer interaction modes

Cons

- Team dynamics management will be key, as stakeholders with different world views are brought together and may not have the requisite skills to truly collaborate
-

Heuristics

- Multiple standards and regulatory requirements (Security, QMS, Industry-specific) that have direct impact on software development
- Existing challenges and tensions between typical gatekeeping profiles and engineering
- Current limited assurances provided by process and automation of validations

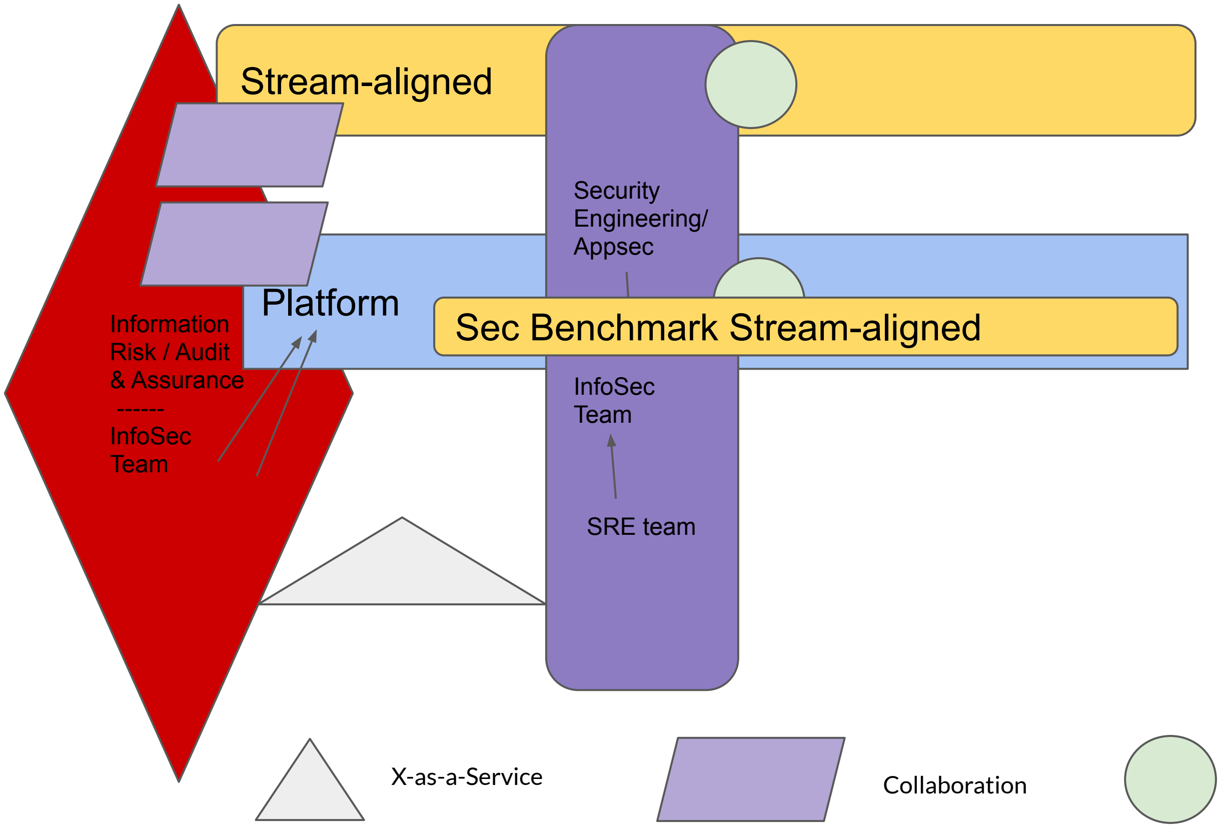
Q&A

Mario Platt

mario@practical-devsecops.com

Twitter: @madplatt
LinkedIn: marioplatt
Medium: @marioplatt

Sample Topology - CISO Functions


Stream-aligned
Security
Engineering/
Appsec
Platform
Sec Benchmark Stream-aligned
Information
Risk / Audit
& Assurance

InfoSec
Team
InfoSec
Team
SRE team
X-as-a-Service
Collaboration
Facilitating