RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **PS-F02**

Integrating Our DevSecOps Product Pipeline with Software Security Standards

Altaz Valani

Director, Research and Insights
Security Compass

#RSAC

"A seed sown in good ground brings forth fruit. A principle, instilled into good mind, brings forth fruit."

Blaise Pascal

Outline

- Intentional security architecture
- Balanced Development Automation (BDA)
- Building accountability through OKRs and Team Leads
- Accelerating knowledge and insights generation

What We All Want

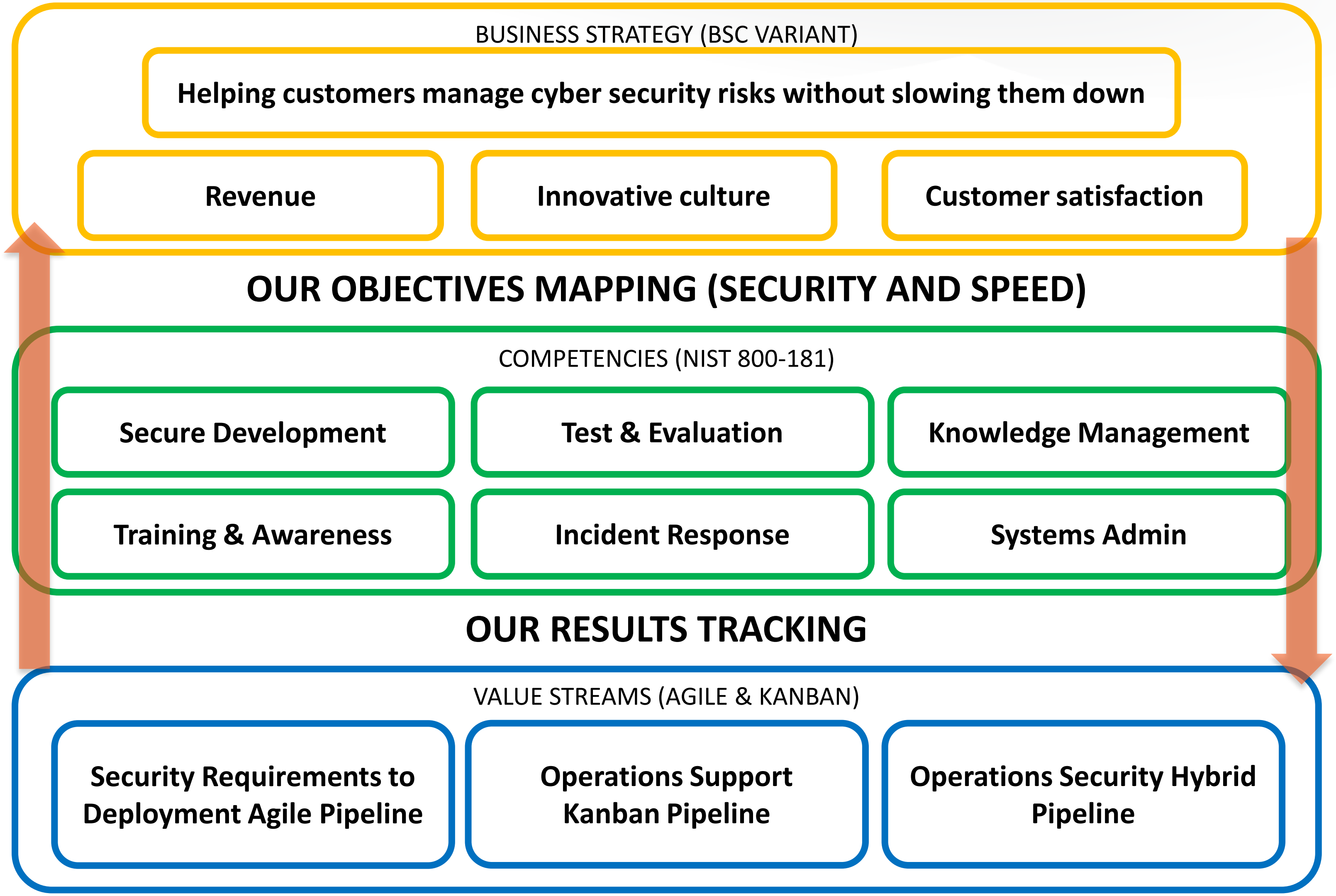
- Innovate fast, stay ahead of the competition, and still be responsible with cyber security.
- Generate policies that leverage industry expertise around security and compliance from best practices all over the world.
- Built in security guidance for developers.
- Provide company leaders with a view into risks.
- Manage the dynamic nature of continually changing security standards and DevOps technologies.

Bottom Line: **Balanced development** that achieves both security and speed

Intentional Security Architecture

Taking an Enterprise Perspective

Being Intentional With Security Architecture



BUSINESS STRATEGY (BSC VARIANT)

Helping customers manage cyber security risks without slowing them down

Revenue

Innovative culture

Customer satisfaction

OUR OBJECTIVES MAPPING (SECURITY AND SPEED)

COMPETENCIES (NIST 800-181)

Secure Development

Test & Evaluation

Knowledge Management

Training & Awareness

Incident Response

Systems Admin

OUR RESULTS TRACKING

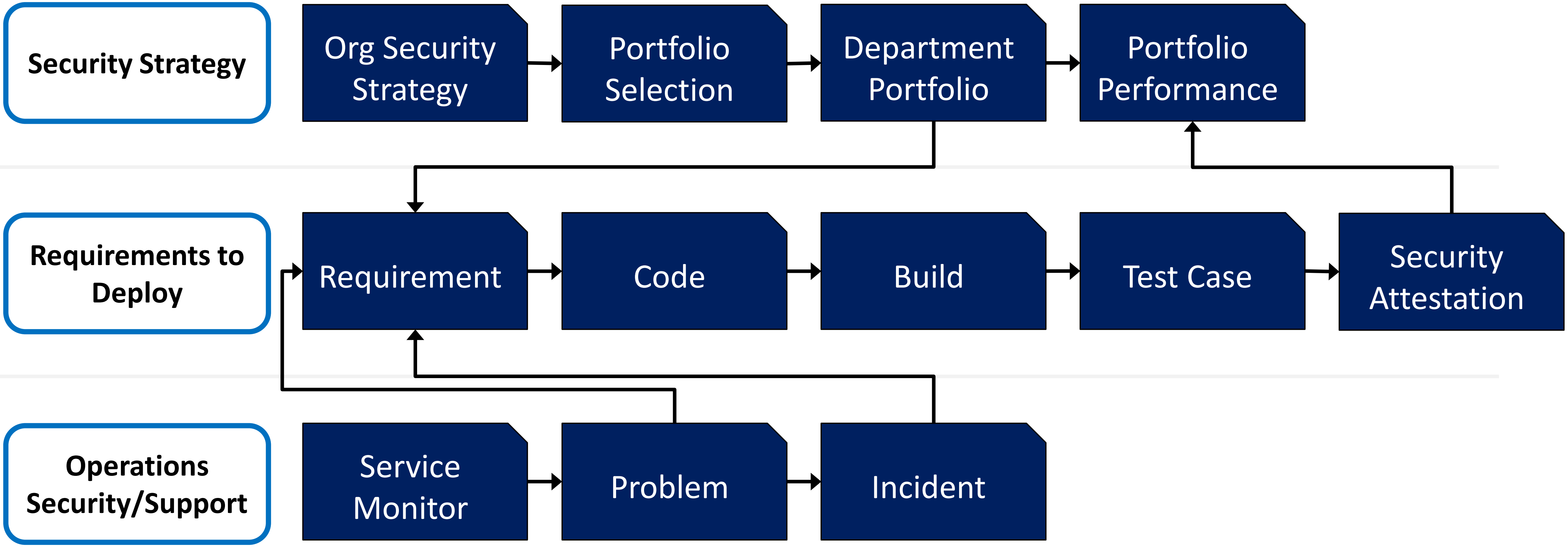
VALUE STREAMS (AGILE & KANBAN)

Security Requirements to Deployment Agile Pipeline

Operations Support Kanban Pipeline

Operations Security Hybrid Pipeline

Artifact Fabric Across Security Architecture



Security Strategy

Org Security Strategy → Portfolio Selection → Department Portfolio → Portfolio Performance

Requirements to Deploy

Requirement → Code → Build → Test Case → Security Attestation

Operations Security/Support

Service Monitor → Problem → Incident

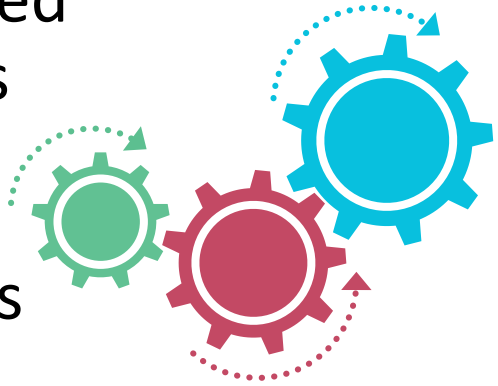
Example Security Policies

1. All our software products **must be** modeled and balanced for cyber security and speed.

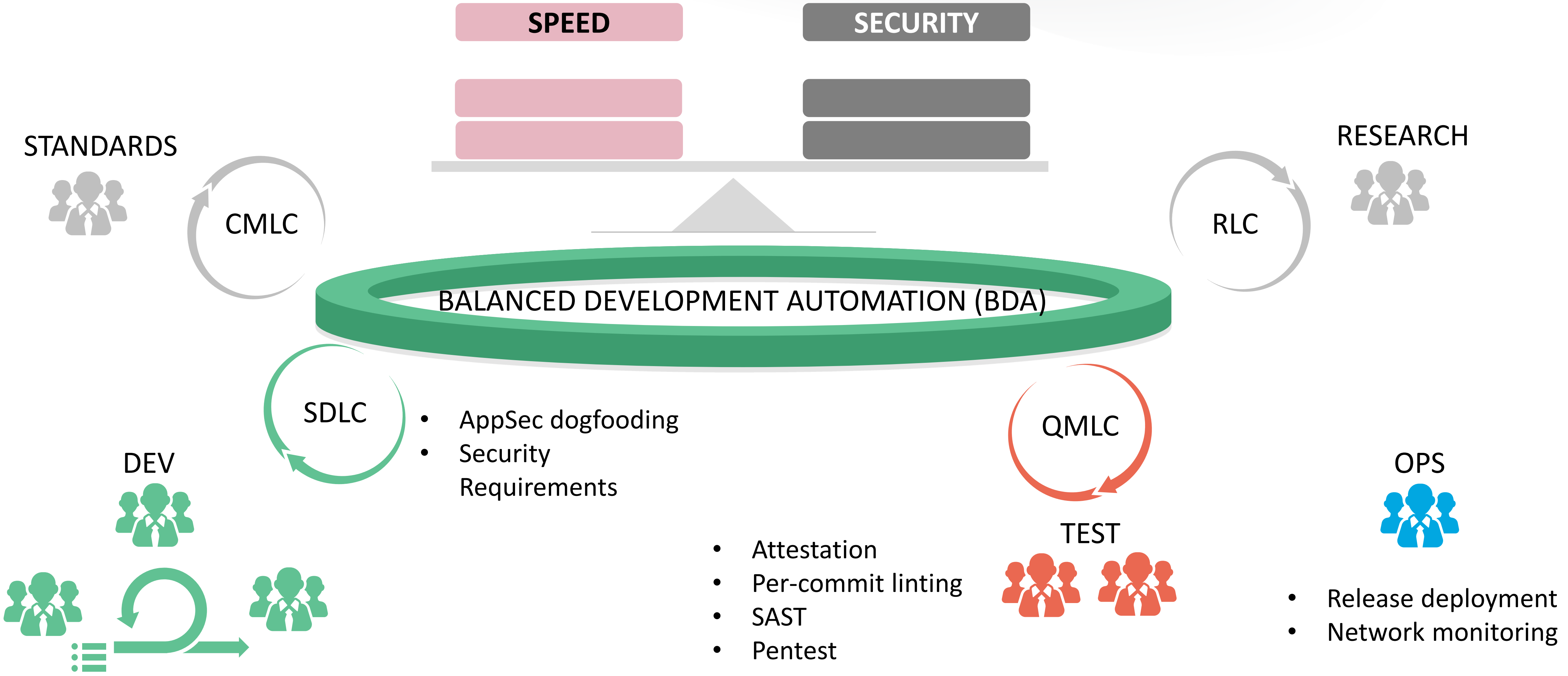
2. All our high priority software security requirements **must be** fixed before shipping.

3. Requirements not applicable **must have** explicit defensibility explaining why they are not applicable and must be approved by the Director of Engineering. Same goes for requirements where the risk is accepted.

4. All parties in the development lifecycle and supporting roles **must be** trained on our security policies and procedures.



Balanced Development to Achieve Both Speed and Risk



SPEED

SECURITY

STANDARDS

CMLC

RESEARCH

RLC

BALANCED DEVELOPMENT AUTOMATION (BDA)

SDLC

- AppSec dogfooding
- Security Requirements

DEV

QMLC

TEST

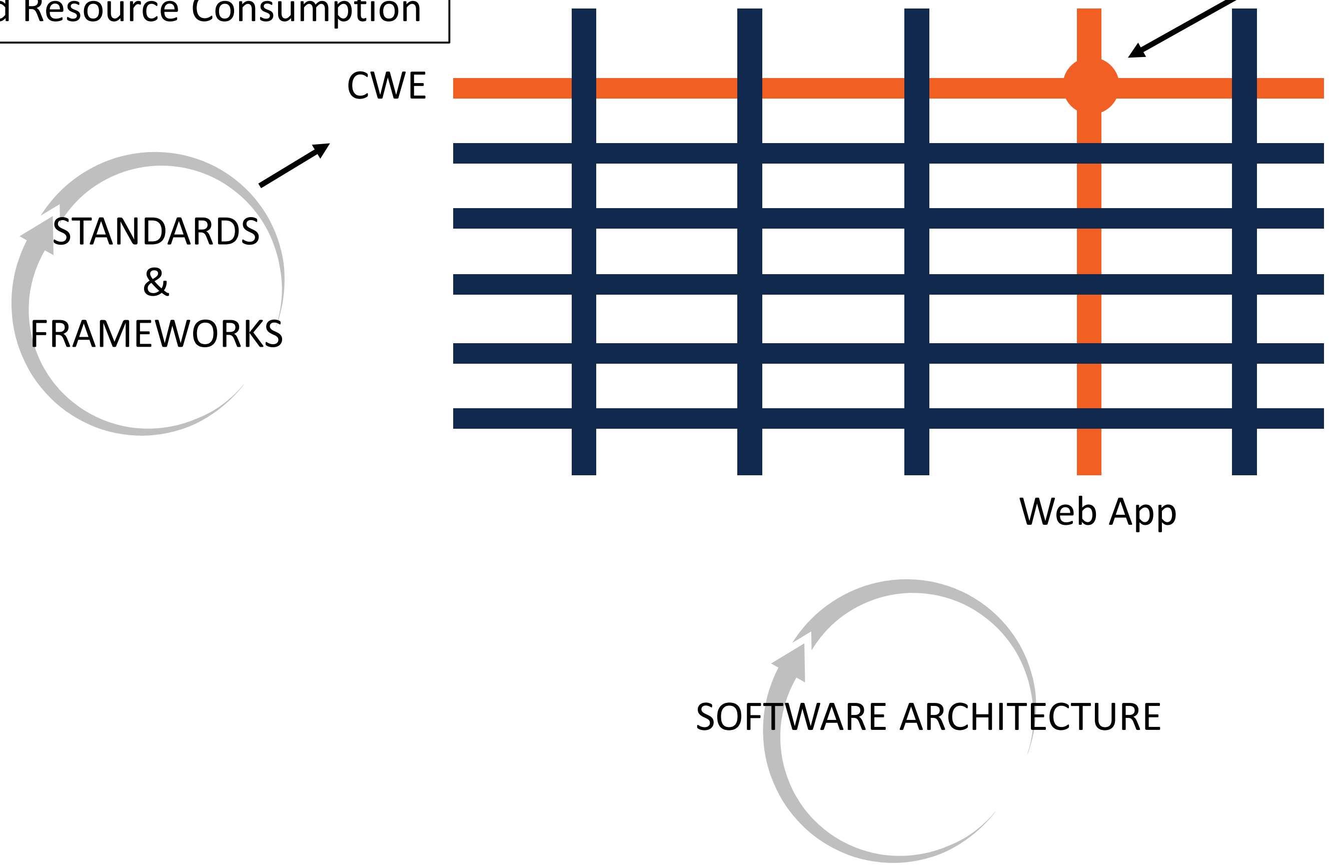
- Attestation
- Per-commit linting
- SAST
- Pentest

OPS

- Release deployment
- Network monitoring

Making Security Policies Actionable in BDA

CWE-400 Uncontrolled Resource Consumption



Limit the following request attributes:

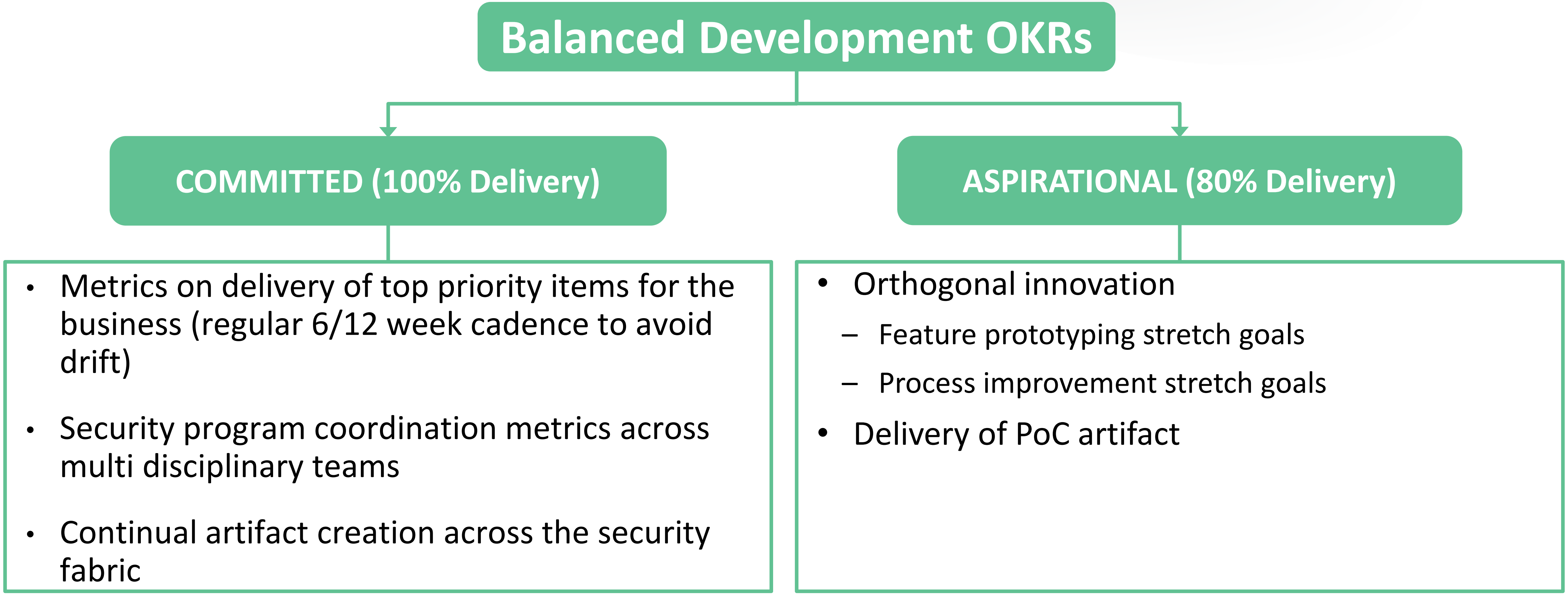
- Request body size
- Number of request header fields
- Request header fields size
- Request line size
- XML request body size

RSA Conference2020

Building in Accountability

Making security objectives stick with OKRs

Making it Stick: Our OKR Journey



Balanced Development OKRs

COMMITTED (100% Delivery)

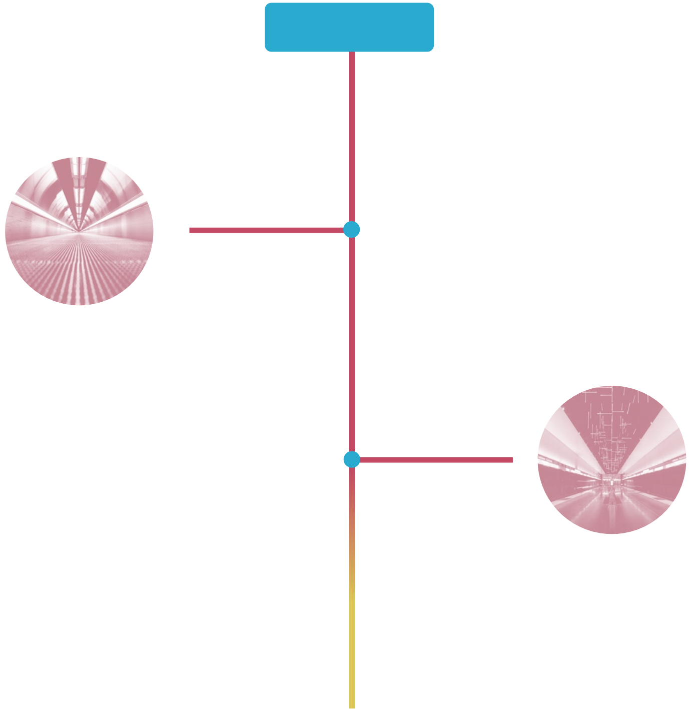
- Metrics on delivery of top priority items for the business (regular 6/12 week cadence to avoid drift)
- Security program coordination metrics across multi disciplinary teams
- Continual artifact creation across the security fabric

ASPIRATIONAL (80% Delivery)

- Orthogonal innovation
  - Feature prototyping stretch goals
  - Process improvement stretch goals
- Delivery of PoC artifact

Bottom line: Poor OKRs are a waste of time for everyone. We need to answer the question, ‘Who cares?’

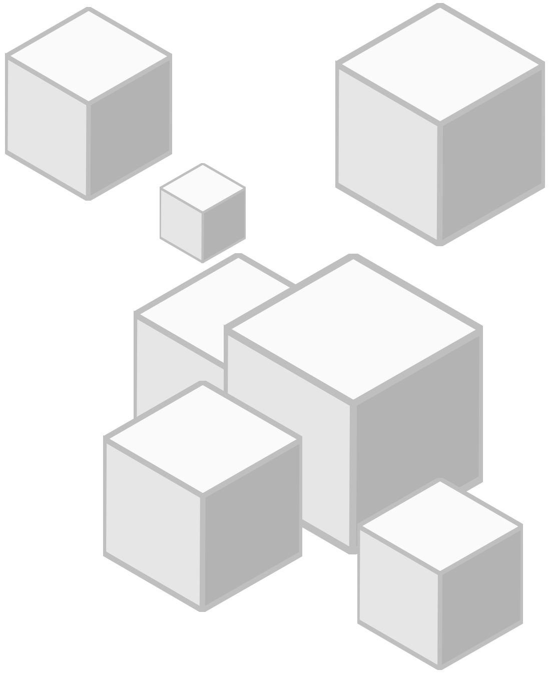
OKRs: What We Learned So Far



- Differentiate between security commitments and aspirational OKRs
- Empathize with the target: internal or external customer focus and how they interact with security
- Set clear milestones for both speed and security
- Security stretch goals should focus on innovation
- Close the security objective only when underlying key results are met

Team Leads Drive Balanced Development Practices

- We handle security tasks at the Dev level through Team Leads as Security Champions
- Product owners focus on features and do not inject security into the pipeline
- Dev team uses balanced automation to identify all security tasks and requirements relating to development work within the current release cycle
- Work in 2 week sprints, with each release being completed in 3 sprints



RSAConference2020

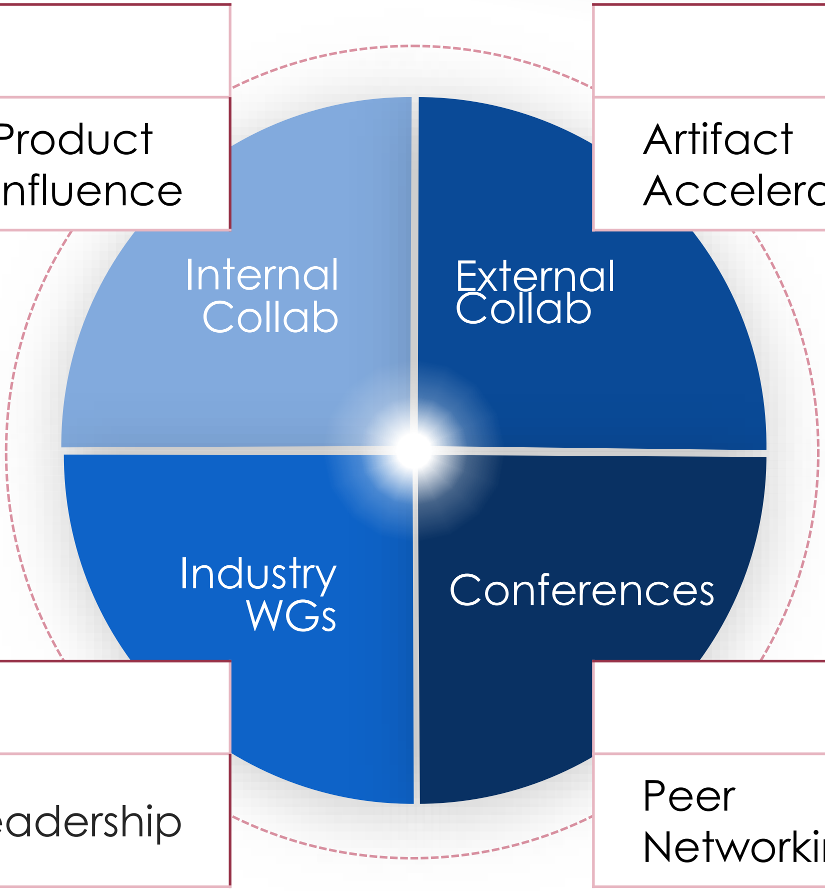
Achieving Rapid Security Knowledge and Insights

Building a collaboration pipeline

Collaboration as a Security Insight Accelerator

OBJECTIVES		
xFunctional Empathy	Idea Diversification	Product Influence

OBJECTIVES		
Artifact Accelerator	Peer Networking	Branding



OBJECTIVES		
Standards Influence	POV Validation	Leadership

OBJECTIVES		
Peer Networking	Thought Leadership	Knowledge & Insights

In conclusion…

Apply What You Have Learned Today

- Short term:
  - Get involved in an industry working group focused on software security
    - OWASP, IEEE, SAFECode, The Open Group
- Mid term:
  - Initiate cross functional security collaboration for balanced development
  - Establish high level committed OKRs that target both speed and security
- Long term:
  - Include aspirational OKRs for innovation
  - Go beyond working groups to expand collaboration with industry peers and academia

RSAConference2020

Thank you

Q&A