OWASP Indonesia Day 2017

Suman Sourav

Director –DevSecOps, Vantage Point Security

VANTAGEPOINT

About me

- Certified Secure Software Lifecycle Professional (CSSLP)
- 12+ Years of Experience in Software Security
- Co-Founder of DevSecOps Singapore & DevSecCon Asia
- Speakers
  - IoT Asia
  - OWASP Singapore
  - DevOps Singapore
  - Jenkins Singapore
  - Security Conferences in USA, China
  - Trained 4000+ developers and 1000+ QA

VANTAGEPOINT

Indonesia Information Security

Important numbers

Average financial losses in information security

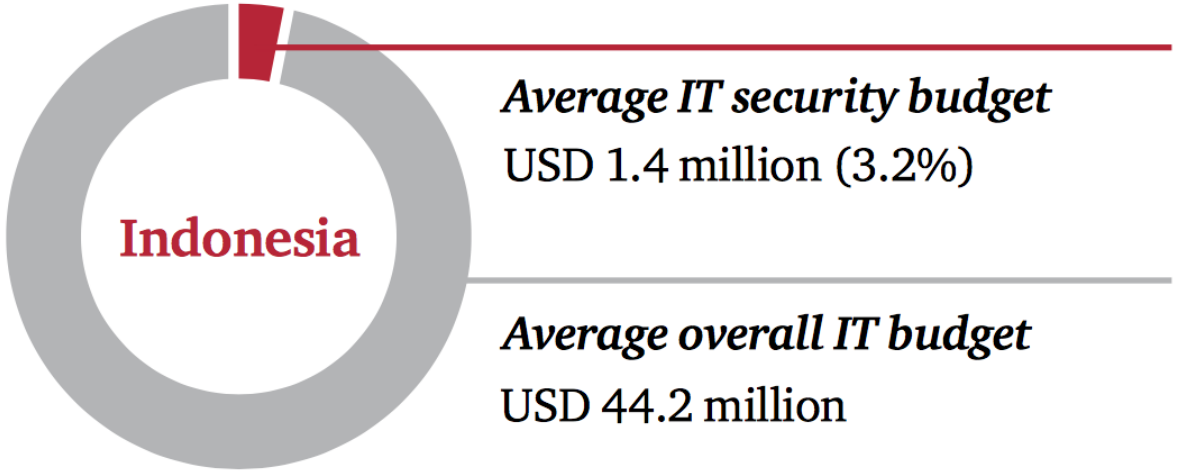
Indonesia USD 1.2 million | USD 2.4 million **Global**

Reference : https://www.pwc.com/id/en/publications/assets/assurance/Risk%20Assurance/gsiss-2017-web.pdf

VANTAGEPOINT

Important numbers

Average IT security budget compared to overall IT budget



Average IT security budget
USD 1.4 million (3.2%)

Average overall IT budget
USD 44.2 million

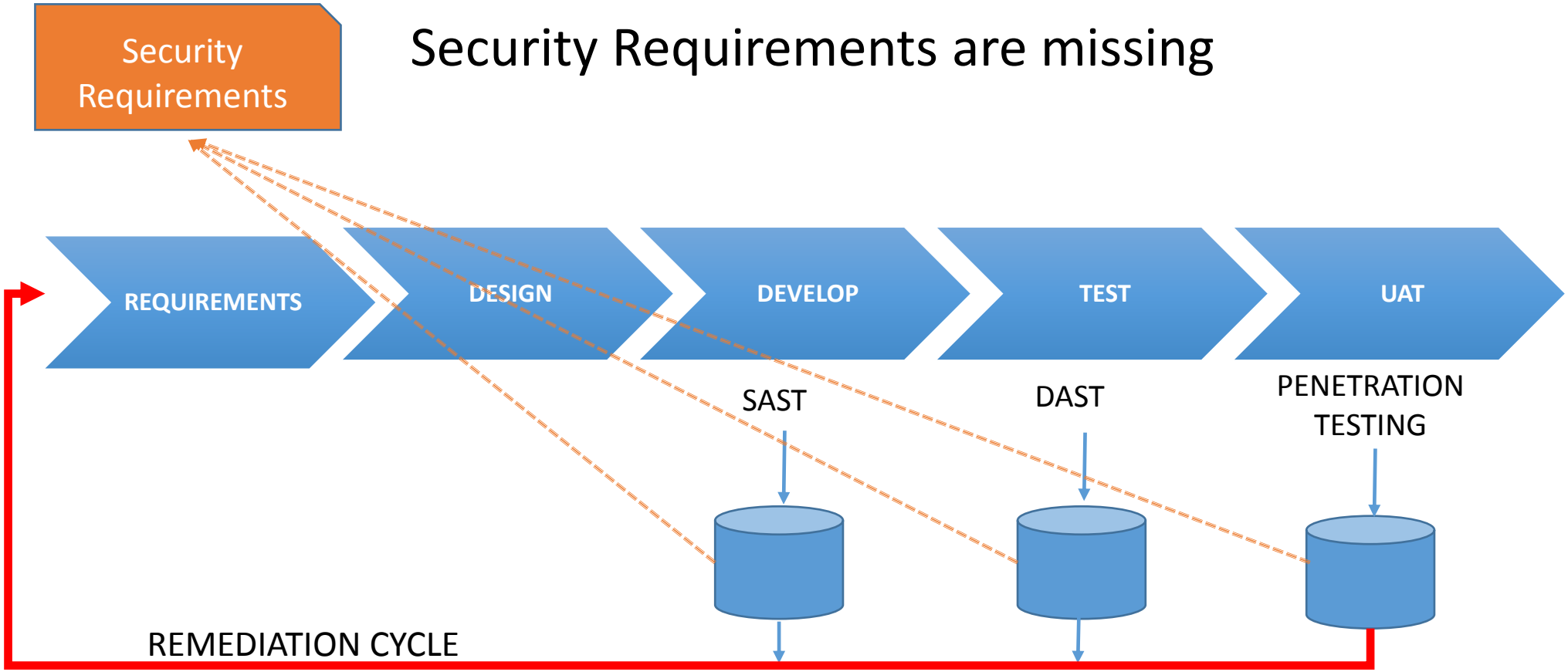
Average IT security budget
USD 5.1 million (3.7%)

Average overall IT budget
USD 138 million

Reference : https://www.pwc.com/id/en/publications/assets/assurance/Risk%20Assurance/gsiss-2017-web.pdf

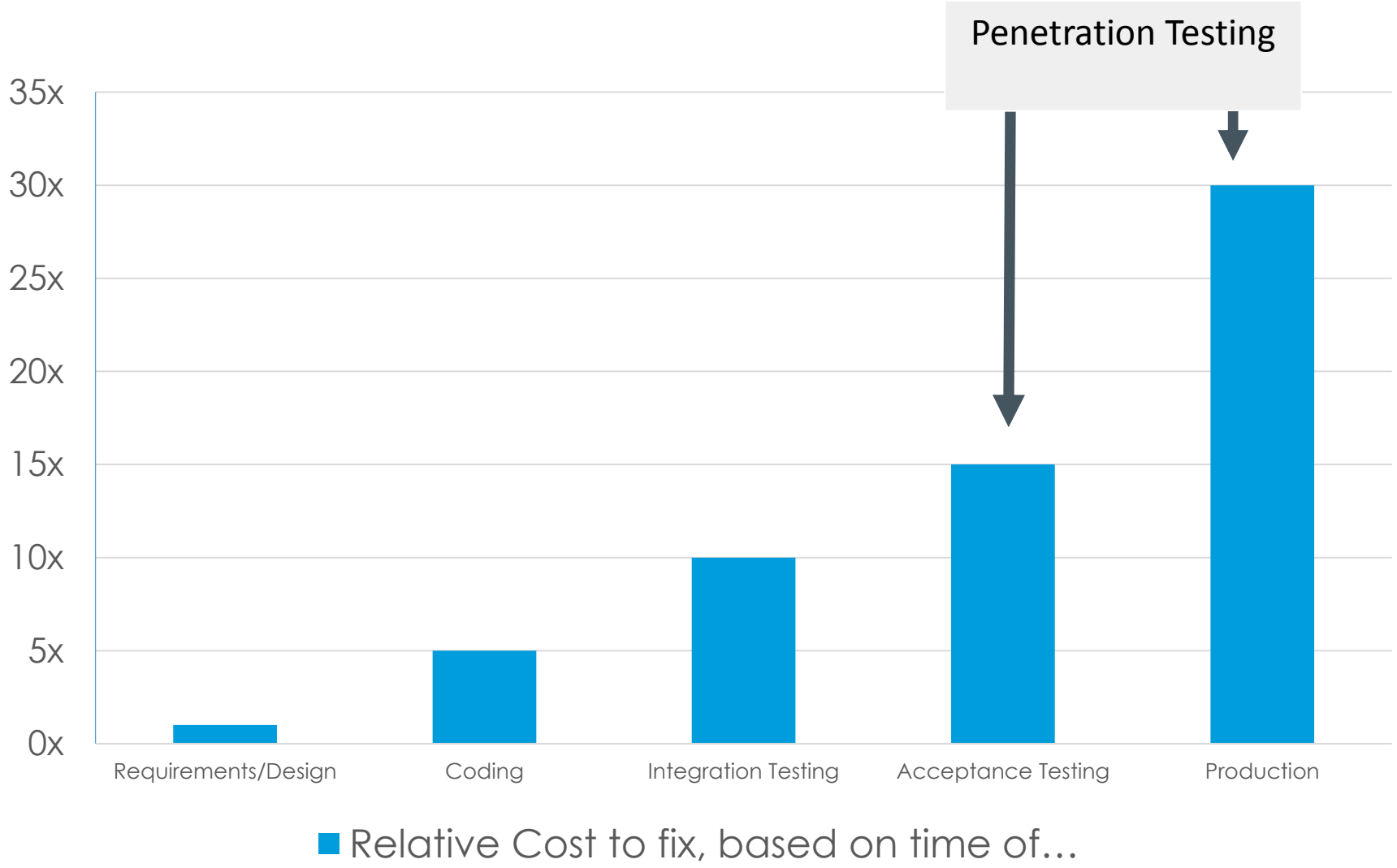
VANTAGEPOINT

Application Security Approach

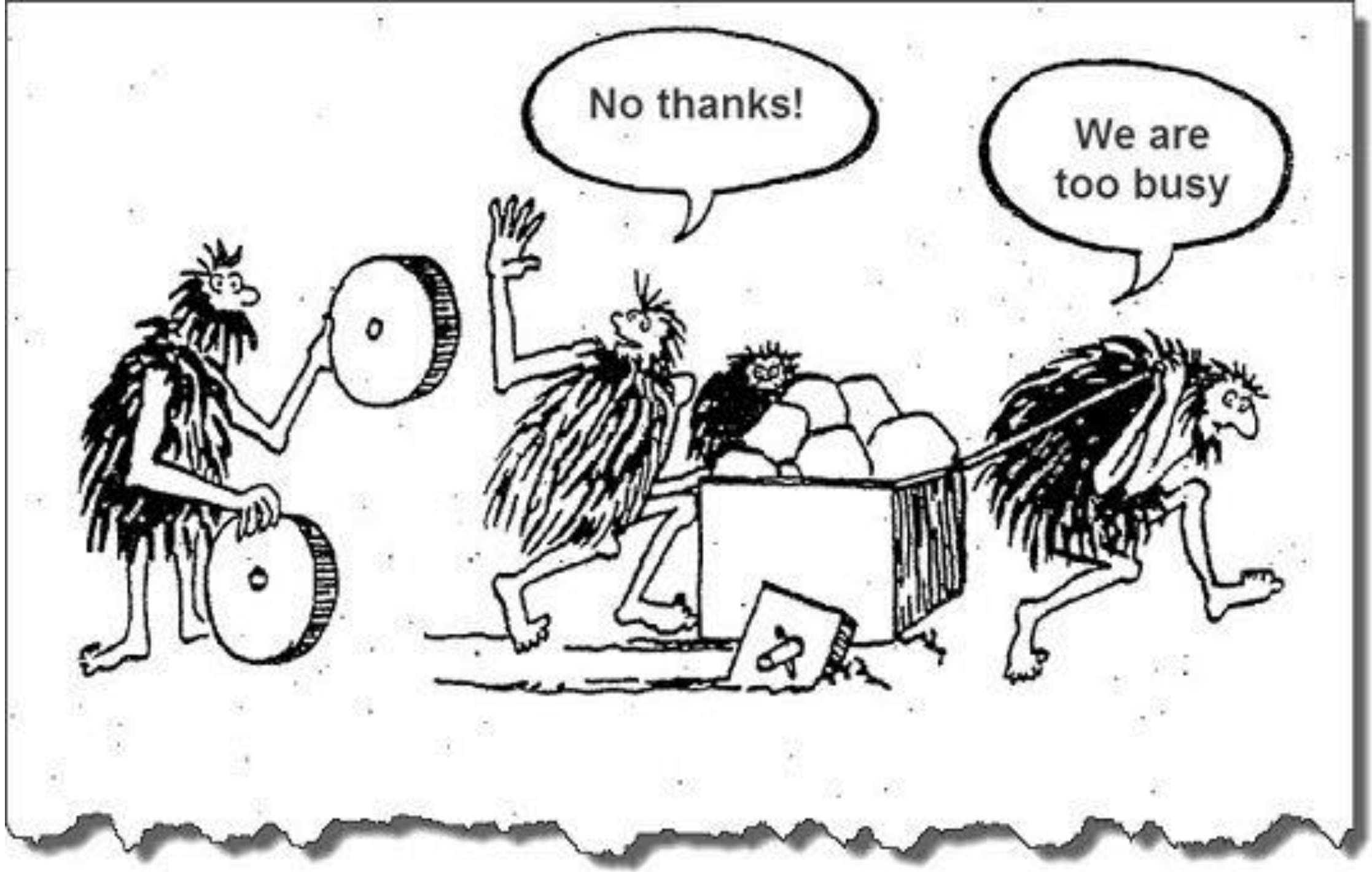


VANTAGEPOINT

Cost of Vulnerability Remediation

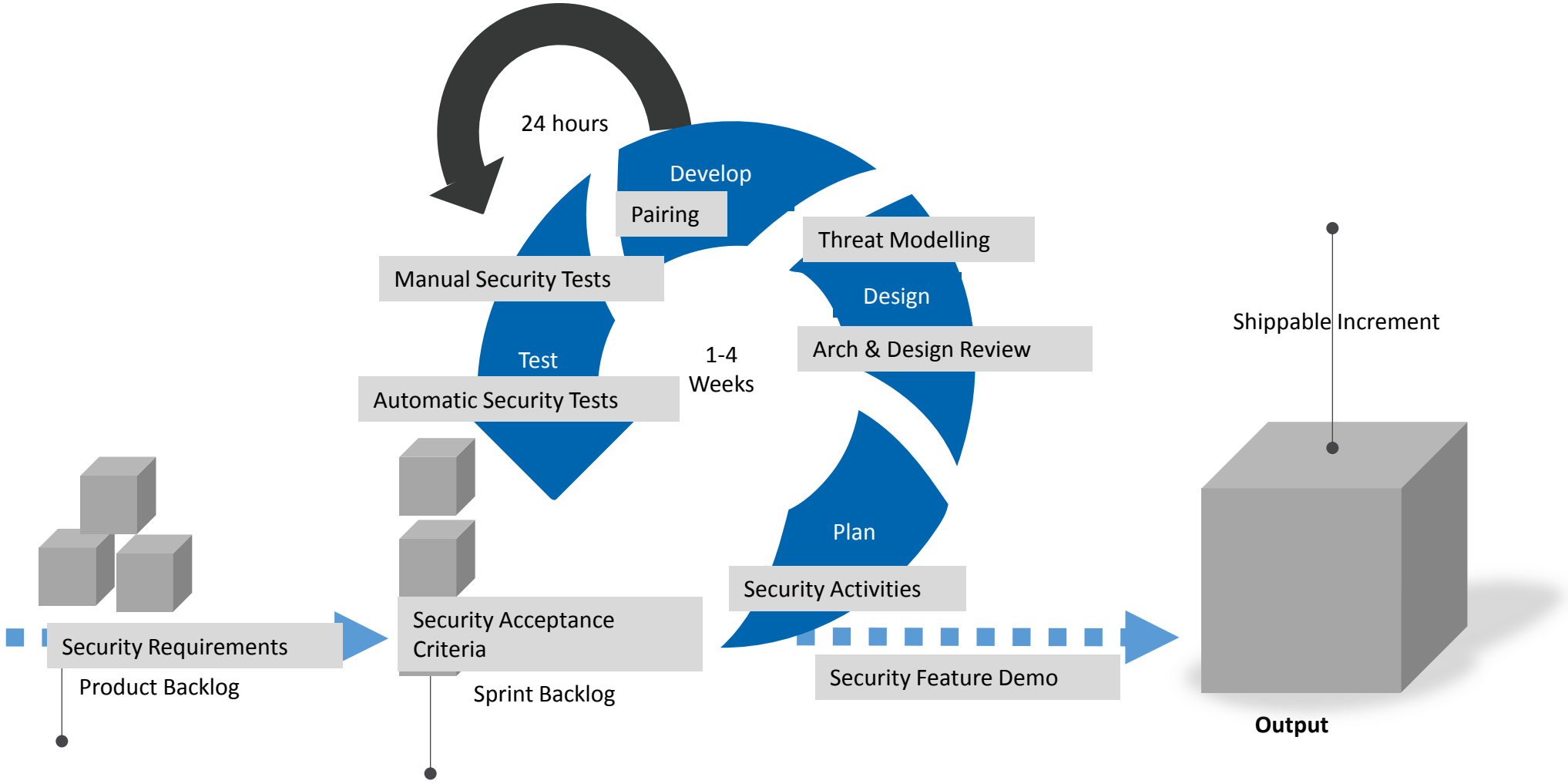


Source: **NIST**


No thanks!
We are too busy

VANTAGEPOINT

Agile Security



Source: **NIST**

VANTAGEPOINT

DevOps & SecOps

DevOps

Rise of the Developer

Lack of Security Orchestration & Automation in the SDLC

SecOps

Overburdened Security

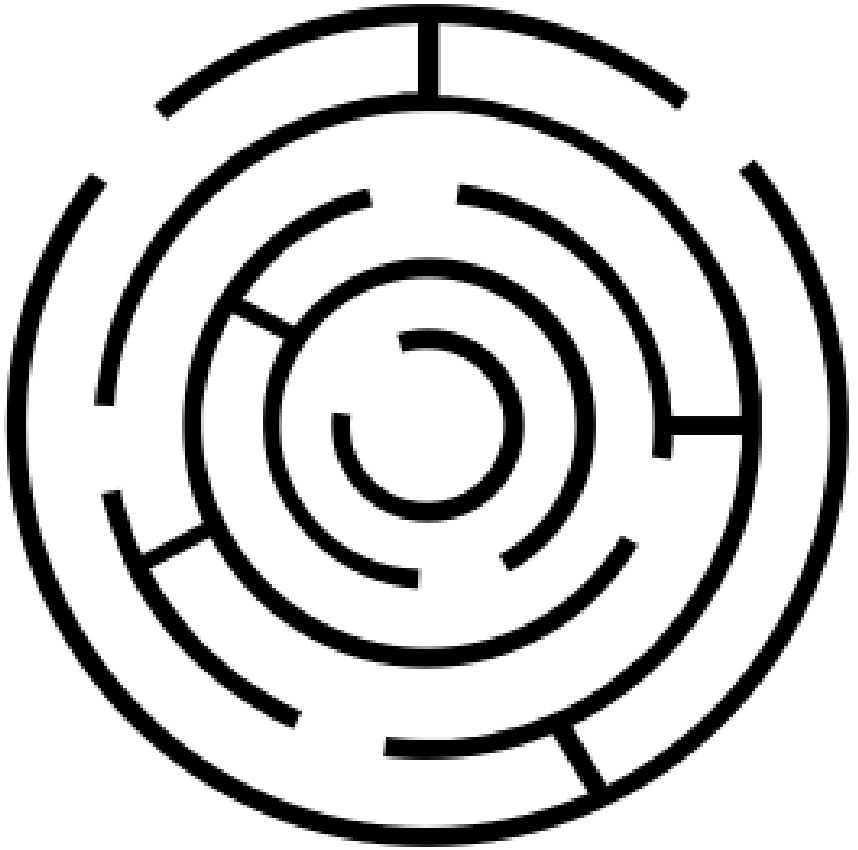
Security

Developer

VANTAGEPOINT

Major Challenges

- Shortage of Application Security Resources
- Lack of awareness in the organization
- Influences of technology vendors
- Slow adoption of security tools in development environment
- Lack of education & training
- No application security dashboard

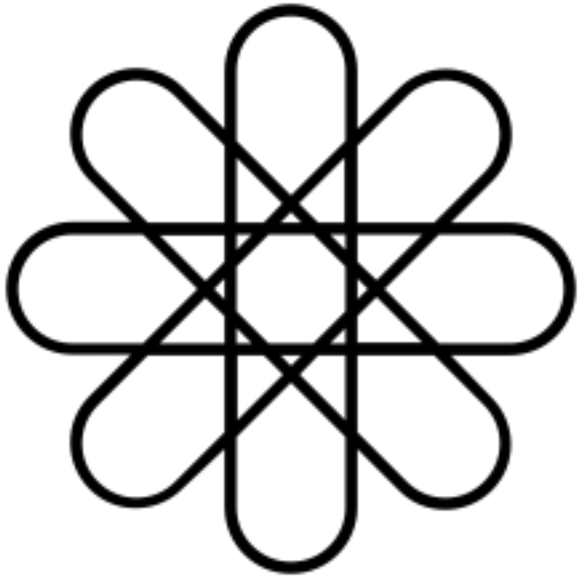


**“What if we don’t change anything at all …
and something magical just happens.”**

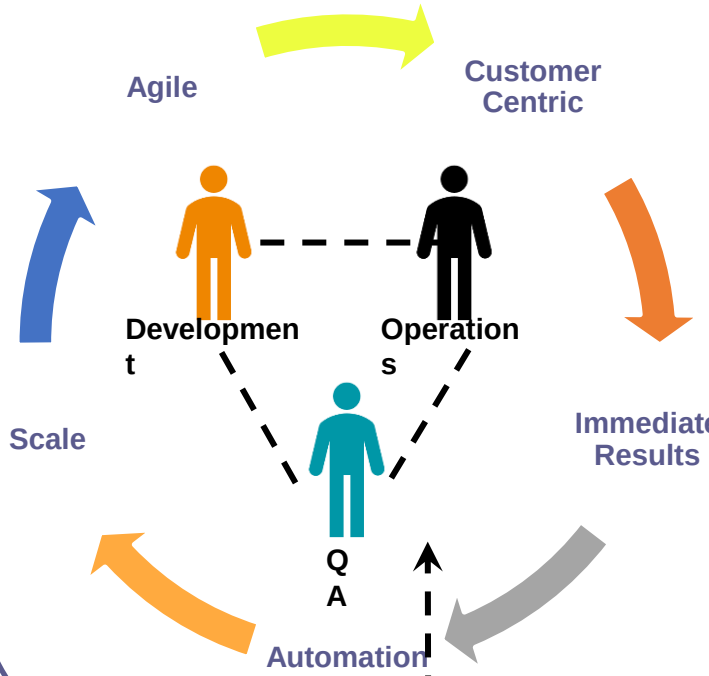
VANTAGEPOINT

Time to Change Our Approach of Application Security

- Define Security Metrics for Application Security
- Build Internal Resources from Development Team
- Define the Application Security Technology Evaluation Process
- Build the DevSecOps Technology Roadmap
- Adoption of Cloud Security Solution
- Adoption of Security As a Service



What we need is : DevSecOps



90%

of surveyed organizations are implementing or piloting DevOps

and

99%

Agree DevOps is an opportunity to improve application security

but only

20%

Are doing application security testing during development

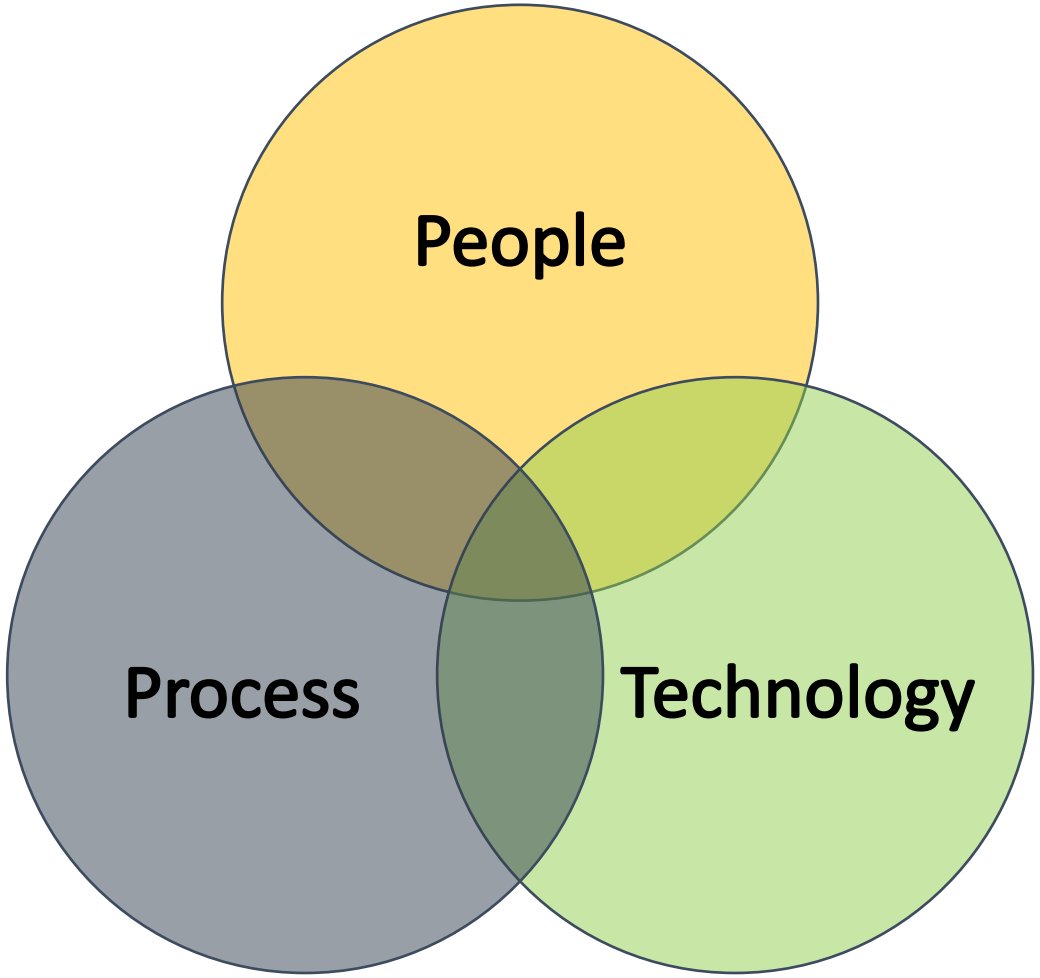
SecOps Needs to Shift Left

SecOps

VANTAGEPOINT

Key Elements

- **People**
  - ✓ Training
  - ✓ Role
- **Process**
  - ✓ Compliance
  - ✓ Certifications
- **Technology**
  - ✓ Security tools
  - ✓ Dev tools



VANTAGEPOINT

People

VANTAGEPOINT

Training Approach

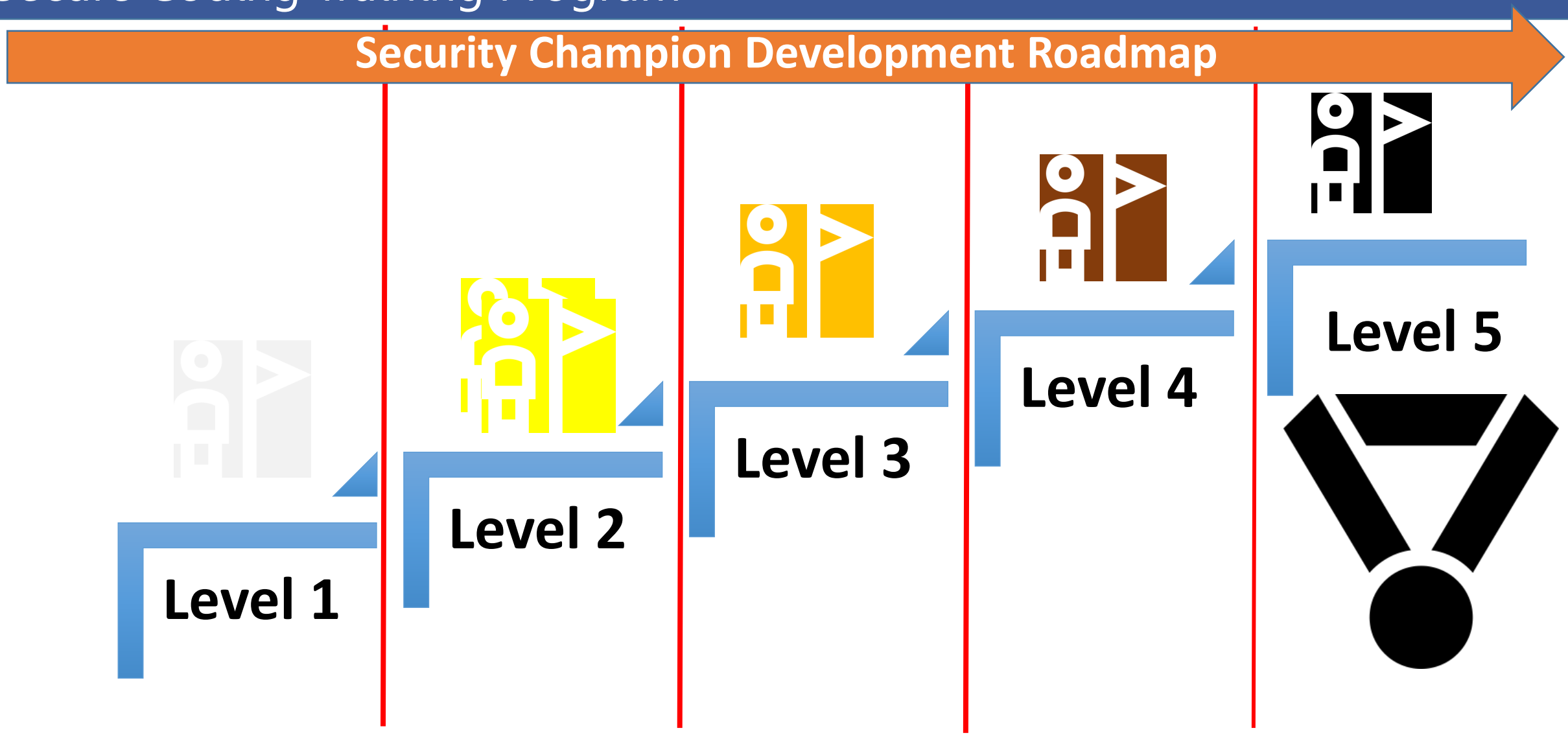
- Culture Change
- ~~Traditional Training~~
  - Shorter Training Duration
  - Integrated in IDE/ALM
- New Joinee Induction Training

- **Product Manager**
  - Secure SDLC
  - Security Requirements
- **Architects**
  - Secure Design Principles
  - Threat Modeling
- **Developer**
  - Secure Coding
  - SAST Tools

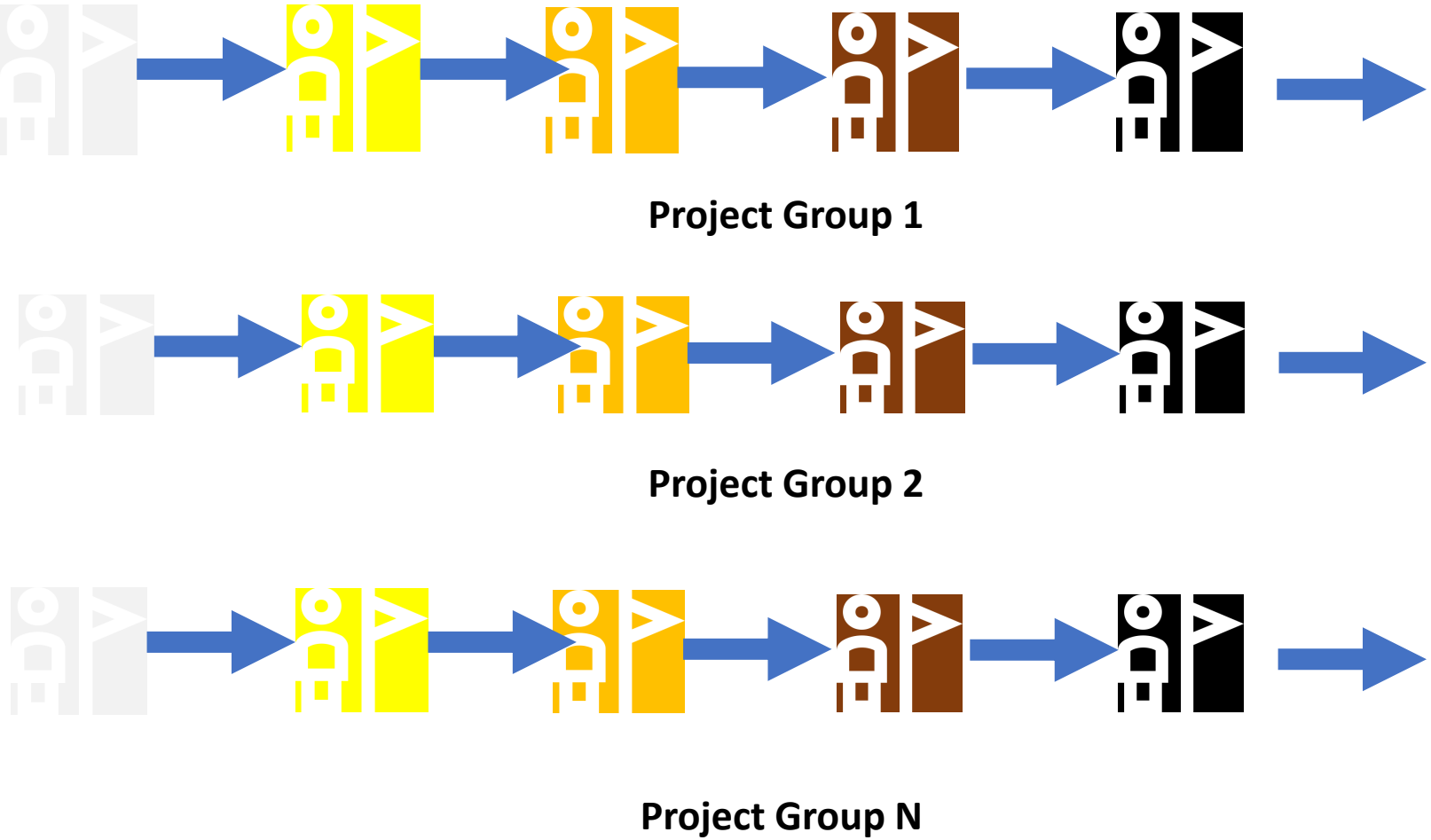
- **QA**
  - Security Testing
  - Dynamic Testing Tools
- **Operation**
  - Security Configurations
  - Secure Deployments

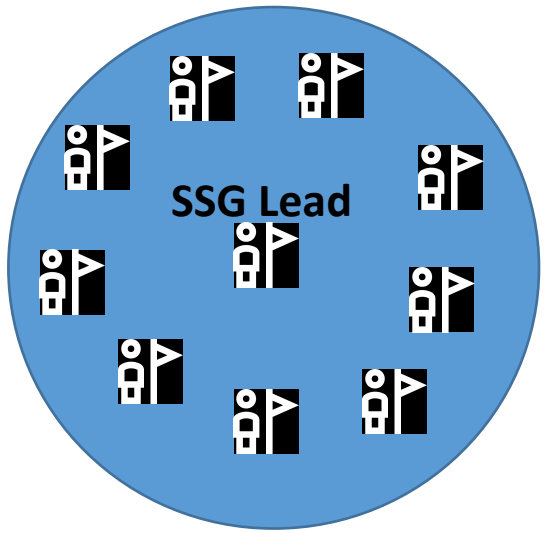
VANTAGEPOINT

Secure Coding Training Program



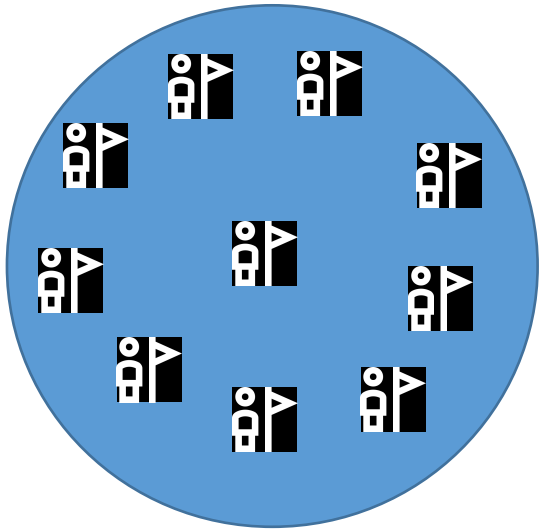
Software Security Group



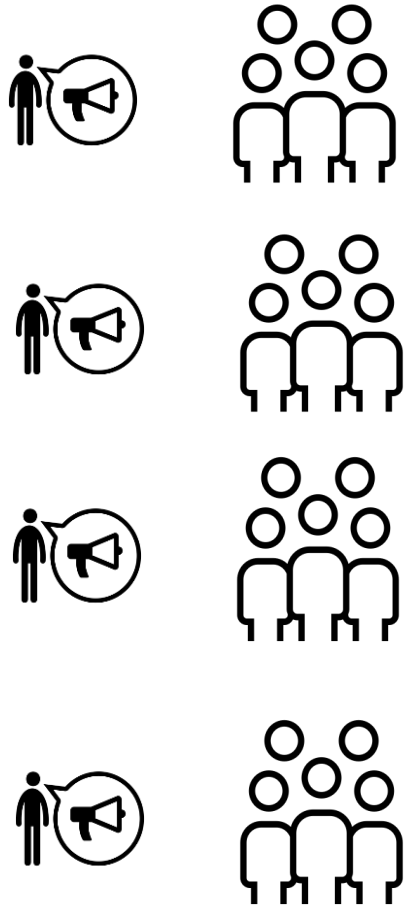


Software Security Group Roles & Responsibilities

SSG



- **Security Best Practices**
- **Security tournaments**
- **Secure Coding Training**
- **Security Policy**
- **Security Process**
- **Security Technologies**
- **Security Forum**
- **Security Events (Internal Conference)**
- **Security Hackathon**
- **Security Summits**

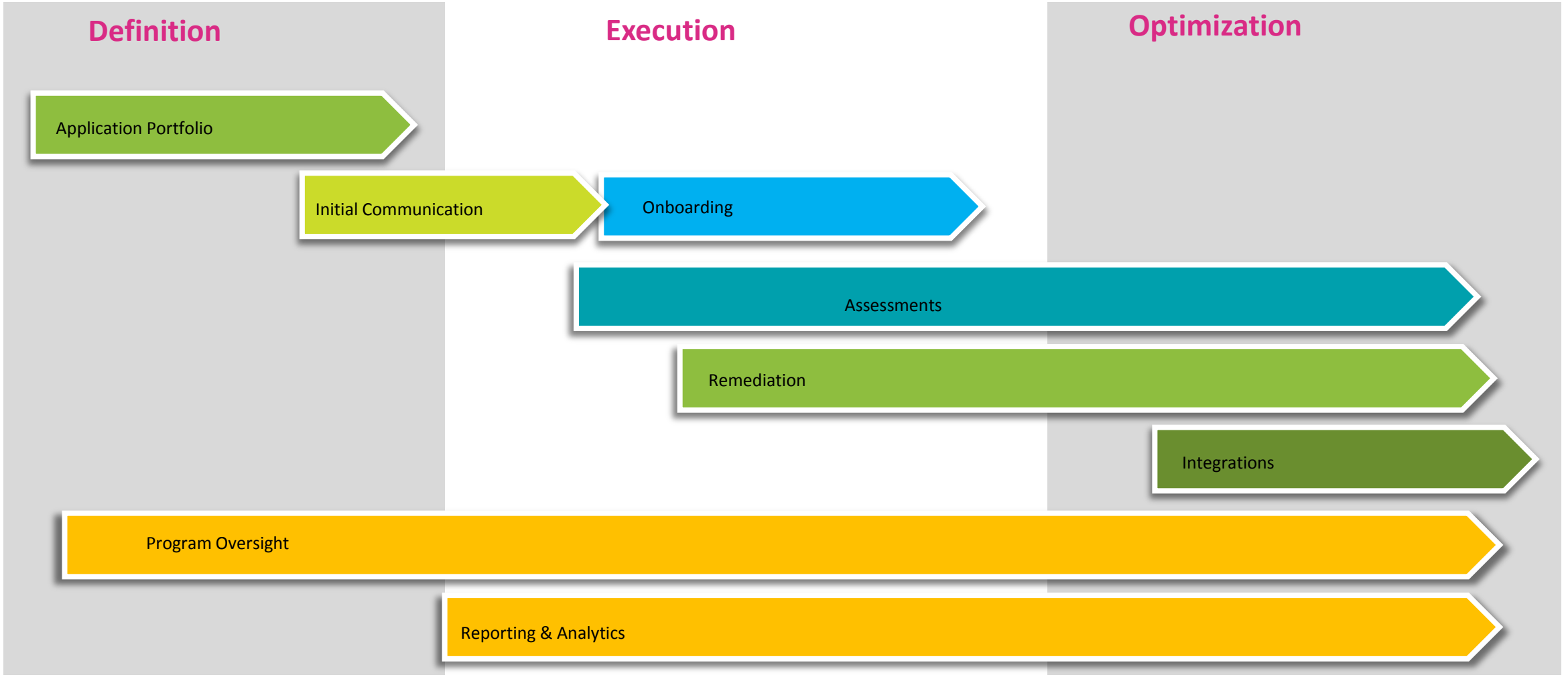



DID WE JUST BECOME BEST FRIENDS?

VANTAGEPOINT

Process

Appsec Program



ISO/IEC 27034

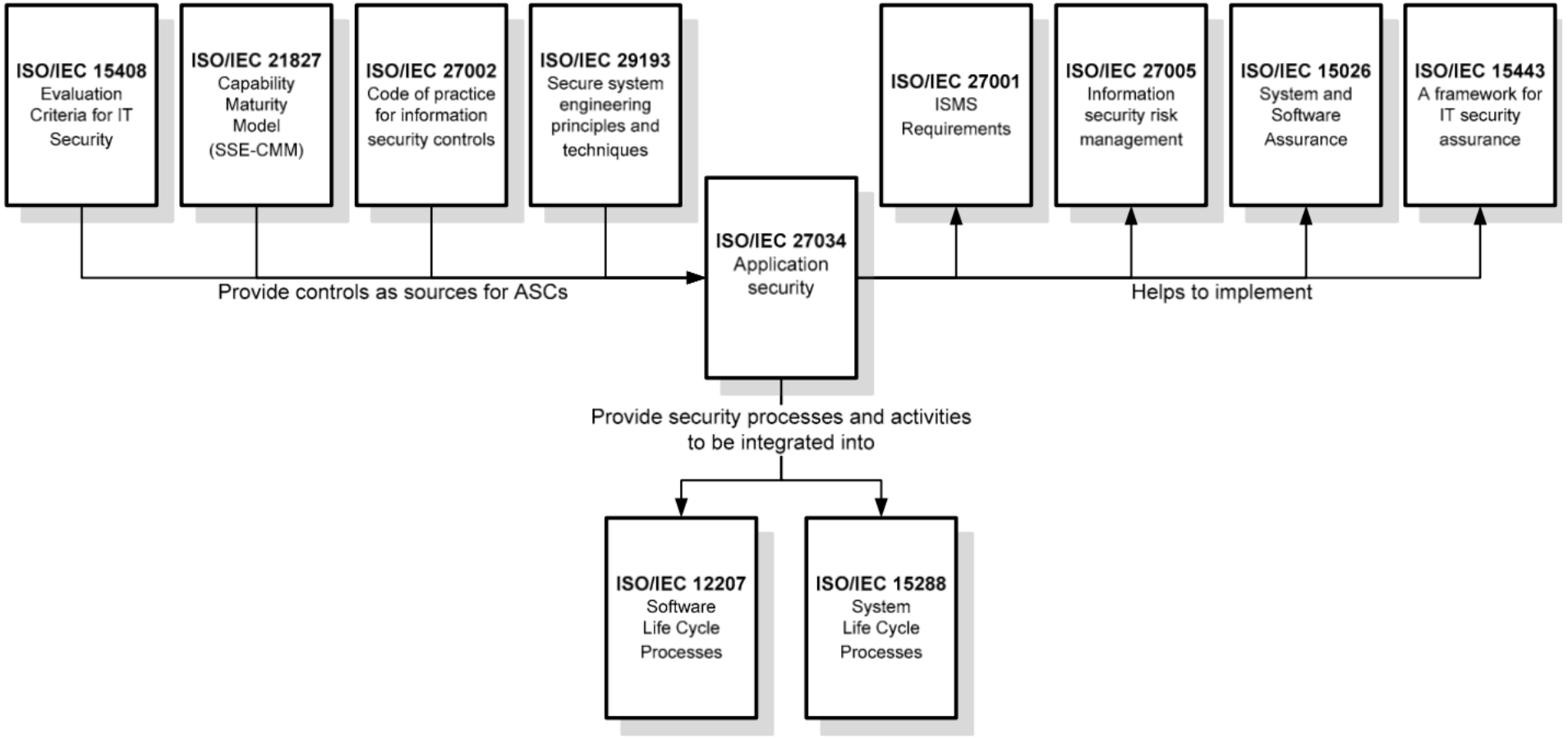
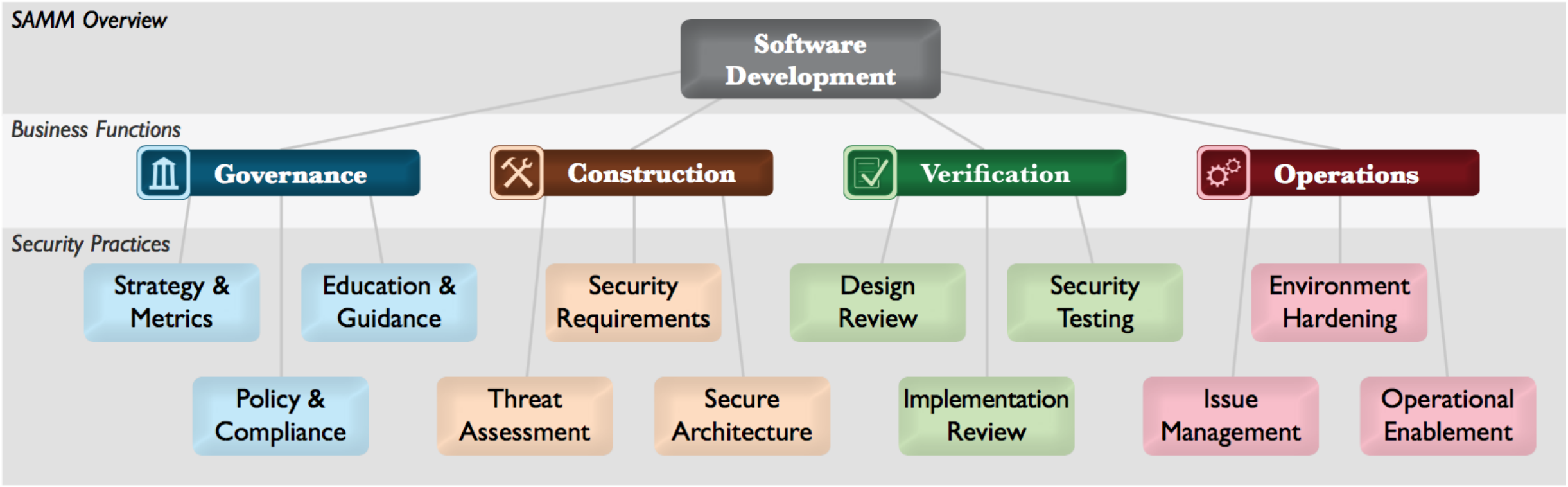


Figure 1 – Relationship to other International Standards

VANTAGEPOINT

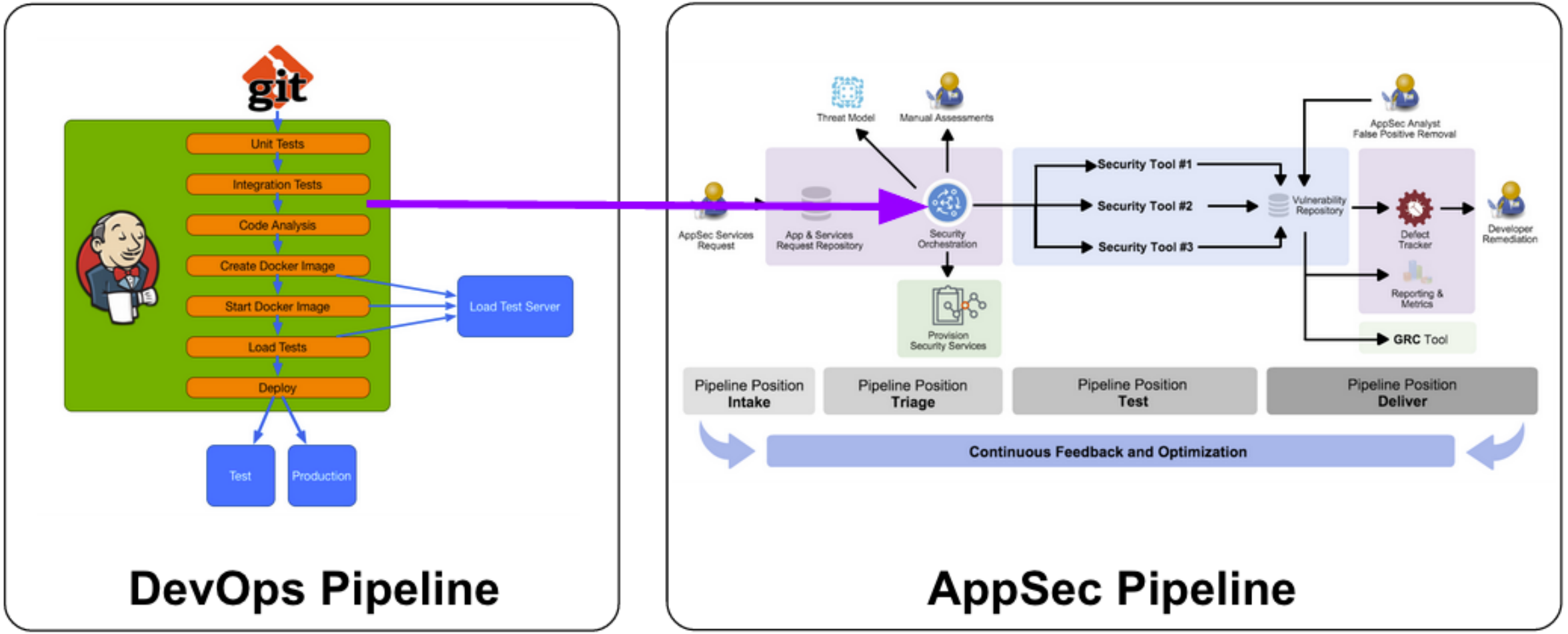
OPEN SAMM



Technology

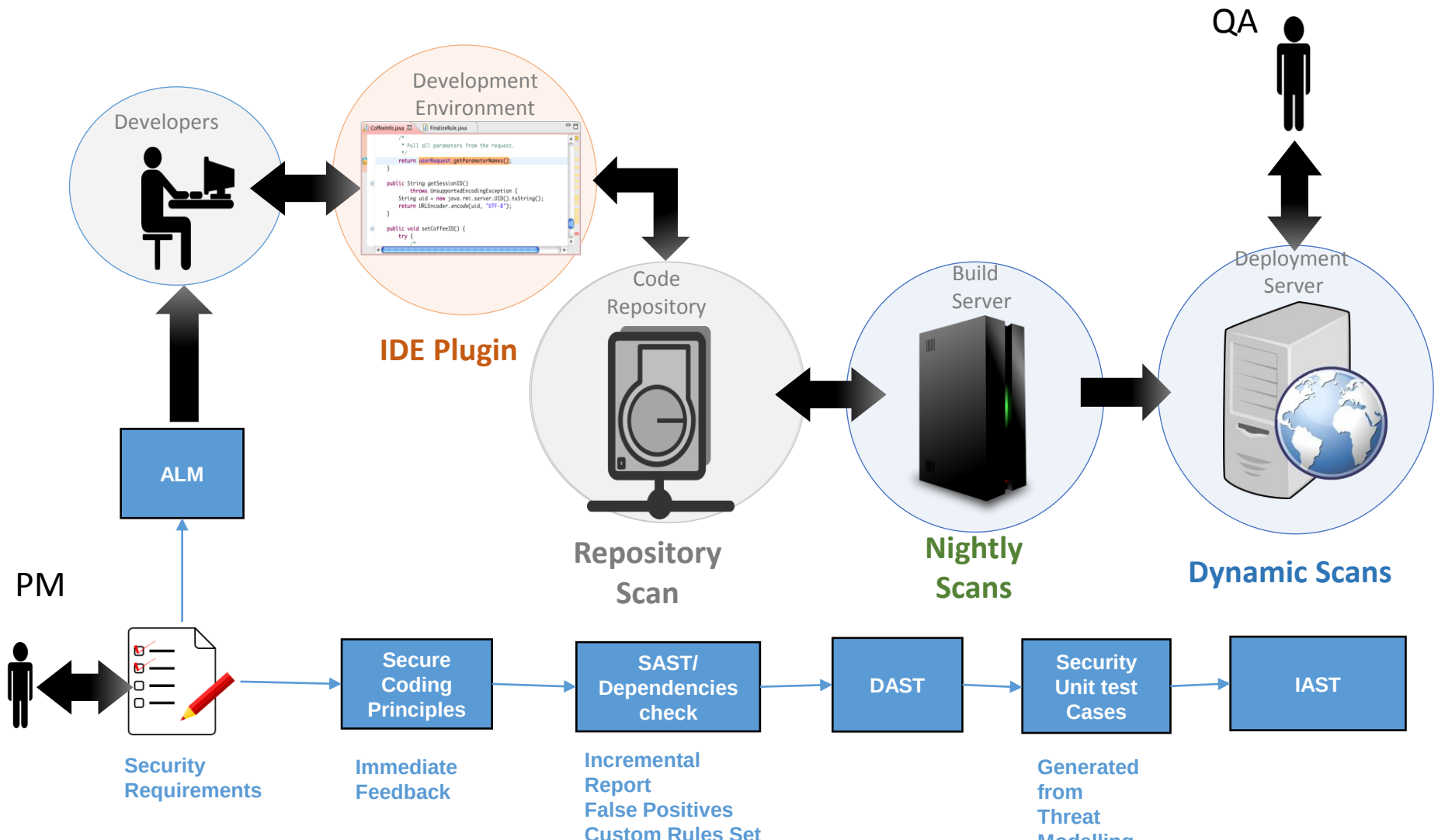
VANTAGEPOINT

OWASP Appsec Pipeline Project



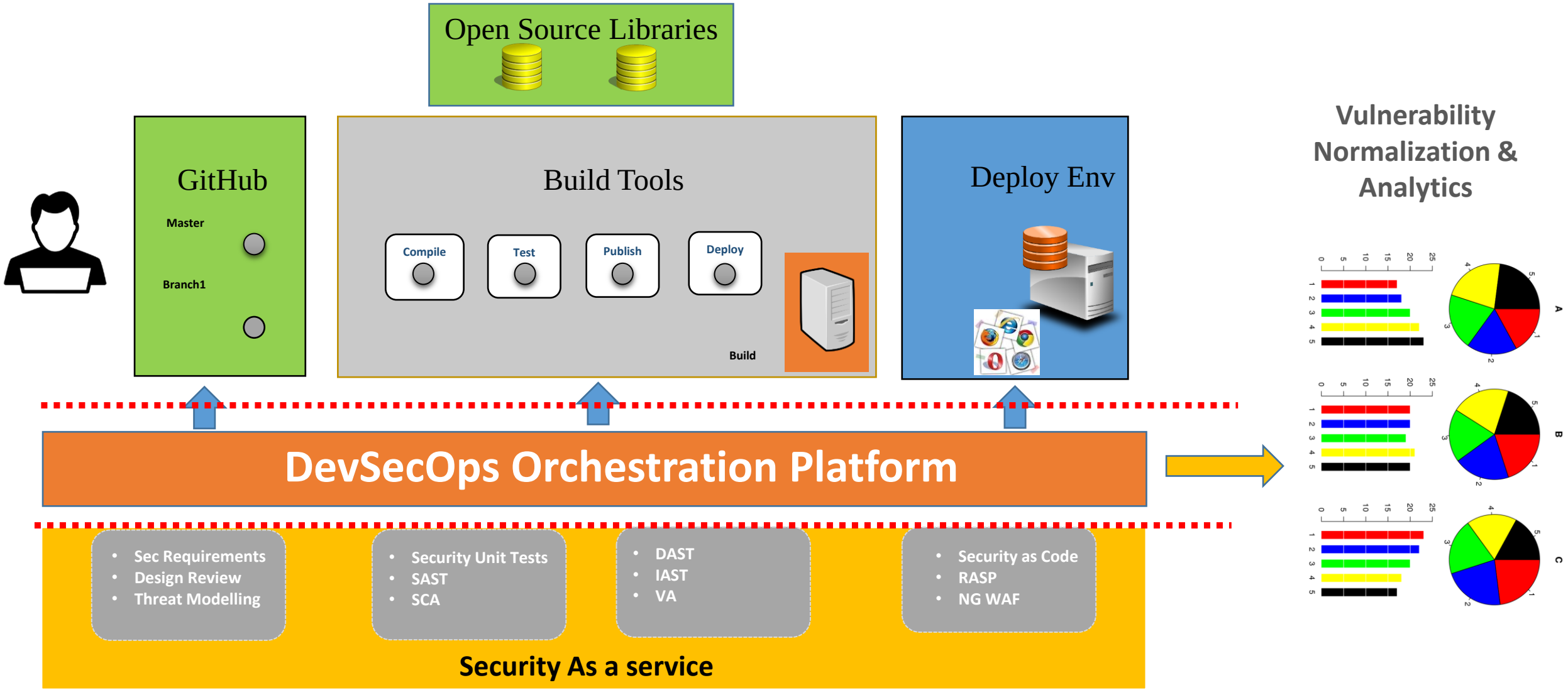
VANTAGEPOINT

Application Security Execution from Left



VANTAGEPOINT

DevSecOps Orchestration




Coming together
is a
beginning,
working together
is success.

VANTAGEPOINT

Q&A

suman.sourav@vantagepoint.sg