SYSTEMS ENGINEERING RESEARCH CENTER

SERC TALKS

WELCOME

How do Agile Methods Reduce Risk Exposure and Improve Security on Highly-Critical Systems?

Robin Yeman, Lockheed Martin Fellow, Lockheed Martin (LM) Information Systems and Global Solution, Agile/DevOpSec SME

April 4 | 1:00 PM ET

- ❑ **Today's session will be recorded.**
- ❑ **An archive of today's talk will be available at: www.sercuarc.org/serc-talks/**
- ❑ **Use the Q&A box to queue questions, reserving the chat box for comments, and questions will be answered during the last 5-10 minutes of the session.**
- ❑ **If you are connected via the dial-in information only, please email questions or comments to serctalks@stevens.edu.**
- ❑ **Any issues? Use the chat feature for any technical difficulties or other comments, or email serctalks@stevens.edu.**

The Systems Engineering Research Center (SERC) is a federally funded University Affiliated Research Center managed by Stevens Institute of Technology.

Any views, opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense, ASD(R&E), nor the SERC.

LOCKHEED MARTIN

Securing the delivery pipeline

NextGenLM

Robin Yeman
Lockheed Martin Fellow

Agenda

1.1 What is Agile

1.2 Why Agile

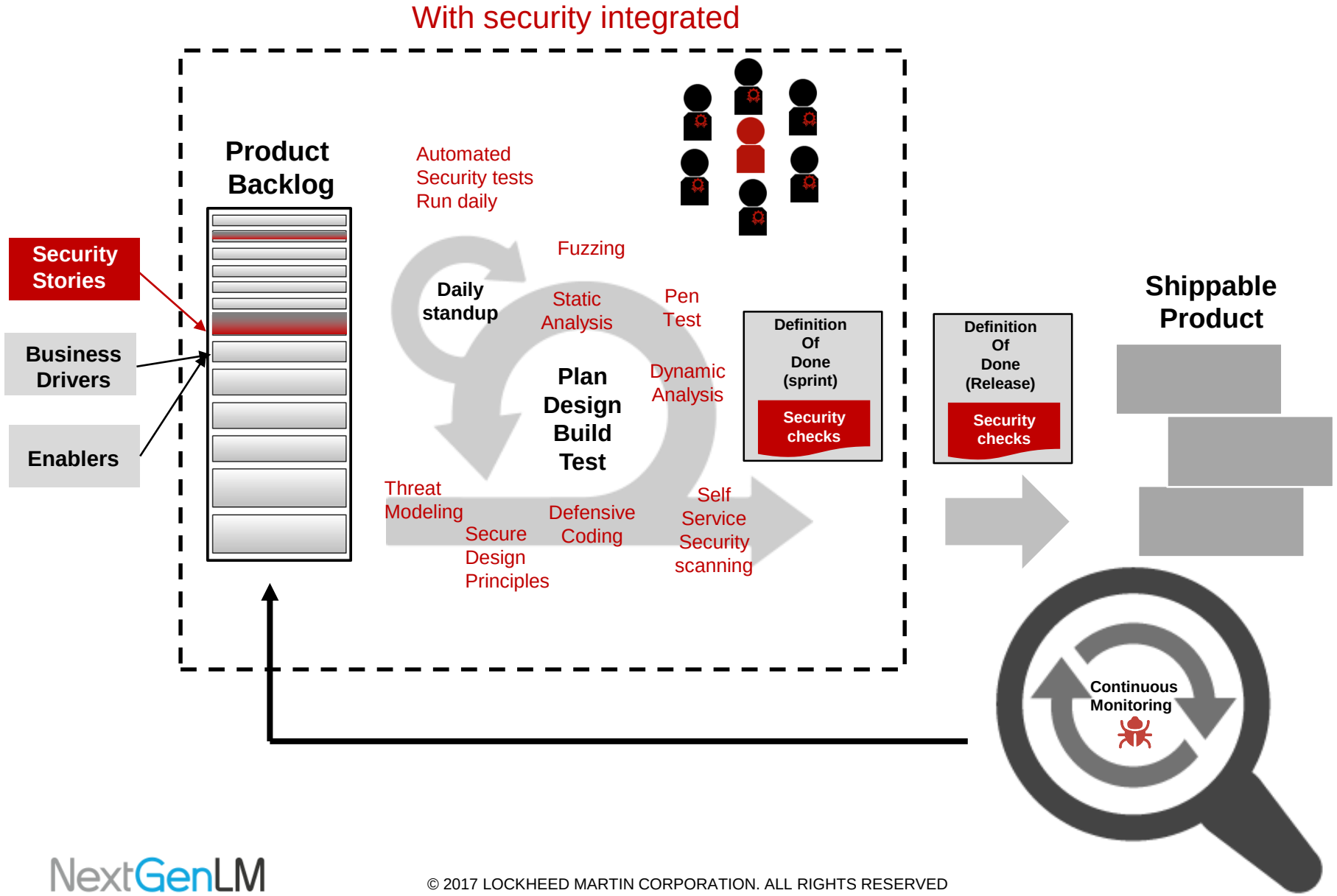
1.3 Agile Improves Security

1.4 The Future

Goals

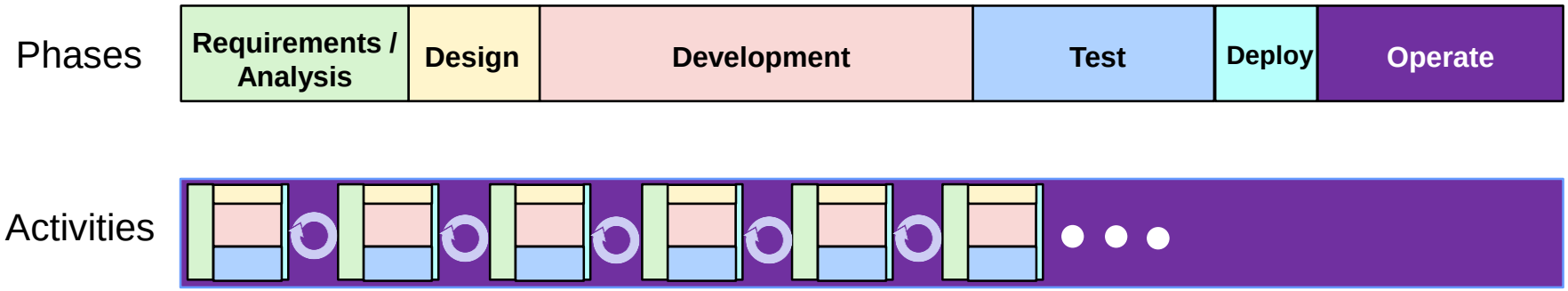
- **Defend**
- **Detect**
- **Deter**

Secure Agile Pipeline



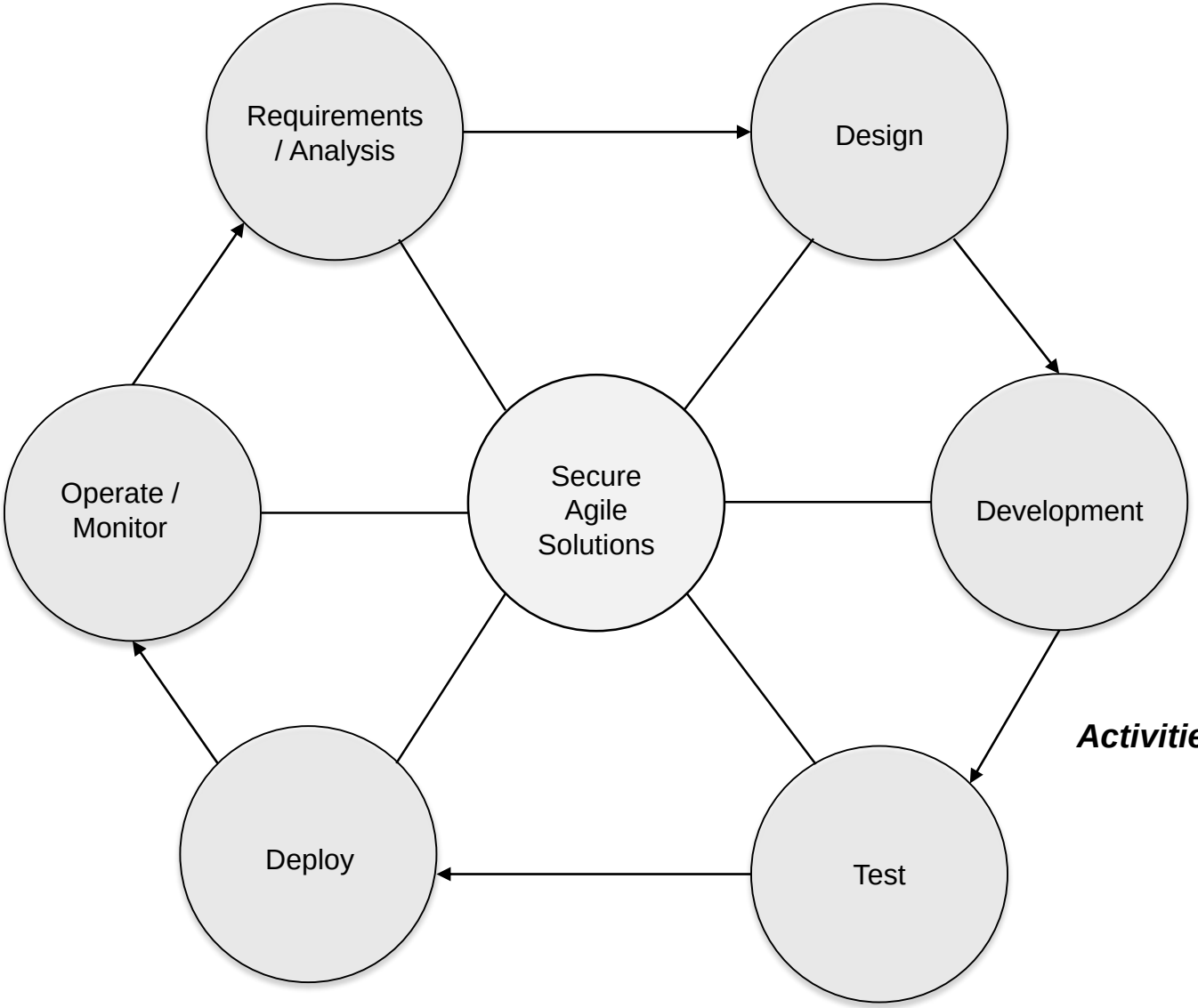
NextGenLM

Waterfall vs Agile Lifecycle



Activities as opposed to phases that have smaller batch sizes and Are repeated.

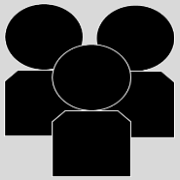
Secure Solutions through Agile



Activities not Phases

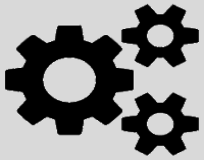
Requirements / Analysis

People



- Cross functional team
- Embedded security SME or security skills

Process



- Include security in product backlog
- Security Test driven development
- Security RMF (NIST)

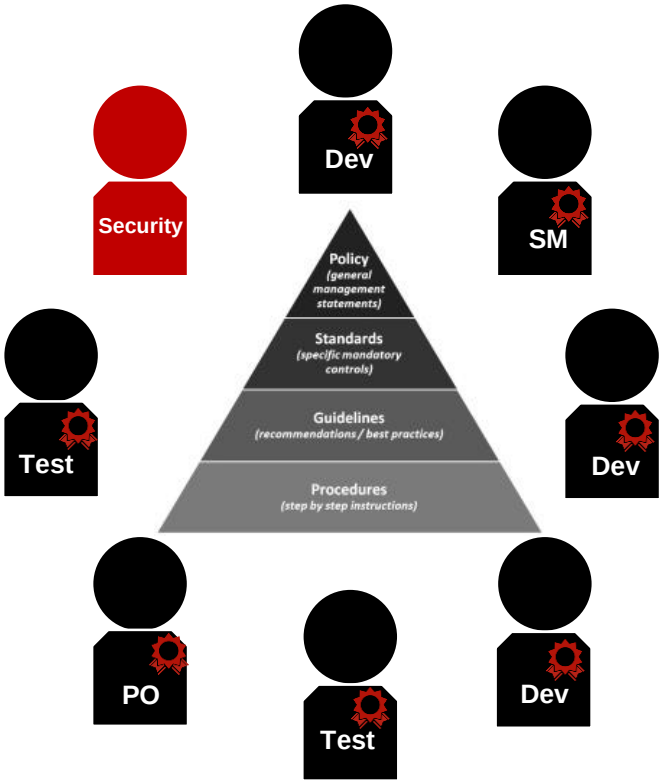
Tools

- Personas
- Mis-user stories
- Security user stories

Beginning our requirements with security in mind enables us to build trust early and prevent downstream friction.

Secure Requirements/Analysis

Cross-functional scrum team



Ensure everyone on team Has security skills

Personas

Harry Hacker

Hacker

Skillset:

Proficient with the latest technology and enjoys leveraging their knowledge to exploit other's weaknesses

Responsibilities:

- Stays current with latest technology
- Observant in nature
- Comfortable with change
- Constantly experimenting with new ideas and evaluating the results
- Identify weakness in people, process, and tools
- Constantly testing boundaries

Definition of Done

Definition of Done Policy / Description

All Work Items completed must meet the following criteria before moving the work item into the done column:

- ✓ All code / tests checked in trunk
- ✓ All Access controls checked
- ✓ High risk code reviewed by security
- ✓ All unit and integration tests passing
- ✓ Security Scanning complete
- ✓ Static analysis complete and with SLA's
- ✓ All acceptance tests written and passing
- ✓ Documentation complete
- ✓ Peer reviews complete
- ✓ Cycle time posted

Hacker Story

As a fraudster, I want to see the details of an order that is not my own so that I can learn another person's private information.

Security Story

As a customer, I want to be sure that the credit card data that I provide for payments are processed and stored securely, so that access by third parties or hackers is impossible

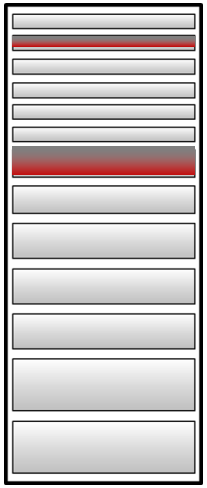
Normal Story

As a customer I want to Store my information in a profile So that I do not have to put information Into system every time I shop.

Enabler Story

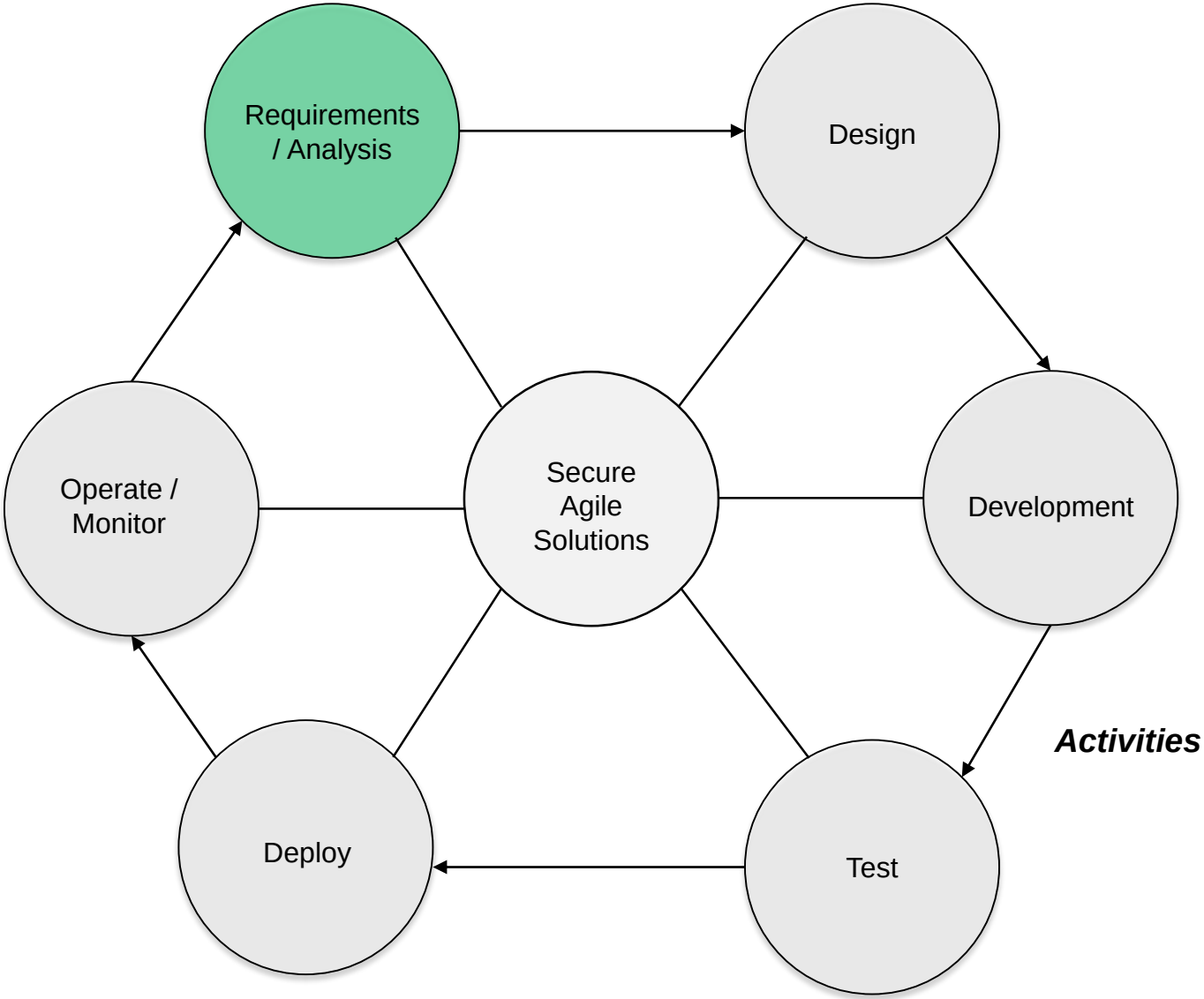
As a team I want to have current security guidelines and procedures so that I can build security into the baseline.

Product Backlog



NextGenLM

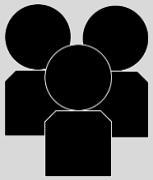
Secure Solutions through Agile



Activities not Phases

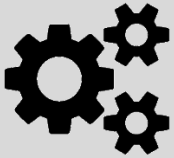
Design

People



- Cross functional team
- Embedded security SME or security skills

Process



- Threat Modeling
- Security Design Principles

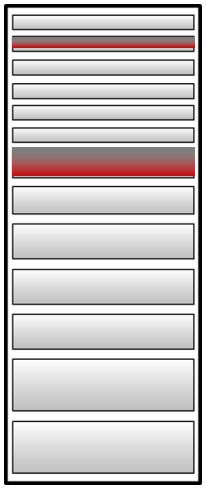
Tools

- Open Design
- Security traceability matrix
- Security Service Catalogue

Security by design moves team focus to vulnerability prevention from vulnerability detection

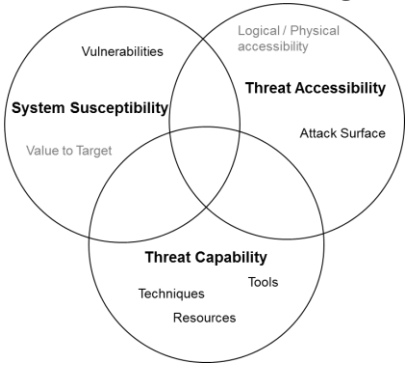
Secure Design

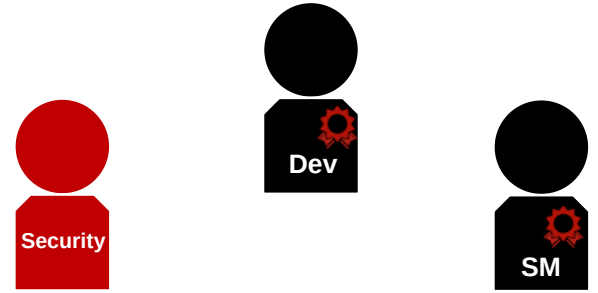
Product Backlog



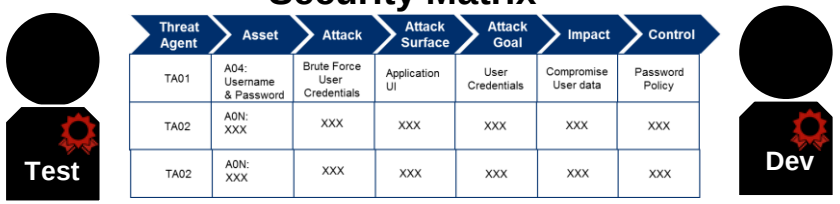
Security Design Principles

Threat Modeling

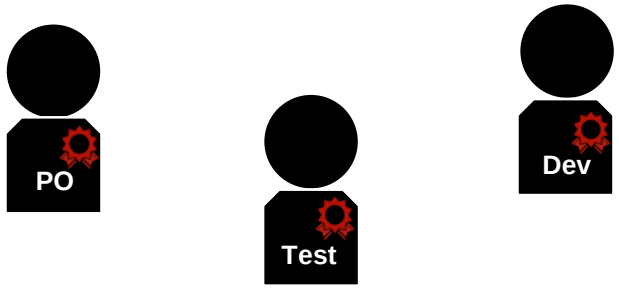




Security Matrix

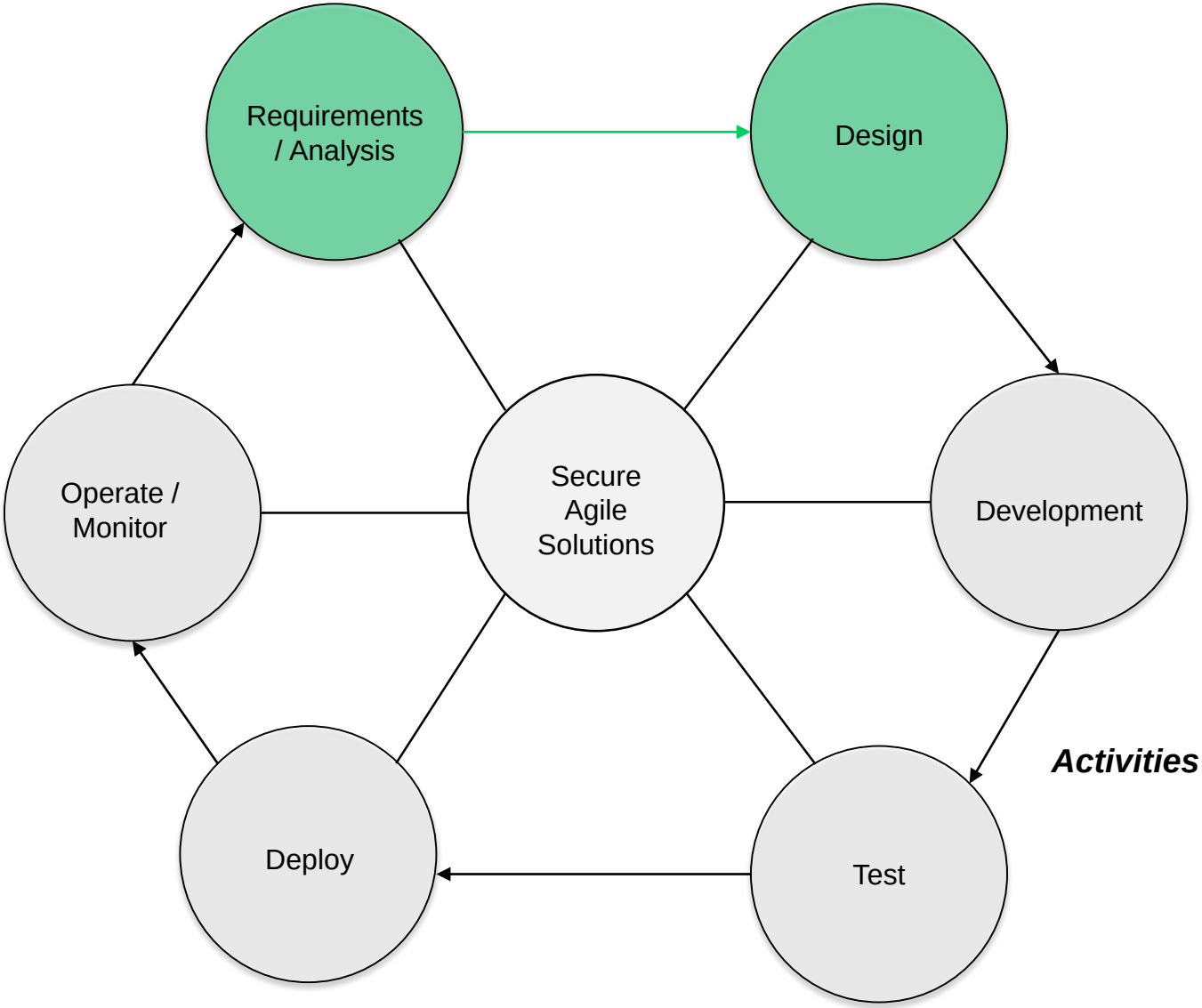


Threat Agent	Asset	Attack	Attack Surface	Attack Goal	Impact	Control
TA01	A04: Username & Password	Brute Force User Credentials	Application UI	User Credentials	Compromise User data	Password Policy
TA02	A0N: XXX	XXX	XXX	XXX	XXX	XXX
TA02	A0N: XXX	XXX	XXX	XXX	XXX	XXX



NextGenLM

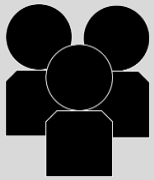
Secure Solutions through Agile



Activities not Phases

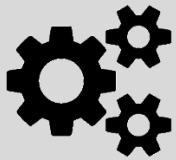
Development

People



- Cross functional team
- Embedded security SME or security skills
- Hacking Skills

Process



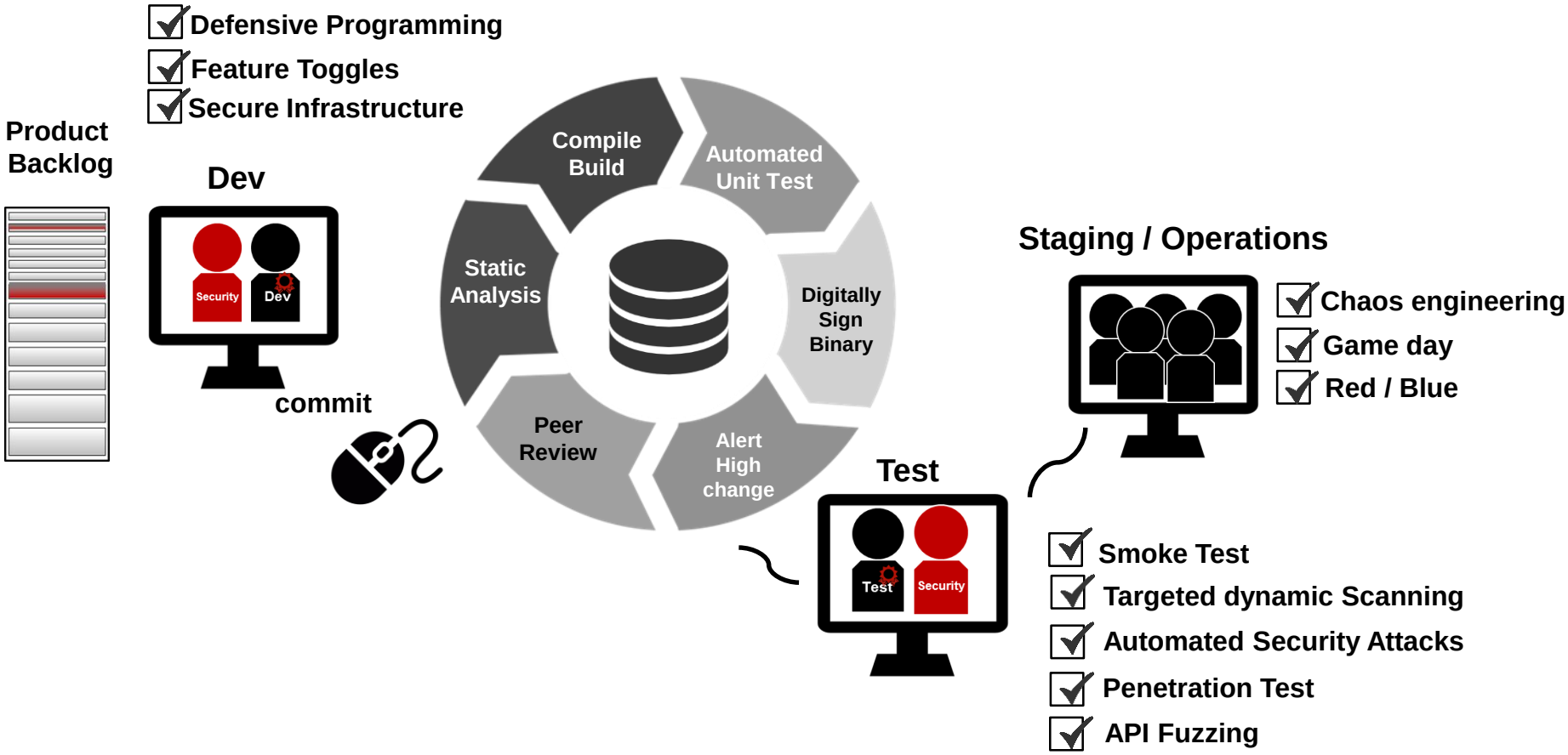
- Build on secure libraries
- Infrastructure as code
- Compliance as code
- Defensive programming
- Compartmentalization
- Feature Toggles
- Peer reviews
- Self-service security scanning
- Security Spikes

Tools

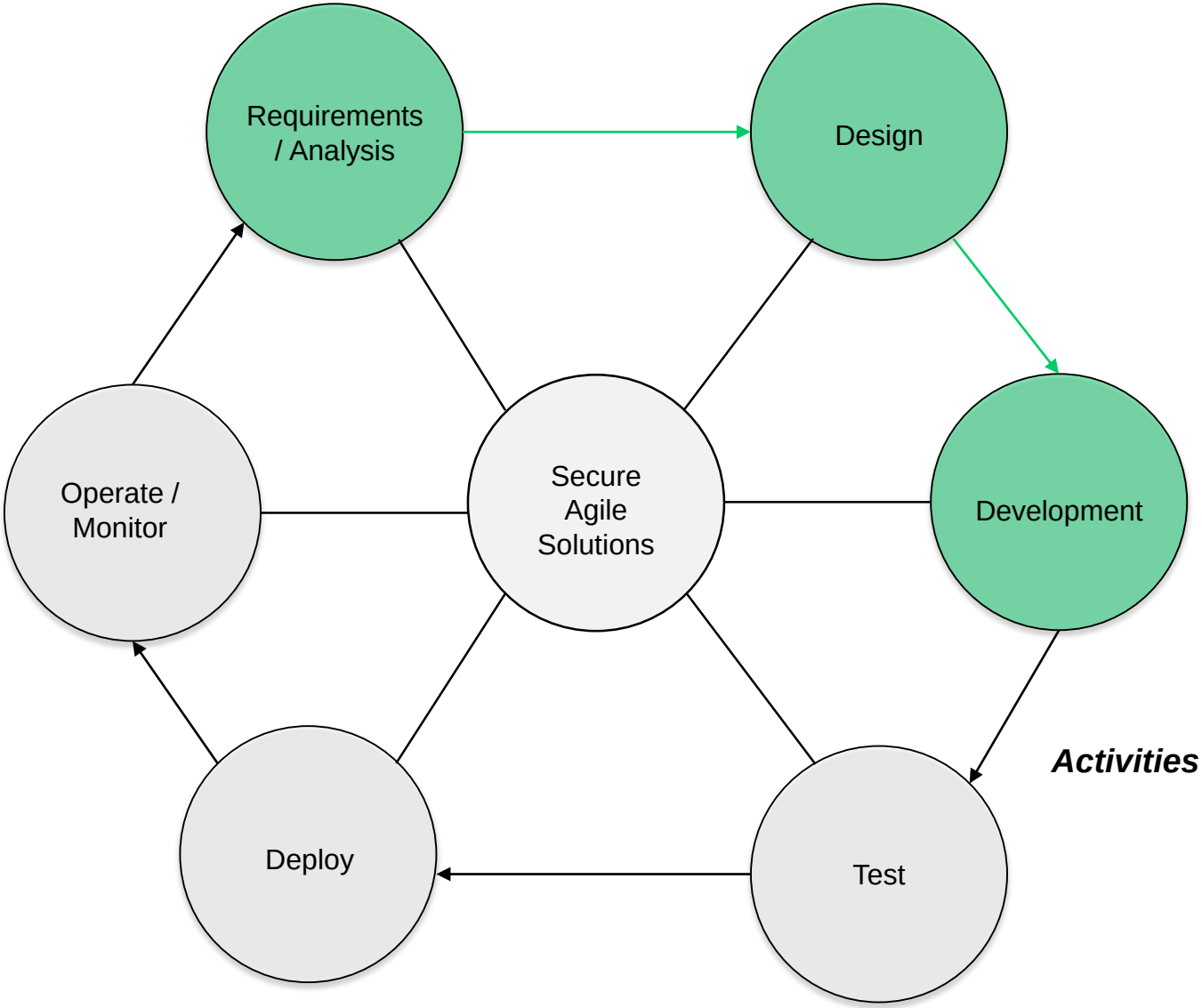
- Security service catalog
- Secure Infrastructure
- Continuous Integration
- Static Analysis
- Audit defense toolkit
- Vulnerability metrics

Moving from control gates to guardrails with automation and workflows

Secure Development Pipeline



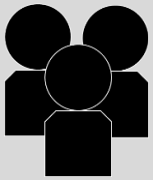
Secure Solutions through Agile



Activities not Phases

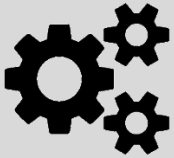
Testing

People



- Cross functional team
- Embedded security SME or security skills
- Hacking Skills
- Automated test SME or skills

Process



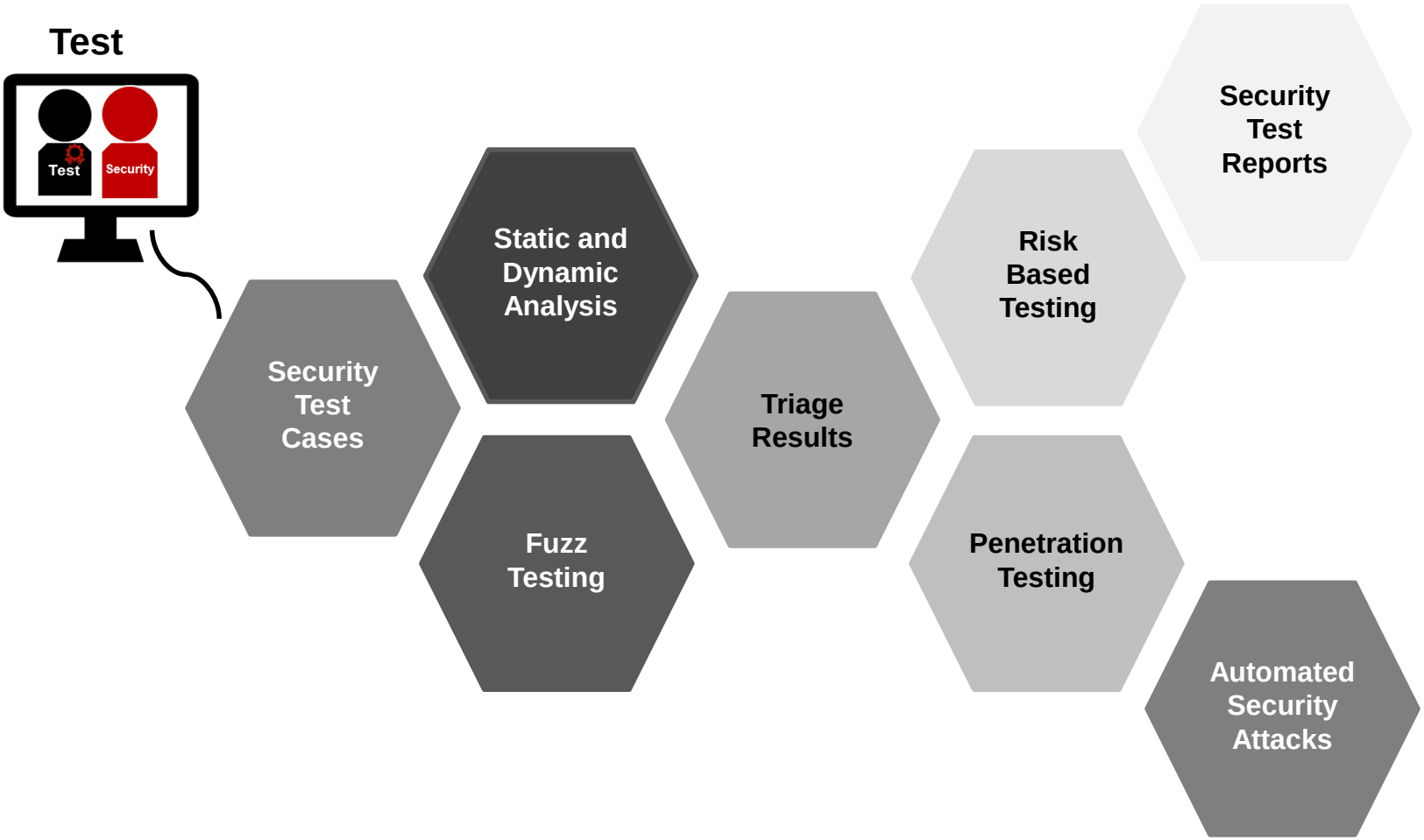
- Fuzz Testing
- Chaos Engineering
- Security Test Cases
- Risk based test
- Penetration Testing

Tools

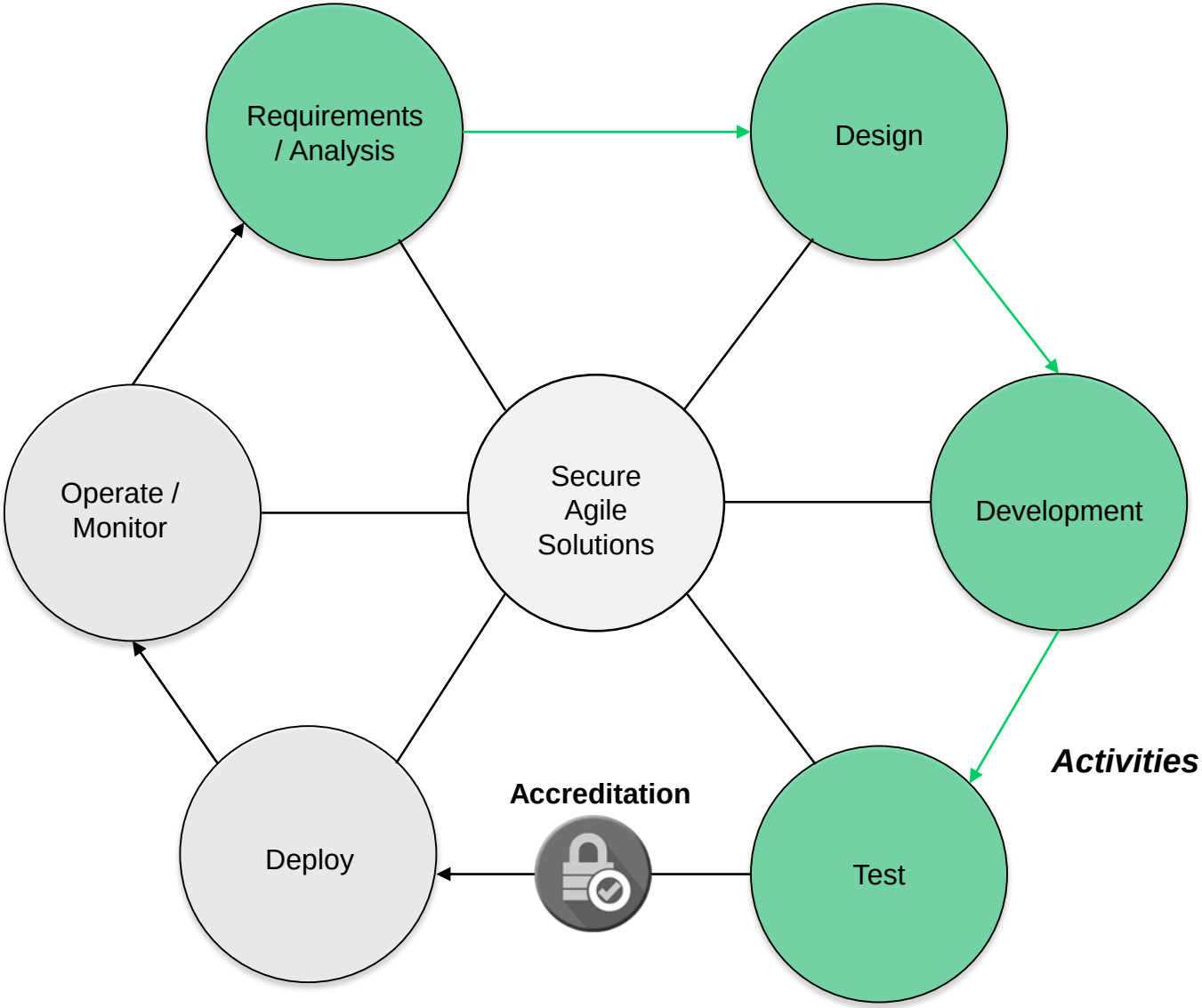
- Automated Test
- Quality / Security reports

Layered Security test levels reduces flaws in the systems we deliver

Security Testing



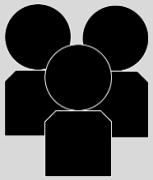
Secure Solutions through Agile



Activities not Phases

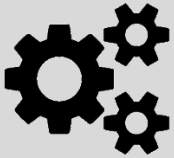
Deploy

People



- Cross functional team
- Embedded security SME or security skills
- Hacking Skills
- Automated test SME or skills
- Operation (representatives)

Process



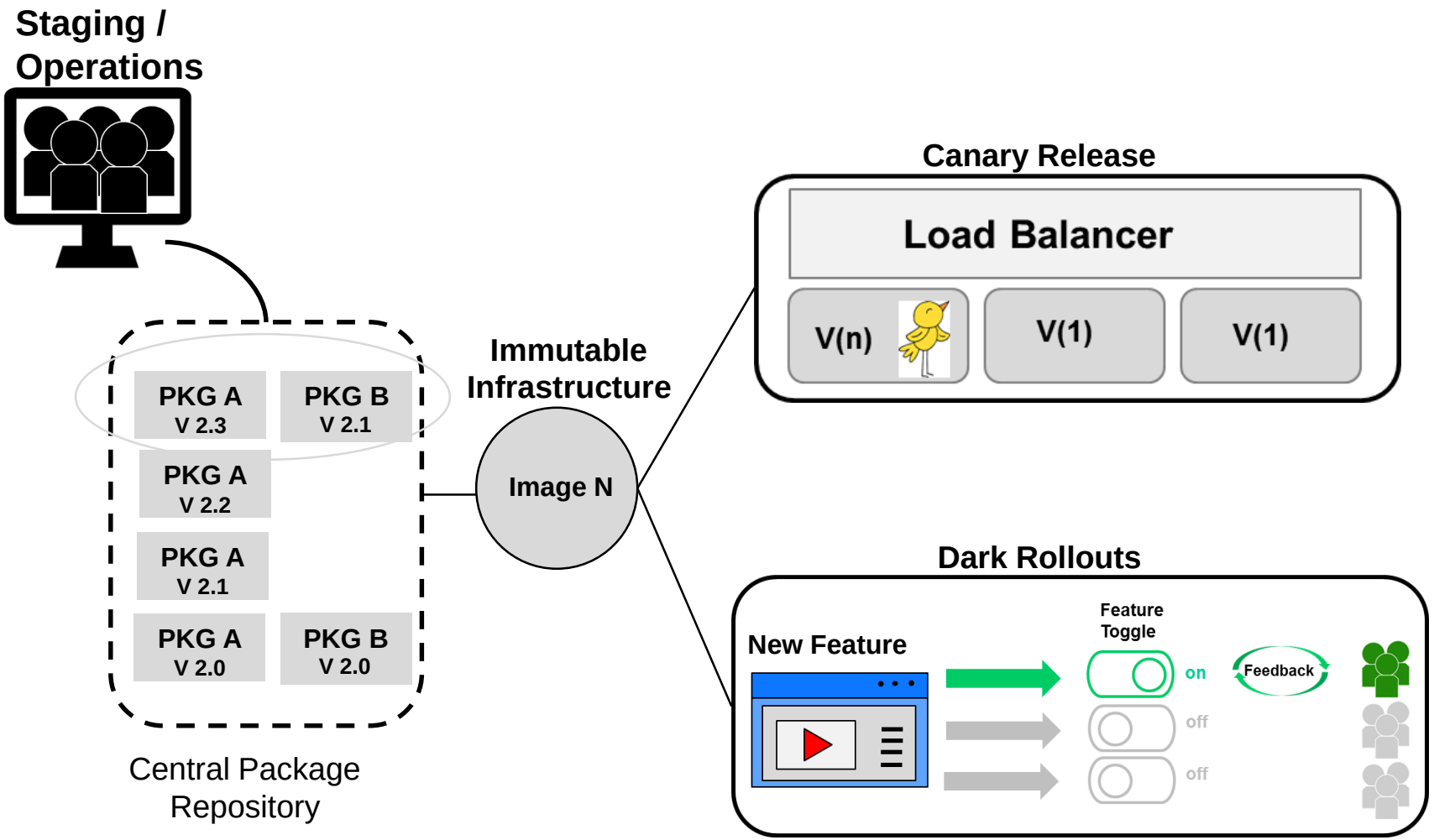
- Secure the Infrastructure
- Dark Roll-outs
- Canary Releases

Tools

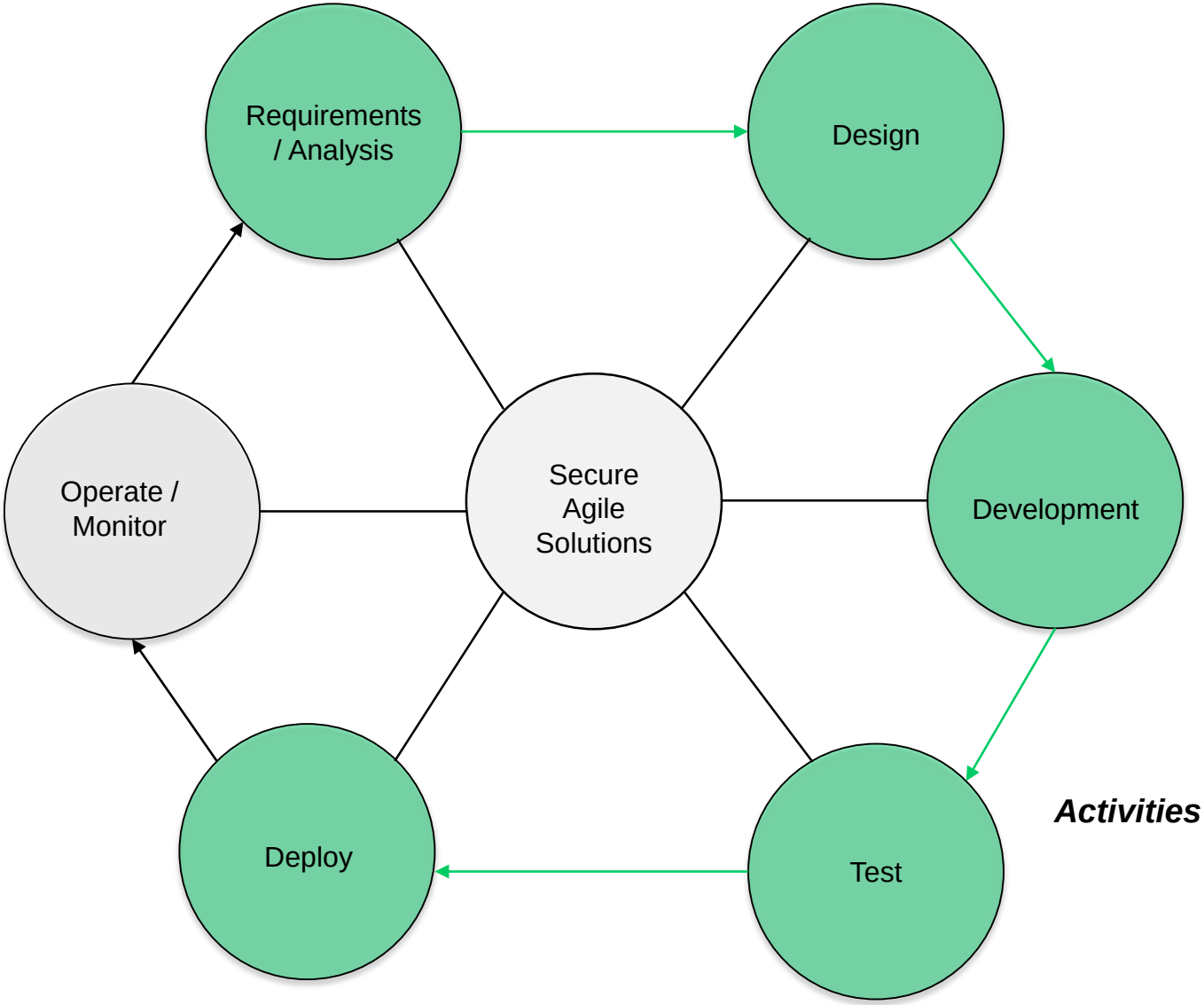
- Immutable Infrastructure
- Containers

Secure deployments take the stress out of delivery and allows use to deploy more often with smaller batches

Secure deployments



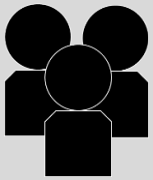
Secure Solutions through Agile



Activities not Phases

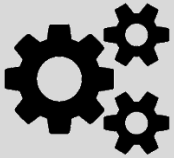
Operate and Monitor

People



- Cross functional team
- Embedded security SME or security skills
- Hacking Skills
- Automated test SME or skills
- Operation (representatives)

Process



- Attack-Driven-Defense
- Game days
- Red Team / Blue Team
- Chaos Engineering
- Blameless post-mortems

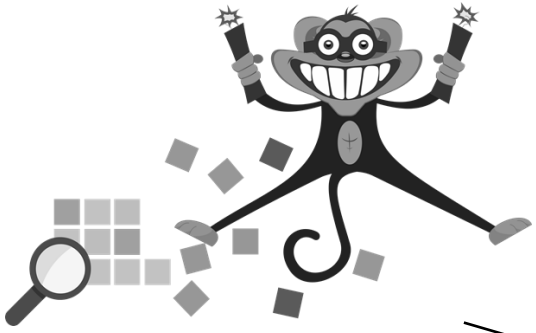
Tools

- Chaos Monkey / Gorilla
- Logging / Monitoring
- Runtime defense
- Bug Bounty

Embracing a culture of continuous improvement results in secure systems

Secure Operations

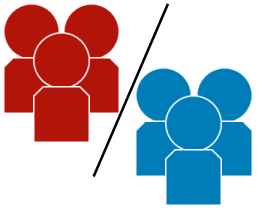
Chaos Engineering



Game Day

Red/Blue Team

- MTTA
- MTTD
- MTTR

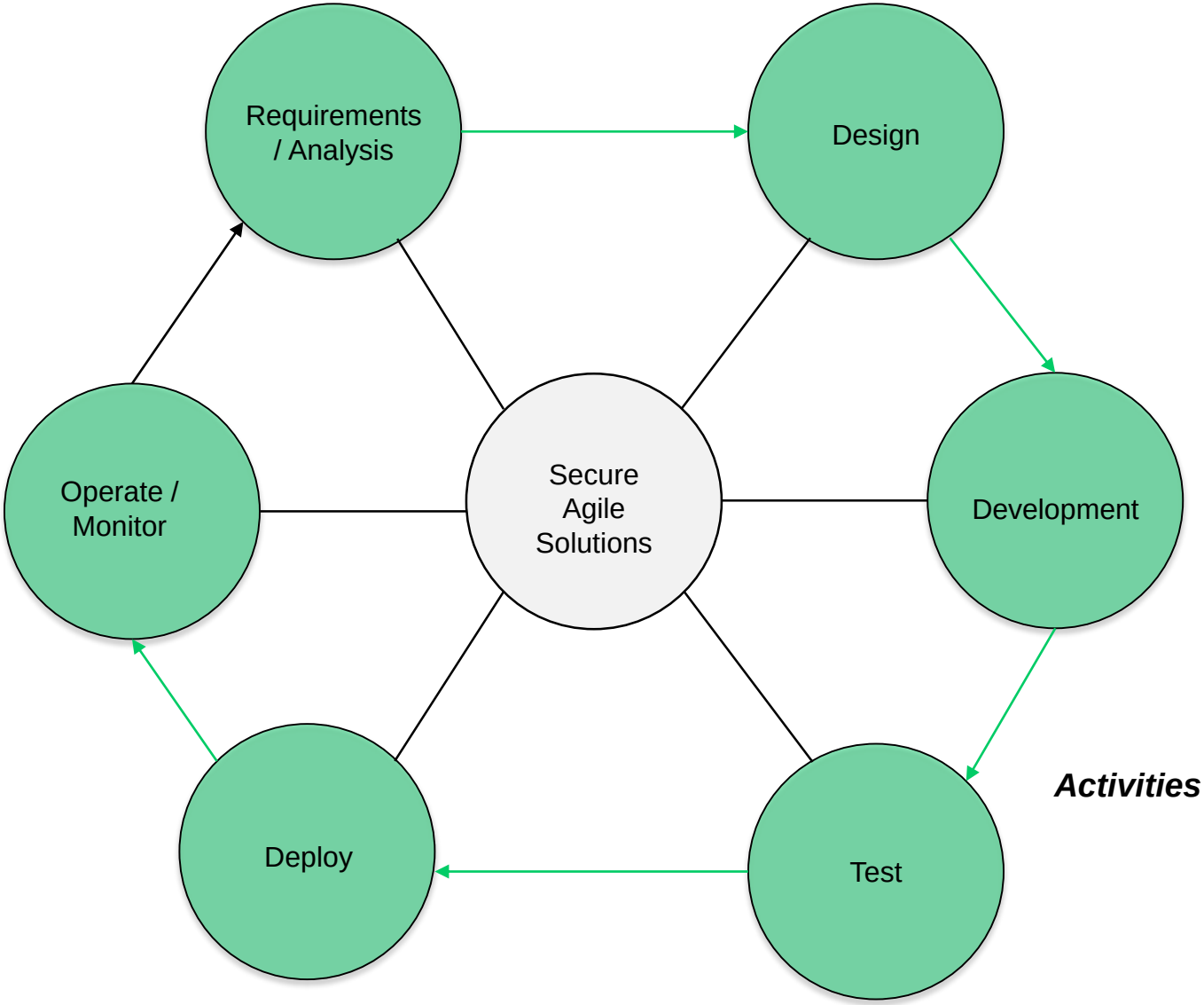


Bug Bounty

Feedback

Product Backlog

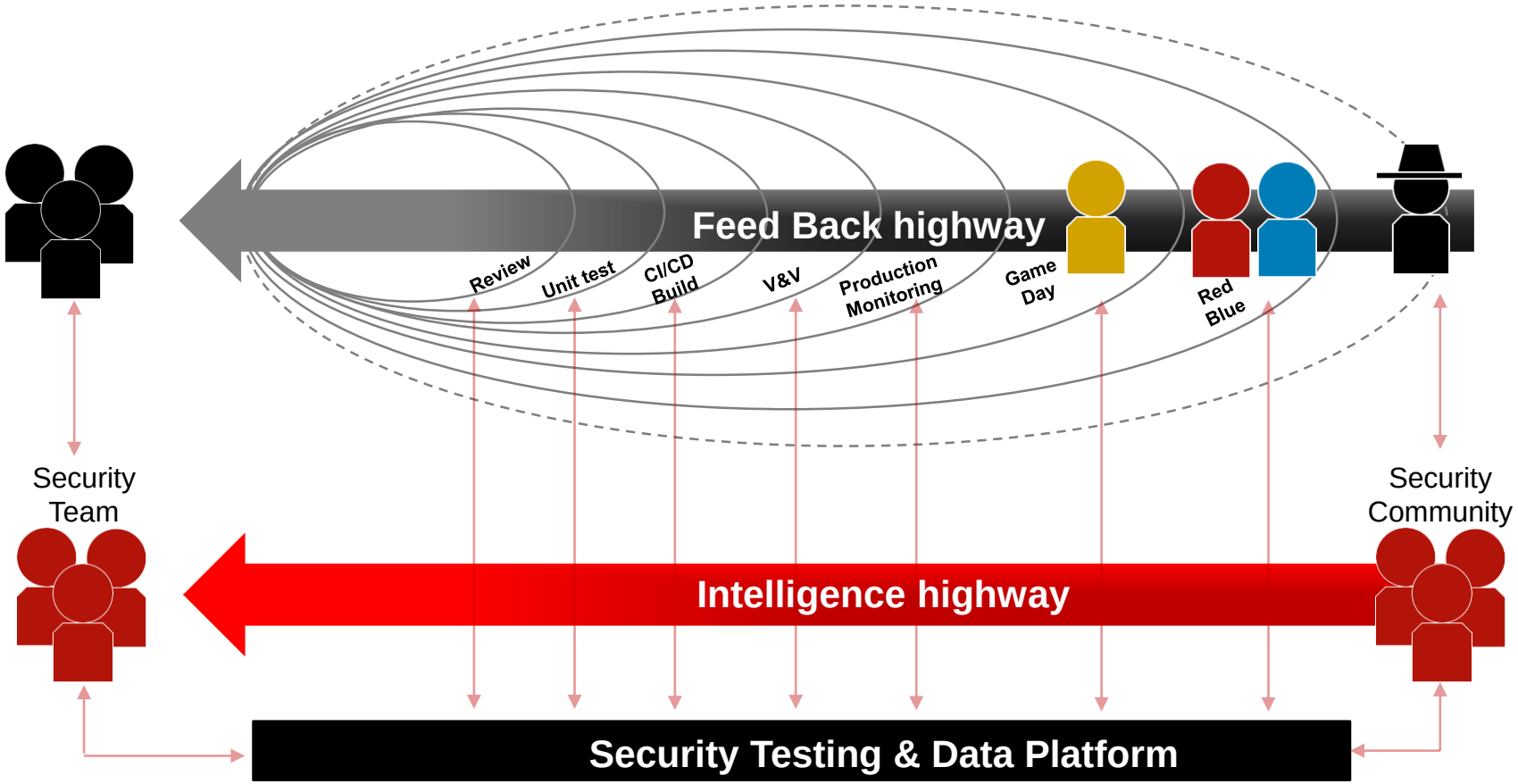
Secure Solutions through Agile



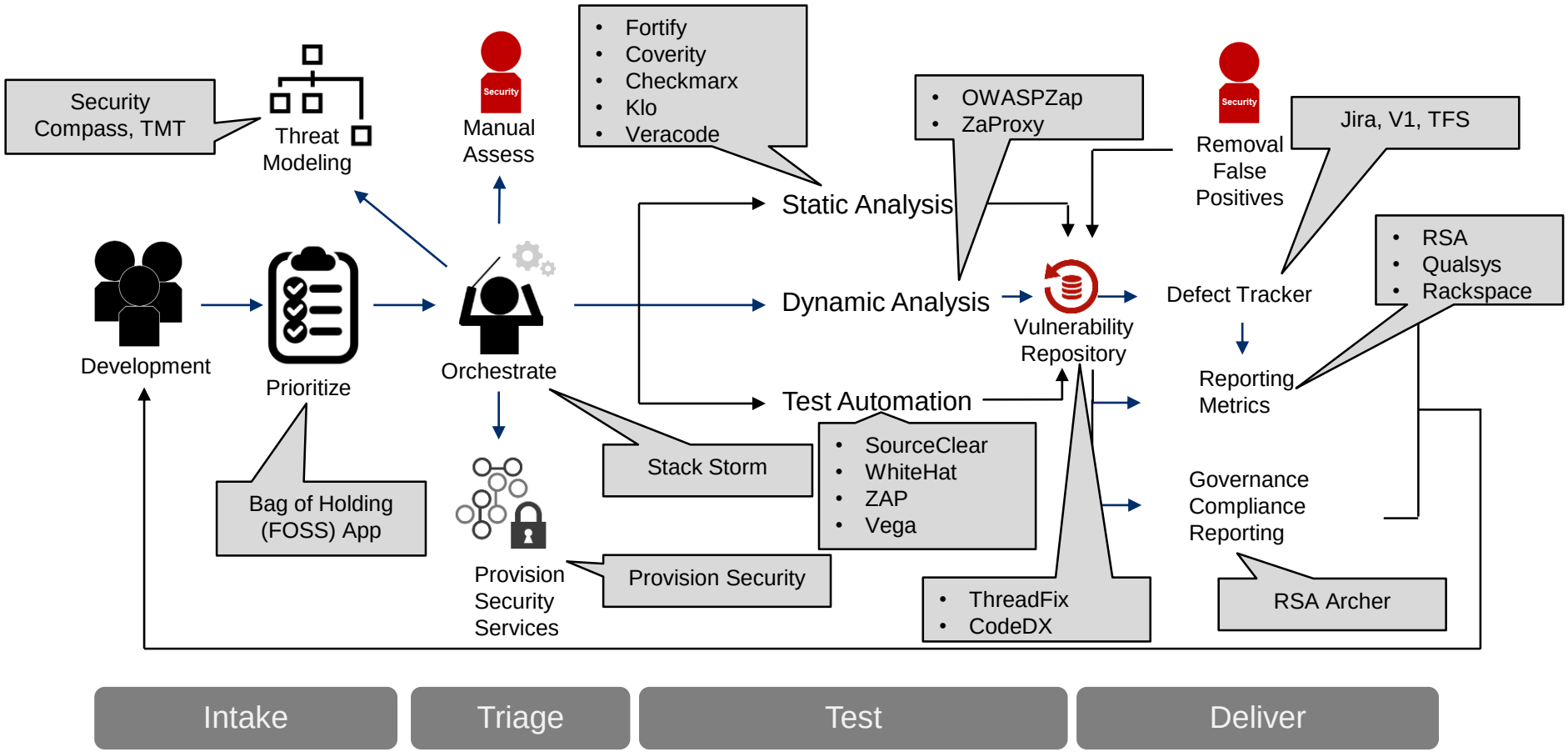
Activities not Phases

Future

DevOpsSec: Seamlessly integrate security into the implementation pipeline; ensuring everyone takes responsibility while continuing to shorten feedback loops



Automated Security Pipeline



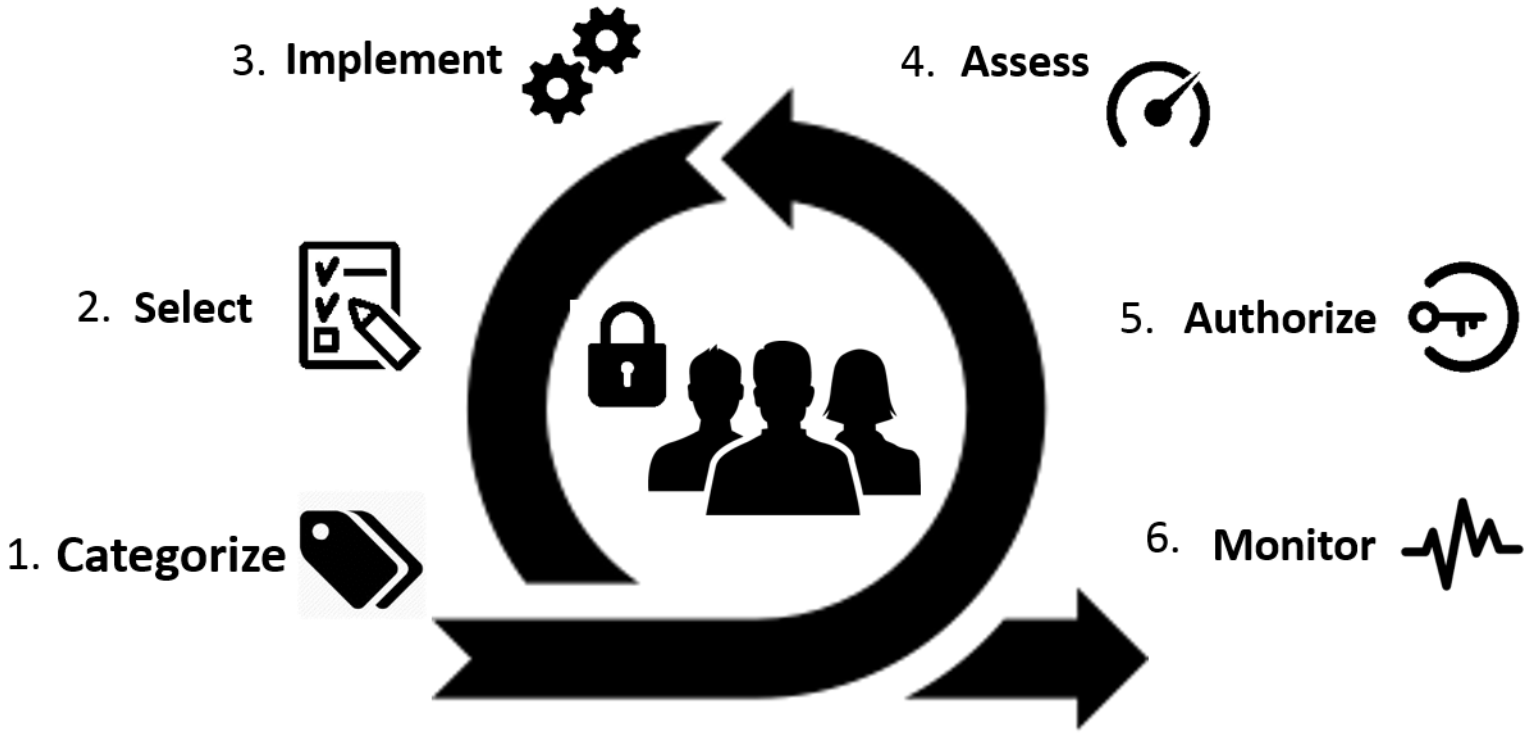
Lockheed Martin Cyber Kill Chain®

Threat Focused Operations Through
Intelligence Driven Defence® *are Critical*

OWG201701004

NextGenLM

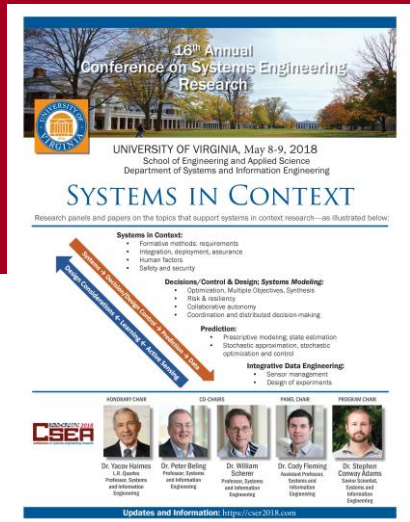
RMF (NIST Risk Mgt Framework)



Upcoming Events

16th Annual Conference on Systems Engineering Research

Hosted by: UNIVERSITY OF VIRGINIA, School of Engineering and Applied Science Department of Systems and Information Engineering
May 8 & 9, 2018



Theme: "Systems in Context"

Key Dates:

Final Paper Submission Due: April 13, 2018

Conference Registration Opens: February 1, 2018

Direct link to registration web page: http://edas.info/r24260

POCs:

Peter A. Beling: pb3a@virginia.edu

William T. Scherer: wts@virginia.edu

Cody H. Fleming: fleming@virginia.edu

Venue: University of Virginia Inn at Darden at the University of Virginia

Reserve rooms (referencing CSER) or online at this link.

For more information visit: https://cser2018.com/.

SERC TALKS

UPCOMING TALKS:

"Successfully Applying Agile Methods for High-Criticality Systems" Series

How Do You Use Agile Methods on Highly-Critical Systems that Require Earned Value Management?

Phyllis Marbach, INCOSE LA Chapter President; Senior Software Engineer at Boeing – Retired

June 6 | 1:00 PM ET | REGISTER NOW

CONTACT

Editor-in-Chief: Dr. Barry Boehm, University of Southern California – boehm@usc.edu

Ms. Maia Canlas, Stevens Institute of Technology – mcanlas@stevens.edu

Thank you for joining us!

Please check back on the SERC website for today's recording and future SERC Talks information!

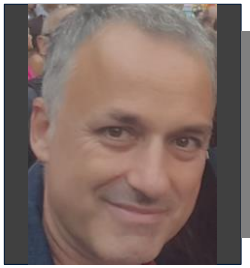
SERC TALKS

UPCOMING TALKS:

"Systems and Software Qualities Tradespace Analysis" Series

Barry Boehm, Chief Scientist, SERC; TRW Professor of Software Engineering and Director, Center for Software Engineering, University of Southern California
August 1 | 1:00 PM ET

Bill Curtis, Senior VP & Chief Scientist, CAST Software; Head of CAST Research Labs, Executive Director, Consortium for IT Software Quality (CISQ)
October 3 | 1:00 PM ET



Xavier Franch, Full Professor, Polytechnic University of Catalonia (BarcelonaTech)
December 11 | 1:00 PM ET

Please visit the SERC Talks page for more information and updates.