



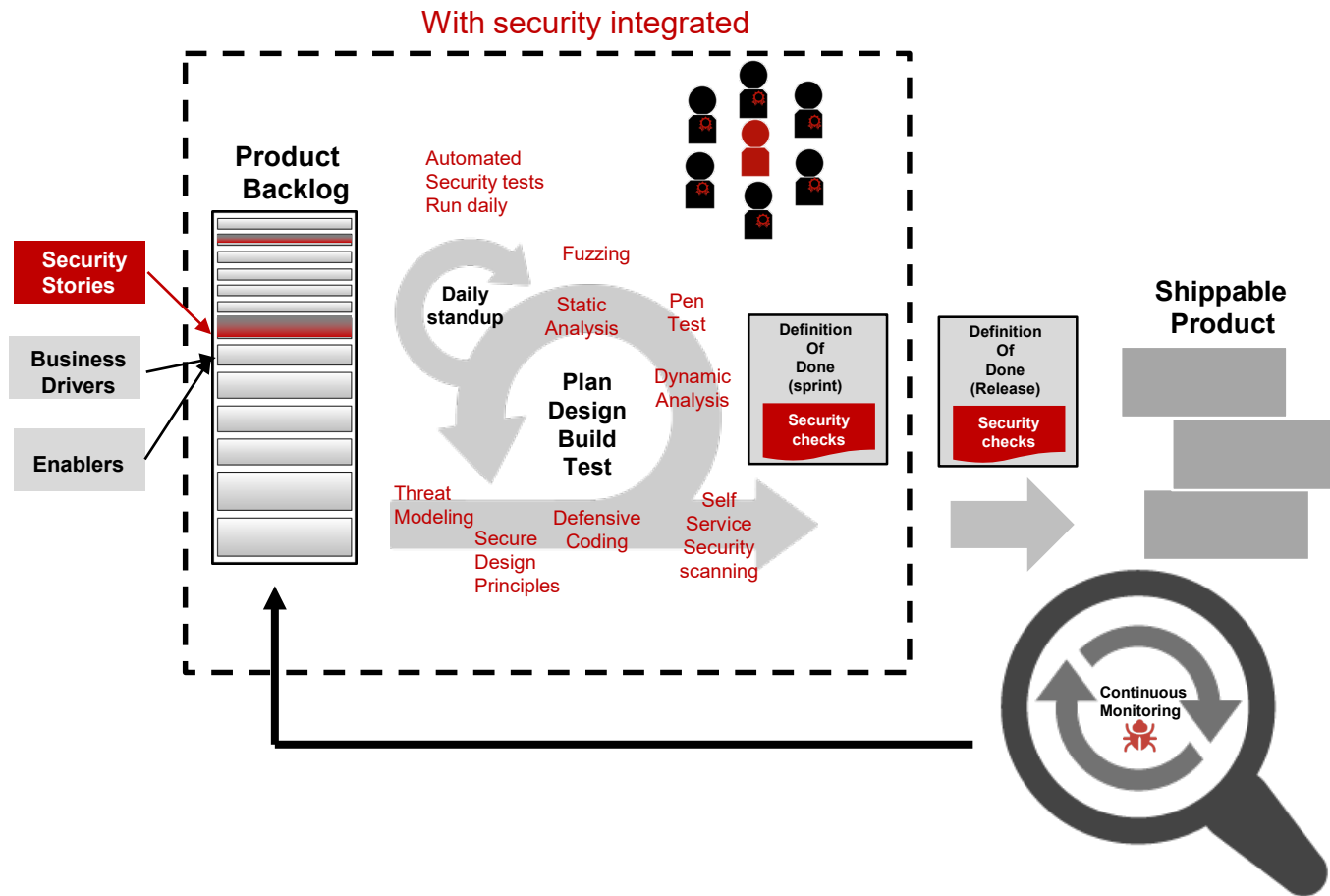
Leveraging DevSecOps to manage program security performance



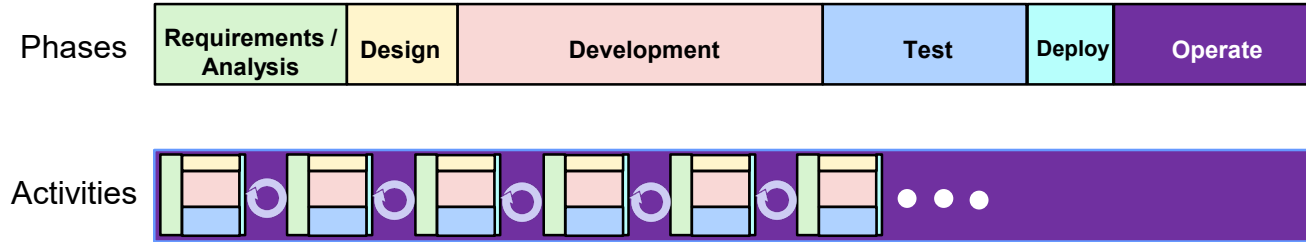
Cyber Security Goals

- Defend (Data, Networks, Systems)
- Deter (Cyber Crime, Terrorist Use of Internet)
- Develop (Capabilities)

DevSecOps enables Secure Delivery



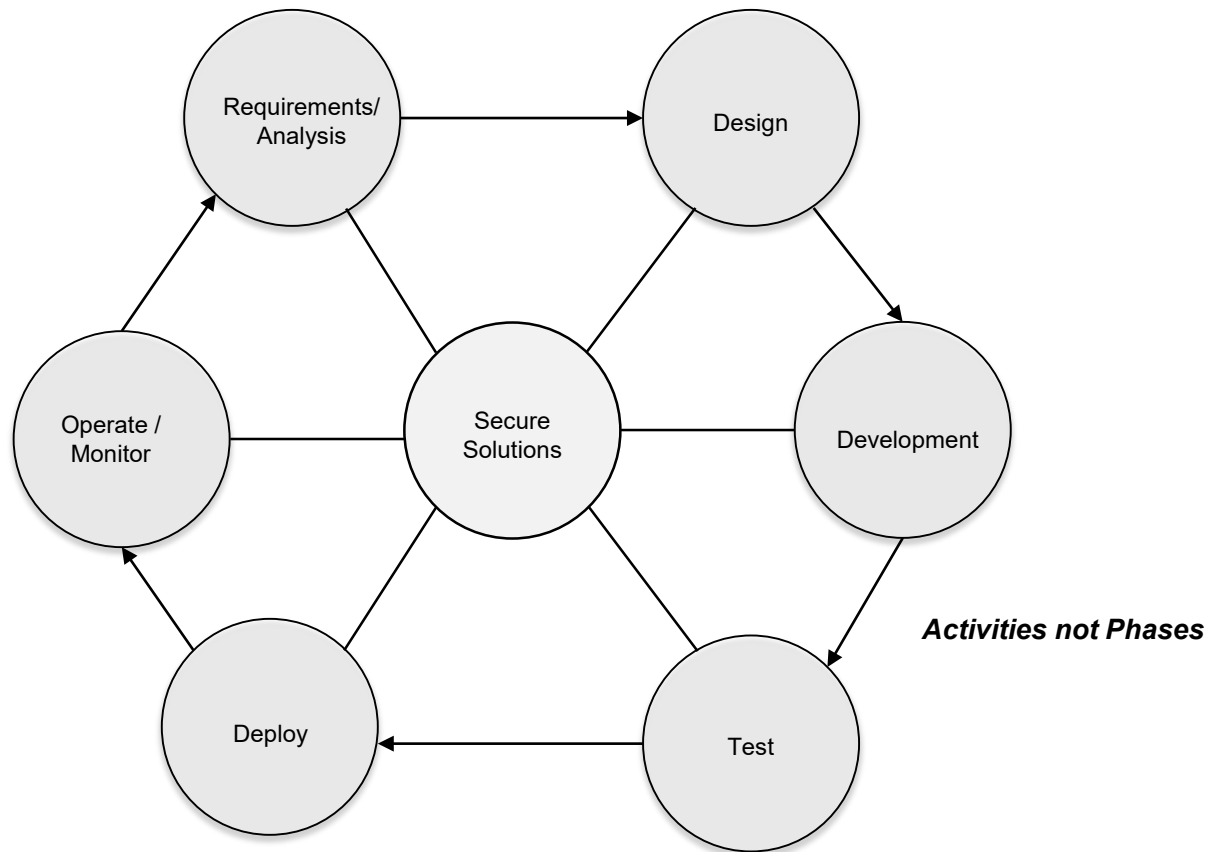
Waterfall vs Agile Lifecycle



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

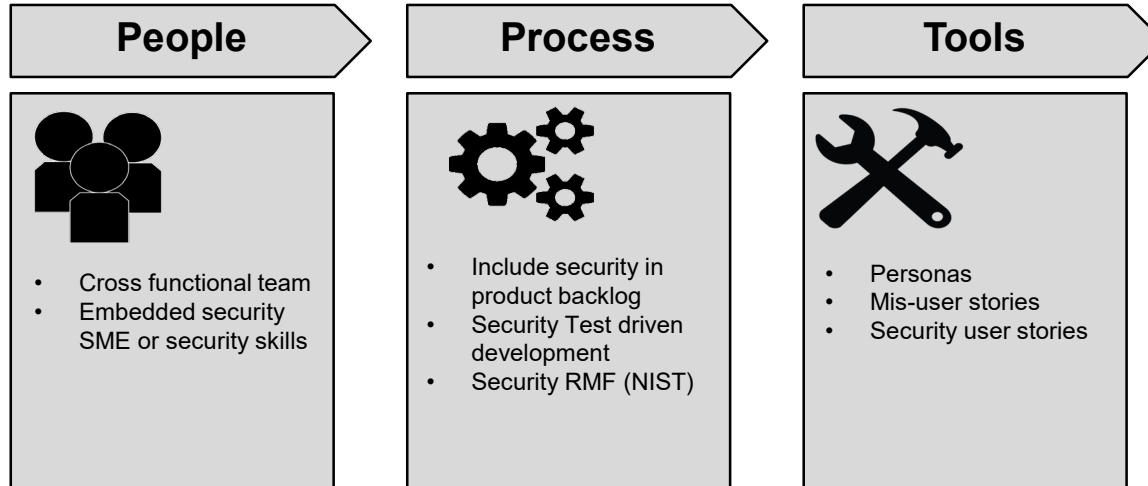


Secure Solutions through Agile



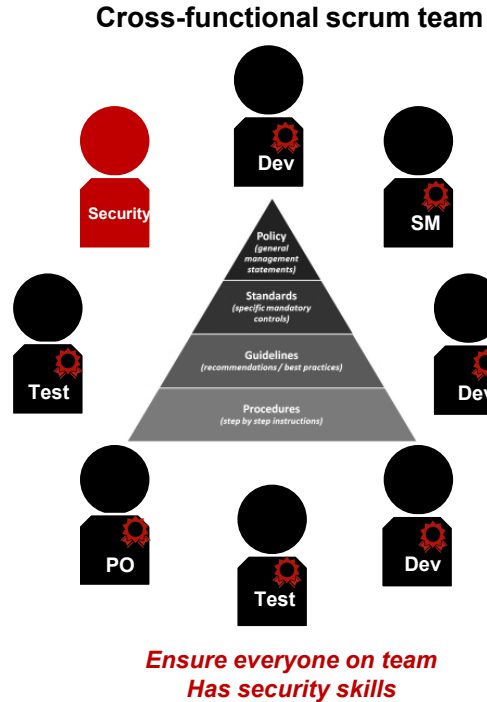


Requirements / Analysis



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

Secure Requirements/Analysis



Personas

Harry Hacker

Skills:

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

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

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

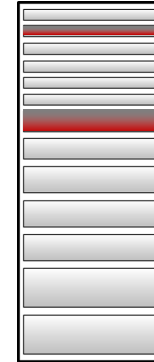
Normal Story

*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.*

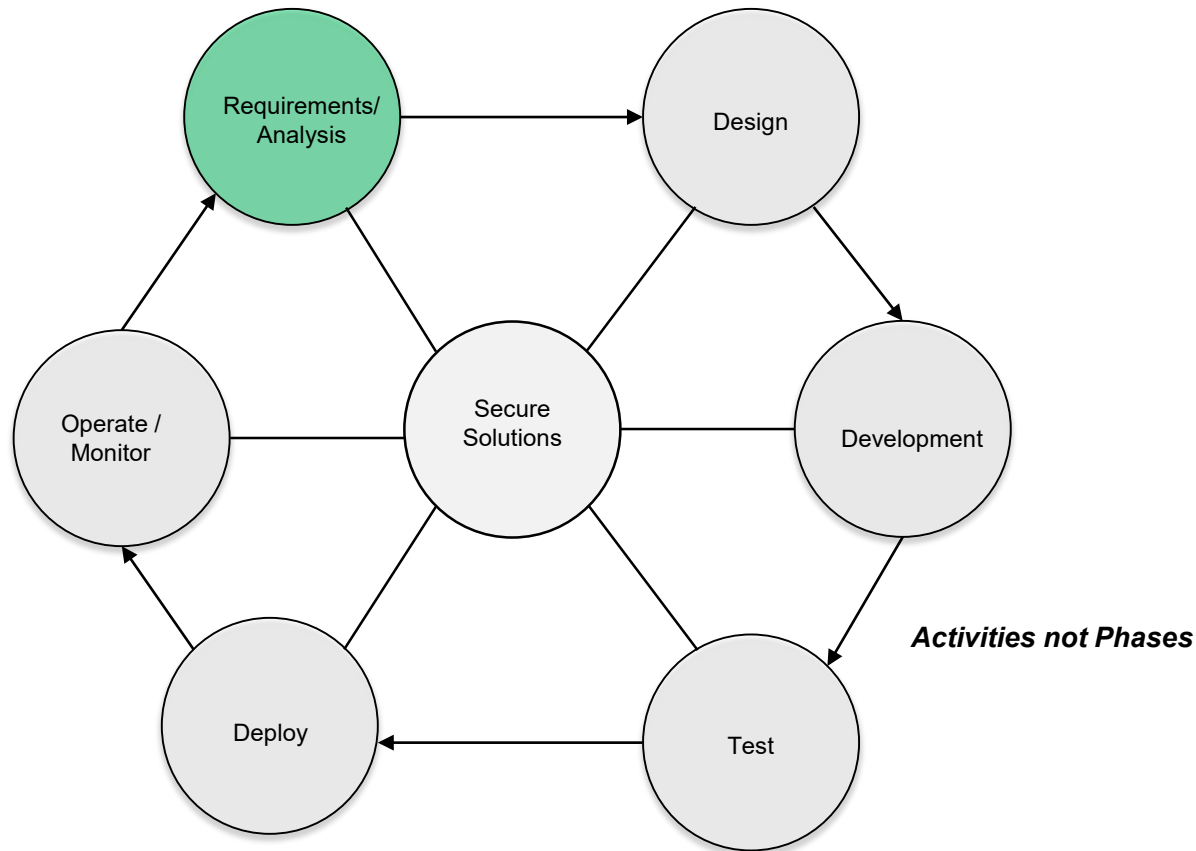
Enabler Story

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

Product Backlog

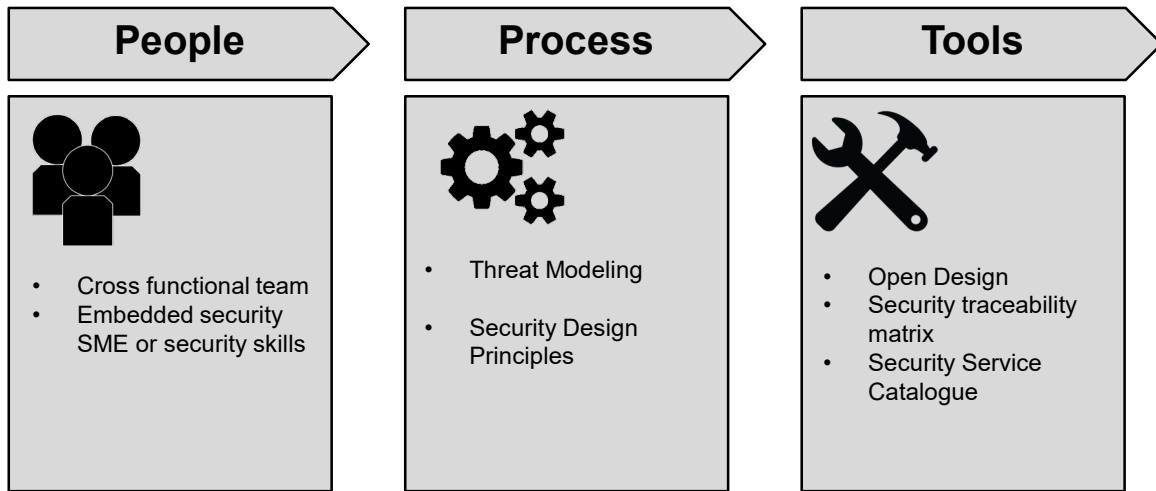


Secure Solutions through DevSecOps





Design

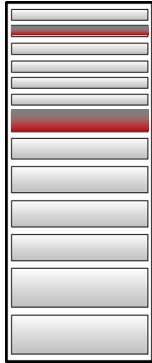


Security by design moves team focus to vulnerability prevention from vulnerability detection



Secure Design

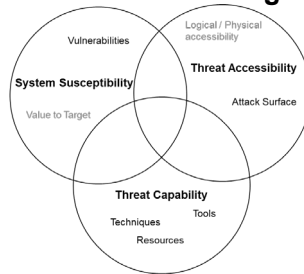
Product Backlog



Security Design Principles

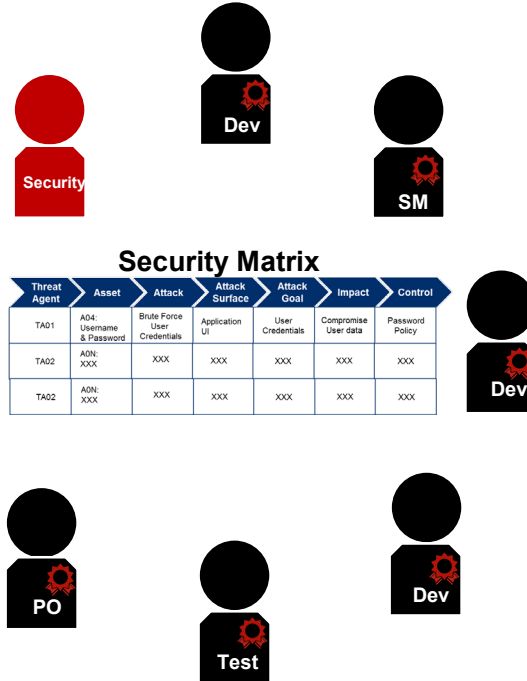


Threat Modeling

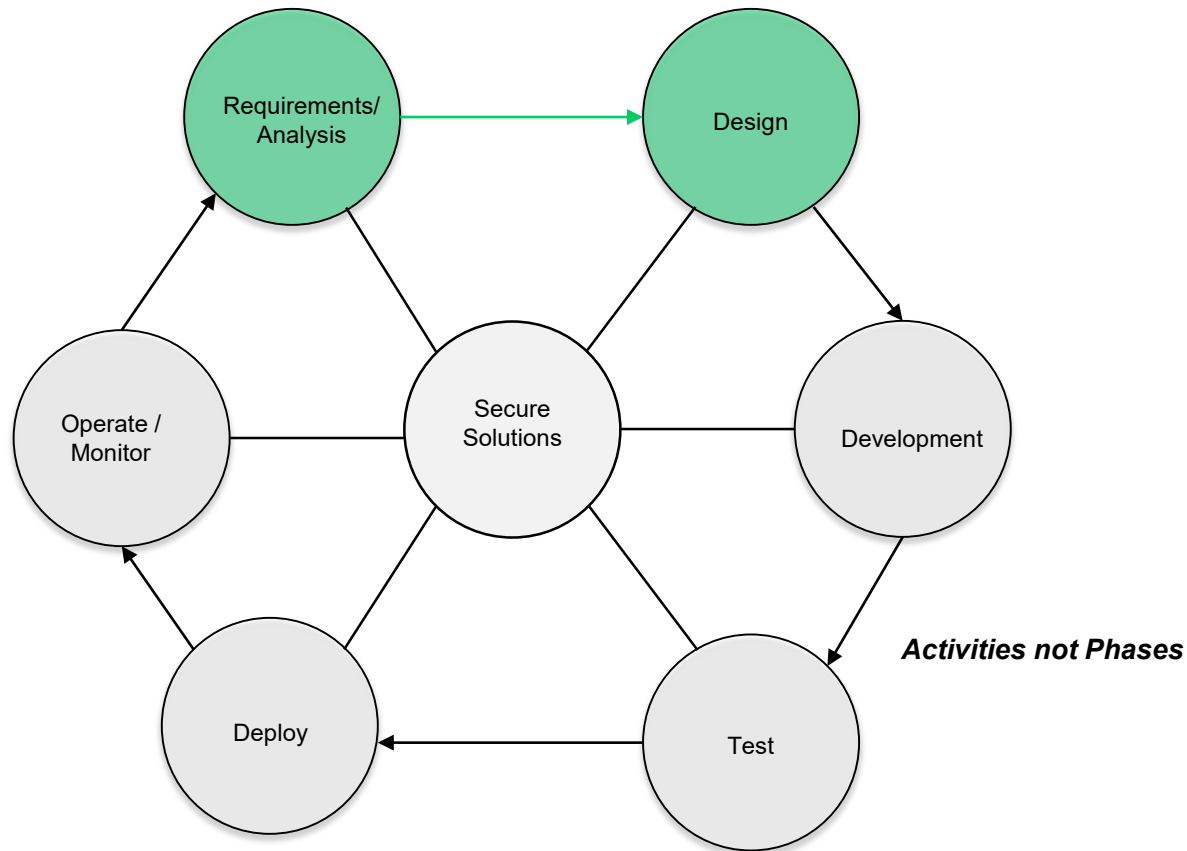


Security Matrix

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

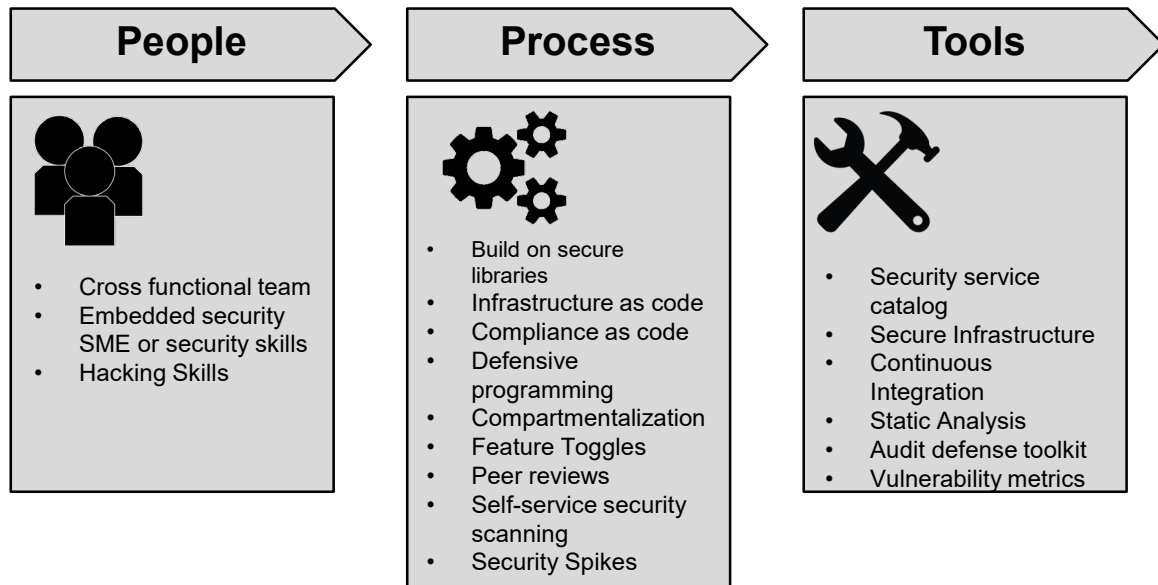


Secure Solutions through DevSecOps



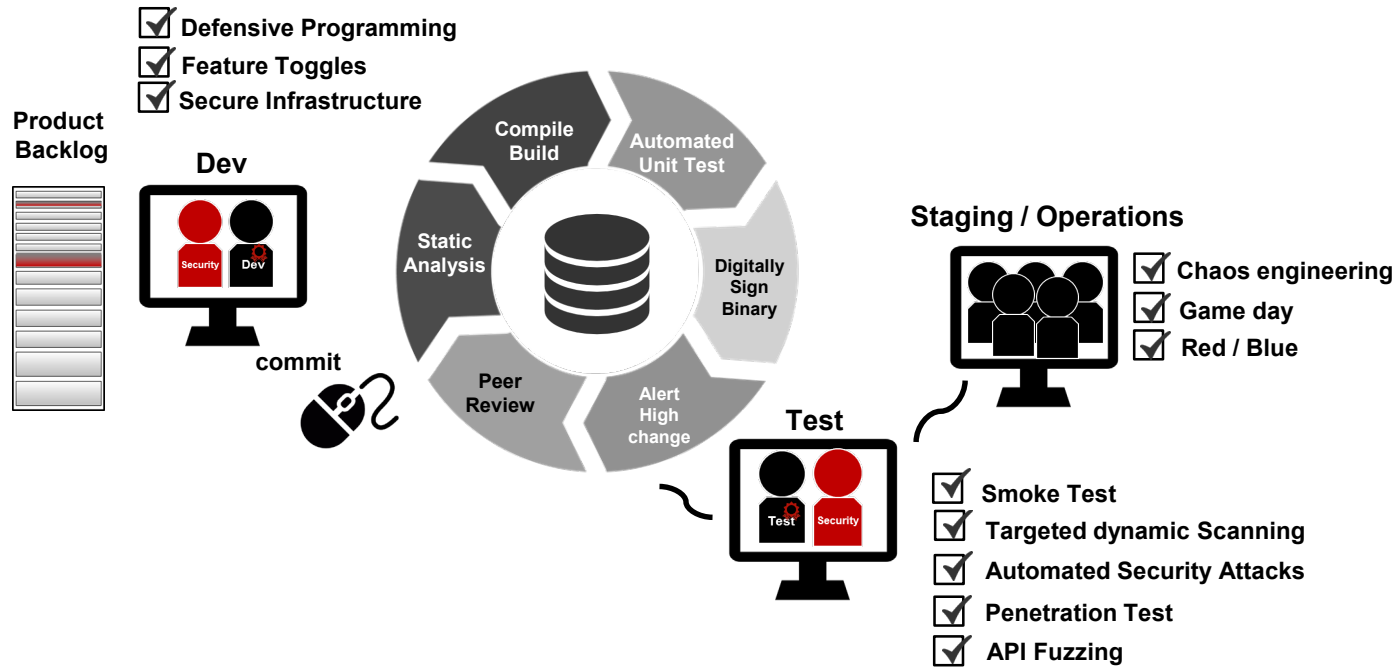


Development

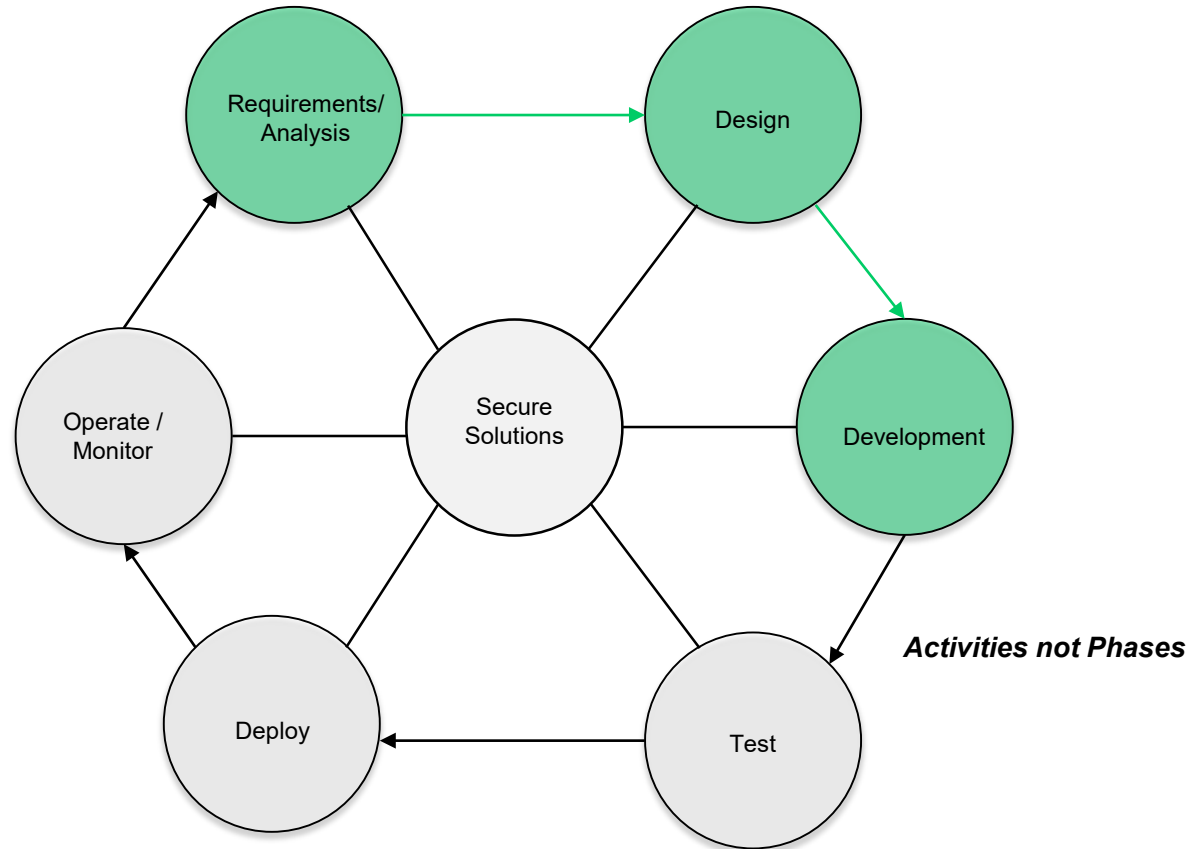


Moving from control gates to guardrails with automation and workflows

Secure Development Pipeline

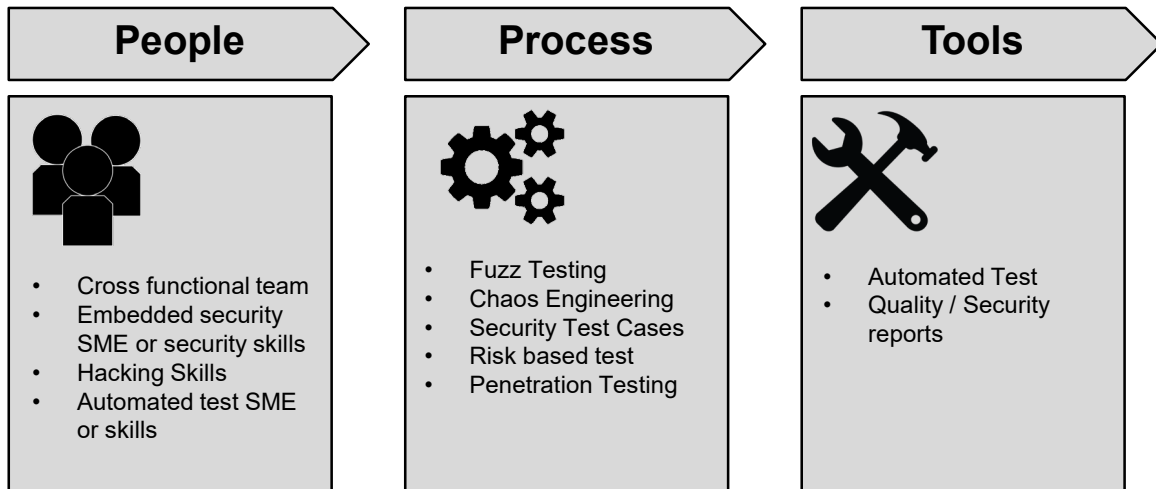


Secure Solutions through DevSecOps





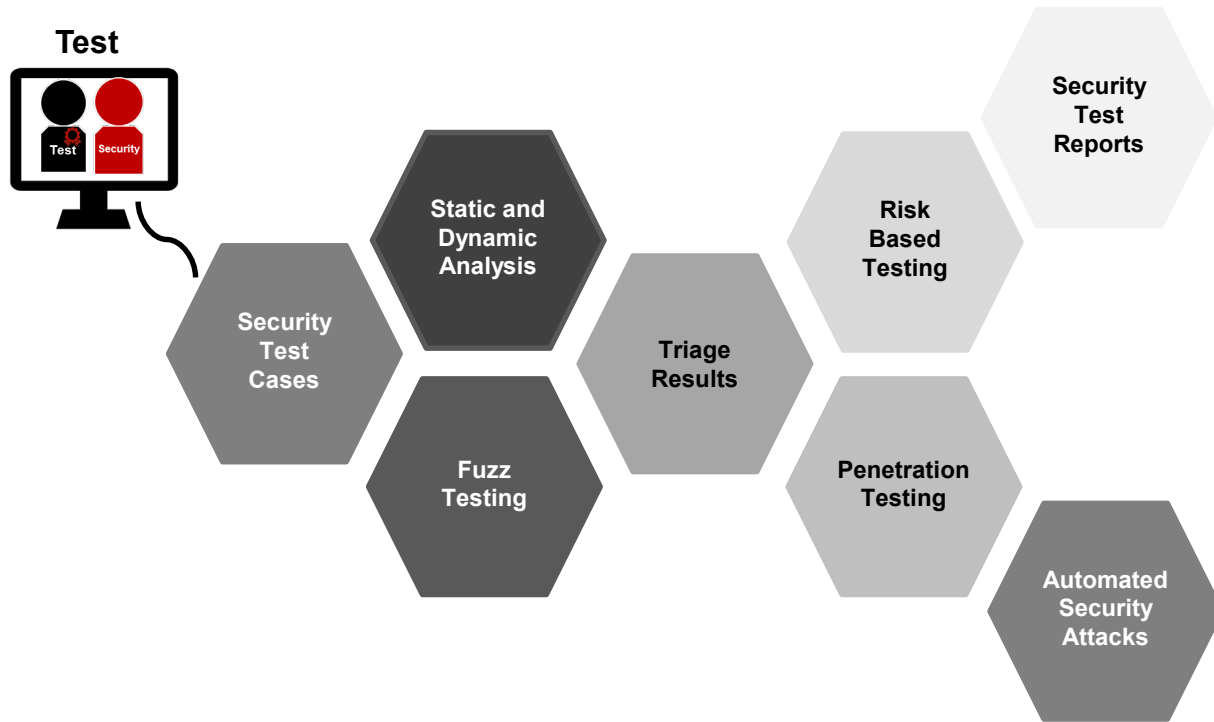
Testing



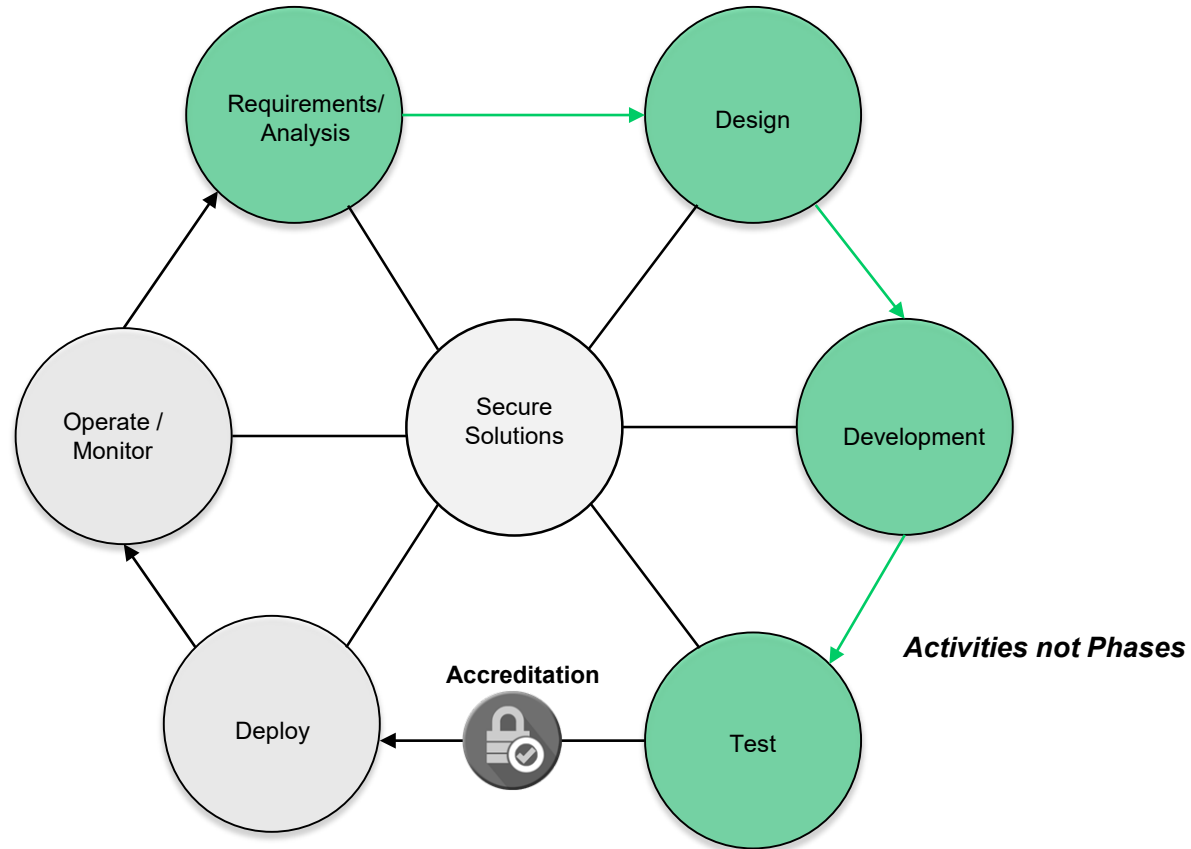
Layered Security test levels reduces flaws in the systems we deliver



Security Testing

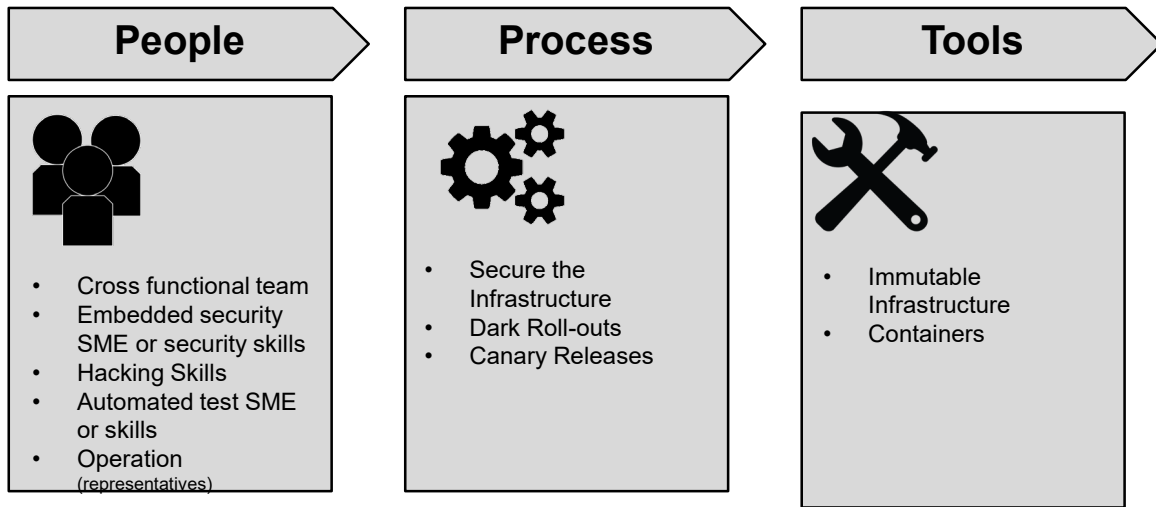


Secure Solutions through DevSecOps





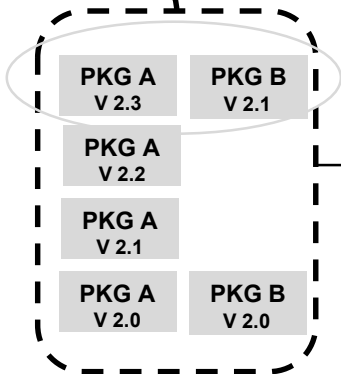
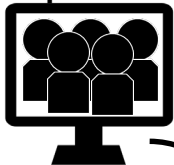
Deploy



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

Secure deployments

Staging /
Operations

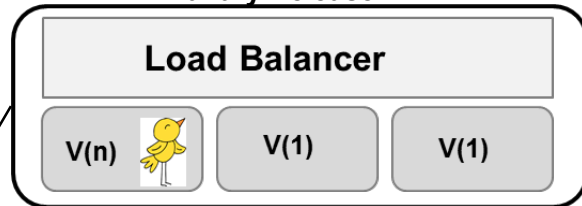


Central Package
Repository

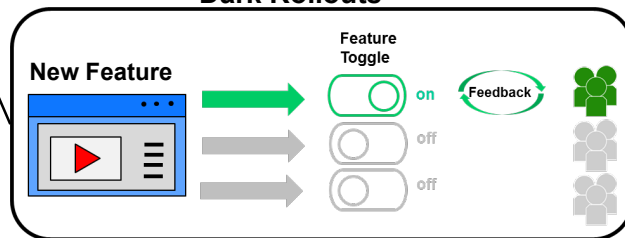
Immutable
Infrastructure



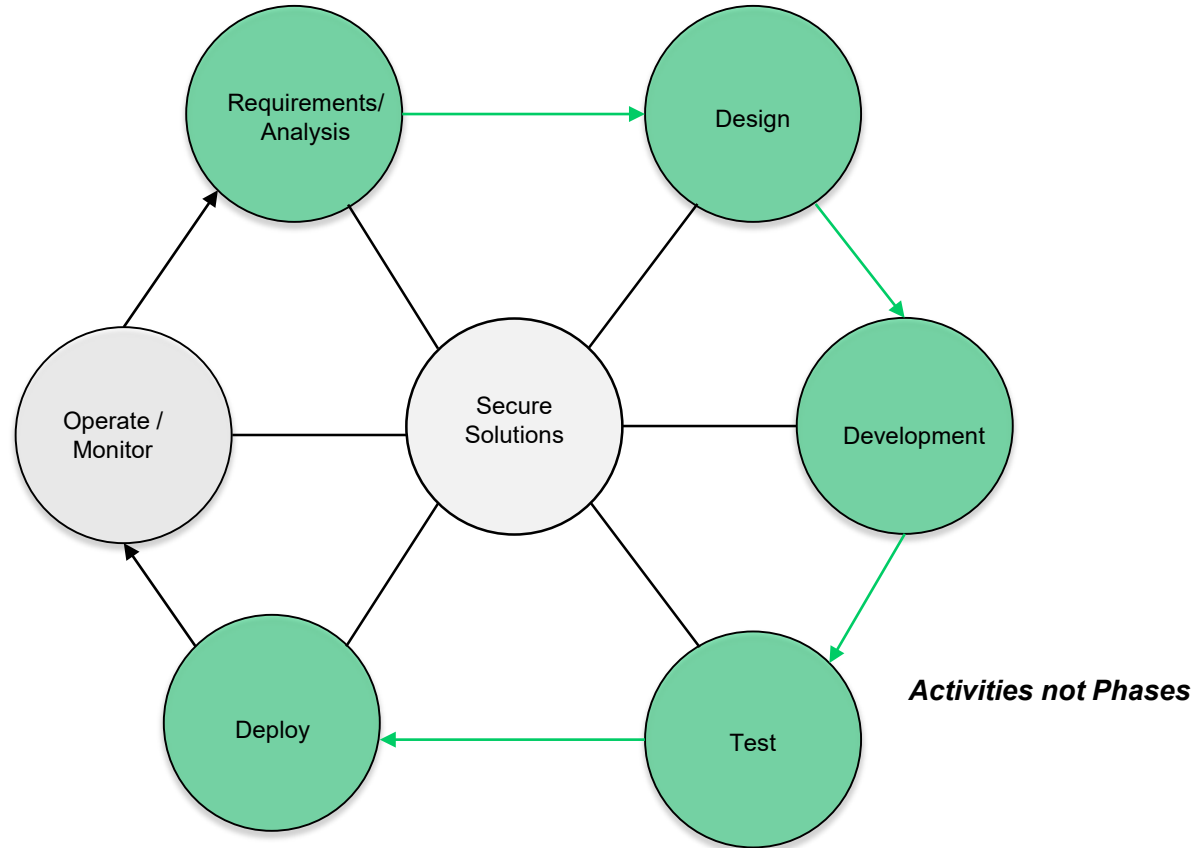
Canary Release



Dark Rollouts

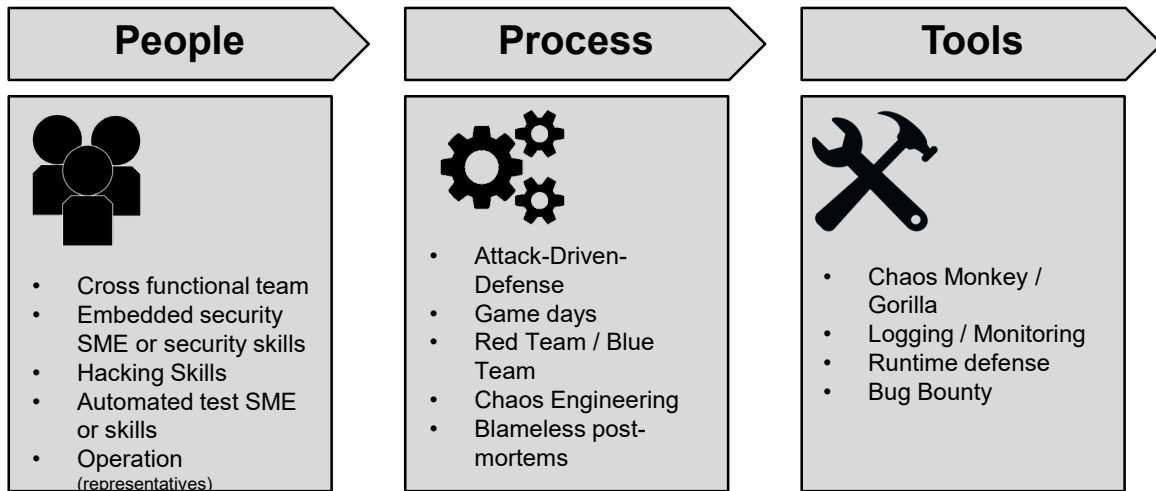


Secure Solutions through DevSecOps



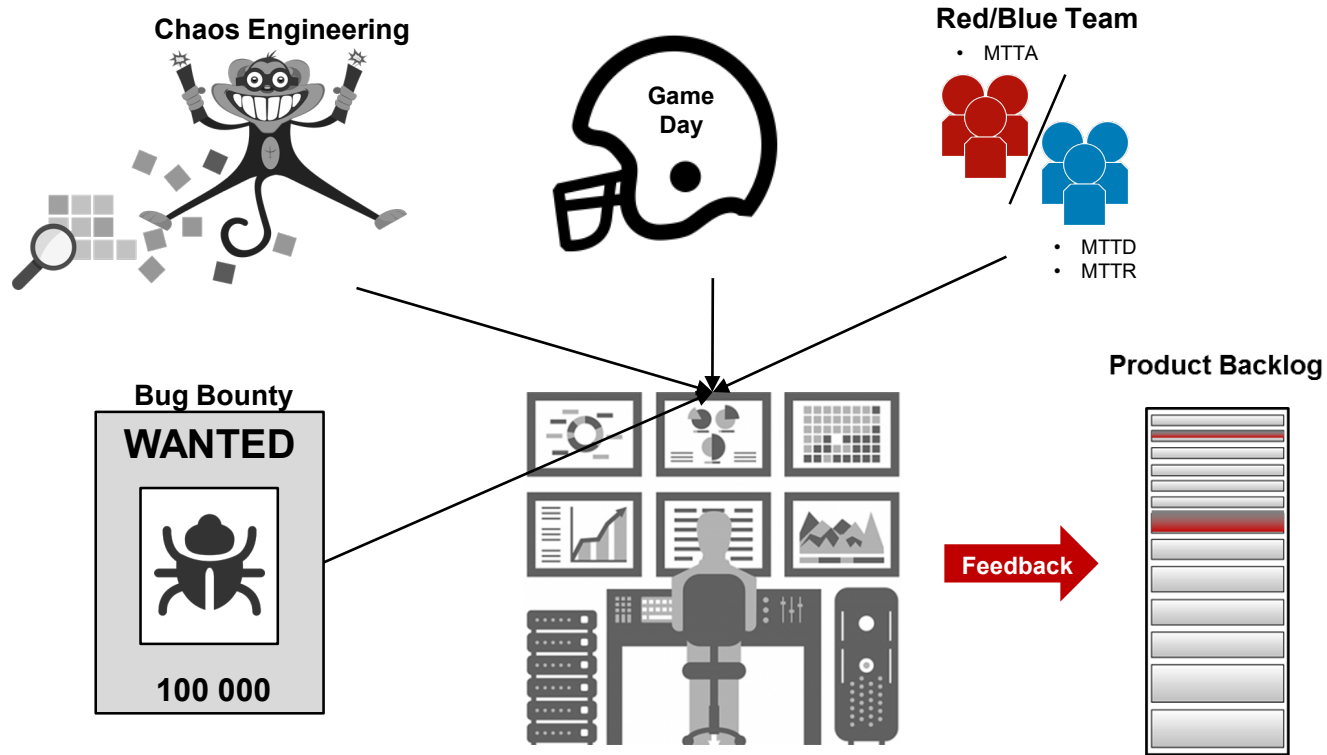


Operate and Monitor

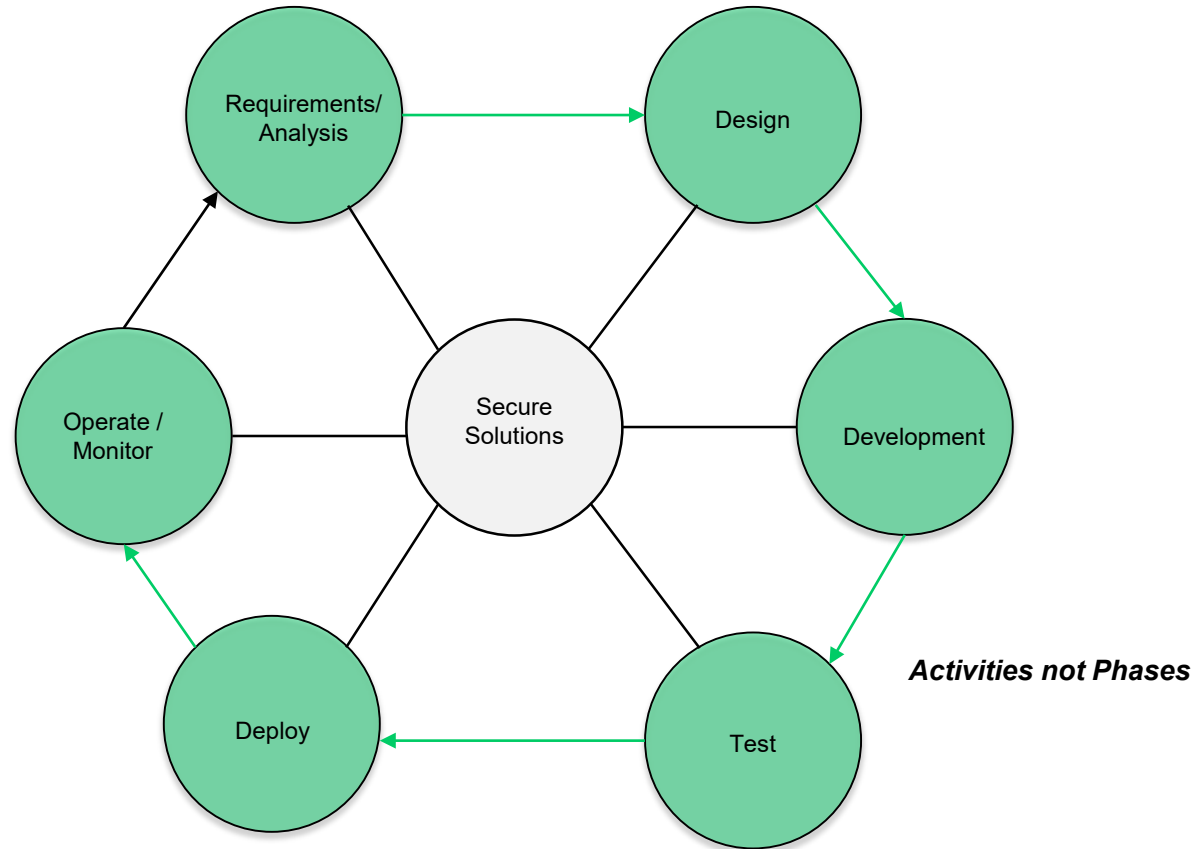


Embracing a culture of continuous improvement results in secure systems

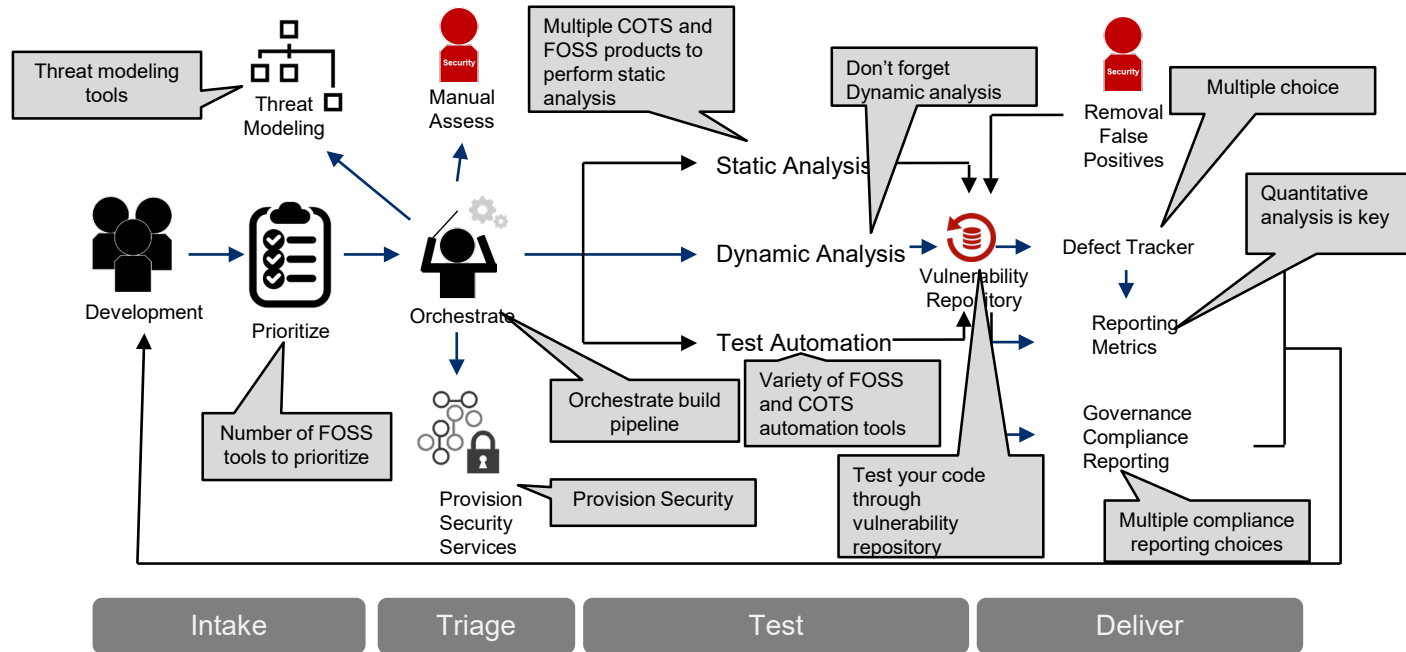
Secure Operations



Secure Solutions through DevSecOps



Automated Security Pipeline





Future

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

