

How to use hacker persona's to successfully build DevSecOps Pipeline

PITTSBURGH
8 July 2020

OLD
FAN
UN
DAYS

● Robin Yeman
● Lockheed Martin Sr. Fellow
● Lockheed Martin
● twitter @robinyeman

Agenda

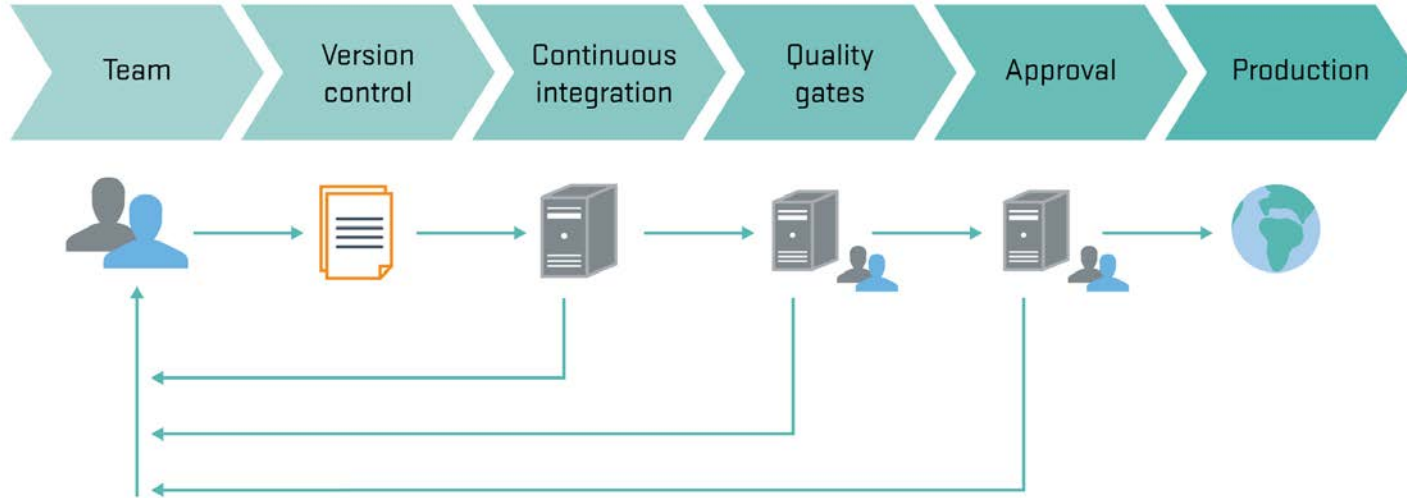
- DevOps and Pipeline
- Securing the pipeline
- Apply the practices

DevOps and delivery pipeline

DevOps

DevOps is “a cross-disciplinary community of practice dedicated to the study of building, evolving and operating rapidly-changing resilient systems at scale.”

- [Jez Humble](#)



Why DevOps

ELITE PERFORMERS

Comparing the elite group against the low performers, we find that elite performers have...



208
TIMES MORE

frequent code deployments



106
TIMES FASTER

lead time from
commit to deploy



2,604
TIMES FASTER

time to recover from incidents



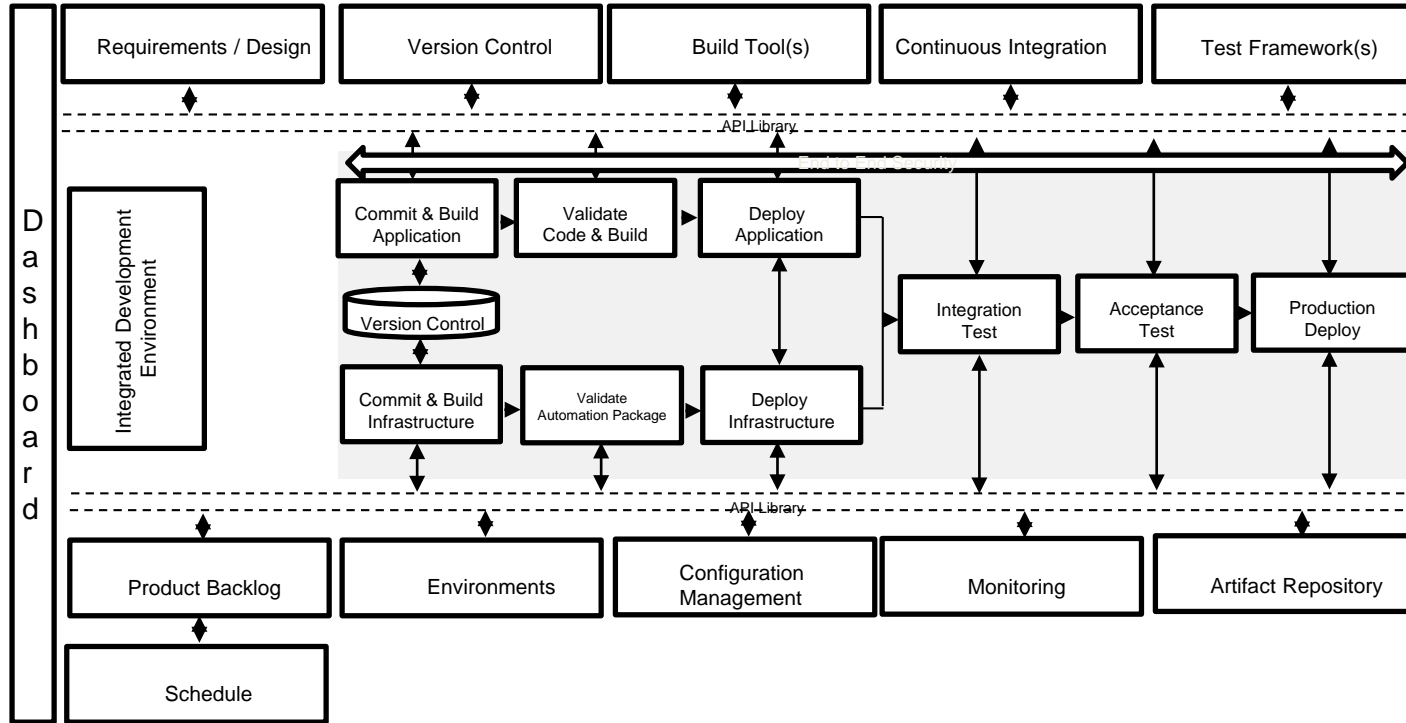
7
TIMES LOWER

change failure rate
(changes are 7x as likely to fail)

Throughput Stability

Forsgren, Nicole. "DevOps Solutions | Google Cloud." *Google*, Google, 22 Aug. 2019, <https://cloud.google.com/devops/state-of-devops/>.

DevOps Pipeline



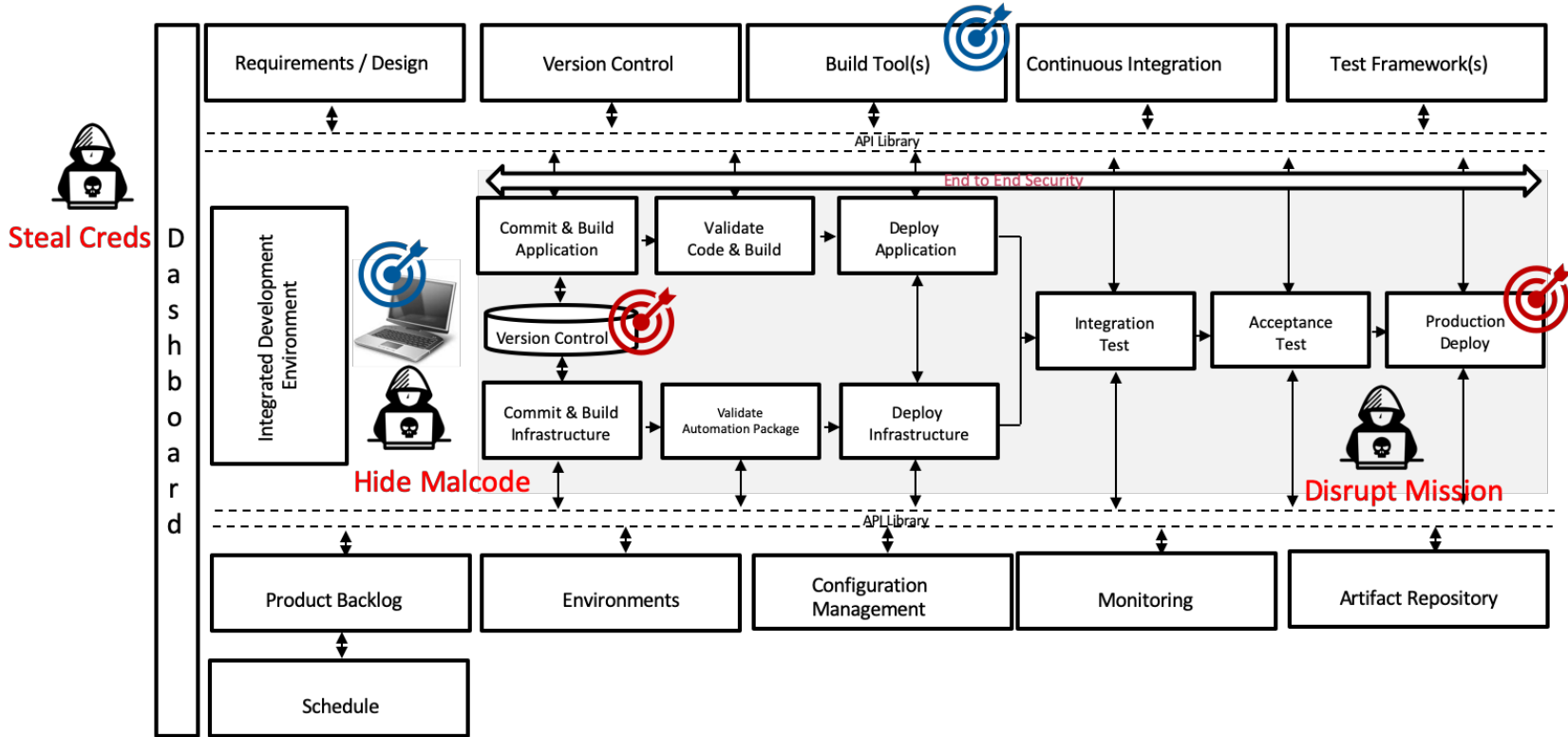
Securing the delivery pipeline

Threat Modeling

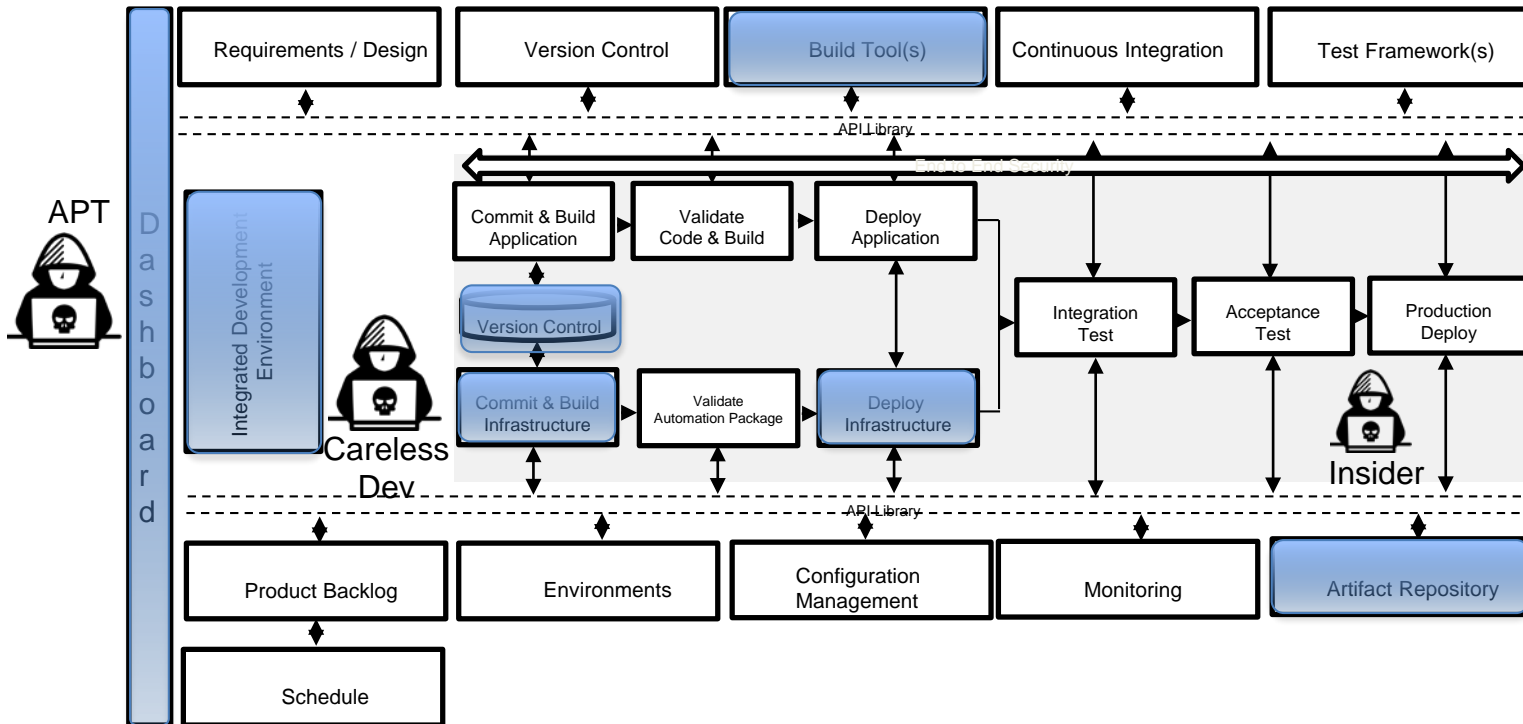
- Using IDDIL-ATC Methodology
 - Gain understanding
 - Assess risk
 - Justify security controls
- Identify Assets
- Define the Attack Surface
- Decompose the System
- Identify Attack Vectors
- List Threat Actors
- Analysis & Assessment
- Triage
- Controls



DevOps Pipeline Threat Model




Attack Surfaces in the pipeline



Defining Persona's

- Alan Cooper's the *Inmates are Running the Asylum*
 - Hypothetical Archetypes
 - Precise & Specific Description of the User
 - Define user's objectives
- Lene Nielson's 4 Perspectives
 - Goal Directed
 - Role-based
 - Engaging
 - Fictional

Marty Malicious Developer	
	Skill set: Extensive coding experience at OS & Kernel level. Develops cyber attack tools. Wants to get paid by his employer as well as his dark web associates.
Identification:	
Real Name: Martin Smith Handles: KRNLKON	
Motivations:	
<ul style="list-style-type: none">➢ Appear aboveboard and ethical (follows rules)➢ Ensure nobody notices I am injecting malicious logic➢ Take full advantage of weak process to remain undetected	
Frustrations:	
<ul style="list-style-type: none">➢ Security controls that limit, block or monitor code changes➢ Inline automated security tools that detect malicious code➢ Automated / manual testing that dis cover malicious code	

Why Hacker Personas?

- Culture & Awareness. Understand adversary tactics & drivers
- Prioritize security risks
- Communicate generalized attacker profiles that identify common black hat hacker motives and desires
 - What does the attacker like to see – identifies exploitable weaknesses
- Justify Security Control Selection
 - What does the attacker not like to see – identifies effective security controls

How do we “discover” hacker personas?

Threat Types (analogous to User Roles)

- Advanced Attackers (APTs, Military, Industrial)
 - Comment Crew, Lazarus Group, Oilrig
- Hacktivists
 - Anonymous, Chaos Computer Club, LulzSec, OurMine
- Insider
 - Spy, Compromised employee, disgruntled employee
- Lone Wolf
 - Iceman, Robert Morris, Julian Assange, Edward Snowden

Sources: [anonymous](#), [attack.mitre.org](#), [apt.threattracking.com](#)

Intelligence Sources

Near Range Threats:

- Internal Intelligence
- Partner Intelligence

Mid Range Threats:

- Open Source Intelligence (OSINT)
- Industry Intelligence

Long Range Threats:

- Homeland Intelligence
- Ally Intelligence



FBI cyber most wanted



Ministry of State Security (MSS)

People's Liberation Army (PLA)

Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU)

JSSD



Zhang Zhang-Gui
Zha Rong
Chai Meng

CVNX (APT10)



ZHU HUA

ZHANG SHILONG

2PLA



Su Bin

VMTHR (APT3)



Wu Yingzhuo
Dong Hao
Xia Lei

APT1



Huang Zhenyu

Wen Xinyu

Sun Kaifang



Gu Chunhui



Wang Dong

RUSSIAN INTERFERENCE IN 2016 U.S. ELECTIONS



Boris Aleksyevich Antonov

Dmitry Sergeevich Badin

Anatoly Sergeevich Kovalev

Nikolay Yuryevich Kozachuk

Aleksyey Viktorovich Lukashchik

Artem Andreyevich Nalchayev



Sergey Aleksandrovich Morgachev



Aleksandr Vladimirovich Ovaschuk



Aleksey Aleksandrovich Potemkin



Ivan Sergeevich Yermakov



Pavel Vyacheslavovich Yershov

DPRK



Park Jin Hyok

IRANIAN DDoS



Ahmad Fathi

Hamid Firoozi

Amin Shokohi



Mohammad Sadeq Ahmadradeqan



Omid Ghaffarina




Sina Keissar

Public name: Lazarus Group

Hacker Persona Examples

Careless Developer


Chuck Careless Developer	
	Skillset: <i>Degree in computer science with less than five years experience. Explores the latest technology at home with the ability to code in multiple languages</i>
Identification:	
Real Name: Charles Diavol Alias: Charles 123	
Motivations:	
<ul style="list-style-type: none">➤ Wants to maximize delivery of software➤ Wants access to use the latest tech and libraries➤ Reduce workload of perceived overhead work	
Frustrations:	
<ul style="list-style-type: none">➤ Governance and compliance that slows him down➤ Ever-growing technical debt➤ Legacy technology	

As a Developer I want check-in features quickly so that I can go move on to something else.

As a Developer I want avoid administrative work so that I can code which is more fun!

As a Developer I want try the latest technology available so that I can keep my skills current.

Malicious Developer


Marty Malicious Developer	
	Skillset: <i>Extensive coding experience at OS & Kernel level. Develops cyber attack tools. Wants to get paid by his employer as well as his dark web associates.</i>
Identification:	
Real Name: Martin Smith Handles: KRNL KON	
Motivations:	
<ul style="list-style-type: none">➤ Appear aboveboard and ethical (follows rules)➤ Ensure nobody notices I am injecting malicious logic➤ Take full advantage of weak process to remain undetected	
Frustrations:	
<ul style="list-style-type: none">➤ Security controls that limit, block or monitor code changes➤ Inline automated security tools that detect malicious code➤ Automated / manual testing that discover malicious code	

As a Malicious Developer I want inject malicious code so that I can see what happens.

As a Malicious Developer I want increasing privilege so that I can view data that has not been shared with me.

As a Malicious Developer I want crash the server so that I can deny service to my co-workers.

Advanced Persistent Threat (APT)

Annie APT	
	Skillset: <i>Highly trained and skilled in cyber attacks of all kinds. Effective social engineer. Skilled at evading detection.</i>
Identification:	
Real Name: Annie Alvarez Handles: Triple Pez, 3Pez, Pez	
Motivations:	
<ul style="list-style-type: none">➤ Use highly effective attacks, including social engineering➤ Gain Trust, Develop relationships through social media➤ After compromise, remain undetected to meet objectives	
Frustrations:	
<ul style="list-style-type: none">➤ When I exploit a target without enough privilege to move forward with my objectives➤ Security controls that block outbound communication	

As a Annie APT I want to eavesdrop on company X and obtain sensitive information that can be sold.

As a Annie APT I want to upload malware on your computer so that I can obtain personal information.

As a Annie APT I want to upload ransomware so that I can extort victims to further my political agenda.

Application and Benefits

USING PERSONAS



Annie

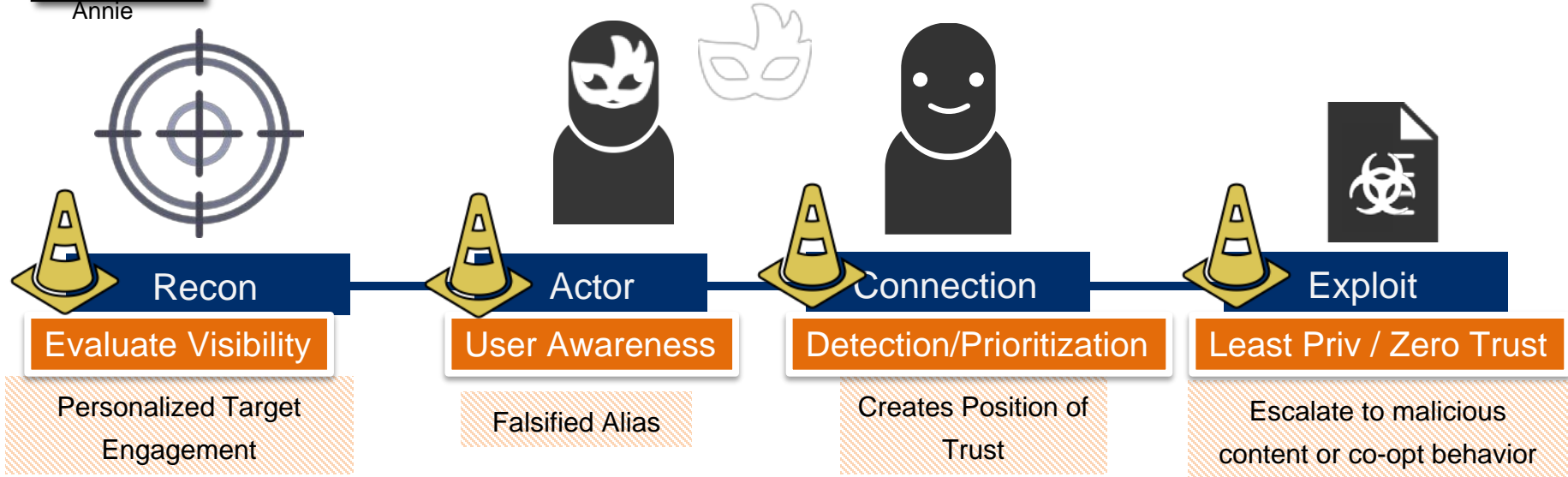
Is Annie capable?

What does Annie want?

What frustrates Annie?

How does Annie benefit?

How do I stop Annie?

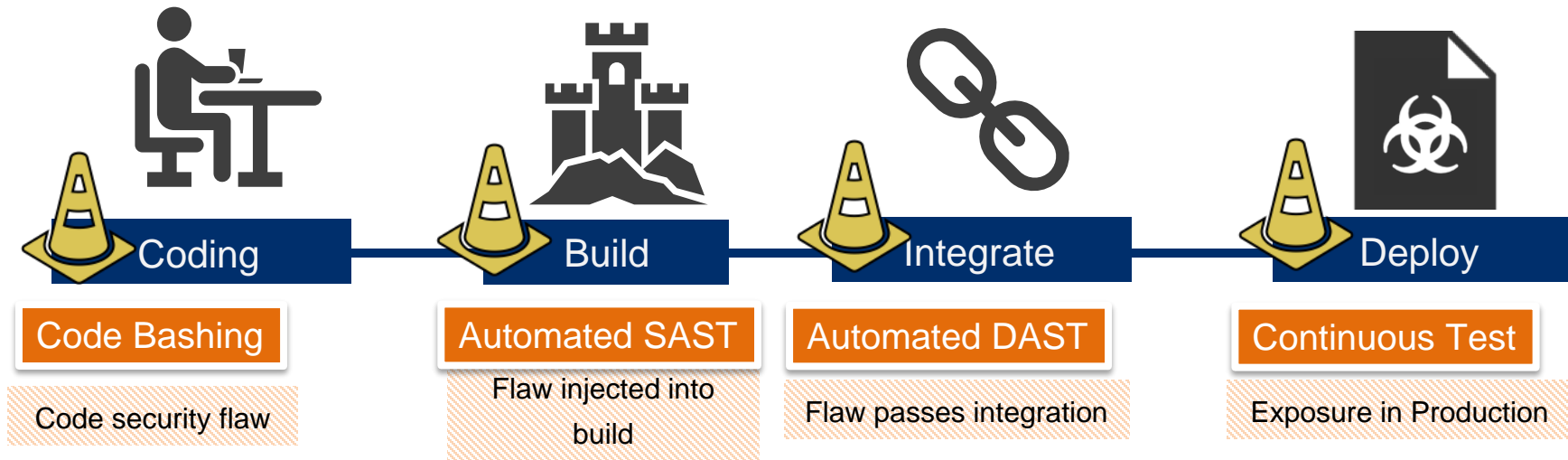


Hacker Persona Benefits

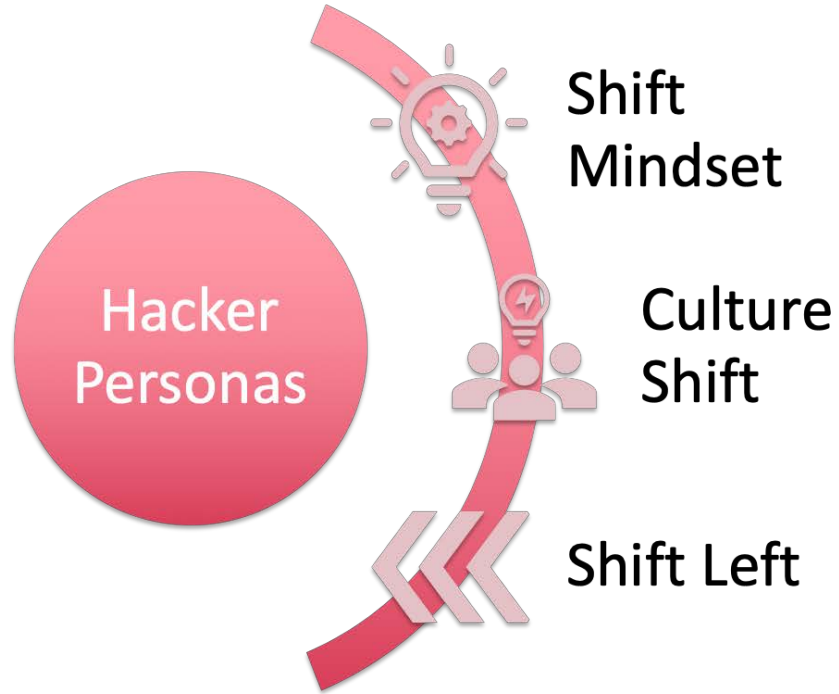


Chuck

“Spatial” (visual) Understanding
Identify effective countermeasures
Prioritize defenses
Measure effectiveness



Positive Shifts



“Lessons” on Personas

- Change culture “Put on the Black Hoodie”
- Build and Socialize Personas
- Agile Security Game – Shostack
- The Phantom Hacker

Future

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

