

Introduction to DevSecOps

Quintessence Anx

Quintessence Anx

Developer Advocate, PagerDuty





Mandi Walls

Developer Advocate,
PagerDuty



Nasim

Yazdani

Program Manager,
PagerDuty

Getting Started

If you have not already joined, please create a community account at **community.pagerduty.com/join/pdu**

We will have a variety of sessions and workshop breakouts to test your knowledge throughout the course in our community.

Redeem points for swag!

- Introductions
- 2 Knowledge Checks
- Post-Course Survey





Doppler Team



Earn Points!

Link in Chat

Agenda

1 Introduction

2 What is DevSecOps?

3 Cultural Shifts

4 Shifting Left

5 Q&A

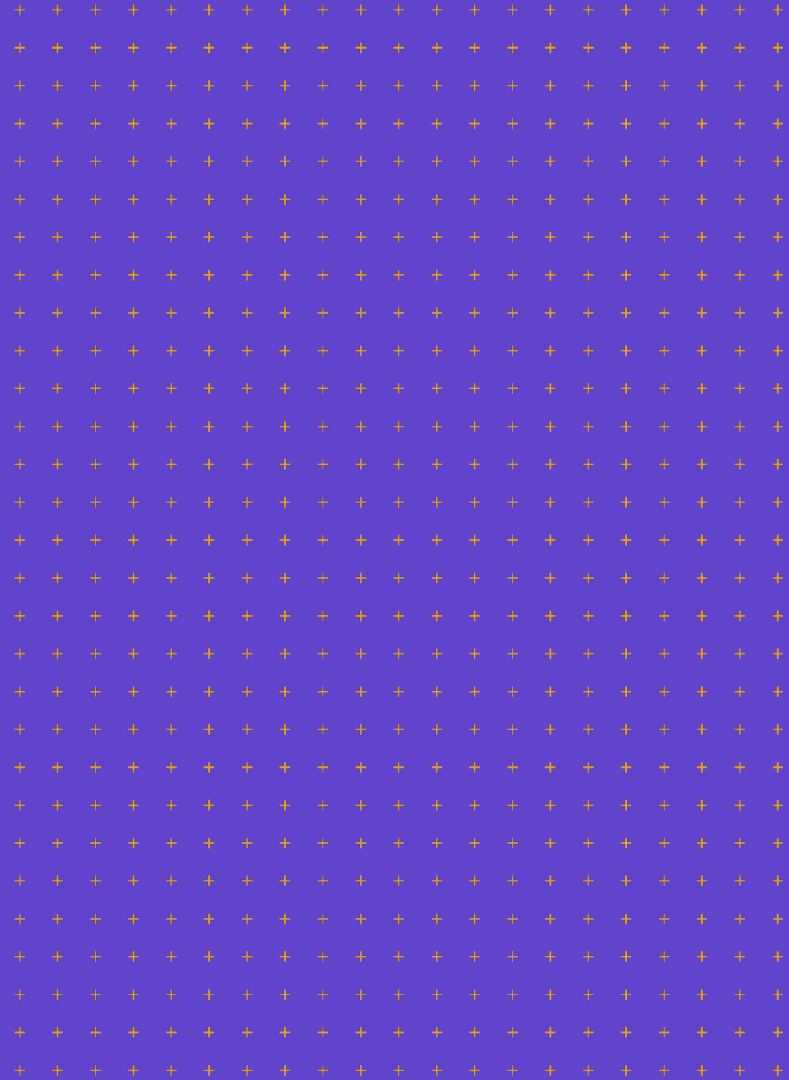




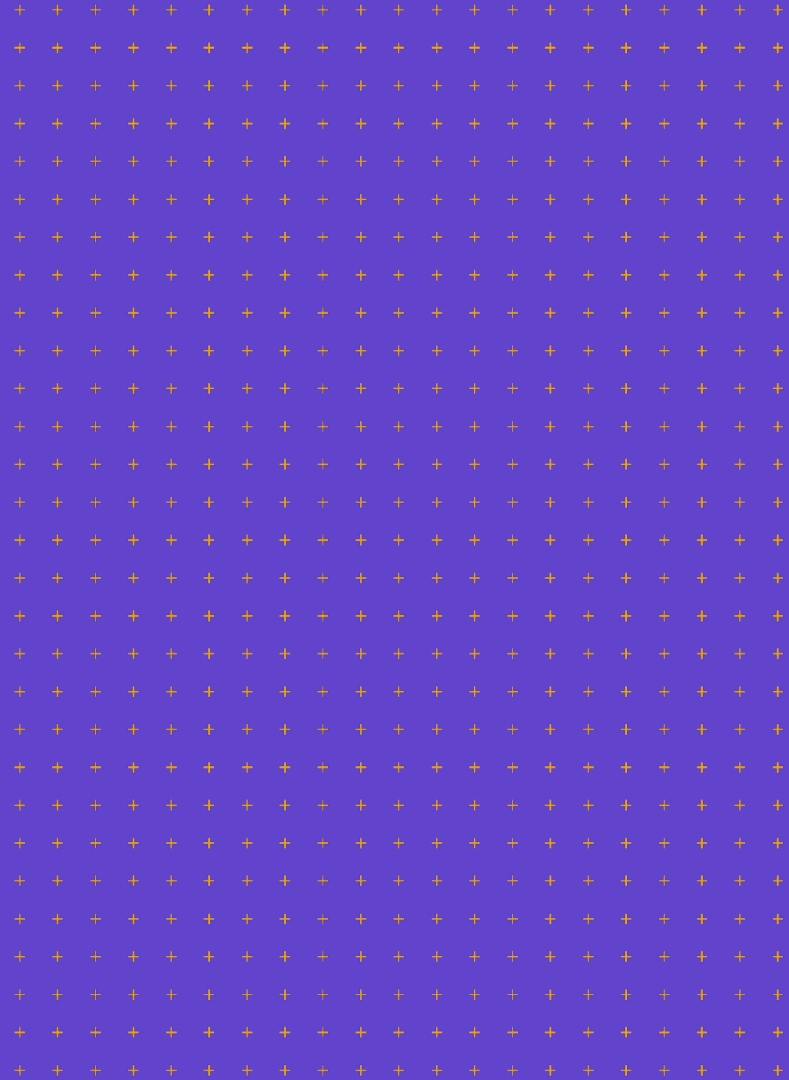
Don't Panic



This will be an
interactive
workshop, as much
as possible



I'll be doing
(some) live
questions in the
presentation.



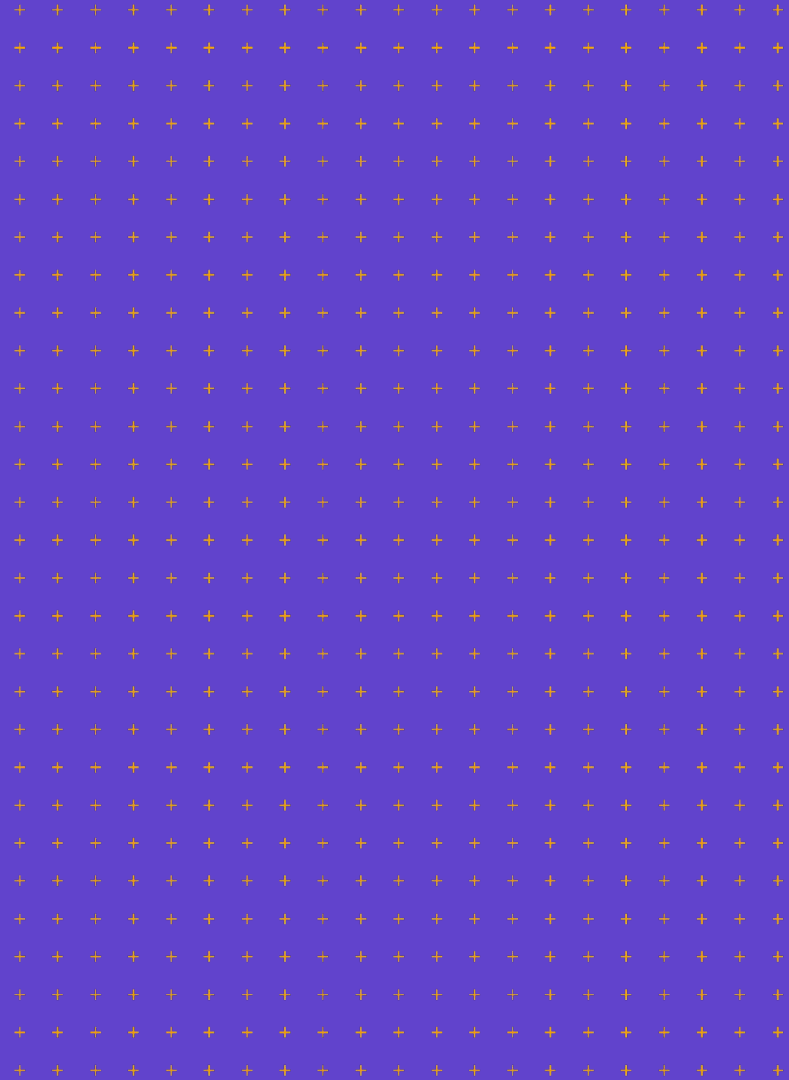


Join at
slido.com
#434 110



Questions will be via Slido

And so it
begins...



Introduction & Context Setting



Join at
slido.com
#434 110



slido

How do you feel development,
operations, and security work
together today?



Join at
slido.com

#434 110



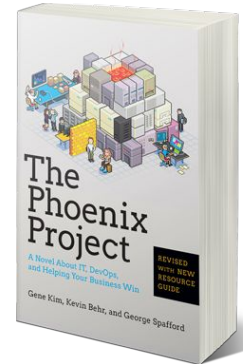
slido

Dev+Ops: how do you feel when you need to work with security?

Security: how do you feel when you need to work with dev and/or ops?



A few questions about The Phoenix Project



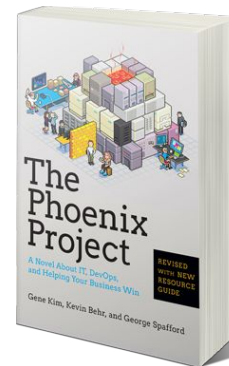


slido

Join at
slido.com
#434 110



Have you read The Phoenix
Project?



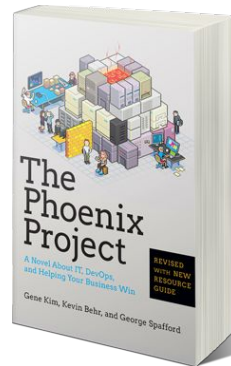


slido

Join at
slido.com
#434 110



How well do you recall the story
overall?



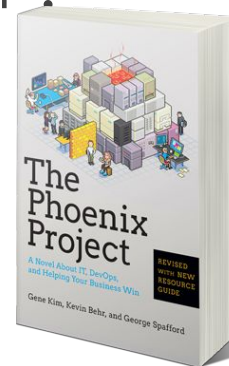


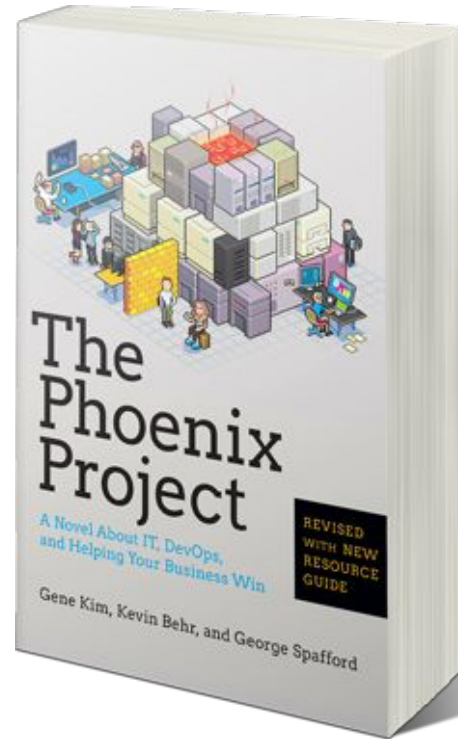
Join at
slido.com
#434 110



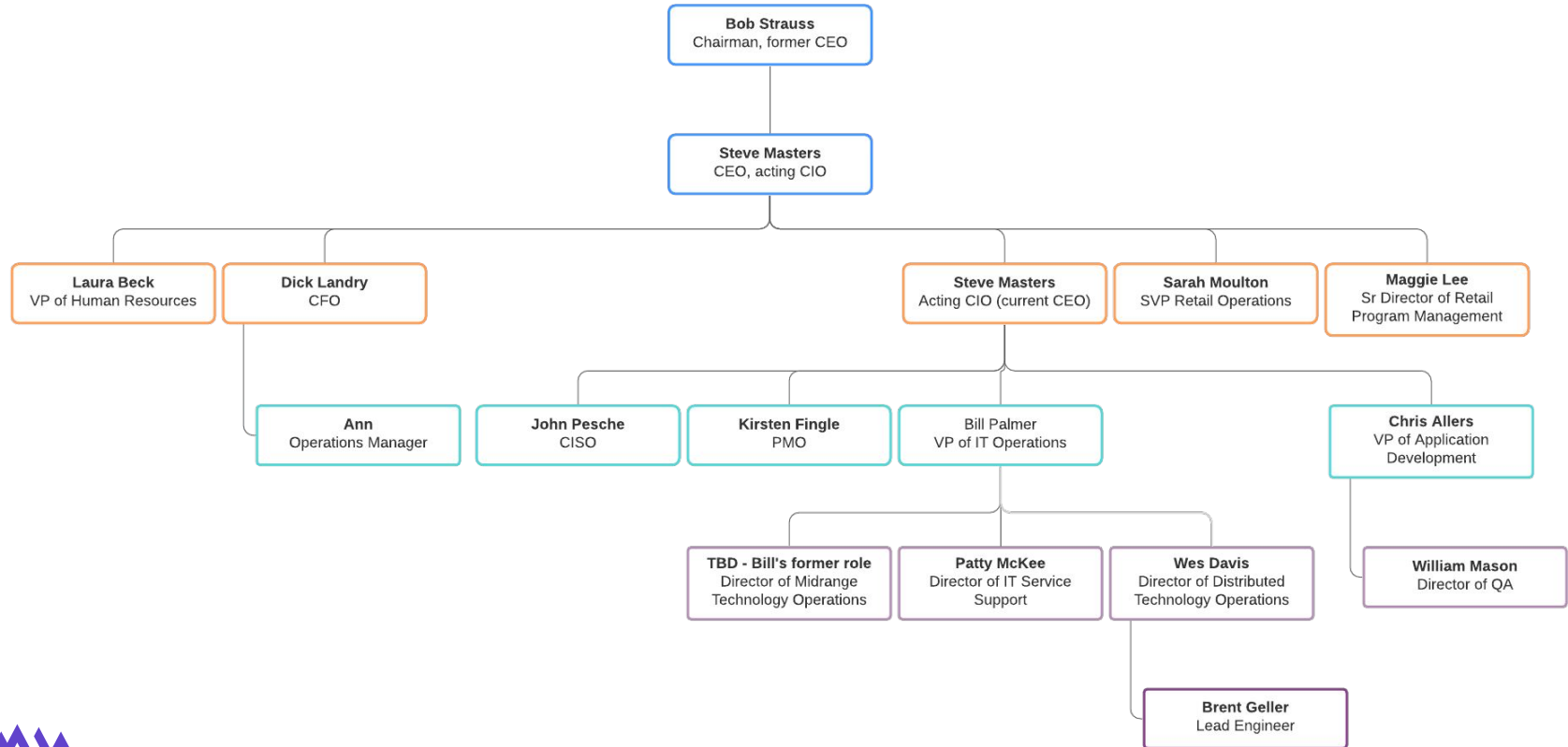
slido

Which character do you most identify with, in terms of your current role or career?

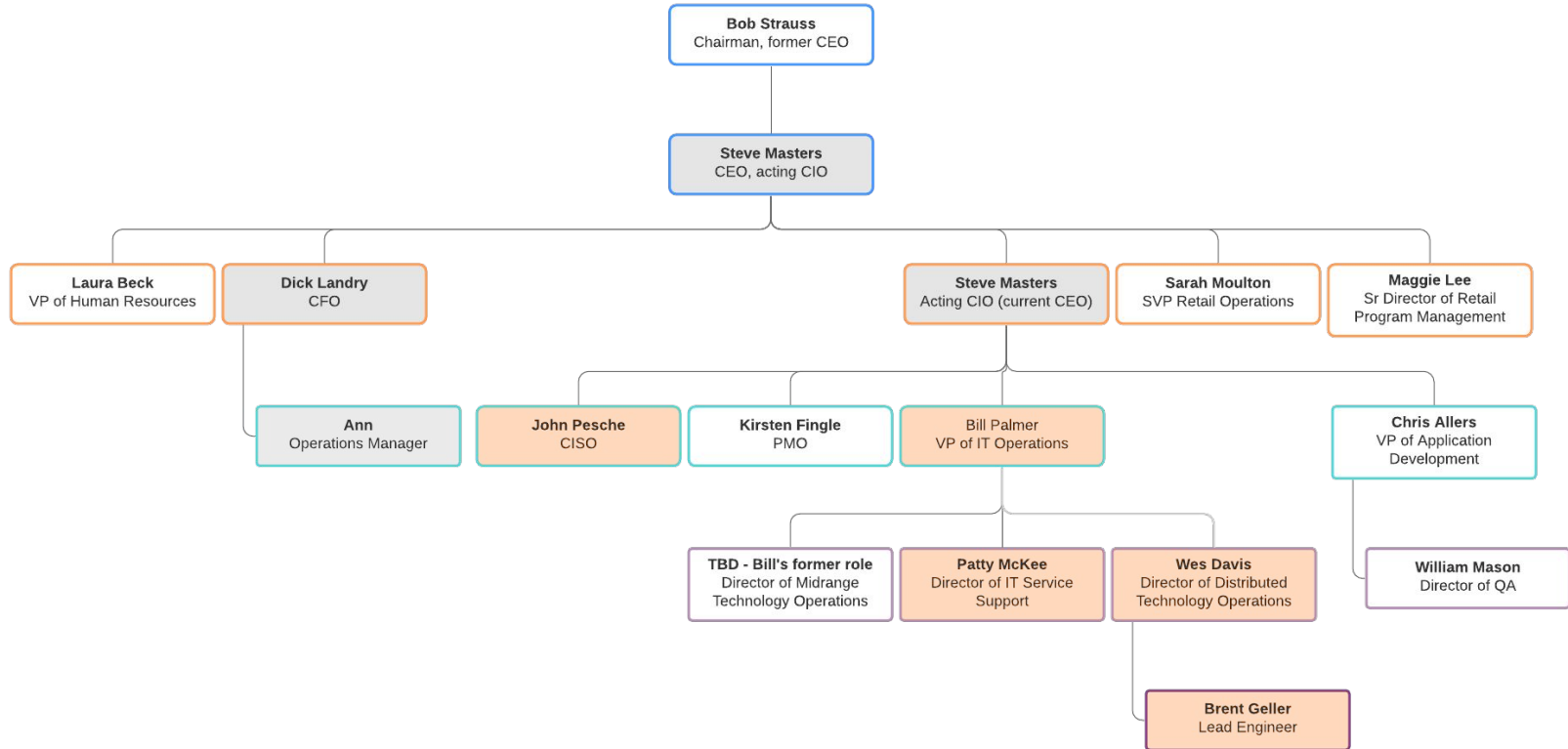




A Basic Phoenix Project Org Chart



A Basic Phoenix Project Org Chart





Let's reflect on this for a
moment

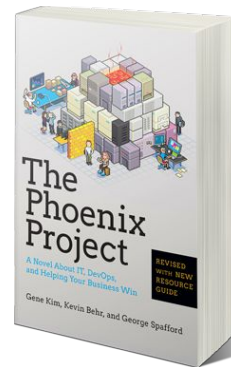


slido

Join at
slido.com
#434 110



How favorably did Bill talk about
developers?



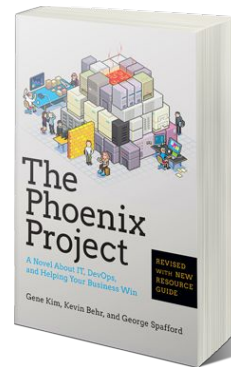


slido

Join at
slido.com
#434 110



How favorably did Bill talk about security?



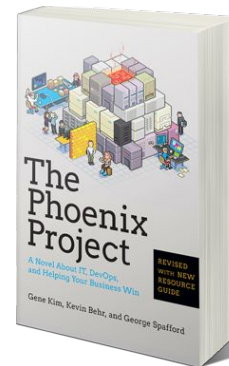


slido

Join at
slido.com
#434 110



How did you view security in this interaction?

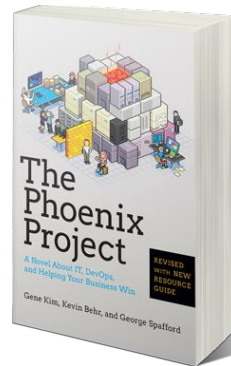




slido

Empathy exercise: how do you think security felt in this interaction, or in parallel real world scenarios?

Join at
slido.com
#434 110





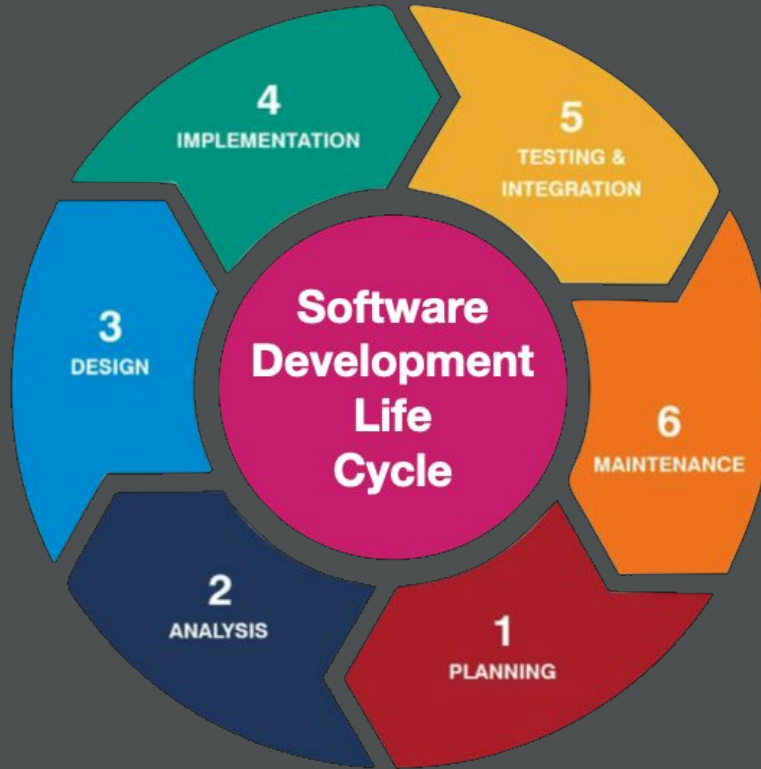
Let's discuss.

What and How of DevSecOps

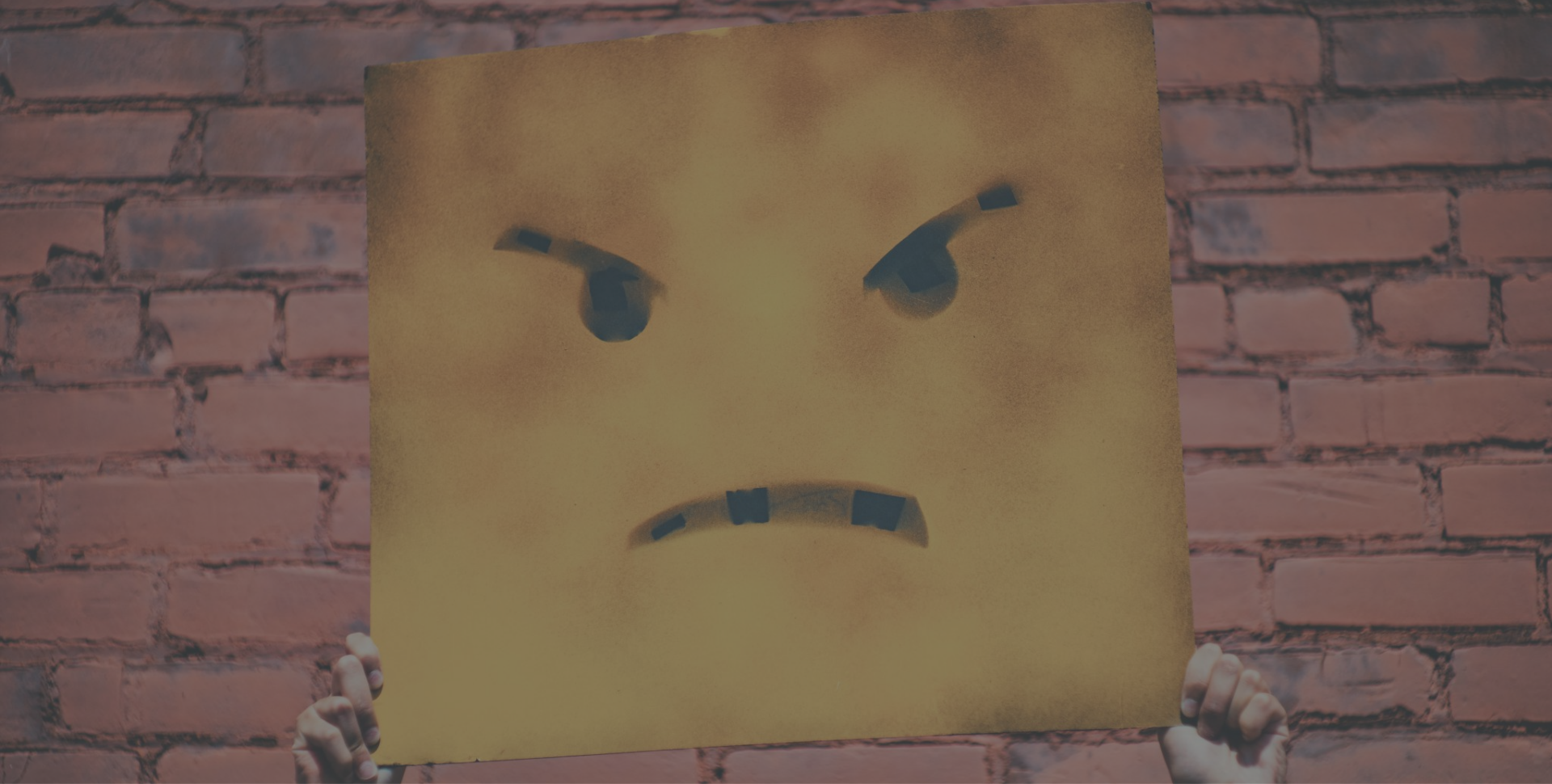
What was that all about? 🤔

The background of the slide features a close-up, slightly blurred photograph of several interlocking puzzle pieces. The pieces are a light, dusty purple color and are scattered across a light gray surface. In the background, a faint world map is visible, with a dashed line and the number '1000' printed on it. The text 'Current Situation' is centered over the puzzle pieces in a clean, white, sans-serif font.

Current Situation



Vaulting over “the wall”





DevSecOps

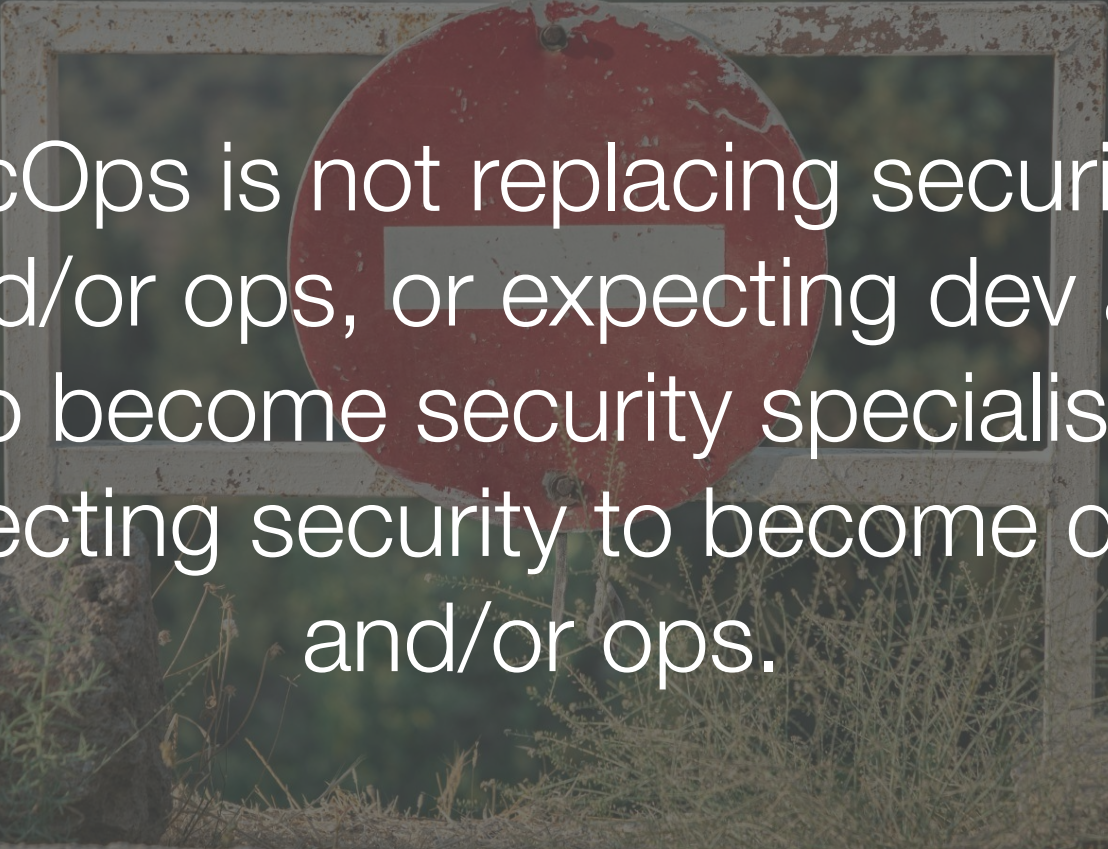


DevSecOps is the set of cultural practices that aims to break down the silo between security and development+operations.

A person in a small boat is seen from a distance on a calm body of water. The boat has left a long, smooth, curved wake that stretches across the water towards the foreground. The water is a dark, muted blue-grey color. The overall scene is serene and minimalist.

Specifically, DevSecOps seeks to address the organizational friction that exists between these teams and departments.

What DevSecOps is not



DevSecOps is not replacing security with dev and/or ops, or expecting dev and/or ops to become security specialists, or expecting security to become devs and/or ops.



and breathe

Phew.



A hammer and a wrench are positioned diagonally on a dark, textured wooden surface. The hammer has a black handle and a silver head. The wrench is silver and has "200mm TEKIRO" engraved on it. The text "DevSecOps is supported by both human activity and tooling." is overlaid in white, sans-serif font across the center of the image.

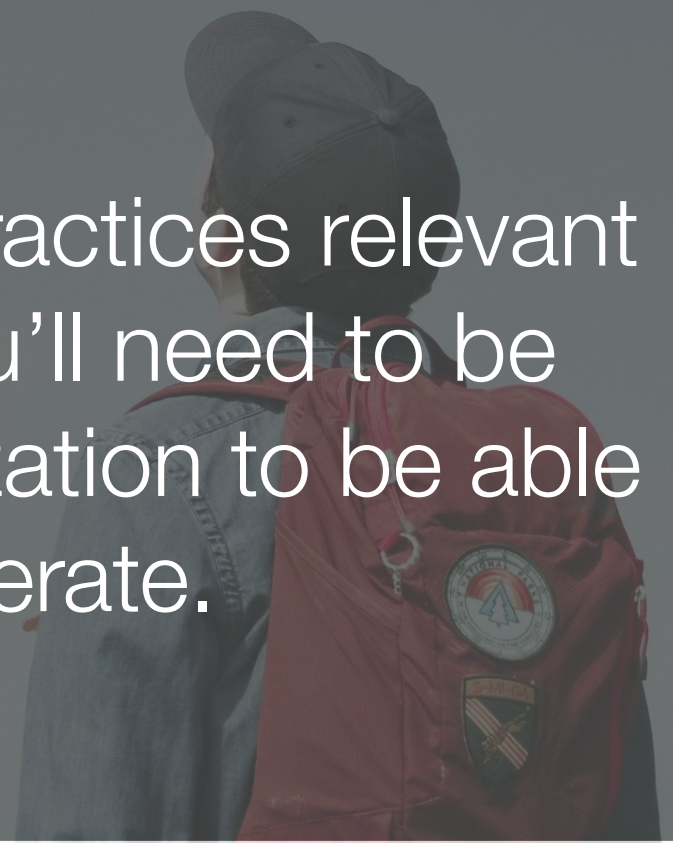
DevSecOps is supported by both human
activity and tooling.

The background of the slide is a dark, atmospheric landscape. It features a winding road that curves through a desolate, rocky terrain. The sky above is filled with stars, suggesting a night scene. The overall color palette is dark blue and black, with some lighter blue highlights on the road and the stars in the sky.

The first step on your DevSecOps
journey: awareness.



Best Practices are a Journey, not a One
Size Fits All



There are a lot of Best Practices relevant to DevSecOps - so you'll need to be aware of self and organization to be able to apply and iterate.



Join at
slido.com
#434 110



slido

Curious: How many of you are
interested in cross discipline
learning?



Join at
slido.com
#434 110



slido

What are some ideas you have for
implementing DevSecOps in your
company?

DevSecOps is implemented by

...



A flock of white birds, possibly swans or geese, is captured in flight against a clear, deep blue sky. The birds are scattered across the frame, with some in the foreground and others further back, creating a sense of depth and movement. Their wings are spread, and they appear to be moving in various directions.

Cultural Changes: Cross Functional Awareness and Empathy



Shifting Left in the Secure Software Development Life Cycle



Security Incident Remediation Process



Let's talk culture first

Cultural Changes



Cultural Aptitude & Empathy

Blameless Culture



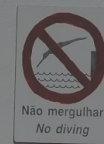
Full Service Ownership



Shadowing



By helping each other, we help ourselves.





Security Champions Program



Join at
slido.com
#434 110

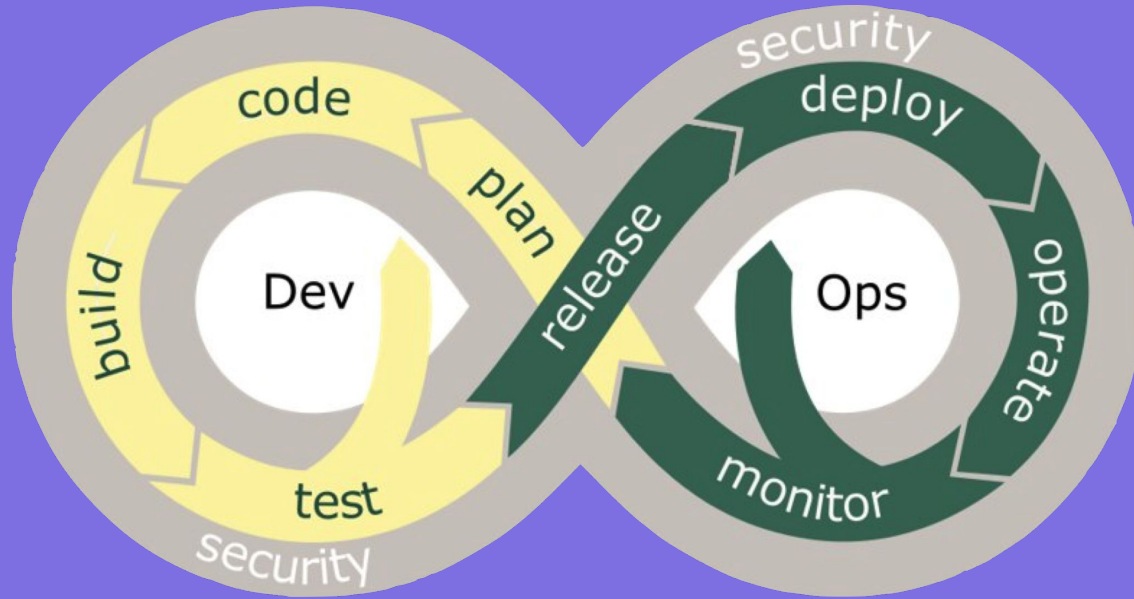


slido

What are some ways you can
support a DevSecOps
transformation at your company?

Shifting Left

Secure SDLC





Join at
slido.com
#434 110



slido

What are some security activities?

Another Secure SDLC

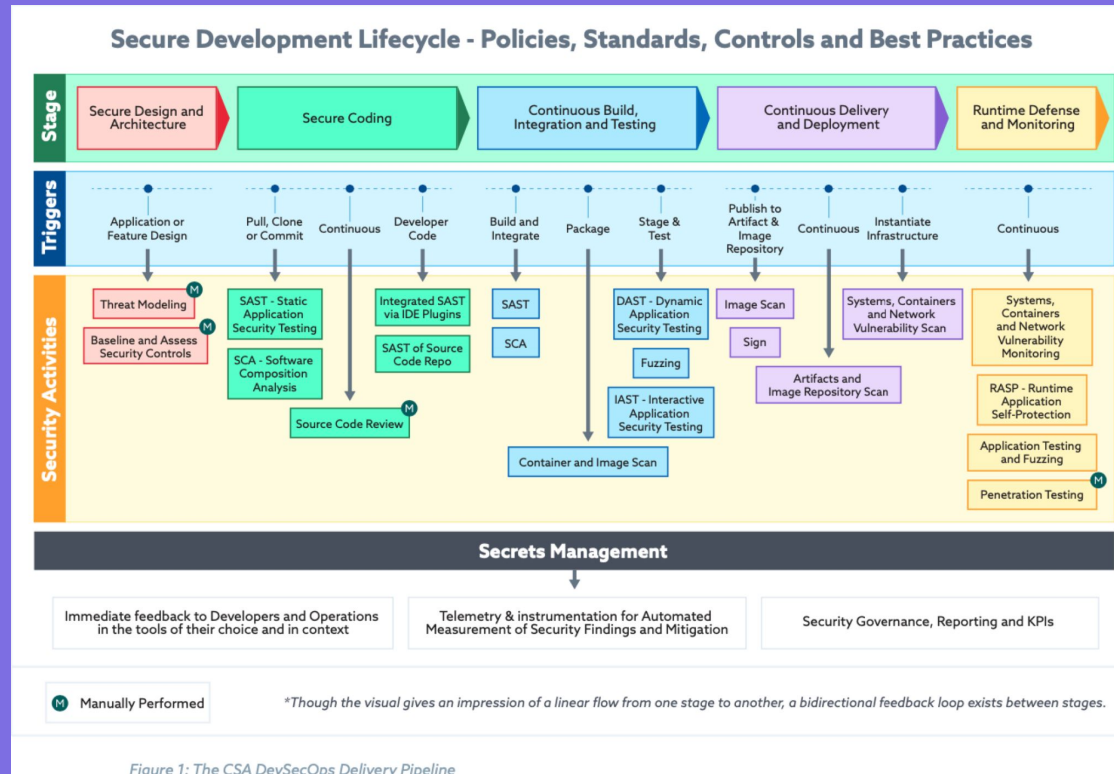


Figure 1: The CSA DevSecOps Delivery Pipeline





Why is it called “shift left”?

An FTL Overview



Secure Design and Code

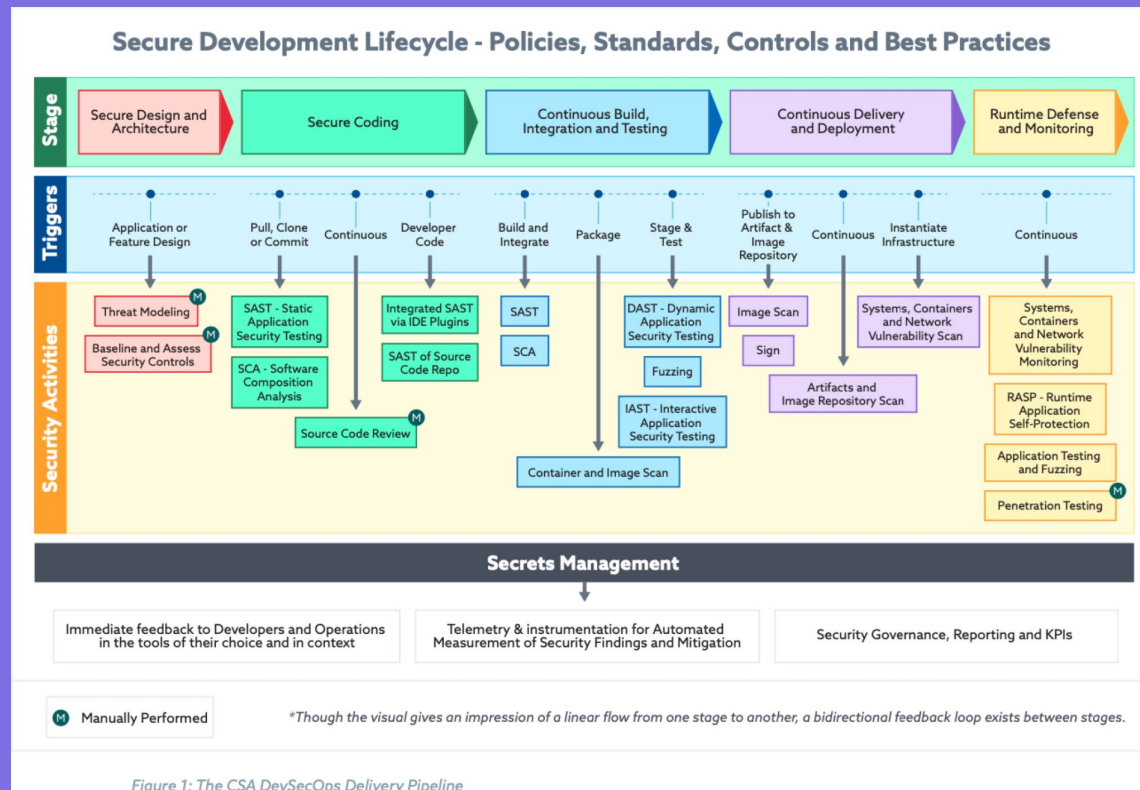
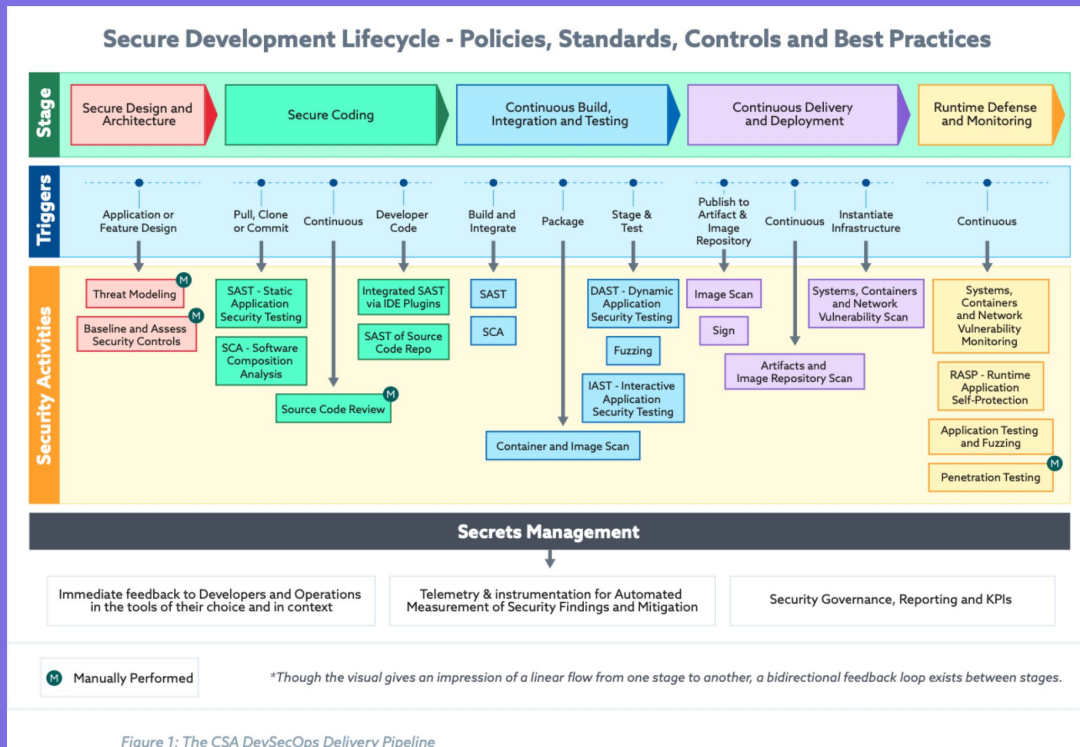


Figure 1: The CSA DevSecOps Delivery Pipeline



Secure Building, Testing, Delivery, & Deployment



Secure Runtime and Monitoring

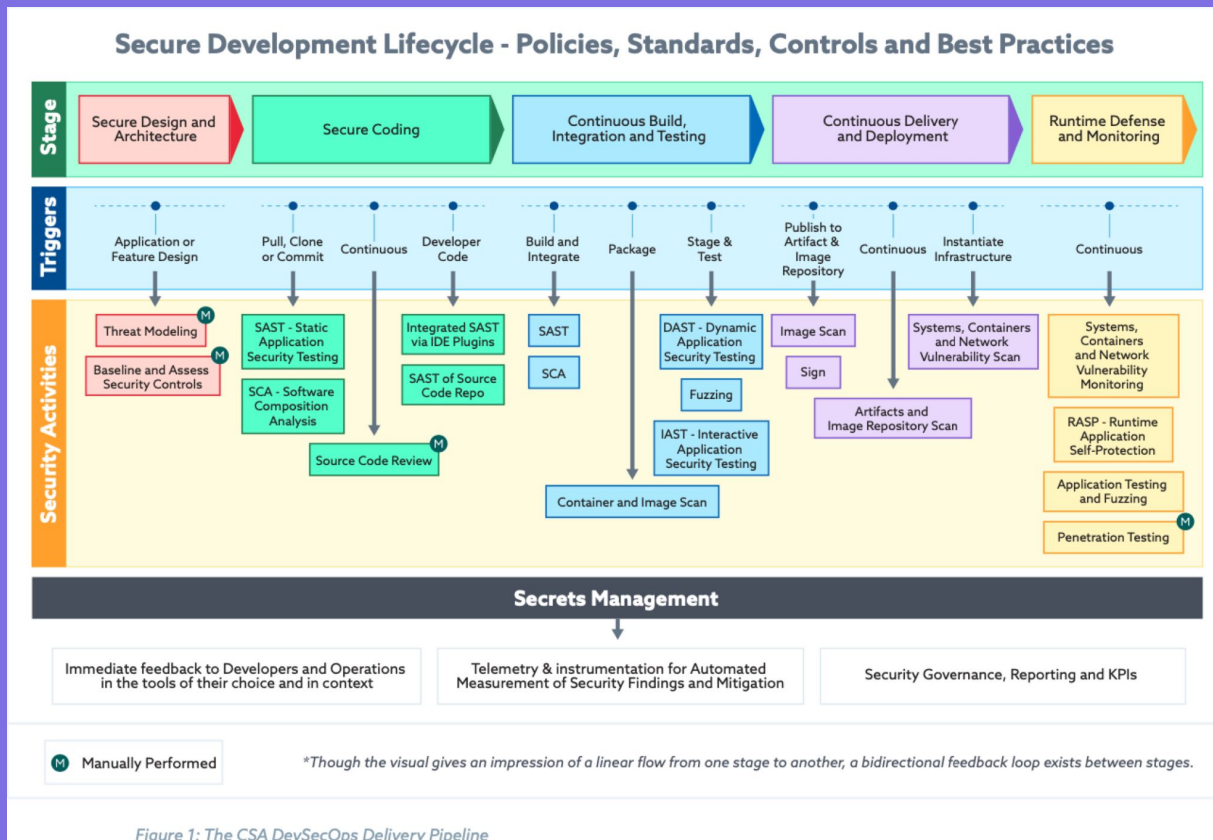


Figure 1: The CSA DevSecOps Delivery Pipeline





Your Mileage May Vary

A group of female soccer players in white and blue uniforms are gathered on a green field, celebrating with their hands raised. Some players have their names and numbers visible on their backs: NAGASATO 12, GORDEN 14, KERR 20, and WILLIAMS 22. Two referees in green shirts and black shorts stand to the right. The background shows a green field with white and green curved lines.

Everyone is relevant

Improve Security Posture

The background image shows two white Bosch security cameras mounted on a dark, textured wall. The cameras are positioned horizontally, facing right. Between them are two small, square, light-colored electrical boxes. Cables run from the cameras down and then horizontally across the wall. The text 'Security Posture' is centered in white, sans-serif font over the middle of the image.

Security Posture



A company's **security posture** is their overall readiness against security threats.



Join at
slido.com
#434 110



slido

What are some ways that your security team helps improve your security posture?



Always Ask

~~What do you do even do here?~~



How do you help us with $\{X\}$? 



A dark-colored smartphone is centered against a dark olive green background. The phone's screen is a dark purple color and displays the text "Security Assessments" in a white, sans-serif font. Behind the text is a large, semi-transparent grey padlock icon, indicating a security or locked state.

Security Assessments

Threat Modeling Exercises



A photograph of a beach with a red flag in the center. The flag is on a wooden pole and is waving. In the background, there is a blue ocean and a blue sky with white clouds. A few people are visible on the beach, and a surfboard is lying on the sand to the left.

Capture the Flag Games

A dark, grayscale image of a laptop keyboard with a magnifying glass held over it, symbolizing investigation or research. The text "Socially Engineer Trainings" is centered over the image in a white, sans-serif font.

Socially Engineer Trainings



Do not trick staff, ever

Example Security Training Slides



Join at
slido.com
#434 110



slido

How many of you have attended a
standard security training and
received benefit from it?





Knowledge



Possession



Inference





Passwords, Answers, etc.



Phone, Yubikey, etc.



Fingerprint, Iris Scan, etc.





2FA or **not 2FA**, that is the question.









Security Training Ops Guide



Join at
slido.com
#434 110



slido

Do you think a training like that
would be more beneficial to your
organization?



Join at
slido.com
#434 110




slido

True or false: Once we do All The Things we will be secure, forever!

Secure Incident Response



Security & Incident Response



A security incident is an incident that actually or potentially violates the security policies of a system or information that the system processes, stores, and/or transmits.



When to trigger a security incident



What happens next?

The Fourteen Steps

1. Stop the attack in progress.
2. Cut off the attack vector.
3. Assemble the response team.
4. Isolate affected instances.
5. Identify timeline of attack.
6. Identify compromised data.
7. Assess risk to other systems.
8. Assess risk of re-attack.
9. Apply additional mitigations, additions to monitoring, etc.
10. Forensic analysis of compromised systems.
11. Internal communication.
12. Involve law enforcement.
13. Reach out to external parties that may have been used as vector for attack.
14. External communication.





Step 1: Stop the attack in progress.



Step 2: Cut off the attack vector.



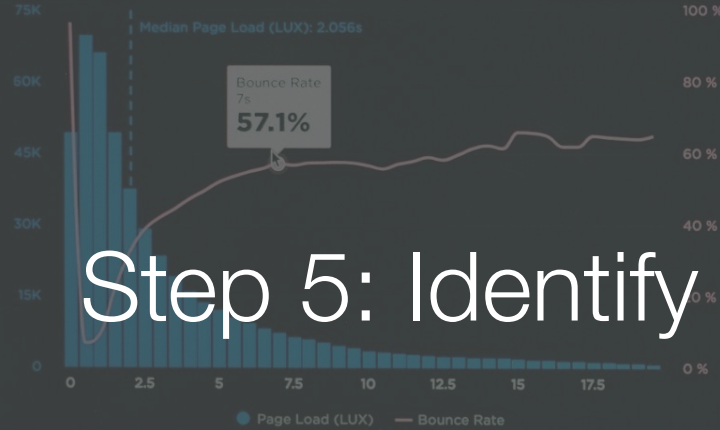
Step 3: Assemble the response team.

The background of the slide is a close-up photograph of many green chili peppers. One red chili pepper is visible in the center, slightly behind the text, serving as a visual metaphor for isolating a specific instance from a larger group.

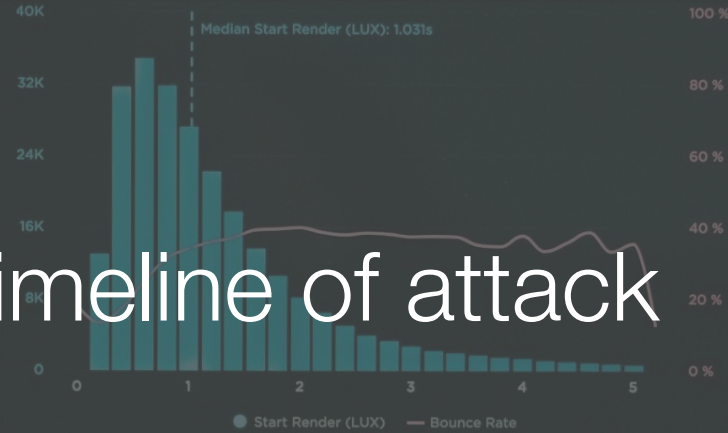
Step 4: Isolate affected instances.

USERS: LAST 7 DAYS USING MEDIAN ▾

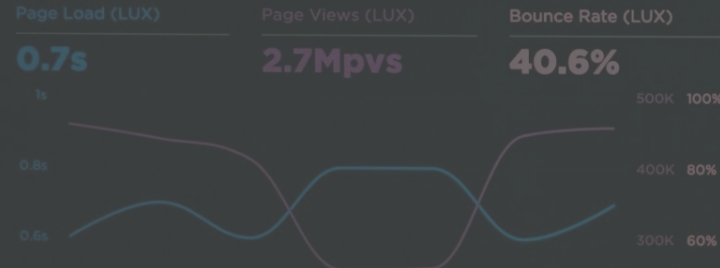
LOAD TIME VS BOUNCE RATE



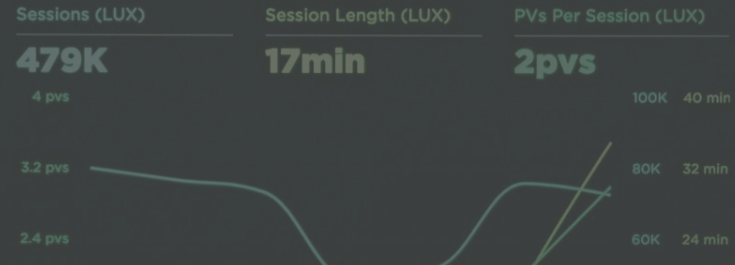
START RENDER VS BOUNCE RATE



PAGE VIEWS VS ONLOAD



SESSIONS



Step 6: Identify compromised data.



Step 7: Assess risk to other systems.

The background of the slide features three metal padlocks and their associated chains. One large padlock is on the right, another is in the center, and a third, smaller padlock is on the left. The chains are draped around them, creating a sense of security or restriction. The lighting is dramatic, with highlights on the metal surfaces and deep shadows in the background.

Step 8: Assess risk of re-attack.

The background image shows a close-up of a metal panel with six analog temperature gauges arranged in two rows of three. Each gauge has a black face with white markings and a needle. The scales range from 0 to 125 degrees Celsius, with major markings at 0, 25, 50, 75, 100, and 125. The gauges are labeled with 'GSR' and various numbers: 982, 983, 984 in the top row, and 985, 986, 987 in the bottom row. The text 'TEMPERATURE' is visible on the bottom-left gauge. The panel is secured with screws.

Step 9: Apply additional mitigations,
additions to monitoring, etc.



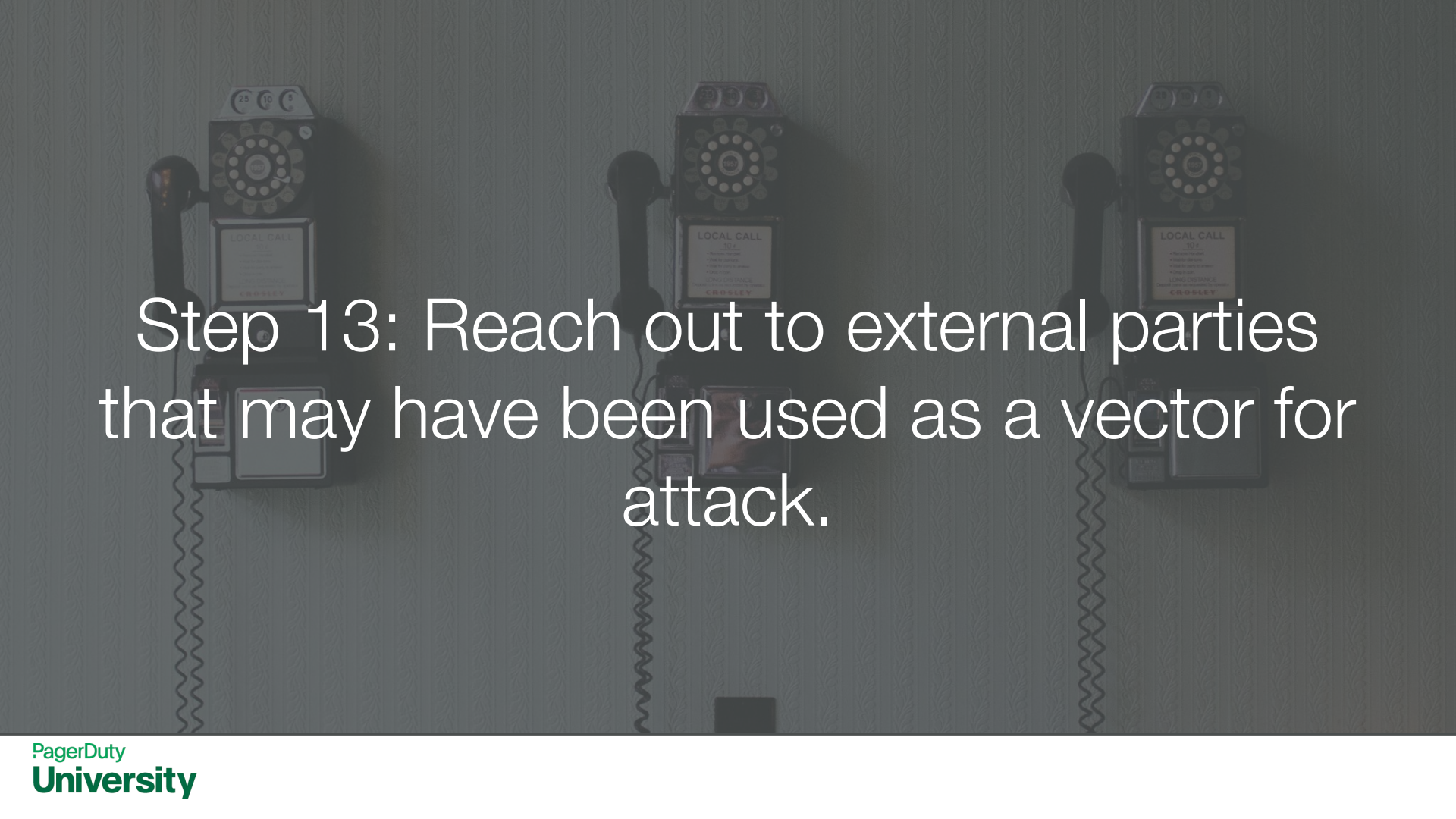
Step 10: Forensic analysis of compromised systems.



Step 11: Internal communication



Step 12: Involve law enforcement.

The background of the slide features three identical vintage rotary telephones mounted on a wall. The telephones are dark-colored with a circular dial and a coiled handset cord. Each phone has a small sign that reads "LOCAL CALL 10¢". The telephones are arranged in a horizontal row, and the text is overlaid in the center of the image.

Step 13: Reach out to external parties that may have been used as a vector for attack.



Step 14: External communication

The Fourteen Steps (Recap)

1. Stop the attack in progress.
2. Cut off the attack vector.
3. Assemble the response team.
4. Isolate affected instances.
5. Identify timeline of attack.
6. Identify compromised data.
7. Assess risk to other systems.
8. Assess risk of re-attack.
9. Apply additional mitigations, additions to monitoring, etc.
10. Forensic analysis of compromised systems.
11. Internal communication.
12. Involve law enforcement.
13. Reach out to external parties that may have been used as vector for attack.
14. External communication.



References and Resources



Resources

PagerDuty DevSecOps Guide

devsecops.pagerduty.com

All PagerDuty Ops Guides - including security training

pagerduty.com/ops-guides/

STRIDE Threat Modeling Framework

[ThoughtWorks Implementation Link](#)

About Capture the Flag (for InfoSec)

ctf101.org

Resources also available
at the PagerDuty
University Booth





Purple Team



Final Exam!

(Kidding, but really earn some points 😊)

[Link in Chat](#)



Thank You

Final Swag Challenge: Survey (in chat)