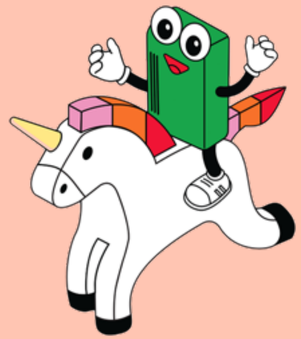
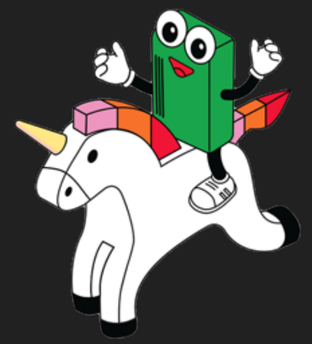
DevSecOps and Secure Incident Response

@QuintessenceAnx
Developer Advocate @ PagerDuty



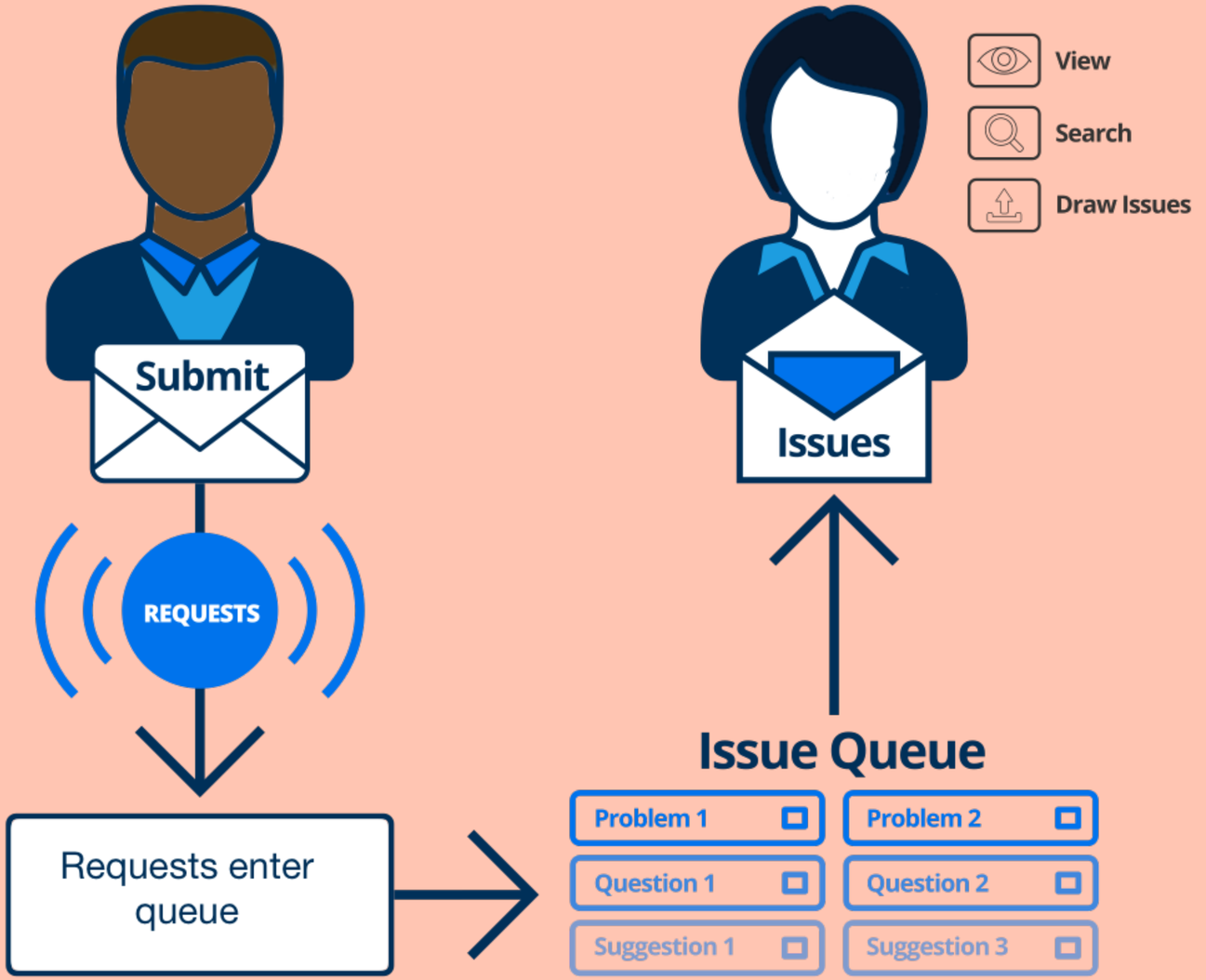
DevSecOps and Secure Incident Response

@QuintessenceAnx
Developer Advocate @ PagerDuty



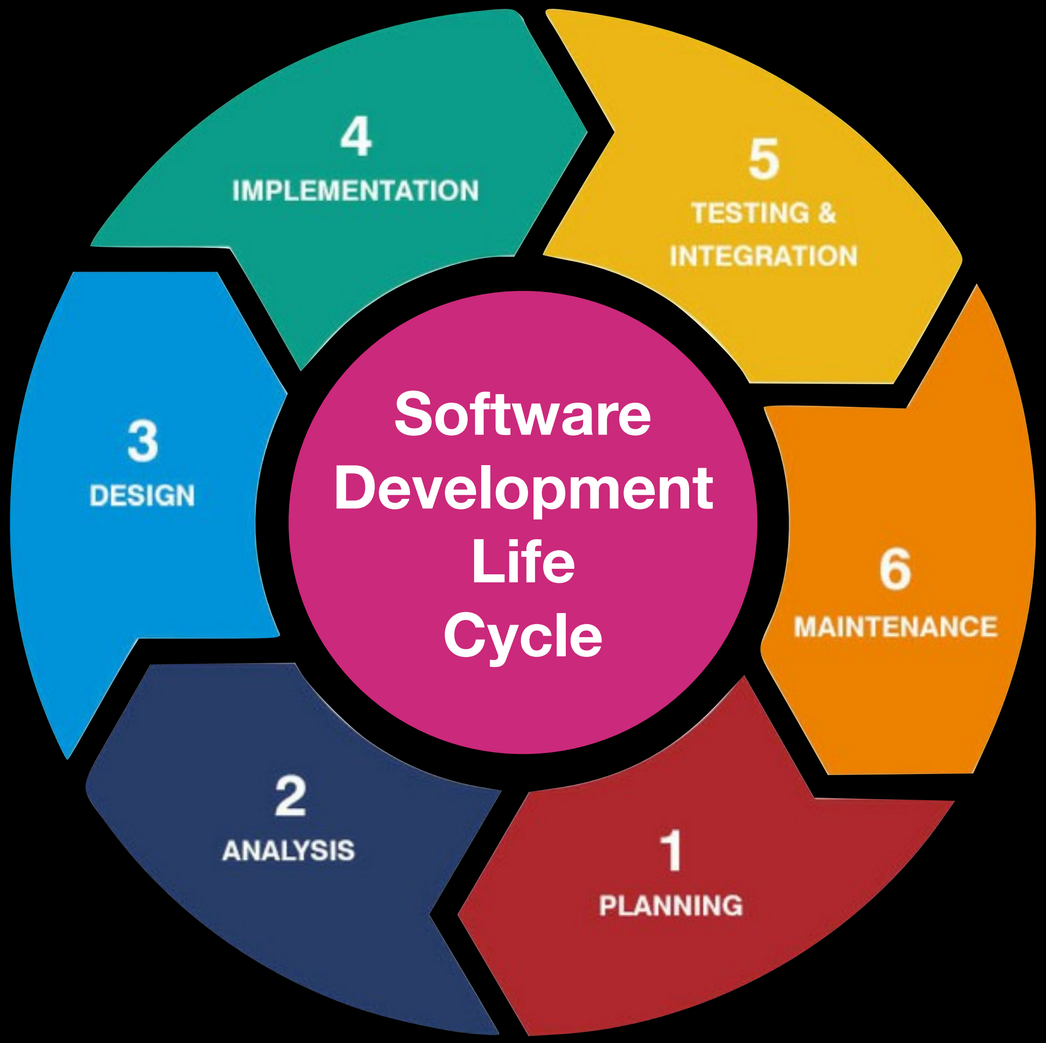
Don't panic

The Now



PagerDuty

@QuintessenceAnx



PagerDuty

@QuintessenceAnx

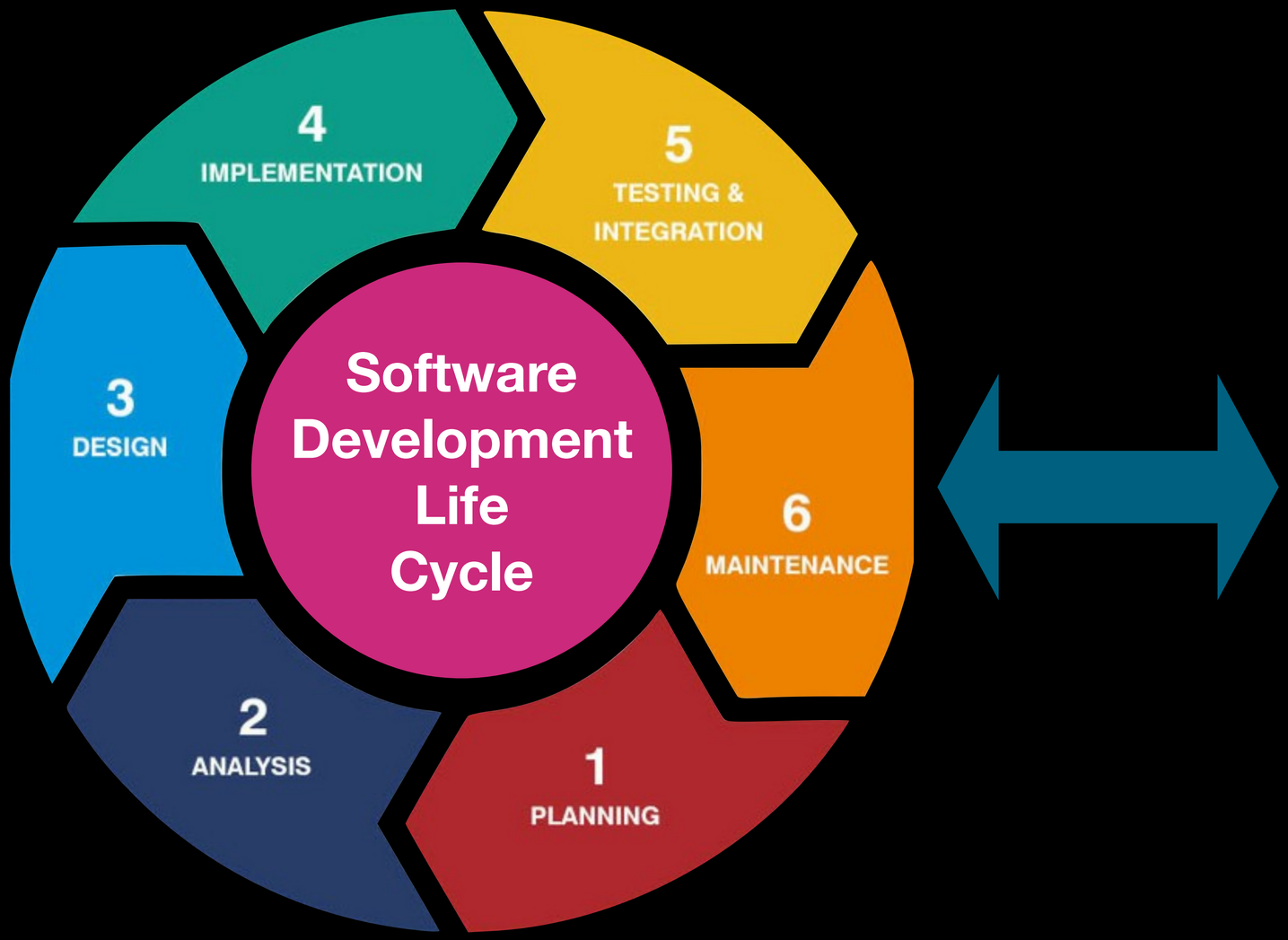
Vault over "The Wall"

for

Security Review

PagerDuty

@QuintessenceAnx



PagerDuty

@QuintessenceAnx

PagerDuty
@QuintessenceAnx

DevSecOps

What is DevSecOps?

DevSecOps stands for development, security, and operations. DevSecOps seeks to integrate security across the SDLC and streamline the workflows between dev, sec, and ops.

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.

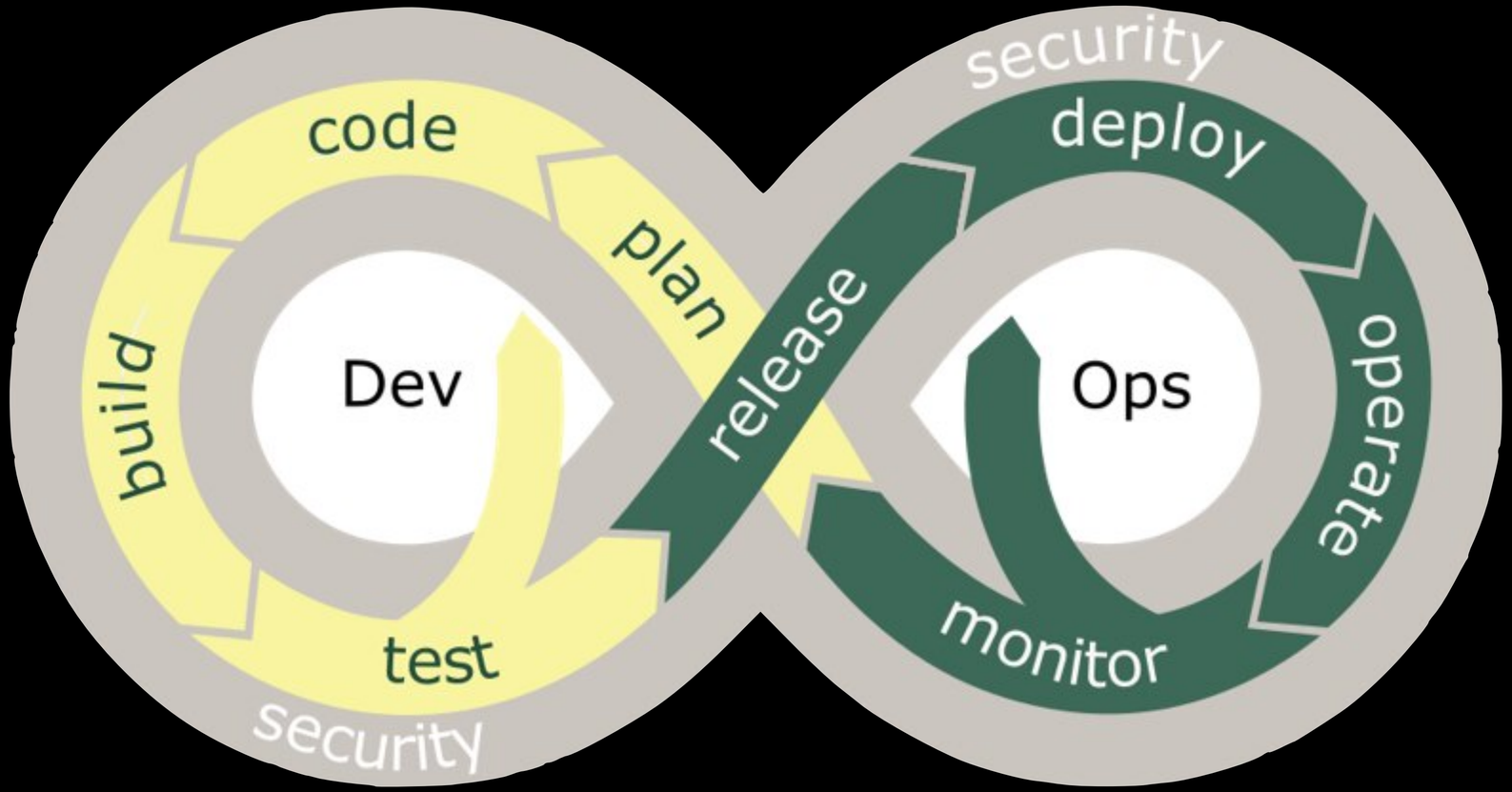
Phew.

PagerDuty
@QuintessenceAnx

How?

The Secure SDLC + Shifting Left

PagerDuty
@QuintessenceAnx



PagerDuty

@QuintessenceAnx

Secure Development Lifecycle - Policies, Standards, Controls and Best Practices

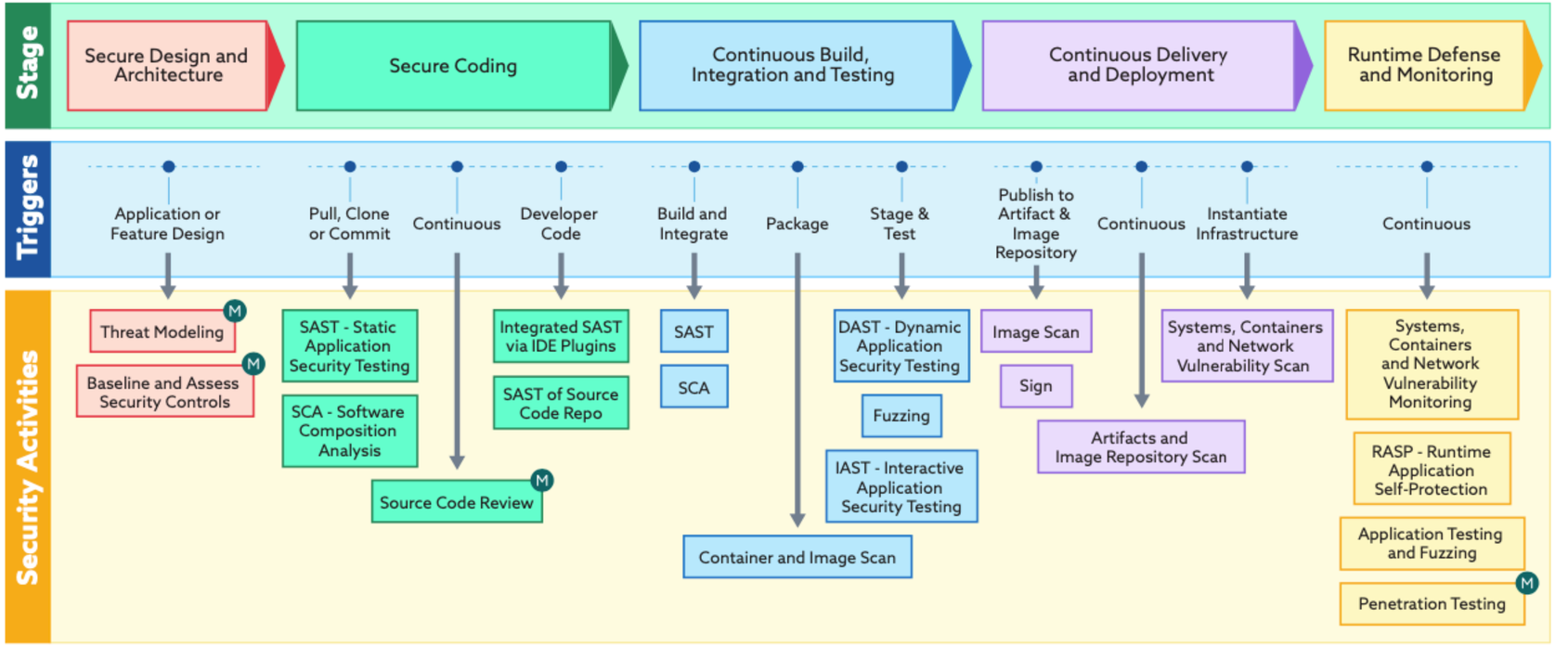


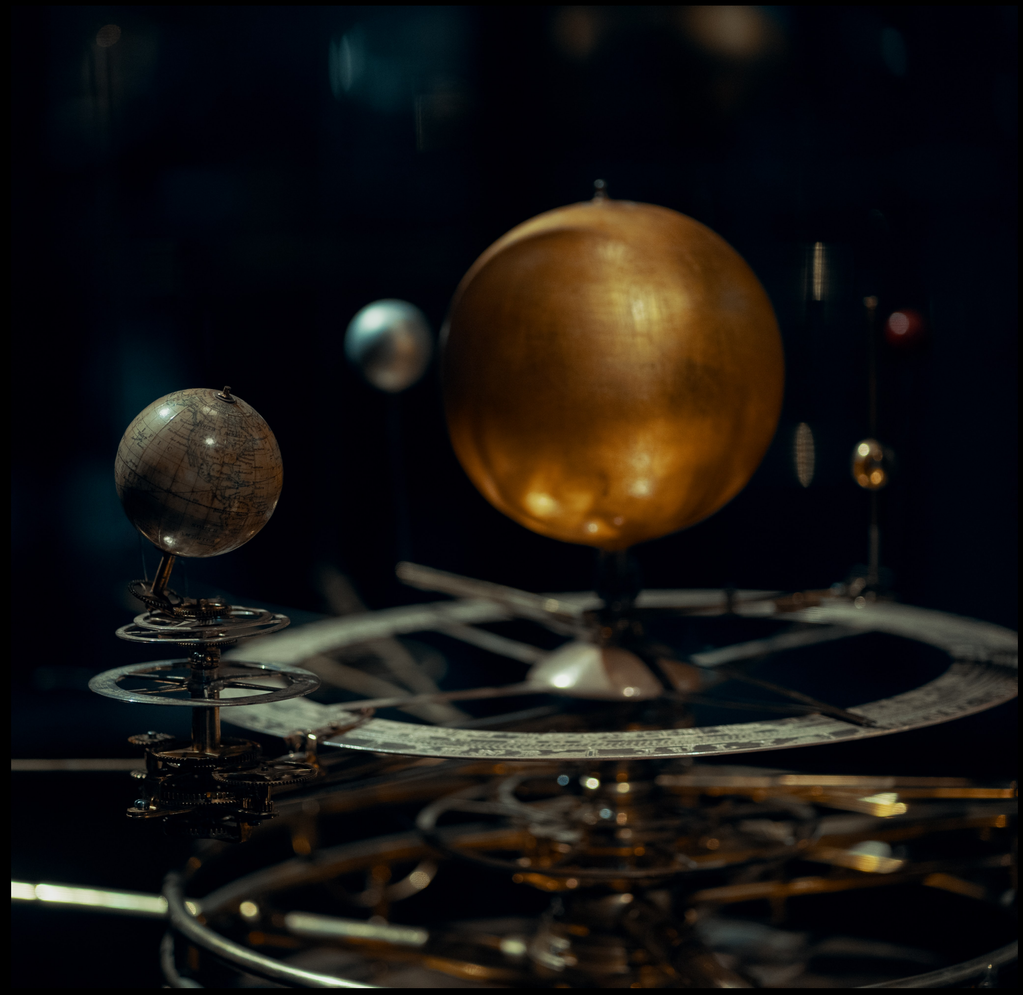
Figure 1: The CSA DevSecOps Delivery Pipeline

PagerDuty

@QuintessenceAnx

SecOps Activities

- Secure architecture / design
- Threat modeling
- Testing, e.g. SAST and DAST
- Scanning images and dependencies
- Fuzzing
- And more!



Shift Left

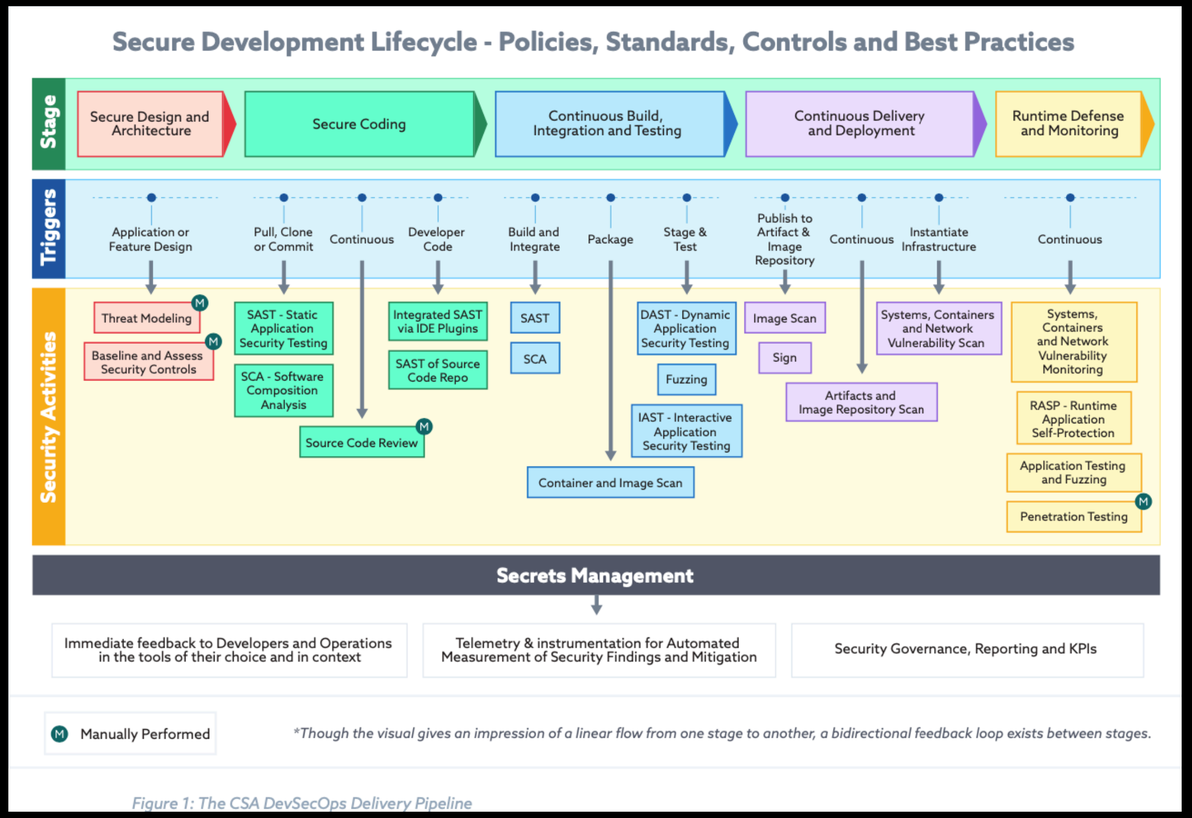


Figure 1: The CSA DevSecOps Delivery Pipeline

PagerDuty

@QuintessenceAnx

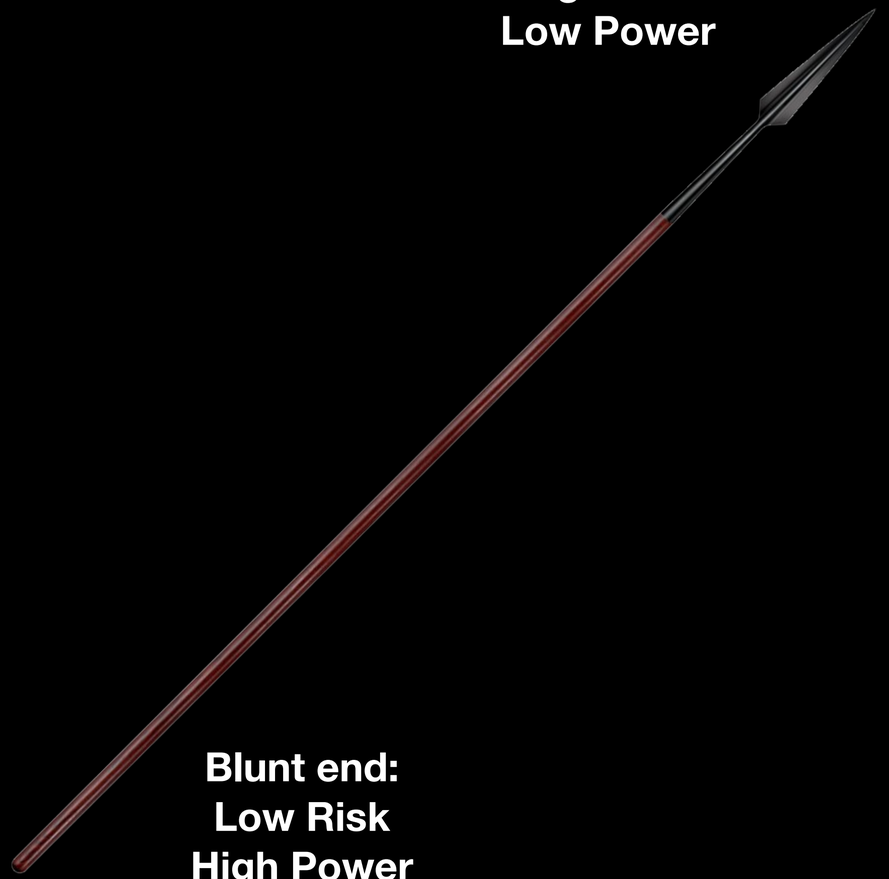
PagerDuty

How?

Cultural Support

Humans.

Sharp end:
High Risk
Low Power



Blunt end:
Low Risk
High Power

PagerDuty

@QuintessenceAnx

Exec Buy-in

Never trick staff, *ever*.

Training

PagerDuty

@QuintessenceAnx

Full Service Ownership

PagerDuty

@QuintessenceAnx

Capture the Flag

PagerDuty

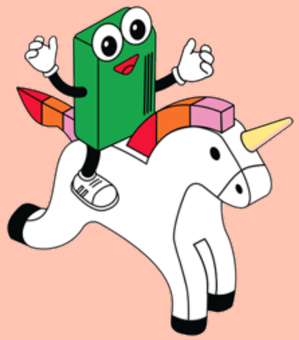
@QuintessenceAnx

Threat Modeling

PagerDuty

@QuintessenceAnx

Secure Incident Response



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, make changes 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.

PagerDuty

@QuintessenceAnx

Stop the attack in progress

Cut off the attack vector

Assemble the response team

Isolate the affected instances

Identify timeline of the attack

Identify compromised data

Assess risk to other systems

Assess risk of re-attack

Apply additional mitigations, additions to monitoring, etc.

Forensic analysis of compromised systems

Internal communication

Involve law enforcement

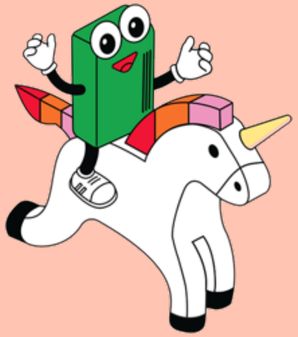
Reach out to external parties that may have been used as attack vectors

External communication

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, make changes 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.

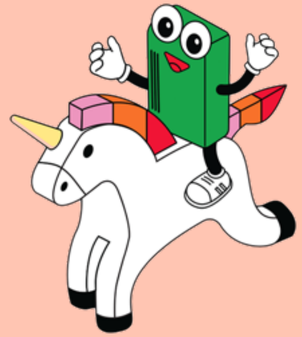
PagerDuty

@QuintessenceAnx



Resources & References

noti.st/quintessence



PagerDuty

@QuintessenceAnx

Questions?

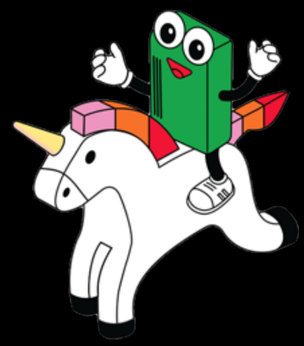
Quintessence Anx
Developer Advocate

PagerDuty

noti.st/quintessence

@QuintessenceAnx

Brand Colors

- PagerDuty Green Hex #06ac38
- Dark Green Hex #005a24
- Clay Hex #94b2a5
- Orange Hex #fa640a
- Peach Hex #ffc5b2
- Yellow Hex #ffe664
- Dark Blue Hex #00607f

PagerDuty