Dan Liao

Elevating DevSecOps: Mastering Security in the Modern Era

29 May 2024

01 **Integration with the SDLC process**

02 **Scaling CI/CD**

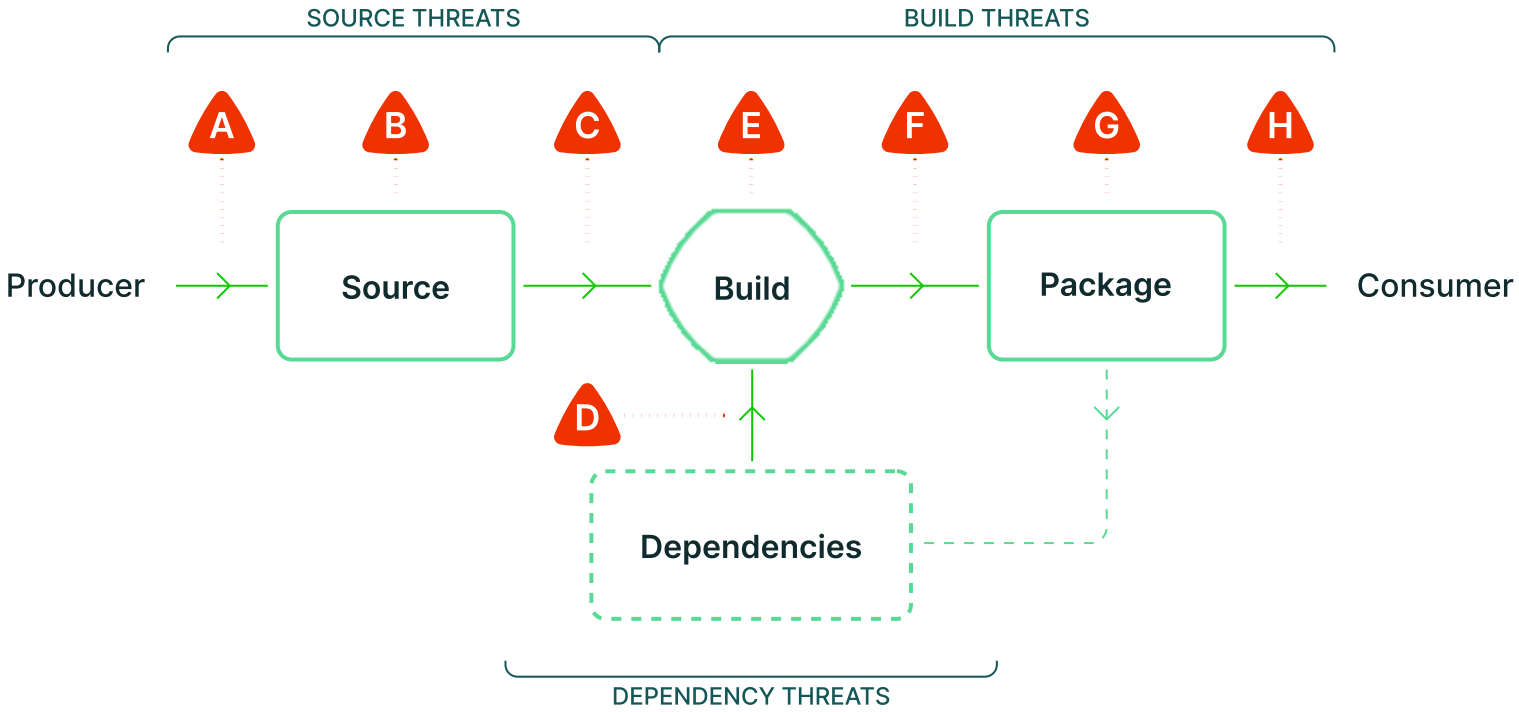
03 **Engineering practices for scalability**

04 **Q&A**

Integration with the SDLC process

- To remain competitive in the market, many organisations are forced to diversify their technical stack to target a broader audience. This often leads to disparity of tooling, workflows and infrastructure.
- What strategy can we adopt to make it more effective?

Integration with the SDLC process



SOURCE THREATS

- **A** Submit unauthorized change
- **B** Compromise source repo
- **C** Build from modified source

DEPENDENCY THREATS

- **D** Use compromised dependency

BUILD THREATS

- **E** Compromise build process
- **F** Upload modified package
- **G** Compromise package registry
- **H** Use compromised package

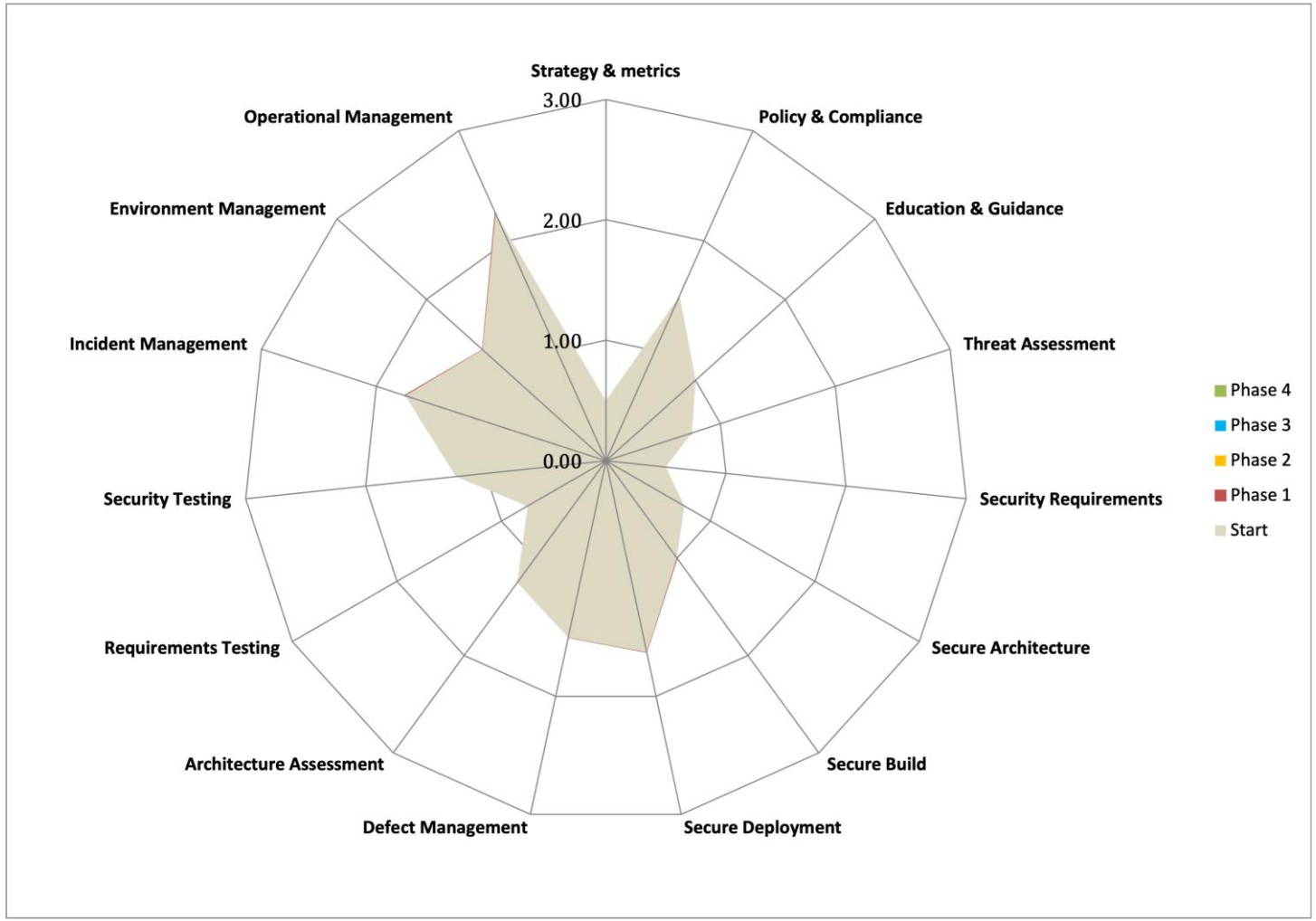
https://slsa.dev/spec/v1.0/threats

Integration with the SDLC process

- An ideal culture is one that brings on accountability and open feedback for continuous improvement.
- Consider the culture that we want to foster in the organisation. The culture helps us determine the level of security responsibility we provide to engineers.

Setting goals

- Assess your organisation with the OWASP Software Assurance Maturity Model (SAMM)



Setting goals

- Things to consider when defining your goals.
  1. Developer experience
  2. Training, knowledge sharing
  3. Forum for collecting feedback

Scaling CI/CD

- How do we ensure that our secure CI/CD is scalability?

1. Recommend a paved path to Production
2. Building abstractions/templates
3. Automate
4. Fast feedback loop (fail fast)
5. Remove bottle necks
6. Embracing AI
7. Feedback to evolve the process to meet changing needs

Engineering practices for scalability

- *Build abstractions, not illusions* (Gregor Hohpe) – Good abstractions should ensure that engineers won't develop a false sense of euphoria.
- Trust but verify
- Collaborate early
- Security is everyone's responsibility – Empower engineers to make the right decisions through training & adopt tooling that prioritises on developer experience.

Key Takeaways

Understand your organisation before making changes to ensure effectiveness

Assess your organization with OWASP SAMM

Scale CI/CD by establishing paved paths

Security is everyone’s responsibility