SDL Unicorns or Thoroughbreds: Application Security in DevOps

Hemanth Srinivasan
Autodesk
Agenda

- Unicorns, Horses & Thoroughbreds
- SDL
  - What is it?
  - How has it evolved?
- Adapting to DevOps
  - Customizing SDL activities
  - SDL Flow
  - Benefits & Challenges
- Takeaways
- Q&A
Unicorns, Horses, Thoroughbreds

- Unicorns
  - Innovators
  - Mythical creatures
- Horses
  - Slow movers
  - Saddled with legacy
- Thoroughbreds
  - Agile and bold
  - Run away from the pack
SDL - Beginnings

- Microsoft SDL
- Security is “built-in”
- Security activities embedded into every SDLC phase
SDL - Agile

- Incremental & iterative
- Align security activities
- Prioritize & break-up
  - Every sprint requirements
  - Bucket requirements
  - One-time requirements
And then

SDL

Dev

Ops

?
The “Three-Ways”

- Flow
  - Automate & Code
  - Pipeline
- Feedback
  - Reviews & Testing
  - Telemetry
- Learning
  - Experiment & Refine
  - Share
SDL - Adaptations

- Training
  - Just in time
- Security requirements
  - Unified
  - Integrated
  - Move to left
- Threat modeling
  - Rapid
  - As Code?
- Static & Dynamic analysis
  - Automate
  - Customize
- Pentests
  - Targeted & Time-bound
  - Bug-bounty
- Infrastructure
  - Automate & Code
  - Blue-Green deployments
Threat modeling as Code
Benefits & Challenges

• Benefits
  • No disruption in Flow
  • End-to-End security
  • Symbiosis

• Challenges
  • Technology
  • Adoption
  • Culture change
  • Security champions

*Interaction between two different organisms living in close physical association, typically to the advantage of both.*

-Wikipedia
Takeaways

- Security, Privacy and Compliance Requirements
- Availability Requirements
- Operational Support Requirements
- Scalability Requirements
- Monitoring Requirements

Agile - CI/CD Pipeline

End-to-end SDL Activities

- SDL Training
- Non-functional Requirements
- Threat Modeling
- 3rd Party Reviews
- Static Code Analysis
- Dependency Checks
- Hardening
- Dynamic Analysis
- Vulnerability scanning
- Penetration Tests
- Bug Bounties
- Hardening
- Pentests
- Bug Bounties
- Vulnerability scanning
- Monitoring
- Incident Response

NFR

- Security, Privacy and Compliance Requirements
- Availability Requirements
- Operational Support Requirements
- Scalability Requirements
- Monitoring Requirements
Takeaways

- Trim & Streamline
- Automate
- Integrate
- Measure & Refine
How seemingly opposite or contrary forces may actually be complementary, interconnected, and interdependent in the natural world, and how they may give rise to each other as they interrelate to one another.

-Wikipedia
- Don’t pretend to be a Unicorn
- Try to be a Thoroughbred instead
  - Focus on Culture & Adoption
  - Right Tools & Technologies
  - Start small then scale
Questions
THANK YOU
Reference

• https://www.microsoft.com/en-us/SDL/
• The DevOps Handbook
• http://plantuml.com/
• https://www.wikipedia.org/
• www for some images