THE EMERGING PRODUCT SECURITY LEADER DISCIPLINE

Matt Clapham
Principal Product Security Leader
GE Digital (Healthcare)
@ProdSec
Agenda

- What is product security
- What is a product security leader
- DevOps vs. DevSecOps
- Important skills
- How each skill takes DevOps to DevSecOps
Who *Hasn’t Heard This One?*

- Web site has a vulnerability
- Finder creates a trendy name and publicizes
- Describe technical root cause
- Provide sample code for 0-day
- Gives 90 days to fix

*There is a better way, product security.*
What is “Product Security”?

**Product**
- Made to be sold
- Contains software
- Talks to other things

**Security**

TRUST
“DEFENDERS SEE THINGS WAY DIFFERENT THAN BLOCKERS.”
-BROOKE SWEAT
"Anyway, I keep picturing all these little kids playing some game in this big field of rye and all. Thousands of little kids, and nobody's around - nobody big, I mean - except me. And I'm standing on the edge of some crazy cliff. What I have to do, I have to catch everybody if they start to go over the cliff - I mean if they're running and they don't look where they're going I have to come out from somewhere and catch them. That's all I do all day. I'd just be the catcher in the rye and all. I know it's crazy, but that's the only thing I'd really like to be."

-HOLDEN CAULFIELD

*The Catcher in the Rye* by J.D. Salinger
Product Security Leader Role

**Does**
- Subject Matter Expert
- Teacher
- Cheerleader
- Influencer
- Policeman

**Does Not**
- Enterprise architecture
- Compliance
- Develop code
- Work with a single team
- Accept risk
DevOps to DevSecOps

DevOps
- Roles
- Culture
- Responsiveness

DevSecOps
- Security in every layer and step
- Something over nothing
- Incremental improvement
- Secure delivery always
- Security ready always
Let’s Talk About...

This Photo by Unknown Author is licensed under CC BY
Software Development

- Thinking about what to do
- Throwing some code together
- Test it (maybe)
- Send it to production
- Ignore bug reports
How to Software Development

- Write or test some code
- Commercial, freemium, or OSS project
- Participated in at least one development cycle
- Ship a feature
- Shipping is a feature
Software DevSecOps

- Puts the Dev in DevOps and DevSecOps
- Familiarity with variety of programming languages and practices
- Builds rapport across development roles
- Security of features
- Security features
Software DevSecOps Examples

- Custom glue to make single sign-on work with web application
- Create a risk analysis dashboard for web service
- Utilize security tested and hardened libraries
- Feature enhancements for 2-factor authentication
Risk Knack
Risk Knack is the Ability to Say...

- That’s risky...
- ...here’s why...
- ...a better way would be to...
- ...and change these layers at the...
- ...so it prevents the potential problem...
- ...with that new privacy regulation...
How to Get the Risk Knack

- Be naturally paranoid
- Be inquisitive
- Be skeptical
- Research multiple viewpoints
- Correct for risk biases
- “What could possibly go wrong?”
Leveraging Risk Knack in DevSecOps

- Use subject expertise to find good, bad, and ugly risks
- Promote secure development culture
- Find simpler, more secure ways to do same things
- Proactive privacy and security features
Risk Knack DevSecOps Outcomes

- Pre-emptively engineer privacy features
- Both client and servers incorporate security
- Change a feature to have more secure defaults
- Educate development team on secure design patterns
Threat Modeling

1. Decompose Application
2. Determine Threats
3. Design Mitigations
4. Implement
How Threat Modeling May be Learned

- Take training
- Read a book
- Experiment with tools
- Model a favorite program or physical process
- Train others
Threat Modeling in DevSecOps

- Decompose complex project into components
- Separate concerns
- Define trust boundaries
- Clarify span of control
- Demonstrate simplicity is lower risk
Threat Modeling in DevSecOps Outcomes

- Reinforces development security training
- Operations team monitors unmitigated threats
- Development team learns to spot and mitigate threats
- Threat model review part of standard release process
IT Security Operations
How to Get IT Security Experience

- Work in CISO organization
- Configure a system or network for least privilege
- Investigate a security incident
- Participate in change management review board
- Analyze cost/benefit of intrusion prevention system
IT Security in DevSecOps

- Operational defense-in-depth
- Cloud, enterprise, or combined
- Prioritization of risks
- Identify security, development, or operations intersections
DevSecOps Examples

- Security Operations has logging signal to analyze
- Operations teams adds security at appropriate layers
- Development team has backlog of security features
- Risk management dashboard with real-time detail
“Learn from the mistakes of others. You can't live long enough to make them all yourself.”

-Eleanor Roosevelt
How to Learn From Other’s Success or Failure

- Study classic defensive patterns
- Analyze what worked
- Research what didn’t
- Break down vulnerability steps to root cause
- Devise ways to identify and prevent root cause
Learn From Other’s DevSecOps Failures

- Not enough signal
- No consideration of insider threats
- Lack of process for addressing vulnerability reports
- Ignoring routine maintenance
Learn From Other’s DevSecOps Successes

- All database interactions use parameterized queries
- Leverage platform and compiler security enhancements
- Minimal network footprint
- Bug bounty program for finders
Penetration Testing

- Reconnaissance
- Scanning
- Gaining Access
- Maintaining Access
- Covering Tracks
Penetration Testing

- ...think like an attacker
- ...decompose the software
- ...break it
- ...break into it
- ...fix it
- ...put the detail in context
How to Get Penetration Testing Experience

- Training
- First hand experimentation with tools
- Deliberately bad web applications
- Certification
- Vulnerability management programs
Penetration Testing in DevSecOps

- Break and then fix all the things
- Fix all the easy things
- Don’t fix the same things twice
- Defend all the unfixed things
Penetration Testing DevSecOps Examples

- Easy security configuration work done
- Security unit tests for key features
- Security regression tests for all features
- Anti-fragile design has multiple cross-covering design
Crypto != \textcircled{B};
How to Learn Enough Crypto

- TLS handshake
- Public vs. private vs. secret keys
- Hashes and salts
- How big to make them all
- Certs, chains, roots, thumbprints, permissions, and pins
- Don’t roll your own
- Don’t be a CA
Cryptography in DevSecOps

- Analyze what threats crypto does not prevent
- What to use when and where
- Key management for operations
- Only modern algorithms and key sizes used
- HTTPS everywhere
DevSecCryptoOps Examples

- Key management features for operations
- Key management features for customers
- No secrets embedded in code
- Tamper evident “Break the glass for access” feature
Certifications

- CISSP®
- CSSLP®
- CEH
- CND
- GIAC
- CompTIA Security+
What Does it Take to Get Certified?

- Focused study in security
- Work experience in security
- Sub-topic specialization
- Taking a test to demonstrate a knowledge at appropriate level
- May require a practical exam
Benefitting from Certifications in DevSecOPs

- Utilize the breadth of knowledge
- Focus specializations on relevant roles for depth
- Cover customer expectations
- Cover legal obligations, if any
DevSecCertifications Outcomes

- Fewer security audit findings version over version
- Report to customers on level of staff training
- Security operations structured for responsiveness
- Secure designs stay up-to-date because of continuing education
Agile and Continuous Delivery

- Threat Modeling
- Security Program
- Penetration Testing
- Compliance
- Secure Operations
- Analytics
- SAST
- DAST
- Security Gates
- CAST
- Architecture
- CAST
- Secure Operations
- Analytics
- Compliance
- Threat Modeling
- Security Program
- Penetration Testing
- SAST
- DAST
- Security Gates
- CAST
- Architecture
Agile and CI/CD

**Agile**
- Processes
- Change
- Delivery

**CI/CD**
- Lifecycle
- Tools
- Automation
DevSecOps Deployment Agility

- Security gates using automated tools
- Incremental security improvement culture
- Security follows its own guidance
- Deployment pipeline automatically tests
- Test driven development
DevSecOps Continuous Agile Examples

- Web Applications Scanner tests must pass to deploy in production
- Build system scans all source code for security vulnerabilities
- Deployment secrets and configuration details are late bound
- Design templates provided preconfigured secure infrastructure
IoT

...because IoT
Learning from Internet of Things

- It’s all software
- Identify all the things
- (Securely) connect all the things
- Resource constrained computing
- Playing catch up for sins of the past
DevSecOps for IoT

- Fight tech debt before it’s too late
- Authentication and authorization everywhere
- No silent failures
- Lifecycle for hardware and software
- Can’t trust client systems
Secure IoT Examples

- Security relevant signal from devices
- Automated correlation analysis of device and cloud logs
- Cloud authenticates devices using embedded private key
- Remotely upgradable software stack
- Devices only follow specific instructions from cloud
Summary

- What is product security
- What is a product security leader
- DevOps vs. DevSecOps
- Important skills
- How each skill takes DevOps to DevSecOps
Applying What We’ve Discussed

- 3 weeks:
  - Reach out to Product Security Leader in your organization

- 3 months:
  - Create or select some security improvements with Product Security Leader

- 6 months:
  - Implement one or more security improvements with Product Security Leader

*Start building DevSecOps culture today!*