It’s Hackers All The Way Down

Experiences in Improving Security by Transferring Adversarial Skills to Product Teams

Joe Gervais
@TryCatchHCF
About The Presenter

Joe Gervais

• 25+ years of industry experience in building and securing production environments (mostly Gov’t / DoD)

• 35+ years of breaking into (and helping secure) networks and systems

• Technical Director / Red Team Ops; Application Security Team Lead; Lead Pentester; Software Engineer

• Former USMC Intelligence Analyst, Intelligence Chief, Counterintelligence Specialist

• Bachelors degree, Cognitive Science; Masters degree, Information Assurance
It’s Hackers All The Way Down

Traditional Approach to AppSec

• Static AppSec Analysis Tools
• Designated InfoSec “Champion” on Product Team
• InfoSec Pentest of Candidate Product / Update
It’s Hackers All The Way Down

Actual Footage of Typical InfoSec Collaboration with Product Team
Why Transfer Hacking Skills to Product Teams?
“If you do not change direction, you may end up where you are heading.”

- Lao Tzu
It’s Hackers All The Way Down

(Story Time)
Problems with Traditional Approach to AppSec

- Does not scale
- Security perspectives are not applied throughout SDLC
- Security feedback to teams arrives too late in the SDLC
- Limited time windows for pentest by InfoSec team
It’s Hackers All The Way Down
It’s Hackers All The Way Down

**OPINION**
The cybersecurity skills shortage is getting worse
More than half of organizations report a “problematic shortage” of cybersecurity skills, and there is no end in sight.

**CYBERSECURITY**
A serious shortage of cybersecurity experts could cost companies hundreds of millions of dollars

**Too few cybersecurity professionals is a gigantic problem for 2019**

Robert Ackerman
@RobAckerman
6:30 am PST
January 27, 2019
It’s Hackers All The Way Down

Breaches / Data Exposures Have Become Common Occurrence
It’s Hackers All The Way Down

Data Breaches Expose 4.1 Billion Records In First Six Months Of 2019

Davey Winder
Senior Contributor to Cybersecurity
I report and analyse breaking cybersecurity and privacy stories
It’s Hackers All The Way Down

A public Jenkins server exposed source code, plaintext passwords, and more data from GE Aviation’s internal commercial infrastructure.
It’s Hackers All The Way Down

Product / SDLC Infrastructure
Increasingly Targeted
It’s Hackers All The Way Down

“It took us awhile to figure out what was going on. The bug was not in git, it was malicious code injected into compromised build infrastructure.”
By training Product teams in adversarial hacking skills, the SDLC becomes inoculated throughout all phases and team positions.
It’s Hackers All The Way Down

Developers Are A Natural Fit

• Developing is hacking
  • Creating things & new solutions
  • Adversarial hacking is just a specific form of hacking
• Technical skills
• Generally Creative Mindset
• Insider Knowledge
It’s Hackers All The Way Down

Experience with QA has been more mixed

- Some have traits of developers
- Others tend to be script-driven & less technical
- Limited ability to triage & identify false positives
It's Hackers All The Way Down

What Could Possibly Go Wrong?
It’s Hackers All The Way Down

“Here Be Dragons”

• Attack Traffic Everywhere (Attribution / Ops Impact)
• Drifting Out Of Scope
• SOC may desensitize to attack traffic on critical networks
• And…
It’s Hackers All The Way Down
It's Hackers All The Way Down

“Here Be Dragons” (cont.)

• Newly unleashed HackerDevs may stray into downloading & executing unvetted adversarial tools, POCs, and code samples

• Already part of their Dev workflow (open source, CodeGuru, etc.) but the hacking realm has extra pitfalls

• Fun conversation with Legal, Compliance, HR, and all of their friends
It’s Hackers All The Way Down

Taming the Dragons

- Legal / Compliance / InfoSec create clear policies & procedures for tools & activities
- Training covering the policies & procedures
- Coordinate carefully between Product team and InfoSec
  - Communicate adversarial activity windows & sources
- Clearly documented scope
Jumpstarting Your Own Adversarial Product Team
It’s Hackers All The Way Down

Sell It To Upper Management

• Address concerns (via policies & procedures)
• Helps to close the resource gap
• Improves development velocity due to reduced resource bottlenecks
• Improves security due to adversarial mindset in effect throughout the SDLC
It’s Hackers All The Way Down

**Sell It To Product Teams**

- Boost your résumé
- Save time in pentests
- Have fun on the side with external Bug Bounty programs
- YOU’RE GETTING TRAINED & PAID TO HACK
It’s Hackers All The Way Down

Sell It To InfoSec

- Improves security due to adversarial mindset in effect throughout the SDLC
- Reduces pressure on AppSec pentesting teams
- Builds internal allies
- Builds internal list of potential candidates for lateral move onto InfoSec / AppSec teams
It’s Hackers All The Way Down

Questions