Demystified DevSecOps
Navigating around Pitfalls

Shannon Lietz  (@devsecops)
<table>
<thead>
<tr>
<th>Year</th>
<th>DEVELOPER</th>
<th>SECURITY</th>
<th>OPERATIONS</th>
<th>&quot;DEVSECOPS&quot;</th>
<th>&quot;RUGGED&quot;</th>
</tr>
</thead>
<tbody>
<tr>
<td>1984</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1989</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1996</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2001</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2011</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PRESENT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Take Responsibility. Give Credit.

@seniorstoryteller

---

**SAFER SOFTWARE SOONER**

---

**IANS**

---

**DEVSECOPS**

---

**HACKERGIRL**

---

**All Day DevOps**

---

*Stripes*

<table>
<thead>
<tr>
<th>Red Team</th>
<th>Red Team</th>
<th>Red Team</th>
</tr>
</thead>
<tbody>
<tr>
<td>Someone said she was born with striped hair</td>
<td>I dunno, I found baby pics of her with striped hair</td>
<td>Whoa! Did they hack her chromosomes or something?</td>
</tr>
<tr>
<td>Nah, man, no way that's natural!</td>
<td>We should be more suspicious of her.</td>
<td>I dunno but she might be the first mutant with striped hair that doesn't sleep.</td>
</tr>
<tr>
<td>shh! She comes!</td>
<td>Hey guys, don't forget I see around corners, have super powers and I'm an alien. Or maybe your recon is wrong.??</td>
<td>She comes!</td>
</tr>
<tr>
<td>Your Level</td>
<td>Your Interest</td>
<td></td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------------------</td>
<td></td>
</tr>
<tr>
<td>▼Beginner</td>
<td>Getting started</td>
<td></td>
</tr>
<tr>
<td>✤ Mid-Level</td>
<td>Making more progress</td>
<td></td>
</tr>
<tr>
<td>★★ Advanced</td>
<td>Efficiencies of Scale</td>
<td></td>
</tr>
</tbody>
</table>
Cloud growth is exponential!!

• Public Cloud adoption is accelerating at a rapid pace...

• Software defined environments allow scale to happen and more decisions to be made daily...

• More people can experiment, learn and fail at a rapid pace to solve for customer demand....

• Creativity is the next frontier...

DevOps hiring is up ~2000% in last 5 years!

• Imagine solving the world’s problems faster by collaborating and taking responsibility.

• In connection with Cloud Computing, *DevOps is the cultural enabler* needed to scale creativity and innovation.

• With the goal of solving customer problems faster, no wonder DevOps is taking over.
Is bureaucracy getting in the way of Continuous Deployments and Real Security?

YOU

Hopefully it’s not going to be another round of “No’s”…

CISO

YOUR CUSTOMER

Why does it take so long for features?
What’s Happening?

value

visible

rugged software
customer-driven innovation
custom-built
product (+rental)
commodity (+utility)

invisible

transparent security
fewer better suppliers
cloud
compute

devsecops
security as code
fewer better suppliers
red team
penetration testing

devops
continuous deployment
compliance as code

customer
domain names
search engine
informational website

agile
continuous integration
traditional security

traditional SDLC

traditional
security

web app
informational website

red team
penetration testing

security as code
compliance

compute

flexible

compute

flexible

compute

Flexibility

flexible

compute

flexible

compute

commodity bound

growth

emerging

Catching up takes commitment

✥
What is DevSecOps?

DevSecOps is the practice of developing safer software sooner by involving all needed parties in the creative process and practicing continuous improvement from high fidelity actionable feedback with context.

**IS**
- A Mindset and Holistic Approach
- A Collection of Processes & Tools
- A Means of Building Security and Compliance into Software
- A Community Driven Effort
- A Strategy Driven by Learning and Experiments

**IS NOT**
- A One-Size-Fits-All Approach
- A Single Tool or Method
- Just a means of adding Security into Continuous Delivery
- Invented by Vendors
- A Strategy Driven by Perfection and Compliance

Shares concepts with Rugged Software, Rugged DevOps, SecDevOps, DevOpsSec, DevOps
Leaning in over Always Saying “No”
Data & Security Science over Fear, Uncertainty and Doubt
Open Contribution & Collaboration over Security-Only Requirements
Consumable Security Services with APIs over Mandated Security Controls & Paperwork
Business Driven Security Scores over Rubber Stamp Security
Red & Blue Team Exploit Testing over Relying on Scans & Theoretical Vulnerabilities
24x7 Proactive Security Monitoring over Reacting after being Informed of an Incident
Shared Threat Intelligence over Keeping Info to Ourselves
Biggest Pitfalls...

1. Cloud is just a fad...
2. DevOps is fleeting...
3. We’re good with our traditional security program...
4. Mistakes are unacceptable!
5. We can find all security issues before launch...
6. Compliance gives us everything we need...
7. We’re under the radar...
8. Our penetration tests haven’t surfaced any of these issues...
9. Our company isn’t ready yet...
10. We’re a waterfall shop...
## DevSecOps Maturity Model & Behaviors

<table>
<thead>
<tr>
<th>Insanity</th>
<th>Reactive</th>
<th>Proactive</th>
<th>Measurable</th>
<th>Continuous</th>
</tr>
</thead>
<tbody>
<tr>
<td>Burp</td>
<td>Crawl</td>
<td>Walk</td>
<td>Run</td>
<td>Fly</td>
</tr>
</tbody>
</table>

### Culture
- **Surprising with lots of Push Back**
- **Full Awareness but Feeling Helpless**
- **Integrated & Talked about by Execs; Feedback loop integrated**
- **Measured by Execs**
- **Context driven decisions**

### Skills
- **Skills developed outside of job function**
- **Skills lining up with job functions**
- **Skill development paired with job**
- **Proactive skill development to meet roadmap demands**
- **Knowledge evolves inline / Lessons savored**

### Program / Outcomes
- **Just getting by**
- **Orderly Processes & Faster Reactions**
- **Reduced number of Incidents**
- **Measurable difference in attacks**
- **Predictive & Proactive**

### Security Priorities
- **P0/Critical Waiting for Attackers**
- **P0 and P1s Some Hygiene**
- **P0 and P1s Compliance**
- **Attack Surface driven & measured**
- **Stay ahead of Bad guys**
Security Hierarchy of Needs at RSA

- Security controls can be simplified for easier adoption and 80% protection using the Security Hierarchy of Needs.

- All of these categories are applicable to any environment.

- Simplifying provides an easier path to success in critical control categories.

What we’ve learned

The Rise of Purple Teams at RSA


• Prove it!

• Why not test like attackers do and get ahead of them?

• Finding problems and reporting has a serious advantage over simply complaining that nobody is listening...
DevSecOps Playbook at SANS

https://www.sans.org/reading-room/whitepapers/analyst/devsecops-playbook-36792

• DevSecOps Playbooks are everywhere and the community is vibrant

• Regardless of “how” you implement for your culture, use playbooks to learn but not follow to the letter...

• Don’t make the mistake of oversimplifying...
The Tao of Security Science at RSA


• Security science is at the heart of the change for DevSecOps.

• Finding ways to chip away at difficult issues is not insurmountable...

• Gathering data early and leveraging it to learn makes all the difference.

"Nothing is more soft and yielding than water, yet for attacking the solid and the strong, nothing is better." - Tao Te Ching (chapter 78)
Security as Code at SANS


- Security is migrating into code.
- It’s time to find the skills and know how to make security decisions with context.
- Don’t underestimate the simple mistakes...

It’s time to shift...

- From THIS:
- To THIS:

Type: "AWS::EC2::SecurityGroupIngress"
Properties:
  CidrIp: String
  CidrIpv6: String
  FromPort: Integer
  GroupId: String
  GroupName: String
  IpProtocol: String
  SourceSecurityGroupName: String
  SourceSecurityGroupIpd: String
  SourceSecurityGroupOwnerld:
Adversary interest and feedback loops are critical to prioritization...

Given thousands of component parts, it’s important to trend your adversaries.

P0 and P1s should never persist since security simply degrades over time.

---

Security Facts

- Original Lines of Code: 300
- Open Source Components: 26
- Type: Embedded
- Version: 1.0
- Intended Version Lifetime/Expiration: 02/2020
- Organization Security Trend at Release: 3.2
- Security Degradation Rating: A
- Request Monthly Customer Maintenance: 2

**% Control Values**

- **Adversary Interest**: 97%
- **Residual Risk**: 8%
- **Preventative Measures**: 93%
  - Access Control: 100%
  - Encryption: 95%
  - Tamper: 91%
- **Detective Measures**: 90%
  - Remote: 90%
  - Local: 90%

*All values are based on modeled Abuse and P&ME造成 for this class of device and appropriate implementation patterns. Your results may fluctuate according to intended business risk profile and operational tolerances that allow for some controls to be less extensive. Actual results may also vary with creative use or experimental implementation.*
DevSecOps Lessons at OWASP

https://vimeo.com/210478219

- Time to focus on component parts to get rid of exploitable attack surface.

- Supply chain issues must be measured to get better.

- Focusing on just the SDLC is not the sole essence of this challenge...
Full Stack Attack at RSA


- Attack Surface is what matters most...

- Attack Maps provide the basics faster than other methods.

- Measure and learn in order to stay ahead.
What’s the best way to organize around it?
How will I know when I am doing it well?

You can get ahead of attackers sooner in the pipeline.
How hard could it be?
Is there some science behind all of this?

**LOCKHEED’S KILL CHAIN**

- **Left of Hack**
  - **Prevention & Detection**
    - Recon
    - Weaponize
  - Recon
  - Delivery

- **Right of Hack**
  - **Incident Response & Forensics**
    - Control
    - Execute
  - Maintain

**MITRE CAPEC**

- % Adjusted for Related Attack Methods

**MITRE ATT&CK**

- % Adjusted for Attack Surface & Environment

**PREDICT**

- Target: 80%

**PREVENTION PATTERNS & CONTROLS**

**DETECTION RULES & PROCESSES**
With your help, Software Safer Sooner can be a reality…

catching up takes commitment
Get Involved and Join the Community

- devsecops.org
- @devsecops on Twitter
- DevSecOps on LinkedIn
- DevSecOps on Github
- RuggedSoftware.org
- Compliance at Velocity