Establishing a DevSecOps Program

Shannon Lietz

DevSecOps Leader &
Sr. Mgr Cloud Security Engineering at Intuit
Who I am

- 25+ years Technology and Security Experience
- Background in Security R&D
- Working with the Cloud before it was called the “Cloud”
- Manage my teams using DevOps and Scrum
- IR & Crisis Management
How was DevSecOps discovered?

Securing at the rate of Innovation...

- Pain
- Trial & Error
- Blood, sweat & tears
- Ouch, my head hurts!

It would have been great to hear this talk a couple years ago....
Case for Change

• DevOps, Agile and Scrum on the rise...
• Workload migrations to software defined environments....
• Enterprises increasingly turning to Public and Private Cloud Providers...
• Talent migrating to progressive companies willing to embrace change...
• Start-ups now have game changing capabilities available for rent... Public Cloud
• Competitive landscape has been changing...
What is DevSecOps?

Problem Statement

• DevOps requires continuous Deployments
• Fast decision making is critical to DevOps success
• Traditional Security just doesn’t scale or move fast enough...

Welcome DevSecOps!!

• Customer focused Mindset
• Scale, Scale, Scale
• Objective Criteria
• Proactive Hunting
• Continuous Detection & Response
Emerging Security Trends

• Shortage of Security Professionals
• Big companies are attempting to scale security to move faster: Facebook, Netflix, LinkedIn, AWS, Intuit
• Industry Leaders talking about the integration of DevOps & Security: Joe Sullivan, Jason Chan, Gene Kim, Josh Corman
• Introduction of DevSecOps at MIRCon in 2014
• SecDevOps at RSA 2015 was full day of dedicated content
• LinkedIn People Search: 8 DevSecOps, 7 SecDevOps, 7 DevOpsSec, 29k+ Cloud Security

@Secure360 or #Sec360 www.Secure360.org
The Art of DevSecOps

DevSecOps

Security Engineering

Security Operations

Compliance Operations

Security Science

Experiment, Automate, Test

Hunt, Detect, Contain

Respond, Manage, Train

Learn, Measure, Forecast
Getting Started

Some basic principles:

• You don’t need to do all of DevSecOps at once.
• Small security teams can have a profound impact.
• Organize around self-service.
• Figure out how to communicate security for the layperson.
Path to DevSecOps

Security as Code?

Security Operations?

Compliance Operations?

Science?

Experiment: Automate Policy Governance

Experiment: Detection via Security Operations

Experiment: Compliance via DevSecOps toolkit

Experiment: Science via Profiling

DevOps + Security

DevOps + DevSecOps

Start Here?
The DevSecOps Mindset

• Customer Focus
• Open & Transparent
• Iteration over Perfection
• Hunting over Reaction

• Hmmm - wait a minute, this sounds like a manifesto -> insert shameless plug here: http://www.devsecops.org
What’s the Work of a DevSecOps Team?

Imagine that you will need to support all facets of security inline with development teams and at speed...

• Do you have **enough security experts** to embed resources in DevOps teams?

• Have you got amazing talent that would **rather hunt** for Security defects than create value?

• Are you ready to invest in **Self-Service** for Security?

• Are you working with a Cloud environment and can **your team code**?
### Ready to make these decisions?

<table>
<thead>
<tr>
<th>Who is responsible?</th>
<th>On-Prem</th>
<th>Partial On-Prem</th>
<th>Outsource w/ No Indemnif.</th>
<th>Outsource w/ Part.Indemnif.</th>
<th>Outsource w/ Full Indemnif.</th>
</tr>
</thead>
<tbody>
<tr>
<td>You</td>
<td>You</td>
<td>You</td>
<td>You</td>
<td>You + Partner</td>
<td>Partner</td>
</tr>
<tr>
<td>Physical Security;</td>
<td></td>
<td>File or Object</td>
<td>File or Object Encryption</td>
<td>File or Object Encryption</td>
<td>Partner Security Controls;</td>
</tr>
<tr>
<td>Secure Handling &amp;</td>
<td></td>
<td>for Sensitive</td>
<td>for Sensitive Data;</td>
<td>for Sensitive Data;</td>
<td>SOC Attestation</td>
</tr>
<tr>
<td>Disposal</td>
<td></td>
<td>Physical Security;</td>
<td>Partner Security;</td>
<td>Partner Security;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Secure Handling</td>
<td>SOC Attestation</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&amp; Disposal</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Where does data transit and get stored?**

<table>
<thead>
<tr>
<th>INTERNAL</th>
<th>PARTNERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>company “owned”</td>
<td>managed services;</td>
</tr>
<tr>
<td>data center or</td>
<td>SaaS; private</td>
</tr>
<tr>
<td>co-location</td>
<td>cloud</td>
</tr>
<tr>
<td>reduced latency;</td>
<td>speed; reduced</td>
</tr>
<tr>
<td>search sensitive</td>
<td>friction;</td>
</tr>
<tr>
<td>data</td>
<td>search sensitive</td>
</tr>
<tr>
<td></td>
<td>data</td>
</tr>
<tr>
<td></td>
<td>speed; reduced</td>
</tr>
<tr>
<td></td>
<td>friction;</td>
</tr>
<tr>
<td></td>
<td>evolving patterns;</td>
</tr>
<tr>
<td></td>
<td>community</td>
</tr>
<tr>
<td></td>
<td>speed; reduced</td>
</tr>
<tr>
<td></td>
<td>friction;</td>
</tr>
<tr>
<td></td>
<td>evolving patterns;</td>
</tr>
<tr>
<td></td>
<td>community</td>
</tr>
<tr>
<td></td>
<td>speed; reduced</td>
</tr>
<tr>
<td></td>
<td>friction;</td>
</tr>
<tr>
<td></td>
<td>indemnification</td>
</tr>
</tbody>
</table>

**What are the innovation benefits?**

| SQL Injection;       | Latency; SQL Injection; | Inability to Search Sensitive Data; | Inability to Search Sensitive Data; |
| Internal Threats;    | Latency; Internal Threats; | SQL Injection; | SQL Injection; |
| Mistakes; Phishing;  | Mistakes; Phishing; | Internal Threats; | Internal Threats; |
| Increased Friction;  | Increased Friction; | Mistakes; Phishing; | Mistakes; Phishing; |
| Slow                 | Slow                | Govt. Requests Unknown; | Govt. Requests Unknown; |
|                      |                     | Reduced Financial | Reduced Financial |
|                      |                     | responsibility     | responsibility     |
|                      |                     |                      |                      |
|                      |                     |                      |                      |

**What are the potential risks?**

| SQL Injection;       | Latency; SQL Injection; | Inability to Search Sensitive Data; | Inability to Search Sensitive Data; |
| Internal Threats;    | Latency; Internal Threats; | SQL Injection; | SQL Injection; |
| Mistakes; Phishing;  | Mistakes; Phishing; | Internal Threats; | Internal Threats; |
| Increased Friction;  | Increased Friction; | Mistakes; Phishing; | Mistakes; Phishing; |
| Slow                 | Slow                | Govt. Requests Unknown; | Govt. Requests Unknown; |
|                      |                     | Reduced Financial | Reduced Financial |
|                      |                     | responsibility     | responsibility     |
|                      |                     |                      |                      |
|                      |                     |                      |                      |

@Secure360 or #Sec360

www.Secure360.org
Or set up “policies” that look like this...

{
    "Version": "2015-05-09",
    "Statement": {
        "Effect": "Allow",
        "Action": [
            "iam:ChangePassword",
            "iam:GetAccountPasswordPolicy"
        ],
        "Resource": "*"
    }
}
And how do you hunt for security issues in software defined environments?

**The Full Stack Hack**

1. Cloud DNS Reveals Private IP of web server
2. Private IP of web server reveals detailed errors or admin interface
3. SSRF or XXE vulnerability exposes Metadata, revealing API Keys
4. API Key allow you to escalate privileges clone system root partition
5. Cloned system gets you SSH keys to app servers and API key with full access
6. With new credentials create trust relationship with external account and clone DB for quiet extraction

---

@Secure360 or #Sec360

www.Secure360.org
Can you communicate security complexity using simple processes?

1. Discover
2. Evaluate
3. Control
4. Communicate
More importantly, how do you translate?

begin

(iam.client.list_role_policies(:role_name => role)[:policy_names]
 - roledb.list_policies(role)).each do |policy|
log.warn("Deleting Policy "#{policy}", which is not part of the approved baseline.")
if policydiff('{}',
  URI.decode(iam.client.get_role_policy(
    :role_name => role,
    :policy_name => policy
  )[:policy_document]),
{argv => ARGV, :diff => options.diff})
end
options.dryrun ? nil : 
  iam.client.delete_role_policy(  
    :role_name => role,  
    :policy_name => policy
)

end

Account Grade:

B

Heal Account?

Account Grade:

B

Heal Account?
Consider the DevSecOps Approach: Incident Drive Development (IDD)

- Share your Security Tools within everyone in your organization
- Everything is an incident, how you deal with it is a matter of priority and severity
- Running campaigns & internal bounty programs, consider giving out t-shirts
- Use your security experts as scientists
- Keep Investigations separate
Your environment should look something like this...

AWS accounts
EC2
CloudTrail
S3
Glacier

ingestion

security tools & data

threat intel

security science

insights

Securi360 conference

Celebrating a decade of guiding security professionals.

@Secure360 or #Sec360

www.Secure360.org
And your team will need to operate like this…

How did we decide which roles would be deployed?
- Human
  - IAM Admin
  - Incident Response
- Read Only
- Services
  - IAM Grantor
  - Instance Roles required to support security services
  - Read Only
It’s not easy but it can make a difference...

• Security stops being the reason nothing gets done.
• Everyone in your organization is responsible for security.
• Security can be a differentiator in most organizations and leads to its own innovation discovery.
Vendors embracing DevSecOps

- AWS
- TAP by Mandiant
- SumoLogic
- Splunk
- OpenDNS

- Evident.io
- AlertLogic
- Tanium
- Outlier Security
- Continuum Security
Resources

• http://www.devsecops.org
• @devsecops
• LinkedIn Group: DevSecOps
• Github: DevSecOps

• shannon@devsecops.org