Securing Infrastructure as Code

Alex Bauert
Zoa Buske
Nathan Larson
Alex Bauert has been working on App Sec for over 15 years in various roles. He has participated in OWASP for 10 yrs and spoken at several OWASP events.

Zoa Buske was a Software Engineer for over 20 years, during which she was a Security advocate in all things. She moved to InfoSec and AppSec a year and a half ago. She has been a local OWASP member since 2013 and has recently joined the leadership team.

Nathan Larson wrote bug-ridden, vulnerable software for two decades before wandering into an OWASP talk and catching the cyber security bug. For the last ten years he’s held himself up as an example to developers of what not to do. His favorite AppSec defect is still SQLi.
Agenda

- Immutable infrastructure
- Testing and Validation for IaC
- Fitting IaC into the AppSec Pipeline
- Threats, Vulnerabilities, Remediation
- IaC best practices
- Is it Security Architecture or Secure Coding?
Ground Rules and Expectations

- Interactive
- Share the knowledge/experience
- Presenting base info and Topics
- Did we mention Interactive?
- No Silver Bullets in the presentation
“A computer lets you make more mistakes faster than any other invention with the possible exceptions of handguns and Tequila.”

— Mitch Ratcliffe
Immutable Infrastructure
Mutable Architecture

- Mutable architecture came from time of hardware servers
  - Each server is an individual
  - Difficult and expensive to reproduce and replace
  - All configuration is manual
  - Configuration drift
  - Poorly understood configuration
Immutable Architecture

- Immutable Architecture came with virtualization
  - Simple, Reliable, Consistent
  - All changes to an environment are made in the code
  - Validated and version-controlled images
  - Designed to be unchanged after deployment
Testing and Validation for IaC
Testing and Validation

- Continuously test and monitor your deployments
- Automated Tests checked in with code
- Use Threat Modeling to inform test
- Automate monitoring and alerts
Fitting IaC into the AppSec Pipeline
The Flow

- Infrastructure Design
- Configuration Management
  - Coding
- Change Management
  - Test & Validate
- Deploy infrastructure
- Maintenance
  - Patch
IaC SDLC

Engineers → Repository → CI/CD → Cloud
IaC Best Practices
Best Practices

- Codify everything
- Document nothing
- Use version control
- Test, deploy, monitor
- Embrace Modularity
Codify Everything

- Environment
- Components
- Configuration
Document Nothing

- Code is:
  - Authoritative record
  - Complete
  - Explicit
- No other documentation needed
Use Version Control

- Protects the code
  - Management
  - Logging
  - Merging
  - Auditable
Test, Deploy, Monitor

- Use the SDLC
  - Test
  - Deploy
  - Monitor
  - Repeat
Embrace Modularity

- Small modules
- Minimize dependencies
- Cohesive
- Better access controls
- Improved debugging
Threats, Vulnerabilities and Remediation, Oh My
Threats

- The Insider
  - Access to everything
  - Across scale
    - Configuration Management
    - Coding
  - Deploy infrastructure

- Configuration Management
  - Templates - 200k misconfigured with vulnerabilities
    - Palo Alto Paper on Cloud Threats
  - Managing Secrets
Part of Supply Chain

- Configuration Management
  - Coding
- Deploys infrastructure
- Validate before deployment
  - Code Review/Testing
  - Check in
  - Validate configuration items
Perspectives

● Tool chain
  ○ Configuration Management
  ○ Coding
  ○ Deployment

● Process
  ○ Pipeline
  ○ Logical Access Management
  ○ Maintaining/Validating the Configuration Templates
## Top 10 Findings in CloudFormation

<table>
<thead>
<tr>
<th>Policy Name</th>
<th>Misconfigured %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon RDS event subscription disabled for DB security groups</td>
<td>99.00%</td>
</tr>
<tr>
<td>AWS Access logging not enabled on S3 buckets</td>
<td>55.33%</td>
</tr>
<tr>
<td>AWS S3 buckets do not have server-side encryption</td>
<td>48.46%</td>
</tr>
<tr>
<td>AWS security group allows traffic from blocked ports</td>
<td>16.96%</td>
</tr>
<tr>
<td>AWS (virtual private cloud) VPC subnets should not allow automatic public IP assignment</td>
<td>6.74%</td>
</tr>
<tr>
<td>Amazon RDS instance with Multi-Availability Zone disabled</td>
<td>43.56%</td>
</tr>
<tr>
<td>AWS S3 buckets are accessible to the public</td>
<td>13.22%</td>
</tr>
<tr>
<td>Amazon RDS instance is not encrypted</td>
<td>41.66%</td>
</tr>
<tr>
<td>Amazon RDS instance with copy tags to snapshots disabled</td>
<td>41.11%</td>
</tr>
<tr>
<td>AWS ECS task definition readonlyRootFilesystem not enabled</td>
<td>86.39%</td>
</tr>
</tbody>
</table>

*From the Palo Alto Cloud Threat Report - Spring 2020*
Top 10 Findings in Terraform

<table>
<thead>
<tr>
<th>Policy Name</th>
<th>Misconfigured %</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS Security Groups allow internet traffic to SSH port (22)</td>
<td>26.61%</td>
</tr>
<tr>
<td>AWS EC2 instance have SSH port open to the internet</td>
<td>26.61%</td>
</tr>
<tr>
<td>AWS Security Group allows traffic from blocked ports</td>
<td>26.38%</td>
</tr>
<tr>
<td>AWS Security Groups with Inbound rule overly permissive to All Traffic</td>
<td>17.92%</td>
</tr>
<tr>
<td>AWS Access logging not enabled on S3 buckets</td>
<td>66.58%</td>
</tr>
<tr>
<td>AWS S3 object versioning is disabled</td>
<td>51.60%</td>
</tr>
<tr>
<td>Amazon RDS event subscription disabled for DB security groups</td>
<td>99.57%</td>
</tr>
<tr>
<td>Storage Accounts without Secure transfer enabled</td>
<td>97.56%</td>
</tr>
<tr>
<td>Amazon RDS snapshots are accessible to the public</td>
<td>79.16%</td>
</tr>
<tr>
<td>AWS ECS task definition execution IAM role not found</td>
<td>70.57%</td>
</tr>
</tbody>
</table>

*From the Palo Alto Cloud Threat Report - Spring 2020*
Flow

● Configuration Management
● Coding
● Change Management - Approval
● Test & Validate
● Deploy infrastructure
● Maintenance
  ○ Patch
  ○ Update configuration
Prevent-Detect

Having a process
- Design is a prerequisite
  - Contextualized Requirements
- Coding & Templates
  - Adding the testing to the cycle
- Test & Validate
  - Code
  - Configuration values
Is it Security Architecture or Secure Coding?
Discussion
References

https://www.digitalocean.com/community/tutorials/what-is-immutable-infrastructure
https://dzone.com/articles/infrastructure-as-code-security
https://blog.sensu.io/infrastructure-as-code-testing-and-monitoring
https://geekflare.com/iac-security-scanner/