Implementing and maintaining a DevSecOps approach in the cloud

George Gerchow - VP of Security & Compliance @sumologic
Agenda

• The Sumo Cloud
• DevSecOps = Baking Security into your DNA
• Sumo Logic Security & Compliance Strategy
• The Cloud Attack that never seems to go away
• Looking to the future of Cloud Security
About Sumo Logic

- Big Data Analytics Company
- Born in the Cloud Seven Years Ago
- Multi Tenant Saas Based Solution
- We were founded with a security first mindset
Sumo Logic at Scale in the Cloud

1,300+ Customers in the cloud

100+ PB Data Analyzed Daily

10K+ EC2 Instances

10M+ Keys Under Management

SECURITY BAKED IN
DevSecOps = Security DNA

- Security Starts with Engineering
- How to "Encourage" good security hygiene in engineering
- A simple engineering mistake can lead to an attack
- Change Management in a DevSecOps world
"Security must be more tightly integrated into the DevOps process to deliver a DevSecOps process that builds in security from the earliest stages of application design."

Gartner Top 10 Strategic Technology Trends for 2016: Adaptive Security Architecture

http://www.gartner.com/document/3225617
How to start ”Baking” Security into your Company DNA

• Review and release code in small chunks
  – We do two week sprints, but stage daily

• Empower the Developer with Security Training
  – When was the last time you sent Dev Types to DefCon?

• A DevSecOps Process Approach
  – Breaking down the future of Change Management
Change Management the DevSecOps way

• The goals for our change management process are that:
  – Anybody can propose a change to the production system, at anytime, and anybody can follow what changes are being proposed.
  – A well-known set of reviewers can quickly and efficiently review changes and decide on whether to implement them.
  – Any change to production needs to leave an audit trail to meet compliance requirements.

• A typical system change request goes through these steps:
  – Create the JIRA issue.
  – Propose the system change request to the Change Management Board.
  – Get three approvals from members of the Change Management Board.
  – Implement the change.
  – Close the JIRA issue.
  – If the CMB rejects the change request, we simply close the JIRA issue.
Getting to a Decision Quickly

- To get from a proposal to approved change in the most expedient manner, we have a dedicated #cmb-public channel in Slack. The typical sequence is:
  - Somebody proposes a system change in the Slack channel, linking to the JIRA ticket.
  - If needed, there is a brief discussion around the risk and details of the change.
  - Three of the members of the CMB approve the change in JIRA.
  - The requester or on-calls implement the change and mark the SCR implemented.
  - Sumo Logic Change Management Board sumobot plugin
    - [https://gist.github.com/weirded/572619a0d3f522a03e5e](https://gist.github.com/weirded/572619a0d3f522a03e5e)
Sumo Logic Security & Compliance Strategy

- Four Areas of combined focus
- Don’t be a speed bump, stay agile
- Identifying CSP useful offering and gaps
- It takes a neighborhood, there is no silver bullet
Security & Compliance Strategy

- Platform Security
- Continuous Monitoring
- Endpoint Protection
- Compliance
People - Team Dynamics

Security and IT ops

Cloud EnG DevOps
The Defense in Depth Approach

Encryption and Key Management
Vulnerability Management

Testing Program

• Every 6 Months
  – IOActive Full Penetration Test
  – IOActive Collector Code Review

• Every Quarter
  – Rapid7 ASV Scans

• Every Week
  – Fully Credentialed Rapid7 Scans of each Build prior to staging

• Every Day
  – Fully Credentialed Rapid7 Scans of every new server instance

Remediation SLA

• Critical Issues
  – Remediation efforts begin immediately, target to patch within 24 hours.

• High Severity issues
  – Remediated within 5 days

• Medium Severity issues
  – Remediated within 60 days

• Low severity issues
  – Addressed in accordance with their business and customer impact
Sumo Logic Compliance
Protecting Customer Data with Best-in-Class Security

- PCI/DSS 3.1 Service Provider Level 1 Certified (3.2 Pending)
- SOC 2 Type attestation
- ISO 27001 certified
- CSA Star certified
- HIPAA-HITECH compliance
- U.S. – EU Privacy Shield
- AES 256-bit encryption at rest
- TLS encryption in transit
- FIPS 140-2 compliant
Tools – CSP Offerings for AWS Operational & Security Visibility
CSP Gaps filled with 3rd party providers

Functional Areas:
• Threat Intelligence
• File Integrity Monitoring
• IDS
• End Point Protection
• Security Analytics

Shared responsibility
The Cloud Attack that never goes away

- Password Hygiene is still the #1 threat to security
- People who should be the most responsible are not
- Audit everything
- BitCoin Miners
- Future of Cloud Security
Bitcoin mining in AWS

**Seeking Free Compute Power! please put your AWS credentials into a config file and upload to GitHub**

- Only 21 Million BitCoin Allowed to be Mined
- International Non Regulated Currency
- AWS GPU EC2 P2 Instances are perfect for mining Bitcoins
- Use two-factor authentication.
- Never hardcode your cloud computing credentials
- Use Identity Access Management

“Don’t put your Amazon credentials into source code and then share that source code in a public place like GitHub!”
Big DDoS attacks affect some Amazon Web Services customers, but AWS chief Andy Jassy assures cloud is secure

- Recent DDoS attacks targeted Dynamic Network Services Inc., better known as Dyn
- Dyn is one of many DNS providers to AWS
- AWS has some services (Shield) in place to help, and we have 3rd party tools but...
- Could AWS eat itself or be used to attack Azure in Mass?

“Security may be critical, but “agility is the single biggest reason enterprise are moving to the cloud”

The latest Akamai security report highlights a 138 percent YoY increase in total DDoS attacks greater than 100 Gbps, with two record DDoS attacks caused by the Mirai Botnet.
In Summary

Simplicity & visibility = scale

DevSecOps: Do more with less

Visibility & compliance
Questions and thank you!