Cloud Forensics – Finding the Needle

Bill Murray, Director – AWS Security Programs

March 24, 2014
What is the Definition of Security?

Navy
What is the Definition of Security?

Army
What is the Definition of Security?

Marines
What is the Definition of Security?

Air Force
Shared Security Responsibilities

**AWS**
- Facilities
- Physical Security
- Physical Infrastructure
- Network Infrastructure
- Virtualization Infrastructure

**Customer**
- Operating System
- Application
- Security Groups
- Network ACLs
- Network Configuration
- Account Management
Finding the Needle

- Finding a needle in a haystack is easy
- Finding the Needle in the Stack of Needles is Hard
Prepare for SCALE!

• One Customer spun up a 50,000 core Instance
• AWS S3 Contains Trillions of Objects
• S3 Processes over 1.5 MILLION Requests/Second
• AWS Charges $ 0.09/month Per GB Of S3 Storage
  • “Glacier” storage is $0.01 per GB
  – Every day AWS adds the equivalent capacity of Amazon.com when it was a $7 Billion dollar enterprise
Perceived Challenges of Cloud 4N6

• The Distance
  – Data is in a remote facility

• The Process
  – Incident Response isn't owned by the customer

• The Toolbox
  – Where do I plug in my EnCase dongle in the cloud?
Actual Advantages of Cloud 4N6

• The Distance
  – Virtual environments allow forensic examination from anywhere
  – Time from compromise to examination greatly reduced
  – Don’t be afraid of data being everywhere

• The Process
  – Cloud environments allow customers to become proactive vice reactive to potential compromise and investigations

• The Toolbox
  – Use the tools that are provided by the CSP to help you
Be Prepared

• Create a Cloud Environment that is ready to do Forensics BEFORE you need it
  – Resource Tagging
  – Meta Data Collection
  – Validation of your VM/AMI
  – Create Forensic Security Groups with Special Permissions

• Prepare for the Worst
  – If the first time you think about cloud forensics is after a compromise – you're too late.
Forensic Capabilities in the Cloud

• More Obvious
• Less Obvious
• Proprietary
Forensic Capabilities in the Cloud

• More Obvious
  – Snapshot of instance to EBS
  – Run your own tool suite against the EBS Volume
    • EnCase
    • FTK
    • Etc
  – Memory Dumps
    • Available by request
  – Log Analysis
    • Ensure the logs go to the right place
      – Read only
      – Write Once
Audit Logs via AWS CloudTrail

- AWS CloudTrail records API calls in your account and delivers logs to your S3 bucket.
- Typically, delivers an event within 15 minutes of the API call.
- Log files are delivered approximately every 5 minutes.
- Currently in us-east-1 and us-west-2
What is in the logs?

- **Who** made the API call?
- **When** was the API call made?
- **What** was the API call?
- **What** were the resources that were acted up on in the API call?
- **Where** was the API call made from?
Write-Once Storage

• What is it good for
  – Tripwire
  – Configuration audits
  – Logs

• Integrity for records of activity, historical configurations

• Further enhanced by moving off-system or limiting availability to a VERY select few
Forensic Capabilities in the Cloud

• Less Obvious
  – Turn on Versioning
    • Allows for comparative analysis
  – Utilize Identity and Access Management
    • Create “forensic only” groups
  – Amazon Cloud Formation Error Logs
  – Determine what logging is available and use it
    • Every Service has some degree of logging
  – Amazon Cloud Trail
  – Create Security/Forensic “Roles”
What’s a Role

- Named IAM entity (name isn’t a secret)
- Set of permissions
- No credentials: Policy specifies who can assume
Security Role

- You need insight when managing the security of many cloud accounts
- Create a “security audit role” with “read” access to policies and configurations you want to monitor.
- For more info or getting started, check out http://docs.aws.amazon.com/IAM/latest/UserGuide/WorkingWithRoles.html
Forensic Capabilities in the Cloud

• Proprietary
  – Cloud Service Providers have additional tools
  – Reach out to Security and Customer Service
  – Know how to escalate!
    • AWS Customer Support is trained to escalate to the Security Team when required
Support for Security

- AWS support is the one-stop shop for AWS customers, for ANY concerns, including security-related
- If support cannot immediately address your concern, they will escalate internally to the appropriate technical team, AWS security included

https://aws.amazon.com/support
Investigation vs Forensics

• Security investigations are done all the time
• Forensics needs to catch up
  – Vetted, accepted tools and practices need updated
  – Chain of Custody needs to be altered
    • Where does the chain start?
• CSPs want to cooperate with tool developers
• Help us Help You!
4N6 in the Cloud

- The Cloud isn’t a scary place for forensics
  - We regularly see $\frac{1}{2}$ TB memory dumps
  - Customers with “Big Data” >PB!
  - Data distributed World Wide
  - Very Small SLAs for IR

The Cloud is the only place for forensics
Other Resources

- AWS Security Blog
  http://blogs.aws.amazon.com/security/
- AWS Security Center
  https://aws.amazon.com/security
- Contact the AWS security team
  aws-security@amazon.com
Thank You!

aws.amazon.com/security

bmurray@amazon.com