Digital Forensics as a Service: DFIR in the Cloud

Toni de la Fuente (@ToniBlyx :: blyx.com)
Lead Security Operations / Senior Cloud Security Architect
Once upon a time...

- Digital Forensics IN and OF the Cloud
- Generic Challenges
- Attacks
- Incident Response
- Hardening

Security IN the Cloud!
Generic Forensics Challenges
Disadvantages and Challenges

<table>
<thead>
<tr>
<th>Cloud</th>
<th>Forensics and Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ubiquity</td>
<td>Enumeration</td>
</tr>
<tr>
<td></td>
<td>Legal jurisdiction</td>
</tr>
<tr>
<td>Elasticity</td>
<td>Preservation of evidence</td>
</tr>
<tr>
<td></td>
<td>Data integrity</td>
</tr>
<tr>
<td>Data persistence (replication)</td>
<td>Chain of custody</td>
</tr>
<tr>
<td></td>
<td>Evidence integrity</td>
</tr>
<tr>
<td>Multi-tenancy</td>
<td>Data attribution</td>
</tr>
<tr>
<td></td>
<td>Chain of custody</td>
</tr>
<tr>
<td>Abstract</td>
<td>Determine the best evidence</td>
</tr>
<tr>
<td></td>
<td>Preservation and visualization of evidence</td>
</tr>
<tr>
<td>Quantity of data and Big Data</td>
<td>Systems that cannot be investigated or managed in a traditional manner</td>
</tr>
<tr>
<td>Knowledge</td>
<td>Trained staff</td>
</tr>
<tr>
<td></td>
<td>Continuous evolution and new features almost daily</td>
</tr>
<tr>
<td>Providers</td>
<td>Service level agreement / service level objectives</td>
</tr>
<tr>
<td></td>
<td>Relationship client-provider / transparency</td>
</tr>
</tbody>
</table>
# Service Level Objectives to Guarantee with Provider

<table>
<thead>
<tr>
<th>IaaS</th>
<th>PaaS</th>
<th>SaaS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provider’s network logs</td>
<td>Web server logs</td>
<td>Web server logs</td>
</tr>
<tr>
<td>DNS providers logs</td>
<td>Application server logs</td>
<td>Application server logs</td>
</tr>
<tr>
<td>Virtual machine hypervisor logs</td>
<td>Tenant operating system logs</td>
<td>Database logs</td>
</tr>
<tr>
<td>Host logs</td>
<td>Host access logs</td>
<td>Host access logs</td>
</tr>
<tr>
<td>API logs</td>
<td>Virtualization platform logs</td>
<td>Virtualization platform logs</td>
</tr>
<tr>
<td>Management portal logs</td>
<td>Management portal logs</td>
<td>Management portal logs</td>
</tr>
<tr>
<td>Packet capture logs</td>
<td>Packet capture logs</td>
<td>Packet capture logs</td>
</tr>
<tr>
<td>Billing records</td>
<td>Billing records</td>
<td>Billing records</td>
</tr>
</tbody>
</table>
# Traditional vs Cloud Forensics

<table>
<thead>
<tr>
<th>Processes</th>
<th>Traditional Forensics</th>
<th>Cloud Forensics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identification</td>
<td>Identification of an event or incident</td>
<td>Multiple tools</td>
</tr>
<tr>
<td>Preservation</td>
<td>Securitization and assessment of the scene</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Documentation of the scene</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Evidence collection: origin of the evidence</td>
<td>Physical hardware</td>
</tr>
<tr>
<td></td>
<td>Evidence collection: location of the evidence</td>
<td>Crime scene</td>
</tr>
<tr>
<td></td>
<td>Marking, packaging and transport</td>
<td>Physical</td>
</tr>
<tr>
<td>Acquisition / Extraction</td>
<td>Acquisition time</td>
<td>Slow</td>
</tr>
<tr>
<td></td>
<td>RAM acquisition</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Hash</td>
<td>Slow</td>
</tr>
<tr>
<td></td>
<td>Erased data recovery</td>
<td>Possible</td>
</tr>
<tr>
<td></td>
<td>Metadata acquisition</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Time stamp</td>
<td>Precise</td>
</tr>
<tr>
<td></td>
<td>Installation (action) of forensic software</td>
<td>Expensive</td>
</tr>
<tr>
<td></td>
<td>Configuration and availability of forensic software</td>
<td>Expensive</td>
</tr>
<tr>
<td></td>
<td>Transport</td>
<td>Yes</td>
</tr>
<tr>
<td>Analysis</td>
<td>Analysis</td>
<td>Slow</td>
</tr>
<tr>
<td>Presentation</td>
<td>Documentation of evidence</td>
<td>Acquired evidence</td>
</tr>
<tr>
<td></td>
<td>Declaration</td>
<td>Common</td>
</tr>
</tbody>
</table>
## Storage Options

<table>
<thead>
<tr>
<th>Type</th>
<th>AWS</th>
<th>Azure</th>
<th>GCP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Objects</td>
<td>S3 Object Storage</td>
<td>Azure Storage</td>
<td>Google Cloud Storage</td>
</tr>
<tr>
<td></td>
<td>• Buckets</td>
<td>• Blob storage</td>
<td>• Buckets</td>
</tr>
<tr>
<td></td>
<td>• 5TB max per object</td>
<td>• 500TB limit per storage account</td>
<td>• 5TB max per object</td>
</tr>
<tr>
<td></td>
<td>• Encryption In-flight and at-rest</td>
<td>• Encryption In-flight and at-rest</td>
<td>• Encryption In-flight and at-rest</td>
</tr>
<tr>
<td>SAN / Block</td>
<td>EBS (Volumes)</td>
<td>Azure Virtual Disks</td>
<td>Google Block Storage</td>
</tr>
<tr>
<td></td>
<td>• Volume size: 1GB to 16TB (in 1GB increments)</td>
<td>• Page blobs</td>
<td>• Volume size: 1GB to 10TB</td>
</tr>
<tr>
<td></td>
<td>• Magnetic, SSD</td>
<td>• Volume size: 32GB to 4TB</td>
<td>• Magnetic, SSD</td>
</tr>
<tr>
<td></td>
<td>• Encryption available</td>
<td>• Standard (Magnetic), SSD premium</td>
<td>• Snapshots</td>
</tr>
<tr>
<td></td>
<td>• Snapshots</td>
<td>• Snapshots</td>
<td>• Encryption by default</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Encryption available</td>
<td></td>
</tr>
<tr>
<td>NAS</td>
<td>Shared Storage (NFS4.0/4.2)</td>
<td>File Storage (SMB3.0)</td>
<td>Single Node File Server + Others</td>
</tr>
<tr>
<td></td>
<td>• EFS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Archive</td>
<td>Glacier</td>
<td>Azure Backup</td>
<td>Google Cloud Storage Nearline</td>
</tr>
<tr>
<td>Migration</td>
<td>Import Export / Snowball</td>
<td>Import Export</td>
<td>Third Party Solution (Iron Mountain, etc.)</td>
</tr>
<tr>
<td>CDN</td>
<td>AWS CloudFront (CDN)</td>
<td>Azure CDN</td>
<td>Google Cloud CDN</td>
</tr>
</tbody>
</table>

* Ephemeral, DBs, Queues, Caching and Storage GW not included
Common Attacks
Common incidents

• Top 3: EC2, IAM, S3
  – Access Keys compromise
  – Information leaks through misconfigured services or DNS
  – Phishing attacks
  – Compromised resources
  – Poisoned AMI
  – Application running in a role
  – Infection through 3rd party services

• Other services (RDS, ES, Redshift)

• What about targeted attacks?
S3 Leaks

- Time Warner (BroadSoft)
- Verizon
- Auto Lender
- U.S. Voters
- And many others!
  https://github.com/nagwww/s3-leaks

- **Amazon Macie**: Machine Learning, discover and classify sensitive data in AWS. PII or intellectual property.
Where to find AWS Access Keys...

- UserData, CloudFormation, Metadata Server
- Code: Github or other source code repositories, versions, commit history*
- Public EBS volumes
- Public AMIs
- Public S3 buckets
- Workstation or Server ~/.aws/credentials or C:\Users\USERNAME\.aws\credentials
- Containers
- Dev Tools: Vagrant images, Packer files, Bamboo, Jenkins...
- Vim swap files
- Service Providers (Slack bots, DataDog, CloudHealth, Okta, OneLogin, etc.)
- Google...

*See truffleHog from dxa4481 in Github
Some fun with Social Engineering...

Change default Spotlight shortcut and don’t trust USBs!
Incident Response
Incident Indicators

• Notifications from AWS
• Access activity (IAM)
• Billing activity (Budget alerts) new cloud IDS!
• API Logs
• CloudWatch Events/Alarms
• Service Specific Events
• Dashboards
  • CloudWatch
  • Personal Health
  • Cost Explorer

• Other
  • Third party (dedicated tools)
  • NIDS (Snort, Suricata, etc.)
  • HIDS (Wazuh/OSSEC, Osquery, rkhunter, Auditd)
  • ELK

https://cloudonaut.io/aws-monitoring-primer/
Cloud Incident Handling Workflow

1. **Incident**
   - Instance Compromise
   - Outside Info Acquisition (instance profile, endpoints, metadata, etc.)

2. **Live or Dead**
   - Live
   - Isolate it?
     - Yes
     - Apply Isolation SG
   - No
     - Stop it
     - Start Forensic Workstation
     - Take snapshot to all volumes
     - TAG Resources under investigation

3. **Dead**
   - Stop it
   - Segregate Network with Internet Access to Scan
   - Attach the Tools Volume
   - Make Volumes to Snapshots
   - Attach Volumes to Forensic Workstation
   - Attach the Evidence Collection Volume
   - Log in to the Forensic Workstation

4. **Yes**
   - Isolate it?
     - Yes
     - Attach the Evidence Collection Volume
     - Log in to the instance
     - Perform Evidence Acquisition
     - Analyze / Further Investigation
     - Create a report
   - No
     - Make API log report if enabled
     - Check new resources created
     - If found Isolate them

5. **Credential Compromise**
   - Revoke Access
   - Revoke Sessions
   - Trigger a Network Capture / VPC Logs
   - Disable Keys

6. **Pre-built Volatility profile**
   - Windows_Life_Response
   - Sysinternals
   - Nirsoft
   - FTK Imager
   - Autopsy
   - Sleuthkit
   - Hashing comparison-gold image, carving, cloud-init, search malware, IOC, etc

7. **Pre-built LiME kml mod**
   - CAINE / SIFT / DEFT
   - FCCU / HELIX3 / FIRE

8. **RAM Acquisition**
   - Perform Timeline

9. **Support Case with Provider**
   - Create Internal Case

10. **Create a report**

---

**Hashing comparison**
- Gold image
- Carving
- Cloud-init
- Search malware
- IOC
- etc.
Assets Acquisition Specific to AWS

- AWS Infrastructure Logs: CloudTrail and VPC FlowLogs
- AWS Service Logs: S3 Logs, RDS Logs, Lambda, API Gateway, Route53, CloudFront, etc.
- Additional data from AWS view: instance profile, endpoints, syslogs, screen, metadata, etc
- More Outside: Limits, check resources creation from given date (all regions)
- Host Based Logs (volume snapshot) Messages/System, security, audit, applications, etc.

Perform Evidence Acquisition
Digital Forensics as a Service? How to be Prepared

• **DFaaS: capabilities** we can use from a **cloud vendor** to perform tasks related to **Digital Forensics**

• Multi Account Strategy
  • Dedicated Account for Forensics
  • Dedicated Account for Security Operations

• Acquisition tools ready to use
  • Live Data

• Acquire data, what data?
• CIS Benchmark security assessment tool (52 checks + 20 additional)
• New “forensics-ready” group of checks:
  • Checks if you are collecting all what you may need in case of an incident
  • Forensics as a Service helper
  • CloudTrail, S3, Config, VPCFlowlog, Macie, GuardDuty, CloudFront, ES, Lambda, ELB/ALB, Route53, Redshift and more

• https://github.com/Alfresco/prowler
Prowler, specific group check for AWS forensics readiness
IRDF Automation Tools
Digital Forensics as a Service: Tools/Challenges

• **Userland / Process Memory Acquisition**
  - AWS System Manager (ssm)
  - `aws_ir, Margaritashotgun` (LiME)
  - Volatility and Rekall automation
  - **ECFS: extended core file snapshot format**
  - Containers
  - Analysis process
  - IOC
  - Something like [LibVMI](https://libvmi.org): VM introspection would help (Volatility integration)

• **Storage Acquisition and Processing**
  - Depends on the Storage used
  - Easier for EBS Snapshots → Volumes
  - [DFTimewolf](https://github.com/threat скр.) (Grr)

• **Multiple Account Tools, Resources and Vendors**
  - We don’t capture just one resource!
  - Enterprise grade

• **Processing collected data**
  - [Turbinia](https://github.com/turbinia)
  - [Plaso](https://plaso.readthedocs.io/en/latest/)
  - [Laika BOSS](https://github.com/laikabooss)
  - [BinaryAlert](https://binary.com)

• **Analyze data**
  - Timeline with ALL ACQUIRED DATA?
  - [Timesketch](https://timesketch.com)

• **EVERYTHING? Room to improve here!**
  - Multiple data formats
  - Multiple sources
  - Correlation
Threat Response Tools

• Incident Response Tool for AWS
  • [http://threatresponse.cloud/](http://threatresponse.cloud/)

• Compromised AWS API credentials (Access Keys)
  • Mitigate compromise: Lock

• Compromised EC2 instance
  • Mitigate compromise
    • Isolation
  • Collect evidence
    • Memory acquisition

• Plugins
  • gather_host (metadata, screen, console)
  • tag_host
  • examineracl_host
  • get_memory
  • isolate_host
  • stop_host
ThreatResponse: aws_ir, margaritashotgun

- Instance compromise [https://youtu.be/-dnljYRMMsU](https://youtu.be/-dnljYRMMsU)
Digital Forensic Analysis of Amazon Linux EC2 Instances

STI Graduate Student Research
by Ken Hartman - January 13, 2018 in Cloud Computing

Companies continue to shift business-critical workloads to cloud services such as Amazon Web Services Elastic Cloud Computing (EC2). With demand for skilled security engineers at an all-time high, many organizations do not have the capability to do an adequate forensic analysis to determine the root cause of an intrusion or to identify indicators of compromise. To help organizations improve their incident response capability, this paper presents specific tactics for the forensic analysis of Amazon Linux that align with the SANS Finding Malware Step by Step process for Microsoft Windows.

Kudos! Ken Hartman https://www.kennethghartman.com
Hardening
Put all what you need in your **well known AMI (gold image)**:
- Hardening applied / Tested (Packer/Vagrant)
  - CIS Benchmark!
- No configuration or access needed
- Local tools
  - Osquery / Wazuh-OSSEC / rkhunter / grr
  - Update rules / serverless
- Local configuration (SELinux/AppArmour)
  - AuditD

- Collect telemetry host network data (Snort/Suricata)

- Collect everything your provider allows you
  - Networking
  - APIs / Accesses (AWS API Call Limit)

- Red Team / Third party pentesting*
Auditing, Assessment and Hardening Tools

• AWS
  • Amazon GuardDuty
  • Amazon Macie
  • AWS Trusted Advisor
  • AWS CloudTrail
  • Amazon Inspector
  • AWS Organizations
  • AWS Config Rules
  • Alfresco: Prowler
  • Wazuh (wodle)
  • Nccgroup: Scout2
  • Netflix: SecurityMonkey
  • Capital One: CloudCustodian
  • AWS CIS Benchmark Python code and Lambda functions
  • CloudSploit
  • Widdix Hardening Templates
  • Awslimitchecker
  • Git Secrets (AWS)

• Azure
  • Security Center
  • OMS Security & Compliance
  • Azure logs Analytics
  • Windows Defender
  • Azure Op Insights
  • MWR Azurite
  • AzSDK
  • AzureStackTools

• GCP
  • Spotify: gcp-audit
  • SecurityMonkey

• ALL:
  • Analytics (ELK, Splunk, etc)
Takeaways

This presentation and some bits already available at:

https://github.com/toniblyx/SANSCloudSecuritySummit2018
Thanks!

Special Thanks to:
Ismael Valenzuela @aboutsecurity
Andrew K. @andrewkrug & ThreatResponse.cloud Team
Alex Maestretti @maestretti
Lorenzo Martinez @lawwait
Lórien Domenech @loriendr
Open Source Community improving Prowler!
Questions?

toni@blyx.com - @ToniBlyx
References

- Dr. Keyun Ruan University College Dublin, Designing a Forensic-enabling Cloud Ecosystem, 2013
- Josiah Dykstra, Digital Forensics for IaaS Cloud Computing, June 2012
- Keyun Ruan, Ibrahim Baggili (PhD), Prof Joe Carthy, Prof Tahar Kechadi University College Dublin, Zayed University, Survey on Cloud forensics and critical criteria for Cloud forensic capability: A preliminary analysis
- Keyun Ruan, Joe Carthy, Tahar Kechadi and Mark Crosbie, Cloud Forensics
- Keyun Ruan, University College Dublin, Cloud Forensics: challenges & opportunitiess, 2010
- NIST Cloud Computing Forensic Science Working Group Information Technology Laboratory, NIST Cloud Computing Forensic Science Challenges, June 2014
- Peter Mell Timothy Grance, NIST Special Publication 800-145, The NIST Definition of Cloud Computing, September 2011
- Report From the First Digital Forensic Research Workshop (DFRWS), A Road Map for Digital Forensic Research, August 2001
- Forensics-as-a-Service (FaaS): Computer Forensic Workflow Management and Processing Using Cloud. Yuanfeng Wen, Xiaoxi Man, Khoa Le and Weidong Shi
- https://static1.squarespace.com/static/5417f7f9e4b0b7770545590/t/56f3c598906340a7f6e78dbd/1458816415654/AWS_Cloud_and_Security.pdf
- Backdooring an AWS account
- Exploring an AWS account post-compromise
- Disrupting AWS logging
- AWS IAM "ReadOnlyAccess" Managed Policy is Too Permissive (For Us)
- Access Keys will kill you before you kill the password
- Account Jumping Post Infection Persistency and Lateral Movement in AWS
- Disrupt CloudTrail and pwning automation tools
- RSA 2017 talk: Cloud Security Automate or Die, same tittle as mine but a bit different approach
- RSA 2017 talk: Securing Serverless applications in the Cloud
- RSA 2017 talk: DevSecOps on the Offense: Automating Amazon Web Services Account Takeover