Cloud Incident Response

Monzy Merza
Director of Cyber Research
Chief Security Evangelist
Splunk, Inc
@monzymerza
#splunk
Cloud dependency and use
Challenges and opportunities in the cloud
A model for cloud IR
Capabilities required for cloud IR
IR scenarios
Takeaways and call to action
What if...

- Visibility was reduced
- Sensors disappeared
- Authorization was transferrable
- Trust exploitation became vector #1
What if...

- Visibility was reduced
- Sensors disappeared
- Authorization was transferrable
- Trust exploitation became vector #1

That world is now!
Cloud Service are Mission Critical

- **Business Applications:**
  - Salesforce
  - ServiceNow
  - Office 365
  - Gmail

- **Sharing and Collaboration:**
  - GitHub
  - Slack
  - HipChat

- **Storage Applications:**
  - Box
  - Google Drive
  - Dropbox

- **Infrastructure Platforms:**
  - Amazon Web Services
  - Windows Azure
  - Google Cloud Platform
Framework for Cloud IR
NIST 800-61r2
Cloud: A Behavioral Model

Identity

Interactions

Resources
Challenges to IP Stewardship

User Autonomy

Technical flexibility

Users create/modify/move/share data in<-> out and across services

Ubiquitous access - geo and device diversity

Encrypted Communication
Identities

Human

Machine
Examples of Interactions

- Create an account
- Start a machine instance
- Share a resource
- Synchronize files
- Manage a process
- Approve a transaction
Examples of Resources

- File sharing services
- Transaction services
- Customer relations management (CRM)
- Compute services
- Applications services
Why Do These Challenges Exist?

1. Local Users and Cloud Services
2. Local Users and Local Services
3. Remote Users and Cloud Services
4. Remote Users and Local Services
Cloud IR: A Simple Model

Identity Used

Interactions with resource

Resources Accessed by Identity
Applying the Simple Model
Cloud Opportunities

- APIs for operation and management
- Centralized authentication and management
- Near real-time impact of changes
- Logging capabilities
Preparing: Resources Accessed

Identify the cloud resources
- Web logs
- Next generation firewall application logs

Determine the methods of collection
- Log files
- API calls

Requirements for automation
- Configuration changes
- Special API keys, licenses
Preparing: Identity Used

- Log User Access
  - On-prem resources
  - Cloud resources

- Enrich User Information
  - Current CMDB for Users
  - HR Business Applications

- Integrate Management
  - Configuration and rollback
  - Notification
Preparing: Interactions w/ Resources

Log User Activity
- Applications
- Infrastructure

Log API Activity
- Cloud services
- On-prem services

Integrate host acquisition
- Memory
- Disk
Preparing: Additional Considerations

Storage
- Logs
- Disk/Memory

Special Access
- Elasticity
- API licenses

Analytics tools
- Data Analysis
- Sharing and Collaboration
Preparing for Cloud IR

- Collect streaming events - log data, API results
- Collect batch data - log data, disk, memory images
- Execute ad hoc collection via APIs - automated or human mediated
- Search and investigate the collections
- Enrich data with third party information - asset/identity, HR, threat intel
- Automate collection/analysis/sharing tasks
Operationalizing the model
Capabilities needed for Cloud Incident Response

- Logs: Infrastructure, Instance, Service
- Memory Forensics
- Disk Forensics
- Versioning, Snapshots
- APIs for Configuration Changes
- APIs for Status Gathering
Operational Considerations for Collection

- **Logs**
  - Streaming or batched
  - Structured or unstructured

- **Binary data**
  - Memory dumps are unstructured
  - Disk forensics require storage

- **Analytics**
  - Out of the box vs Custom
  - Collaboration requires integration

- **Automation**
  - Test and Rollback
  - Human mediation
Hybrid Cloud + Onprem

Automation/API friendly

Collaboration and sharing ready
Attack and IR Scenarios
Joe creates a shared link on a cloud storage folder and emails it to an accomplice. Over the course of a month, Joe posts company proprietary data to the folder. And over the course of the month, Joe's accomplice makes copies of the data.
IR: Linkin’ Joe

Identity

• Log data: cloud storage, on-prem auth
• Enrich with: DLP or watch listed files, HR watch list, local file access

Resources

• Search for unauthenticated access to a folder

Interactions

• Search for large number of files moving to a specific folder
• Make a list of file names uploaded/downloaded to folder
Stolen cloud infrastructure keys are used to instantiate new instances and access existing instances.
IR: Pickpocket

Identity
- Identify the keys that were stolen
- Enrich log data: threat intel, IP, domains, file names, service names

Resources
- Log data: cloud infrastructure, cloud instance, threat intel
- Host data: memory dump, cloud instance snapshot
- Search other cloud instances for discovered indicators

Interactions
- Search log data for: use of keys, number of instances, durations of sessions
- Search memory: installed services, open ports, file names

Contain
- API: Disable keys
- API: Modify security zones for instances spawned by infected key use
N’synch - synch folder propagator

Malware propagates by copying itself to auto synch folders for cloud storage service
N’synch IR

Identity
• Identify owner of infected file

Resources
• Cloud storage, email
• Search storage logs for file operations

Interactions
• Search host logs for reg keys, services, files, sockets

Contain
• API: remove propagating file
• API: change permissions on infected folders
Takeaways and Call to Action
Call to Action for Cloud IR

Collect Data from Anywhere

Search Based on New Criteria

Enrich from internal, external sources on demand

Automation, Workflows, Sharing
Cloud IR: A Simple Model

Identity
Used

Interactions with resource

Resources Accessed by Identity
Thank You

@monzymerza
mmerza@splunk.com
monzymerza@gmail.com
#splunk