THE EVOLUTION OF CLOUD FORENSICS AND INCIDENT RESPONSE

Ramy F. Rahman
Cloud Architect
Across 12 Multi Cloud Environments

• VPC Flow Logs Turned off

14011551 VPCs/NSGs
IAM Users Without MFA 133 Users
Root Account Without MFA 27 Users
IMDSv2 Not Enabled 50,000+ EC2
MOCK ATTACK SCENARIO
FOOTHOLD: COMPROMISED AWS CREDENTIALS WITHOUT 2FA
IAM IN THE CLOUD IS COMPLEX. USE CIEM.

(CLOUD INFRASTRUCTURE ENTITLEMENT MANAGEMENT)
CONFIGURATIONS, FLOW LOGS, AND ADMIN ACTIVITY SHOULD BE TRACKED. USE CSPM. (CLOUD SECURITY POSTURE MANAGEMENT)
CWPP VS. EDR WHICH ONE AND WHY?
(CLOUD WORKLOAD PROTECTION PLATFORM VS ENDPOINT DETECTION AND RESPONSE)
CALL TO ACTION: BACK TO BASICS

- **ENSURE LOGGING IS ENABLED**
  - VPC flow logs, CloudTrail logs at the very least
  - OS and Application logs from Cloud hosts
  - AWS System Session Manager Logs

- **COLLECT AND AGGREGATE LOGS CENTRALLY FOR CORRELATION AND ANALYSIS**
  - e.g. CloudWatch, Devo, 3rd party integrations Splunk for AWS, Azure or GCP, Prisma Cloud or any CSPM tool

- **REWRITE INCIDENT RESPONSE PLAYBOOKS TO SUPPORT CLOUD NATIVE SERVICES**
ADDITIONAL CONSIDERATIONS

• CONSIDER AWS/GCP ORGANIZATIONS AND USE SERVICE CONTROL POLICIES

• ALIGN WITH THE MITRE FRAMEWORK FOR CLOUD

• DEPLOY AN EDR FOR CLOUD HOSTS AND CWPP SOLUTION THAT CAN MONITOR MORE GRANULARLY AT THE HOST LEVEL. UNDERSTAND ADVANTAGES OF BOTH
Attack Scenario Leveraging MITRE ATT&CK® Matrix for Enterprise Cloud

MITRE released this attack matrix for Enterprise Cloud that I feel is a good reference for walking through some of the aspects of an example enterprise cloud attack that we can identify once we have Prisma Cloud deployed. For this blog series, I’ll be covering techniques in initial access, persistence, privilege escalation and defense evasion tactic phases.

<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Persistence</th>
<th>Privilege Escalation</th>
<th>Defense Evasion</th>
<th>Credential Access</th>
<th>Discovery</th>
<th>Lateral Movement</th>
<th>Collection</th>
<th>Exfiltration</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 techniques</td>
<td>5 techniques</td>
<td>1 technique</td>
<td>5 techniques</td>
<td>4 techniques</td>
<td>9 techniques</td>
<td>2 techniques</td>
<td>4 techniques</td>
<td>1 technique</td>
<td>4 techniques</td>
</tr>
<tr>
<td>Drive-by Compromise</td>
<td>Account Manipulation</td>
<td>Valid Accounts</td>
<td>Impair Defenses</td>
<td>Modify Cloud</td>
<td>Brute Force</td>
<td>Account Discovery</td>
<td>Internal Spearphishing</td>
<td>Data from Cloud Storage Object</td>
<td>Transfer Data to Cloud Account</td>
</tr>
<tr>
<td>Exploit Public-Facing Application</td>
<td>Create Account</td>
<td></td>
<td>Compute Infrastructure</td>
<td>Steal Application Access Token</td>
<td>Use Alternate Authentication Material</td>
<td>Cloud Infrastructure Discovery</td>
<td>Use Alternate Authentication Material</td>
<td>Data from Information Repositories</td>
<td>Data Staged</td>
</tr>
<tr>
<td>Prisning</td>
<td></td>
<td></td>
<td>Unused/Unsupported Cloud Regions</td>
<td>Steal Web Session Cookie</td>
<td>Unsecured Credentials</td>
<td>Cloud Service Dashboard</td>
<td>Cloud Service Discovery</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trusted Relationship</td>
<td>Office Application Startup</td>
<td></td>
<td>Use Alternate Authentication Material</td>
<td></td>
<td></td>
<td>Network Service Scanning</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Valid Accounts</td>
<td>Valid Accounts</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Proprietary and CONFIDENTIAL. Do Not Distribute. © 2021 Optiv Security Inc. All Rights Reserved.
February 01, 2021

The Evolution of Cloud Forensics and Incident Response

With the adoption of cloud infrastructure rapidly changing our attack landscape, we find ourselves with SOC and IR teams asking for some of the same visibility they had in the data center in the cloud. In some scenarios, the traditional SOC/IR tools are hardly practical or cost-effective. Due to the ephemeral nature of cloud infrastructure, a lot of the traditional security operations motions need to evolve to replicate the high-fidelity forensics that have given security teams the peace of mind to know what happened, on what host and what traffic traversed the cloud. In this blog we will leverage several native and third-party tools to capture malicious activities that can be performed on a cloud host to provide guidance on cloud forensics and the evolution of security operations and incident response.

Overview of Infrastructure

For this blog series, we will be focused on AWS and EC2 hosts, but many of the tools will be public and private cloud-agnostic. The initial visibility we would want aligns with tools traditionally used for configuration management. Who modified the firewall? What rules were changed? What were the permissions given to an IAM role? For this visibility, we will leverage Palo Alto Networks Prisma Cloud to replicate monitoring of an environment that an SOC would want in a centralized dashboard.