CLOUD THREAT HUNTING

Jim Reavis
CEO and Founder
Cloud Security Alliance
December 2017
# About the Cloud Security Alliance

“To promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing.”

<table>
<thead>
<tr>
<th>Building Security Best Practices for Next Generation IT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global, Not-for-Profit Organization</td>
</tr>
<tr>
<td>Research and Educational Programs</td>
</tr>
<tr>
<td>Cloud Provider Certification – CSA Star</td>
</tr>
<tr>
<td>User Certification – CCSK</td>
</tr>
<tr>
<td>The Globally Authoritative Source for Trust in the Cloud</td>
</tr>
</tbody>
</table>
88,000+ INDIVIDUAL MEMBERS
80+ CHAPTERS
400+ CORPORATE MEMBERS
35+ ACTIVE WORKING GROUPS

2009 CSA FOUNDED

Strategic partnerships with governments, research institutions, professional associations and industry

CSA research is FREE!

SEATTLE/BELLINGHAM, WA // US HEADQUARTERS
EDINBURGH // EMEA HEADQUARTERS
SINGAPORE // ASIA PACIFIC HEADQUARTERS
Cloud Definitions

Essential Characteristics

Resource Pooling

Service Models

SaaS (Software as a Service)
PaaS (Platform as a Service)
IaaS (Infrastructure as a Service)

Deployment Models

Public  Private  Hybrid  Community

presentation Modality

Presentation Platform

APIs
Applications

Data  Metadata  Content

Integration & Middleware

APIs

Core Connectivity & Delivery
Abstraction
Hardware
Facilities

NIST

CSA Cloud Reference Model
Cloud Security Focus

This is where the security action is
Stakes are high for Data Protection

- General Data Protection Requirements (GDPR)
  - 4% of annual global turnover or €20 Million (whichever is greater)
- I will spare you a logo wall of shame listing of breached companies, fired CEOs, etc

https://gdpr.cloudsecurityalliance.org/
CSA Top Threats Report

1. Data Breaches
2. Compromised Credentials and IAM
3. Insecure APIs
4. System and App Vulnerabilities
5. Account Hijacking
6. Malicious Insiders
7. APTs
8. Data Loss
9. Insufficient Due Diligence
10. Nefarious Use and Abuse
11. Denial of Service
12. Shared Technology Vulnerabilities

https://cloudsecurityalliance.org/group/top-threats/
Threat 1: Data Breach

- Ranking based upon impact rather than prevalence
- Compromised credentials, sloppy admin & poor programming practices loom large
- Incidents primarily have a root cause in cloud user mistakes, e.g., “AWS bucket slosh” (S3)
Threat 2: Insufficient Identity, Credential and Access Management

- Compromised credentials a path of least resistance
- Multi-factor authentication recommended – mandatory for privileged accounts
- Identity federation to prevent credential sprawl
- See also Threat 5: Account Hijacking
Threat 3: Insecure APIs and Interfaces

• Agility, “on demand”, continuous deployment creates pressure to develop “too quickly”
• Vetting of all 3rd party API services and the cloud layers lacking
• Secure development lifecycle practices as critical as ever
Threat 12: Shared Technology Vulnerabilities

- VM Side channel attacks
- VENOM vulnerability
- Hypervisor??
- Hardware bugs, supply chain
About Security Guidance V4

- Fundamental cloud security research that started CSA
- 4th version, released July 2017
- Architecture

- Governing in the Cloud
  - Governance and Enterprise Risk Management
  - Legal
  - Compliance & Audit Management
  - Information Governance

- Operating in the Cloud
  - Management Plane & Business Continuity
  - Infrastructure Security
  - Virtualization & Containers
  - Incident Response
  - Application Security
  - Data Security & Encryption
  - Identity Management
  - Security as a Service
  - Related Technologies
Related advice from CSA Guidance V4

- SLAs and setting expectations between provider and customer responsibilities

- Cloud customers must understand the content and format of data that the cloud provider will supply for analysis purposes and evaluate whether the available forensics data satisfies legal chain of custody requirements.

- Cloud customers should also embrace continuous and serverless monitoring of cloud-based resources to detect potential issues earlier than in traditional data centers.
Related advice from CSA Guidance V4

- Data sources should be stored or copied into locations that maintain availability during incidents.
- Cloud-based applications should leverage automation and orchestration to streamline and accelerate the response, including containment and recovery.
- For each cloud service provider used, the approach to detecting and handling incident involving the resources hosted at that provider must be planned and described in the enterprise incident response plan.
Related advice from CSA Guidance V4

• The SLA with each cloud service provider must guarantee support for the incident handling required for the effective execution of the enterprise incident response plan. This must cover each stage of the incident handling process: detection, analysis, containment, eradication, and recovery.

• Testing will be conducted at least annually or whenever there are significant changes to the application architecture. Customers should seek to integrate their testing procedures with that of their provider (and other partners) to the greatest extent possible.
Why IaaS not the primary focus?

- Well funded, mature security teams
- State of the art technology
- Collaboration with competitors could be better, but they do communicate
- We need IaaS cloud providers to enable their customers for threat intelligence sharing & secure-by-default usage of platforms (among many other things)
- Need to solve the “provider within a provider” problem – it’s the ecosystem stupid!
The cloud ecosystem threat problem

- Attacks may take on very different meaning in the context of an ecosystem

Galactic Bank’s cloud presence
Cloud Security Industry Summit

- Started by Intel
- Participation from major cloud providers and major tech companies
- Cloud Security Alliance participates
- Strength is a focus on firmware/BIOS issues
- Recent firmware integrity whitepaper
CSA Cloud CISC

- CSA Cloud Cyber Incident Sharing Center
- Our effort to drive standards in incident response and threat intelligence sharing in the cloud
- Features an operation threat intelligence exchange
  - Initial data indicates a lot of common actors hitting cloud customers separately
- Addressing issues such as anonymization, attribution and legal/SLAs related to the cloud reference model
Looking to the future: Dynamic Digital Enterprise

- Massive increase in compute
- Cloud Computing is the back end
- Internet of Things is the endpoint
- Compute is Everywhere …
- But, you won’t know where Anything is
- Devices, software, network routes continuously modified
- The corporation is a virtual, software-defined construct – the Dynamic Digital Enterprise
- The corporation will have many more software partners than today – but some will exist for only seconds at a time
- Existing security will not scale
Automation for securing the Dynamic Digital Enterprise

- Artificial Intelligence is the brain managing the digital enterprise
- Blockchain provides the trusted language & rules
- Software Defined Networking dynamically organizes computers
- DevOps automates the Cloud
- Autonomics automates the IoT
- We call this “Self-Driving Information Security”
To sum it up

• Familiar threats exist in cloud, but can take on new dimensions and consequences
• More cloud-specific threats exist as well
• Tier 1 cloud providers have excellent security programs, but the ecosystem does not necessarily benefit as they might
• Enabling the SaaS layer (commercial or end user) essential for threat hunting
• Tricky legal & SLA issues are as big of an impediment as the PR & competitive issues
• Look to the future and understand the scale needed. Automation needed, cannot rely on the historical backchannels
• CSA has a lot of free research and a community to assist
THANK YOU!

Contact CSA

Email: info@cloudsecurityalliance.org
Twitter: @Cloudsa
Site: www.cloudsecurityalliance.org
Learn: www.cloudsecurityalliance.org/research/cloudbytes
Download: www.cloudsecurityalliance.org/download