Enterprise Defense Vs. Security Monitoring and Response "in the cloud"

Garrett Schubert
Manager, Incident Response and Threat Intelligence
05-26-2016
What is Cloud Security?!?!

1. What is the Cloud? Cloud vs. Enterprise Security

2. The game of Security Monitoring and Response (aka SOC)

3. People, Process, Technology

4. Similarities\Difference

5. Use Cases
# Shared Responsibility Model

<table>
<thead>
<tr>
<th>On-Premises</th>
<th>IaaS</th>
<th>PaaS</th>
<th>SaaS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications</td>
<td>Data</td>
<td>Runtime</td>
<td>Virtualization</td>
</tr>
<tr>
<td>Middleware</td>
<td>O/S</td>
<td>Servers</td>
<td>Storage</td>
</tr>
<tr>
<td>Networking</td>
<td></td>
<td></td>
<td>Networking</td>
</tr>
</tbody>
</table>

- **Green**: Customer
- **Blue**: Microsoft
Amazon Web Services (AWS)
Shared Security Responsibility Model

- Customer Data
- Platform, Application, Identity & Access Management
- Operating System, Network and Firewall Configuration
  - Client-Side Data Encryption & Data Integrity Authentication
  - Server-Side Encryption (File/Server and/or Data)
  - Network Traffic Protection (Encryption/Integrity/Identity)

- Deployment and Management
- Compute
- Database
- Storage
- AWS Networking Services
- AWS Global Infrastructure
- Availability Zones/Regions
- Edge Locations
The Game is the same..

HOLD THE WALL!
...But the field has changed
People
Process

• Practice makes Perfect – Run drills

• Identify responsibilities across teams\vendors

• Define expectations before hand - SLA

• Communication

• Rinse and repeat
Technology

• Don’t assume you have the logs you used too

• Are you on shared resources? - PaaS

• What do you mean there is no Network IDS options?!?!

• You mean my competitors are in the same Virtual Network as me?

• “It feels like we are going back in time”
• Threat intelligence Programs

• Vulnerabilities and Exploits Assessment

• Your team!

• Your Mission: “Finding the bad guy, get him out, figure what he\she did. Make sure it does not happen again!” (Who is accountable?)

• “Crown Jewels” – Value of the data

• Questions from your CISO
The Deltas

• Threat actor assessment:
  • Intelligence: OSINT, social media
  • Location, location, location: Collateral damage
  • Visibility: Industry is behind
  • Who responsible
  • Security dependencies
  • Risk profile – Who is liable?
Everything is okay in the end. If it’s not okay, then it’s not the end 😃

hacked by

!!!!!! Islam Hacker Team !!!!!!
Donsoufiane2@gmail.com
pin:ISIS

Game Over
Take-Aways

1. "Trust fall" - Accept the fact that you are not in control (at least as much as you want to be)
2. Hold the bar high!
3. Technology needs to catch up
4. Don’t forget the basics
5. The game is the same but the field has changed
6. What is the risk equation now?
7. Fight for visibility!
Questions
Thank you