AN OSINT APPROACH TO THIRD PARTY CLOUD SERVICE PROVIDER EVALUATION

Lokesh Pidawekar
@MaverickRocky02
#whois

- Cloud and Application Security Architect @ **Cisco**
- Information Assurance and Cybersecurity Masters from Northeastern University, Boston
Third Party Cloud Providers Ecosystem

Enterprise Business Functions have embraced third party cloud applications for critical business operations

- CRM
- Infrastructure provider
- Service Desk
- Mails
- Storage
- Marketing catalogues
- Dogs, cats blah blah
How do companies assess these providers

At Bit Discovery we’re often asked about our competitors for asset inventory. After speaking with over 100 companies (literally), by far our #1 competitor is Microsoft Excel. When an inventory exists, that’s what's most common. We can do better.

3:39 PM - 11 Jul 2018
Assessment Tools

• Excel Sheets
• Word Documents
• Over coffee, drinks
• Third party consultants, tools etc.
Typical Process

1. Send questionnaire
2. Meet with the provider
3. Understand their security controls
4. Recommend few things
5. Approve
Categories of question

- Application Security
- Identity and Access Management
- Data Security
- Vulnerability Management
- Infrastructure security
- Secure Operations
- Incident Response
- Privacy
- Logging and monitoring
Challenges in current process

• Point in time
• Laborious and time consuming
• Does not provide continuous monitoring
Proposed Solution

Corelating available information from Internet aka OSINT
Architecting the solution

- Collect information from various sources
- Rank the sources based on the **impact** and **accuracy** of information
- Complement with the information collected from the provider

<table>
<thead>
<tr>
<th>CSP Name</th>
<th>SSL</th>
<th>Umbrella Score</th>
<th>Security Headers</th>
<th>Shodan Vuln</th>
<th>OpenBug Bounty Vuln</th>
<th>Vulners</th>
<th>IaaS</th>
<th>SOC2</th>
<th>Overall Health</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSP Name</td>
<td>A</td>
<td>B+</td>
<td>A</td>
<td>A</td>
<td>D</td>
<td>B</td>
<td>AWS</td>
<td>Yes</td>
<td>B+</td>
</tr>
<tr>
<td>CSP Name</td>
<td>C</td>
<td>B</td>
<td>C</td>
<td>B</td>
<td>A</td>
<td>B</td>
<td>Azure</td>
<td>Yes</td>
<td>B</td>
</tr>
<tr>
<td>CSP Name</td>
<td>A</td>
<td>A-</td>
<td>C</td>
<td>A+</td>
<td>C</td>
<td>A</td>
<td>GCP</td>
<td>Yes</td>
<td>A-</td>
</tr>
<tr>
<td>Category</td>
<td>Tools</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------------------------</td>
<td>--------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asset discovery</td>
<td>Shodan, Bluto, SpiderFoot</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSL score, Security Headers</td>
<td>SSLScan, htbridge, HTTP observatory</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mobile</td>
<td>Htbridge Mobile Scan, Vulners,</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threat Hunting</td>
<td>Greynoise.io</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit Reports</td>
<td>CSA Star Registry</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vulnerability data</td>
<td>OpenBugBounty, PunkSPIDER, Vulners</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Company details</td>
<td>Crunchbase</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Code Search</td>
<td>nerdydata</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP Reputation</td>
<td>Cisco Talos</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Search</td>
<td>DNSDumpster, Domaintools etc.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Breach Information</td>
<td>Google Search etc.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Build vs Buy

Some Commercial tools that can help

<table>
<thead>
<tr>
<th>Category</th>
<th>Tools</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Access Security Broker</td>
<td>Cisco CloudLock, Skyhigh, Bitglass</td>
</tr>
<tr>
<td>Asset discovery</td>
<td>BitDiscovery</td>
</tr>
<tr>
<td>Third party risk measurement</td>
<td>Bitsight, securityscorecard</td>
</tr>
<tr>
<td>Mobile</td>
<td>NowSecure Intel</td>
</tr>
<tr>
<td>Threat Hunting</td>
<td>Recorded Future</td>
</tr>
<tr>
<td>Audit Reports</td>
<td>sharedassessments</td>
</tr>
<tr>
<td>Financial Viability</td>
<td>Dun &amp; Bradstreet</td>
</tr>
</tbody>
</table>

@MaverickRocky02
Mobile – NowSecure Intel

SURF TO GET A FREE ANALYSIS REPORT ON ME: [bit.ly/2mtDLAm](http://bit.ly/2mtDLAm)

@MaverickRocky02
Advantages

• Continuous health check of the providers
• Can be used to make acquisition/partnership decisions
• Can be used to make policy based segregation decision
Drawbacks and scope for improvement

- False Positives / Noise
- Limited information
- Can not be the sole decision making point
Conclusion

Present day Enterprise
- Cloud services have become ubiquitous
- Enterprises are looking to identify ways for fast tracking security assurance for third party cloud services to meet the speed of business

Value of proposed solution
- Reduce the number of questions
- Provide a continuous stream of intelligence for given cloud providers.

Hope for a better future
- Cloud providers should find a common platform to share security details
- API based information gathering

@MaverickRocky02
Q&A

@MaverickRocky02