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

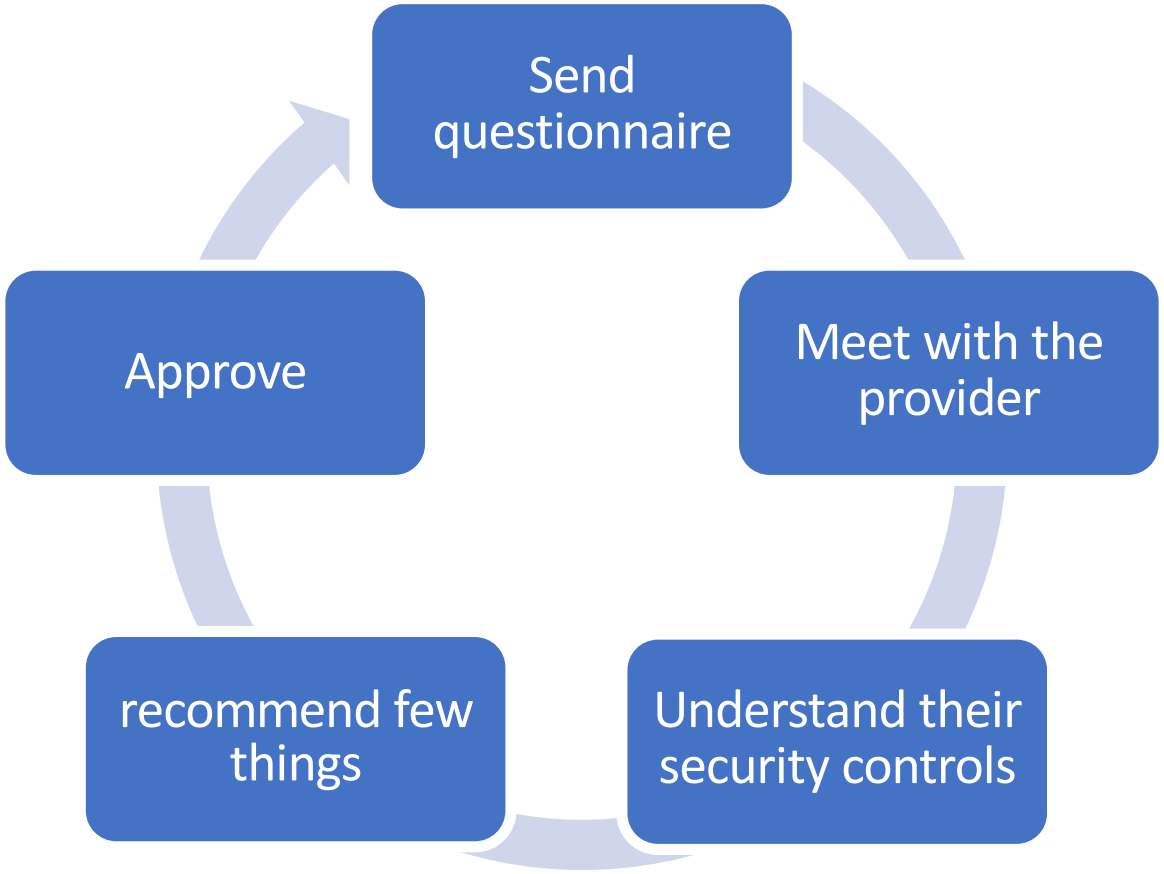
- CRM
- Infrastructure provider
- Service Desk
- Mails
- Storage
- Marketing catalogues
- Dogs, cats blah blah

How do companies assess these providers

Assessment Tools

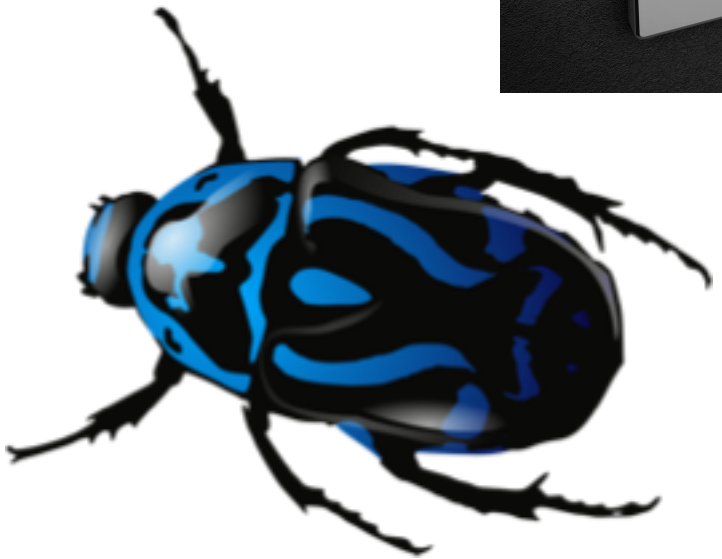
- Excel Sheets
- Word Documents
- Over coffee, drinks
- Third party consultants, tools etc.

Typical Process



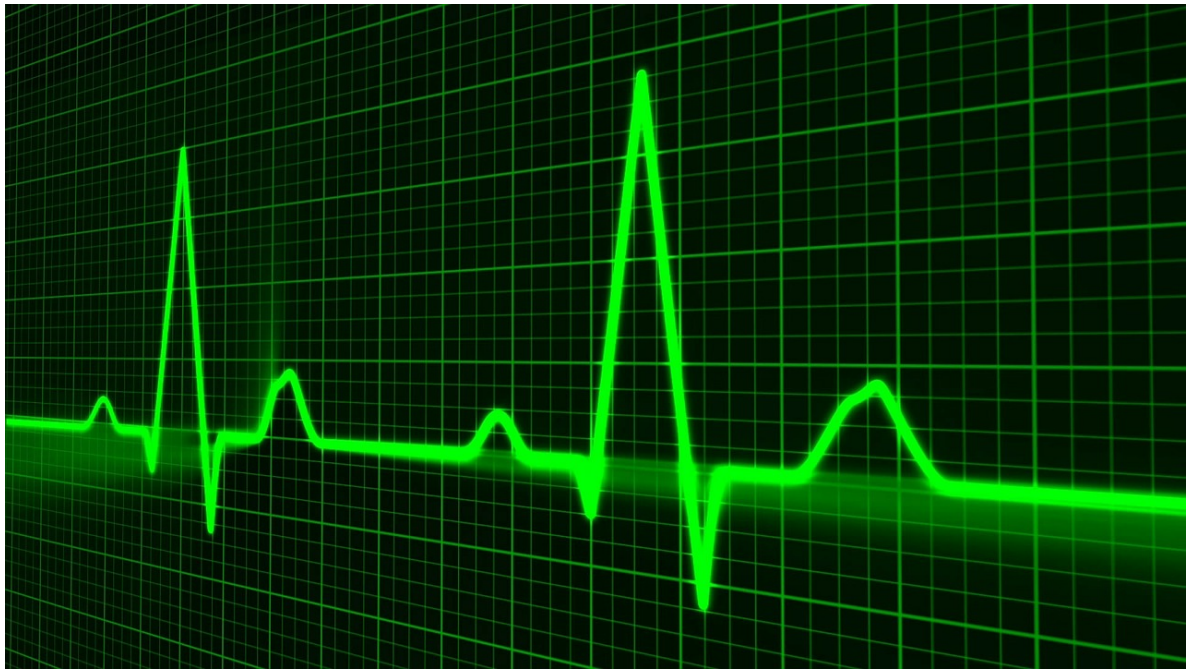
Categories of question

- 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

CSP	SSL	Umbrella Score	Security Headers	Shodan Vuln	OpenBugBounty Vuln	Vulners	IaaS	SOC2	Overall Health
CSP Name	A	B+	A	A	D	B	AWS	Yes	B+
CSP Name	C	B	C	B	A	B	Azure	Yes	B
CSP Name	A	A-	C	A+	C	A	GCP	Yes	A-

Resources

Category	Tools
Asset discovery	Shodan, Bluto, SpiderFoot
SSL score, Security Headers	SSLScan, htbridge, HTTP observatory
Mobile	Htbridge Mobile Scan, Vulners,
Threat Hunting	Greynoise.io
Audit Reports	CSA Star Registry
Vulnerability data	OpenBugBounty, PunkSPIDER, Vulners
Company details	Crunchbase
Code Search	nerdydata
IP Reputation	Cisco Talos
DNS Search	DNSDumpster, Domaintools etc.
Breach Information	Google Search etc.

Build vs Buy

Some Commercial tools that can help

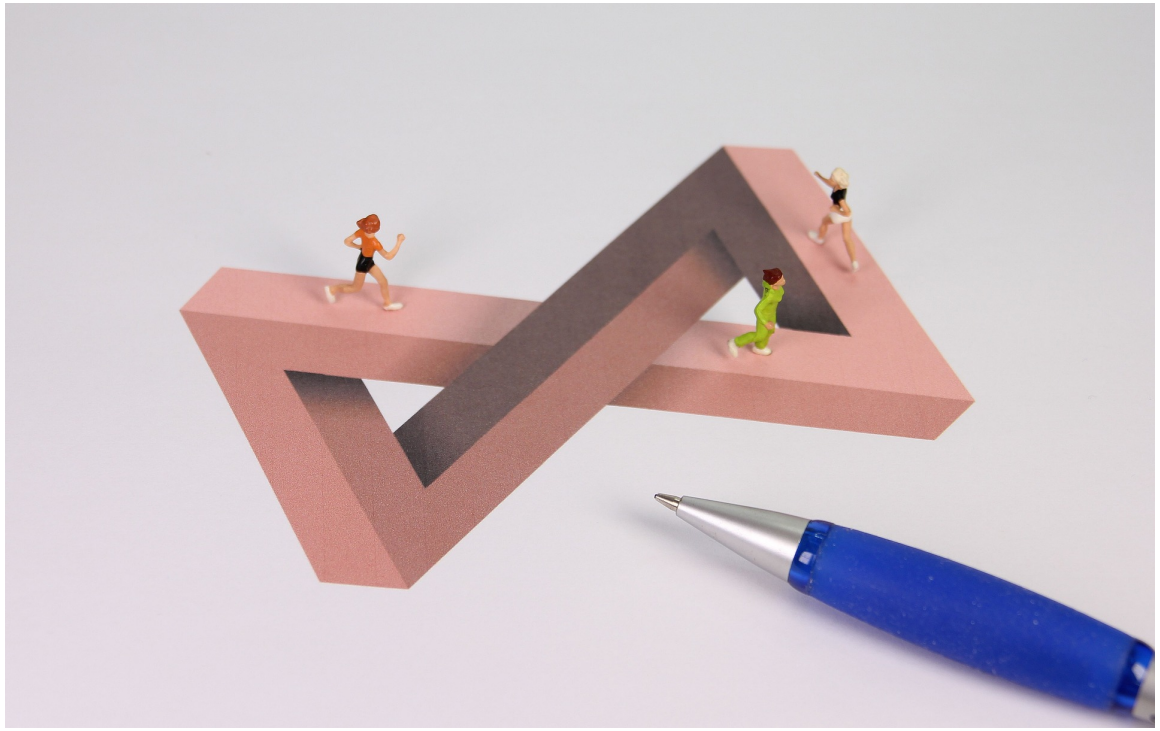
Category	Tools
Cloud Access Security Broker	Cisco CloudLock, Skyhigh, Bitglass
Asset discovery	BitDiscovery
Third party risk measurement	Bitsight, securityscorecard
Mobile	NowSecure Intel
Threat Hunting	Recorded Future
Audit Reports	sharedassessments
Financial Viability	Dun & Bradstreet

Mobile – NowSecure Intel

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

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

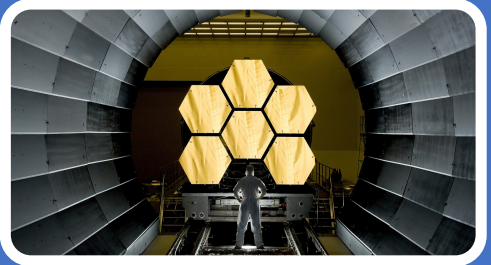
Conclusion

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

Q&A

@MaverickRocky02