

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



Northeastern

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



Jeremiah Grossman ✓

@jeremiahg

Following



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.

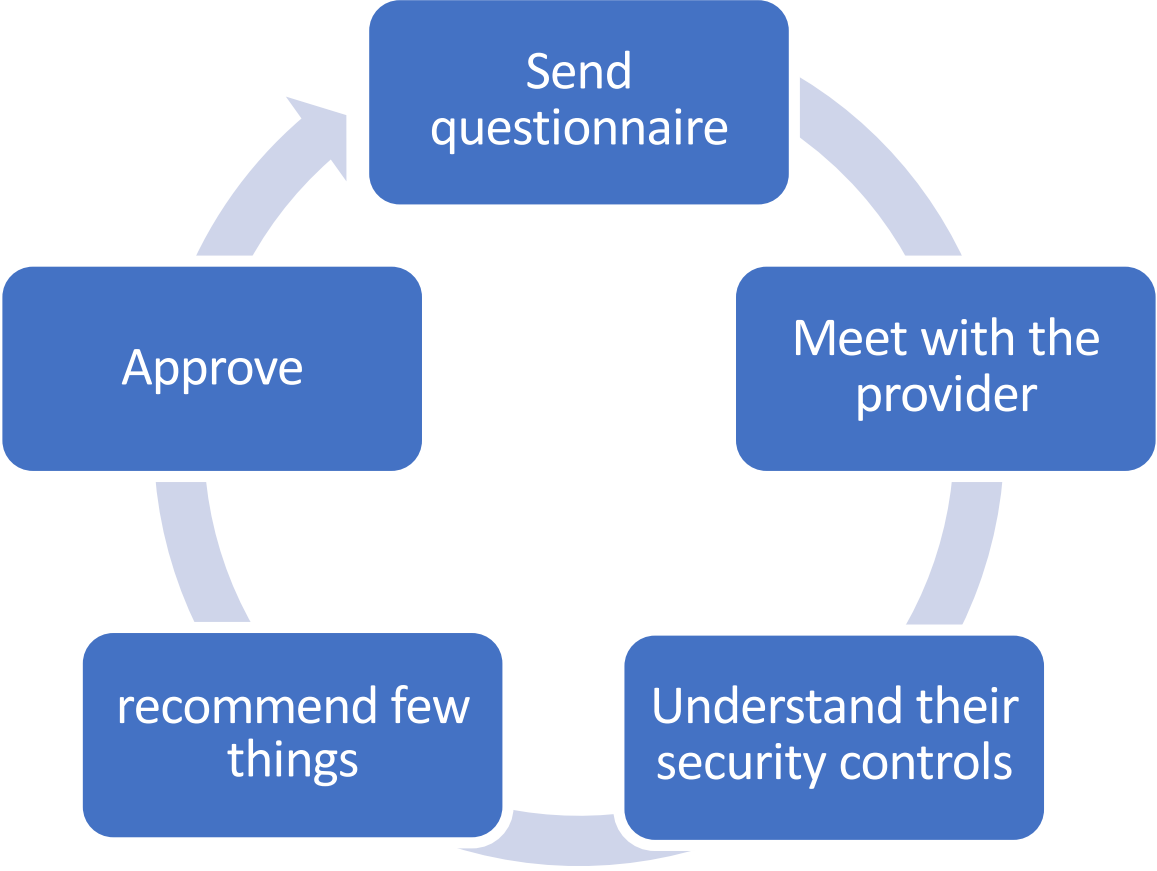
3:39 PM - 11 Jul 2018

Assessment Tools

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



Typical Process



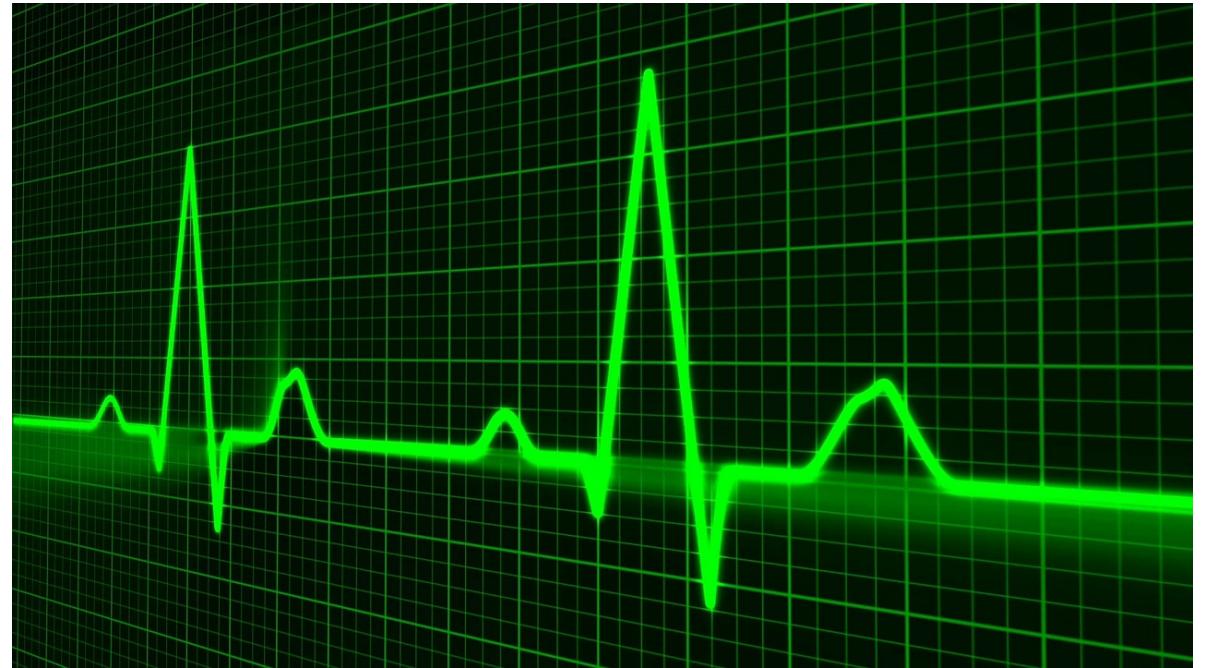
Categories of question

- 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



Man-in-the-Middle Attack (HIGH) [Severity: HIGH] [Category: NETWORK]

One or more sensitive values were intercepted in transit, due to a lack of proper certificate validation. This is a high-risk vulnerability as it is possible for an attacker on the same network to easily retrieve this information. It is encouraged to review the table below, which displays the type of data that was intercepted, whether it is sent in plain text or a special encoding, the actual value that was recovered, the related URL, and some additional context around this violation.

DESCRIPTION

Searches for sensitive data that can be intercepted over the network due to improper certificate validation and/or hostname verification. Sensitive data currently includes Username, Password, GPS Coordinates, Wi-Fi Mac Address, IMEI, Device Serial Number, and Phone number. This is related to the Hostname Verification issue.

REGULATORY

CWE: [CVE-2015-1656](#)

FOIAA, LOW: [5C-11 CRYPTOGRAPHIC PROTECTION AC-21 PUBLICLY ACCESSIBLE CONTENT](#)

FOIAA, MED: [5C-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY](#)

OWASP: [Mobile Top 10: M3 Insecure Communication](#)

GDPR: [GDPR Article 25](#)
[GDPR Article 32](#)

FFIEC: [FFIEC CISP, Appendix 2](#)

PCI: [PCI DSS Requirement 4.1](#)

HIPAA: [HIPAA 164.512\(b\)\(2\), Standard: Transmission security](#)

HTTP Requests (MEDIUM) [Severity: MEDIUM] [Category: NETWORK]

HTTP requests were detected during dynamic analysis. Every HTTP request can potentially reveal information about the behaviors and identities of the user. Although this may seem extreme given some applications, attackers look for this to make inferences about user behavior and uncover their identity.

DESCRIPTION

Network requests are evaluated for unencrypted connections (HTTP). Any endpoints that meet this criteria will be shown in the context table below.

REGULATORY

CWE: [CWE-311 - Missing Encryption of Sensitive Data](#)
[CWE-319 - Cleartext Transmission of Sensitive Information](#)

NSA: [ETP-DIT-11](#)
[ECL-HTTP, EX-1.1](#)
[ECL-HTTP, EX-1.2](#)

FOIAA, LOW: [5C-11 CRYPTOGRAPHIC PROTECTION](#)

FOIAA, MED: [5C-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY](#)

OWASP: [Mobile Top 10: M3 Insecure Communication](#)

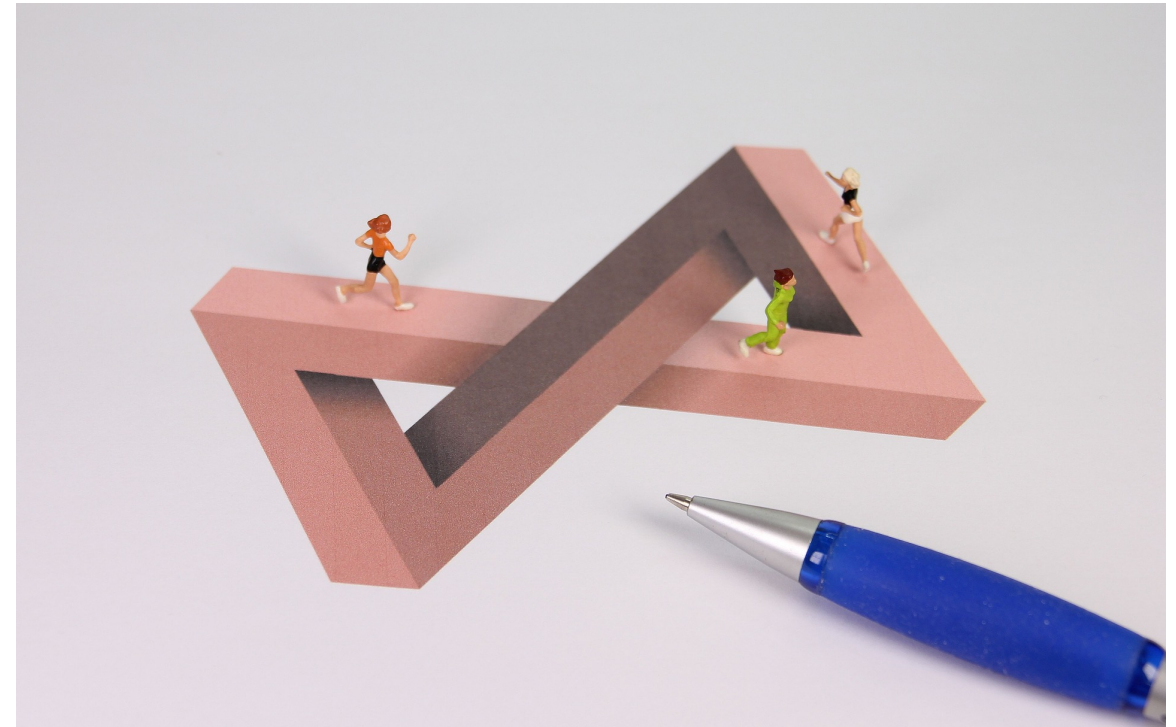
URLs

URL
http://194.154.167.31:80/wp7wp3ad
http://2001:47c:4e8:002::a:443/wp7wp3ad
http://2001:47c:4e8:002::a:80/wp7wp3ad

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

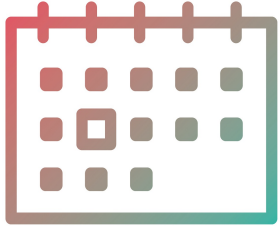


Drawbacks and scope for improvement

- 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