Multi-cloud Privacy

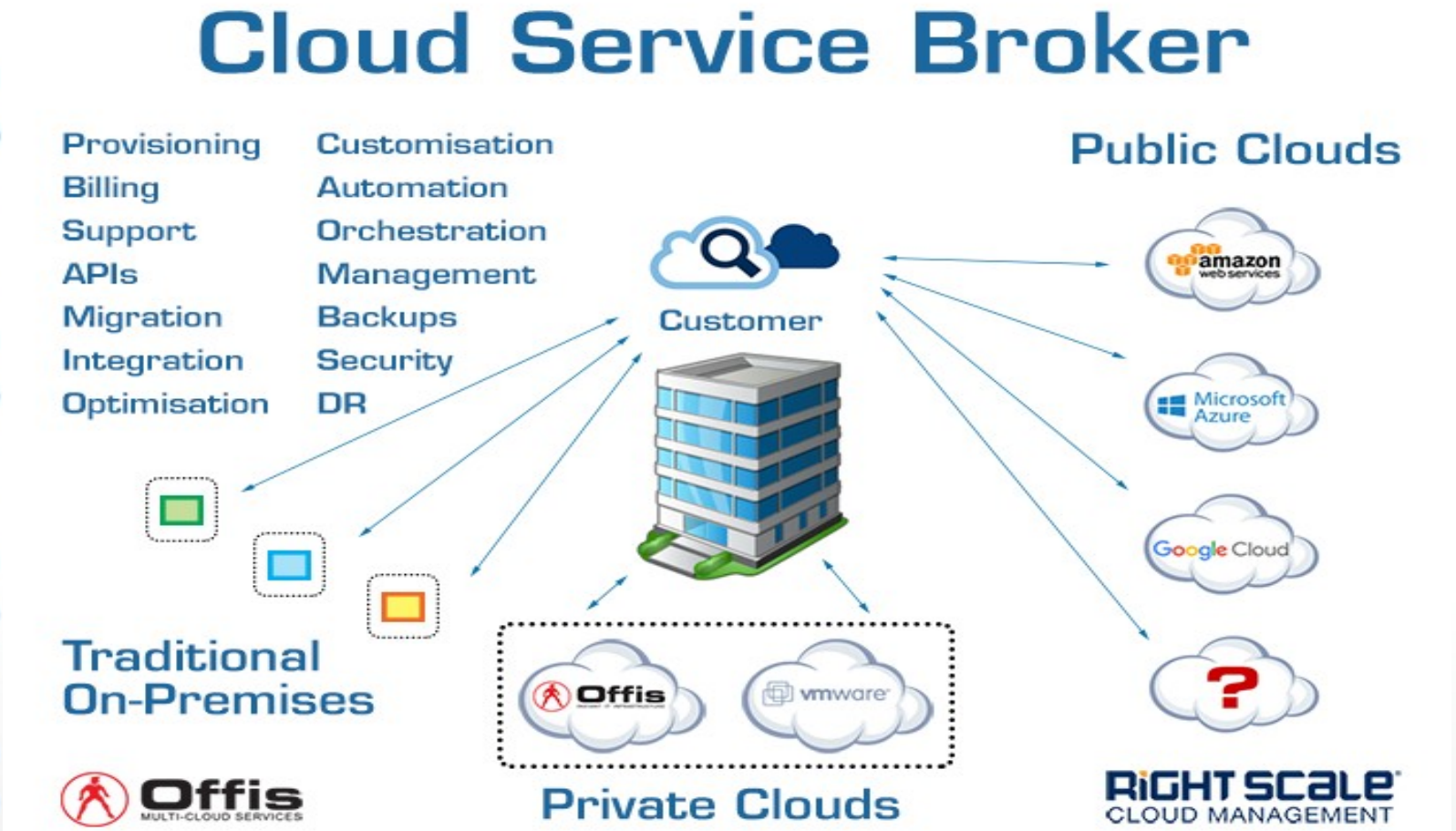
MITRE ATT&CK + OWASP Top 10 Privacy Risks

Data Security

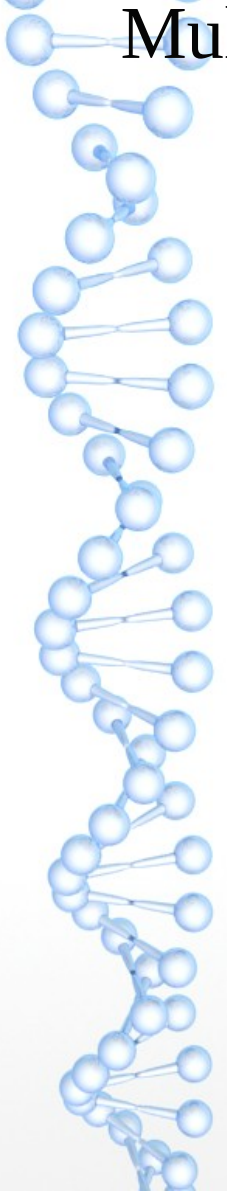
Data Privacy

By Valdez Ladd MBA, CISSP, CISA, and Mauricio Tavares - Cyberdude

Hybrid / multi-cloud security & OWASP Top 10 Privacy Risks



Multi-Cloud Security – OWASP Top 10 Privacy Risks



P1 Web Application Vulnerabilities

P2 Operator-sided Data Leakage

P3 Insufficient Data Breach Response

P4 Insufficient Deletion of personal data

P5 Non-transparent Policies, Terms and Conditions

P6 Collection of data not required for the primary purpose

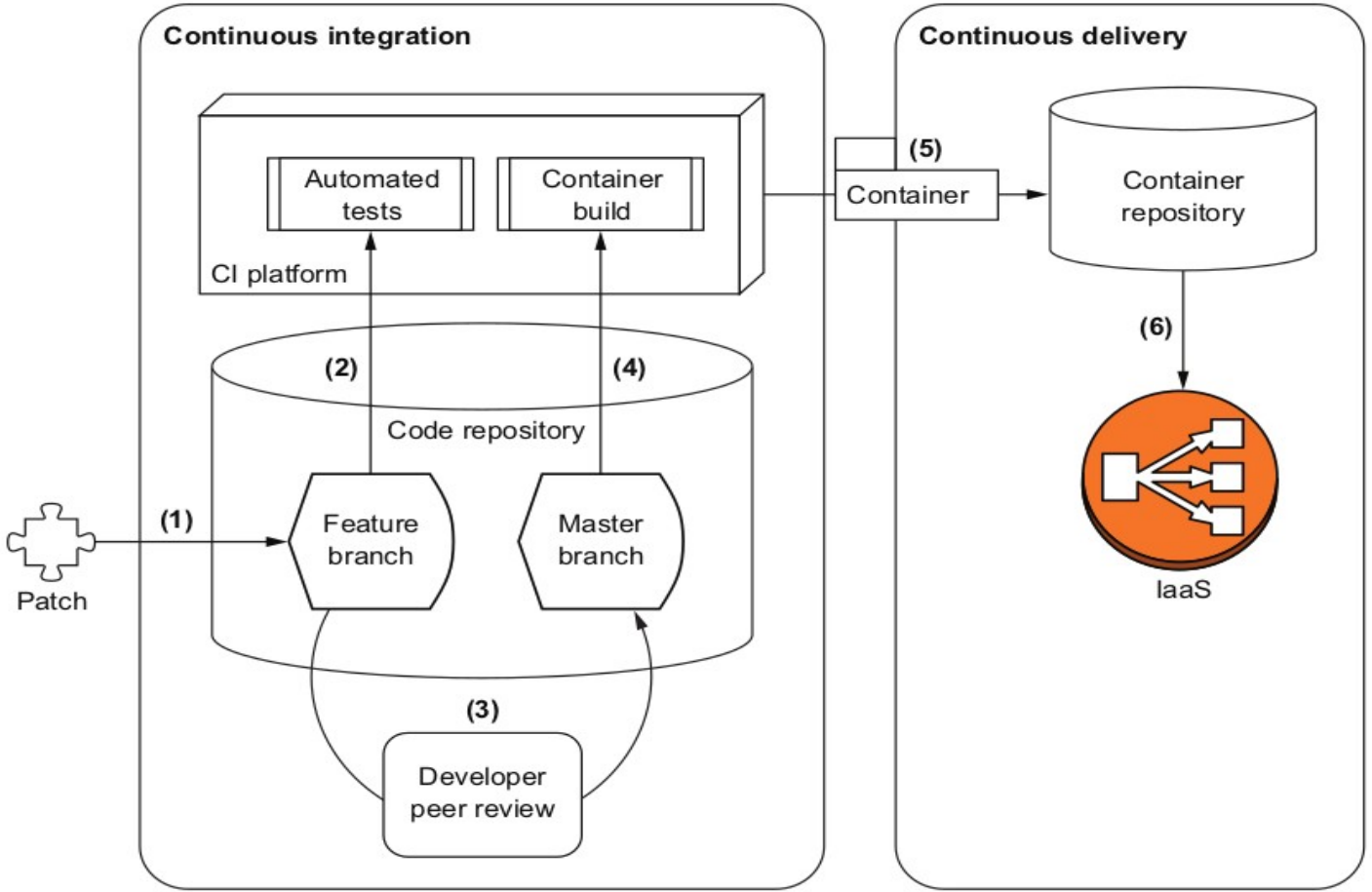
P7 Sharing of data with third party

P8 Outdated personal data

P9 Missing or Insufficient Session Expiration

P10 Insecure Data Transfer

Hybrid / Multi-cloud Security & OWASP T0P 10 Privacy



Multi-Cloud Security – OWASP Top 10 Privacy

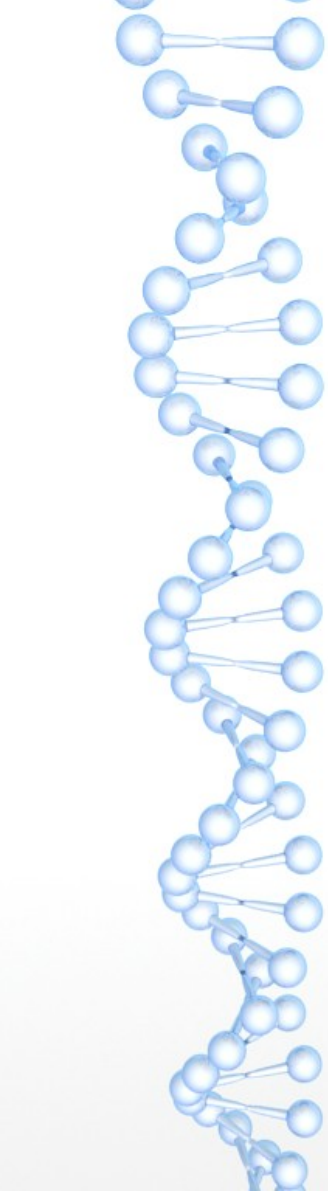
Why is the Top 10 Privacy so obscure ?

Why is the Top 10 Vulnerabilities so popular?

Spoiler Alert !

TOOLS, Tools, tools, …, but little integration...

Multi-Cloud Security – OWASP Top 10 Privacy



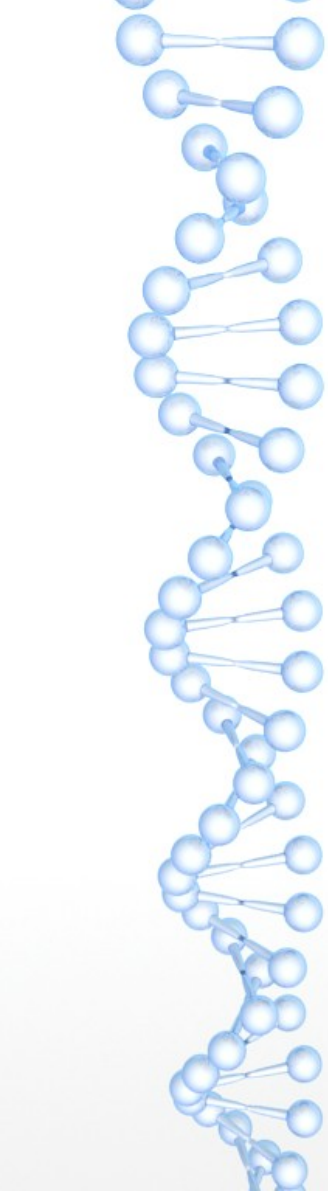
"Breaches (or pen-tests) pinpoint multiple points of failure within the business' processes and procedures. Multiple processes and procedures had to fail for millions of customer records to be ex-filtrated, and for that ex-filtration to go undetected." - Accenture Inc.

Root cause analysis – Developers
- Operations
- or Security

Multi-Cloud Security – OWASP Top 10 Privacy

P1	Web Application Vulnerabilities	High	Very high
P2	Operator-sided Data Leakage	High	Very high
P3	Insufficient Data Breach Response	High	Very high
P4	Insufficient Deletion of Personal Data	Very high	High
P5	Non-transparent Policies, Terms and Conditions	Very high	High
P6	Collection of data not required for the primary purpose	Very high	High
P7	Sharing of Data with Third Party	High	High
P8	Outdated personal data	High	Very high
P9	Missing or insufficient Session Expiration	Medium	Very high
P10	Insecure Data Transfer	Medium	Very high

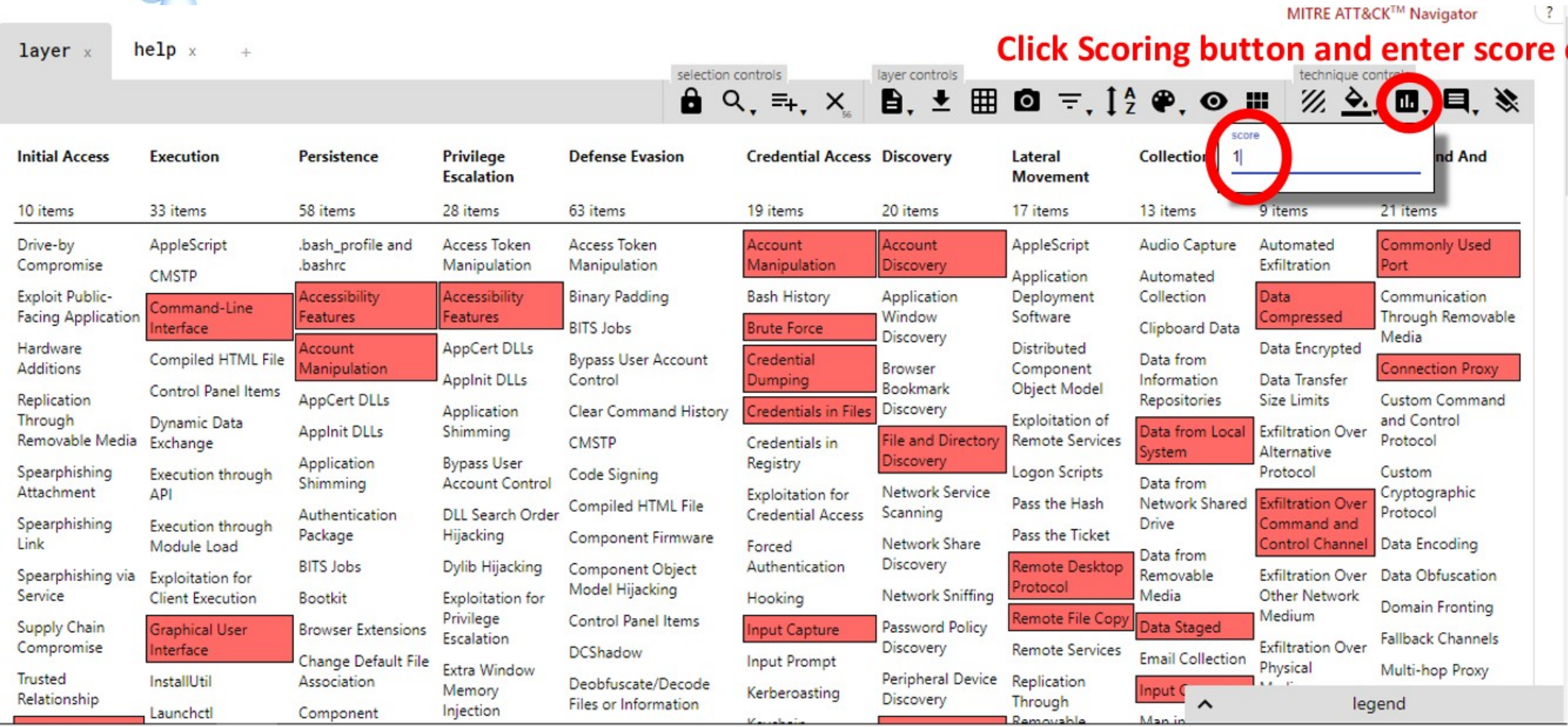
Multi-Cloud Security – OWASP Top 10 Privacy



"Breaches (or pen-tests) pinpoint multiple points of failure within the business' processes and procedures. Multiple processes and procedures had to fail for millions of customer records to be ex-filtrated, and for that ex-filtration to go undetected." - Accenture Inc.

Root cause analysis – Developers
- Operations
- or Security

Multi-Cloud Security – OWASP Top 10 Privacy Risks



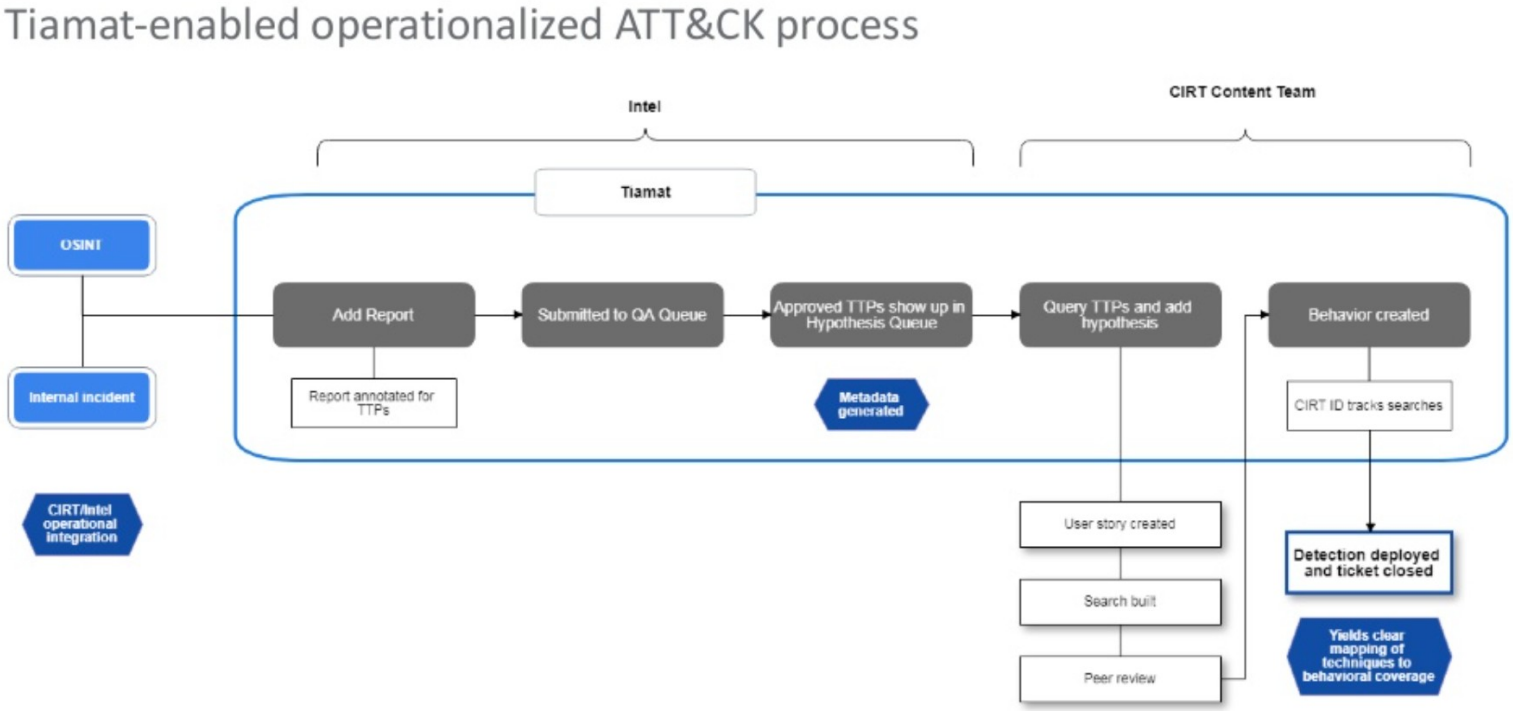
Multi-Cloud Security – OWASP Top 10 Privacy
MITRE ATT&CK

MITRE ATT&CK - Initial access: APT19

Techniques Used

Domain	ID	Name	Use
Enterprise	T1043	Commonly Used Port	APT19 used TCP port 80 for C2.[1]
Enterprise	T1132	Data Encoding	An APT19 HTTP malware variant used Base64 to encode communications to the C2 server.[4]
Enterprise	T1140	Deobfuscate/Decode Files or Information	An APT19 HTTP malware variant decrypts strings using single-byte XOR keys.[4]

Hybrid /multi-Cloud Security – OWASP Top 10 Privacy Risk & MITRE ATT&CK



Multi-Cloud Security
OWASP Top 10 Privacy & MITRE ATT&CK

Security	Privacy
Compiled HTML File	# Records ?
Control Panel Items	But what else..?
Dynamic Data Exchange	
Execution through API	
Execution through Module Load	
Exploitation for Client Execution	

HTTP malware variant used Base64 to encode communications to the C2 server.[4]

HTTP malware variant decrypts strings using single-byte XOR keys.[4]

Multi-Cloud Security – OWASP Top 10 Privacy MITRE ATT&CK

Data dictionary			
Designation	**Classification**	**Compensating controls, if any**	**Contains publicly identifiable information (IP addresses, etc.)**
Invoices	**SPECIFIC INDIVIDUALS ONLY**		
Customers' email addresses	**WORKGROUPS CONFIDENTIAL**		Used as main identifier on login.
Database credentials	**WORKGROUPS CONFIDENTIAL**	Only usable from with AWS	
Application logs	**WORKGROUPS CONFIDENTIAL**		Contains publicly identifiable information (IP addresses, etc.)
Aggregate revenue	**STAFF CONFIDENTIAL**	Made public quarterly	Also available in the payment service, no damage if lost.
Application source code	**PUBLIC**		Already available on GitHub

Multi-Cloud Security – OWASP Top 10 Privacy

P1	Web Application Vulnerabilities	High	Very high
P2	Operator-sided Data Leakage	High	Very high
P3	Insufficient Data Breach Response	High	Very high
P4	Insufficient Deletion of Personal Data	Very high	High
P5	Non-transparent Policies, Terms and Conditions	Very high	High
P6	Collection of data not required for the primary purpose	Very high	High
P7	Sharing of Data with Third Party	High	High
P8	Outdated personal data	High	Very high
P9	Missing or insufficient Session Expiration	Medium	Very high
P10	Insecure Data Transfer	Medium	Very high

Multi-Cloud Security – OWASP Top 10 Privacy MITRE ATT&CK

Security	Privacy
Compiled HTML File	Web application vulnerabilities
Control Panel Items	Insufficient Breach Response
Dynamic Data Exchange	More….?
Execution through API	
Execution through Module Load	
Exploitation for Client Execution	

Multi-Cloud Security – OWASP Top 10Privacy MITRE ATT&CK

Security	Privacy
Compiled HTML File Control Panel Items Dynamic Data Exchange Execution through API Execution through Module Load Exploitation for Client Execution	**Benefits** **Better Security / Privacy Correlation** coding / refactoring – TDD ? ** Privacy-by- (re) Discovery & better Privacy by Design