

# Multi-cloud Privacy

## MITRE ATT&CK + OWASP Top 10 Privacy Risks

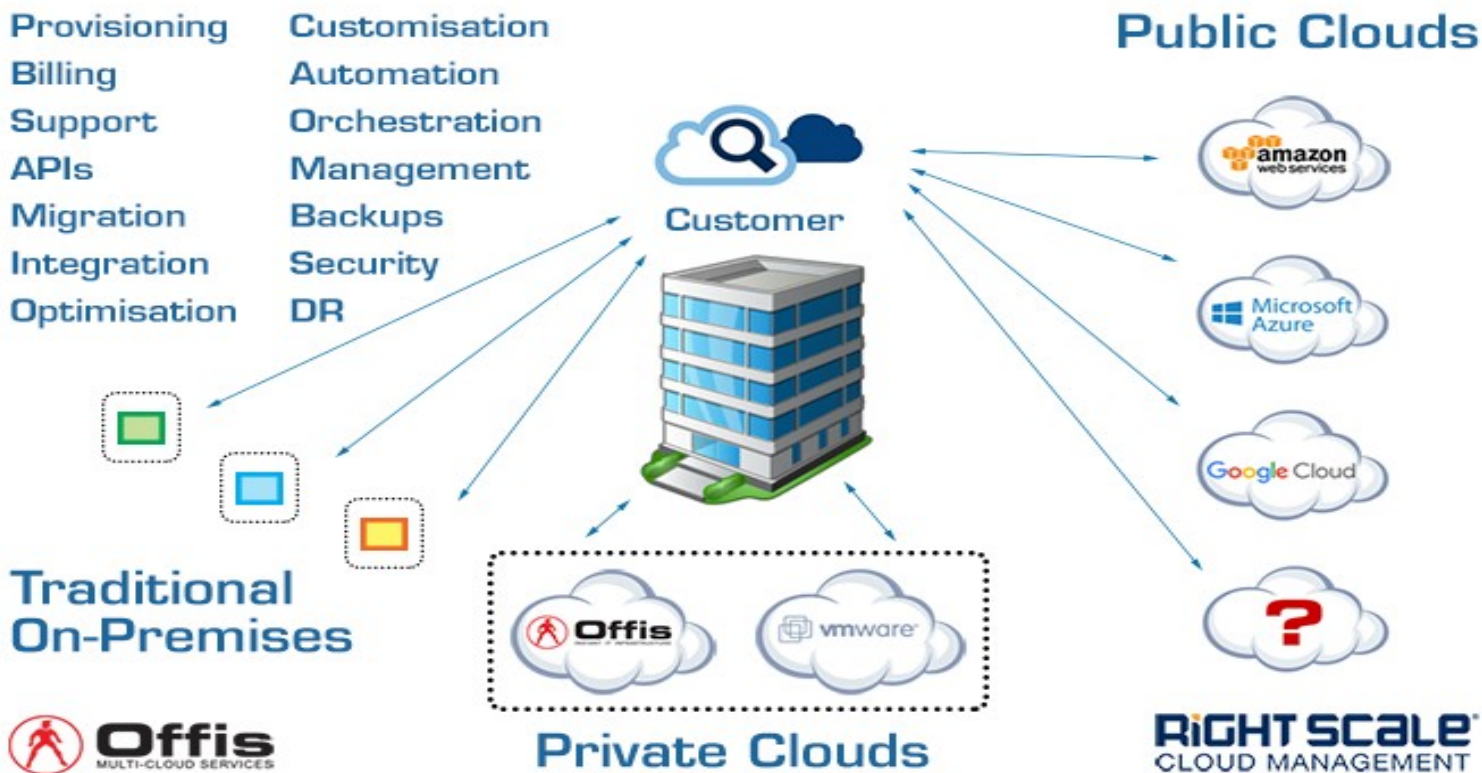
Data Security



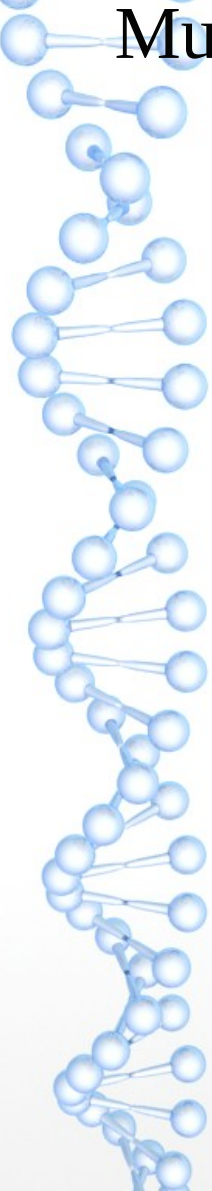
Data Privacy

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

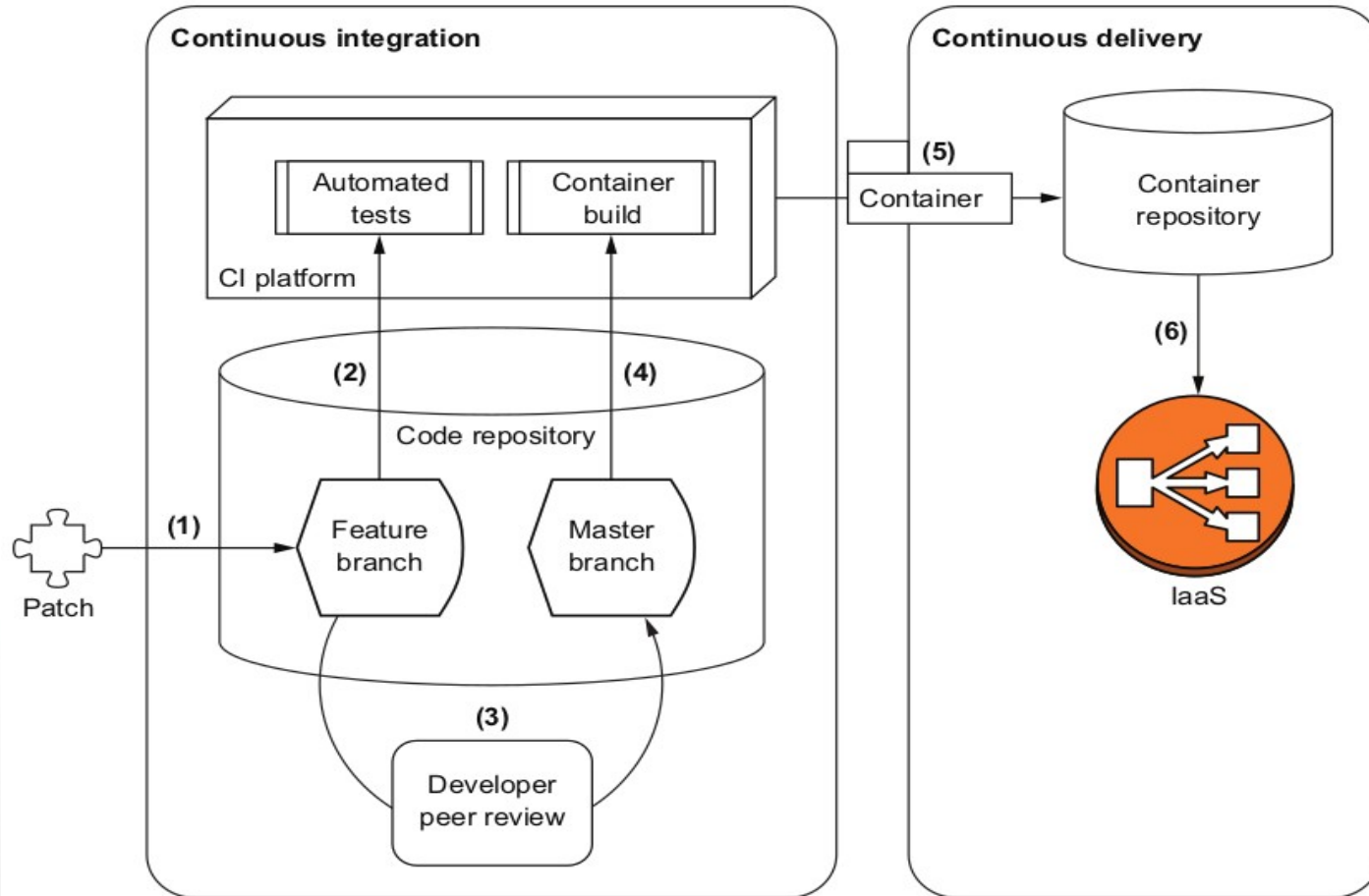
## Cloud Service Broker

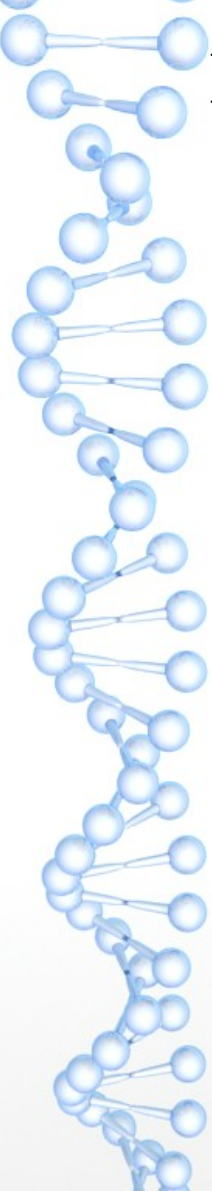


# Multi-Cloud Security – OWASP Top 10 Privacy Risks

- 
- 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  - P8 Outdated personal data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 TOP 10 Privacy





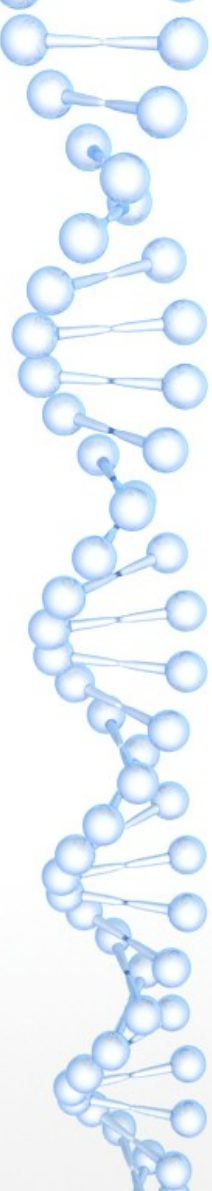
# Multi-Cloud Security – OWASP Top 10 Privacy

Why is the Top 10 Privacy so obscure ?

Why is the Top 10 Vulnerabilities so popular?

Spoiler Alert !

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



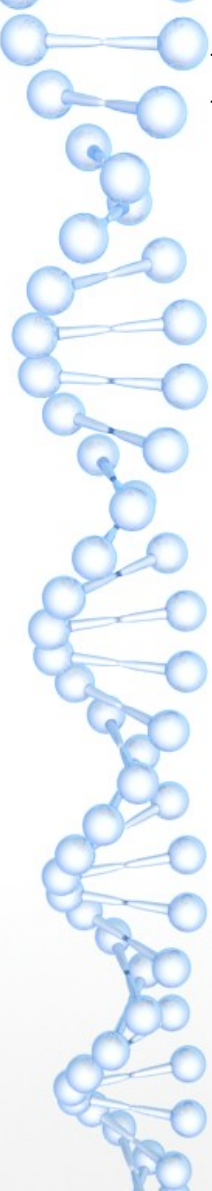
# Multi-Cloud Security – OWASP Top 10 Privacy

“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.

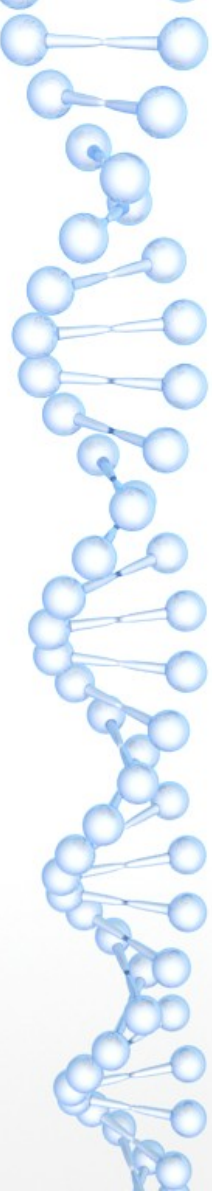
Root cause analysis – Developers  
- Operations  
- or Security





# 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

MITRE ATT&CK™ Navigator

Click Scoring button and enter score

layer x help x +

selection controls layer controls technique controls

score 1 |

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Impact
10 items	33 items	58 items	28 items	63 items	19 items	20 items	17 items	13 items	9 items	21 items
Drive-by Compromise	AppleScript CMSTP	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	Command-Line Interface	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Compiled HTML File	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	AppCert DLLs	Applnit DLLs	Bypass User Account Control	Credential Dumping	Bookmarks	Exploitation of Remote Services	Data from Information Repositories	Data Transfer	Custom Command and Control Protocol
Spearphishing Attachment	Dynamic Data Exchange	Applnit DLLs	Application Shimmming	Clear Command History	Credentials in Files	Discovery	Logon Scripts	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through API	Application Shimmming	Bypass User Account Control	Code Signing	Credentials in Registry	File and Directory Discovery	Pass the Hash	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through Module Load	Authentication Package	DLL Search Order Hijacking	Compiled HTML File	Exploitation for Credential Access	Network Service Scanning	Pass the Ticket	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Exploitation for Client Execution	BITS Jobs	Dylib Hijacking	Component Firmware	Forced Authentication	Network Share Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Component Object Model Hijacking	Hooking	Network Sniffing	Remote File Copy	Data Staged	Fallback Channels	Multi-hop Proxy
	Graphical User Interface	Browser Extensions	Change Default File Association	Control Panel Items	Input Capture	Password Policy Discovery	Remote Services	Email Collection		
	InstallUtil	Component	Extra Window Memory Injection	DCShadow	Input Prompt	Peripheral Device Discovery	Replication Through Removable	Input C		
	Launchctl	Component		Deobfuscate/Decode Files or Information	Kerberoasting					

legend



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

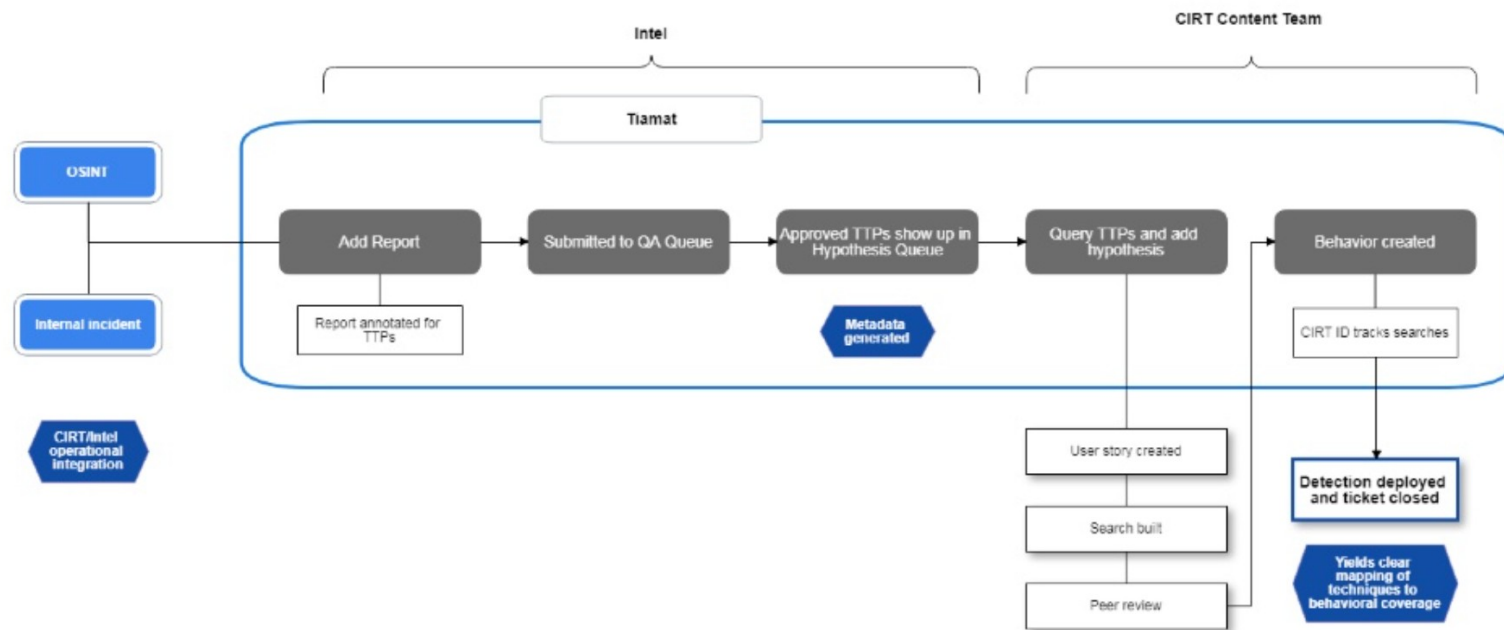
**MITRE ATT&CK - Initial access: APT19**

## Techniques Used

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

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

Tiamat-enabled operationalized ATT&CK process





# Multi-Cloud Security

## OWASP Top 10 Privacy & MITRE ATT&CK

### Security

Compiled HTML File  
Control Panel Items  
Dynamic Data Exchange  
Execution through API  
Execution through Module Load  
Exploitation for Client Execution

### Privacy

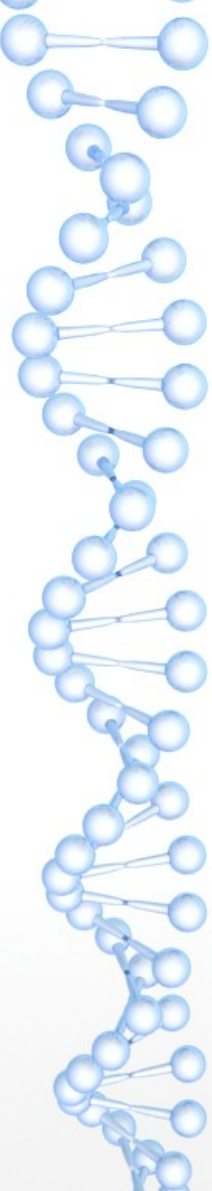
# Records ?

But what else..?

HTTP malware variant used Base64 to encode communications to the C2 server.<sup>[4]</sup>

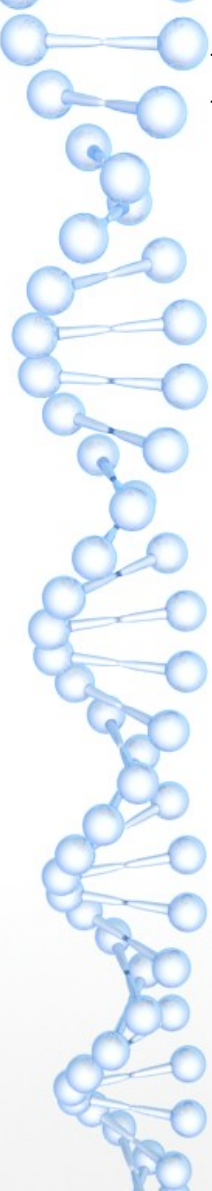
HTTP malware variant decrypts strings using single-byte XOR keys.<sup>[4]</sup>

# 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	<b>SPECIFIC INDIVIDUALS ONLY</b>		
Customers' email addresses	<b>WORKGROUPS CONFIDENTIAL</b>		Used as main identifier on login.
Database credentials	<b>WORKGROUPS CONFIDENTIAL</b>	Only usable from with AWS	
Application logs	<b>WORKGROUPS CONFIDENTIAL</b>		Contains publicly identifiable information (IP addresses, etc.)
Aggregate revenue	<b>STAFF CONFIDENTIAL</b>	Made public quarterly	Also available in the payment service, no damage if lost.
Application source code	<b>PUBLIC</b>		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	
Control Panel Items	
Dynamic Data Exchange	Web application vulnerabilities
Execution through API	Insufficient Breach Response
Execution through Module Load	More....?
Exploitation for Client Execution	



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

## Security

Compiled HTML File  
Control Panel Items  
Dynamic Data Exchange  
Execution through API  
Execution through Module Load  
Exploitation for Client Execution

## Privacy

### Benefits

### Better Security / Privacy Correlation

coding / refactoring – TDD ?

\*\* Privacy-by- (re) Discovery  
& better Privacy by Design