Cloud & Identity Evaluation Methodology

Table of Contents

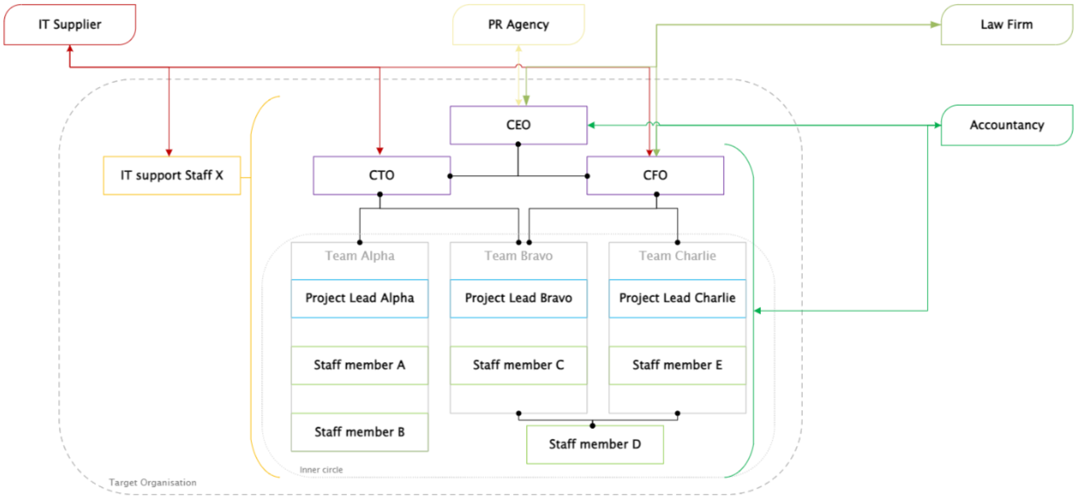
1. Goals

This evaluation aims to evaluate the effectiveness of solutions when dealing with cloud and identity focused attackers. Identity based attacks are defined threats that focus on impersonating, stealing or misusing an entity's digital identity to achieve its goals. Examples of such behaviours include exploiting identity management systems, user credentials and authentication systems.

2. Environment

A target organisation is maintained with digital identities and communication patterns to reflect roles within an organisation. Communications are defined as any exchange of information between two parties via an electronic method. These can be via e-mail, messaging platforms (Teams, Slack etc) or shared network resources.

These patterns are described below:



a. Internal common communication patterns and file types:

Source	Destination	Direction	Frequency	Type
Purple staff	Purple staff	Bi-directional	High	Email, Direct Message, Office File types
Purple staff	Green staff	Bi-directional	Low	Email, Direct Message
Purple staff	All	One way	Low	Email, Direct Message
CTO	Alpha & Bravo	Bi-directional	Medium	Email, Direct Message, Office File types, Archives, Executables
CFO	Bravo & Charlie	Bi-directional	Medium	Email, Direct Message, Office File types, Archives, Executables

Blue staff	Blue staff	Bi-directional	Medium	Email, Direct Message, Office File types
Green staff	Green staff	Bi-directional	High	Email, Direct Message, Office File types
Alpha team	Alpha team	Bi-directional	High	Email, Direct Message, Office File types, executables

Source	Destination	Direction	Frequency	Type
IT Support Staff	All (group)	Bi-directional	Medium	Email, Direct Message, Office File types
IT Support Staff	All (individual)	Bi-directional	Low	Email, Direct Message, Office File types, executables

b. External common communication patterns and file types

Source	Destination	Direction	Frequency	Type
IT support, CTO, CFO	IT Supplier	One way	Low	Email, Office File types
CEO	PR Agency	Bi-directional	Medium	Email, Office File types
CEO, CFO	Law Firm	Bi-directional	Medium	Email, Office File types
CEO, CFO	Accountancy	Bi-directional	Medium	Email, Office File types
Accountancy	All (individual)	One way	Low	Email, Office File types
PR Agency	Blue & Purple	Bi-directional	Low	Email, Office File types

Within the organisation, shared network resources and cloud apps are accessed by the staff members.

3. Execution

The evaluation has 3 phases, behaviour baselining, attack and legitimate behaviour.

Behaviour baselining is executed for a recommended duration of two weeks where “normal” behaviour of the target organisation is observed. Key metrics will be taken are alert volume and any deviation necessary in behaviour due to the product interaction with the environment. Solutions can deviate from the two-week period if necessary to get an accurate understanding of the organisation, this will have an impact on the duration of the legitimate section of the evaluation and will be disclosed in the report.

The attacking period is comprised of two phases. The test corpus is split into scenarios based on specific goals of attackers. If tested solutions do not have complete coverage of the corpus these will be considered out of scope and disclosed in any reporting.

The attacking scenarios are focused on identity and cloud assets of the target organisation.

Identity scenarios focus on targeting an organization's digital identities with the primary objective of gaining unauthorized access or leveraging communication channels to establish a foothold within the organization. The key metrics are visibility and alert efficiency.

Cloud asset scenarios focus on targeting an organization's cloud infrastructure, services, and data with the primary objective of exploiting misconfigurations, vulnerabilities, or weak access controls to compromise sensitive assets or gain unauthorized access. While there is crossover of tradecraft between the two types of scenarios, identity is the core point of exploiting a victim organisation.

Legitimate behaviour is executed after the attacking period with any necessary adjustments on the target organisation after the attacking period. The key metrics measure are alert efficiency and false positive rate.

4. Attack Rating

Scenarios include specific metrics to evaluate the solution's effectiveness in addressing the threat.

a) Identity Scenario Rating

Ongoing attack rating is represented by the detections occurring during the attacker's activity.

Post compromise rating is represented by any detections or data enriched after the activity has occurred.

Alert efficiency is calculated as a percentage using the baselined number of informational alerts gathered during the baselining period. The total number of alerts during each phase of the test is disclosed.

b) Cloud Asset Detection Rating

Ratings will be given per attack sequence. While direct references to the corresponding ATT&CK technique are useful they are not required to earn detection points. Data sources are marked and mapped to the corresponding source but do not influence the final accuracy rating. Within each defined tactic scope of a test case the solution must detect 50% of the techniques used to earn the maximum grade.

For example:

Sequence	Technique	Tactic	Min # Ts	Rating
Intrusion	T1566.001	Initial Access (1)	1	+10
Infiltration	T1204 T1059.001 T1047	Execution (3)	1	+10
	T1053.005 T1078.002 T1078.003 T1078.004 T1547.001	Persistence (5)	1	
	T1053.005 T1078.002 T1078.003 T1078.004	Privilege Escalation (4)	2	
	T1070.004 T1070.006 T1036.005 T1140 T1484.002 T1562.004 T1562.001 T1562.002 T1070.008	Defense Evasion (9)	4	
	T1555.003 T1606.001 T1003.006 T1558.003 T1539	Credential Access (5)	2	
Propagation	T1087.002 T1482 T1018	Discovery (3)	1	+10
	T1021.006	Lateral Movement(1)	1	
	T1005 T1114.002 T1560.001 T1213.003 T1074.002	Collection (5)	2	
	T1048.002	Exfiltration (1)	1	

5. Legitimate Rating

Alert efficiency and false positives are the two key metrics that affect the legitimate rating and are major factors that can increase the running costs of a solution.

Alert efficiency is measured during all three phases of the engagement with the total number of alerts during the engagement disclosed. This metric is disclosed for each phase of the engagement.

Legitimate scenarios are crafted to reflect common behaviour in an organisation. These are provided during the deployment phase of the product. Any learned behaviour that affects the standard practices of the solution is reflected in the final report.

Rating:

Severity Level	Unknown behaviour	Learned/Established Behaviour
Informational/No/Low Priority	+10	+10
Amber/Medium	+5	-5
Red/High	0	-10
Configuration change required (modifier)	+5	

The configuration change modifier can be applied to any sub-optimal rating achieved.

6.Configuration disclosure

A full configuration and licencing disclosure is taken as part of any public report. If possible, this will be hosted under Artifact Security website. Linked references to the tested vendor resource are also acceptable.

7.Change Log

04/11/2024 – v1 Document created – Identifier - Cloud & Identity Evaluation 2025 v1.0