O365 MITRE ATT&CK MODEL

Version	1.0
Author	Mohammed Arief A
Designation	Security Lead
Date	07 OCT 2022

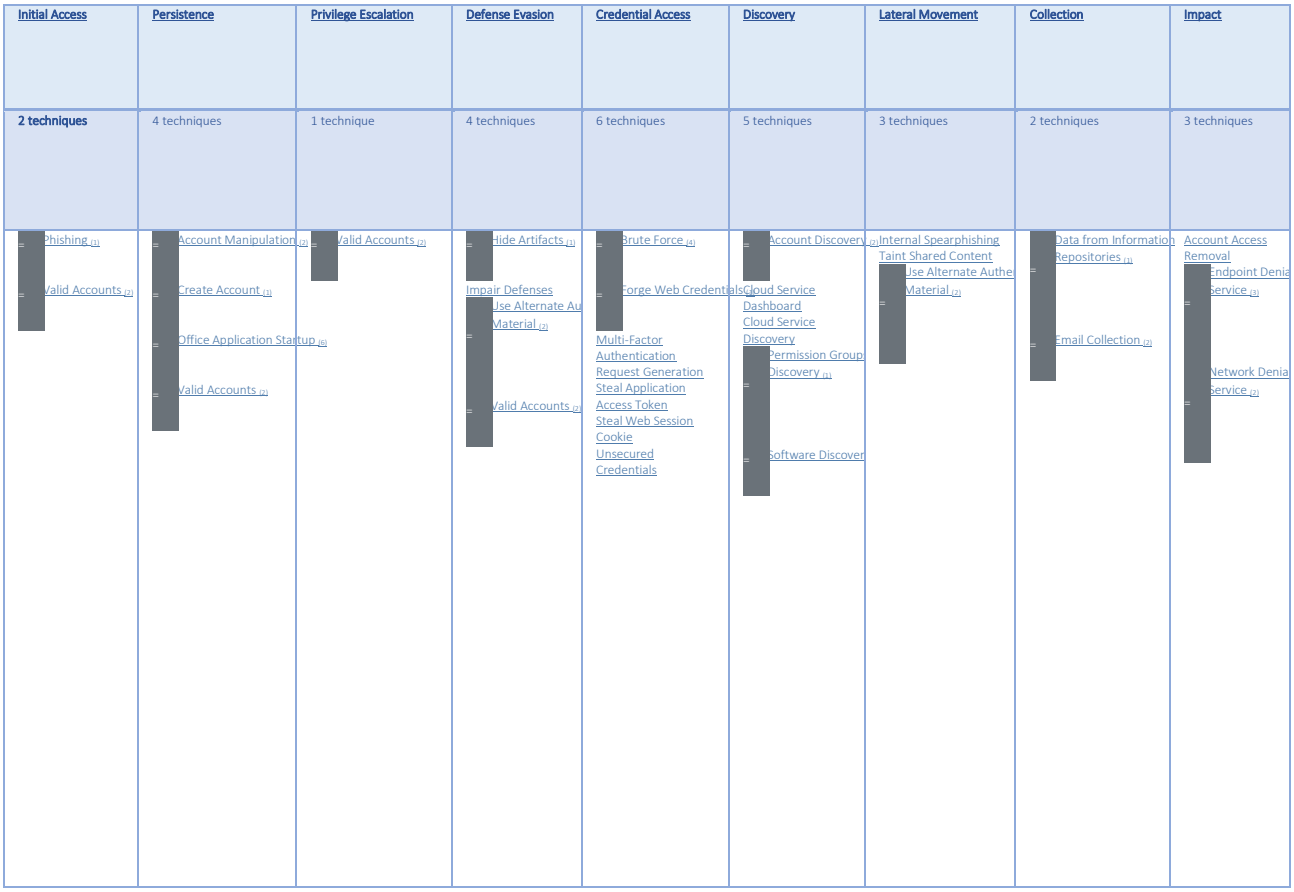
Overview:

MITRE ATT&CK® is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

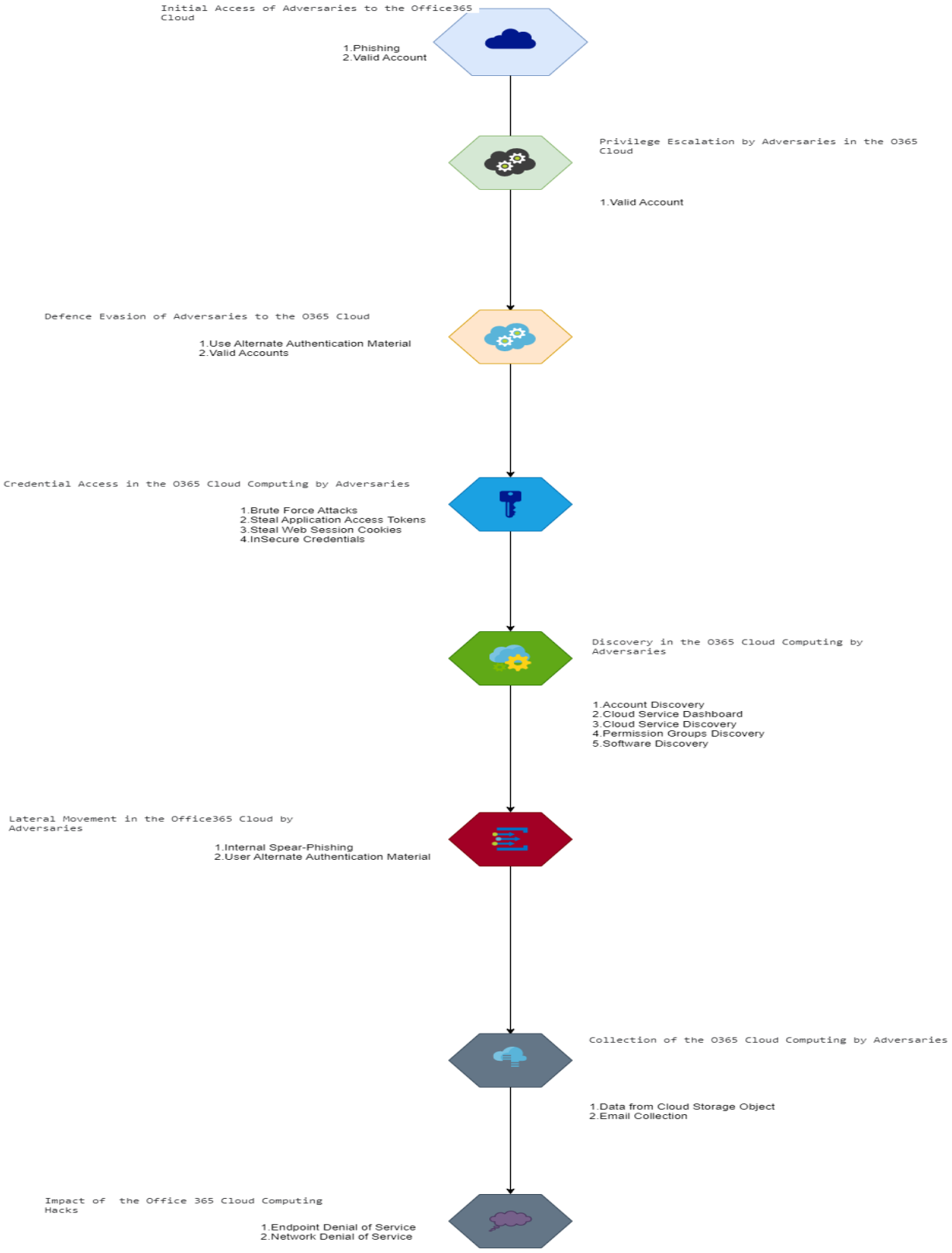
Matrix:

TA0001: Initial Access	TA0003: Persistence	TA0004: Privilege Escalation	TA0005: Defense Evasion	TA0007: Discovery	TA0006: Credential Access	TA0008: Lateral Movement	TA0009: Collection	TA0040: Impact
T1566: Phishing	T1098: Account Manipulation	T1078: Valid Accounts	T1564: Hide Artifacts	T1087: Account Discovery	T1110: Brute Force	T1534: Internal Spearphishing	T1213: Data from Information Repositories	T1531: Account Access Removal
T1078: Valid Accounts	T1136: Create Account		T1562: Impair Defenses	T1538: Cloud Service Dashboard	T1606: Forge Web Credentials	T1080: Taint Shared Content	T1114: Email Collection	T1499: Endpoint Denial of Service
	T1137: Office Application Startup		T1550: Use Alternate Authentication Material	T1526: Cloud Service Discovery	T1621: Multi-Factor Authentication Request Generation	T1550: Use Alternate Authentication Material		T1498: Network Denial of Service
	T1078: Valid Accounts		T1078: Valid Accounts	T1069: Permission Groups Discovery	T1528: Steal Application Access Token			
				T1518: Software Discovery	T1539: Steal Web Session Cookie			
					T1552: Unsecured Credentials			

MITRE Overview:



Workflow:


Initial Access of Adversaries to the Office365 Cloud
1.Phishing
2.Valid Account
Privilege Escalation by Adversaries in the O365 Cloud
1.Valid Account
Defence Evasion of Adversaries to the O365 Cloud
1.Use Alternate Authentication Material
2.Valid Accounts
Credential Access in the O365 Cloud Computing by Adversaries
1.Brute Force Attacks
2.Steal Application Access Tokens
3.Steal Web Session Cookies
4.InSecure Credentials
Discovery in the O365 Cloud Computing by Adversaries
1.Account Discovery
2.Cloud Service Dashboard
3.Cloud Service Discovery
4.Permission Groups Discovery
5.Software Discovery
Lateral Movement in the Office365 Cloud by Adversaries
1.Internal Spear-Phishing
2.User Alternate Authentication Material
Collection of the O365 Cloud Computing by Adversaries
1.Data from Cloud Storage Object
2.Email Collection
Impact of the Office 365 Cloud Computing Hacks
1.Endpoint Denial of Service
2.Network Denial of Service