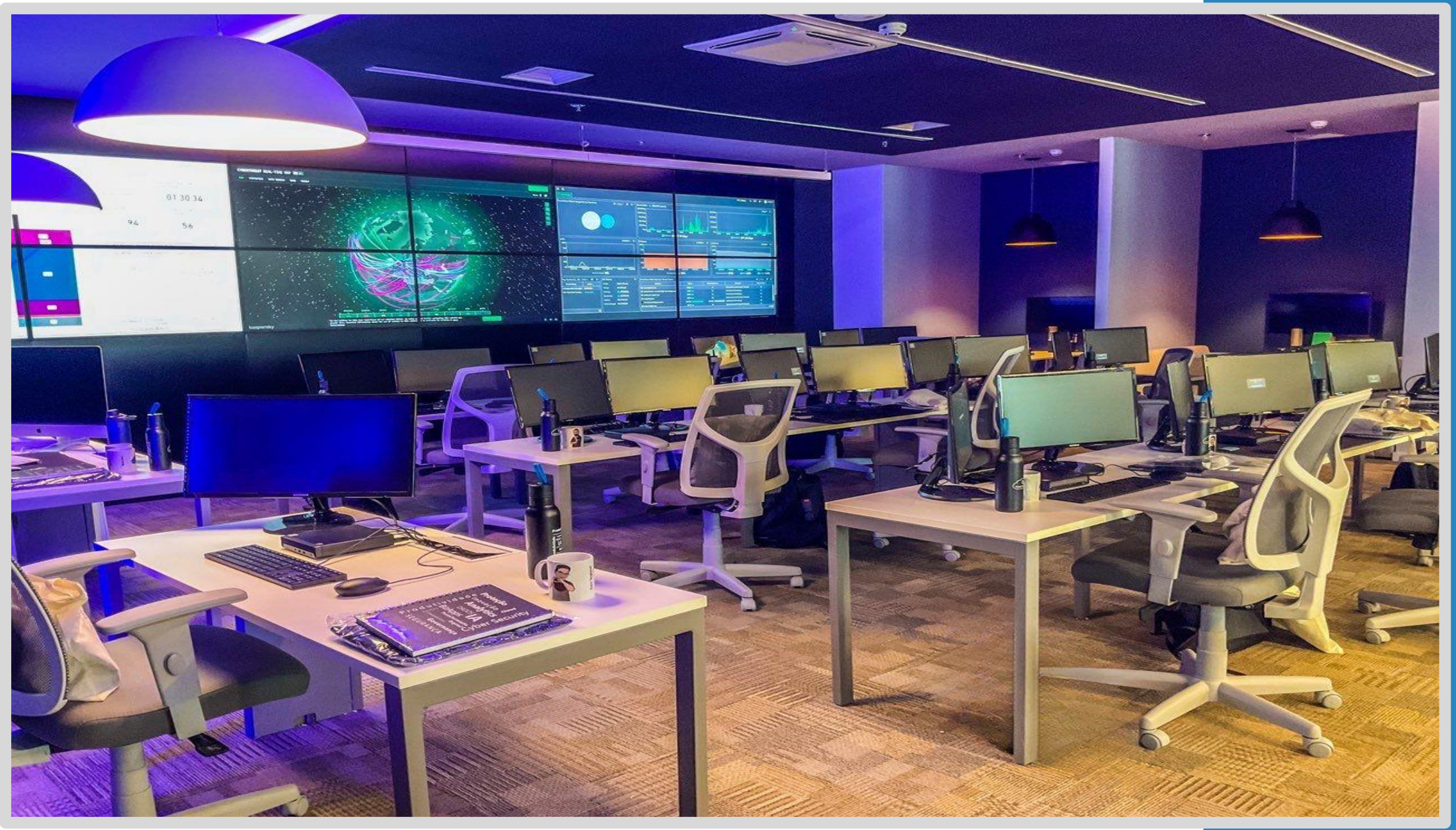


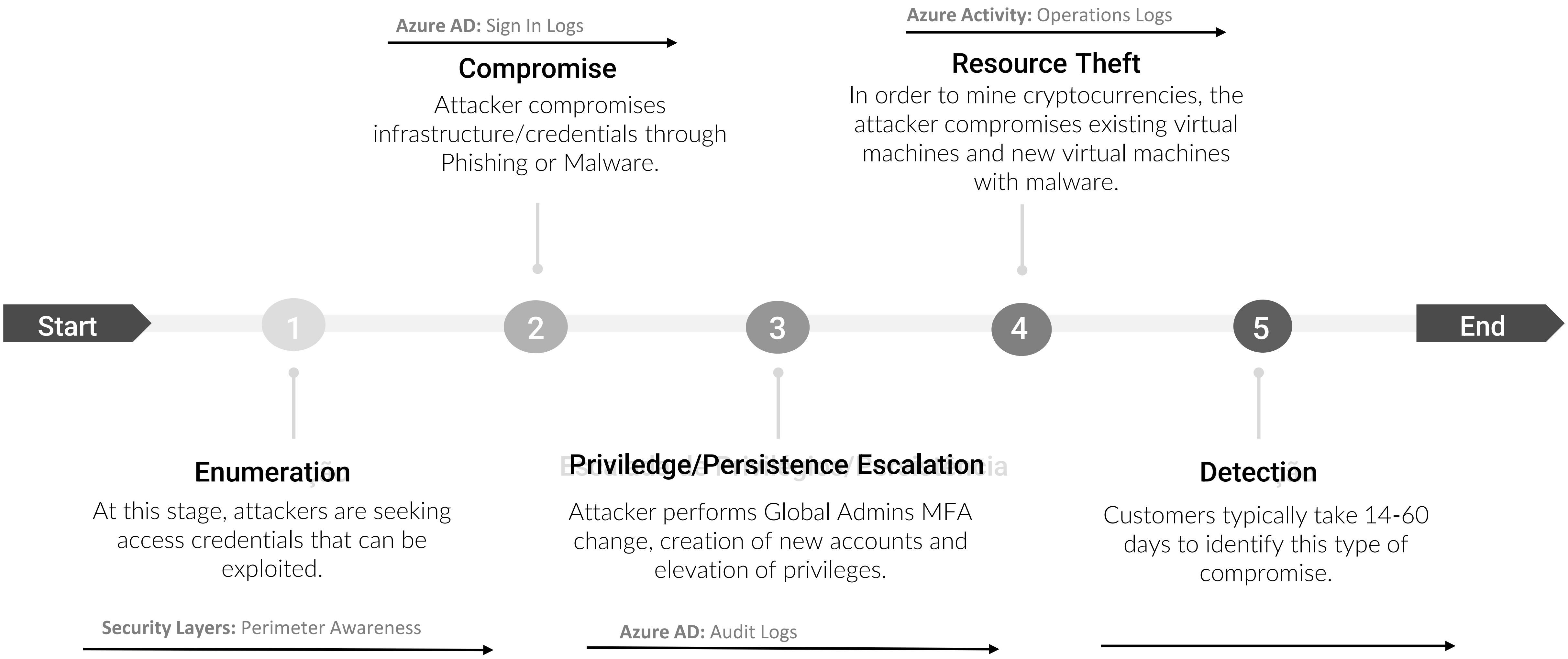
Cloud Target

Productivity | Security | Governance

Cyber Defense Center
&
Managed Security Services

#ZeroTrust #AI

CDC: ATTACKER ACTIONS



Security Layers: Perimeter Awareness

Enumeration

At this stage, attackers are seeking access credentials that can be exploited.

Azure AD: Sign In Logs

Compromise

Attacker compromises infrastructure/credentials through Phishing or Malware.

Azure AD: Audit Logs

Priviledge/Persistence Escalation

Attacker performs Global Admins MFA change, creation of new accounts and elevation of privileges.

Azure Activity: Operations Logs

Resource Theft

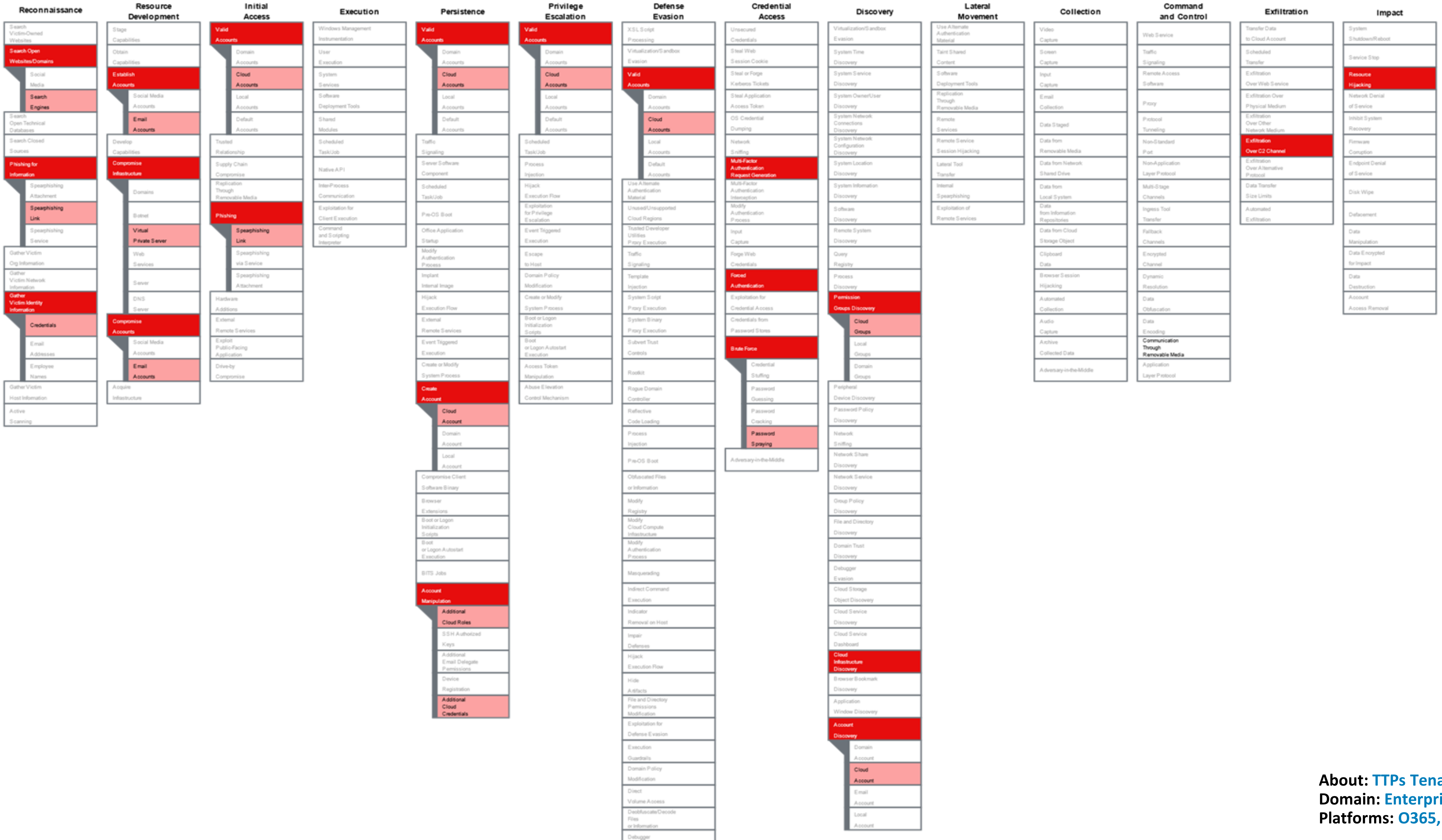
In order to mine cryptocurrencies, the attacker compromises existing virtual machines and new virtual machines with malware.

Detection

Customers typically take 14-60 days to identify this type of compromise.

CDC: TTPs – Mitre ATT&CK

Cloud Target



Reconnaissance
- Search Victim-Owned Websites
- **Search Open Websites/Domains**
  - Social Media
  - **Search Engines**
- Search Open Technical Databases
- Search Closed Sources
- **Phishing for Information**
  - Spearphishing Attachment
  - **Spearphishing Link**
  - Spearphishing Service
- Gather Victim Org Information
- Gather Victim Network Information
- **Gather Victim Identity Information**
  - **Credentials**
  - Email Addresses
  - Employee Names
- Gather Victim Host Information
- Active Scanning

Resource Development
- Stage Capabilities
- Obtain Capabilities
- **Establish Accounts**
  - Social Media Accounts
  - **Email Accounts**
- Develop Capabilities
- **Compromise Infrastructure**
  - Domains
  - Botnet
  - **Virtual Private Server**
  - Web Services
  - Server
  - DNS Server
- **Compromise Accounts**
  - Social Media Accounts
  - **Email Accounts**
- Acquire Infrastructure

Initial Access
- **Valid Accounts**
  - Domain Accounts
  - **Cloud Accounts**
  - Local Accounts
  - Default Accounts
- Trusted Relationship
- Supply Chain Compromise
- Replication Through Removable Media
- **Phishing**
  - **Spearphishing Link**
  - Spearphishing via Service
  - Spearphishing Attachment
- Hardware Additions
- External Remote Services
- Exploit Public-Facing Application
- Drive-by Compromise

Execution
- Windows Management Instrumentation
- User Execution
- System Services
- Software Deployment Tools
- Shared Modules
- Scheduled Task/Job
- Native API
- Inter-Process Communication
- Exploitation for Client Execution
- Command and Scripting Interpreter

Persistence
- **Valid Accounts**
  - Domain Accounts
  - **Cloud Accounts**
  - Local Accounts
  - Default Accounts
- Traffic Signaling
- Server Software Component
- Scheduled Task/Job
- Pre-OS Boot
- Office Application Startup
- Modify Authentication Process
- Implant Internal Image
- Hijack Execution Flow
- External Remote Services
- Event Triggered Execution
- Create or Modify System Process
- **Create Account**
  - **Cloud Account**
  - Domain Account
  - Local Account
- Compromise Client Software Binary
- Browser Extensions
- Boot or Logon Initialization Scripts
- Boot or Logon Autostart Execution
- BITS Jobs
- **Account Manipulation**
  - **Additional Cloud Roles**
  - SSH Authorized Keys
  - Additional Email Delegate Permissions
  - Device Registration
  - **Additional Cloud Credentials**

Privilege Escalation
- **Valid Accounts**
  - Domain Accounts
  - **Cloud Accounts**
  - Local Accounts
  - Default Accounts
- Scheduled Task/Job
- Process Injection
- Hijack Execution Flow
- Exploitation for Privilege Escalation
- Event Triggered Execution
- Escape to Host
- Domain Policy Modification
- Create or Modify System Process
- Boot or Logon Initialization Scripts
- Boot or Logon Autostart Execution
- Access Token Manipulation
- Abuse Elevation Control Mechanism

Defense Evasion
- XSL Script Processing
- Virtualization/Sandbox Evasion
- **Valid Accounts**
  - Domain Accounts
  - **Cloud Accounts**
  - Local Accounts
  - Default Accounts
- Use Alternate Authentication Material
- Unused/Unsupported Cloud Regions
- Trusted Developer Utilities Proxy Execution
- Traffic Signaling
- Template Injection
- System Script Proxy Execution
- System Binary Proxy Execution
- Subvert Trust Controls
- Rootkit
- Rogue Domain Controller
- Reflective Code Loading
- Process Injection
- Pre-OS Boot
- Obfuscated Files or Information
- Modify Registry
- Modify Cloud Compute Infrastructure
- Modify Authentication Process
- Masquerading
- Indirect Command Execution
- Indicator Removal on Host
- Impair Defenses
- Hijack Execution Flow
- Hide Artifacts
- File and Directory Permissions Modification
- Exploitation for Defense Evasion
- Execution Guardrails
- Domain Policy Modification
- Direct Volume Access
- Deobfuscate/Decode Files or Information
- Debugger

Credential Access
- Unsecured Credentials
- Steal Web Session Cookie
- Steal or Forge Kerberos Tickets
- Steal Application Access Token
- OS Credential Dumping
- Network Sniffing
- **Multi-Factor Authentication Request Generation**
- Multi-Factor Authentication Interception
- Modify Authentication Process
- Input Capture
- Forge Web Credentials
- **Forced Authentication**
- Exploitation for Credential Access
- Credentials from Password Stores
- **Brute Force**
  - Credential Stuffing
  - Password Guessing
  - Password Cracking
  - **Password Spraying**
- Adversary-in-the-Middle

Discovery
- Virtualization/Sandbox Evasion
- System Time Discovery
- System Service Discovery
- System Owner/User Discovery
- System Network Connections Discovery
- System Network Configuration Discovery
- System Location Discovery
- System Information Discovery
- Software Discovery
- Remote System Discovery
- Query Registry
- Process Discovery
- **Permission Groups Discovery**
  - **Cloud Groups**
  - Local Groups
  - Domain Groups
- Peripheral Device Discovery
- Password Policy Discovery
- Network Sniffing
- Network Share Discovery
- Network Service Discovery
- Group Policy Discovery
- File and Directory Discovery
- Domain Trust Discovery
- Debugger Evasion
- Cloud Storage Object Discovery
- Cloud Service Discovery
- Cloud Service Dashboard
- **Cloud Infrastructure Discovery**
- Browser Bookmark Discovery
- Application Window Discovery
- **Account Discovery**
  - Domain Account
  - **Cloud Account**
  - Email Account
  - Local Account

Lateral Movement
- Use Alternate Authentication Material
- Taint Shared Content
- Software Deployment Tools
- Replication Through Removable Media
- Remote Services
- Remote Service Session Hijacking
- Lateral Tool Transfer
- Internal Spearphishing
- Exploitation of Remote Services

Collection
- Video Capture
- Screen Capture
- Input Capture
- Email Collection
- Data Staged
- Data from Removable Media
- Data from Network Shared Drive
- Data from Local System
- Data from Information Repositories
- Data from Cloud Storage Object
- Clipboard Data
- Browser Session Hijacking
- Automated Collection
- Audio Capture
- Archive Collected Data
- Adversary-in-the-Middle

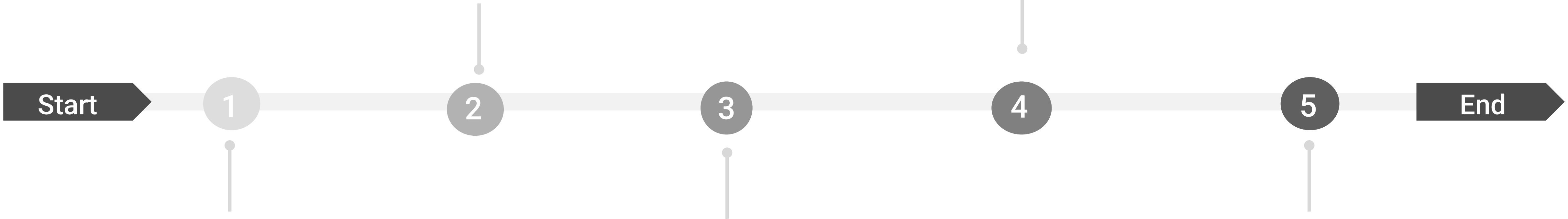
Command and Control
- Web Service
- Traffic Signaling
- Remote Access Software
- Proxy
- Protocol Tunneling
- Non-Standard Port
- Non-Application Layer Protocol
- Multi-Stage Channels
- Ingress Tool Transfer
- Fallback Channels
- Encrypted Channel
- Dynamic Resolution
- Data Obfuscation
- Data Encoding
- Communication Through Removable Media
- Application Layer Protocol

Exfiltration
- Transfer Data to Cloud Account
- Scheduled Transfer
- Exfiltration Over Web Service
- Exfiltration Over Physical Medium
- Exfiltration Over Other Network Medium
- **Exfiltration Over C2 Channel**
- Exfiltration Over Alternative Protocol
- Data Transfer Size Limits
- Automated Exfiltration

Impact
- System Shutdown/Reboot
- Service Stop
- **Resource Hijacking**
- Network Denial of Service
- Inhibit System Recovery
- Firmware Corruption
- Endpoint Denial of Service
- Disk Wipe
- Defacement
- Data Manipulation
- Data Encrypted for Impact
- Data Destruction
- Account Access Removal

About: TTPs Tenants Compromised
Domain: Enterprise ATT&CK v11
Platforms: O365, Azure AD, SaaS e IaaS

CDC: Cloud Target Solution – CTAntifraud



Enummeration

Pentest

We perform **quarterly** penetration tests on Microsoft Azure platforms mapping vulnerabilities and recommending solutions.

Compromise

Identity and Access Management

24x7 Azure AD monitoring, focusing on Sign -in attempts, Apps & Service Main activities with unusual signs that indicate compromise. This monitoring stops the attacker in the initial phase.

Privillege/Persistence Escalation

Access and Identity Management

24x7 Azure AD monitoring focusing on anomalous behavior. This being creation of new users with administrative privileges or non- interactive activities of Apps & Service Principals. This monitoring indicates that the environment has already been compromised and the attacker is persisting.

Resource Theft

Workload Compliance and Security

24x7 behavior and activity monitoring caused by Azure subscriptions and their resources (if available MDC). Through this service pack, we are able to identify anomalous Azure activities. For instance, the creation of a VM. This is the impact stage, leading to financial losses to the customer.

Detection and Response

SOC/CSIRT

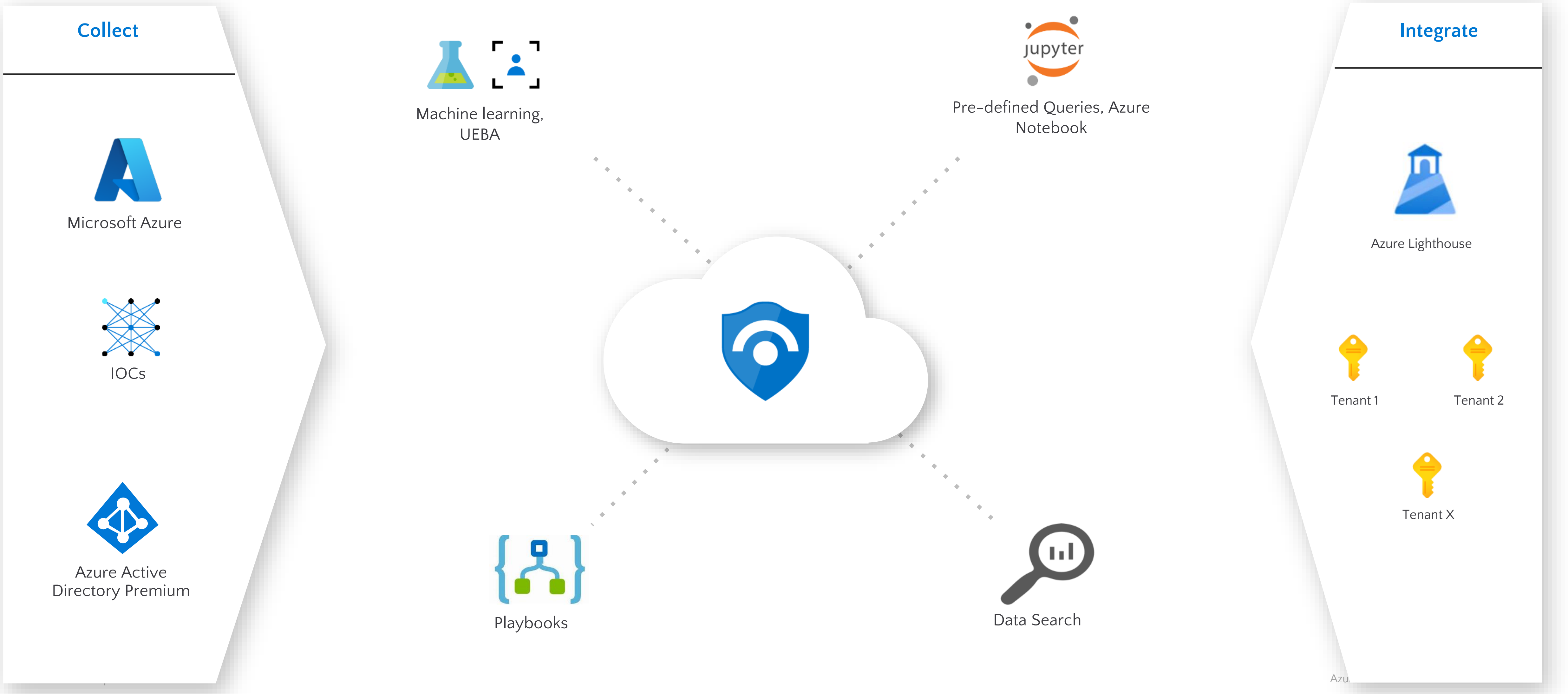
With a team focused **24x7** on detecting and responding to security incidents using Microsoft Sentinel as a SIEM tool, we are able to detect the initial stage of an attack in less than 30 minutes (test VM).

Alert: User Creation, Elevation of Privileges, Virtual Machine Creation.

Automation: Credencial blocking, notification of specific individuals.

CDC: Cloud Target Solution – CTAntifraud

Cloud Target



Collect

Microsoft Azure

IOCs

Azure Active Directory Premium

Machine learning, UEBA

Pre-defined Queries, Azure Notebook

Playbooks

Data Search

Integrate

Azure Lighthouse

Tenant 1

Tenant 2

Tenant X

Azu