Azure Incident Response Cheat Sheet

Introduction

With the rapid migration to the cloud, it's becoming increasingly difficult to keep track of all of the different data sources, commands, and tools available from each Cloud Service Provider (CSP). This cheat sheet is designed to provide incident responders and security professionals with an overview of key best practices, data sources, and tools that they can have at their disposal when responding to an incident in an Azure environment.

Active Directory (AKA Entra ID)

Azure Active Directory is Azure's cloud-based identity and access management service. It enables single sign-on and multi-factor authentication to help protect users from password fatigue and phishing attacks. It also provides group and device management capabilities.

When responding to an incident Involving AD, leverage these commands to perform key actions:

Identify and Deactivate Potentially Compromised User Accounts

Azure Active Directory has a built-in tool for identifying risky users and risky sign-ins. Head to the security menu and under "report," you can find the risky users. You can search through user/sign-in data for the past 30 days to aid your investigation.

There is also the "Risk detections" tab that contains reports for things such as anonymous IP addresses or password spray attacks that cover the last 90 days.

Deactivate an Azure Active Directory User Account

```
az ad user update --id <user_id> --account-enabled false
```

Identify which Applications AD Provides Authentication for

List Azure Active Directory Users

```
az ad user list
```

List Application Owners

```
az ad app owner list --id <Identifier_url, app_id,
or obj_id>
```

List Oauth2 Permission Grants

```
az ad app permission list-grants
```

List API permissions an App has Requested

```
az ad app permission list --id <app_id>
```

List Azure Active Directory Apps

```
az ad app list --all --display-name
```

Identify and Disable Legacy Authentication Methods

Identifying legacy authentication methods:

1. Navigate to the Azure portal > Azure Active Directory > Sign-in logs
2. Add the Client App column if it isn't shown by clicking on Columns > Client App
3. Select Add filters > Client App > choose all of the legacy authentication protocols and select Apply

Microsoft provides a guide to blocking legacy authentication whether directly or indirectly and guidance on which option suits different environments.

Snapshots

Snapshots in Azure are a crucial feature for digital forensics purposes. They are point-in-time copies of your Azure instances. These snapshots serve as backups and can be used for forensics and incident response.

Create a Snapshot:

```
az snapshot create -g
<Resourcegroup> -n
<snapshot_name> --source
<Source>
```

Grant read-only access to a Snapshot:

```
az snapshot grant-access
--duration-in-seconds 3600
--name <Snapshot_name>
--resource-group
<Resourcegroup>
```

Download Snapshot:

```
azcopy cp “<snapshot URL>"
“c:\temp\snapshot.vhd"
--check-md5 nocheck
```

List Snapshots in a resource Group:

```
az snapshot list
--resource-group
<Resourcegroup>
```

Get info about a snapshot:

```
az snapshot show  --name
<Snapshot_name>
```

Key Logs in Azure

Tenant logs (enabled by default with 30 days retention)
Contain **Sign-in Logs** consisting of Sign-in history and activity and **Audit Logs** consisting of active directory changes.

Subscription logs (activity logs) (enabled by default with 90 days retention)
Contain logs that detail operations on each Azure service at the management plane. These logs are used to determine the *who, what*, and *when* for any write operations with a single activity log for each Azure subscription.

Resource logs (requires enablement)
Contain logs about operations on each Azure service at the data plane level. These logs are used to track events such as database requests or key vault access attempts. The content of resource logs varies by service and resource type.

Extracting and Accessing Logs

Azure Portal
Within the Azure portal, users can easily access both Tenant and Subscription logs.

- **Tenant logs:** Sign-in logs and audit logs can be downloaded in CSV or JSON format (up to 100,000 rows for sign-in logs or 250,000 for audit logs).
- **Subscription logs (activity logs):** Can be downloaded in CSV format only (up to 1,000 rows)

Log Analytics Workspace
If configured correctly, **resource**, **operating system** and **application logs** can all be sent to the same workspace and queried via KQL (Kusto query language) and exported.

Storage Account
Logs can be exported to a storage account and be retained for as long as needed (though storage fees apply). A JSON file will be created for each hour of logs.

Event Hub
Event Hub provides real-time data processing. Once data is in the event hub, it can be accessed either via a SIEM or via its API. More information about using Event Hub can be found here.

Azure Incident Preparedness

Know Your Data

Know where sensitive data is stored, processed and backed up.

List All Storage Accounts

```
az storage account list
```

List All Virtual Machines

```
az vm list
```

Have Backups and Test That They Work

Azure has a native backup service called Azure Backup with support for VMs, databases, and other services. This can provide protection from both data loss and ransomware.

Restrict Administrative Accounts

A policy of least privilege should be followed. Microsoft has a detailed guide on locking down accounts here.

Require Multi-Factor Authentication for all User Accounts

Enabling multi factor authentication can protect against phishing and brute force attacks.

Check if User has MFA Enabled

(PowerShell)

```
$Msolcred = Get-credential
Connect-MsolService -Credential $MsolCred
Get-MsolUser -All | where
{$_.StrongAuthenticationMethods -ne $null} |
Select-Object -Property UserPrincipalName,
DisplayName
```

Check Users with no MFA Enabled

(PowerShell)

```
Get-MsolUser -All | where
{$_.StrongAuthenticationMethods.Count -eq
0} | Select-Object -Property
UserPrincipalName, DisplayName
```

Review Azure Security Center Settings

Azure Security Center provides a centralized overview of security issues and configuration options. Unfortunately, many of the most useful features need to be enabled (at cost) in advance of any breach.

Get Security Alerts for Current Subscription

```
az security alert list
```

Get Security Alerts for a Resource Group

```
az security alert list -g “<ResourceGroup>”
```

List all Alerts Suppression Rules on Current Subscription

```
az security alerts-suppression-rule list
```

Limit Network and Remote Access

Limit any connectivity to the internet from your machines as much as possible. Microsoft has a guide on filtering network traffic using network security groups here.

List Security Groups with SSH (22) Open to Internet

```
az network nsg list \ --query
"[?securityRules[?access == 'Allow']].[name]
&& [?securityRules[?destinationPortRange ==
'22']].[name]"
```

List Security Groups with RDP (3389) Open to Internet

```
az network nsg list \ --query
"[?securityRules[?access == 'Allow']].[name]
&& [?securityRules[?destinationPortRange ==
'3389']].[name]"
```

Enable Logging

if logging is not correctly enabled and configured, there may be no record of key events or changes. This could lead to a incomplete investigation. Both Data Dog and Secure Works have great tutorials on how to ensure full logging is enabled.

Open Source Tools

Azure AD Incident Response PowerShell Module: A wide range tool kit for dealing with compromised AD response
Sparrow: Identifies compromised accounts in AD
Mandiant Azure AD Investigator: Powershell Module for detecting artefacts and other threat actor activity
Azure Hound: Collects various data from Azure
Hawk: Retrieves data for 365 Investigations
CrowdStrike Reporting Tool for Azure: Identifies possible security issues with permissions and configuration settings
Cloud Forensic Utils: Retrieves forensic data from virtual machines
Microsoft Extractor Suite: A tool to streamline log and data extraction across microsoft products

Azure Native Tools

Azure Security Center
Basic/default monitoring via logs and analytics engine

Azure Sentinel
SIEM and automation across entire environment

Azure Defender
Advanced workload protection for select resources

Cado Tools

Cado Security provides the first and only cloud-native digital forensics platform for enterprises. By automating data capture and processing across cloud and container environments, the Cado platform enables security teams to effectively investigate and respond to cyber incidents at cloud speed.

If you'd like to learn more about what Cado Security is doing to help advance investigations and incident response, **request a demo today**.

More Information

Further reading and resources:

SANS Posters and cheat sheets
SANS Azure Log extraction

Microsoft playbooks for particular scenarios:

Phishing Investigation
Password Spray Investigation
Ransomware Attack

App Consent Grant
Compromised or Malicious Application
Forensic / Legal Investigation