# *Office 365 Extractor*
# *Cheat Sheet*

This cheat sheet contains operations and keywords that are commonly used to search the unified audit log for suspicious activity. The following four categories are common areas to begin analysis:

## Forwarding Rules

***Detect new rules***

- New-InboxRule
- New-TransportRule

***Detect rules being modified***

- Set-Mailbox
- Set-InboxRule
- Set-TransportRule

***Detect active rules***

- DeliverToMailboxAndForward
- ForwardingSMTPAddress
- ForwardingAddress
- SentTo
- BlindCopyTo
- ForwardTo

## Permission Changes

***Detect mailbox permission changes***

- Add-MailboxPermission
- Add-RecipientPermission

***Detect folder permission changes***

- Add-MailboxFolderPermission
- Set-MailboxFolderPermission

***Detect group or role changes***

- Add member to role
- Add member to group

## Login Activity

***Detect brute forcing attacks***

- IdsLocked
- UserKey=“Not Available”

***Detect suspicious logins***

- MailboxLogin
- UserLoggedIn
- UserLoginFailed

***Detect MFA errors***

- UserStrongAuthClientAuthNRequired
- UserStrongAuthClientAuthNRequiredInterrupt

## Access Activity

***Detect access of a mailbox or item***

- Sync access
- Bind access

***Detect OAuth applications***

- Add oAuth2PermissionGrant
- Consent to application
- Add app role Assignment grant to user

pwc

**Contact Us**
nl_incidentresponse@pwc.com

**GitHub**
www.github.com/PwC-IR/
Office-365-Extractor