Project Claritas – Office365 Integratie: User Manual

Met de Office365 cloud integratie kan u op één overzicht statistieken zien van de EntraID (AzureAD) logs. De informatie gaat over de events, sign-ins, secure score e.d.. We gebruikten Kibana en Elastic Search voor het representeren van de data op een leesbare manier, in één dashboard. U hoeft enkel de stappen te volgen die in deze user manual staan om de integratie op te zetten en te gebruiken.

Contents

1. Setup

1.1. Setup

1.1.1. EntraID: setup

Om de cloud integratie te gebruiken, moet er een app geregistreerd worden in EntraID. Volg deze stappen om correct een app te registreren met de juiste API permissies.

1. Login op https://admin.microsoft.com
2. Kies links ‘Identity’
3. Ga links naar: ‘Identity > Applications > App registrations’.
4. Klik op ‘New registration’.
5. Kies een naam en klik op ‘Register’.
6. Ga naar ‘API Permissions’.
7. Klik op ‘Add permission’.
8. Kies ‘Office 365 Management APIs’.
9. Kies ‘Application permissions’.
10. Vink volgende opties aan:
    - ‘ActivityFeed.Read’,
    - ‘ActivityFeed.ReadDlp’,

- ‘ServiceHealth.Read’.

11. Klik op ‘Add permissions’.
12. Herhaal stap 6 tot en met 10:
    - Kies ‘Microsoft Graph’.
    - Vink volgende opties aan:
        - ‘Application.Read.All’,
        - ‘AuditLog.Read.All’,
        - ‘Directory.Read.All’,
        - ‘SecurityEvents.Read.All’.
13. Klik op ‘Grant admin consent for’.

1.1.2. EntraID: vereiste gegevens terugvinden

Voor de volgende setups moeten er enkele gegevens vanuit EntraID gekopiëerd worden. Deze gegevens kan men alsvolgt vinden:

1.1.2.1. Tenant ID

1. Ga naar ‘Identity’.
2. Klik op ‘Overview’.
3. Onder ‘Basic Information’ kan de ‘Tenant ID’ teruggevonden worden.

1.1.2.2. Application ID

1. Ga links naar: ‘Identity > Applications > App registrations’.
2. Klik op de app die hiervoor werd aangemaakt.
3. Bij de overview van de app registration staat de ‘Application (client) ID’.

1.1.2.3. Client Secret

Om een ‘Client secret’ te krijgen, moet er een ‘client secret’ worden aangemaakt. Let op: na het aanmaken van het ‘client secret’ kan dit slechts één maal bekeken worden. Indien u naar een andere pagina navigeert, zal u het ‘client secret’ niet meer kunnen bekijken. Om de integraties te laten werken, mag er steeds maar één client secret tegelijk zijn. Anders zal de integratie niet naar behoren werken.

1. Ga links naar: ‘Identity > Applications > App registrations’.
2. Klik op de app die hiervoor werd aangemaakt.
3. Klik op ‘Certificates & Secrets’.
4. Klik op ‘New client secret’.
5. Vul de gevraagde gegevens in (‘Description’ en ‘Expiration’).
6. Het ‘client secret’ kan teruggevonden worden onder ‘Value’. Let op: het is deze waarde die gecensureerd zal worden wanneer u de pagina verlaat.

Indien u al een ‘client secret’ heeft, maar deze moet vervangen, bijvoorbeeld omdat u de waarde niet meer weet, dan kan u dat doen door op het vuilbak-icoon te klikken naast het ‘client secret’.

1.1.3. Microsoft Office 365: setup I: Scripts

Om de scripts te laten werken, moet de github repo gepulled worden. Python, de Elasticsearch Python library en Ansible moeten correct geïnstalleerd worden. Er moet ook een config file aangepast worden zodat de scripts correct werken.

1. Open een terminal van de Security Onion.
2. Voer de volgende commando's uit:
    1. git clone https://github.com/jonas638/SecurityProjectCloud.git
    2. sudo dnf install python3
    3. curl -O https://bootstrap.pypa.io/get-pip.py
    4. sudo python3 get-pip.py
    5. sudo pip3 install elasticsearch
    6. sudo pip3 install requests
3. Navigeer vervolgens naar de PythonElasticSearchScripts directory met gebruik van het 'cd' commando.
4. We moeten eerst enkele path's aanpassen. Pas telkens in de hieronder vermelde scripts config_path aan naar het pad van je config.json.
    - datastream_audit_logs.py
    - datastream_sec_score.py
    - datastream_signIns.py
    - Deze scripts bevinden zich in de 'datastreams' directory onder PythonElasticSearchScripts. Hier is een voorbeeld om een script aan te passen:
    1. Voer het volgende commando uit: sudo nano datastream_audit_logs.py
    2. Pas de waarde aan voor config_path.
    3. Doe ctrl + X.
    4. Druk 'Y'.
    5. Druk 'enter'.
    - securityScore.py
      Dit script bevindt zich in de 'securityScore' directory onder PythonElasticSearchScripts.
    - signIns_to_datastream.py
      Dit script bevindt zich in de 'tennantSignIns' directory onder PythonElasticSearchScripts.
    - Audit_to_datastream.py
      Dit script bevindt zich in de 'audit' directory onder PythonElasticSearchScripts.
5. Open config.json. Voer hiervoor volgend commando uit: sudo nano config.json
6. Vul de volgende gegevens in tussen de aanhalingstekens. Volg '1.1.2. EntraID: vereiste gegevens terugvinden' om de juiste waarden te krijgen.

- tenant_secret: vul hier uw 'client secret' in.
- client_id: vul hier uw 'application ID' in.
- tenant_id: vul hier uw 'tenant ID' in.
- security-onion_username: voer hier het email dat u instelde bij de installatie van uw Security Onion in.
- security-onion_password: voer hier het wachtwoord dat u instelde bij de installatie van uw Security Onion in.

7. Bewaar de instellingen door 'ctrl' en 'x' tegelijkertijd in te drukken. Druk vervolgens op Y om 'yes' te selecteren. Druk vervolgens op 'enter' om de config te bewaren.
8. Nu moeten we het path instellen.
9. Om ansible te installeren, voert u de volgende commando's uit in de terminal van uw Security Onion:
    1. sudo dnf install epel-release
    2. sudo dnf install ansible
10. Vervolgens runnen we het ansible playbook. Voer de volgende commando's uit in de terminal van uw Security Onion:
    1. cd /pad-naar-PythonElasticSearchScripts/auto_config
    2. ansible-playbook playbook.yml
11. Tenslotte moet de machine herstart worden. Voer het volgende commando uit in de terminal van uw Security Onion: sudo reboot

Tot slot moet u weten dat deze scripts regelmatig worden uitgevoerd, en daarbij logboeken genereren in /home/admin/PythonElasticSearchScripts/Logs/. Indien er een probleem is met de integratie, dan kan u deze logbestanden bekijken om te debuggen. Na verloop van tijd kunnen deze logbestanden behoorlijk groot worden en dus veel ruimte in beslag nemen. U dient dit in de gaten te houden. Wanneer deze bestanden te groot worden, dan mag u deze verwijderen. Het verwijderen van deze bestanden heeft geen effect op de werking van de integratie.

1.1.4. Microsoft Office 365: setup II: Kibana

Om de integratie toe te voegen, moeten de eerste keer enkele stappen ondernomen worden. De volgende stappen maken gebruik van Kibana.

1. Log in op het Security Onion dashboard.
2. Klik op 'Kibana' (sidebar: onder 'tools').
3. Open de sidebar.
4. Klik op 'Add integrations'
5. Bij 'Search for integrations' (niet de searchbar bovenaan): zoek en open 'Microsoft 365'.
6. Klik op 'Add Microsoft 365'.
7. Vul hier de volgende waarden in:

- ‘Base URL of Office Management API’: dit veranderd u enkel indien u een custom URL heeft. Anders laat u de default-waarde (‘https://manage.office.com’)
- ‘Interval’: deze waarde bepaalt het interval in de tijd waarmee de logs worden opgehaald. De standaard-waarde is ‘3m’ (3 minuten).
- ‘Directory (tenant) ID’: deze waarde is verplicht.
- ‘Application (client) ID’: deze waarde is verplicht.
- ‘Client Secret’: deze waarde is verplicht.

U kan de waarden terugvinden zoals beschreven bij ‘1.1.2. EntraID: vereiste gegevens terugvinden’.

Let op:

- Indien andere waarden veranderd worden, wordt de werking van de integratie niet gegarandeerd.
- Indien deze waarden foutief worden ingevoerd, zal de integratie niet werken. U kan indien nodig deze waarden op een later tijdstip altijd veranderen. Dit wordt later behandeld.

8. Selecteer vervolgens onderaan ‘Existing hosts’ en kies ‘so-grid-nodes_general’.
9. Klik vervolgens op ‘Save and continue’.
   Het opzetten van de integratie kan even duren.

Vervolgens moeten er dataviews gemaakt worden. Dit doet u als volgt:

1. Zoek in de search bar bovenaan ‘Data Views’. Kies ‘Kibana / Data Views’.
2. U moet 3 data views aanmaken.
   Let op: zorg ervoor dat de namen die hier beschreven staan exact (hoofdletter, kleine letter) worden overgenomen, tenzij anders vermeld. Anders werkt de integratie niet.
    1. logs-o365
        1. Klik op ‘Create data view’
        2. Kies als naam ‘logs-o365’
        3. Typ bij ‘Index pattern’: ‘logs-o365.audit’;
            - Vervolgens verschijnt er rechts een data stream bij ‘Matching sources’, zorg dat de waarde die u invoert bij ‘Index pattern’ de exacte naam van deze data stream is.
        4. Selecteer bij ‘Timestamp field’ de optie ‘@timestamp’.
        5. Klik op ‘Save data view to Kibana’.
    2. Identity Secure Score
        1. Klik op ‘Create data view’
        2. Kies als naam ‘Identity Secure Score’
        3. Typ bij ‘Index pattern’: ‘security_scores_stream’;

4. Selecteer bij ‘Timestamp field’ de optie ‘@timestamp’.
5. Klik op ‘Save data view to Kibana’.

3. Sign Ins
    1. Klik op ‘Create data view’
    2. Kies als naam ‘Sign Ins’
    3. Typ bij ‘Index pattern’: ‘sign_ins_stream’;
    4. Selecteer bij ‘Timestamp field’ de optie ‘@timestamp’.
    5. Klik op ‘Save data view to Kibana’.
4. Audit Logs O365
    1. Klik op ‘Create data view’
    2. Kies als naam ‘Audit Logs O365’
    3. Typ bij ‘Index pattern’: ‘audit_logs_stream’;
    4. Selecteer bij ‘Timestamp field’ de optie ‘@timestamp’.
    5. Klik op ‘Save data view to Kibana’.

Nu moet er een ‘search’ aangemaakt worden. Dit kan u als volgt doen:

Let op: zorg ervoor dat de namen die hier beschreven staan exact (hoofdletter, kleine letter) worden overgenomen, tenzij anders vermeld. Anders werkt de integratie niet.

1. Open Kibana
2. Zoek in de search bar bovenaan ‘Discover’
3. Links bovenaan staat een lichtblauwe knop. Klik hierop en selecteer ‘Audit Logs O365’.
4. Klik rechtsbovenaan op ‘Save’ en kies als titel ‘Audit Logs O365’.
5. Klik vervolgens op ‘Save’.

Nu kunnen we het dashboard toevoegen. Dit kan u als volgt doen:

1. Open Kibana.
2. Zoek in de search bar bovenaan ‘Saved Objects’.
3. Klik op ‘Import’.
4. Open het bestand ‘o365Dashboard.ndjson’ bij ‘Select a file to import’ (of sleep het bestand naar dit vak.).
5. Selecteer ‘Request action on conflict’.
6. Klik op ‘Import’.
7. Kies ‘Overwrite’.
8. Klik op ‘Done’.
9. U kan het dashboard terugvinden als ‘[Logs o365] Audit Dashboard’.

1.2. Indien de EntraID tenant-gegevens veranderen

U zal de gegevens voor de integratie moeten veranderen. Dit kan bijvoorbeeld voorvallen wanneer het ‘client secret’ vervalt. Wanneer deze vervalt, hangt af van de eerder gemaakte instellingen. Indien het ‘client secret’ vervalt, of u de waarde van het ‘client

secret' niet meer weet, dan moet u een nieuw 'client secret' aanmaken. De stappen om de gegevens terug te vinden kan u vinden onder '1.1.2. EntraID: vereiste gegevens terugvinden'.

1.2.1. Microsoft Office 365: Wanneer de gegevens veranderen II: Scripts

1. Open een terminal van de Security Onion.
2. Navigeer vervolgens naar de PythonElasticSearchScripts directory. Voer hiervoor volgend commando uit: cd /home/admin/PythonElasticSearchScripts
3. Open config.json. Voer hiervoor volgend commando uit: sudo nano config.json
4. Vul de volgende gegevens in tussen de aanhalingstekens. Volg '1.1.2. EntraID: vereiste gegevens terugvinden' om de juiste waarden te krijgen.
    - tenant_secret: vul hier uw 'client secret' in.
    - client_id: vul hier uw 'application ID' in.
    - tenant_id: vul hier uw 'tenant ID' in.
    - security-onion_username: voer hier het email dat u instelde bij de installatie van uw Security Onion in.
    - security-onion_password: voer hier het wachtwoord dat u instelde bij de installatie van uw Security Onion in.
5. Bewaar de instellingen door 'ctrl' en 'x' tegelijkertijd in te drukken. Druk vervolgens op Y om 'yes' te selecteren. Druk vervolgens op 'enter' om de config te bewaren.

1.2.2. Microsoft Office 365: Wanneer de gegevens veranderen II: Kibana

1. Log in op het Security Onion dashboard.
2. Klik op 'Kibana' (sidebar: onder 'tools').
3. Open de sidebar.
4. Onder management: klik op 'integrations'.
5. Bij 'Search for integrations' (niet de searchbar bovenaan): zoek en open 'Microsoft 365'.
6. Klik op 'Integration policies'.
7. Onder 'Actions': klik op de 3 punten, kies 'Edit integration'.
8. Vul hier de volgende waarden in:
    - 'Base URL of Office Management API': dit veranderd u enkel indien u een custom URL heeft. Anders laat u de default-waarde ('https://manage.office.com')
    - 'Interval': deze waarde bepaalt het interval in de tijd waarmee de logs worden opgehaald. De standaard-waarde is '3m' (3 minuten).
    - 'Directory (tenant) ID': deze waarde is verplicht.

- ‘Application (client) ID’: deze waarde is verplicht.
- ‘Client Secret’: deze waarde is verplicht.

U kan de waarden terugvinden zoals beschreven bij ‘1.1.2. EntraID: vereiste gegevens terugvinden’.

Let op:

- Indien andere waarden veranderd worden, wordt de werking van de integratie niet gegarandeerd.
- Indien deze waarden foutief worden ingevoerd, zal de integratie niet werken. U kan indien nodig deze waarden op een later tijdstip altijd veranderen. Dit wordt later behandeld.

9. Indien alles correct is ingevuld: klik op ‘Save integration’.

2. Gebruik van de integratie

Het dashboard zal beschikbaar zijn via het central dashboard van het project en via Kibana. U kan het Kibana dashboard bereiken via het Security Onion dashboard. In Kibana zelf kan u indien nodig zoeken naar het ‘[Logs o365] Audit Dashboard’ .

Het dashboard op Kibana bestaat uit 3 secties. Deze 3 secties worden elks gevormd door panelen. Op elk paneel kan u data terugvinden, georganiseerd in een grafiek, tabel, donut, etc.. In dit deel kan u van elk paneel terugvinden welke data er voorgesteld wordt.

U kan de tijdsschaal bovenaan aanpassen. Standaard staat deze op ‘Last 24 hours’. We adviseren om dit zo te houden, maar het is aangewezen om aan het begin van de werkweek deze even aan te passen tot 72 uur om verdachte activiteiten tijdens het weekend op te sporen, bijvoorbeeld één of meerdere logins. De panelen zullen enkel data binnen het geselecteerde tijdsbestek weergeven.

Indien de data in een table wordt gepresenteerd, kan u deze ook sorteren. Dit doet u door op de titel van de kolom te klikken en ‘Sort ascending’ of ‘Sort descending’. U kan ook kolommen op deze manier verbergen.

2.1. Sectie 1: generieke info

2.1.1. Audit Event Count

Dit geeft het totaal aantal audit logs weer.

2.1.2. Audit Event Type

Dit geeft de verhouding tussen events en alerts weer.

2.1.3. Events Histogram

Dit geeft het aantal events per service over de tijd weer.

2.1.4. Audit Geolocation

Dit geeft de geolocatie van de audits weer.

2.1.5. Data Loss Prevention Alerts

Dit geeft alerts weer van data die dreigt gelekt te worden weer. Indien er 'No data' staat, wil dit zeggen dat er geen data dreigt te lekken (volgens Office 365).

2.2. Sectie 2: Users

2.2.1. User Logins by Time

Dit geeft het aantal logins per gebruiker over de tijd weer. De gebruikers met de meeste logins worden weergegeven. Deze statistiek kan een indicator zijn van ongeauthoriseerde toegang tot uw Office 365, bijvoorbeeld wanneer er 's nacht's logins plaatsvinden of tijdens het weekend.

2.2.2. Top Failure Reasons and User

Dit geeft de meest voorkomende redenen van falen voor authenticatie bij de gebruikers met de meeste gefaalde pogingen weer.

2.2.3. Amount of Successful Logins

Dit geeft het aantal succesvolle logins weer.

2.2.4. Login Geolocation

Deze kaart geeft de geolocatie van de logins weer. Wanneer er een login gebeurd vanuit het buitenland, dan kan dit verdacht zijn.

2.2.5. Last Login Attempts

Dit geeft de laatste succesvolle en gefaalde loginpogingen weer, samen met de geolocatie en het IP adres.

2.2.6. Top Users by Authentication Outcome

Dit geeft de top gebruikers weer per uitkomst van de authenticatie. (De meeste succesvolle loginpogingen, en de meeste gefaalde loginpogingen.).

2.2.7. Events by Time

Dit geeft het aantal events over de tijd weer per gebruiker. Deze statistiek kan een indicator zijn van ongeauthoriseerde toegang tot uw Office 365, bijvoorbeeld wanneer er 's nacht's events plaatsvinden of tijdens het weekend.

2.2.8. User Actions

Dit geeft de meest recente acties weer met de relevante gebruikersnaam. Deze acties zijn inclusief succesvolle en gefaalde loginpogingen, maar kunnen ook andere belangrijke acties bevatten, zoals: het toevoegen van een gebruiker aan een rol of groep, het toevoegen van een eigenaar aan een groep, het toevoegen van een apparaat, e.d..

2.2.9. User Count

Dit geeft het aantal gebruikers in uw EntraID tenant weer. Dit getal is exclusief verwijderde gebruikers.

2.3. Sectie 3: Identity Secure Score & Events

In deze sectie kan u de secure score, de events en de volledige logs terugvinden.

2.3.1. Identity Secure Score

De identity secure score is een schaal die aangeeft hoe veilig uw EntraID is. Indien de secure score onder de 60% ligt, dan is uw EntraID zeer onveilig, en dan moet dit meteen worden opgelost. Indien de secure score tussen 60% en 80% ligt, dan is de beveiliging 'ondermaats', en moet hier aandacht aan besteed worden. Indien de secure score boven 80% ligt, dan wordt uw EntraID over het algemeen als 'veilig' beschouwd, en moet u niet onmiddelijk iets aanpassen. U kan onder dit paneel een ander paneel met een url vinden. Als u op deze url klikt, dan wordt u omgeleid naar de EntraID pagina waar u de secure score kan terugvinden. U moet hiervoor mogelijks inloggen. Op deze pagina kan u de redenen voor de secure score terugvinden. De secure score wordt zowel op het Kibana dashboard als in EntraID slechts eenmaal per 24 uur geüpdated.

2.3.2. Events & Alerts

Dit geeft de events en alerts met uitgebreidere informatie weer. U kan hier de event- of alertcategorie, de uitkomst van het event of alert, vanwaar het event of de alert komt, en nog meer, terugvinden.

2.3.3. Audit Logs Table

Dit geeft de audit logs op een leesbaardere wijze weer. U vindt hier de activiteiten, de tijd, de gebruiker, de service die de activiteit logde, en meer.

2.3.4. Full Logs 1

Hier kan u de volledige logs terugvinden.

2.3.5. Full Logs 2

Hier kan u de logs terugvinden, zoals u deze zou vinden op EntraID. Full Logs 2 is leesbaarder dan Full Logs 1, maar bevat minder informatie.