

Identifying Inactive Accounts Via Sentinel

WARNING: The following whitepaper on Identifying Inactive Accounts via Sentinel is provided as-is with no guarantees of accuracy nor sufficiency & adequacy to fulfill the assessment objectives for 3.5.6, “Disable identifiers after a defined period of inactivity.” Users are responsible for testing and validating functionality based upon their architecture.

3.5.6, Disable identifiers after a defined period of inactivity

The purpose of this whitepaper on “Identifying Inactive Accounts via Sentinel” is to provide a how-to guide on setting up an Azure Sentinel analytic to identify inactive accounts per the approved Organizationally Defined Parameter (ODP) for 3.5.6[a].

This analytic **only** works if the entire organization depends on using Azure AD for access to Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). This analytic also presumes your organization is using Microsoft Azure Sentinel as your Security Incident & Event Management (SIEM) solution to fulfill 3.3, Audit & Accountability, requirements. This analytic will not work with other SIEMs but may point you on the path to make it work in other platforms.

The Security Requirement

Below is a composite Security Requirement table form NIST SP 800-171 and NIST SP 800-171A for 3.5.6, Disable identifiers after a defined period of inactivity.

3.5.6	SECURITY REQUIREMENT Disable identifiers after a defined period of inactivity.
	DISCUSSION Inactive identifiers pose a risk to organizational information because attackers may exploit an inactive identifier to gain undetected access to organizational devices. The owners of the inactive accounts may not notice if unauthorized access to the account has been obtained.
	ASSESSMENT OBJECTIVE Determine if:
	3.5.6[a] a period of inactivity after which an identifier is disabled is defined.
	3.5.6[b] identifiers are disabled after the defined period of inactivity.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS
	Examine SELECT FROM: Identification and authentication policy; procedures addressing identifier management; procedures addressing account management; system security plan; system design documentation; system configuration settings and associated documentation; list of system accounts; list of identifiers generated from physical access control devices; other relevant documents or records
	Interview SELECT FROM: Personnel with identifier management responsibilities; personnel with information security responsibilities; system or network administrators; system developers.
	Test SELECT FROM: Mechanisms supporting or implementing identifier management.

Dependent Organization Defined Parameters (ODP)

This Analytic depends on the Organization Seeking Certification (OSC) having the following [approved ODPs](#) established by the organization:

Identifying Inactive Accounts Via Sentinel

- 3.3.1[e] retention requirements for audit records are defined.
- 3.5.6[a] a period of inactivity after which an identifier is disabled is defined.

If there are multiple ODPs for either of these, this query may not function properly.

Building the Analytic

Building the Azure Sentinel analytic to identify inactive accounts is a three-step process:

1. Create the “exempt_inactive_accounts” Watchlist
2. Create the identify_inactive_accounts query
3. Create the Alert

These steps are detailed below.

Step 1: Create the Watchlist

The analytic uses a watchlist to exempt user accounts from generating false alerts.

For more information about Azure Sentinel watchlists, please go to [Watchlists in Microsoft Sentinel – Microsoft Sentinel | Microsoft Learn](#); and, for more detailed instructions about creating watchlists, please go to [Create new watchlists – Microsoft Sentinel | Microsoft Learn](#).

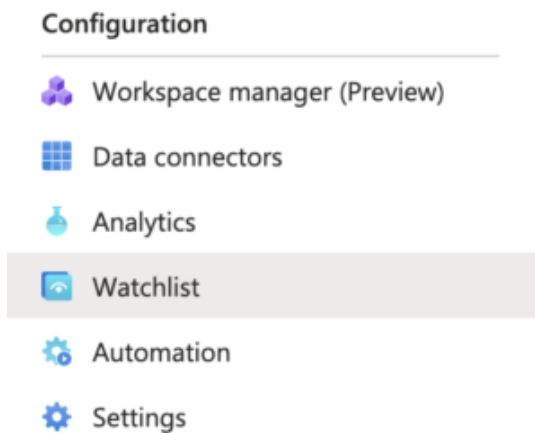
You can download our sample watchlist file for easy importing at https://peakinfosec.com/wp-content/uploads/2024/05/exempt_inactive_accounts.csv.

You can also pre-populate the information prior to import using the template or update the template as is and manage it via the watchlist’s user interface in Azure Sentinel.

The template has the following fields:

UserDisplayName	UserPrincipalName	UserId	AccountObjectId	Comments
Ellen Contoso	ellen@contoso.com	151a894c-7338-41c5-bedb1-54a2571a920b	151a894c-7338-41c5-bedb1-54a2571a920b	Add notes here

To get the Watchlist Wizard started, click on the Watchlist item under Configuration on the left sidebar.



Identifying Inactive Accounts Via Sentinel

Then to start the Watchlist Wizard, click on “New.”



Step 1a: Fill in Watchlist Wizard General Information

Microsoft Azure Government Search resources, services, and docs (G+/)

Home > Microsoft Sentinel | Watchlist >

Watchlist wizard

General Source Review + create

Name * exempt_inactive_accounts

Description exempt_inactive_accounts watchlist

Alias * exempt_inactive_accounts

Watchlist Wizard Step 1 using Azure Sentinel to create exempt_inactive_accounts

Once you start the Watchlist Wizard in Azure Sentinel, you will see the form above appear. Populate the form with the following information:

- **Name***: exempt_inactive_accounts
- Description: exempt inactive accounts watchlist
- **Alias***: exempt_inactive_accounts

Do not deviate the from items in **Bold Red**. When you are done, click “Next: Source>” at the bottom of the screen.

Step 1b: Fill in Watchlist Wizard Source Information

Microsoft Azure Government Search resources, services, and docs (G+/)

Home > Microsoft Sentinel | Watchlist >

Watchlist wizard

General Source Review + create

Source type * Local file

File type * CSV file with a header (.csv)

Number of lines before row with headings * 0

Upload file * exempt_inactive_accounts.csv

SearchKey * AccountObjectId

File preview | First 50 rows and first 5 columns

UserDisplayName	UserPrincipalName	UserId	AccountObjectId	Comments
Ellen Contoso	ellen@contoso.com	151a894c-7338-41c5-...	151a894c-7338-...	Add notes here

Identifying Inactive Accounts Via Sentinel

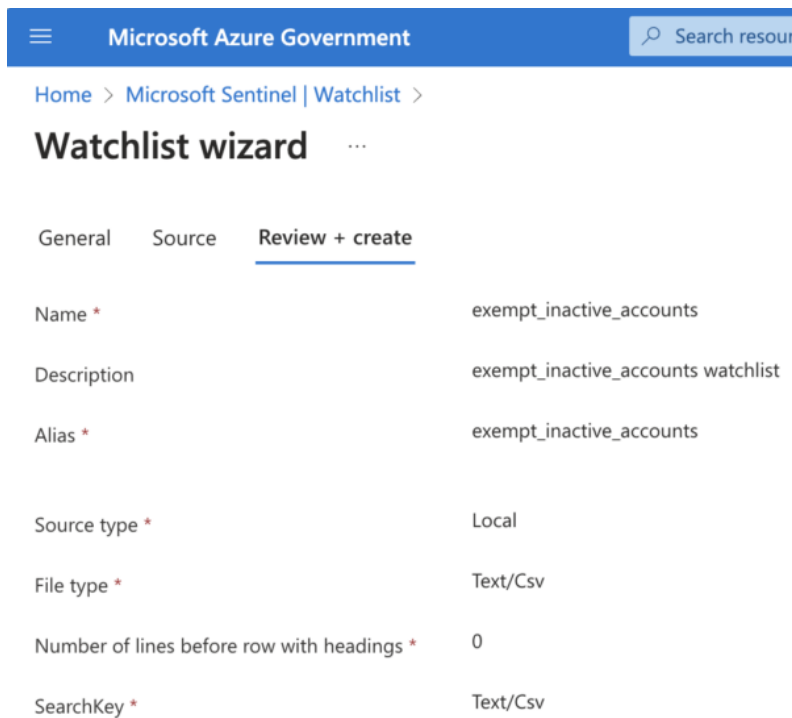
For this form, leave the first 3 settings as shown in the picture above.

Upload the exempt_inactive_accounts.csv file you created manually or sue dour template. Once you do, you should see the file preview match the content of the file.

Last thing to do is to set the SearchKey* to **AccountObjectId**.

Now you can hit “Next: Review + Create>” at the bottom of the page.

Step 1c: Watchlist Wizard Review and Create



The screenshot shows the 'Review + create' step of the Watchlist Wizard in the Microsoft Azure Government portal. The breadcrumb navigation is 'Home > Microsoft Sentinel | Watchlist >'. The title is 'Watchlist wizard'. The 'Review + create' tab is selected. The form contains the following fields:

Field	Value
Name *	exempt_inactive_accounts
Description	exempt_inactive_accounts watchlist
Alias *	exempt_inactive_accounts
Source type *	Local
File type *	Text/Csv
Number of lines before row with headings *	0
SearchKey *	Text/Csv

The next screen should look like the one above. Description may be different because that can be tailored as you see fit.

If it does, click “Create” at the bottom of the page.

After it creates the exempt_inactive_accounts watchlist, you may need to refresh your screen for it to show up in the list.

Step 2: Create the Analytic

To create the analytic, click on Logs under General on the left sidebar.

The next thing to do is to copy the query below and past it into the log editor.

```
let watchlist = (_GetWatchlist('exempt_inactive_accounts') | project UserId);
SigninLogs
//
// Change (365d) to reflect the organization's audit record retention in Sentinel
//
| where TimeGenerated > ago(365d)
```

Identifying Inactive Accounts Via Sentinel

```
| sort by TimeGenerated desc
| project TimeGenerated, UserDisplayName, UserPrincipalName, UserId, IsInteractive
| project-rename SignInTimeGenerated =TimeGenerated
| join kind=fullouter (
  IdentityInfo
  | summarize arg_max(TimeGenerated, *) by AccountObjectId
  | project AccountObjectId, IsAccountEnabled, Department, Manager
)
  on $left.UserId == $right.AccountObjectId
| summarize arg_max(SignInTimeGenerated, *) by UserId
| project
  SignInTimeGenerated,
  UserDisplayName,
  UserPrincipalName,
  Department,
  Manager,
  IsAccountEnabled,
  IsInteractive,
  UserId,
  AccountObjectId
| sort by
  SignInTimeGenerated asc,
  UserDisplayName asc,
  UserPrincipalName,
  IsAccountEnabled,
  IsInteractive,
  UserId,
  AccountObjectId
| where IsAccountEnabled == true
//
// Added due to potentially inactive admin for FOCI monitoring
//
| where UserPrincipalName !contains "admin"
//
// Change "@peakinfosec" to reflect the organization's tenant/domain name
//
| where UserPrincipalName contains "@peakinfosec"
| where SignInTimeGenerated < ago(90d)
| where UserId !in~ (watchlist)
```

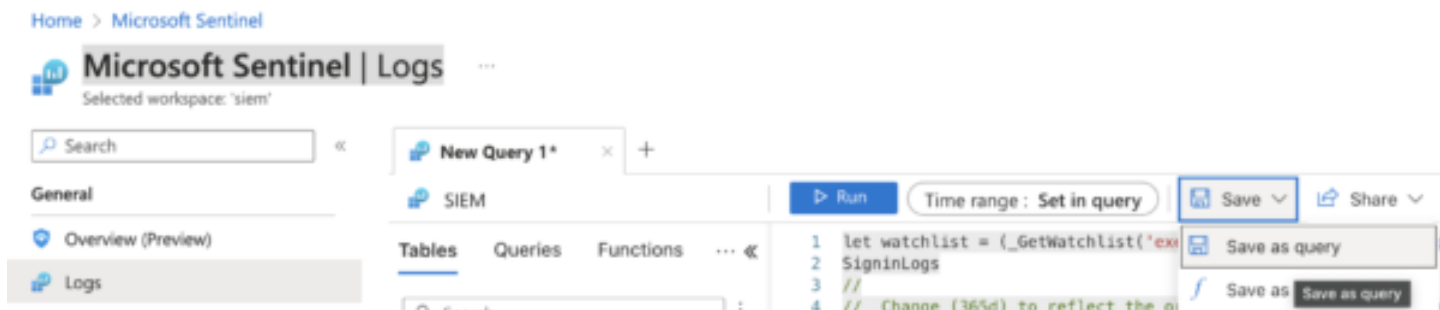
There are two places where the analytics' logic is based on Peak InfoSec and need to be changed. In the online version, these occur at lines 6 and 43 with the preceding comments section providing instructions. In this the PDF version, the lines of code are highlighted.

After updating the queries logic, you can run the query and see if it returns any results.

Presuming everything works, you next steps are to save the query, as shown below.



Identifying Inactive Accounts Via Sentinel



We suggest naming the query “Inactive_Users_Query.”

Next Steps

Next steps are to turn the query into an Azure Sentinel Alert.

More information about creating Azure Sentinel Alerts and playbooks can be found at [Create incidents from alerts in Microsoft Sentinel | Microsoft Learn](#).

Revision History

Date	Revision
28 May 2024	Initial Publication of the whitepaper. Correction can be submitted to cmmc@peakinfosec.us