Microsoft Sentinel Documentation

Created: 11/07/2023 16:02:27

Resource Group: azuresentinel

Workspace Name: gabazuresentinel

|  |
| --- |
|  |

Installed Solutions 5

(Deprecated) New Dynamics 365 User Agent 5

Akamai Security 5

Amazon Web Services 5

Analytics Health & Audit 5

Attacker Tools Threat Protection Essentials 6

Azure Active Directory 6

Azure Active Directory Identity Protection 6

Azure Activity 6

Cisco Meraki 6

Cisco Umbrella 7

Citrix ADC 7

CrowdStrike Falcon Endpoint Protection 7

Cybersecurity Maturity Model Certification (CMMC) 2.0 7

Endpoint Threat Protection Essentials 8

Log4j Vulnerability Detection 8

Maturity Model For Event Log Management M2131 8

Microsoft 365 8

Microsoft 365 Defender 9

Microsoft Defender for Cloud 9

Microsoft Defender for Endpoint 9

Microsoft Sentinel - Continuous Threat Monitoring for GitHub 9

SAP applications 9

Sentinel SOAR Essentials 10

SOC Handbook 10

Teams 10

Threat Intelligence 10

Windows Security Events 11

Workspace Usage Report 11

Zero Trust (TIC 3.0) 11

Custom Workbooks 12

Workbook Templates 13

Hunts 16

Another Hunt 16

Book Demo 16

GAB Test Hunt 16

Third Hunt 16

Repositories 17

Test 17

Gary GitHub 17

Data Connectors 18

[Deprecated] Akamai Security Events via Legacy Agent 18

[Recommended] Akamai Security Events via AMA 18

Amazon Web Services 18

Amazon Web Services S3 18

Azure Active Directory 18

Azure Active Directory Identity Protection 18

Azure Activity 18

Cisco Meraki 18

Cisco Umbrella (using Azure Function) 18

Citrix ADC (former NetScaler) 18

Crowdstrike Falcon Data Replicator (using Azure Function) 18

CrowdStrike Falcon Endpoint Protection 18

Gary's Demonstration Connector 18

GitHub Enterprise Audit Log 18

GitHub Enterprise Audit Log 18

Microsoft 365 (formerly, Office 365) 18

Microsoft 365 Defender 18

Microsoft Defender for Cloud 18

Microsoft Defender for Endpoint 18

Microsoft Defender Threat Intelligence (Preview) 18

Microsoft Sentinel for SAP 18

Security Events via Legacy Agent 18

Threat intelligence - TAXII 18

Threat Intelligence Platforms 18

Threat Intelligence Upload Indicators API (Preview) 18

Windows Security Events via AMA 18

Analytic Rules 19

Watchlists 22

Automation Rules 25

Settings 27

User Entity Behavior Analytics 27

Anomalies 27

Is workspace a central workspace? 27

Allow Microsoft Sentinel engineers to access your data? 27

Resource Groups that can run playbooks 27

Auditing and Health Monitoring 27

# Installed Solutions

## (Deprecated) New Dynamics 365 User Agent

**Version:** 1.0.1

**Type:** Standalone

**Short Description:** This standalone content is deprecated. We will NOT update this content in the future. Please install \*\*sentinel4dynamics365.sentinel4dynamics365\*\* instead

**Data Connectors:** 0**, Workbooks:** 0**, Analytic Rules:** 1**, Hunting Queries:** 0**, Azure Functions:** 0**, Playbooks:** 0**, Parsers:** 0

## Akamai Security

**Version:** 3.0.0

**Type:** Solution

**Short Description:** <None provided>

**Data Connectors:** 2**, Workbooks:** 0**, Analytic Rules:** 0**, Hunting Queries:** 0**, Azure Functions:** 0**, Playbooks:** 0**, Parsers:** 1

## Amazon Web Services

**Version:** 2.0.5

**Type:** Solution

**Short Description:** <None provided>

**Data Connectors:** 2**, Workbooks:** 2**, Analytic Rules:** 55**, Hunting Queries:** 36**, Azure Functions:** 0**, Playbooks:** 0**, Parsers:** 0

## Analytics Health & Audit

**Version:** 1.0.0

**Type:** Standalone

**Short Description:** This workbook provides visibility on the health and audit of your analytics rules. You will be able to find out whether an analytics rule is running as expected and get a list of changes made to an analytic rule.

**Data Connectors:** 0**, Workbooks:** 1**, Analytic Rules:** 0**, Hunting Queries:** 0**, Azure Functions:** 0**, Playbooks:** 0**, Parsers:** 0

## Attacker Tools Threat Protection Essentials

**Version:** 2.0.2

**Type:** Solution

**Short Description:** <None provided>

**Data Connectors:** 0**, Workbooks:** 0**, Analytic Rules:** 4**, Hunting Queries:** 2**, Azure Functions:** 0**, Playbooks:** 0**, Parsers:** 0

## Azure Active Directory

**Version:** 3.0.2

**Type:** Solution

**Short Description:** <None provided>

**Data Connectors:** 1**, Workbooks:** 2**, Analytic Rules:** 61**, Hunting Queries:** 0**, Azure Functions:** 0**, Playbooks:** 11**, Parsers:** 0

## Azure Active Directory Identity Protection

**Version:** 2.0.0

**Type:** Solution

**Short Description:** <None provided>

**Data Connectors:** 1**, Workbooks:** 0**, Analytic Rules:** 1**, Hunting Queries:** 0**, Azure Functions:** 0**, Playbooks:** 0**, Parsers:** 0

## Azure Activity

**Version:** 2.0.6

**Type:** Solution

**Short Description:** <None provided>

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 12**, Hunting Queries:** 14**, Azure Functions:** 0**, Playbooks:** 0**, Parsers:** 0

## Cisco Meraki

**Version:** 2.0.3

**Type:** Solution

**Short Description:** <None provided>

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 0**, Hunting Queries:** 0**, Azure Functions:** 0**, Playbooks:** 5**, Parsers:** 1

## Cisco Umbrella

**Version:** 2.0.4

**Type:** Solution

**Short Description:** <None provided>

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 10**, Hunting Queries:** 10**, Azure Functions:** 0**, Playbooks:** 4**, Parsers:** 1

## Citrix ADC

**Version:** 3.0.0

**Type:** Solution

**Short Description:** <None provided>

**Data Connectors:** 1**, Workbooks:** 0**, Analytic Rules:** 0**, Hunting Queries:** 0**, Azure Functions:** 0**, Playbooks:** 0**, Parsers:** 1

## CrowdStrike Falcon Endpoint Protection

**Version:** 2.0.7

**Type:** Solution

**Short Description:** <None provided>

**Data Connectors:** 2**, Workbooks:** 1**, Analytic Rules:** 2**, Hunting Queries:** 0**, Azure Functions:** 0**, Playbooks:** 3**, Parsers:** 2

## Cybersecurity Maturity Model Certification (CMMC) 2.0

**Version:** 2.0.2

**Type:** Solution

**Short Description:** <None provided>

**Data Connectors:** 0**, Workbooks:** 1**, Analytic Rules:** 2**, Hunting Queries:** 0**, Azure Functions:** 0**, Playbooks:** 3**, Parsers:** 0

## Endpoint Threat Protection Essentials

**Version:** 2.0.2

**Type:** Solution

**Short Description:** <None provided>

**Data Connectors:** 0**, Workbooks:** 0**, Analytic Rules:** 13**, Hunting Queries:** 10**, Azure Functions:** 0**, Playbooks:** 0**, Parsers:** 0

## Log4j Vulnerability Detection

**Version:** 2.0.4

**Type:** Solution

**Short Description:** <None provided>

**Data Connectors:** 0**, Workbooks:** 2**, Analytic Rules:** 4**, Hunting Queries:** 10**, Azure Functions:** 0**, Playbooks:** 2**, Parsers:** 0

## Maturity Model For Event Log Management M2131

**Version:** 2.0.1

**Type:** Solution

**Short Description:** <None provided>

**Data Connectors:** 0**, Workbooks:** 1**, Analytic Rules:** 8**, Hunting Queries:** 4**, Azure Functions:** 0**, Playbooks:** 1**, Parsers:** 0

## Microsoft 365

**Version:** 2.0.0

**Type:** Solution

**Short Description:** <None provided>

**Data Connectors:** 1**, Workbooks:** 3**, Analytic Rules:** 14**, Hunting Queries:** 20**, Azure Functions:** 0**, Playbooks:** 0**, Parsers:** 0

## Microsoft 365 Defender

**Version:** 2.0.5

**Type:** Solution

**Short Description:** <None provided>

**Data Connectors:** 1**, Workbooks:** 3**, Analytic Rules:** 9**, Hunting Queries:** 4**, Azure Functions:** 0**, Playbooks:** 0**, Parsers:** 0

## Microsoft Defender for Cloud

**Version:** 2.0.0

**Type:** Solution

**Short Description:** <None provided>

**Data Connectors:** 1**, Workbooks:** 0**, Analytic Rules:** 1**, Hunting Queries:** 0**, Azure Functions:** 0**, Playbooks:** 0**, Parsers:** 0

## Microsoft Defender for Endpoint

**Version:** 2.0.1

**Type:** Solution

**Short Description:** <None provided>

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 1**, Hunting Queries:** 2**, Azure Functions:** 0**, Playbooks:** 16**, Parsers:** 2

## Microsoft Sentinel - Continuous Threat Monitoring for GitHub

**Version:** 1.0.52

**Type:** Solution

**Short Description:** <None provided>

**Data Connectors:** 0**, Workbooks:** 0**, Analytic Rules:** 0**, Hunting Queries:** 0**, Azure Functions:** 0**, Playbooks:** 0**, Parsers:** 0

## SAP applications

**Version:** 2.0.76

**Type:** Solution

**Short Description:** <None provided>

**Data Connectors:** 1**, Workbooks:** 3**, Analytic Rules:** 62**, Hunting Queries:** 0**, Azure Functions:** 0**, Playbooks:** 3**, Parsers:** 0

## Sentinel SOAR Essentials

**Version:** 2.0.1

**Type:** Solution

**Short Description:** <None provided>

**Data Connectors:** 0**, Workbooks:** 0**, Analytic Rules:** 0**, Hunting Queries:** 0**, Azure Functions:** 0**, Playbooks:** 12**, Parsers:** 0

## SOC Handbook

**Version:** 2.0.1

**Type:** Solution

**Short Description:** <None provided>

**Data Connectors:** 0**, Workbooks:** 13**, Analytic Rules:** 0**, Hunting Queries:** 0**, Azure Functions:** 0**, Playbooks:** 0**, Parsers:** 0

## Teams

**Version:** 2.0.0

**Type:** Solution

**Short Description:** <None provided>

**Data Connectors:** 0**, Workbooks:** 1**, Analytic Rules:** 0**, Hunting Queries:** 0**, Azure Functions:** 0**, Playbooks:** 4**, Parsers:** 0

## Threat Intelligence

**Version:** 2.0.5

**Type:** Solution

**Short Description:** <None provided>

**Data Connectors:** 4**, Workbooks:** 1**, Analytic Rules:** 38**, Hunting Queries:** 5**, Azure Functions:** 0**, Playbooks:** 0**, Parsers:** 0

## Windows Security Events

**Version:** 2.0.4

**Type:** Solution

**Short Description:** <None provided>

**Data Connectors:** 2**, Workbooks:** 2**, Analytic Rules:** 20**, Hunting Queries:** 43**, Azure Functions:** 0**, Playbooks:** 0**, Parsers:** 0

## Workspace Usage Report

**Version:** 1.6.2

**Type:** Standalone

**Short Description:** Gain insights into your workspace's usage. In this workbook, you can view your workspace’s data consumption, latency, recommended tasks and Cost and Usage statistics.

**Data Connectors:** 0**, Workbooks:** 1**, Analytic Rules:** 0**, Hunting Queries:** 0**, Azure Functions:** 0**, Playbooks:** 0**, Parsers:** 0

## Zero Trust (TIC 3.0)

**Version:** 2.0.4

**Type:** Solution

**Short Description:** <None provided>

**Data Connectors:** 0**, Workbooks:** 1**, Analytic Rules:** 1**, Hunting Queries:** 0**, Azure Functions:** 0**, Playbooks:** 3**, Parsers:** 0

# Custom Workbooks

|  |  |  |
| --- | --- | --- |
| **Name** | **Content Source** | **Content Name** |
| AMA migration tracker - gabazuresentinel | Custom | -- |
| Analytics Efficiency - gabazuresentinel | Custom | -- |
| Azure Activity | Custom | -- |
| Azure Activity - gabazuresentinel | ContentHub | Azure Activity |
| Azure AD Audit logs - gabazuresentinel | ContentHub | Azure Active Directory |
| Azure DDoS Protection Workbook - gabazuresentinel | Custom | -- |
| CallPlaybook | Custom | -- |
| Codeless Connector | Custom | -- |
| Drilldown | Custom | -- |
| DrillIntoWorkbook | Custom | -- |
| GitHub - 06/11/2022 23:39 | Custom | -- |
| Incident overview - gabazuresentinel | Custom | -- |
| Log Sources & Analytic Rules Coverage - gabazuresentinel | Custom | -- |
| MergeDemo | Custom | -- |
| Security Operations Efficiency - gabazuresentinel | Custom | -- |
| Solution Data | Custom | -- |
| Threat Intelligence - gabazuresentinel | Custom | -- |
| Workspace Usage Report - gabazuresentinel | Custom | -- |
| ZeroTrust(TIC3.0) - gabazuresentinel | ContentHub | ZeroTrust(TIC3.0) |

# Workbook Templates

|  |  |
| --- | --- |
| **Name** | **Content Source** |
| Analytics Efficiency | SOC Handbook |
| Analytics Health & Audit | Standalone |
| AnomaliesVisulization | SOC Handbook |
| AnomalyData | SOC Handbook |
| Attack Surface Reduction Dashboard | SOC Handbook |
| Automation health | Standalone |
| AWS Network Activities | Amazon Web Services |
| AWS User Activities | Amazon Web Services |
| Azure Activity | Standalone |
| Azure AD Audit logs | Azure Active Directory |
| Azure AD Sign-in logs | Azure Active Directory |
| Cisco Umbrella | Standalone |
| CiscoMerakiWorkbook | Standalone |
| CrowdStrike Falcon Endpoint Protection | Standalone |
| CybersecurityMaturityModelCertification(CMMC)2.0 | Standalone |
| Event Analyzer | Windows Security Events |
| Exchange Online | Microsoft 365 |
| GitHub Security | Standalone |
| GithubWorkbook | Standalone |
| Identity & Access | Windows Security Events |
| Incident overview | Standalone |
| Incident overview | Standalone |
| Incident Tasks Workbook | Standalone |
| IntSights IOC Workbook | SOC Handbook |
| Investigation Insights | Standalone |
| Log4j Impact Assessment | Standalone |
| Log4j Post Compromise Hunting | Standalone |
| MaturityModelForEventLogManagementM2131 | Standalone |
| Microsoft 365 Defender MDOWorkbook | Microsoft 365 Defender |
| Microsoft Defender For EndPoint | Standalone |
| Microsoft Defender For Identity | Standalone |
| Microsoft Sentinel Central | SOC Handbook |
| Microsoft Sentinel Cost | SOC Handbook |
| Microsoft Teams | Teams |
| MITRE ATT&CK Workbook | SOC Handbook |
| Office 365 | Microsoft 365 |
| Security Alerts | SOC Handbook |
| Security Operations Efficiency | Standalone |
| Security Operations Efficiency | Standalone |
| Security Status | SOC Handbook |
| SharePoint & OneDrive | Microsoft 365 |
| Threat Intelligence | Standalone |
| Workspace Usage Report | Standalone |
| ZeroTrust(TIC3.0) | Standalone |

# Hunts

## Another Hunt

<p elementtiming="184">This is the description</p>

Status: Active Hypothesis: Validated Assigned To: Gary Bushey

## Book Demo

<p elementtiming="219">This is a <u elementtiming="222">demo</u> for the <strong elementtiming="223">book</strong></p>

Status: Active Hypothesis: Unknown Assigned To: Gary Bushey

## GAB Test Hunt

<p elementtiming="1087">This is the Description. Sadly it can hold HTML but I cannot display HTML in Word</p>

Status: New Hypothesis: Invalidated Assigned To: Gary Bushey

## Third Hunt

<p elementtiming="184">This is the third hunt</p>

Status: New Hypothesis: Unknown Assigned To: <unassigned>

# Repositories

## Test

**Description:**

**Source Control:** AzureDevOps

**Repository URL:** https://dev.azure.com/garybushey/60b7c155-64c2-4a6c-ad40-974d5537f78b/\_apis/git/repositories/d9bda818-9f47-4508-9136-0b7d8c905ea7

**Content Types:**

AnalyticsRule

AutomationRule

HuntingQuery

Parser

Playbook

Workbook

## Gary GitHub

**Description:** This is a Github repo that I want to connect to

**Source Control:** GitHub

**Repository URL:** https://github.com/garybushey/AzSentinelAnalyticsRules

**Content Types:**

AnalyticsRule

AutomationRule

HuntingQuery

Parser

Playbook

Workbook

# Data Connectors

## [Deprecated] Akamai Security Events via Legacy Agent

## [Recommended] Akamai Security Events via AMA

## Amazon Web Services

## Amazon Web Services S3

## Azure Active Directory

## Azure Active Directory Identity Protection

## Azure Activity

## Cisco Meraki

## Cisco Umbrella (using Azure Function)

## Citrix ADC (former NetScaler)

## Crowdstrike Falcon Data Replicator (using Azure Function)

## CrowdStrike Falcon Endpoint Protection

## Gary's Demonstration Connector

## GitHub Enterprise Audit Log

## GitHub Enterprise Audit Log

## Microsoft 365 (formerly, Office 365)

## Microsoft 365 Defender

## Microsoft Defender for Cloud

## Microsoft Defender for Endpoint

## Microsoft Defender Threat Intelligence (Preview)

## Microsoft Sentinel for SAP

## Security Events via Legacy Agent

## Threat intelligence - TAXII

## Threat Intelligence Platforms

## Threat Intelligence Upload Indicators API (Preview)

## Windows Security Events via AMA

# Analytic Rules

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Severity** | **Name** | **Rule Type** | **Status** | **Tactics** | **Techniques** |
| High | Advanced Multistage Attack Detection | Fusion | Enabled | Collection  CommandAndControl  CredentialAccess  DefenseEvasion  Discovery  Execution  Exfiltration  Impact  InitialAccess  LateralMovement  Persistence  PrivilegeEscalation |  |
| Medium | SAP - Multiple Subnets by User | Scheduled | Disabled | CredentialAccess  InitialAccess  Collection |  |
| Low | PowerShell Test | Scheduled | Enabled |  |  |
| Low | PowerShell Test1 | Scheduled | Disabled |  |  |
| Low | PowerShell Test2 | Scheduled | Disabled |  |  |
| Low | PowerShell Test3 | Scheduled | Disabled |  |  |
| Medium | Test Rule | Scheduled | Disabled | Collection  CommandAndControl |  |
| Medium | Lateral Movement via DCOM | Scheduled | Enabled | LateralMovement | T1021 |
| Low | New Dynamics 365 User Agent | Scheduled | Enabled | InitialAccess | T1078 |
| Medium | (Preview) Anomalous RDP Login Detections | MLBehaviorAnalytics | Enabled | InitialAccess |  |
| Medium | (Preview) Anomalous SSH Login Detection | MLBehaviorAnalytics | Enabled | InitialAccess |  |
| Medium | GABTest | Scheduled | Disabled |  |  |
| High | User Assigned Privileged Role | Scheduled | Enabled | Persistence | T1078 |
| Medium | Book Test | Scheduled | Enabled | Reconnaissance  Collection | T1595  T1557 |
| Medium | Creation of CRUD DynamoDB policy and then privilege escalation. | Scheduled | Enabled | PrivilegeEscalation | T1484 |
| Low | Accessed files shared by temporary external user | Scheduled | Enabled | InitialAccess |  |

# Watchlists

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Alias** | **Source** | **Created Time** | **Last Updated** |
| booktest | testingforbook | Network Addresses.csv | 10/24/2023 3:33:48 PM | 10/24/2023 3:33:48 PM |
| Campaign | Log4j | Log4j.csv | 12/22/2022 9:29:06 AM | 2/6/2023 9:28:13 AM |
| gabtest | GaryTest | Remote file | 10/24/2023 3:27:36 PM | 10/24/2023 3:27:36 PM |
| High Value Assets Watchlist | networkdata3 | Remote file | 10/24/2023 3:29:43 PM | 10/24/2023 3:29:43 PM |
| NetworkData | networkdata | Network Addresses.csv | 11/4/2023 12:54:14 PM | 11/4/2023 12:54:14 PM |
| Rules Tags | RuleTags | Local file | 10/20/2022 8:31:06 AM | 10/20/2022 8:31:06 AM |
| RuleTasks | RuleTasks | RuleTasks.csv | 12/11/2022 2:41:48 PM | 12/11/2022 2:41:48 PM |
| SAP - Critical Authorizations | SAP - Critical Authorizations | SAP - Critical Authorizations.csv | 11/12/2022 10:37:17 AM | 10/24/2023 1:04:30 PM |
| SAP - Excluded Networks | SAP - Excluded Networks | SAP - Excluded Networks.csv | 11/12/2022 10:37:17 AM | 10/24/2023 1:04:30 PM |
| SAP - Excluded Users | SAP - Excluded Users | SAP - Excluded Users.csv | 11/12/2022 10:37:17 AM | 10/24/2023 1:04:30 PM |
| SAP - FTP Servers | SAP - FTP Servers | SAP - FTP Servers.csv | 11/12/2022 10:37:17 AM | 10/24/2023 1:04:30 PM |
| SAP - Networks | SAP - Networks | SAP - Networks.csv | 11/12/2022 10:37:17 AM | 10/24/2023 1:04:29 PM |
| SAP - Obsolete Function Modules | SAP - Obsolete Function Modules | SAP - Obsolete Function Modules.csv | 11/12/2022 10:37:17 AM | 10/24/2023 1:04:27 PM |
| SAP - Obsolete Programs | SAP - Obsolete Programs | SAP - Obsolete Programs.csv | 11/12/2022 10:37:17 AM | 10/24/2023 1:04:30 PM |
| SAP - Privileged Users | SAP - Privileged Users | SAP - Privileged Users.csv | 11/12/2022 10:37:17 AM | 10/24/2023 1:04:30 PM |
| SAP - Sensitive ABAP Programs | SAP - Sensitive ABAP Programs | SAP - Sensitive ABAP Programs.csv | 11/12/2022 10:37:17 AM | 10/24/2023 1:04:29 PM |
| SAP - Sensitive Function Modules | SAP - Sensitive Function Modules | SAP - Sensitive Function Modules.csv | 11/12/2022 10:37:17 AM | 10/24/2023 1:04:26 PM |
| SAP - Sensitive Profiles | SAP - Sensitive Profiles | SAP - Sensitive Profiles.csv | 11/12/2022 10:37:17 AM | 10/24/2023 1:04:29 PM |
| SAP - Sensitive Roles | SAP - Sensitive Roles | SAP - Sensitive Roles.csv | 11/12/2022 10:37:17 AM | 10/24/2023 1:04:27 PM |
| SAP - Sensitive Tables | SAP - Sensitive Tables | SAP - Sensitive Tables.csv | 11/12/2022 10:37:17 AM | 10/24/2023 1:04:29 PM |
| SAP - Sensitive Transactions | SAP - Sensitive Transactions | SAP - Sensitive Transactions.csv | 11/12/2022 10:37:17 AM | 10/24/2023 1:04:31 PM |
| SAP - Systems | SAP - Systems | SAP - Systems.csv | 11/12/2022 10:37:17 AM | 10/24/2023 1:04:30 PM |
| SAP - Transactions for ABAP Generations | SAP - Transactions for ABAP Generations | SAP - Transactions for ABAP Generations.csv | 11/12/2022 10:37:17 AM | 10/24/2023 1:04:26 PM |
| SAP\_Dynamic\_Audit\_Log\_Monitor\_Configuration | SAP\_Dynamic\_Audit\_Log\_Monitor\_Configuration | SAP\_Dynamic\_Audit\_Log\_Monitor\_Configuration.csv | 11/12/2022 10:37:17 AM | 10/24/2023 1:04:30 PM |
| SAP\_User\_Config | SAP\_User\_Config | SAP\_User\_Config.csv | 11/12/2022 10:37:17 AM | 10/24/2023 1:04:30 PM |
| SAPAlertRulesMetadata | SAPAlertRulesMetadata | SAPAlertRulesMetadata.csv | 10/24/2023 1:04:27 PM | 10/24/2023 1:04:27 PM |
| SAPSolutionConfig | SAPSolutionConfig | SAPSolutionConfig.csv | 10/24/2023 1:04:30 PM | 10/24/2023 1:04:30 PM |
| SAPSystemParameters | SAPSystemParameters | SAPSystemParameters.csv | 10/24/2023 1:04:26 PM | 10/24/2023 1:04:26 PM |
| SolutionData | SolutionData | Remote file | 10/9/2023 2:51:42 PM | 10/9/2023 2:51:42 PM |
| TaskTemplates | TaskTemplates | TaskTemplates.csv | 12/11/2022 2:24:51 PM | 12/11/2022 2:24:51 PM |

# Automation Rules

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Order** | **Display Name** | **Trigger** | **Analytic Rule Name** | **Actions** | **Expiration Date** |
| 1 | Task Test | Incidents Created | All | Task Test | Indefinite |
| 1 | test | Incidents Created | All | test | Indefinite |
| 1 | Add task | Incidents Updated | All | Add task | Indefinite |
| 1 | GaryTest | Incidents Created | All | GaryTest | Indefinite |
| 1 | GaryTest | Incidents Created | All | GaryTest | Indefinite |
| 1 | BookTest | Incidents Created | All | BookTest | Indefinite |
| 1 | Alert Rule | Alerts Created | PowerShell Test  SAP - Multiple Subnets by User  PowerShell Test2 | Alert Rule | Indefinite |
| 1 | Book Test | Incidents Created | All | Book Test | Indefinite |
| 2 | AddTasksToIncident | Incidents Created | All | AddTasksToIncident | Indefinite |
| 2 | Run Playbook to reset AAD password | Incidents Created | All | Run Playbook to reset AAD password | Indefinite |
| 2 | Use Case Automation Rule | Incidents Updated | All | Use Case Automation Rule | Indefinite |
| 3 | Open\_AI | Incidents Created | All | Open\_AI | Indefinite |

# Settings

## User Entity Behavior Analytics

Enabled: True

Directory services:

Azure Active Directory

Directory sources:

Audit Logs

Azure Activity

Security Events

Sign In Logs

## Anomalies

Enabled: True

## Is workspace a central workspace?

True

## Allow Microsoft Sentinel engineers to access your data?

Enabled: False

## Resource Groups that can run playbooks

AzureSentinel

## Auditing and Health Monitoring

Analytics

Automation

Data Collection - Connectors