Microsoft Sentinel Solutions Documentation

Created: 03/15/2023 16:49:39

42Crunch Microsoft Sentinel Connector 11

Abnormal Security Events 14

AbuseIPDB 15

AgileSec Analytics Connector 16

AI Analyst Darktrace 17

AIShield - AI Security Monitoring for Microsoft Sentinel 18

Akamai Security 20

Alibaba Cloud (Preview) 21

Amazon Web Services 22

Apache Http Server 37

Apache Tomcat 40

ARGOS Cloud Security for Microsoft Sentinel 43

Arista NDR for Microsoft Sentinel 45

Armorblox for Microsoft Sentinel 47

Aruba ClearPass 49

Atlassian Confluence Audit 50

Atlassian Jira Audit 51

Attacker Tools Threat Protection Essentials 55

Australian Cyber Security Centre 57

Auth0 58

Automated Logic WebCTRL 59

AWS Athena 60

AWS IAM 61

Azure Active Directory Identity Protection 63

Azure Active Directory solution for Sentinel 65

Azure Activity solution for Sentinel 81

Azure Batch Account solution for Sentinel 86

Azure Cognitive Search solution for Sentinel (Preview) 87

Azure Data Lake Storage Gen1 solution for Sentinel (Preview) 88

Azure DDoS Protection solution for Sentinel 89

Azure DevOps Auditing 91

Azure Event Hubs solution for Sentinel (Preview) 98

Azure Firewall Solution for Sentinel (Preview) 99

Azure Information Protection solution for Sentinel 103

Azure Key Vault solution for Sentinel 105

Azure Kubernetes Service (AKS) solution for Sentinel 107

Azure Logic Apps solution for Sentinel 109

Azure Network Security Groups solution for Sentinel 110

Azure Security Benchmark 112

Azure Sentinel for WatchGuard Firebox 114

Azure Service Bus solution for Sentinel (Preview) 115

Azure SQL Database solution for sentinel (Preview) 116

Azure Storage solution for Sentinel 120

Azure Stream Analytics solution for Sentinel (Preview) 121

Azure Web Application Firewall solution for Sentinel 122

Barracuda WAF Sentinel Solution 125

BETTER Mobile Threat Defense (MTD) 126

Bitglass Solution 128

Blackberry CylancePROTECT 131

Box Solution 132

Broadcom SymantecDLP 135

Check Point for Microsoft Sentinel solutions 136

CheckPhish by Bolster 137

Cisco ACI Solution 138

Cisco ASA Solution 139

Cisco Duo Security 141

Cisco Firepower eStreamer 144

Cisco ISE 146

Cisco Meraki Solution 150

Cisco Secure Endpoint Solution 152

Cisco SEG Solution 156

Cisco Stealthwatch Solution 160

Cisco UCS 161

Cisco Umbrella 162

Cisco WSA 166

Citrix ADC 169

Citrix Analytics Application for Microsoft Sentinel 170

Citrix WAF Solution for Sentinel 172

Claroty 174

Cloud Identity Threat Protection Essentials 177

Cloud Service Threat Protection Essentials 179

Cloudflare (Deprecated) 180

Cloudflare for Microsoft Sentinel 183

Cognni for Microsoft Sentinel 186

Cohesity Security Integration for Microsoft Sentinel 189

Common Event Format solution for Sentinel 191

Continuous Diagnostics& Mitigation 192

Contrast Protect for Microsoft Sentinel 193

Corelight for Microsoft Sentinel 195

CrowdStrike Falcon Endpoint Protection 198

CyberArk Enterprise Password Vault (EPV)/Sentinel 201

CyberArk EPM/Sentinel Integration 203

Cyberpion Security Logs 204

Cybersecurity Maturity Model Certification (CMMC) 2.0 206

Darktrace for Microsoft Sentinel 208

Delinea Secret Server for Microsoft Sentinel 210

Dev 0270 Detection and Hunting 211

DEV-0537 Detection and Hunting (Preview) 213

Digital Guardian Data Loss Prevention Solution 214

Digital Shadows SearchLight for Microsoft Sentinel 217

DomainTools Iris Investigate for Microsoft Sentinel 219

Dynamics 365 - Connector Only 221

Dynatrace Software Intelligence Platform with Microsoft Sentinel 222

Eaton Foreseer (Preview) 225

Egress Defend Connector for Microsoft Sentinel 226

Elastic Agent Solution (Preview) 227

Endpoint Threat Protection Essentials 228

ESET Inspect integration for Microsoft Sentinel 233

ESET PROTECT integration for Azure Sentinel 234

Exabeam Advanced Analytics 235

ExtraHop Reveal(x) for Microsoft Sentinel 236

F5 Advanced WAF Integration via Syslog/CEF for Microsoft Sentinel 237

F5 Advanced WAF Integration via Telemetry Streaming for Microsoft Sentinel 238

FalconForce FalconFriday Analytics for Microsoft Sentinel 240

Farsight DNSDB for Microsoft Sentinel 248

FireEye Network Security 249

Flare for Microsoft Sentinel 250

Forcepoint CASB 251

Forcepoint CSG 252

Forcepoint DLP 253

Forcepoint NGFW 254

Forescout 255

Forescout eyeExtend for Microsoft Sentinel 256

Fortinet FortiGate 257

Fortinet FortiWeb Cloud 259

Gitlab 260

Google ApigeeX 263

Google Cloud Platform Cloud Monitoring Solution 264

Google Cloud Platform DNS Solution 265

Google Cloud Platform IAM 269

Google Workspace Reports 272

Holm Security for Azure Sentinel 276

HYAS Insight 277

HYAS Insight for Microsoft Sentinel 278

iboss Connector for Microsoft Sentinel 282

Illumio Core 284

Illusive Attack Surface Analysis and Incident Logs for Microsoft Sentinel 285

Imperva WAF Cloud Solution 287

Infoblox Cloud for Microsoft Sentinel 290

Infoblox NIOS 292

InsightVM CloudAPI 296

ISC Bind 298

Ivanti Unified Endpoint Management 299

Jamf Protect for Microsoft Sentinel 300

Jboss 302

Joshua Cyberisk Vision 303

Juniper IDP Solution 304

Juniper SRX 305

Kaspersky Security Center 306

KQL Training 307

Lastpass Enterprise Activity Monitoring 308

Legacy IOC based Threat Protection 311

Log4j Vulnerability Detection 331

Lookout Cloud Security Platform for Microsoft Sentinel 336

Lookout Mobile Threat Defense for Microsoft Sentinel 337

MarkLogic Audit 339

Maturity Model For Event Log Management M2131 340

McAfee ePolicy Orchestrator Solution 343

McAfee Network Security Platform Solution 347

Microsoft 365 Defender solution for Sentinel 348

Microsoft 365 solution for Sentinel 352

Microsoft Defender for Cloud Apps solution for Sentinel 358

Microsoft Defender for Cloud solution for Sentinel 360

Microsoft Defender for Endpoint 362

Microsoft Defender for Identity solution for Sentinel 365

Microsoft Defender for IoT solution for Microsoft Sentinel 367

Microsoft Defender for Office 365 372

Microsoft PowerBI solution for Sentinel 374

Microsoft Project solution for Sentinel 375

Microsoft Purview Information Protection 376

Microsoft Purview Insider Risk Management 377

Microsoft Purview solution for Sentinel 381

Microsoft Sentinel - Continuous Threat Monitoring for GitHub (Preview) 383

Microsoft Sentinel Deception (Honey Tokens) Solution 388

Microsoft Sentinel for Teams (Preview) 389

Microsoft Sentinel Solution for Dynamics 365 CE Apps (Preview) 391

Microsoft Sentinel solution for SAP® applications 396

Microsoft Sentinel Training Lab Solution (Preview) 416

Microsoft Sysmon For Linux Solution 417

Microsoft Windows SQL Server Database Audit 418

Minemeld 420

MongoDB Audit 421

Morphisec UTPP 422

Mulesoft 423

NC Protect Data Connector for Microsoft Sentinel 424

Netskope Data Connector for Microsoft Sentinel 425

Network Threat Protection Essentials 426

Netwrix Auditor (Preview) 428

Neustar IP GeoPoint 429

Nginx 430

NIST SP 800-53 433

Noname Security for Microsoft Sentinel 435

Nozomi Networks 436

NXLog AIX Audit for Azure Sentinel 437

NXLog BSM macOS for Microsoft Sentinel 438

NXLog DNS Logs for Azure Sentinel 439

NXLog LinuxAudit for Microsoft Sentinel 440

Okta Single Sign-On Solution 441

One Identity Safeguard On Demand 444

OneLogin IAM 445

OpenCTI 446

OpenVPN 448

Oracle Cloud Infrastructure 449

Oracle Database Audit Solution 452

Oracle WebLogic Server 455

Orca Security Alerts 458

OSSEC 459

Palo Alto Networks Cortex Data Lake Solution 460

Palo Alto PAN-OS Solution (Preview) 463

Palo Alto Prisma Cloud CSPM Solution 468

PCI DSS Compliance 472

Perimeter 81 473

PingFederate 474

PostgreSQL 478

Proofpoint On demand (POD) Email Security 479

Proofpoint TAP Solution 482

Pulse Connect Secure 485

Qualys VM Knowledgebase 487

Qualys VM Solution 488

Recorded Future Intelligence for Microsoft Sentinel 491

Red Canary Connector for Microsoft Sentinel 494

ReversingLabs Content Pack 495

RiskIQ Illuminate Solution 496

RSA SecurID Solution (Preview) 502

Rubrik Integration with Sentinel for Ransomware Protection 503

SailPoint for Microsoft Sentinel 505

Salesforce Service Cloud 507

Security Threat Essentials 509

SecurityBridge App for Microsoft Sentinel 512

SecurityScorecard Ratings for Microsoft Sentinel 514

Semperis Directory Services Protector 516

Senserva Offer for Microsoft Sentinel 518

Sentinel SOAR Essentials 524

SentinelOne 526

ServiceNow 530

Shadowbyte's Threat Intelligence for Sentinel 531

SIGNL4 – Mobile Alerting for Microsoft Sentinel 532

Slack Audit Solution 533

SlashNext URL Threat Analysis and IR for Microsoft Sentinel 536

Snowflake 537

SOC Handbook solution for Microsoft Sentinel 540

SOC Process Framework(Preview) 544

SonicWall Network Security for Microsoft Sentinel 547

Sonrai Security for Microsoft Sentinel 548

Sophos Cloud Optix 551

Sophos Endpoint Protection Solution 552

Sophos XG Firewall Solution 553

Squadra Technologies secRMM 555

SquidProxy 556

Symantec Endpoint Protection Solution 557

Symantec Integrated Cyber Defense 559

Symantec ProxySG Solution 560

Symantec VIP 562

Synack Integration for Microsoft Sentinel 564

Syslog solution for Sentinel 565

Talon Connector for Microsoft Sentinel 568

Tanium Microsoft Sentinel Connector 569

Tenable App for Microsoft Sentinel 571

TheHive Solution 573

Theom for Microsoft Sentinel Solution - Data Cloud and Data Lakehouse Attack Detection 575

Threat Analysis & Response 580

Threat Intelligence 581

ThreatX WAF 590

Trend Micro Apex One Solution 591

Trend Micro Cloud App Security 594

Trend Micro Deep Security for Microsoft Sentinel 597

Trend Micro TippingPoint for Microsoft Sentinel 599

Trend Vision One for Microsoft Sentinel 600

Ubiquiti UniFi 602

UEBA Essentials 605

URLhaus 607

vArmour Application Controller for Microsoft Sentinel 609

Vectra AI Stream for Microsoft Sentinel 611

Vectra Detect for Microsoft Sentinel 613

VirusTotal 615

VMware Carbon Black Cloud 617

VMware ESXi 621

VMware vCenter 624

Watchlists Utilities Solution 626

Windows Firewall 629

Windows Forwarded Events 631

Windows Security Events 633

Windows Server DNS 644

WireX Network Forensics Platform for Microsoft Sentinel 648

WithSecure™ Elements via Connector for Microsoft Sentinel 649

Workplace from Facebook 650

Zero Networks Segment for Microsoft Sentinel 651

Zero Trust (TIC 3.0) Solution 654

Zimperium MTD for Sentinel 656

ZINC Open Source Threat Protection 657

Zoom Reports 659

Zscaler Internet Access for Microsoft Sentinel 660

Zscaler Private Access 663

# 42Crunch Microsoft Sentinel Connector

Actively Monitor and Defend Your APIs with the 42Crunch micro-API Firewall and Microsoft Sentinel

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 11**, Hunting Queries:** 0**, Watchlists:** 0**, Playbooks:** 0, Parsers: 0

## Data Connectors

### API Protection

Connects the 42Crunch API protection to Azure Log Analytics via the REST API interface

## Workbooks

### 42Crunch API Protection Workbook

Monitor and protect APIs using the 42Crunch API microfirewall

**Required Data Types**

## Analytic Rules

### API - Account Takeover

42Crunch API protection against account takeover

**Required Data Connectors**

42CrunchAPIProtection

### API - Anomaly Detection

42Crunch API protection anomaly detection

**Required Data Connectors**

42CrunchAPIProtection

### API - API Scraping

42Crunch API protection against API scraping

**Required Data Connectors**

42CrunchAPIProtection

### API - BOLA

42Crunch API protection against BOLA

**Required Data Connectors**

42CrunchAPIProtection

### API - Rate limiting

42Crunch API protection against first-time access

**Required Data Connectors**

42CrunchAPIProtection

### API - Invalid host access

42Crunch API protection against invalid host access

**Required Data Connectors**

42CrunchAPIProtection

### API - JWT validation

42Crunch API protection against JWT validation

**Required Data Connectors**

42CrunchAPIProtection

### API - Kiterunner detection

42Crunch API protection against Kiterunner enumeration

**Required Data Connectors**

42CrunchAPIProtection

### API - Password Cracking

42Crunch API protection against password cracking

**Required Data Connectors**

42CrunchAPIProtection

### API - Rate limiting

42Crunch API protection against rate limiting

**Required Data Connectors**

42CrunchAPIProtection

### API - Suspicious Login

42Crunch API protection against suspicious login

**Required Data Connectors**

42CrunchAPIProtection

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Abnormal Security Events

The Abnormal Security data connector provides the capability to ingest threat and case logs into Azure Sentinel using the Abnormal Security Rest API

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

## Data Connectors

### AbnormalSecurity (using Azure Function)

The Abnormal Security data connector provides the capability to ingest threat and case logs into Microsoft Sentinel using the [Abnormal Security Rest API.](https://app.swaggerhub.com/apis/abnormal-security/abx/)

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# AbuseIPDB

AbuseIPDB

**Data Connectors:** 0**, Workbooks:** 0**, Analytic Rules:** 0**, Hunting Queries:** 0**, Watchlists:** 0**, Playbooks:** 3, Parsers: 0

## Data Connectors

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

### AbuseIPDB Enrich Incident By IP Info

Once a new sentinal incident is created, this playbook gets triggered and performs the following actions:

1. [Gets Information](https://docs.abuseipdb.com/#check-endpoint) from AbuseIPDB by IP`s, provided in the alert custom entities.

2. Enriches the incident with the obtained info.

### AbuseIPDB Report a IPs To AbuselPDB After Checking By User In MSTeams

When a new sentinel incident is created, this playbook gets triggered and performs the following actions:

1. Sends an adaptive card to the Teams channel where the analyst can choose an action to be taken.

### AbuseIPDB Blacklist Ip To Threat Intelligence

By every day reccurence, this playbook gets triggered and performs the following actions:

1. Gets [list](https://docs.abuseipdb.com/#blacklist-endpoint) of the most reported IP addresses form the Blacklist Endpoint.

## Parsers

# AgileSec Analytics Connector

AgileSec Analytics automates the discovery and analysis of machines identities and cryptographic mechanisms deployed across a digital ecosystem. The connector allows exporting crypto findings to Azure Sentinel for further analysis.

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

## Data Connectors

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# AI Analyst Darktrace

The Darktrace connector and workbook allows users to connect Darktrace's real-time alerting with Microsoft Sentinel and enables the creation of custom Dashboards and alerts to improve investigations.

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

## Data Connectors

### AI Analyst Darktrace

The Darktrace connector lets users connect Darktrace Model Breaches in real-time with Azure Sentinel, allowing creation of custom Dashboards, Workbooks, Notebooks and Custom Alerts to improve investigation. Azure Sentinel's enhanced visibility into Darktrace logs enables monitoring and mitigation of security threats.

## Workbooks

### AI Analyst Darktrace Model Breach Summary

A workbook containing relevant KQL queries to help you visualise the data in model breaches from the Darktrace Connector

**Required Data Types**

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# AIShield - AI Security Monitoring for Microsoft Sentinel

Secure your AI workloads against emerging AI Security threats and connect with Microsoft Sentinel to get real-time insights into your AI model security posture

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

## Data Connectors

### AIShield

[AIShield](https://www.boschaishield.com/) connector allows users to connect with AIShield custom defense mechanism logs with Microsoft Sentinel, allowing the creation of dynamic Dashboards, Workbooks, Notebooks and tailored Alerts to improve investigation and thwart attacks on AI systems. It gives users more insight into their organization's AI assets security posturing and improves their AI systems security operation capabilities.

## Workbooks

## Analytic Rules

### AIShield - Image classification model extraction vulnerability detection

This alert creates an incident when Image classification model extraction vulnerability detected from the AIShield.

**Required Data Connectors**

BoschAIShield

### AIShield - Image classification model evasion vulnerability detection

This alert creates an incident when Image classification model evasion vulnerability detected from the AIShield.

**Required Data Connectors**

BoschAIShield

### AIShield - Natural language processing model extraction vulnerability detection

This alert creates an incident when Natural language processing model extraction vulnerability detected from the AIShield.

**Required Data Connectors**

BoschAIShield

### AIShield - Tabular classification model extraction vulnerability detection

This alert creates an incident when Tabular classification model extraction vulnerability detected from the AIShield.

**Required Data Connectors**

BoschAIShield

### AIShield - TimeSeries Forecasting model extraction vulnerability detection

This alert creates an incident when TimeSeries Forecasting model extraction vulnerability detected from the AIShield.

**Required Data Connectors**

BoschAIShield

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### AIShield

Category: Samples

Function Alias: AIShield

# Akamai Security

The Akamai Security Solution for Microsoft Sentinel enables ingestion of Akamai Security Solutions events using the Common Event Format (CEF) into Microsoft Sentinel for Security Monitoring.

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

## Data Connectors

### Akamai Security Events

Akamai Solution for Sentinel provides the capability to ingest [Akamai Security Events](https://www.akamai.com/us/en/products/security/) into Microsoft Sentinel. Refer to [Akamai SIEM Integration documentation](https://developer.akamai.com/tools/integrations/siem) for more information.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### AkamaiSIEMEvent

Category: Samples

Function Alias: AkamaiSIEMEvent

# Alibaba Cloud (Preview)

The Alibaba Cloud solution provides the capability to retrieve logs from cloud applications using the Cloud API and more events into Microsoft Sentinel through the REST API.

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

## Data Connectors

### AliCloud (using Azure Function)

The [AliCloud](https://www.alibabacloud.com/product/log-service) data connector provides the capability to retrieve logs from cloud applications using the Cloud API and store events into Microsoft Sentinel through the [REST API](https://aliyun-log-python-sdk.readthedocs.io/api.html). The connector provides ability to get events which helps to examine potential security risks, analyze your team's use of collaboration, diagnose configuration problems and more.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### AliCloud

Category: Samples

Function Alias: AliCloud

# Amazon Web Services

The Amazon Web Services solution for Microsoft Sentinel allows you to enable Security monitoring of AWS services by allowing ingestion of logs from the AWS CloudTrail platform, VPC Flow Logs, AWS GuardDuty and AWS CloudWatch.

**Data Connectors:** 2**, Workbooks:** 2**, Analytic Rules:** 54**, Hunting Queries:** 36**, Watchlists:** 0**, Playbooks:** 0, Parsers: 0

## Data Connectors

### Amazon Web Services

Follow these instructions to connect to AWS and stream your CloudTrail logs into Microsoft Sentinel.

### Amazon Web Services S3

This connector allows you to ingest AWS service logs, collected in AWS S3 buckets, to Microsoft Sentinel. The currently supported data types are:

\* AWS CloudTrail

\* VPC Flow Logs

\* AWS GuardDuty

## Workbooks

### AWS Network Activities

Gain insights into AWS network related resource activities, including the creation, update, and deletions of security groups, network ACLs and routes, gateways, elastic load balancers, VPCs, subnets, and network interfaces.

**Required Data Types**

AWSCloudTrail

AWS

### AWS User Activities

Gain insights into AWS user activities, including failed sign-in attempts, IP addresses, regions, user agents, and identity types, as well as potential malicious user activities with assumed roles.

**Required Data Types**

AWSCloudTrail

AWS

## Analytic Rules

### Changes to internet facing AWS RDS Database instances

Amazon Relational Database Service (RDS) is scalable relational database in the cloud.

If your organization have one or more AWS RDS Databases running, monitoring changes to especially internet facing AWS RDS (Relational Database Service)

Once alerts triggered, validate if changes observed are authorized and adhere to change control policy.

More information: https://medium.com/@GorillaStack/the-most-important-aws-cloudtrail-security-events-to-track-a5b9873f8255

and RDS API Reference Docs: https://docs.aws.amazon.com/AmazonRDS/latest/APIReference/API\_Operations.html

**Required Data Connectors**

AWS

AWSS3

### Changes to Amazon VPC settings

Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the AWS Cloud where you can launch AWS resources

in a virtual network that you define.

This identifies changes to Amazon VPC (Virtual Private Cloud) settings such as new ACL entries,routes, routetable or Gateways.

More information: https://medium.com/@GorillaStack/the-most-important-aws-cloudtrail-security-events-to-track-a5b9873f8255

and AWS VPC API Docs: https://docs.aws.amazon.com/AWSEC2/latest/APIReference/OperationList-query-vpc.html

**Required Data Connectors**

AWS

AWSS3

### Changes made to AWS CloudTrail logs

Attackers often try to hide their steps by deleting or stopping the collection of logs that could show their activity.

This alert identifies any manipulation of AWS CloudTrail, Cloudwatch/EventBridge or VPC Flow logs.

More Information: AWS CloudTrail API: https://docs.aws.amazon.com/awscloudtrail/latest/APIReference/API\_Operations.html

AWS Cloudwatch/Eventbridge API: https://docs.aws.amazon.com/eventbridge/latest/APIReference/API\_Operations.html

AWS DelteteFlowLogs API : https://docs.aws.amazon.com/AWSEC2/latest/APIReference/API\_DeleteFlowLogs.html

**Required Data Connectors**

AWS

AWSS3

### Login to AWS Management Console without MFA

Multi-Factor Authentication (MFA) helps you to prevent credential compromise. This alert identifies logins to the AWS Management Console without MFA.

You can limit this detection to trigger for adminsitrative accounts if you do not have MFA enabled on all accounts.

This is done by looking at the eventName ConsoleLogin and if the AdditionalEventData field indicates MFA was NOT used

and the ResponseElements field indicates NOT a Failure. Thereby indicating that a non-MFA login was successful.

**Required Data Connectors**

AWS

AWSS3

### Monitor AWS Credential abuse or hijacking

Looking for GetCallerIdentity Events where the UserID Type is AssumedRole

An attacker who has assumed the role of a legitimate account can call the GetCallerIdentity function to determine what account they are using.

A legitimate user using legitimate credentials would not need to call GetCallerIdentity since they should already know what account they are using.

More Information: https://duo.com/decipher/trailblazer-hunts-compromised-credentials-in-aws

AWS STS GetCallerIdentity API: https://docs.aws.amazon.com/STS/latest/APIReference/API\_GetCallerIdentity.html

**Required Data Connectors**

AWS

AWSS3

### Full Admin policy created and then attached to Roles, Users or Groups

Identity and Access Management (IAM) securely manages access to AWS services and resources.

Identifies when a policy is created with Full Administrators Access (Allow-Action:\*,Resource:\*).

This policy can be attached to role,user or group and may be used by an adversary to escalate a normal user privileges to an adminsitrative level.

AWS IAM Policy Grammar: https://docs.aws.amazon.com/IAM/latest/UserGuide/reference\_policies\_grammar.html

and AWS IAM API at https://docs.aws.amazon.com/IAM/latest/APIReference/API\_Operations.html

**Required Data Connectors**

AWS

AWSS3

### Changes to AWS Security Group ingress and egress settings

A Security Group acts as a virtual firewall of an instance to control inbound and outbound traffic.

Hence, ingress and egress settings changes to AWS Security Group should be monitored as these can expose the enviornment to new attack vectors.

More information: https://medium.com/@GorillaStack/the-most-important-aws-cloudtrail-security-events-to-track-a5b9873f8255.

**Required Data Connectors**

AWS

AWSS3

### Changes to AWS Elastic Load Balancer security groups

Elastic Load Balancer distributes incoming traffic across multiple instances in multiple availability Zones. This increases the fault tolerance of your applications.

Unwanted changes to Elastic Load Balancer specific security groups could open your environment to attack and hence needs monitoring.

More information: https://medium.com/@GorillaStack/the-most-important-aws-cloudtrail-security-events-to-track-a5b9873f8255

and https://aws.amazon.com/elasticloadbalancing/.

**Required Data Connectors**

AWS

AWSS3

### NRT Login to AWS Management Console without MFA

Multi-Factor Authentication (MFA) helps you to prevent credential compromise. This alert identifies logins to the AWS Management Console without MFA.

You can limit this detection to trigger for administrative accounts if you do not have MFA enabled on all accounts.

This is done by looking at the eventName ConsoleLogin and if the AdditionalEventData field indicates MFA was NOT used

and the ResponseElements field indicates NOT a Failure. Thereby indicating that a non-MFA login was successful.

**Required Data Connectors**

AWS

AWSS3

### AWS Guard Duty Alert

Amazon GuardDuty is a threat detection service that continuously monitors your AWS accounts and workloads for malicious activity and delivers detailed security findings for visibility and remediation. This templates create an alert for each Amazon GuardDuty finding.

**Required Data Connectors**

AWSS3

### ECR image scan findings high or critical

AWS ECR Image scan detected critical or high-severity vulnerabilities in your container image.

**Required Data Connectors**

AWS

### Suspicious command sent to EC2

An attacker with the necessary permissions could be executing code remotely on a machine and saving the output to his own S3 bucket. Verify this action with the user identity.

**Required Data Connectors**

AWS

### Successful API executed from a Tor exit node

A successful API execution was detected from an IP address categorized as a TOR exit node by Threat Intelligence.

**Required Data Connectors**

AWS

### GuardDuty detector disabled or suspended

GuardDuty Detector was disabled or suspended, possibly by an attacker trying to avoid detection of its malicious activities. Verify with the user identity that this activity is legitimate.

**Required Data Connectors**

AWS

### CloudFormation policy created then used for privilege escalation

Detected creation of new Cloudformation policy and usage of one of the attach policy events (AttachUserPolicy/AttachRolePolicy/AttachGroupPolicy). This might indicate a privilege escalation technique that attackers could use.

**Required Data Connectors**

AWS

### Creation of CRUD DynamoDB policy and then privilege escalation.

Detected creation of new CRUD DynamoDB policy and usage of one of the attach policy operations (AttachUserPolicy/AttachRolePolicy/AttachGroupPolicy). This might indicate a privilege escalation technique that attackers could use.

**Required Data Connectors**

AWS

### Creation of new CRUD IAM policy and then privilege escalation.

Detected creation of new CRUD IAM policy and usage of one of the attach policy operations (AttachUserPolicy/AttachRolePolicy/AttachGroupPolicy). This might indicate a privilege escalation technique that attackers could use.

**Required Data Connectors**

AWS

### Creation of CRUD KMS policy and then privilege escalation

Detected creation of new CRUD KMS policy and usage of one of the attach policy operations (AttachUserPolicy/AttachRolePolicy/AttachGroupPolicy). This might indicate a privilege escalation technique that attackers could use.

**Required Data Connectors**

AWS

### Created CRUD S3 policy and then privilege escalation

Detected creation of new CRUD S3 policy and afterwards used one of the attach policy operations (AttachUserPolicy/AttachRolePolicy/AttachGroupPolicy). This might indicate a privilege escalation technique that attackers could use.

**Required Data Connectors**

AWS

### Creation of CRUD Lambda policy and then privilege escalation

Detected creation of new CRUD Lambda policy and usage of the attach policy events (AttachUserPolicy/AttachRolePolicy/AttachGroupPolicy). This might indicate a privilege escalation technique that attackers could use.

**Required Data Connectors**

AWS

### Creation of DataPipeline policy and then privilege escalation.

Detected creation of new Datapipeline policy and usage of the attach policy operations (AttachUserPolicy/AttachRolePolicy/AttachGroupPolicy). This might indicate a privilege escalation technique that attackers could use.

**Required Data Connectors**

AWS

### Creation of EC2 policy and then privilege escalation

Detected creation of new EC2 policy and afterwards used one of the attach policy operations (AttachUserPolicy/AttachRolePolicy/AttachGroupPolicy). This might indicate a privilege escalation technique that attackers could use.

**Required Data Connectors**

AWS

### Creation of Glue policy and then privilege escalation

Detected creation of new Glue policy and usage one of the attach policy operations (AttachUserPolicy/AttachRolePolicy/AttachGroupPolicy). This might indicate a privilege escalation technique that attackers could use.

**Required Data Connectors**

AWS

### Creation of Lambda policy and then privilege escalation

Detected creation of new Lambda policy and usage of one of the attach policy operations (AttachUserPolicy/AttachRolePolicy/AttachGroupPolicy). This might indicate a privilege escalation technique that attackers could use.

**Required Data Connectors**

AWS

### Creation of SSM policy and then privilege escalation

Detected creation of new SSM policy and afterwards used one of the attach policy operations (AttachUserPolicy/AttachRolePolicy/AttachGroupPolicy). This might indicate a privilege escalation technique that attackers could use.

**Required Data Connectors**

AWS

### Creating keys with encrypt policy without MFA

Detection of KMS keys where action kms:Encrypt is accessible for everyone (also outside of your organization). This is an idicator that your account is compromised and the attacker uses the encryption key to compromise another company.

**Required Data Connectors**

AWS

### Automatic image scanning disabled for ECR

Image Scanning for ECR was disabled, which could lead to missing vulnerable container images in your environment. Attackers could disable the Image Scanning for defense evasion purposes.

**Required Data Connectors**

AWS

### Changes made to AWS CloudTrail logs

Attackers often try to hide their steps by deleting or stopping the collection of logs that could show their activity.

This alert identifies any manipulation of AWS CloudTrail, Cloudwatch/EventBridge or VPC Flow logs.

More Information: AWS CloudTrail API: https://docs.aws.amazon.com/awscloudtrail/latest/APIReference/API\_Operations.html

AWS Cloudwatch/Eventbridge API: https://docs.aws.amazon.com/eventbridge/latest/APIReference/API\_Operations.html

AWS DelteteFlowLogs API : https://docs.aws.amazon.com/AWSEC2/latest/APIReference/API\_DeleteFlowLogs.html

**Required Data Connectors**

AWS

### Network ACL with all the open ports to a specified CIDR

Detected network ACL with all the ports open to a specified CIDR. This could lead to potential lateral movements or initial access attacks. Make sure to mitigate this risk.

**Required Data Connectors**

AWS

### Suspicious overly permessive KMS key policy created

An overly permissive key policy was created, resulting in KMS keys where the kms:Encrypt action is accessible to everyone (even outside of the organization). This could mean that your account is compromised and that the attacker is using the encryption key to compromise other organizations.

**Required Data Connectors**

AWS

### Privilege escalation with AdministratorAccess managed policy

Detected usage of AttachUserPolicy/AttachGroupPolicy/AttachRolePolicy on AdministratorAccess managed policy. Attackers could use these events for privilege escalation. Verify these actions with the user.

**Required Data Connectors**

AWS

### Privilege escalation with admin managed policy

Detected usage of AttachUserPolicy/AttachGroupPolicy/AttachRolePolicy on admin managed policy. Attackers could use these operations for privilege escalation. Verify these actions with the user.

**Required Data Connectors**

AWS

### Privilege escalation with FullAccess managed policy

Detected usage of AttachUserPolicy/AttachGroupPolicy/AttachRolePolicy on FullAccess managed policy. Attackers could use these operations for privilege escalation. Verify these actions with the user.

**Required Data Connectors**

AWS

### Privilege escalation via CloudFormation policy

Detected usage of AttachUserPolicy/AttachGroupPolicy/AttachRolePolicy on CloudFormation policy. Attackers could use these events for privilege escalation. Verify these actions with the user.

**Required Data Connectors**

AWS

### Privilege escalation via CRUD DynamoDB policy

Detected usage of AttachUserPolicy/AttachGroupPolicy/AttachRolePolicy by CRUD DynamoDB Policy. Attackers could use these operations for privilege escalation. Verify these actions with the user.

**Required Data Connectors**

AWS

### Privilege escalation via CRUD IAM policy

Detected usage of AttachUserPolicy/AttachGroupPolicy/AttachRolePolicy by CRUD IAM policy. Attackers could use these operations for privilege escalation. Verify these actions with the user.

**Required Data Connectors**

AWS

### Privilege escalation via CRUD KMS policy

Detected usage of AttachUserPolicy/AttachGroupPolicy/AttachRolePolicy by CRUD KMS policy. Attackers could use these operations for privilege escalation. Verify these actions with the user.

**Required Data Connectors**

AWS

### Privilege escalation via CRUD Lambda policy

Detected usage of AttachUserPolicy/AttachGroupPolicy/AttachRolePolicy by CRUD Lambda policy. Attackers could use these operations for privilege escalation. Verify these actions with the user.

**Required Data Connectors**

AWS

### Privilege escalation via CRUD S3 policy

Detected usage of AttachUserPolicy/AttachGroupPolicy/AttachRolePolicy by CRUD S3 Policy. Attackers could use these operations for privilege escalation. Verify these actions with the user.

**Required Data Connectors**

AWS

### Privilege escalation via DataPipeline policy

Detected usage of AttachUserPolicy/AttachGroupPolicy/AttachRolePolicy on Datapipeline policy. Attackers could use these operations for privilege escalation. Verify these actions with the user.

**Required Data Connectors**

AWS

### Privilege escalation via EC2 policy

Detected usage of AttachUserPolicy/AttachGroupPolicy/AttachRolePolicy on EC2 policy. Attackers could use these operations for privilege escalation. Verify these actions with the user.

**Required Data Connectors**

AWS

### Privilege escalation via Glue policy

Detected usage of AttachUserPolicy/AttachGroupPolicy/AttachRolePolicy on Glue policy. Attackers could use these operations for privilege escalation. Verify these actions with the user.

**Required Data Connectors**

AWS

### Privilege escalation via Lambda policy

Detected usage of AttachUserPolicy/AttachGroupPolicy/AttachRolePolicy on Lambda policy. Attackers could use these operations for privilege escalation. Verify these actions with the user.

**Required Data Connectors**

AWS

### Privilege escalation via SSM policy

Detected usage of AttachUserPolicy/AttachGroupPolicy/AttachRolePolicy on SSM Policy. Attackers could use these operations for privilege escalation. Verify these actions with the user.

**Required Data Connectors**

AWS

### RDS instance publicly exposed

Detected publicly exposed RDS instance, which could lead to a leakage of sensitive data.

**Required Data Connectors**

AWS

### Successful brute force attack on S3 Bucket.

A successful brute force attack on an S3 bucket was detected. Verify these actions, and if needed, remediate the compromise.

**Required Data Connectors**

AWS

### S3 bucket access point publicly exposed

Detected S3 bucket publicly exposed via access point, which could lead to sensitive information leakage to the public. Verify the S3 object configurations.

**Required Data Connectors**

AWS

### S3 bucket exposed via ACL

Detected S3 bucket publicly exposed via ACL, which could lead for sensitive information leakage to the public. Verify the S3 object configurations.

**Required Data Connectors**

AWS

### S3 bucket exposed via policy

Detected S3 bucket publicly exposed via policy, this could lead for sensitive information leakage to the public. Verify the S3 object configurations.

**Required Data Connectors**

AWS

### S3 object publicly exposed

Detected S3 bucket that's publicly exposed, which could lead to sensitive information leakage to the public. Verify the S3 object configurations.

**Required Data Connectors**

AWS

### S3 bucket suspicious ransomware activity

Suspicious S3 bucket activity indicating ransomware was detected.

An attacker might download all the objects in a compromised S3 bucket, encrypt them with his own key, then upload them back to the same bucket, overwriting the existing ones.

**Required Data Connectors**

AWS

### SAML update identity provider

Attackers could update the SAML provider in order to create unauthorized but valid tokens and represent them to services that trust SAML tokens from the environment. These tokens can then be used to access resources. More about this API at https://docs.aws.amazon.com/IAM/latest/APIReference/API\_UpdateSAMLProvider.html

**Required Data Connectors**

AWS

### Policy version set to default

An attacker with SetDefaultPolicyVersion permissions could escalate privileges through existing policy versions that are not currently in use. More about this API at https://docs.aws.amazon.com/IAM/latest/APIReference/API\_SetDefaultPolicyVersion.html

**Required Data Connectors**

AWS

### SSM document is publicly exposed

Detected a SSM document that is publicly exposed, which could lead to sensitive information leakage to the public. Verify the object configurations.

**Required Data Connectors**

AWS

## Hunting Queries

### Changes made to AWS IAM policy

Amazon Web Services Hunting Query 1

### IAM Privilege Escalation by Instance Profile attachment

Amazon Web Services Hunting Query 2

### Privileged role attached to Instance

Amazon Web Services Hunting Query 3

### Suspicious credential token access of valid IAM Roles

Amazon Web Services Hunting Query 4

### Unused or Unsupported Cloud Regions

Amazon Web Services Hunting Query 5

### Suspicious EC2 launched without a key pair

Amazon Web Services Hunting Query 6

### IAM assume role policy brute force

Amazon Web Services Hunting Query 7

### Bucket versioning suspended

Amazon Web Services Hunting Query 8

### New access key created to user

Amazon Web Services Hunting Query 9

### CreateLoginProfile detected

Amazon Web Services Hunting Query 10

### ECR image scan findings low

Amazon Web Services Hunting Query 11

### ECR image scan findings medium

Amazon Web Services Hunting Query 12

### Excessive execution of discovery events

Amazon Web Services Hunting Query 13

### Failed brute force on S3 bucket

Amazon Web Services Hunting Query 14

### Multiple failed login attempts to an existing user without MFA

Amazon Web Services Hunting Query 15

### IAM AccessDenied discovery events

Amazon Web Services Hunting Query 16

### Changes made to AWS IAM objects

Amazon Web Services Hunting Query 17

### Lambda function throttled

Amazon Web Services Hunting Query 18

### Lambda layer imported from external account

Amazon Web Services Hunting Query 19

### Lambda UpdateFunctionCode

Amazon Web Services Hunting Query 20

### Login profile updated

Amazon Web Services Hunting Query 21

### Modification of route-table attributes

Amazon Web Services Hunting Query 22

### Modification of subnet attributes

Amazon Web Services Hunting Query 23

### Modification of vpc attributes

Amazon Web Services Hunting Query 24

### Network ACL deleted

Amazon Web Services Hunting Query 25

### New AccessKey created for Root user

Amazon Web Services Hunting Query 26

### CreatePolicyVersion with excessive permissions

Amazon Web Services Hunting Query 27

### RDS instance master password changed

Amazon Web Services Hunting Query 28

### Risky role name created

Amazon Web Services Hunting Query 29

### S3 bucket has been deleted

Amazon Web Services Hunting Query 30

### S3 bucket encryption modified

Amazon Web Services Hunting Query 31

### Suspicious activity of STS token related to EC2

Amazon Web Services Hunting Query 32

### Suspicious activity of STS token related to ECS

Amazon Web Services Hunting Query 33

### Suspicious activity of STS token related to Glue

Amazon Web Services Hunting Query 34

### Suspicious activity of STS Token related to Kubernetes worker node

Amazon Web Services Hunting Query 35

### Suspicious activity of STS token related to Lambda

Amazon Web Services Hunting Query 36

## Watchlists

## Playbooks

## Parsers

# Apache Http Server

The Apache HTTP Server data connector provides the capability to ingest Apache HTTP Server events into Microsoft Sentinel.

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 10**, Hunting Queries:** 10**, Watchlists:** 0**, Playbooks:** 0, Parsers: 1

## Data Connectors

### Apache HTTP Server

The Apache HTTP Server data connector provides the capability to ingest [Apache HTTP Server](http://httpd.apache.org/) events into Microsoft Sentinel. Refer to [Apache Logs documentation](https://httpd.apache.org/docs/2.4/logs.html) for more information.

## Workbooks

### Apache HTTP Server

Sets the time name for analysis

**Required Data Types**

## Analytic Rules

### Apache - Apache 2.4.49 flaw CVE-2021-41773

Detects using Apache 2.4.49 flaw CVE-2021-41773

**Required Data Connectors**

ApacheHTTPServer

### Apache - Command in URI

Detects command in URI

**Required Data Connectors**

ApacheHTTPServer

### Apache - Known malicious user agent

Detects known malicious user agents

**Required Data Connectors**

ApacheHTTPServer

### Apache - Multiple client errors from single IP

Detects multiple client errors from one source in short timeframe

**Required Data Connectors**

ApacheHTTPServer

### Apache - Multiple server errors from single IP

Detects multiple server errors from one source in short timeframe

**Required Data Connectors**

ApacheHTTPServer

### Apache - Private IP in URL

Detects requests to unusual URL

**Required Data Connectors**

ApacheHTTPServer

### Apache - Put suspicious file

Detects PUT or POST of suspicious file

**Required Data Connectors**

ApacheHTTPServer

### Apache - Request from private IP

Detects requests from private IP

**Required Data Connectors**

ApacheHTTPServer

### Apache - Requests to rare files

Shows requests to rare files

**Required Data Connectors**

ApacheHTTPServer

### Apache - Request to sensitive files

Detects request to sensitive files.

**Required Data Connectors**

ApacheHTTPServer

## Hunting Queries

### Apache - Top files requested with errors

ApacheHTTPServer Hunting Query 1

### Apache - Top Top files requested

ApacheHTTPServer Hunting Query 2

### Apache - Rare files requested

ApacheHTTPServer Hunting Query 3

### Apache - Rare user agents with client errors

ApacheHTTPServer Hunting Query 4

### Apache - Rare URLs requested

ApacheHTTPServer Hunting Query 5

### Apache - Rare user agents

ApacheHTTPServer Hunting Query 6

### Apache - Requests to unexisting files

ApacheHTTPServer Hunting Query 7

### Apache - Unexpected Post Requests

ApacheHTTPServer Hunting Query 8

### Apache - Top URLs with client errors

ApacheHTTPServer Hunting Query 9

### Apache - Top URLs with server errors

ApacheHTTPServer Hunting Query 10

## Watchlists

## Playbooks

## Parsers

### ApacheHTTPServer

Category: Samples

Function Alias: ApacheHTTPServer

# Apache Tomcat

The Apache Tomcat data connector provides the capability to ingest Apache Tomcat events into Azure Sentinel.

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 10**, Hunting Queries:** 11**, Watchlists:** 0**, Playbooks:** 0, Parsers: 1

## Data Connectors

### Apache Tomcat

The Apache Tomcat data connector provides the capability to ingest [Apache Tomcat](http://tomcat.apache.org/) events into Microsoft Sentinel. Refer to [Apache Tomcat documentation](http://tomcat.apache.org/tomcat-10.0-doc/logging.html) for more information.

## Workbooks

### ApacheTomcat

Sets the time name for analysis

**Required Data Types**

Tomcat\_CL

ApacheTomcat

Analytic Rules

### Tomcat - Commands in URI

Detects commands in URI

**Required Data Connectors**

ApacheTomcat

### Tomcat - Known malicious user agent

Detects known malicious user agents

**Required Data Connectors**

ApacheTomcat

### Tomcat - Multiple client errors from single IP address

Detects multiple client errors from one source in short timeframe

**Required Data Connectors**

ApacheTomcat

### Tomcat - Multiple empty requests from same IP

Detects multiple empty requests from same IP

**Required Data Connectors**

ApacheTomcat

### Tomcat - Multiple server errors from single IP address

Detects multiple server errors from one source in short timeframe

**Required Data Connectors**

ApacheTomcat

### Tomcat - Put file and get file from same IP address

Detects put or get files from one source in short timeframe

**Required Data Connectors**

ApacheTomcat

### Tomcat - Request from localhost IP address

Detects request from localhost IP address.

**Required Data Connectors**

ApacheTomcat

### Tomcat - Request to sensitive files

Detects request to sensitive files.

**Required Data Connectors**

ApacheTomcat

### Tomcat - Sql injection patterns

Detects possible sql injection patterns

**Required Data Connectors**

ApacheTomcat

### Tomcat - Server errors after multiple requests from same IP

Detects server errors after multiple requests from same IP address.

**Required Data Connectors**

ApacheTomcat

## Hunting Queries

### Tomcat - Request to forbidden file

Tomcat Hunting Query 1

### Tomcat - Abnormal request size

Tomcat Hunting Query 2

### Tomcat - Catalina errors

Tomcat Hunting Query 3

### Tomcat - Rare files requested

Tomcat Hunting Query 4

### Tomcat - Rare URLs requested

Tomcat Hunting Query 5

### Tomcat - Top files with error requests

Tomcat Hunting Query 6

### Tomcat - Top URLs client errors

Tomcat Hunting Query 7

### Tomcat - Top URLs server errors

Tomcat Hunting Query 8

### Tomcat - Uncommon user agent strings

Tomcat Hunting Query 9

### Tomcat - Rare user agents with client errors

Tomcat Hunting Query 10

### Tomcat - Rare user agents with server errors

Tomcat Hunting Query 11

## Watchlists

## Playbooks

## Parsers

### ApacheTomcat Data Parser

Category: Samples

Function Alias: TomcatEvent

# ARGOS Cloud Security for Microsoft Sentinel

Integrate ARGOS Cloud Security into Microsoft Sentinel SIEM to have all your cloud security issues (CSPM, CAASM, and CIEM) in one spot.

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

## Data Connectors

### ARGOS Cloud Security

The ARGOS Cloud Security integration for Microsoft Sentinel allows you to have all your important cloud security events in one place. This enables you to easily create dashboards, alerts, and correlate events across multiple systems. Overall this will improve your organization's security posture and security incident response.

## Workbooks

### ARGOS Cloud Security

The ARGOS Cloud Security integration for Microsoft Sentinel allows you to have all your important cloud security events in one place.

**Required Data Types**

## Analytic Rules

### ARGOS Cloud Security - Exploitable Cloud Resources

Exploitable Cloud Security Issues are ones that expose cloud resources to the internet and allow initial access to your environment.

**Required Data Connectors**

ARGOSCloudSecurity

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Arista NDR for Microsoft Sentinel

The Arista NDR and Microsoft Sentinel integration sends detection model matches from the Arista NDR Platform to Microsoft Sentinel.

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

## Data Connectors

### Awake Security

The Awake Security CEF connector allows users to send detection model matches from the Awake Security Platform to Microsoft Sentinel. Remediate threats quickly with the power of network detection and response and speed up investigations with deep visibility especially into unmanaged entities including users, devices and applications on your network. The connector also enables the creation of network security-focused custom alerts, incidents, workbooks and notebooks that align with your existing security operations workflows.

## Workbooks

### Arista Awake

Sets the time name for analysis

**Required Data Types**

## Analytic Rules

### Awake Security - High Match Counts By Device

This query searches for devices with unexpectedly large number of activity match.

**Required Data Connectors**

AristaAwakeSecurity

### Awake Security - High Severity Matches By Device

This query searches for devices with high severity event(s).

**Required Data Connectors**

AristaAwakeSecurity

### Awake Security - Model With Multiple Destinations

This query searches for devices with multiple possibly malicious destinations.

**Required Data Connectors**

AristaAwakeSecurity

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Armorblox for Microsoft Sentinel

Armorblox’s integration with Microsoft Sentinel reduces complexity in your SOC while enhancing security posture by accelerating advanced threat detection, investigation, and response.

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

## Data Connectors

### Armorblox (using Azure Function)

The [Armorblox](https://www.armorblox.com/) data connector provides the capability to ingest incidents from your Armorblox instance into Microsoft Sentinel through the REST API. The connector provides ability to get events which helps to examine potential security risks, and more.

## Workbooks

### Armorblox

INCIDENTS FROM SELECTED TIME RANGE

**Required Data Types**

Armorblox\_CL

Armorblox

## Analytic Rules

### Armorblox Needs Review Alert

This rule generates an alert for an Armorblox incident where the remediation action is "Needs Review".

**Required Data Connectors**

Armorblox

## Hunting Queries

## Watchlists

## Playbooks

### Needs-Review-Incident-Email-Notification

This playbook will send an email notification when a new incident is created in Microsoft Sentinel.

## Parsers

# Aruba ClearPass

Connects your Aruba ClearPass with Microsoft Sentinel

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

## Data Connectors

### Aruba ClearPass

The [Aruba ClearPass](https://www.arubanetworks.com/products/security/network-access-control/secure-access/) connector allows you to easily connect your Aruba ClearPass with Microsoft Sentinel, to create custom dashboards, alerts, and improve investigation. This gives you more insight into your organization’s network and improves your security operation capabilities.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### ArubaClearPass

Category: Samples

Function Alias: ArubaClearPass

# Atlassian Confluence Audit

The Atlassian Confluence Audit solution provides the capability to ingest Confluence Audit Records into Microsoft Sentinel.

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

## Data Connectors

### Atlassian Confluence Audit (using Azure Function)

The [Atlassian Confluence](https://www.atlassian.com/software/confluence) Audit data connector provides the capability to ingest [Confluence Audit Records](https://support.atlassian.com/confluence-cloud/docs/view-the-audit-log/) for more information. The connector provides ability to get events which helps to examine potential security risks, analyze your team's use of collaboration, diagnose configuration problems and more.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### ConfluenceAudit

Category: Samples

Function Alias: ConfluenceAudit

# Atlassian Jira Audit

The Atlassian Jira Audit data connector provides the capability to ingest Jira Audit Records events into Azure Sentinel through the REST API.

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 10**, Hunting Queries:** 10**, Watchlists:** 0**, Playbooks:** 7, Parsers: 0

## Data Connectors

### Atlassian Jira Audit (using Azure Function)

The [Atlassian Jira](https://www.atlassian.com/software/jira) Audit data connector provides the capability to ingest [Jira Audit Records](https://support.atlassian.com/jira-cloud-administration/docs/audit-activities-in-jira-applications/) events into Microsoft Sentinel through the REST API. Refer to [API documentation](https://developer.atlassian.com/cloud/jira/platform/rest/v3/api-group-audit-records/) for more information. The connector provides ability to get events which helps to examine potential security risks, analyze your team's use of collaboration, diagnose configuration problems and more.

## Workbooks

### AtlassianJiraAudit

Sets the time name for analysis

**Required Data Types**

AtlassianJiraNativePoller\_CL

AtlassianJira

## Analytic Rules

### Jira - Global permission added

Detects when global permission added.

**Required Data Connectors**

JiraAuditAPI

### Jira - New site admin user

Detects new site admin user.

**Required Data Connectors**

JiraAuditAPI

### Jira - New user created

Detects when new user was created.

**Required Data Connectors**

JiraAuditAPI

### Jira - Permission scheme updated

Detects when permission scheme was updated.

**Required Data Connectors**

JiraAuditAPI

### Jira - New site admin user

Detects new site admin user.

**Required Data Connectors**

JiraAuditAPI

### Jira - Project roles changed

Detects when project roles were changed.

**Required Data Connectors**

JiraAuditAPI

### Jira - User's password changed multiple times

Detects when user's password was changed multiple times from different IP addresses.

**Required Data Connectors**

JiraAuditAPI

### Jira - User removed from group

Detects when a user was removed from group.

**Required Data Connectors**

JiraAuditAPI

### Jira - User removed from project

Detects when a user was removed from project.

**Required Data Connectors**

JiraAuditAPI

### Jira - Workflow scheme copied

Detects when workflow scheme was copied.

**Required Data Connectors**

JiraAuditAPI

## Hunting Queries

### Jira - Blocked tasks

AtlassianJiraAudit Hunting Query 1

### Jira - New users

AtlassianJiraAudit Hunting Query 2

### Jira - Project versions released

AtlassianJiraAudit Hunting Query 3

### Jira - Project versions

AtlassianJiraAudit Hunting Query 4

### Jira - Updated projects

AtlassianJiraAudit Hunting Query 5

### Jira - Updated users

AtlassianJiraAudit Hunting Query 6

### Jira - Updated workflow schemes

AtlassianJiraAudit Hunting Query 7

### Jira - Updated workflows

AtlassianJiraAudit Hunting Query 8

### Jira - Users' IP addresses

AtlassianJiraAudit Hunting Query 9

### Jira - Workflow schemes added to projects

AtlassianJiraAudit Hunting Query 10

## Watchlists

## Playbooks

### Create Jira Issue alert-trigger

This playbook will open a Jira Issue when a new incident is opened in Microsoft Sentinel.

### Create Jira Issue incident-trigger

This playbook will open a Jira Issue when a new incident is opened in Microsoft Sentinel.

### Create And Update Jira Issue

This playbook will create or update incident in Jira. When incident is created, playbook will run and create issue in Jira. When incident is updated, playbook will run and add update to comment section.

### Sync Jira to Sentinel - Assigned User

This Playbook will sync the assigned user from JIRA to Microsoft Sentinel.

### Sync Jira to Sentinel - public comments

This Playbook will sync the public comments from JIRA to Microsoft Sentinel.

### Sync Jira from Sentinel - Create incident

This Playbook will create JIRA incidents for every Microsoft Sentinel which is created. It includes additional information such as tactics, affected user etc.

### Sync Jira to Sentinel - Status

This Playbook will sync the status from JIRA to Microsoft Sentinel.

## Parsers

# Attacker Tools Threat Protection Essentials

The Attacker Tools Threat Protection Essentials solution contains security content that is relevant for detection of tools commonly used by attackers in various campaigns.

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

## Data Connectors

## Workbooks

## Analytic Rules

### Probable AdFind Recon Tool Usage

Identifies the host and account that executed AdFind by hash and filename in addition to common and unique flags that are used by many threat actors in discovery.

**Required Data Connectors**

MicrosoftThreatProtection

### Credential Dumping Tools - Service Installation

This query detects the installation of a Windows service that contains artifacts from credential dumping tools such as Mimikatz.

Ref: https://blueteamblog.com/darkside-ransomware-operations-preventions-and-detections

**Required Data Connectors**

SecurityEvents

### Credential Dumping Tools - File Artifacts

This query detects the creation of credential dumping tools files. Several credential dumping tools export files with hardcoded file names.

Ref: https://jpcertcc.github.io/ToolAnalysisResultSheet/

**Required Data Connectors**

SecurityEvents

### Powershell Empire cmdlets seen in command line

Identifies instances of PowerShell Empire cmdlets in powershell process command line data.

**Required Data Connectors**

SecurityEvents

WindowsSecurityEvents

WindowsSecurityEvents

WindowsForwardedEvents

## Hunting Queries

### Cobalt Strike DNS Beaconing

Attacker Tools Threat Protection Essentials Hunting Query 1

### Potential Impacket Execution

Attacker Tools Threat Protection Essentials Hunting Query 2

## Watchlists

## Playbooks

## Parsers

# Australian Cyber Security Centre

This solution allows customers to share threat intelligence with the Australian Cyber Security Centre (ACSC) through the Cyber Threat Intelligence Sharing (CTIS) program.

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

## Data Connectors

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

### AusCtisExportTaggedIndicators

This playbook gets triggered every hour and perform the following actions:

1. Get all the threat intelligence indicators from Sentinel Workspace with given tag.

2. Filter all the indicators whose export in not completed.

3. Export the indicators to provided TAXII server.

## Parsers

# Auth0

The Auth0 Access Management solution for Microsoft Sentinel provides the capability to ingest Auth0 log events into your Microsoft Sentinel workspace.

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

## Data Connectors

### Auth0 Access Management (using Azure Function)

The [Auth0 Access Management](https://auth0.com/access-management) data connector provides the capability to ingest [Auth0 log events](https://auth0.com/docs/api/management/v2/#!/Logs/get\_logs) into Microsoft Sentinel

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### Auth0

Category: Samples

Function Alias: Auth0

# Automated Logic WebCTRL

You can stream the audit logs from the WebCTRL SQL server hosted on Windows machines connected to your Microsoft Sentinel.

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

## Data Connectors

### Automated Logic WebCTRL

You can stream the audit logs from the WebCTRL SQL server hosted on Windows machines connected to your Microsoft Sentinel. This connection enables you to view dashboards, create custom alerts and improve investigation. This gives insights into your Industrial Control Systems that are monitored or controlled by the WebCTRL BAS application.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# AWS Athena

Amazon Athena is an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL.

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

## Data Connectors

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

### AWS Athena - Execute Query and Get Results

When a new sentinel incident is created, this playbook gets triggered and performs the following actions:

1. It executes the query specified during playbook setup on given database.

2. Downloads the query result and adds as a comment to the incident.

## Parsers

# AWS IAM

The Amazon Web Services (AWS) Identity and Access Management (IAM) Solution for Microsoft Sentinel allows you to manage resources in AWS via playbooks thats use the AWS IAM API.

**Data Connectors:** 0**, Workbooks:** 0**, Analytic Rules:** 0**, Hunting Queries:** 0**, Watchlists:** 0**, Playbooks:** 3, Parsers: 0

## Data Connectors

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

### AWS IAM - Add tag to user

Once a new Microsoft Sentinel incident is created, this playbook gets triggered and performs the following actions:

1. Gets users from the incident.

2. [Adds tag](https://docs.aws.amazon.com/IAM/latest/APIReference/API\_TagUser.html) to users in AWS (tag key and value are defined during the playbook deployment).

3. Adds information about added tags as a comment to the incident.

### AWS IAM - Delete access keys

Once a new Microsoft Sentinel incident is created, this playbook gets triggered and performs the following actions:

1. Gets users from the incident.

2. [Get list of access keys](https://docs.aws.amazon.com/IAM/latest/APIReference/API\_ListAccessKeys.html) from these users.

3. Delete selected access keys.

4. Adds information about deleted user's access keys as a comment to the incident.

### AWS IAM - Enrich incident with user info

Once a new Microsoft Sentinel incident is created, this playbook gets triggered and performs the following actions:

1. Gets users from the incident.

2. Obtains information about users in AWS IAM.

3. Adds obtained information as a comment to the incident.

## Parsers

# Azure Active Directory Identity Protection

The Azure Active Directory Identity Protection solution for Microsoft Sentinel allows you to ingest Security alerts reported in AAD Identity Protection for risky users and events in Azure Active Directory.

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

## Data Connectors

### Azure Active Directory Identity Protection

Azure Active Directory Identity Protection provides a consolidated view at risk users, risk events and vulnerabilities, with the ability to remediate risk immediately, and set policies to auto-remediate future events. The service is built on Microsoft’s experience protecting consumer identities and gains tremendous accuracy from the signal from over 13 billion logins a day. Integrate Microsoft Azure Active Directory Identity Protection alerts with Microsoft Sentinel to view dashboards, create custom alerts, and improve investigation. For more information, see the [Microsoft Sentinel documentation ](https://go.microsoft.com/fwlink/p/?linkid=2220065&wt.mc\_id=sentinel\_dataconnectordocs\_content\_cnl\_csasci).

[Get Azure Active Directory Premium P1/P2 ](https://aka.ms/asi-ipcconnectorgetlink)

## Workbooks

## Analytic Rules

### Correlate Unfamiliar sign-in properties and atypical travel alerts

The combination of an Unfamiliar sign-in properties alert and an Atypical travel alert about the same user within a +10m or -10m window is considered a high severity incident.

**Required Data Connectors**

AzureActiveDirectoryIdentityProtection

BehaviorAnalytics

## Hunting Queries

## Watchlists

## Playbooks

### Confirm AAD Risky User - Alert Triggered

This playbook will set the Risky User property in AAD using Graph API.

### Confirm AAD Risky User - Incident Triggered

For each account entity included in the incident, this playbook will set the Risky User property in AAD using Graph API using a Beta API.

### Dismiss AAD Risky User - Alert Triggered

This playbook will dismiss the Risky User property in AAD using AAD Connectors.

### Dismiss AAD Risky User – Incident Triggered

This playbook will dismiss the Risky User property in AAD using AAD Connectors.

### Identity Protection response from Teams

Run this playbook on incidents which contains suspiciouse AAD identities. For each account, this playbook posts an adaptive card in the SOC Microsoft Teams channel, including the potential risky user information given by Azure AD Identity Protection. The card offers to confirm the user as compromised or dismiss the compromised user in AADIP. It also allows to configure the Microsoft Sentinel incident. A summary comment will be posted to document the action taken and user information. [Learn more about Azure AD Identity Protection](https://docs.microsoft.com/azure/active-directory/identity-protection/overview-identity-protection)

## Parsers

# Azure Active Directory solution for Sentinel

The Azure Active Directory solution for Microsoft Sentinel enables you to ingest Azure Active Directory Audit,Sign-in,Provisioning,Risk Events and Risky User/Service Principal logs using Diagnostic Settings into Microsoft Sentinel.

**Data Connectors:** 1**, Workbooks:** 2**, Analytic Rules:** 48**, Hunting Queries:** 0**, Watchlists:** 0**, Playbooks:** 6, Parsers: 0

## Data Connectors

### Azure Active Directory

Gain insights into Azure Active Directory by connecting Audit and Sign-in logs to Microsoft Sentinel to gather insights around Azure Active Directory scenarios. You can learn about app usage, conditional access policies, legacy auth relate details using our Sign-in logs. You can get information on your Self Service Password Reset (SSPR) usage, Azure Active Directory Management activities like user, group, role, app management using our Audit logs table. For more information, see the [Microsoft Sentinel documentation](https://go.microsoft.com/fwlink/?linkid=2219715&wt.mc\_id=sentinel\_dataconnectordocs\_content\_cnl\_csasci).

## Workbooks

### Azure AD Audit logs

Gain insights into Azure Active Directory by connecting Microsoft Sentinel and using the audit logs to gather insights around Azure AD scenarios.

You can learn about user operations, including password and group management, device activities, and top active users and apps.

**Required Data Types**

AuditLogs

AzureActiveDirectory

### Azure AD Sign-in logs

Gain insights into Azure Active Directory by connecting Microsoft Sentinel and using the sign-in logs to gather insights around Azure AD scenarios.

You can learn about sign-in operations, such as user sign-ins and locations, email addresses, and IP addresses of your users, as well as failed activities and the errors that triggered the failures.

**Required Data Types**

SigninLogs

AzureActiveDirectory

## Analytic Rules

### Account Created and Deleted in Short Timeframe

Search for user principal name (UPN) events. Look for accounts created and then deleted in under 24 hours. Attackers may create an account for their use, and then remove the account when no longer needed.

Ref : https://docs.microsoft.com/azure/active-directory/fundamentals/security-operations-user-accounts#short-lived-account

**Required Data Connectors**

AzureActiveDirectory

### Account created or deleted by non-approved user

Identifies accounts that were created or deleted by a defined list of non-approved user principal names. Add to this list before running the query for accurate results.

Ref : https://docs.microsoft.com/azure/active-directory/fundamentals/security-operations-user-accounts

**Required Data Connectors**

AzureActiveDirectory

### Modified domain federation trust settings

This will alert when a user or application modifies the federation settings on the domain or Update domain authentication from Managed to Federated.

For example, this alert will trigger when a new Active Directory Federated Service (ADFS) TrustedRealm object, such as a signing certificate, is added to the domain.

Modification to domain federation settings should be rare. Confirm the added or modified target domain/URL is legitimate administrator behavior.

To understand why an authorized user may update settings for a federated domain in Office 365, Azure, or Intune, see: https://docs.microsoft.com/office365/troubleshoot/active-directory/update-federated-domain-office-365.

For details on security realms that accept security tokens, see the ADFS Proxy Protocol (MS-ADFSPP) specification: https://docs.microsoft.com/openspecs/windows\_protocols/ms-adfspp/e7b9ea73-1980-4318-96a6-da559486664b.

For further information on AuditLogs please see https://docs.microsoft.com/azure/active-directory/reports-monitoring/reference-audit-activities.

**Required Data Connectors**

AzureActiveDirectory

### Password spray attack against ADFSSignInLogs

Identifies evidence of password spray activity against Connect Health for AD FS sign-in events by looking for failures from multiple accounts from the same IP address within a time window.

Reference: https://adfshelp.microsoft.com/References/ConnectHealthErrorCodeReference

**Required Data Connectors**

AzureActiveDirectory

### Admin promotion after Role Management Application Permission Grant

This rule looks for a service principal being granted the Microsoft Graph RoleManagement.ReadWrite.Directory (application) permission before being used to add an Azure AD object or user account to an Admin directory role (i.e. Global Administrators).

This is a known attack path that is usually abused when a service principal already has the AppRoleAssignment.ReadWrite.All permission granted. This permission Allows an app to manage permission grants for application permissions to any API.

A service principal can promote itself or other service principals to admin roles (i.e. Global Administrators). This would be considered a privilege escalation technique.

Ref : https://docs.microsoft.com/graph/permissions-reference#role-management-permissions, https://docs.microsoft.com/graph/api/directoryrole-post-members?view=graph-rest-1.0&tabs=http

**Required Data Connectors**

AzureActiveDirectory

### Anomalous sign-in location by user account and authenticating application

This query over Azure Active Directory sign-in considers all user sign-ins for each Azure Active

Directory application and picks out the most anomalous change in location profile for a user within an

individual application. An alert is generated for recent sign-ins that have location counts that are anomalous

over last day but also over the last 3-day and 7-day periods.

Please note that on workspaces with larger volume of Signin data (~10M+ events a day) may timeout when using this default query time period.

It is recommended that you test and tune this appropriately for the workspace.

**Required Data Connectors**

AzureActiveDirectory

AzureActiveDirectory

### Authentication Methods Changed for Privileged Account

Identifies authentication methods being changed for a privileged account. This could be an indication of an attacker adding an auth method to the account so they can have continued access.

Ref : https://docs.microsoft.com/azure/active-directory/fundamentals/security-operations-privileged-accounts#things-to-monitor-1

**Required Data Connectors**

AzureActiveDirectory

### Azure Active Directory PowerShell accessing non-AAD resources

This will alert when a user or application signs in using Azure Active Directory PowerShell to access non-Active Directory resources, such as the Azure Key Vault, which may be undesired or unauthorized behavior.

For capabilities and expected behavior of the Azure Active Directory PowerShell module, see: https://docs.microsoft.com/powershell/module/azuread/?view=azureadps-2.0.

For further information on Azure Active Directory Signin activity reports, see: https://docs.microsoft.com/azure/active-directory/reports-monitoring/concept-sign-ins.

**Required Data Connectors**

AzureActiveDirectory

AzureActiveDirectory

### Azure AD Role Management Permission Grant

Identifies when the Microsoft Graph RoleManagement.ReadWrite.Directory (Delegated or Application) permission is granted to a service principal.

This permission allows an application to read and manage the role-based access control (RBAC) settings for your company's directory.

An adversary could use this permission to add an Azure AD object to an Admin directory role and escalate privileges.

Ref : https://docs.microsoft.com/graph/permissions-reference#role-management-permissions

Ref : https://docs.microsoft.com/graph/api/directoryrole-post-members?view=graph-rest-1.0&tabs=http

**Required Data Connectors**

AzureActiveDirectory

### Azure Portal Signin from another Azure Tenant

This query looks for sign in attempts to the Azure Portal where the user who is signing in from another Azure tenant,

and the IP address the login attempt is from is an Azure IP. A threat actor who compromises an Azure tenant may look

to pivot to other tenants leveraging cross-tenant delegated access in this manner.

**Required Data Connectors**

AzureActiveDirectory

### Brute Force Attack against GitHub Account

Attackers who are trying to guess your users' passwords or use brute-force methods to get in. If your organization is using SSO with Azure Active Directory, authentication logs to GitHub.com will be generated. Using the following query can help you identify a sudden increase in failed logon attempt of users.

**Required Data Connectors**

AzureActiveDirectory

AzureActiveDirectory

### Brute force attack against a Cloud PC

Identifies evidence of brute force activity against a Windows 365 Cloud PC by highlighting multiple authentication failures and by a successful authentication within a given time window.

**Required Data Connectors**

AzureActiveDirectory

### Bulk Changes to Privileged Account Permissions

Identifies when changes to multiple users permissions are changed at once. Investigate immediately if not a planned change. This setting could enable an attacker access to Azure subscriptions in your environment.

Ref : https://docs.microsoft.com/azure/active-directory/fundamentals/security-operations-privileged-identity-management

**Required Data Connectors**

AzureActiveDirectory

### Attempt to bypass conditional access rule in Azure AD

Identifies an attempt to Bypass conditional access rule(s) in Azure Active Directory.

The ConditionalAccessStatus column value details if there was an attempt to bypass Conditional Access

or if the Conditional access rule was not satisfied (ConditionalAccessStatus == 1).

References:

https://docs.microsoft.com/azure/active-directory/conditional-access/overview

https://docs.microsoft.com/azure/active-directory/reports-monitoring/concept-sign-ins

https://docs.microsoft.com/azure/active-directory/reports-monitoring/reference-sign-ins-error-codes

ConditionalAccessStatus == 0 // Success

ConditionalAccessStatus == 1 // Failure

ConditionalAccessStatus == 2 // Not Applied

ConditionalAccessStatus == 3 // unknown

**Required Data Connectors**

AzureActiveDirectory

AzureActiveDirectory

### Credential added after admin consented to Application

This query will identify instances where Service Principal credentials were added to an application by one user after the application was granted admin consent rights by another user.

If a threat actor obtains access to an account with sufficient privileges and adds the alternate authentication material triggering this event, the threat actor can now authenticate as the Application or Service Principal using this credential.

Additional information on OAuth Credential Grants can be found in RFC 6749 Section 4.4 or https://docs.microsoft.com/azure/active-directory/develop/v2-oauth2-client-creds-grant-flow.

For further information on AuditLogs please see https://docs.microsoft.com/azure/active-directory/reports-monitoring/reference-audit-activities

**Required Data Connectors**

AzureActiveDirectory

### Attempts to sign in to disabled accounts

Identifies failed attempts to sign in to disabled accounts across multiple Azure Applications.

Default threshold for Azure Applications attempted to sign in to is 3.

References: https://docs.microsoft.com/azure/active-directory/reports-monitoring/reference-sign-ins-error-codes

50057 - User account is disabled. The account has been disabled by an administrator.

**Required Data Connectors**

AzureActiveDirectory

AzureActiveDirectory

### Distributed Password cracking attempts in AzureAD

Identifies distributed password cracking attempts from the Azure Active Directory SigninLogs.

The query looks for unusually high number of failed password attempts coming from multiple locations for a user account.

References: https://docs.microsoft.com/azure/active-directory/reports-monitoring/reference-sign-ins-error-codes

50053 Account is locked because the user tried to sign in too many times with an incorrect user ID or password.

50055 Invalid password, entered expired password.

50056 Invalid or null password - Password does not exist in store for this user.

50126 Invalid username or password, or invalid on-premises username or password.

**Required Data Connectors**

AzureActiveDirectory

AzureActiveDirectory

### Explicit MFA Deny

User explicitly denies MFA push, indicating that login was not expected and the account's password may be compromised.

**Required Data Connectors**

AzureActiveDirectory

AzureActiveDirectory

### Failed login attempts to Azure Portal

Identifies failed login attempts in the Azure Active Directory SigninLogs to the Azure Portal. Many failed logon

attempts or some failed logon attempts from multiple IPs could indicate a potential brute force attack.

The following are excluded due to success and non-failure results:

References: https://docs.microsoft.com/azure/active-directory/reports-monitoring/reference-sign-ins-error-codes

0 - successful logon

50125 - Sign-in was interrupted due to a password reset or password registration entry.

50140 - This error occurred due to 'Keep me signed in' interrupt when the user was signing-in.

**Required Data Connectors**

AzureActiveDirectory

AzureActiveDirectory

### First access credential added to Application or Service Principal where no credential was present

This will alert when an admin or app owner account adds a new credential to an Application or Service Principal where there was no previous verify KeyCredential associated.

If a threat actor obtains access to an account with sufficient privileges and adds the alternate authentication material triggering this event, the threat actor can now authenticate as the Application or Service Principal using this credential.

Additional information on OAuth Credential Grants can be found in RFC 6749 Section 4.4 or https://docs.microsoft.com/azure/active-directory/develop/v2-oauth2-client-creds-grant-flow

For further information on AuditLogs please see https://docs.microsoft.com/azure/active-directory/reports-monitoring/reference-audit-activities.

**Required Data Connectors**

AzureActiveDirectory

### Mail.Read Permissions Granted to Application

This query look for applications that have been granted (Delegated or App/Role) permissions to Read Mail (Permissions field has Mail.Read) and subsequently has been consented to. This can help identify applications that have been abused to gain access to mailboxes.

**Required Data Connectors**

AzureActiveDirectory

### Suspicious application consent similar to O365 Attack Toolkit

This will alert when a user consents to provide a previously-unknown Azure application with the same OAuth permissions used by the MDSec O365 Attack Toolkit (https://github.com/mdsecactivebreach/o365-attack-toolkit).

The default permissions/scope for the MDSec O365 Attack toolkit change sometimes but often include contacts.read, user.read, mail.read, notes.read.all, mailboxsettings.readwrite, files.readwrite.all, mail.send, files.read, and files.read.all.

Consent to applications with these permissions should be rare, especially as the knownApplications list is expanded, especially as the knownApplications list is expanded. Public contributions to expand this filter are welcome!

For further information on AuditLogs please see https://docs.microsoft.com/azure/active-directory/reports-monitoring/reference-audit-activities.

**Required Data Connectors**

AzureActiveDirectory

### Suspicious application consent similar to PwnAuth

This will alert when a user consents to provide a previously-unknown Azure application with the same OAuth permissions used by the FireEye PwnAuth toolkit (https://github.com/fireeye/PwnAuth).

The default permissions/scope for the PwnAuth toolkit are user.read, offline\_access, mail.readwrite, mail.send, and files.read.all.

Consent to applications with these permissions should be rare, especially as the knownApplications list is expanded. Public contributions to expand this filter are welcome!

For further information on AuditLogs please see https://docs.microsoft.com/azure/active-directory/reports-monitoring/reference-audit-activities.

**Required Data Connectors**

AzureActiveDirectory

### MFA Rejected by User

Identifies accurances where a user has rejected an MFA prompt. This could be an indicator that a threat actor has compromised the username and password of this user account and is using it to try and log into the account.

Ref : https://docs.microsoft.com/azure/active-directory/fundamentals/security-operations-user-accounts#monitoring-for-failed-unusual-sign-ins

**Required Data Connectors**

AzureActiveDirectory

### Multiple admin membership removals from newly created admin.

This query detects when newly created Global admin removes multiple existing global admins which can be an attempt by adversaries to lock down organization and retain sole access.

Investigate reasoning and intention of multiple membership removal by new Global admins and take necessary actions accordingly.

**Required Data Connectors**

AzureActiveDirectory

### New access credential added to Application or Service Principal

This will alert when an admin or app owner account adds a new credential to an Application or Service Principal where a verify KeyCredential was already present for the app.

If a threat actor obtains access to an account with sufficient privileges and adds the alternate authentication material triggering this event, the threat actor can now authenticate as the Application or Service Principal using this credential.

Additional information on OAuth Credential Grants can be found in RFC 6749 Section 4.4 or https://docs.microsoft.com/azure/active-directory/develop/v2-oauth2-client-creds-grant-flow

For further information on AuditLogs please see https://docs.microsoft.com/azure/active-directory/reports-monitoring/reference-audit-activities.

**Required Data Connectors**

AzureActiveDirectory

### NRT Modified domain federation trust settings

This will alert when a user or application modifies the federation settings on the domain or Update domain authentication from Managed to Federated.

For example, this alert will trigger when a new Active Directory Federated Service (ADFS) TrustedRealm object, such as a signing certificate, is added to the domain.

Modification to domain federation settings should be rare. Confirm the added or modified target domain/URL is legitimate administrator behavior.

To understand why an authorized user may update settings for a federated domain in Office 365, Azure, or Intune, see: https://docs.microsoft.com/office365/troubleshoot/active-directory/update-federated-domain-office-365.

For details on security realms that accept security tokens, see the ADFS Proxy Protocol (MS-ADFSPP) specification: https://docs.microsoft.com/openspecs/windows\_protocols/ms-adfspp/e7b9ea73-1980-4318-96a6-da559486664b.

For further information on AuditLogs please see https://docs.microsoft.com/azure/active-directory/reports-monitoring/reference-audit-activities.

**Required Data Connectors**

AzureActiveDirectory

### NRT MFA Rejected by User

Identifies occurrences where a user has rejected an MFA prompt. This could be an indicator that a threat actor has compromised the username and password of this user account and is using it to try and log into the account.

Ref : https://docs.microsoft.com/azure/active-directory/fundamentals/security-operations-user-accounts#monitoring-for-failed-unusual-sign-ins

**Required Data Connectors**

AzureActiveDirectory

### NRT New access credential added to Application or Service Principal

This will alert when an admin or app owner account adds a new credential to an Application or Service Principal where a verify KeyCredential was already present for the app.

If a threat actor obtains access to an account with sufficient privileges and adds the alternate authentication material triggering this event, the threat actor can now authenticate as the Application or Service Principal using this credential.

Additional information on OAuth Credential Grants can be found in RFC 6749 Section 4.4 or https://docs.microsoft.com/azure/active-directory/develop/v2-oauth2-client-creds-grant-flow

For further information on AuditLogs please see https://docs.microsoft.com/azure/active-directory/reports-monitoring/reference-audit-activities.

**Required Data Connectors**

AzureActiveDirectory

### NRT PIM Elevation Request Rejected

Identifies when a user is rejected for a privileged role elevation via PIM. Monitor rejections for indicators of attacker compromise of the requesting account.

Ref : https://docs.microsoft.com/azure/active-directory/fundamentals/security-operations-privileged-identity-management

**Required Data Connectors**

AzureActiveDirectory

### NRT Privileged Role Assigned Outside PIM

Identifies a privileged role being assigned to a user outside of PIM

Ref : https://docs.microsoft.com/azure/active-directory/fundamentals/security-operations-privileged-accounts#things-to-monitor-1

**Required Data Connectors**

AzureActiveDirectory

### NRT User added to Azure Active Directory Privileged Groups

This will alert when a user is added to any of the Privileged Groups.

For further information on AuditLogs please see https://docs.microsoft.com/azure/active-directory/reports-monitoring/reference-audit-activities.

For Administrator role permissions in Azure Active Directory please see https://docs.microsoft.com/azure/active-directory/users-groups-roles/directory-assign-admin-roles

**Required Data Connectors**

AzureActiveDirectory

### PIM Elevation Request Rejected

Identifies when a user is rejected for a privileged role elevation via PIM. Monitor rejections for indicators of attacker compromise of the requesting account.

Ref : https://docs.microsoft.com/azure/active-directory/fundamentals/security-operations-privileged-identity-management

**Required Data Connectors**

AzureActiveDirectory

### Privileged Accounts - Sign in Failure Spikes

Identifies spike in failed sign-ins from Privileged accounts. Privileged accounts list can be based on IdentityInfo UEBA table or built-in watchlist.

Spike is determined based on Time series anomaly which will look at historical baseline values.

Ref : https://docs.microsoft.com/azure/active-directory/fundamentals/security-operations-privileged-accounts#things-to-monitor

**Required Data Connectors**

AzureActiveDirectory

AzureActiveDirectory

### Privileged Role Assigned Outside PIM

Identifies a privileged role being assigned to a user outside of PIM

Ref : https://docs.microsoft.com/azure/active-directory/fundamentals/security-operations-privileged-accounts#things-to-monitor-1

**Required Data Connectors**

AzureActiveDirectory

### Rare application consent

This will alert when the "Consent to application" operation occurs by a user that has not done this operation before or rarely does this.

This could indicate that permissions to access the listed Azure App were provided to a malicious actor.

Consent to application, Add service principal and Add OAuth2PermissionGrant should typically be rare events.

This may help detect the Oauth2 attack that can be initiated by this publicly available tool - https://github.com/fireeye/PwnAuth

For further information on AuditLogs please see https://docs.microsoft.com/azure/active-directory/reports-monitoring/reference-audit-activities.

**Required Data Connectors**

AzureActiveDirectory

### Password spray attack against Azure AD Seamless SSO

This query detects when there is a spike in Azure AD Seamless SSO errors. They may not be caused by a Password Spray attack, but the cause of the errors might need to be investigated.

Azure AD only logs the requests that matched existing accounts, thus there might have been unlogged requests for non-existing accounts.

**Required Data Connectors**

AzureActiveDirectory

### GitHub Signin Burst from Multiple Locations

This alerts when there Signin burst from multiple locations in GitHub (AAD SSO).

**Required Data Connectors**

AzureActiveDirectory

AzureActiveDirectory

### Sign-ins from IPs that attempt sign-ins to disabled accounts

Identifies IPs with failed attempts to sign in to one or more disabled accounts and where that same IP has had successful signins from other accounts.

This could indicate an attacker who obtained credentials for a list of accounts and is attempting to login with those accounts, some of which may have already been disabled.

References: https://docs.microsoft.com/azure/active-directory/reports-monitoring/reference-sign-ins-error-codes

50057 - User account is disabled. The account has been disabled by an administrator.

**Required Data Connectors**

AzureActiveDirectory

AzureActiveDirectory

### Brute force attack against Azure Portal

Identifies evidence of brute force activity against Azure Portal by highlighting multiple authentication failures

and by a successful authentication within a given time window.

Default Failure count is 10 and default Time Window is 20 minutes.

References: https://docs.microsoft.com/azure/active-directory/reports-monitoring/reference-sign-ins-error-codes.

**Required Data Connectors**

AzureActiveDirectory

AzureActiveDirectory

### Password spray attack against Azure AD application

Identifies evidence of password spray activity against Azure AD applications by looking for failures from multiple accounts from the same

IP address within a time window. If the number of accounts breaches the threshold just once, all failures from the IP address within the time range

are bought into the result. Details on whether there were successful authentications by the IP address within the time window are also included.

This can be an indicator that an attack was successful.

The default failure acccount threshold is 5, Default time window for failures is 20m and default look back window is 3 days

Note: Due to the number of possible accounts involved in a password spray it is not possible to map identities to a custom entity.

References: https://docs.microsoft.com/azure/active-directory/reports-monitoring/reference-sign-ins-error-codes.

**Required Data Connectors**

AzureActiveDirectory

AzureActiveDirectory

### Successful logon from IP and failure from a different IP

Identifies when a user account successfully logs onto an Azure App from one IP and within 10 mins failed to logon to the same App via a different IP.

This may indicate a malicious attempt at password guessing based on knowledge of the users account.

**Required Data Connectors**

AzureActiveDirectory

AzureActiveDirectory

### Suspicious application consent for offline access

This will alert when a user consents to provide a previously-unknown Azure application with offline access via OAuth.

Offline access will provide the Azure App with access to the listed resources without requiring two-factor authentication.

Consent to applications with offline access and read capabilities should be rare, especially as the knownApplications list is expanded. Public contributions to expand this filter are welcome!

For further information on AuditLogs please see https://docs.microsoft.com/azure/active-directory/reports-monitoring/reference-audit-activities.

**Required Data Connectors**

AzureActiveDirectory

### Suspicious Service Principal creation activity

This alert will detect creation of an SPN, permissions granted, credentials created, activity and deletion of the SPN in a time frame (default 10 minutes)

**Required Data Connectors**

AzureActiveDirectory

### External guest invitation followed by Azure AD PowerShell signin

By default guests have capability to invite more external guest users, guests also can do suspicious Azure AD enumeration. This detection look at guests

users, who have been invited or have invited recently, who also are logging via various PowerShell CLI.

Ref : 'https://danielchronlund.com/2021/11/18/scary-azure-ad-tenant-enumeration-using-regular-b2b-guest-accounts/

**Required Data Connectors**

AzureActiveDirectory

AzureActiveDirectory

### User Accounts - Sign in Failure due to CA Spikes

Identifies spike in failed sign-ins from user accounts due to conditional access policied.

Spike is determined based on Time series anomaly which will look at historical baseline values.

Ref : https://docs.microsoft.com/azure/active-directory/fundamentals/security-operations-user-accounts#monitoring-for-failed-unusual-sign-ins

**Required Data Connectors**

AzureActiveDirectory

AzureActiveDirectory

### User added to Azure Active Directory Privileged Groups

This will alert when a user is added to any of the Privileged Groups.

For further information on AuditLogs please see https://docs.microsoft.com/azure/active-directory/reports-monitoring/reference-audit-activities.

For Administrator role permissions in Azure Active Directory please see https://docs.microsoft.com/azure/active-directory/users-groups-roles/directory-assign-admin-roles

**Required Data Connectors**

AzureActiveDirectory

### User Assigned Privileged Role

Identifies when a new privileged role is assigned to a user. Any account eligible for a role is now being given privileged access. If the assignment is unexpected or into a role that isn't the responsibility of the account holder, investigate.

Ref : https://docs.microsoft.com/azure/active-directory/fundamentals/security-operations-privileged-accounts#things-to-monitor-1

**Required Data Connectors**

AzureActiveDirectory

## Hunting Queries

## Watchlists

## Playbooks

### Block AAD user - Alert

For each account entity included in the alert, this playbook will disable the user in Azure Active Directoy, add a comment to the incident that contains this alert and notify manager if available. Note: This playbook will not disable admin user!

### Block AAD user - Incident

For each account entity included in the incident, this playbook will disable the user in Azure Active Directoy, add a comment to the incident that contains this alert and notify manager if available. Note: This playbook will not disable admin user!

### Prompt User - Alert

This playbook will ask the user if they completed the action from the alert in Microsoft Sentinel. If so, it will close the incident and add a comment. If not, it will post a message to teams for the SOC to investigate and add a comment to the incident.

### Prompt User - Incident

This playbook will ask the user if they completed the action from the Incident in Microsoft Sentinel. If so, it will close the incident and add a comment. If not, it will post a message to teams for the SOC to investigate and add a comment to the incident.

### Reset Azure AD User Password - Alert Trigger

This playbook will reset the user password using Graph API. It will send the password (which is a random guid substring) to the user's manager. The user will have to reset the password upon login.

### Reset Azure AD User Password - Incident Trigger

This playbook will reset the user password using Graph API. It will send the password (which is a random guid substring) to the user's manager. The user will have to reset the password upon login.

## Parsers

# Azure Activity solution for Sentinel

The Azure Activity solution for Microsoft Sentinel enables you to ingest Azure Activity Administrative, Security, Service Health, Alert, Recommendation, Policy, Autoscale and Resource Health logs using Diagnostic Settings into Microsoft Sentinel.

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

## Data Connectors

### Azure Activity

Azure Activity Log is a subscription log that provides insight into subscription-level events that occur in Azure, including events from Azure Resource Manager operational data, service health events, write operations taken on the resources in your subscription, and the status of activities performed in Azure. For more information, see the [Microsoft Sentinel documentation ](https://go.microsoft.com/fwlink/p/?linkid=2219695&wt.mc\_id=sentinel\_dataconnectordocs\_content\_cnl\_csasci).

## Workbooks

### Azure Activity

Gain extensive insight into your organization's Azure Activity by analyzing, and correlating all user operations and events.

You can learn about all user operations, trends, and anomalous changes over time.

This workbook gives you the ability to drill down into caller activities and summarize detected failure and warning events.

**Required Data Types**

AzureActivity

AzureActivity

## Analytic Rules

### Azure Active Directory Hybrid Health AD FS New Server

This detection uses AzureActivity logs (Administrative category) to identify the creation or update of a server instance in an Azure AD Hybrid health AD FS service.

A threat actor can create a new AD Health ADFS service and create a fake server instance to spoof AD FS signing logs. There is no need to compromise an on-prem AD FS server.

This can be done programmatically via HTTP requests to Azure. More information in this blog: https://o365blog.com/post/hybridhealthagent/

**Required Data Connectors**

AzureActivity

### Azure Active Directory Hybrid Health AD FS Service Delete

This detection uses AzureActivity logs (Administrative category) to identify the deletion of an Azure AD Hybrid health AD FS service instance in a tenant.

A threat actor can create a new AD Health ADFS service and create a fake server to spoof AD FS signing logs.

The health AD FS service can then be deleted after it is not longer needed via HTTP requests to Azure.

More information in this blog https://o365blog.com/post/hybridhealthagent/

**Required Data Connectors**

AzureActivity

### Azure Active Directory Hybrid Health AD FS Suspicious Application

This detection uses AzureActivity logs (Administrative category) to a suspicious application adding a server instance to an Azure AD Hybrid health AD FS service or deleting the AD FS service instance.

Usually the Azure AD Connect Health Agent application with ID cf6d7e68-f018-4e0a-a7b3-126e053fb88d and ID cb1056e2-e479-49de-ae31-7812af012ed8 is used to perform those operations.

**Required Data Connectors**

AzureActivity

### Suspicious number of resource creation or deployment activities

Indicates when an anomalous number of VM creations or deployment activities occur in Azure via the AzureActivity log.

The anomaly detection identifies activities that have occurred both since the start of the day 1 day ago and the start of the day 7 days ago.

The start of the day is considered 12am UTC time.

**Required Data Connectors**

AzureActivity

### Creation of expensive computes in Azure

Identifies the creation of large size/expensive VMs (GPU or with large no of virtual CPUs) in Azure.

Adversary may create new or update existing virtual machines sizes to evade defenses

or use it for cryptomining purposes.

For Windows/Linux Vm Sizes - https://docs.microsoft.com/azure/virtual-machines/windows/sizes

Azure VM Naming Conventions - https://docs.microsoft.com/azure/virtual-machines/vm-naming-conventions

**Required Data Connectors**

AzureActivity

### Suspicious granting of permissions to an account

Identifies IPs from which users grant access to other users on azure resources and alerts when a previously unseen source IP address is used.

**Required Data Connectors**

AzureActivity

BehaviorAnalytics

### NRT Azure Active Directory Hybrid Health AD FS New Server

This detection uses AzureActivity logs (Administrative category) to identify the creation or update of a server instance in an Azure AD Hybrid health AD FS service.

A threat actor can create a new AD Health ADFS service and create a fake server instance to spoof AD FS signing logs. There is no need to compromise an on-prem AD FS server.

This can be done programmatically via HTTP requests to Azure. More information in this blog: https://o365blog.com/post/hybridhealthagent/

**Required Data Connectors**

AzureActivity

### NRT Creation of expensive computes in Azure

Identifies the creation of large size/expensive VMs (GPU or with large no of virtual CPUs) in Azure.

Adversary may create new or update existing virtual machines sizes to evade defenses

or use it for cryptomining purposes.

For Windows/Linux Vm Sizes - https://docs.microsoft.com/azure/virtual-machines/windows/sizes

Azure VM Naming Conventions - https://docs.microsoft.com/azure/virtual-machines/vm-naming-conventions

**Required Data Connectors**

AzureActivity

### New CloudShell User

Identifies when a user creates an Azure CloudShell for the first time.

Monitor this activity to ensure only expected user are using CloudShell

**Required Data Connectors**

AzureActivity

### Suspicious Resource deployment

Identifies when a rare Resource and ResourceGroup deployment occurs by a previously unseen Caller.

**Required Data Connectors**

AzureActivity

### Rare subscription-level operations in Azure

This query looks for a few sensitive subscription-level events based on Azure Activity Logs.

For example this monitors for the operation name 'Create or Update Snapshot' which is used for creating backups but could be misused by attackers

to dump hashes or extract sensitive information from the disk.

**Required Data Connectors**

AzureActivity

### Mass Cloud resource deletions Time Series Anomaly

This query generates baseline pattern of cloud resource deletions by an user and generated anomaly

when any unusual spike is detected.

These anomalies from unusual or privileged users could be an indication of cloud infrastructure

take-down by an adversary

**Required Data Connectors**

AzureActivity

## Hunting Queries

### Microsoft Sentinel Analytics Rules Administrative Operations

Azure Activity Hunting Query 1

### Anomalous Azure Operation Hunting Model

Azure Activity Hunting Query 2

### Azure storage key enumeration

Azure Activity Hunting Query 3

### AzureActivity Administration From VPS Providers

Azure Activity Hunting Query 4

### Azure Network Security Group NSG Administrative Operations

Azure Activity Hunting Query 5

### Azure VM Run Command executed from Azure IP address

Azure Activity Hunting Query 6

### Microsoft Sentinel Connectors Administrative Operations

Azure Activity Hunting Query 7

### Microsoft Sentinel Workbooks Administrative Operations

Azure Activity Hunting Query 8

### Azure Virtual Network Subnets Administrative Operations

Azure Activity Hunting Query 9

### Common deployed resources

Azure Activity Hunting Query 10

### Creation of an anomalous number of resources

Azure Activity Hunting Query 11

### Granting permissions to account

Azure Activity Hunting Query 12

### Port opened for an Azure Resource

Azure Activity Hunting Query 13

### Rare Custom Script Extension

Azure Activity Hunting Query 14

## Watchlists

## Playbooks

## Parsers

# Azure Batch Account solution for Sentinel

The Azure Batch Account solution for Microsoft Sentinel enables you to ingest Azure Batch Account diagnostics logs

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

## Data Connectors

### Azure Batch Account

Azure Batch Account is a uniquely identified entity within the Batch service. Most Batch solutions use Azure Storage for storing resource files and output files, so each Batch account is usually associated with a corresponding storage account. This connector lets you stream your Azure Batch account diagnostics logs into Microsoft Sentinel, allowing you to continuously monitor activity. For more information, see the [Microsoft Sentinel documentation](https://go.microsoft.com/fwlink/p/?linkid=2224103&wt.mc\_id=sentinel\_dataconnectordocs\_content\_cnl\_csasci).

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Azure Cognitive Search solution for Sentinel (Preview)

The Azure Cognitive Search solution for Microsoft Sentinel enables you to ingest Azure Cognitive Search diagnostics logs using Diagnostic Settings into Microsoft Sentinel.

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

## Data Connectors

### Azure Cognitive Search

Azure Cognitive Search is a cloud search service that gives developers infrastructure, APIs, and tools for building a rich search experience over private, heterogeneous content in web, mobile, and enterprise applications. This connector lets you stream your Azure Cognitive Search diagnostics logs into Microsoft Sentinel, allowing you to continuously monitor activity.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Azure Data Lake Storage Gen1 solution for Sentinel (Preview)

The Azure Data Lake Storage Gen1 solution for Microsoft Sentinel enables you to ingest Azure Data Lake Storage Gen1 diagnostics logs using Diagnostic Settings into Microsoft Sentinel.

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

## Data Connectors

### Azure Data Lake Storage Gen1

Azure Data Lake Storage Gen1 is an enterprise-wide hyper-scale repository for big data analytic workloads. Azure Data Lake enables you to capture data of any size, type, and ingestion speed in one single place for operational and exploratory analytics. This connector lets you stream your Azure Data Lake Storage Gen1 diagnostics logs into Microsoft Sentinel, allowing you to continuously monitor activity. For more information, see the [Microsoft Sentinel documentation](https://go.microsoft.com/fwlink/p/?linkid=2223812&wt.mc\_id=sentinel\_dataconnectordocs\_content\_cnl\_csasci).

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Azure DDoS Protection solution for Sentinel

The Azure DDoS Protection Solution for Microsoft Sentinel enables you to easily ingest Azure DDoS Protection Standard logs to Microsoft Sentinel.

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

## Data Connectors

### Azure DDoS Protection

Connect to Azure DDoS Protection Standard logs via Public IP Address Diagnostic Logs. In addition to the core DDoS protection in the platform, Azure DDoS Protection Standard provides advanced DDoS mitigation capabilities against network attacks. It's automatically tuned to protect your specific Azure resources. Protection is simple to enable during the creation of new virtual networks. It can also be done after creation and requires no application or resource changes. For more information, see the [Microsoft Sentinel documentation](https://go.microsoft.com/fwlink/p/?linkid=2219760&wt.mc\_id=sentinel\_dataconnectordocs\_content\_cnl\_csasci).

## Workbooks

### Azure DDoS Protection Workbook

This workbook visualizes security-relevant Azure DDoS events across several filterable panels. Offering a summary tab, metrics and a investigate tabs across multiple workspaces.

**Required Data Types**

AzureDiagnostics

DDOS

## Analytic Rules

### DDoS Attack IP Addresses - Percent Threshold

Identifies IP addresses that generate over 5% of traffic during DDoS attack mitigation

**Required Data Connectors**

DDOS

### DDoS Attack IP Addresses - PPS Threshold

Identifies IP addresses that generates maximal traffic rate over 10k PPS during DDoS attack mitigation

**Required Data Connectors**

DDOS

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Azure DevOps Auditing

The Azure DevOps Auditing solution for Microsoft Sentinel allows monitoring Azure DevOps audit events to enable detection of malicious and/or unauthorized access and modification in the repository or pipelines.

**Data Connectors:** 0**, Workbooks:** 0**, Analytic Rules:** 18**, Hunting Queries:** 17**, Watchlists:** 0**, Playbooks:** 0, Parsers: 0

## Data Connectors

## Workbooks

## Analytic Rules

### Azure DevOps Agent Pool Created Then Deleted

As well as adding build agents to an existing pool to execute malicious activity within a pipeline, an attacker could create a complete new agent pool and use this for execution.

Azure DevOps allows for the creation of agent pools with Azure hosted infrastructure or self-hosted infrastructure. Given the additional customizability of self-hosted agents this

detection focuses on the creation of new self-hosted pools. To further reduce false positive rates the detection looks for pools created and deleted relatively quickly (within 7 days by default),

as an attacker is likely to remove a malicious pool once used in order to reduce/remove evidence of their activity.

**Required Data Connectors**

(none listed)

### Azure DevOps Audit Stream Disabled

Azure DevOps allow for audit logs to be streamed to external storage solutions such as SIEM solutions. An attacker looking to hide malicious Azure DevOps activity from defenders may look to disable data streams

before conducting activity and then re-enabling the stream after (so as not to raise data threshold-based alarms). Looking for disabled audit streams can identify this activity, and due to the nature of the action

its unlikely to have a high false positive rate.

**Required Data Connectors**

(none listed)

### Azure DevOps New Extension Added

Extensions add additional features to Azure DevOps. An attacker could use a malicious extension to conduct malicious activity.

This query looks for new extensions that are not from a configurable list of approved publishers.

**Required Data Connectors**

(none listed)

### Azure DevOps PAT used with Browser.

Personal Access Tokens (PATs) are used as an alternate password to authenticate into Azure DevOps. PATs are intended for programmatic access use in code or applications.

This can be prone to attacker theft if not adequately secured. This query looks for the use of a PAT in authentication but from a User Agent indicating a browser.

This should not be normal activity and could be an indicator of an attacker using a stolen PAT.

**Required Data Connectors**

(none listed)

### Azure DevOps Pipeline modified by a new user.

There are several potential pipeline steps that could be modified by an attacker to inject malicious code into the build cycle. A likely attacker path is the modification to an existing pipeline that they have access to.

This detection looks for users modifying a pipeline when they have not previously been observed modifying or creating that pipeline before. This query also joins events with data to Azure AD Identity Protection (AAD IdP)

in order to show if the user conducting the action has any associated AAD IdP alerts. You can also choose to filter this detection to only alert when the user also has AAD IdP alerts associated with them.

**Required Data Connectors**

(none listed)

### Azure DevOps Retention Reduced

AzureDevOps retains items such as run records and produced artifacts for a configurable amount of time. An attacker looking to reduce the footprint left by their malicious activity may look to reduce the retention time for artifacts and runs.

This query will look for where retention has been reduced to the minimum level - 1, or reduced by more than half.

**Required Data Connectors**

(none listed)

### Azure DevOps Variable Secret Not Secured

Credentials used in the build process may be stored as Azure DevOps variables. To secure these variables they should be stored in KeyVault or marked as Secrets.

This detection looks for new variables added with names that suggest they are credentials but where they are not set as Secrets or stored in KeyVault.

**Required Data Connectors**

(none listed)

### Azure DevOps Build Variable Modified by New User.

Variables can be configured and used at any stage of the build process in Azure DevOps to inject values. An attacker with the required permissions could modify

or add to these variables to conduct malicious activity such as changing paths or remote endpoints called during the build. As variables are often changed by users,

just detecting these changes would have a high false positive rate. This detection looks for modifications to variable groups where that user has not been observed

modifying them before.

**Required Data Connectors**

(none listed)

### Azure DevOps Administrator Group Monitoring

This detection monitors for additions to projects or project collection administration groups in an Azure DevOps Organization.

**Required Data Connectors**

(none listed)

### Azure DevOps Pull Request Policy Bypassing - Historic allow list

This detection builds an allow list of historic PR policy bypasses and compares to recent history, flagging pull request bypasses that are not manually in the allow list and not historically included in the allow list.

**Required Data Connectors**

(none listed)

### Azure DevOps Service Connection Addition/Abuse - Historic allow list

This detection builds an allow list of historic service connection use by Builds and Releases and compares to recent history, flagging growth of service connection use which are not manually included in the allow list and

not historically included in the allow list Build/Release runs. This is to determine if someone is hijacking a build/release and adding many service connections in order to abuse or dump credentials from service connections.

**Required Data Connectors**

(none listed)

### Azure DevOps Personal Access Token (PAT) misuse

This Alert detects whenever a PAT is used in ways that PATs are not normally used. May require an allow list and baselining.

Reference - https://docs.microsoft.com/azure/devops/organizations/accounts/use-personal-access-tokens-to-authenticate?view=azure-devops&tabs=preview-page

Use this query for baselining:

AzureDevOpsAuditing

| distinct OperationName

**Required Data Connectors**

(none listed)

### Azure DevOps Pipeline Created and Deleted on the Same Day

An attacker with access to Azure DevOps could create a pipeline to inject artifacts used by other pipelines,

or to create a malicious software build that looks legitimate by using a pipeline that incorporates legitimate elements.

An attacker would also likely want to cover their tracks once conducting such activity. This query looks for Pipelines

created and deleted within the same day, this is unlikely to be legitimate user activity in the majority of cases.

**Required Data Connectors**

(none listed)

### Azure DevOps Service Connection Abuse

Flags builds/releases that use a large number of service connections if they aren't manually in the allow list.

This is to determine if someone is hijacking a build/release and adding many service connections in order to abuse

or dump credentials from service connections.

**Required Data Connectors**

(none listed)

### External Upstream Source Added to Azure DevOps Feed

The detection looks for new external sources added to an Azure DevOps feed. An allow list can be customized to explicitly allow known good sources.

An attacker could look to add a malicious feed in order to inject malicious packages into a build pipeline.

**Required Data Connectors**

(none listed)

### New Agent Added to Pool by New User or Added to a New OS Type.

As seen in attacks such as SolarWinds attackers can look to subvert a build process by controlling build servers. Azure DevOps uses agent pools to execute pipeline tasks.

An attacker could insert compromised agents that they control into the pools in order to execute malicious code. This query looks for users adding agents to pools they have

not added agents to before, or adding agents to a pool of an OS that has not been added to that pool before. This detection has potential for false positives so has a

configurable allow list to allow for certain users to be excluded from the logic.

**Required Data Connectors**

(none listed)

### New PA, PCA, or PCAS added to Azure DevOps

In order for an attacker to be able to conduct many potential attacks against Azure DevOps they will need to gain elevated permissions.

This detection looks for users being granted key administrative permissions. If the principal of least privilege is applied, the number of

users granted these permissions should be small. Note that permissions can also be granted via Azure AD groups and monitoring of these

should also be conducted.

**Required Data Connectors**

(none listed)

### NRT Azure DevOps Audit Stream Disabled

Azure DevOps allow for audit logs to be streamed to external storage solutions such as SIEM solutions. An attacker looking to hide malicious Azure DevOps activity from defenders may look to disable data streams

before conducting activity and then re-enabling the stream after (so as not to raise data threshold-based alarms). Looking for disabled audit streams can identify this activity, and due to the nature of the action

its unlikely to have a high false positive rate.

**Required Data Connectors**

(none listed)

## Hunting Queries

### Azure DevOps- AAD Conditional Access Disabled

AzureDevOpsAuditing Hunting Query 1

### Azure DevOps- Addtional Org Admin added

AzureDevOpsAuditing Hunting Query 2

### Azure DevOps - Build Check Deleted.

AzureDevOpsAuditing Hunting Query 3

### Azure DevOps - Build Deleted After Pipeline Modification

AzureDevOpsAuditing Hunting Query 4

### Azure DevOps - Internal Upstream Package Feed Added.

AzureDevOpsAuditing Hunting Query 5

### Azure DevOps - New Agent Pool Created

AzureDevOpsAuditing Hunting Query 6

### Azure DevOps - New Package Feed Created

AzureDevOpsAuditing Hunting Query 7

### Azure DevOps - New PAT Operation

AzureDevOpsAuditing Hunting Query 8

### Azure DevOps - New Release Approver

AzureDevOpsAuditing Hunting Query 9

### Azure DevOps - New Release Pipeline Created

AzureDevOpsAuditing Hunting Query 10

### Azure DevOps - Variable Created and Deleted

AzureDevOpsAuditing Hunting Query 11

### Azure DevOps Display Name Changes

AzureDevOpsAuditing Hunting Query 12

### Azure DevOps Pull Request Policy Bypassing

AzureDevOpsAuditing Hunting Query 13

### Azure DevOps- Guest users access enabled

AzureDevOpsAuditing Hunting Query 14

### Azure DevOps- Project visibility changed to public

AzureDevOpsAuditing Hunting Query 15

### Azure DevOps- Public project created

AzureDevOpsAuditing Hunting Query 16

### Azure DevOps- Public project enabled by admin

AzureDevOpsAuditing Hunting Query 17

## Watchlists

## Playbooks

## Parsers

# Azure Event Hubs solution for Sentinel (Preview)

The Azure Event Hubs solution for Microsoft Sentinel enables you to ingest Azure Event Hubs diagnostics logs using Diagnostic Settings into Microsoft Sentinel

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

## Data Connectors

### Azure Event Hub

Azure Event Hubs is a big data streaming platform and event ingestion service. It can receive and process millions of events per second. This connector lets you stream your Azure Event Hub diagnostics logs into Microsoft Sentinel, allowing you to continuously monitor activity.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Azure Firewall Solution for Sentinel (Preview)

This solution provides built-in customizable threat detections, workbook, hunting queries and automation for the Azure Firewall service on top of Azure Sentinel.

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 6**, Hunting Queries:** 5**, Watchlists:** 0**, Playbooks:** 3, Parsers: 0

## Data Connectors

### Azure Firewall

Connect to Azure Firewall. Azure Firewall is a managed, cloud-based network security service that protects your Azure Virtual Network resources. It's a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability. For more information, see the [Microsoft Sentinel documentation](https://go.microsoft.com/fwlink/p/?linkid=2220124&wt.mc\_id=sentinel\_dataconnectordocs\_content\_cnl\_csasci).

## Workbooks

### Azure Firewall

Gain insights into Azure Firewall events. You can learn about your application and network rules, see metrics for firewall activities across URLs, ports, and addresses across multiple workspaces.

**Required Data Types**

AzureDiagnostics

AzureFirewall

## Analytic Rules

### Several deny actions registered

Identifies attack pattern when attacker tries to move, or scan, from resource to resource on the network and creates an incident when a source has more than 1 registered deny action in Azure Firewall.

**Required Data Connectors**

AzureFirewall

### Port Sweep

Identifies a source IP scanning same open ports on the Azure Firewall IPs. This can indicate malicious scanning of port by an attacker, trying to reveal IPs with specific ports open in the organization. The ports can be compromised by attackers for initial access, most often by exploiting vulnerability.

Configurable Parameters:

- Port sweep time - the time range to look for multiple hosts scanned. Default is set to 30 seconds.

- Minimum different hosts threshold - alert only if more than this number of hosts scanned. Default is set to 200.

**Required Data Connectors**

AzureFirewall

### Port Scan

Identifies a source IP scanning multiple open ports on Azure Firewall. This can indicate malicious scanning of ports by an attacker, trying to reveal open ports in the organization that can be compromised for initial access.

Configurable Parameters:

- Port scan time - the time range to look for multiple ports scanned. Default is set to 30 seconds.

- Minimum different ports threshold - alert only if more than this number of ports scanned. Default is set to 100.

**Required Data Connectors**

AzureFirewall

### Multiple Sources Affected by the Same TI Destination

Identifies multiple machines trying to reach out to the same destination blocked by TI in Azure Firewall. This can indicate attack on the organization by the same attack group.

Configurable Parameters:

- Minimum affected threshold - alert only if more than this number of hosts affected. Default is set to 5.

**Required Data Connectors**

AzureFirewall

### Abnormal Port to Protocol

Identifies communication for well known protocol over a non-standard port based on learning period activity. This can indicate malicious communication (C2) or exfiltration by attackers trying to communicate over known ports (22:SSH, 80:HTTP) but dont use the known protocol headers to match the port number.

Configurable Parameters:

- Learning period time - learning period for protocol learning in days. Default is set to 7.

**Required Data Connectors**

AzureFirewall

### Abnormal Deny Rate for Source IP

Identifies abnormal deny rate for specific source IP to destination IP based on the normal average and standard deviation learned during a configured period. This can indicate potential exfiltration, initial access or C2, where attacker tries to exploit the same vulnerability on machines in the organization, but is being blocked by firewall rules.

Configurable Parameters:

- Minimum of stds threshold - the number of stds to use in the threshold calculation. Default is set to 3.

- Learning period time - learning period for threshold calculation in days. Default is set to 5.

- Bin time - learning buckets time in hours. Default is set to 1 hour.

- Minimum threshold - minimum threshold for alert. Default is set to 5.

- Minimum bucket threshold - minimum learning buckets threshold for alert. Default is set to 5.

**Required Data Connectors**

AzureFirewall

## Hunting Queries

### First Time Source IP to Destination Using Port

Azure Firewall Hunting Query 1

### First Time Source IP to Destination

Azure Firewall Hunting Query 2

### Source IP Abnormally Connects to Multiple Destinations

Azure Firewall Hunting Query 3

### Uncommon Port for Organization

Azure Firewall Hunting Query 4

### Uncommon Port to IP

Azure Firewall Hunting Query 5

## Watchlists

## Playbooks

### Block IP - Azure Firewall IP groups

This playbook allows blocking/allowing IPs in Azure Firewall. It allows to make changes on IP groups, which are attached to rules, instead of make direct changes on Azure Firewall. It also allows using the same IP group for multiple firewalls. [Learn more about IP Groups in Azure Firewall](https://docs.microsoft.com/azure/firewall/ip-groups)

### Azure Firewall - Add IP Address to Threat Intel Allow list

This playbook allows the SOC to automatically response to Microsoft Sentinel incidents which includes IPs, by adding the IPs to the TI Allow list in Azure Firewall Policy.

### BlockIP-Azure Firewall New Rule

This playbook uses the Azure Firewall connector to add IP Address to the Deny Network Rules collection based on the Microsoft Sentinel Incident

## Parsers

# Azure Information Protection solution for Sentinel

The Azure Information Protection Solution for Microsoft Sentinel integrates Microsoft Azure Information Protection logs to view dashboards, create custom alerts, and improve investigation.

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

## Data Connectors

### Azure Information Protection

\*\*Azure Information Protection\*\* helps protect your data whether it’s stored in the cloud or in on-premises infrastructures. Control and help secure email, documents, and sensitive data that you share outside your company. From easy classification to embedded labels and permissions, enhance data protection at all times with Azure Information Protection. With Azure Information Protection you can:

- Classify your data based on sensitivity​.

- Protect your data at all times.

- Add visibility and control by powerful logging and reporting​.

- Collaborate more securely with others.

Integrate Microsoft Azure Information Protection logs with Sentinel to view dashboards, create custom alerts, and improve investigation.

[Get started with Azure Information Protection >](https://aka.ms/asi-aip-get-started)

## Workbooks

### Azure Information Protection - Usage Report

The Azure Information Protection Usage report workbook provides information on the volume of labeled and protected documents and emails over time, label distribution of files by label type, along with where the label was applied.

**Required Data Types**

InformationProtectionLogs\_CL

AzureInformationProtection

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Azure Key Vault solution for Sentinel

Azure Key Vault Solution for Microsoft Sentinel enables you to stream Azure Key Vault diagnostics logs into Microsoft Sentinel, allowing you to continuously monitor activity in all your instances.

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

## Data Connectors

### Azure Key Vault

Azure Key Vault is a cloud service for securely storing and accessing secrets. A secret is anything that you want to tightly control access to, such as API keys, passwords, certificates, or cryptographic keys. This connector lets you stream your Azure Key Vault diagnostics logs into Microsoft Sentinel, allowing you to continuously monitor activity in all your instances. For more information, see the [Microsoft Sentinel documentation](https://go.microsoft.com/fwlink/p/?linkid=2220125&wt.mc\_id=sentinel\_dataconnectordocs\_content\_cnl\_csasci).

## Workbooks

## Analytic Rules

### Sensitive Azure Key Vault operations

Identifies when sensitive Azure Key Vault operations are used. This includes: VaultDelete, KeyDelete, SecretDelete, SecretPurge, KeyPurge, SecretBackup, KeyBackup.

Any Backup operations should match with expected scheduled backup activity.

**Required Data Connectors**

AzureKeyVault

### Mass secret retrieval from Azure Key Vault

Identifies mass secret retrieval from Azure Key Vault observed by a single user.

Mass secret retrival crossing a certain threshold is an indication of credential dump operations or mis-configured applications.

You can tweak the EventCountThreshold based on average count seen in your environment

and also filter any known sources (IP/Account) and useragent combinations based on historical analysis to further reduce noise

**Required Data Connectors**

AzureKeyVault

### Azure Key Vault access TimeSeries anomaly

Indentifies a sudden increase in count of Azure Key Vault secret or vault access operations by CallerIPAddress. The query leverages a built-in KQL anomaly detection algorithm

to find large deviations from baseline Azure Key Vault access patterns. Any sudden increase in the count of Azure Key Vault accesses can be an

indication of adversary dumping credentials via automated methods. If you are seeing any noise, try filtering known source(IP/Account) and user-agent combinations.

TimeSeries Reference Blog: https://techcommunity.microsoft.com/t5/azure-sentinel/looking-for-unknown-anomalies-what-is-normal-time-series/ba-p/555052

**Required Data Connectors**

AzureKeyVault

### NRT Sensitive Azure Key Vault operations

Identifies when sensitive Azure Key Vault operations are used. This includes: VaultDelete, KeyDelete, SecretDelete, SecretPurge, KeyPurge, SecretBackup, KeyBackup.

Any Backup operations should match with expected scheduled backup activity.

**Required Data Connectors**

AzureKeyVault

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Azure Kubernetes Service (AKS) solution for Sentinel

The Azure Kubernetes Services (AKS) solution allows you to ingest AKS activity logs using Diagnostic Setting into Microsoft Sentinel.

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

## Data Connectors

### Azure Kubernetes Service (AKS)

Azure Kubernetes Service (AKS) is an open-source, fully-managed container orchestration service that allows you to deploy, scale, and manage Docker containers and container-based applications in a cluster environment. This connector lets you stream your Azure Kubernetes Service (AKS) diagnostics logs into Microsoft Sentinel, allowing you to continuously monitor activity in all your instances. For more information, see the [Microsoft Sentinel documentation](https://go.microsoft.com/fwlink/p/?linkid=2219762&wt.mc\_id=sentinel\_dataconnectordocs\_content\_cnl\_csasci).

## Workbooks

### Azure Kubernetes Service (AKS) Security

See insights about the security of your AKS clusters. The workbook helps to identify sensitive operations in the clusters and get insights based on Azure Defender alerts.

**Required Data Types**

SecurityAlert

AzureDiagnostics

AzureSecurityCenter

AzureKubernetes

## Analytic Rules

## Hunting Queries

### Determine users with cluster admin role

Azure kubernetes Service Hunting Query 1

### Azure RBAC AKS created role details

Azure kubernetes Service Hunting Query 2

## Watchlists

## Playbooks

## Parsers

# Azure Logic Apps solution for Sentinel

The Azure Logic Apps solution for Microsoft Sentinel enables you to ingest Azure Logic App diagnostics logs using Diagnostic Settings into Microsoft Sentinel.

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

## Data Connectors

### Azure Logic Apps

Azure Logic Apps is a cloud-based platform for creating and running automated workflows that integrate your apps, data, services, and systems. This connector lets you stream your Azure Logic Apps diagnostics logs into Microsoft Sentinel, allowing you to continuously monitor activity.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Azure Network Security Groups solution for Sentinel

The Azure Network Security Group solution enables you to stream and ingest diagnostic logs from your Azure NSG instances for Security Monitoring in to Microsoft Sentinel using Resource Diagnostic settings.

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

## Data Connectors

### Network Security Groups

Azure network security groups (NSG) allow you to filter network traffic to and from Azure resources in an Azure virtual network. A network security group includes rules that allow or deny traffic to a virtual network subnet, network interface, or both.

When you enable logging for an NSG, you can gather the following types of resource log information:

- \*\*Event:\*\* Entries are logged for which NSG rules are applied to VMs, based on MAC address.

- \*\*Rule counter:\*\* Contains entries for how many times each NSG rule is applied to deny or allow traffic. The status for these rules is collected every 300 seconds.

This connector lets you stream your NSG diagnostics logs into Microsoft Sentinel, allowing you to continuously monitor activity in all your instances. For more information, see the [Microsoft Sentinel documentation](https://go.microsoft.com/fwlink/p/?linkid=2223718&wt.mc\_id=sentinel\_dataconnectordocs\_content\_cnl\_csasci).

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Azure Security Benchmark

The Azure Security Benchmark v3 Solution is designed to enable Cloud Architects, Security Engineers, and Governance Risk Compliance Professionals to gain situational awareness for cloud security posture and hardening.

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

## Data Connectors

## Workbooks

### Azure Security Benchmark

Azure Security Benchmark v3 Workbook provides a mechanism for viewing log queries, azure resource graph, and policies aligned to ASB controls across Microsoft security offerings, Azure, Microsoft 365, 3rd Party, On-Premises, and Multi-cloud workloads. This workbook enables Security Architects, Engineers, SecOps Analysts, Managers, and IT Pros to gain situational awareness visibility for the security posture of cloud workloads. There are also recommendations for selecting, designing, deploying, and configuring Microsoft offerings for alignment with respective ASB requirements and practices.

**Required Data Types**

## Analytic Rules

### Azure Security Benchmark Posture Changed

This alert is designed to monitor Azure policies aligned with the Azure Security Benchmark Regulatory Compliance initiative. The alert triggers when policy compliance falls below 70% within a 1 week time-frame.

**Required Data Connectors**

(none listed)

## Hunting Queries

## Watchlists

## Playbooks

### Notify-GovernanceComplianceTeam

This Security Orchestration, Automation, & Response (SOAR) capability is designed for configuration with the solution's analytics rules. When analytics rules trigger this automation notifies the governance compliance team of respective details via Teams chat and exchange email. This automation reduces requirements to manually monitor the workbook or analytics rules while increasing response times.

### Create-AzureDevOpsTask

This playbook will create the Azure DevOps task filled with the Microsoft Sentinel incident details.

### Create Jira Issue

This playbook will open a Jira Issue when a new incident is opened in Microsoft Sentinel.

## Parsers

# Azure Sentinel for WatchGuard Firebox

Microsoft Azure Sentinel is a scalable, cloud-native security information event management (SIEM) and security orchestration automated response (SOAR) solution on WatchGuard Firebox Cloud.

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

## Data Connectors

### WatchGuard Firebox

WatchGuard Firebox （https://www.watchguard.com/wgrd-products/firewall-appliances and https://www.watchguard.com/wgrd-products/cloud-and-virtual-firewalls） is security products/firewall-appliances. Watchguard Firebox will send syslog to Watchguard Firebox collector agent.The agent then sends the message to the workspace.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### WatchGuardFirebox

Category: Samples

Function Alias: WatchGuardFirebox

# Azure Service Bus solution for Sentinel (Preview)

The Azure Service Bus solution for Microsoft Sentinel enables you to ingest Azure Service Bus diagnostics logs using Diagnostic Settings into Microsoft Sentinel.

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

## Data Connectors

### Azure Service Bus

Azure Service Bus is a fully managed enterprise message broker with message queues and publish-subscribe topics (in a namespace). This connector lets you stream your Azure Service Bus diagnostics logs into Microsoft Sentinel, allowing you to continuously monitor activity.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Azure SQL Database solution for sentinel (Preview)

This solution provides built-in customizable threat detection for Azure SQL PaaS services on top of Microsoft Sentinel.

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 10**, Hunting Queries:** 8**, Watchlists:** 0**, Playbooks:** 0, Parsers: 0

## Data Connectors

### Azure SQL Databases

Azure SQL is a fully managed, Platform-as-a-Service (PaaS) database engine that handles most database management functions, such as upgrading, patching, backups, and monitoring, without necessitating user involvement. This connector lets you stream your Azure SQL databases audit and diagnostic logs into Microsoft Sentinel, allowing you to continuously monitor activity in all your instances.

## Workbooks

### Azure SQL Database Workbook

Sets the time window in days to search around the alert

**Required Data Types**

AzureDiagnostics

SecurityAlert

SecurityIncident

AzureSql

## Analytic Rules

### Credential errors stateful anomaly on database

This query batches of distinct SQL queries that failed with error codes that might indicate malicious attempts to gain illegitimate access to the data. When Brute Force attacks are attempted, majority of logins will use wrong credentials, thus will fail with error code 18456. Thus, if we see a large number of logins with such error codes, this could indicate Brute Force attack.

**Required Data Connectors**

AzureSql

### Firewall errors stateful anomaly on database

This query batches of distinct SQL queries that failed with error codes that might indicate malicious attempts to gain illegitimate access to the data. When attacker attempts to scan or gain access to server protected by firewall, he will be blocked by firewall and fail with error code 40615. Thus, if we see a large number of logins with such error codes, this could indicate attempts to gain access.

**Required Data Connectors**

AzureSql

### Syntax errors stateful anomaly on database

This query batches of distinct SQL queries that failed with error codes that might indicate malicious attempts to gain illegitimate access to the data. When blind type of attacks are performed (such as SQL injection of fuzzying), the attempted queries are often malformed and fail on wrong syntax (error 102) or wrong escaping (error 105). Thus, if a large number of different queries fail on such errors in a short amount of time, this might indicate attempted attack.

**Required Data Connectors**

AzureSql

### Drop attempts stateful anomaly on database

This query detects batches of distinct SQL queries that execute (or attempt to) commands that could indicate potential security issues - such as attempts to drop tables or databases (e.g. for data vandalism).

**Required Data Connectors**

AzureSql

### Execution attempts stateful anomaly on database

This query detects batches of distinct SQL queries that execute (or attempt to) commands that could indicate potential security issues - such as attempts to execute shell commands (e.g. for running illegitimate code).

**Required Data Connectors**

AzureSql

### Firewall rule manipulation attempts stateful anomaly on database

This query detects batches of distinct SQL queries that execute (or attempt to) commands that could indicate potential security issues - such as attempts to manipulate firewall rules (e.g. for allowing malicious access to the database).

**Required Data Connectors**

AzureSql

### OLE object manipulation attempts stateful anomaly on database

This query detects batches of distinct SQL queries that execute (or attempt to) commands that could indicate potential security issues - such as attempts to manipulate OLE objects (e.g. for running malicious commands).

**Required Data Connectors**

AzureSql

### Outgoing connection attempts stateful anomaly on database

This query detects batches of distinct SQL queries that execute (or attempt to) commands that could indicate potential security issues - such as attempts to access external sites or resources (e.g. for downloading malicious content).

**Required Data Connectors**

AzureSql

### Affected rows stateful anomaly on database

Goal: To detect anomalous data change/deletion. This query detects SQL queries that changed/deleted a large number of rows, which is significantly higher than normal for this database. The detection is calculated inside recent time window (defined by 'detectionWindow' parameter), and the anomaly is calculated based on previous training window

(defined by 'trainingWindow' parameter). The user can set the minimal threshold for anomaly by changing the threshold parameters volThresholdZ and volThresholdQ (higher threshold will detect only more severe anomalies).

**Required Data Connectors**

AzureSql

### Response rows stateful anomaly on database

Goal: To detect anomalous data exfiltration. This query detects SQL queries that accessed a large number of rows, which is significantly higher than normal for this database.

The calculation is made inside recent time window (defined by 'detectionWindow' parameter), and the anomaly is calculated based on previous training window

(defined by 'trainingWindow' parameter). The user can set the minimal threshold for anomaly by changing the threshold parameters volThresholdZ and volThresholdQ (higher thresholds will detect only more severe anomalies).

**Required Data Connectors**

AzureSql

## Hunting Queries

### Anomalous Query Execution Time

Azure SQL Database solution for sentinel Hunting Query 1

### Boolean Blind SQL Injection

Azure SQL Database solution for sentinel Hunting Query 2

### Anomalous Query Execution Time

Azure SQL Database solution for sentinel Hunting Query 3

### Prevalence Based SQL Query Size Anomaly

Azure SQL Database solution for sentinel Hunting Query 4

### Suspicious SQL Stored Procedures

Azure SQL Database solution for sentinel Hunting Query 5

### Time Based SQL Query Size Anomaly

Azure SQL Database solution for sentinel Hunting Query 6

### Affected rows stateful anomaly on database - hunting query

Azure SQL Database solution for sentinel Hunting Query 7

### Response rows stateful anomaly on database - hunting query

Azure SQL Database solution for sentinel Hunting Query 8

## Watchlists

## Playbooks

## Parsers

# Azure Storage solution for Sentinel

The Azure Storage account Solution for Microsoft Sentinel enables you to stream Azure Storage accounts diagnostics logs into your Microsoft Sentinel workspace, allowing you to continuously monitor activity in all your instances.

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

## Data Connectors

### Azure Storage Account

Azure Storage account is a cloud solution for modern data storage scenarios. It contains all your data objects: blobs, files, queues, tables, and disks. This connector lets you stream Azure Storage accounts diagnostics logs into your Microsoft Sentinel workspace, allowing you to continuously monitor activity in all your instances, and detect malicious activity in your organization. For more information, see the [Microsoft Sentinel documentation](https://go.microsoft.com/fwlink/p/?linkid=2220068&wt.mc\_id=sentinel\_dataconnectordocs\_content\_cnl\_csasci).

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Azure Stream Analytics solution for Sentinel (Preview)

The Azure Stream Analytics solution for Microsoft Sentinel enables you to ingest Azure Stream Analytics diagnostics logs using Diagnostic Settings into Microsoft Sentinel.

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

## Data Connectors

### Azure Stream Analytics

Azure Stream Analytics is a real-time analytics and complex event-processing engine that is designed to analyze and process high volumes of fast streaming data from multiple sources simultaneously. This connector lets you stream your Azure Stream Analytics hub diagnostics logs into Microsoft Sentinel, allowing you to continuously monitor activity.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Azure Web Application Firewall solution for Sentinel

The Azure Web Application Firewall (WAF) solution for Microsoft Sentinel allows you to ingest Diagnostic Metrics from Application Gateway, Front Door and CDN into Microsoft Sentinel.

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

## Data Connectors

### Azure Web Application Firewall (WAF)

Connect to the Azure Web Application Firewall (WAF) for Application Gateway, Front Door, or CDN. This WAF protects your applications from common web vulnerabilities such as SQL injection and cross-site scripting, and lets you customize rules to reduce false positives. Follow these instructions to stream your Microsoft Web application firewall logs into Microsoft Sentinel. For more information, see the [Microsoft Sentinel documentation](https://go.microsoft.com/fwlink/p/?linkid=2223546&wt.mc\_id=sentinel\_dataconnectordocs\_content\_cnl\_csasci).

## Workbooks

### Microsoft Web Application Firewall (WAF) - firewall events

Gain insights into your organization's Azure web application firewall (WAF). You will get visibility in to your application gateway firewall. You can view anomalies and trends across all firewall event triggers, attack events, blocked URL addresses and more.

**Required Data Types**

AzureDiagnostics

WAF

### Microsoft Web Application Firewall (WAF) - gateway access events

Gain insights into your organization's Azure web application firewall (WAF). You will get visibility in to your application gateway access events. You can view anomalies and trends across received and sent data, client IP addresses, URL addresses and more, and drill down into details.

**Required Data Types**

AzureDiagnostics

WAF

### Microsoft Web Application Firewall (WAF) - overview

Gain insights into your organization's Azure web application firewall (WAF). You will get a general overview of your application gateway firewall and application gateway access events.

**Required Data Types**

AzureDiagnostics

WAF

### Microsoft Web Application Firewall (WAF) - Azure WAF

Gain insights into your organization's Azure web application firewall (WAF) across various services such as Azure Front Door Service and Application Gateway. You can view event triggers, full messages, attacks over time, among other data. Several aspects of the workbook are interactable to allow users to further understand their data

**Required Data Types**

AzureDiagnostics

WAF

## Analytic Rules

### A potentially malicious web request was executed against a web server

Detects unobstructed Web Application Firewall (WAF) activity in sessions where the WAF blocked incoming requests by computing the

ratio between blocked requests and unobstructed WAF requests in these sessions (BlockvsSuccessRatio metric). A high ratio value for

a given client IP and hostname calls for further investigation of the WAF data in that session, due to the significantly high number

of blocked requests and a few unobstructed logs which may be malicious but have passed undetected through the WAF. The successCode

variable defines what the detection thinks is a successful status code, and should be altered to fit the environment.

**Required Data Connectors**

WAF

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Barracuda WAF Sentinel Solution

Barracuda WAF solution package for Azure Sentinel offers threat intelligence insights for the attacks targeted at the web application. These insights can be used to create incident response rules and follow up action to avoid such attempts.

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

## Data Connectors

### Barracuda Web Application Firewall

The Barracuda Web Application Firewall (WAF) connector allows you to easily connect your Barracuda logs with Microsoft Sentinel, to view dashboards, create custom alerts, and improve investigation. This gives you more insight into your organization’s network and improves your security operation capabilities.

[For more information >​](https://aka.ms/CEF-Barracuda)

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# BETTER Mobile Threat Defense (MTD)

BETTER Mobile delivers powerful mobile security protection on Microsoft Azure platform

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

## Data Connectors

### BETTER Mobile Threat Defense (MTD)

The BETTER MTD Connector allows Enterprises to connect their Better MTD instances with Microsoft Sentinel, to view their data in Dashboards, create custom alerts, use it to trigger playbooks and expands threat hunting capabilities. This gives users more insight into their organization's mobile devices and ability to quickly analyze current mobile security posture which improves their overall SecOps capabilities.

## Workbooks

### BETTER Mobile Threat Defense (MTD)

Workbook using the BETTER Mobile Threat Defense (MTD) connector, to give insights into your mobile devices, installed application and overall device security posture.

**Required Data Types**

BetterMTDDeviceLog\_CL

BetterMTDAppLog\_CL

BetterMTDIncidentLog\_CL

BetterMTDNetflowLog\_CL

BetterMTD

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Bitglass Solution

Bitglass delivers data and threat protection for any interaction, on any device, anywhere. Operating at cloud scale across global network, Bitglass delivers unrivaled performance and uptime to ensure secure business continuity for largest organizations.

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 10**, Hunting Queries:** 10**, Watchlists:** 0**, Playbooks:** 0, Parsers: 1

## Data Connectors

### Bitglass (using Azure Function)

The [Bitglass](https://www.bitglass.com/) data connector provides the capability to retrieve security event logs of the Bitglass services and more events into Microsoft Sentinel through the REST API. The connector provides ability to get events which helps to examine potential security risks, analyze your team's use of collaboration, diagnose configuration problems and more.

## Workbooks

### Bitglass

Sets the time name for analysis

**Required Data Types**

BitglassLogs\_CL

Bitglass

## Analytic Rules

### Bitglass - Multiple files shared with external entity

Detects when multiple files shared with external entity.

**Required Data Connectors**

Bitglass

### Bitglass - Impossible travel distance

Detects logins from different geo locations.

**Required Data Connectors**

Bitglass

### Bitglass - Multiple failed logins

Detects multiple failed logins.

**Required Data Connectors**

Bitglass

### Bitglass - New admin user

Detects new admin user.

**Required Data Connectors**

Bitglass

### Bitglass - Login from new device

Detects when a user logins from new device.

**Required Data Connectors**

Bitglass

### Bitglass - New risky user

Detects new risky user.

**Required Data Connectors**

Bitglass

### Bitglass - The SmartEdge endpoint agent was uninstalled

Detects when SmartEdge endpoint agent was uninstalled.

**Required Data Connectors**

Bitglass

### Bitglass - Suspicious file uploads

Detects suspicious file upload activity.

**Required Data Connectors**

Bitglass

### Bitglass - User login from new geo location

Detects user login from new geo location.

**Required Data Connectors**

Bitglass

### Bitglass - User Agent string has changed for user

Detects when User Agent string has changed for user.

**Required Data Connectors**

Bitglass

## Hunting Queries

### Bitglass - Applications used

Bitglass Hunting Query 1

### Bitglass - Insecure web protocol

Bitglass Hunting Query 2

### Bitglass - Login failures

Bitglass Hunting Query 3

### Bitglass - New applications

Bitglass Hunting Query 4

### Bitglass - New users

Bitglass Hunting Query 5

### Bitglass - Privileged login failures

Bitglass Hunting Query 6

### Bitglass - Risky users

Bitglass Hunting Query 7

### Bitglass - Risky users

Bitglass Hunting Query 8

### Bitglass - Uncategorized resources

Bitglass Hunting Query 9

### Bitglass - User devices

Bitglass Hunting Query 10

## Watchlists

## Playbooks

## Parsers

### Bitglass Data Parser

Category: Samples

Function Alias: Bitglass

# Blackberry CylancePROTECT

The Blackberry CylancePROTECT solution allows you to easily connect your CylancePROTECT logs with Microsoft Sentinel.

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

## Data Connectors

### Blackberry CylancePROTECT

The [Blackberry CylancePROTECT](https://www.blackberry.com/us/en/products/blackberry-protect) connector allows you to easily connect your CylancePROTECT logs with Microsoft Sentinel. This gives you more insight into your organization's network and improves your security operation capabilities.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### CylancePROTECT

Category: Samples

Function Alias: CylancePROTECT

# Box Solution

Box is a single, secure, easy-to-use platform built for the entire content lifecycle, from file creation and sharing, to co-editing, signature, classification, and retention.

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 10**, Hunting Queries:** 10**, Watchlists:** 0**, Playbooks:** 0, Parsers: 1

## Data Connectors

### Box (using Azure Function)

The Box data connector provides the capability to ingest [Box enterprise's events](https://developer.box.com/guides/events/#admin-events) into Microsoft Sentinel using the Box REST API. Refer to [Box documentation](https://developer.box.com/guides/events/enterprise-events/for-enterprise/) for more information.

## Workbooks

### Box

Sets the time name for analysis

**Required Data Types**

BoxEvents\_CL

BoxDataConnector

## Analytic Rules

### Box - Abmormal user activity

Detects spikes (deviations from avarage) in user activity.

**Required Data Connectors**

BoxDataConnector

### Box - Executable file in folder

Detects executable files in folders.

**Required Data Connectors**

BoxDataConnector

### Box - Forbidden file type downloaded

Detects when new user downloads forbidden file types.

**Required Data Connectors**

BoxDataConnector

### Box - Inactive user login

Detects user login after long inactivity period.

**Required Data Connectors**

BoxDataConnector

### Box - Item shared to external entity

Detects when an item was shared to external entity.

**Required Data Connectors**

BoxDataConnector

### Box - Many items deleted by user

Detects when a user deletes many items in short period of time.

**Required Data Connectors**

BoxDataConnector

### Box - New external user

Detects when new user created with SourceLogin containing non-corporate domain.

**Required Data Connectors**

BoxDataConnector

### Box - File containing sensitive data

Detects files which potentialy may contain sensitive data such as passwords, authentication tokens, secret keys.

**Required Data Connectors**

BoxDataConnector

### Box - User logged in as admin

Detects when user logged in as admin.

**Required Data Connectors**

BoxDataConnector

### Box - User role changed to owner

Detects when user collaboration role is changed to owner.

**Required Data Connectors**

BoxDataConnector

## Hunting Queries

### Box - IP list for admin users

Box Hunting Query 1

### Box - Deleted users

Box Hunting Query 2

### Box - Inactive admin users

Box Hunting Query 3

### Box - Inactive users

Box Hunting Query 4

### Box - New users

Box Hunting Query 5

### Box - Suspicious or sensitive files

Box Hunting Query 6

### Box - Downloaded data volume per user

Box Hunting Query 7

### Box - New users

Box Hunting Query 8

### Box - Uploaded data volume per user

Box Hunting Query 9

### Box - Users with owner permissions

Box Hunting Query 10

## Watchlists

## Playbooks

## Parsers

### Box Data Parser

Category: Samples

Function Alias: BoxEvents

# Broadcom SymantecDLP

The Broadcom Symantec Data Loss Prevention (DLP) connector allows you to easily connect your Symantec DLP with Microsoft Sentinel.

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

## Data Connectors

### Braodcom Symantec DLP

The [Broadcom Symantec Data Loss Prevention (DLP)](https://www.broadcom.com/products/cyber-security/information-protection/data-loss-prevention) connector allows you to easily connect your Symantec DLP with Azure Sentinel, to create custom dashboards, alerts, and improve investigation. This gives you more insight into your organization’s information, where it travels, and improves your security operation capabilities.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### SymantecDLP

Category: Samples

Function Alias: SymantecDLP

# Check Point for Microsoft Sentinel solutions

Check Point's Logic Apps Connector and Sentinel Playbook templates

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

## Data Connectors

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

### checkpoint-add-host-to-group

This playbook will create Check Point objects and add to block group

## Parsers

# CheckPhish by Bolster

The Bolster’s phishing and scam protection service provides accurate detection and takedown of phishing and scam sites.

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

## Data Connectors

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

### CheckPhish - Get URL reputation

This playbooks will be used to submit URL to CheckPhish and gets the repution of URL (Scan result)

## Parsers

# Cisco ACI Solution

Cisco Application Centric Infrastructure built on top of the industry-leading Cisco Nexus 9000 platform, is part of intent-based networking framework to enable agility and resiliency in the data center.

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

## Data Connectors

### Cisco Application Centric Infrastructure

[Cisco Application Centric Infrastructure (ACI)](https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/solution-overview-c22-741487.html) data connector provides the capability to ingest [Cisco ACI logs](https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/all/syslog/guide/b\_ACI\_System\_Messages\_Guide/m-aci-system-messages-reference.html) into Microsoft Sentinel.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### CiscoACI Data Parser

Category: Samples

Function Alias: CiscoACIEvent

# Cisco ASA Solution

The Cisco ASA Family of security devices protects corporate networks and data centers of all sizes. It provides users with highly secure access to data and network resources - anytime, anywhere, using any device.

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

## Data Connectors

### Cisco ASA

The Cisco ASA firewall connector allows you to easily connect your Cisco ASA logs with Microsoft Sentinel, to view dashboards, create custom alerts, and improve investigation. This gives you more insight into your organization's network and improves your security operation capabilities.

## Workbooks

### Cisco - ASA

Gain insights into your Cisco ASA firewalls by analyzing traffic, events, and firewall operations.

This workbook analyzes Cisco ASA threat events and identifies suspicious ports, users, protocols and IP addresses.

You can learn about trends across user and data traffic directions, and drill down into the Cisco filter results.

Easily detect attacks on your organization by monitoring management operations, such as configuration and logins.

**Required Data Types**

CommonSecurityLog

CiscoASA

## Analytic Rules

### Cisco ASA - threat detection message fired

Identifies when the Cisco ASA Threat Detection engine fired an alert based on malicious activity occurring on the network inicated by DeviceEventClassID 733101-733105

Resources: https://www.cisco.com/c/en/us/td/docs/security/asa/syslog/b\_syslog/syslogs9.html

Details on how to further troubleshoot/investigate: https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/113685-asa-threat-detection.html

**Required Data Connectors**

CiscoASA

### Cisco ASA - average attack detection rate increase

This will help you determine if Cisco ASA devices are under heavier attack than normal over the last hour versus the previous 6 hours based on DeviceEventClassID 733100

References: https://www.cisco.com/c/en/us/td/docs/security/asa/syslog/b\_syslog/syslogs9.html

Details on how to further troubleshoot/investigate: https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/113685-asa-threat-detection.html

**Required Data Connectors**

CiscoASA

## Hunting Queries

## Watchlists

## Playbooks

### Block IP - Cisco ASA

This playbook allows blocking/allowing of IPs in Cisco ASA, using a Network Object Group. The Network Object Group itself should be part of an Access Control Entry.

### Cisco ASA - Create or remove access rules on an interface for IP Addresses

This playbook allows blocking/unblocking of IPs in Cisco ASA, using \*\*Access Control Entries\*\* which will be created in an access control list.

### Cisco ASA - Create or Inbound Access Rule On Interface

This playbook allows blocking/unblocking of IPs in Cisco ASA, using \*\*Access Rules\*\* which will be created on an interface.

## Parsers

# Cisco Duo Security

The Cisco Duo Security solution allows you to ingest authentication logs, administrator logs, telephony logs, offline enrolment logs and Trust Monitor events into Microsoft Sentinel using the Cisco Duo Admin API.

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 10**, Hunting Queries:** 10**, Watchlists:** 0**, Playbooks:** 0, Parsers: 1

## Data Connectors

### Cisco Duo Security (using Azure Function)

The Cisco Duo Security data connector provides the capability to ingest [authentication logs](https://duo.com/docs/adminapi#authentication-logs), [administrator logs](https://duo.com/docs/adminapi#administrator-logs), [telephony logs](https://duo.com/docs/adminapi#telephony-logs), [offline enrollment logs](https://duo.com/docs/adminapi#offline-enrollment-logs) and [Trust Monitor events](https://duo.com/docs/adminapi#trust-monitor) into Microsoft Sentinel using the Cisco Duo Admin API. Refer to [API documentation](https://duo.com/docs/adminapi) for more information.

## Workbooks

### CiscoDuoSecurity

Sets the time name for analysis

**Required Data Types**

## Analytic Rules

### Cisco Duo - AD sync failed

Detects when AD syncronization failed.

**Required Data Connectors**

CiscoDuoSecurity

### Cisco Duo - Admin user deleted

Detects when admin user is deleted.

**Required Data Connectors**

CiscoDuoSecurity

### Cisco Duo - Multiple admin 2FA failures

Detects when multiple admin 2FA failures occurs.

**Required Data Connectors**

CiscoDuoSecurity

### Cisco Duo - Admin password reset

Detects when admin's password was reset.

**Required Data Connectors**

CiscoDuoSecurity

### Cisco Duo - Multiple user login failures

Detects when multiple user login failures occurs.

**Required Data Connectors**

CiscoDuoSecurity

### Cisco Duo - Multiple users deleted

Detects when multiple users were deleted.

**Required Data Connectors**

CiscoDuoSecurity

### Cisco Duo - New access device

Detects new access device.

**Required Data Connectors**

CiscoDuoSecurity

### Cisco Duo - Admin user created

Detects when new admin user is created.

**Required Data Connectors**

CiscoDuoSecurity

### Cisco Duo - Authentication device new location

Detects new location of authentication device.

**Required Data Connectors**

CiscoDuoSecurity

### Cisco Duo - Unexpected authentication factor

Detects when unexpected authentication factor used.

**Required Data Connectors**

CiscoDuoSecurity

## Hunting Queries

### Cisco Duo - Admin failure authentications

CiscoDuoSecurity Hunting Query 1

### Cisco Duo - Delete actions

CiscoDuoSecurity Hunting Query 2

### Cisco Duo - Admin failure authentications

CiscoDuoSecurity Hunting Query 3

### Cisco Duo - Authentication errors

CiscoDuoSecurity Hunting Query 4

### Cisco Duo - Authentication error reasons

CiscoDuoSecurity Hunting Query 5

### Cisco Duo - Deleted users

CiscoDuoSecurity Hunting Query 6

### Cisco Duo - Fraud authentications

CiscoDuoSecurity Hunting Query 7

### Cisco Duo - New users

CiscoDuoSecurity Hunting Query 8

### Cisco Duo - Devices with vulnerable OS

CiscoDuoSecurity Hunting Query 9

### Cisco Duo - Devices with unsecure settings

CiscoDuoSecurity Hunting Query 10

## Watchlists

## Playbooks

## Parsers

### CiscoDuoSecurity Data Parser

Category: Samples

Function Alias: CiscoDuo

# Cisco Firepower eStreamer

The Cisco Event Streamer (a.k.a eStreamer) allows you to stream Firepower System events to external client applications. You can stream host, discovery, correlation, compliance allow list, intrusion, user activity, file, malware, and connection data.

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

## Data Connectors

### Cisco Firepower eStreamer

eStreamer is a Client Server API designed for the Cisco Firepower NGFW Solution. The eStreamer client requests detailed event data on behalf of the SIEM or logging solution in the Common Event Format (CEF).

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

### Block URL - Cisco Firepower

This playbook allows blocking of FQDNs in Cisco Firepower, using a \*\*Network Group object\*\*. This allows making changes to a Network Group selected members, instead of making Access List Entries. The Network Group object itself should be part of an Access List Entry.1. For the URLs of the incident, extract the FQDN 2. Check if FQDNs are already selected for the Network Group object 3. For the FQDNs not already selected for the Network Group object, check if there is an existing FQDN object in Cisco Firepower, if it does not exist create it 4. Add the FQDN object to the Network Group object, so it gets blocked 5. Comment is added to Microsoft Sentinel incident

### Block IP - Cisco Firepower

This playbook allows blocking of IPs in Cisco Firepower, using a \*\*Network Group object\*\*. This allows making changes to a Network Group selected members, instead of making Access List Entries. The Network Group object itself should be part of an Access List Entry.When a new Sentinel incident is created, this playbook gets triggered and performs below actions. 1. For the IPs we check if they are already selected for the Network Group object 2. For the IPs not already selected for the Network Group object, add it so it gets blocked 3. Comment is added to Microsoft Sentinel incident ![Microsoft Sentinel comment](https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/Solutions/Cisco%20Firepower%20EStreamer/Playbooks/CiscoFirepower-BlockFQDN-NetworkGroup/Images/BlockFQDN-NetworkGroup-AzureSentinel-Comments.png) \*\* IP is added to Cisco Firepower Network Group object:\*\* ![Cisco Firepower Network Group object](https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/Solutions/Cisco%20Firepower%20EStreamer/Playbooks/CiscoFirepower-BlockFQDN-NetworkGroup/Images/BlockFQDN-NetworkGroup-CiscoFirepowerAdd.png)

### Block IP - Take Action from Teams - Cisco Firepower

This playbook allows blocking of IPs in Cisco Firepower, using a \*\*Network Group object\*\*. This allows making changes to a Network Group selected members, instead of making Access List Entries. The Network Group object itself should be part of an Access List Entry.When a new Sentinel incident is created, this playbook gets triggered and performs below actions. 1. For the IPs we check if they are already selected for the Network Group object 2. An adaptive card is sent to a Teams channel with information about the incident and giving the option to ignore an IP, or depending on it's current status block it by adding it to the Network Group object or unblock it by removing it from the Network Group object ![Teams Adaptive Card preview](https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/Solutions/Cisco%20Firepower%20EStreamer/Playbooks/CiscoFirepower-BlockIP-Teams/Images/BlockIP-Teams-AdaptiveCard.png) 3. The chosen changes are applied to the Network Group object 4. Comment is added to Microsoft Sentinel incident ![Microsoft Sentinel comment](https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/Solutions/Cisco%20Firepower%20EStreamer/Playbooks/CiscoFirepower-BlockIP-Teams/Images/BlockIP-Teams-AzureSentinel-Comments.png) \*\* IP is added to Cisco Firepower Network Group object:\*\* ![Cisco Firepower Network Group object](https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/Solutions/Cisco%20Firepower%20EStreamer/Playbooks/CiscoFirepower-BlockFQDN-NetworkGroup/Images/BlockFQDN-NetworkGroup-CiscoFirepowerAdd.png) \*\*Playbook overview:\*\* ![Playbook overview](https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/Solutions/Cisco%20Firepower%20EStreamer/Playbooks/CiscoFirepower-BlockIP-Teams/Images/BlockIP-Teams-LogicApp.png)

## Parsers

# Cisco ISE

The Cisco ISE solution for Microsoft Sentinel enables you to ingest Cisco ISE’s NAC logs into Microsoft Sentinel, providing insight into network threats and vulnerabilities.

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 10**, Hunting Queries:** 10**, Watchlists:** 0**, Playbooks:** 3, Parsers: 1

## Data Connectors

### Cisco Identity Services Engine

The Cisco Identity Services Engine (ISE) data connector provides the capability to ingest [Cisco ISE](https://www.cisco.com/c/en/us/products/security/identity-services-engine/index.html) events with Microsoft Sentinel. It helps you gain visibility into what is happening in your network, such as who is connected, which applications are installed and running, and much more. Refer to [Cisco ISE logging mechanism documentation](https://www.cisco.com/c/en/us/td/docs/security/ise/2-7/admin\_guide/b\_ise\_27\_admin\_guide/b\_ISE\_admin\_27\_maintain\_monitor.html#reference\_BAFBA5FA046A45938810A5DF04C00591) for more information.

## Workbooks

### Cisco ISE

Sets the time name for analysis

**Required Data Types**

## Analytic Rules

### CiscoISE - ISE administrator password has been reset

Detects when the ISE administrator password has been reset.

**Required Data Connectors**

CiscoISE

### CiscoISE - Attempt to delete local store logs

Detects when attempt to delete local store logs failed.

**Required Data Connectors**

CiscoISE

### CiscoISE - Backup failed

Detects when backup activity failed.

**Required Data Connectors**

CiscoISE

### CiscoISE - Certificate has expired

Detects certificate expiration.

**Required Data Connectors**

CiscoISE

### CiscoISE - Command executed with the highest privileges from new IP

Detects command execution with PrivilegeLevel - 15 from new source.

**Required Data Connectors**

CiscoISE

### CiscoISE - Command executed with the highest privileges by new user

Detects command execution with PrivilegeLevel - 15 by user for wich there was no such activity detected earlier.

**Required Data Connectors**

CiscoISE

### CiscoISE - Device changed IP in last 24 hours

Detects when device changes IP address in last 24 hours.

**Required Data Connectors**

CiscoISE

### CiscoISE - Device PostureStatus changed to non-compliant

Detects when device changes PostureStatus from "Compliant".

**Required Data Connectors**

CiscoISE

### CiscoISE - Log collector was suspended

Detects when log collector was suspended.

**Required Data Connectors**

CiscoISE

### CiscoISE - Log files deleted

Detects log file deleting activity.

**Required Data Connectors**

CiscoISE

## Hunting Queries

### CiscoISE - Authentication attempts to suspended user account

Cisco ISE Hunting Query 1

CiscoISE - Dynamic authorization failed

Cisco ISE Hunting Query 2

### CiscoISE - Expired certificate in the client certificates chain

Cisco ISE Hunting Query 3

### CiscoISE - Failed authentication events

Cisco ISE Hunting Query 4

### CiscoISE - Failed login attempts via SSH CLI (users)

Cisco ISE Hunting Query 5

### CiscoISE - Guest authentication failed

Cisco ISE Hunting Query 6

### CiscoISE - Guest authentication succeeded

Cisco ISE Hunting Query 7

### CiscoISE - Rare or new useragent

Cisco ISE Hunting Query 8

### CiscoISE - Sources with high number of 'Failed Authentication' events

Cisco ISE Hunting Query 9

### CiscoISE - Attempts to suspend the log collector

Cisco ISE Hunting Query 10

## Watchlists

## Playbooks

### CiscoISE-False Positives Clear Policies

This playbook gets triggered when a new sentinel incident is created

1.For each MAC address (MACAddress provided in the alert custom entities) in the incident checks if it is was rejected in Cisco ISE.

2.If MAC address was rejected, checks if it is in the safe list (safe list is a custom [Watchlist](https://docs.microsoft.com/azure/sentinel/watchlists) that contains safe MAC addresses). If it is in safe list, releases endpoint with this MAC address in Cisco ISE.

3.Adds comment to the incident with information about the released endpoints.

### CiscoISE-SuspendGuestUser

When a new sentinel incident is created, this playbook gets triggered and performs the following actions:

1. For each Account in the incident suspends user in Cisco ISE by its name.

2. Adds comment to the incident with information about suspended users.

### CiscoISE-TakeEndpointActionFromTeams

When a new sentinel incident is created, this playbook gets triggered and performs the following actions:

1. Sends an adaptive card to the Teams channel where the analyst can choose an action to be taken.

2. Assigns a policy (policy name is provided during the deployment stage) to an and point (\*MACAddress\* of the endpoint is provided in the alert custom entities) depending on the action chosen in the adaptive card.

3. Changes incident status and severity depending on the action chosen in the adaptive card.

4. Adds comment to the incident with information about the actions taken.

## Parsers

### CiscoISE

Category: Samples

Function Alias: CiscoISE

# Cisco Meraki Solution

Cisco Meraki connector connects to Cisco Meraki Dashboard API service endpoint and programmatically manages and monitors Meraki networks at scale.

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

## Data Connectors

### Cisco Meraki

The [Cisco Meraki](https://meraki.cisco.com/) connector allows you to easily connect your Cisco Meraki (MX/MR/MS) logs with Microsoft Sentinel. This gives you more insight into your organization's network and improves your security operation capabilities.

## Workbooks

### CiscoMerakiWorkbook

Gain insights into the Events from Cisco Meraki Solution and analyzing all the different types of Security Events. This workbook also helps in identifying the Events from affected devices, IPs and the nodes where malware was successfully detected.

IP data received in Events is correlated with Threat Intelligence to identify if the reported IP address is known bad based on threat intelligence data.

**Required Data Types**

meraki\_CL

CiscoMerakiNativePoller

ThreatIntelligenceIndicator

CiscoMeraki

CiscoMerakiNativePolling

ThreatIntelligence

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

### Block Device Client - Cisco Meraki

This playbook checks if malicious device client is blocked by Cisco Meraki network.1. Fetches a list of potentially device clients 2. If malicious device client is not blocked by Cisco meraki network then blocks it.

### Block IP Address - Cisco Meraki

This playbook checks if malicious IP address is blocked or unblocked by Cisco Meraki MX network.1. Fetches a list of potentially malicious IP addresses 2. If malicious IP address is not blocked by Cisco meraki network then blocks it.

### Block URL - Cisco Meraki

This playbook checks if malicious URL is blocked in Cisco Meraki network.1. Fetches a list of potentially malicious URLs 2. If malicious URL is not blocked by Cisco meraki network then blocks it.

### IP Address Enrichment - Cisco Meraki

This playbook checks if malicious IP address is blocked or unblocked by Cisco Meraki MX network.1. Fetches a list of potentially malicious IP addresses 2. Enrich the incident with IP status information.

### URL Enrichment - Cisco Meraki

This playbook checks if malicious URL is blocked or unblocked by Cisco Meraki network.1. Fetches a list of potentially malicious URLs 2. Enrich the incident with URL status information.

## Parsers

### Cisco Meraki Data Parser

Category: Samples

Function Alias: CiscoMeraki

# Cisco Secure Endpoint Solution

Cisco Secure Endpoint unifies user and endpoint security. With a built-in platform called SecureX, it delivers integrated XDR capabilities and more to bolster your endpoint protection and maximize your endpoint security operational efficiency.

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 11**, Hunting Queries:** 10**, Watchlists:** 0**, Playbooks:** 0, Parsers: 1

## Data Connectors

### Cisco Secure Endpoint (AMP) (using Azure Function)

The Cisco Secure Endpoint (formerly AMP for Endpoints) data connector provides the capability to ingest Cisco Secure Endpoint [audit logs](https://api-docs.amp.cisco.com/api\_resources/AuditLog?api\_host=api.amp.cisco.com&api\_version=v1) and [events](https://api-docs.amp.cisco.com/api\_actions/details?api\_action=GET+%2Fv1%2Fevents&api\_host=api.amp.cisco.com&api\_resource=Event&api\_version=v1) into Microsoft Sentinel.

## Workbooks

### Cisco Secure Endpoint

Sets the time name for analysis

**Required Data Types**

CiscoSecureEndpoint

CiscoSecureEndpoint

## Analytic Rules

### Cisco SE High Events Last Hour

Find events from Cisco Secure Endpoint that are of High severity in the last hour.

**Required Data Connectors**

CiscoSecureEndpoint

### Cisco SE - Connection to known C2 server

This rule is triggered when connection to known C2 is detected from host.

**Required Data Connectors**

CiscoSecureEndpoint

### Cisco SE - Dropper activity on host

Detects possible dropper activity on host.

**Required Data Connectors**

CiscoSecureEndpoint

### Cisco SE - Generic IOC

This rule is triggered when generic IOC is observed on host.

**Required Data Connectors**

CiscoSecureEndpoint

### Cisco SE - Malware execusion on host

Detects malware execution on host.

**Required Data Connectors**

CiscoSecureEndpoint

### Cisco SE - Malware outbreak

Detects possible malware outbreak.

**Required Data Connectors**

CiscoSecureEndpoint

### Cisco SE - Multiple malware on host

This rule triggers when multiple malware where detected on host.

**Required Data Connectors**

CiscoSecureEndpoint

### Cisco SE - Policy update failure

Detects policy updates failures.

**Required Data Connectors**

CiscoSecureEndpoint

### Cisco SE - Ransomware Activity

This rule is triggered when possible ransomware activity is detected on host.

**Required Data Connectors**

CiscoSecureEndpoint

### Cisco SE - Unexpected binary file

Detects binary files in uncommon locations.

**Required Data Connectors**

CiscoSecureEndpoint

### Cisco SE - Possible webshell

Detects possible webshell on host.

**Required Data Connectors**

CiscoSecureEndpoint

## Hunting Queries

### Cisco SE - Infected hosts

Cisco Secure Endpoint Hunting Query 1

### Cisco SE - Infected users

Cisco Secure Endpoint Hunting Query 2

### Cisco SE - User Logins

Cisco Secure Endpoint Hunting Query 3

### Cisco SE - Malicious files

Cisco Secure Endpoint Hunting Query 4

### Cisco SE - Modified agents on hosts

Cisco Secure Endpoint Hunting Query 5

### Cisco SE - Rare scanned files

Cisco Secure Endpoint Hunting Query 6

### Cisco SE - Scanned files

Cisco Secure Endpoint Hunting Query 7

### Cisco SE - Suspicious powershel downloads

Cisco Secure Endpoint Hunting Query 8

### Cisco SE - Uncommon application behavior

Cisco Secure Endpoint Hunting Query 9

### Cisco SE - Vulnerable applications

Cisco Secure Endpoint Hunting Query 10

## Watchlists

## Playbooks

## Parsers

### CiscoSecureEndpoint Data Parser

Category: Samples

Function Alias: CiscoSecureEndpoint

# Cisco SEG Solution

The Cisco Secure Email Gateway (SEG) solution provides the capability to ingest Cisco SEG Consolidated Event Logs into Microsoft Sentinel.

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 11**, Hunting Queries:** 10**, Watchlists:** 0**, Playbooks:** 0, Parsers: 1

## Data Connectors

### Cisco Secure Email Gateway

The [Cisco Secure Email Gateway (SEG)](https://www.cisco.com/c/en/us/products/security/email-security/index.html) data connector provides the capability to ingest [Cisco SEG Consolidated Event Logs](https://www.cisco.com/c/en/us/td/docs/security/esa/esa14-0/user\_guide/b\_ESA\_Admin\_Guide\_14-0/b\_ESA\_Admin\_Guide\_12\_1\_chapter\_0100111.html#con\_1061902) into Microsoft Sentinel.

## Workbooks

### Cisco Secure Email Gateway

Sets the time name for analysis

**Required Data Types**

CommonSecurityLog

CiscoSEG

## Analytic Rules

### Cisco SEG - DLP policy violation

Detects DLP policy violation.

**Required Data Connectors**

CiscoSEG

### Cisco SEG - Malicious attachment not blocked

Detects mails with malicious attachments which were not blocked.

**Required Data Connectors**

CiscoSEG

### Cisco SEG - Multiple large emails sent to external recipient

Detects possible data exfiltration.

**Required Data Connectors**

CiscoSEG

### Cisco SEG - Multiple suspiciuos attachments received

Detects possibly phishing emails.

**Required Data Connectors**

CiscoSEG

### Cisco SEG - Possible outbreak

Detects possible outbreak activity.

**Required Data Connectors**

CiscoSEG

### Cisco SEG - Potential phishing link

Detects mails with suspicious links.

**Required Data Connectors**

CiscoSEG

### Cisco SEG - Suspicious link

Detects mails with suspicious links.

**Required Data Connectors**

CiscoSEG

### Cisco SEG - Suspicious sender domain

Detects suspicious sender domain age.

**Required Data Connectors**

CiscoSEG

### Cisco SEG - Unexpected link

Detects mails with suspicious links.

**Required Data Connectors**

CiscoSEG

### Cisco SEG - Unexpected attachment

Detects possibly malicious attachments.

**Required Data Connectors**

CiscoSEG

### Cisco SEG - Unscannable attacment

Detects unscannable attachments in mails.

**Required Data Connectors**

CiscoSEG

## Hunting Queries

### Cisco SEG - Dropped incoming mails

CiscoSEG Hunting Query 1

### Cisco SEG - Dropped outgoing mails

CiscoSEG Hunting Query 2

### Cisco SEG - DKIM failures

CiscoSEG Hunting Query 3

### Cisco SEG - DMARK failures

CiscoSEG Hunting Query 4

### Cisco SEG - SPF failures

CiscoSEG Hunting Query 5

### Cisco SEG - Failed incoming TLS connections

CiscoSEG Hunting Query 6

### Cisco SEG - Failed outgoing TLS connections

CiscoSEG Hunting Query 7

### Cisco SEG - Insecure protocol

CiscoSEG Hunting Query 8

### Cisco SEG - Sources of spam mails

CiscoSEG Hunting Query 9

### Cisco SEG - Top users receiving spam mails

CiscoSEG Hunting Query 10

## Watchlists

## Playbooks

## Parsers

### Cisco SEG Data Parser

Category: Samples

Function Alias: CiscoSEGEvent

# Cisco Stealthwatch Solution

The Cisco Stealthwatch solution provides the capability to ingest Cisco Stealthwatch events into Microsoft Sentinel.

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

## Data Connectors

### Cisco Stealthwatch

The [Cisco Stealthwatch](https://www.cisco.com/c/en/us/products/security/stealthwatch/index.html) data connector provides the capability to ingest [Cisco Stealthwatch events](https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/management\_console/securit\_events\_alarm\_categories/SW\_7\_2\_1\_Security\_Events\_and\_Alarm\_Categories\_DV\_1\_0.pdf) into Microsoft Sentinel. Refer to [Cisco Stealthwatch documentation](https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/system\_installation\_configuration/SW\_7\_3\_2\_System\_Configuration\_Guide\_DV\_1\_0.pdf) for more information.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### CiscoStealthwatch Data Parser

Category: Samples

Function Alias: StealthwatchEvent

# Cisco UCS

The Cisco UCS solution for Microsoft Sentinel enables you to ingest Cisco UCS faults, events, and audit logs into Microsoft Sentinel

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

## Data Connectors

### Cisco UCS

The [Cisco Unified Computing System (UCS)](https://www.cisco.com/c/en/us/products/servers-unified-computing/index.html) connector allows you to easily connect your Cisco UCS logs with Azure Sentinel This gives you more insight into your organization's network and improves your security operation capabilities.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### CiscoUCS

Category: Samples

Function Alias: CiscoUCS

# Cisco Umbrella

The Cisco Umbrella solution for Microsoft Sentinel enables you to ingest Cisco Umbrella events stored in Amazon S3 into Microsoft Sentinel using the Amazon S3 REST API.

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

## Data Connectors

### Cisco Umbrella (using Azure Function)

The Cisco Umbrella data connector provides the capability to ingest [Cisco Umbrella](https://docs.umbrella.com/) events stored in Amazon S3 into Microsoft Sentinel using the Amazon S3 REST API. Refer to [Cisco Umbrella log management documentation](https://docs.umbrella.com/deployment-umbrella/docs/log-management) for more information.

## Workbooks

### Cisco Umbrella

Gain insights into Cisco Umbrella activities, including the DNS, Proxy and Cloud Firewall data. Workbook shows general information along with threat landscape including categories, blocked destinations and URLs.

**Required Data Types**

Cisco\_Umbrella\_dns\_CL

Cisco\_Umbrella\_proxy\_CL

Cisco\_Umbrella\_ip\_CL

Cisco\_Umbrella\_cloudfirewall\_CL

CiscoUmbrellaDataConnector

## Analytic Rules

### Cisco Umbrella - Connection to non-corporate private network

IP addresses of broadband links that usually indicates users attempting to access their home network, for example for a remote session to a home computer.

**Required Data Connectors**

CiscoUmbrellaDataConnector

### Cisco Umbrella - Connection to Unpopular Website Detected

Detects first connection to an unpopular website (possible malicious payload delivery).

**Required Data Connectors**

CiscoUmbrellaDataConnector

### Cisco Umbrella - Crypto Miner User-Agent Detected

Detects suspicious user agent strings used by crypto miners in proxy logs.

**Required Data Connectors**

CiscoUmbrellaDataConnector

### Cisco Umbrella - Empty User Agent Detected

Rule helps to detect empty and unusual user agent indicating web browsing activity by an unusual process other than a web browser.

**Required Data Connectors**

CiscoUmbrellaDataConnector

### Cisco Umbrella - Hack Tool User-Agent Detected

Detects suspicious user agent strings used by known hack tools

**Required Data Connectors**

CiscoUmbrellaDataConnector

### Cisco Umbrella - Windows PowerShell User-Agent Detected

Rule helps to detect Powershell user-agent activity by an unusual process other than a web browser.

**Required Data Connectors**

CiscoUmbrellaDataConnector

### Cisco Umbrella - Rare User Agent Detected

Rule helps to detect a rare user-agents indicating web browsing activity by an unusual process other than a web browser.

**Required Data Connectors**

CiscoUmbrellaDataConnector

### Cisco Umbrella - Request Allowed to harmful/malicious URI category

It is reccomended that these Categories shoud be blocked by policies because they provide harmful/malicious content..

**Required Data Connectors**

CiscoUmbrellaDataConnector

### Cisco Umbrella - Request to blocklisted file type

Detects request to potentially harmful file types (.ps1, .bat, .vbs, etc.).

**Required Data Connectors**

CiscoUmbrellaDataConnector

### Cisco Umbrella - URI contains IP address

Malware can use IP address to communicate with C2.

**Required Data Connectors**

CiscoUmbrellaDataConnector

## Hunting Queries

### Cisco Umbrella - Anomalous FQDNs for domain

CiscoUmbrella Hunting Query 1

### Cisco Umbrella - 'Blocked' User-Agents.

CiscoUmbrella Hunting Query 2

### Cisco Umbrella - DNS Errors.

CiscoUmbrella Hunting Query 3

### Cisco Umbrella - DNS requests to unreliable categories.

CiscoUmbrella Hunting Query 4

### Cisco Umbrella - Higher values of count of the Same BytesIn size

CiscoUmbrella Hunting Query 5

### Cisco Umbrella - High values of Uploaded Data

CiscoUmbrella Hunting Query 6

### Cisco Umbrella - Possible connection to C2.

CiscoUmbrella Hunting Query 7

### Cisco Umbrella - Possible data exfiltration

CiscoUmbrella Hunting Query 8

### Cisco Umbrella - Proxy 'Allowed' to unreliable categories.

CiscoUmbrella Hunting Query 9

### Cisco Umbrella - Requests to uncategorized resources

CiscoUmbrella Hunting Query 10

## Watchlists

## Playbooks

### CiscoUmbrella-AddIpToDestinationList

This playbook showcases an example of triggering an incident within a targeted Teams channel and opening up a ticket within Service Now. Additionally The playbook will also list playbooks that can be initiated from teams using an adaptive card and callbacks that will take action upon certain entities identified in the incident.

### CiscoUmbrella-AssignPolicyToIdentity

This playbook showcases an example of triggering an incident within a targeted Teams channel and opening up a ticket within Service Now. Additionally The playbook will also list playbooks that can be initiated from teams using an adaptive card and callbacks that will take action upon certain entities identified in the incident.

### CiscoUmbrella-BlockDomain

This playbook showcases an example of triggering an incident within a targeted Teams channel and opening up a ticket within Service Now. Additionally The playbook will also list playbooks that can be initiated from teams using an adaptive card and callbacks that will take action upon certain entities identified in the incident.

### CiscoUmbrella-GetDomainInfo

This playbook showcases an example of triggering an incident within a targeted Teams channel and opening up a ticket within Service Now. Additionally The playbook will also list playbooks that can be initiated from teams using an adaptive card and callbacks that will take action upon certain entities identified in the incident.

## Parsers

### CiscoUmbrella Data Parser

Category: Samples

Function Alias: Cisco\_Umbrella

# Cisco WSA

The Cisco Web Security Appliance (WSA) solution provides the capability to ingest Cisco WSA Access Logs into Microsoft Sentinel.

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 11**, Hunting Queries:** 10**, Watchlists:** 0**, Playbooks:** 0, Parsers: 1

## Data Connectors

### Cisco Web Security Appliance

[Cisco Web Security Appliance (WSA)](https://www.cisco.com/c/en/us/products/security/web-security-appliance/index.html) data connector provides the capability to ingest [Cisco WSA Access Logs](https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa\_14-0/User-Guide/b\_WSA\_UserGuide\_14\_0/b\_WSA\_UserGuide\_11\_7\_chapter\_010101.html) into Microsoft Sentinel.

## Workbooks

### CiscoWSA

Sets the time name for analysis

**Required Data Types**

## Analytic Rules

### Cisco WSA - Access to unwanted site

Detects when users attempting to access sites from high risk category.

**Required Data Connectors**

CiscoWSA

### Cisco WSA - Unexpected uploads

Detects unexpected file uploads.

**Required Data Connectors**

CiscoWSA

### Cisco WSA - Multiple errors to resource from risky category

Detects multiple connection errors to resource from risky category.

**Required Data Connectors**

CiscoWSA

### Cisco WSA - Multiple errors to URL

Detects multiple connection errors to URL.

**Required Data Connectors**

CiscoWSA

### Cisco WSA - Multiple infected files

Detects multiple infected files on same source.

**Required Data Connectors**

CiscoWSA

### Cisco WSA - Multiple attempts to download unwanted file

Detects when multiple attempts to download unwanted file occur.

**Required Data Connectors**

CiscoWSA

### Cisco WSA - Suspected protocol abuse

Detects possible protocol abuse.

**Required Data Connectors**

CiscoWSA

### Cisco WSA - Internet access from public IP

Detects internet access from public IP.

**Required Data Connectors**

CiscoWSA

### Cisco WSA - Unexpected file type

Detects unexpected file type.

**Required Data Connectors**

CiscoWSA

### Cisco WSA - Unexpected URL

Detects unexpected URL.

**Required Data Connectors**

CiscoWSA

### Cisco WSA - Unscannable file or scan error

Detects unscanned downloaded file.

**Required Data Connectors**

CiscoWSA

## Hunting Queries

### Cisco WSA - Blocked files

CiscoWSA Hunting Query 1

### Cisco WSA - Rare aplications

CiscoWSA Hunting Query 2

### Cisco WSA - Top aplications

CiscoWSA Hunting Query 3

### Cisco WSA - Top URLs

CiscoWSA Hunting Query 4

### Cisco WSA - Uncategorized URLs

CiscoWSA Hunting Query 5

### Cisco WSA - Uploaded files

CiscoWSA Hunting Query 6

### Cisco WSA - Rare URL with error

CiscoWSA Hunting Query 7

### Cisco WSA - URL shorteners

CiscoWSA Hunting Query 8

### Cisco WSA - Potentially risky resources

CiscoWSA Hunting Query 9

### Cisco WSA - User errors

CiscoWSA Hunting Query 10

## Watchlists

## Playbooks

## Parsers

### CiscoWSA Data Parser

Category: Samples

Function Alias: CiscoWSAEvent

# Citrix ADC

The Citrix ADC (formerly NetScaler) enables you to ingest Citrix ADC logs into Microsoft Sentinel. Refer the Citrix ADC log collection guide for more details.

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

## Data Connectors

### Citrix ADC (former NetScaler)

The [Citrix ADC (former NetScaler)](https://www.citrix.com/products/citrix-adc/) data connector provides the capability to ingest Citrix ADC logs into Microsoft Sentinel.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### CitrixADCEvent

Category: Samples

Function Alias: CitrixADCEvent

# Citrix Analytics Application for Microsoft Sentinel

Export and correlate the users’ data from your Citrix IT environment to Microsoft Sentinel and get deeper insights into your organization’s security posture. View the insightful dashboards that are unique to Citrix Analytics for Security.

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

## Data Connectors

### CITRIX SECURITY ANALYTICS

Citrix Analytics (Security) integration with Microsoft Sentinel helps you to export data analyzed for risky events from Citrix Analytics (Security) into Microsoft Sentinel environment. You can create custom dashboards, analyze data from other sources along with that from Citrix Analytics (Security) and create custom workflows using Logic Apps to monitor and mitigate security events.

## Workbooks

### Citrix Analytics

Citrix Analytics for Security aggregates and correlates information across network traffic, users, files and endpoints in Citrix environments. This generates actionable insights that enable Citrix administrators and security teams to remediate user security threats through automation while optimizing IT operations. Machine learning and artificial intelligence empowers Citrix Analytics for Security to identify and take automated action to prevent data exfiltration. While delivered as a cloud service, Citrix Analytics for Security can generate insights from resources located on-premises, in the cloud, or in hybrid architectures. The Citrix Analytics Workbook further enhances the value of both your Citrix Analytics for Security and Microsoft Sentinel. The Workbook enables you to integrate data sources together, helping you gain even richer insights. It also gives Security Operations (SOC) teams the ability to correlate data from disparate logs, helping you identify and proactively remediate security risk quickly. Additionally, valuable dashboards that were unique to the Citrix Analytics for Security can now be implemented in Sentinel. You can also create new custom Workbooks that were not previously available, helping extend the value of both investments.

**Required Data Types**

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Citrix WAF Solution for Sentinel

Citrix WAF Solution for Sentinel is an industry-leading enterprise-grade WAF solution. Citrix WAF mitigates threats against your public-facing assets, including websites, apps, and APIs.

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

## Data Connectors

### Citrix WAF (Web App Firewall)

Citrix WAF (Web App Firewall) is an industry leading enterprise-grade WAF solution. Citrix WAF mitigates threats against your public-facing assets, including websites, apps, and APIs. From layer 3 to layer 7, Citrix WAF includes protections such as IP reputation, bot mitigation, defense against the OWASP Top 10 application threats, built-in signatures to protect against application stack vulnerabilities, and more.

Citrix WAF supports Common Event Format (CEF) which is an industry standard format on top of Syslog messages . By connecting Citrix WAF CEF logs to Microsoft Sentinel, you can take advantage of search & correlation, alerting, and threat intelligence enrichment for each log.

## Workbooks

### Citrix WAF (Web App Firewall)

Gain insight into the Citrix WAF logs

**Required Data Types**

CommonSecurityLog

CitrixWAF

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Claroty

The Claroty solution for Microsoft Sentinel enables ingestion of  Continuous Threat Detection and Secure Remote Access events into Microsoft Sentinel.

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 10**, Hunting Queries:** 10**, Watchlists:** 0**, Playbooks:** 0, Parsers: 1

## Data Connectors

### Claroty

The [Claroty](https://claroty.com/) data connector provides the capability to ingest [Continuous Threat Detection](https://claroty.com/continuous-threat-detection/) and [Secure Remote Access](https://claroty.com/secure-remote-access/) events into Microsoft Sentinel.

## Workbooks

### Claroty

Sets the time name for analysis

**Required Data Types**

## Analytic Rules

### Claroty - Asset Down

Triggers asset is down.

**Required Data Connectors**

Claroty

### Claroty - Critical baseline deviation

Detects when critical deviation from baseline occurs.

**Required Data Connectors**

Claroty

### Claroty - Login to uncommon location

Detects user login to uncommon location.

**Required Data Connectors**

Claroty

### Claroty - Multiple failed logins by user

Detects multiple failed logins by same user.

**Required Data Connectors**

Claroty

### Claroty - Multiple failed logins to same destinations

Detects multiple failed logins to same destinations.

**Required Data Connectors**

Claroty

### Claroty - New Asset

Triggers when a new asset has been added into the environment.

**Required Data Connectors**

Claroty

### Claroty - Policy violation

Detects policy violations.

**Required Data Connectors**

Claroty

### Claroty - Suspicious activity

Detects suspicious behavior that is generally indicative of malware.

**Required Data Connectors**

Claroty

### Claroty - Suspicious file transfer

Detects suspicious file transfer activity.

**Required Data Connectors**

Claroty

### Claroty - Treat detected

Detects Collection of known malware commands and control servers.

**Required Data Connectors**

Claroty

## Hunting Queries

### Claroty - Baseline deviation

Claroty Hunting Query 1

### Claroty - Conflict assets

Claroty Hunting Query 2

### Claroty - Critical Events

Claroty Hunting Query 3

### Claroty - PLC logins

Claroty Hunting Query 4

### Claroty - User failed logins

Claroty Hunting Query 5

### Claroty - Network scan sources

Claroty Hunting Query 6

### Claroty - Network scan targets

Claroty Hunting Query 7

### Claroty - Unapproved access

Claroty Hunting Query 8

### Claroty - Unresolved alerts

Claroty Hunting Query 9

### Claroty - Write and Execute operations

Claroty Hunting Query 10

## Watchlists

## Playbooks

## Parsers

### Claroty Data Parser

Category: Samples

Function Alias: ClarotyEvent

# Cloud Identity Threat Protection Essentials

The Cloud Identity Threat Protection Essentials solution looks for most common cloud focused identity attacks such as Suspicious Sign-ins, privilege grants, MFA disable etc.

**Data Connectors:** 0**, Workbooks:** 0**, Analytic Rules:** 2**, Hunting Queries:** 8**, Watchlists:** 0**, Playbooks:** 0, Parsers: 0

## Data Connectors

## Workbooks

## Analytic Rules

### MFA disabled for a user

Multi-Factor Authentication (MFA) helps prevent credential compromise. This alert identifies when an attempt has been made to disable MFA for a user

**Required Data Connectors**

AzureActiveDirectory

AWS

### New External User Granted Admin

This query will detect instances where a newly invited external user is granted an administrative role. By default this query

will alert on any granted administrative role, however this can be modified using the roles variable if false positives occur

in your environment. The maximum delta between invite and escalation to admin is 60 minues, this can be configured using the

deltaBetweenInviteEscalation variable.

**Required Data Connectors**

AzureActiveDirectory

## Hunting Queries

### Suspicious Sign-in to Privileged Account

Cloud Identity Threat Protection Essentials Hunting Query 1

### Attempts to sign in to disabled accounts by IP address

Cloud Identity Threat Protection Essentials Hunting Query 2

### Attempts to sign in to disabled accounts by account name

Cloud Identity Threat Protection Essentials Hunting Query 3

### Signins from Nord VPN Providers

Cloud Identity Threat Protection Essentials Hunting Query 4

### Signins From VPS Providers

Cloud Identity Threat Protection Essentials Hunting Query 5

### User Granted Access and Grants others Access

Cloud Identity Threat Protection Essentials Hunting Query 6

### Interactive STS refresh token modifications

Cloud Identity Threat Protection Essentials Hunting Query 7

### Application Granted EWS Permissions

Cloud Identity Threat Protection Essentials Hunting Query 8

## Watchlists

## Playbooks

## Parsers

# Cloud Service Threat Protection Essentials

The Cloud Service Threat Protection Essentials contains security content that is relevant for detection of attacks against various cloud services like key vault, storage, compute etc.

**Data Connectors:** 0**, Workbooks:** 0**, Analytic Rules:** 0**, Hunting Queries:** 2**, Watchlists:** 0**, Playbooks:** 0, Parsers: 0

## Data Connectors

## Workbooks

## Analytic Rules

## Hunting Queries

### Azure Resources assigned Public IP Addresses

Cloud Service Threat Protection Essentials Hunting Query 1

### Azure Key Vault Access Policy Manipulation

Cloud Service Threat Protection Essentials Hunting Query 2

## Watchlists

## Playbooks

## Parsers

# Cloudflare (Deprecated)

The Cloudflare solution provides the capability to ingest Cloudflare logs into Microsoft Sentinel using the Cloudflare Logpush and Azure Blob Storage. Refer to Cloudflare documentation for more information.

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 10**, Hunting Queries:** 10**, Watchlists:** 0**, Playbooks:** 0, Parsers: 1

## Data Connectors

### Cloudflare (Preview) (using Azure Function)

The Cloudflare data connector provides the capability to ingest [Cloudflare logs](https://developers.cloudflare.com/logs/) into Microsoft Sentinel using the Cloudflare Logpush and Azure Blob Storage. Refer to [Cloudflare documentation](https://developers.cloudflare.com/logs/logpush) for more information.

## Workbooks

### Cloudflare

Sets the time name for analysis

**Required Data Types**

Cloudflare\_CL

CloudflareDataConnector

## Analytic Rules

### Cloudflare - Bad client IP

Detects requests from IP with bad reputation index.

**Required Data Connectors**

CloudflareDataConnector

### Cloudflare - Empty user agent

Detects requests where user agent is empty.

**Required Data Connectors**

CloudflareDataConnector

### Cloudflare - Multiple error requests from single source

Detects multiple failure requests from single source in short timeframe.

**Required Data Connectors**

CloudflareDataConnector

### Cloudflare - Multiple user agents for single source

Detects requests with different user agents from one source in short timeframe.

**Required Data Connectors**

CloudflareDataConnector

### Cloudflare - Client request from country in blocklist

Detects requests from countries which are in blocklist.

**Required Data Connectors**

CloudflareDataConnector

### Cloudflare - Unexpected POST requests

Detects post requests to unusual extensions.

**Required Data Connectors**

CloudflareDataConnector

### Cloudflare - Unexpected client request

Detects client requests to unusual client request.

**Required Data Connectors**

CloudflareDataConnector

### Cloudflare - Unexpected URI

Detects client requests to unusual URI.

**Required Data Connectors**

CloudflareDataConnector

### Cloudflare - WAF Allowed threat

Detects WAF "Allowed" action on threat events.

**Required Data Connectors**

CloudflareDataConnector

### Cloudflare - XSS probing pattern in request

Detects XSS probing patterns.

**Required Data Connectors**

CloudflareDataConnector

## Hunting Queries

### Cloudflare - Client errors

Cloudflare Hunting Query 1

### Cloudflare - Client TLS errors

Cloudflare Hunting Query 2

### Cloudflare - Files requested

Cloudflare Hunting Query 3

### Cloudflare - Rare user agents

Cloudflare Hunting Query 4

### Cloudflare - Server errors

Cloudflare Hunting Query 5

### Cloudflare - Server TLS errors

Cloudflare Hunting Query 6

### Cloudflare - Top Network rules

Cloudflare Hunting Query 7

### Cloudflare - Top WAF rules

Cloudflare Hunting Query 8

### Cloudflare - Unexpected countries

Cloudflare Hunting Query 9

### Cloudflare - Unexpected edge response

Cloudflare Hunting Query 10

## Watchlists

## Playbooks

## Parsers

### Cloudflare

Category: Samples

Function Alias: Cloudflare

# Cloudflare for Microsoft Sentinel

Easily integrate Cloudflare with Microsoft Sentinel

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 10**, Hunting Queries:** 10**, Watchlists:** 0**, Playbooks:** 0, Parsers: 1

## Data Connectors

### Cloudflare (Preview) (using Azure Function)

The Cloudflare data connector provides the capability to ingest [Cloudflare logs](https://developers.cloudflare.com/logs/) into Microsoft Sentinel using the Cloudflare Logpush and Azure Blob Storage. Refer to [Cloudflare documentation](https://developers.cloudflare.com/logs/logpush) for more information.

## Workbooks

### Cloudflare

Sets the time name for analysis

**Required Data Types**

Cloudflare\_CL

CloudflareDataConnector

## Analytic Rules

### Cloudflare - Bad client IP

Detects requests from IP with bad reputation index.

**Required Data Connectors**

CloudflareDataConnector

### Cloudflare - Empty user agent

Detects requests where user agent is empty.

**Required Data Connectors**

CloudflareDataConnector

### Cloudflare - Multiple error requests from single source

Detects multiple failure requests from single source in short timeframe.

**Required Data Connectors**

CloudflareDataConnector

### Cloudflare - Multiple user agents for single source

Detects requests with different user agents from one source in short timeframe.

**Required Data Connectors**

CloudflareDataConnector

### Cloudflare - Client request from country in blocklist

Detects requests from countries which are in blocklist.

**Required Data Connectors**

CloudflareDataConnector

### Cloudflare - Unexpected POST requests

Detects post requests to unusual extensions.

**Required Data Connectors**

CloudflareDataConnector

### Cloudflare - Unexpected client request

Detects client requests to unusual URI.

**Required Data Connectors**

CloudflareDataConnector

### Cloudflare - Unexpected URI

Detects client requests to unusual URI.

**Required Data Connectors**

CloudflareDataConnector

### Cloudflare - WAF Allowed threat

Detects WAF "Allowed" action on threat events.

**Required Data Connectors**

CloudflareDataConnector

### Cloudflare - XSS probing pattern in request

Detects XSS probing patterns.

**Required Data Connectors**

CloudflareDataConnector

## Hunting Queries

### Cloudflare - Client errors

Cloudflare Hunting Query 1

### Cloudflare - Client TLS errors

Cloudflare Hunting Query 2

### Cloudflare - Files requested

Cloudflare Hunting Query 3

### Cloudflare - Rare user agents

Cloudflare Hunting Query 4

### Cloudflare - Server errors

Cloudflare Hunting Query 5

### Cloudflare - Server TLS errors

Cloudflare Hunting Query 6

### Cloudflare - Top Network rules

Cloudflare Hunting Query 7

### Cloudflare - Top WAF rules

Cloudflare Hunting Query 8

### Cloudflare - Unexpected countries

Cloudflare Hunting Query 9

### Cloudflare - Unexpected edge response

Cloudflare Hunting Query 10

## Watchlists

## Playbooks

## Parsers

### Cloudflare

Category: Samples

Function Alias: Cloudflare

# Cognni for Microsoft Sentinel

Cognni autonomously maps your previously unidentified critical information assets and detects undiagnosed incidents. This recognizes risks to your critical information, triages the severity of the incidents, and compiles incident details.

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 15**, Hunting Queries:** 0**, Watchlists:** 0**, Playbooks:** 0, Parsers: 0

## Data Connectors

### Cognni

The Cognni connector offers a quick and simple integration with Microsoft Sentinel. You can use Cognni to autonomously map your previously unclassified important information and detect related incidents. This allows you to recognize risks to your important information, understand the severity of the incidents, and investigate the details you need to remediate, fast enough to make a difference.

## Workbooks

### Cognni Important Information Incidents

Gain intelligent insights into the risks to your important financial, legal, HR, and governance information. This workbook lets you monitor your at-risk information to determine when and why incidents occurred, as well as who was involved. These incidents are broken into high, medium, and low risk incidents for each information category.

**Required Data Types**

CognniIncidents\_CL

CognniSentinelDataConnector

## Analytic Rules

### Cognni Incidents for Highly Sensitive Business Information

Display incidents in which highly sensitive business information was placed at risk by user sharing.

**Required Data Connectors**

CognniSentinelDataConnector

### Cognni Incidents for Highly Sensitive Financial Information

Display incidents in which highly sensitive financial information was placed at risk by user sharing.

**Required Data Connectors**

CognniSentinelDataConnector

### Cognni Incidents for Highly Sensitive Governance Information

Display incidents in which highly sensitive governance information was placed at risk by user sharing.

**Required Data Connectors**

CognniSentinelDataConnector

### Cognni Incidents for Highly Sensitive HR Information

Display incidents in which highly sensitive HR information was placed at risk by user sharing.

**Required Data Connectors**

CognniSentinelDataConnector

### Cognni Incidents for Highly Sensitive Legal Information

Display incidents in which highly sensitive legal information was placed at risk by user sharing.

**Required Data Connectors**

CognniSentinelDataConnector

### Cognni Incidents for Low Sensitivity Business Information

Display incidents in which low sensitivity business information] was placed at risk by user sharing.

**Required Data Connectors**

CognniSentinelDataConnector

### Cognni Incidents for Low Sensitivity Financial Information

Display incidents in which low sensitivity financial information was placed at risk by user sharing.

**Required Data Connectors**

CognniSentinelDataConnector

### Cognni Incidents for Low Sensitivity Governance Information

Display incidents in which low sensitivity governance information] was placed at risk by user sharing.

**Required Data Connectors**

CognniSentinelDataConnector

### Cognni Incidents for Low Sensitivity HR Information

Display incidents in which low sensitive HR information was placed at risk by user sharing.

**Required Data Connectors**

CognniSentinelDataConnector

### Cognni Incidents for Low Sensitivity Legal Information

Display incidents in which low sensitivity legal information was placed at risk by user sharing.

**Required Data Connectors**

CognniSentinelDataConnector

### Cognni Incidents for Medium Sensitivity Business Information

Display incidents in which medium sensitivity business information was placed at risk by user sharing.

**Required Data Connectors**

CognniSentinelDataConnector

### Cognni Incidents for Medium Sensitivity Financial Information

Display incidents in which medium sensitive financial information was placed at risk by user sharing.

**Required Data Connectors**

CognniSentinelDataConnector

### Cognni Incidents for Medium Sensitivity Governance Information

Display incidents in which medium sensitivity governance information was placed at risk by user sharing.

**Required Data Connectors**

CognniSentinelDataConnector

### Cognni Incidents for Medium Sensitivity HR Information

Display incidents in which medium sensitivity HR information was placed at risk by user sharing.

**Required Data Connectors**

CognniSentinelDataConnector

### Cognni Incidents for Medium Sensitivity Legal Information

Display incidents in which medium sensitivity legal information was placed at risk by user sharing.

**Required Data Connectors**

CognniSentinelDataConnector

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Cohesity Security Integration for Microsoft Sentinel

This is an integration for use with Microsoft Sentinel's cloud-native security information and event manager (SIEM/SOAR) platform, to enable Security Operators and ITOps the automation and operational simplicity to respond to threats and recover.

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

## Data Connectors

### Cohesity (using Azure Function)

The Cohesity function apps provide the ability to ingest Cohesity Datahawk ransomware alerts into Microsoft Sentinel.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

### Cohesity Incident Email

This playbook sends an email to the recipient with the details related to the incidents.

### Restore From Last Cohesity Snapshot

This playbook restores the latest good Data Hawk (Helios) snapshot.

### Close Cohesity Helios Incident

This playbook closes the corresponding Cohesity DataHawk (Helios) ticket.

### Cohesity Create or Update ServiceNow incident

This playbook creates and updates the incident in the ServiceNow platform.

### Delete Cohesity incident blobs

This playbook deletes the blobs on Azure storage created by an incident that is generated by Cohesity function apps.

## Parsers

# Common Event Format solution for Sentinel

The Common Event Format (CEF) solution for Microsoft Sentinel allows you to ingest logs from any product and/or appliance that can send logs in the Common Event Format (CEF) over Syslog messages.

**Data Connectors:** 2**, Workbooks:** 0**, Analytic Rules:** 0**, Hunting Queries:** 0**, Watchlists:** 0**, Playbooks:** 0, Parsers: 0

## Data Connectors

### Common Event Format (CEF)

Common Event Format (CEF) is an industry standard format on top of Syslog messages, used by many security vendors to allow event interoperability among different platforms. By connecting your CEF logs to Microsoft Sentinel, you can take advantage of search & correlation, alerting, and threat intelligence enrichment for each log. For more information, see the [Microsoft Sentinel documentation](https://go.microsoft.com/fwlink/p/?linkid=2223902&wt.mc\_id=sentinel\_dataconnectordocs\_content\_cnl\_csasci).

### Common Event Format (CEF) via AMA

Common Event Format (CEF) is an industry standard format on top of Syslog messages, used by many security vendors to allow event interoperability among different platforms. By connecting your CEF logs to Microsoft Sentinel, you can take advantage of search & correlation, alerting, and threat intelligence enrichment for each log. For more information, see the [Microsoft Sentinel documentation](https://go.microsoft.com/fwlink/p/?linkid=2223547&wt.mc\_id=sentinel\_dataconnectordocs\_content\_cnl\_csasci).

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Continuous Diagnostics& Mitigation

This solution enables Compliance Teams, Architects, SecOps Analysts, and Consultants to gain situational awareness for cloud workload security posture. This solution is designed to augment staffing through automation, visibility, assessment, monitoring

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

## Data Connectors

## Workbooks

### ContinuousDiagnostics&Mitigation

Select the time range for this Overview.

**Required Data Types**

## Analytic Rules

### CDM\_ContinuousDiagnostics&Mitigation\_PostureChanged

This alert is designed to monitor Azure policies aligned with the Continuous Diagnostics & Mitigation (CDM) Program. The alert triggers when policy compliance falls below 70% within a 1 week timeframe.

**Required Data Connectors**

(none listed)

## Hunting Queries

### CDM\_ContinuousDiagnostics&Mitigation\_Posture

ContinuousDiagnostics&Mitigation Hunting Query 1

## Watchlists

## Playbooks

## Parsers

# Contrast Protect for Microsoft Sentinel

Contrast Protect for Microsoft Sentinel delivers real-time application security monitoring and protection.

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

## Data Connectors

### Contrast Protect

Contrast Protect mitigates security threats in production applications with runtime protection and observability. Attack event results (blocked, probed, suspicious...) and other information can be sent to Microsoft Microsoft Sentinel to blend with security information from other systems.

## Workbooks

### Contrast Protect

Select the time range for this Overview.

**Required Data Types**

## Analytic Rules

### Contrast Blocks

Creates Incidents for Blocked events sourced from the Contrast Protect agent.

**Required Data Connectors**

ContrastProtect

### Contrast Exploits

Creates Incidents for Exploit events sourced from the Contrast Protect agent.

**Required Data Connectors**

ContrastProtect

### Contrast Probes

Creates Incidents for Probed events sourced from the Contrast Protect agent.

**Required Data Connectors**

ContrastProtect

### Contrast Suspicious

Creates Incidents for Suspicious events sourced from the Contrast Protect agent.

**Required Data Connectors**

ContrastProtect

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Corelight for Microsoft Sentinel

Corelight for Microsoft Sentinel enables incident responders and threat hunters who use Microsoft Sentinel to work faster and more effectively. The data connector enables ingestion of events from Zeek and Suricata via Corelight Sensors into Sentinel.

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 10**, Hunting Queries:** 10**, Watchlists:** 0**, Playbooks:** 0, Parsers: 1

## Data Connectors

### Corelight

The [Corelight](https://corelight.com/) data connector enables incident responders and threat hunters who use Microsoft Sentinel to work faster and more effectively. The data connector enables ingestion of events from [Zeek](https://zeek.org/) and [Suricata](https://suricata-ids.org/) via Corelight Sensors into Microsoft Sentinel.

## Workbooks

### Corelight

Sets the time name for analysis

**Required Data Types**

Corelight\_CL

Corelight

## Analytic Rules

### Corelight - C2 DGA Detected Via Repetitive Failures

Detects large amounts of DNS resolution failures.

**Required Data Connectors**

Corelight

### Corelight - External Proxy Detected

Detects external proxy usage.

**Required Data Connectors**

Corelight

### Corelight - Forced External Outbound SMB

Detects SMB requests that originate internally and communicate with an external IP address.

**Required Data Connectors**

Corelight

### Corelight - Multiple Compressed Files Transferred over HTTP

Detects compressed archives transferre over HTTP.

**Required Data Connectors**

Corelight

### Corelight - Multiple files sent over HTTP with abnormal requests

Detects sources sending multiple compressed files greater than 10MBs sent over HTTP in a short amount of time.

**Required Data Connectors**

Corelight

### Corelight - Network Service Scanning Multiple IP Addresses

Identify scanning of services that may be available on the internal network.

**Required Data Connectors**

Corelight

### Corelight - Possible Webshell

Detects post requests to unusual extensions.

**Required Data Connectors**

Corelight

### Corelight - Possible Webshell (Rare PUT or POST)

Detects rare post requests to a single webserver location.

**Required Data Connectors**

Corelight

### Corelight - SMTP Email containing NON Ascii Characters within the Subject

Detects where an emails contain non ascii characters within the Subject.

**Required Data Connectors**

Corelight

### Corelight - Possible Typo Squatting or Punycode Phishing HTTP Request

Detects when an HTTP request was made to a domain that was using unicode/punycode.

**Required Data Connectors**

Corelight

## Hunting Queries

### Corelight - Abnormal Email Subject

Corelight Hunting Query 1

### Corelight - Compressed Files Transferred over HTTP

Corelight Hunting Query 2

### Corelight - Top sources of data transferred

Corelight Hunting Query 3

### Corelight - External Facing Services

Corelight Hunting Query 4

### Corelight - Files in logs

Corelight Hunting Query 5

### Corelight - File transferred by source

Corelight Hunting Query 6

### Corelight - Multiple Remote SMB Connections from single client

Corelight Hunting Query 7

### Corelight - Obfuscated binary filenames

Corelight Hunting Query 8

### Corelight - Rare PUT or POST

Corelight Hunting Query 9

### Corelight - Repetitive DNS Failures

Corelight Hunting Query 10

## Watchlists

## Playbooks

## Parsers

### Corelight

Category: Samples

Function Alias: Corelight

# CrowdStrike Falcon Endpoint Protection

The CrowdStrike Falcon Endpoint Protection connector allows you to easily connect your CrowdStrike Falcon Event Stream with Microsoft Sentinel, to create custom dashboards, alerts, and improve investigation.

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

## Data Connectors

### Crowdstrike Falcon Data Replicator (using Azure Function)

The [Crowdstrike](https://www.crowdstrike.com/) Falcon Data Replicator connector provides the capability to ingest raw event data from the [Falcon Platform](https://www.crowdstrike.com/blog/tech-center/intro-to-falcon-data-replicator/) events into Microsoft Sentinel. The connector provides ability to get events from Falcon Agents which helps to examine potential security risks, analyze your team's use of collaboration, diagnose configuration problems and more.

### CrowdStrike Falcon Endpoint Protection

The [CrowdStrike Falcon Endpoint Protection](https://www.crowdstrike.com/endpoint-security-products/) connector allows you to easily connect your CrowdStrike Falcon Event Stream with Microsoft Sentinel, to create custom dashboards, alerts, and improve investigation. This gives you more insight into your organization's endpoints and improves your security operation capabilities.

## Workbooks

### CrowdStrike Falcon Endpoint Protection

Sets the time name for analysis

**Required Data Types**

CrowdstrikeReplicatorLogs\_CL

CrowdstrikeReplicator

## Analytic Rules

### Critical or High Severity Detections by User

Creates an incident when a large number of Critical/High severity CrowdStrike Falcon sensor detections is triggered by a single user

**Required Data Connectors**

CrowdStrikeFalconEndpointProtection

### Critical Severity Detection

Creates an incident when a CrowdStrike Falcon sensor detection is triggered with a Critical Severity

**Required Data Connectors**

CrowdStrikeFalconEndpointProtection

## Hunting Queries

## Watchlists

## Playbooks

### Crowdstrike API authentication

This is Crowdstrike base template which is used to generate access token and this is used in actual crowdstrike templates. This playbook gets triggered when a new Http request is created and this is being called from other Crowdstrike playbooks.

### Endpoint enrichment - Crowdstrike

When a new Microsoft Sentinel incident is created, this playbook gets triggered and performs below actions:1. Fetches the device information from Crowdstrike 2. Enrich the incident with device information from Crowdstrike

### Isolate endpoint - Crowdstrike

When a new Microsoft Sentinel incident is created, this playbook gets triggered and performs below actions:1. Fetches the device information from Crowdstrike 2. Contain host if it is not already contained 3. Enrich the incident with device information from Crowdstrike

![Comment example](https://github.com/Azure/Azure-Sentinel/blob/master/Solutions/CrowdStrike%20Falcon%20Endpoint%20Protection/Playbooks/CrowdStrike\_ContainHost/images/Incident\_Comment.png?raw=true)

4. Close the incident if contained the host

## Parsers

### CrowdStrikeFalconEventStream

Category: Samples

Function Alias: CrowdStrikeFalconEventStream

### CrowdstrikeReplicator

Category: Samples

Function Alias: CrowdstrikeReplicator

# CyberArk Enterprise Password Vault (EPV)/Sentinel

The CyberArk Privileged Access Security connector allows you to connect your Digital Vault Syslog events with Azure Sentinel CEF Data Connector

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

## Data Connectors

### CyberArk Enterprise Password Vault (EPV) Events

CyberArk Enterprise Password Vault generates an xml Syslog message for every action taken against the Vault. The EPV will send the xml messages through the Sentinel.xsl translator to be converted into CEF standard format and sent to a syslog staging server of your choice (syslog-ng, rsyslog). The Log Analytics agent installed on your syslog staging server will import the messages into Microsoft Log Analytics. Refer to the [CyberArk documentation](https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/DV-Integrating-with-SIEM-Applications.htm) for more guidance on SIEM integrations.

## Workbooks

### CyberArk EPV Events

The CyberArk Syslog connector allows you to easily connect all your CyberArk security solution logs with your Microsoft Sentinel, to view dashboards, create custom alerts, and improve investigation. Integration between CyberArk and Microsoft Sentinel makes use of the CEF Data Connector to properly parse and display CyberArk Syslog messages.

**Required Data Types**

CommonSecurityLog

CyberArk

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# CyberArk EPM/Sentinel Integration

Extract security events from CyberArk Endpoint Privilege Manager (EPM) into Microsoft Sentinel

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

## Data Connectors

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Cyberpion Security Logs

Cyberpion connector to receive Action Items onto Microsoft Sentinel

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

## Data Connectors

### Cyberpion Security Logs

The Cyberpion Security Logs data connector, ingests logs from the Cyberpion system directly into Sentinel. The connector allows users to visualize their data, create alerts and incidents and improve security investigations.

## Workbooks

### Cyberpion Overview

Use Cyberpion's Security Logs and this workbook, to get an overview of your online assets, gain insights into their current state, and find ways to better secure your ecosystem.

**Required Data Types**

CyberpionActionItems\_CL

CyberpionSecurityLogs

## Analytic Rules

### High Urgency Cyberpion Action Items

This query creates an alert for active Cyberpion Action Items with high urgency (9-10).

Urgency can be altered using the "min\_urgency" variable in the query.

**Required Data Connectors**

CyberpionSecurityLogs

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Cybersecurity Maturity Model Certification (CMMC) 2.0

The Microsoft Sentinel: Cybersecurity Maturity Model Certification (CMMC) 2.0 Solution provides a mechanism for viewing log queries aligned to CMMC 2.0 requirements across the Microsoft portfolio.

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

## Data Connectors

## Workbooks

### CybersecurityMaturityModelCertificationCMMC2.0

**Required Data Types**

## Analytic Rules

### CMMC 2.0 Level 1 (Foundational) Readiness Posture

CMMC 2.0 Level 1 (Foundational) assessments have deviated from configured threshold baselines. This alert is triggered when CMMC2.0 policy compliance is assessed below 70% compliance in 7 days.

**Required Data Connectors**

(none listed)

### CMMC 2.0 Level 2 (Advanced) Readiness Posture

CMMC 2.0 Level 2 (Advanced) assessments have deviated from configured threshold baselines. This alert is triggered when CMMC2.0 policy compliance is assessed below 70% compliance in 7 days.

**Required Data Connectors**

(none listed)

## Hunting Queries

## Watchlists

## Playbooks

### Notify\_GovernanceComplianceTeam

This playbook will create the Azure DevOps task filled with the Microsoft Sentinel incident details.

### Create-AzureDevOpsTask

This playbook will create the Azure DevOps task filled with the Microsoft Sentinel incident details.

### Create Jira Issue

This playbook will open a Jira Issue when a new incident is opened in Microsoft Sentinel.

## Parsers

# Darktrace for Microsoft Sentinel

The Darktrace Microsoft Sentinel solution lets users connect Darktrace AI-based alerting in real-time with Microsoft Sentinel, allowing creation of custom Dashboards, Workbooks, Notebooks and Custom Alerts to improve investigation.

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

## Data Connectors

### Darktrace Connector for Microsoft Sentinel REST API

The Darktrace REST API connector pushes real-time events from Darktrace's Product Suite to Microsoft Sentinel and is designed to be used with the Darktrace Solution for Sentinel. The connector writes logs to a custom log table titled "darktrace\_model\_alerts\_CL"; Model Breaches, AI Analyst Incidents, System Alerts and Antigena Email alerts can be ingested - additional filters can be set up on Darktrace system configuration page. Data is pushed to Sentinel from Darktrace appliances, see [Customer Portal Setup Instructions for more information](https://customerportal.darktrace.com/product-guides/main/azure-sentinel-introduction).

## Workbooks

### Darktrace

The Darktrace Workbook visualises Model Breach and AI Analyst data received by the Darktrace Data Connector and visualises events across the network, SaaS, IaaS and Email.

**Required Data Types**

## Analytic Rules

### Darktrace Model Breach

This rule creates Microsoft Sentinel Alerts based on Darktrace Model Breaches, fetched every 5 minutes.

**Required Data Connectors**

DarktraceRESTConnector

### Darktrace AI Analyst

This rule creates Microsoft Sentinel Incidents based on Darktrace AI Analyst Incidents, fetched every 5 minutes.

**Required Data Connectors**

DarktraceRESTConnector

### Darktrace System Status

This rule creates Microsoft Sentinel Alerts based on Darktrace system status alerts for health monitoring, fetched every 5 minutes.

**Required Data Connectors**

DarktraceRESTConnector

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Delinea Secret Server for Microsoft Sentinel

Delinea's flagship Privileged Access Management (PAM) & Endpoint Security Least Privilege SaaS offer

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

## Data Connectors

### Delinea Secret Server

Common Event Format (CEF) from Delinea Secret Server

## Workbooks

### Delinea Secret Server Workbook

The Delinea Secret Server Syslog connector

**Required Data Types**

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Dev 0270 Detection and Hunting

Microsoft threat intelligence teams have been tracking multiple ransomware campaigns and have tied these attacks to DEV-0270.

**Data Connectors:** 0**, Workbooks:** 0**, Analytic Rules:** 3**, Hunting Queries:** 0**, Watchlists:** 0**, Playbooks:** 0, Parsers: 0

## Data Connectors

## Workbooks

## Analytic Rules

### Dev-0270 Malicious Powershell usage

DEV-0270 heavily uses powershell to achieve their objective at various stages of their attack. To locate powershell related activity tied to the actor, Microsoft Sentinel customers can run the following query.

**Required Data Connectors**

SecurityEvents

MicrosoftThreatProtection

### Dev-0270 Registry IOC - September 2022

The query below identifies modification of registry by Dev-0270 actor to disable security feature as well as to add ransom notes

**Required Data Connectors**

SecurityEvents

MicrosoftThreatProtection

### Dev-0270 WMIC Discovery

The query below identifies dllhost.exe using WMIC to discover additional hosts and associated domains in the environment.

**Required Data Connectors**

SecurityEvents

MicrosoftThreatProtection

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# DEV-0537 Detection and Hunting (Preview)

DEV-0537, also known as LAPSUS$ is known for using a pure extortion and destruction model without deploying ransomware payloads

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

## Data Connectors

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Digital Guardian Data Loss Prevention Solution

Digital Guardian is a data protection platform that discovers, classifies and controls data movement across endpoints, networks, and the cloud.

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 10**, Hunting Queries:** 10**, Watchlists:** 0**, Playbooks:** 0, Parsers: 1

## Data Connectors

### Digital Guardian Data Loss Prevention

[Digital Guardian Data Loss Prevention (DLP)](https://digitalguardian.com/platform-overview) data connector provides the capability to ingest Digital Guardian DLP logs into Microsoft Sentinel.

## Workbooks

### DigitalGuardianDLP

Sets the time name for analysis

**Required Data Types**

## Analytic Rules

### Digital Guardian - Sensitive data transfer over insecure channel

Detects sensitive data transfer over insecure channel.

**Required Data Connectors**

DigitalGuardianDLP

### Digital Guardian - Exfiltration using DNS protocol

Detects exfiltration using DNS protocol.

**Required Data Connectors**

DigitalGuardianDLP

### Digital Guardian - Exfiltration to online fileshare

Detects exfiltration to online fileshare.

**Required Data Connectors**

DigitalGuardianDLP

### Digital Guardian - Exfiltration to private email

Detects exfiltration to private email.

**Required Data Connectors**

DigitalGuardianDLP

### Digital Guardian - Exfiltration to external domain

Detects exfiltration to external domain.

**Required Data Connectors**

DigitalGuardianDLP

### Digital Guardian - Bulk exfiltration to external domain

Detects bulk exfiltration to external domain.

**Required Data Connectors**

DigitalGuardianDLP

### Digital Guardian - Multiple incidents from user

Detects multiple incidents from user.

**Required Data Connectors**

DigitalGuardianDLP

### Digital Guardian - Possible SMTP protocol abuse

Detects possible SMTP protocol abuse.

**Required Data Connectors**

DigitalGuardianDLP

### Digital Guardian - Unexpected protocol

Detects RDP protocol usage for data transfer which is not common.

**Required Data Connectors**

DigitalGuardianDLP

### Digital Guardian - Incident with not blocked action

Detects when incident has not block action.

**Required Data Connectors**

DigitalGuardianDLP

## Hunting Queries

### Digital Guardian - Incident domains

Digital Guardian Data Loss Prevention Hunting Query 1

### Digital Guardian - Files sent by users

Digital Guardian Data Loss Prevention Hunting Query 2

### Digital Guardian - Users' incidents

Digital Guardian Data Loss Prevention Hunting Query 3

### Digital Guardian - Insecure file transfer sources

Digital Guardian Data Loss Prevention Hunting Query 4

### Digital Guardian - Inspected files

Digital Guardian Data Loss Prevention Hunting Query 5

### Digital Guardian - New incidents

Digital Guardian Data Loss Prevention Hunting Query 6

### Digital Guardian - Rare destination ports

Digital Guardian Data Loss Prevention Hunting Query 7

### Digital Guardian - Rare network protocols

Digital Guardian Data Loss Prevention Hunting Query 8

### Digital Guardian - Rare Urls

Digital Guardian Data Loss Prevention Hunting Query 9

### Digital Guardian - Urls used

Digital Guardian Data Loss Prevention Hunting Query 10

## Watchlists

## Playbooks

## Parsers

### DigitalGuardianDLP Data Parser

Category: Samples

Function Alias: DigitalGuardianDLPEvent

# Digital Shadows SearchLight for Microsoft Sentinel

Seamlessly integrate SearchLight™ alerts into Microsoft Sentinel, giving you actionable intelligence where you need it most to orchestrate responses.

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

## Data Connectors

### Digital Shadows Searchlight (using Azure Function)

The Digital Shadows data connector provides ingestion of the incidents and alerts from Digital Shadows SearchLight into the Microsoft Sentinel using the REST API. The connector will provide the incidents and alerts information such that it helps to examine, diagnose and analyse the potential security risks and threats

## Workbooks

### Digital Shadows SearchLight

For gaining insights into Digital Shadows logs.

**Required Data Types**

DigitalShadows\_CL

DigitalShadowsSearchlightAzureFunctions

## Analytic Rules

### Digital Shadows Incident Creation for exclude-app

Digital Shadows Analytic rule for generating Sentinel incidents for the data ingested by app polling for excluded classifications

**Required Data Connectors**

DigitalShadows

### Digital Shadows Incident Creation for include-app

Digital Shadows Analytic rule for generating Sentinel incidents for the data ingested by app polling for included classifications

**Required Data Connectors**

DigitalShadows

## Hunting Queries

## Watchlists

## Playbooks

### Digital Shadows Playbook to Update Incident Status

This playbook will update the status of Microsoft Sentinel incidents to match the status of the alerts imported from Digital Shadows SearchLight1. This playbook triggers when a Microsoft Sentinel Alert is created by the Digital Shadows Data Connector 2. The status of the inbound Digital Shadows alert is inspected and the Microsoft Sentinel Incident status is updated to match

## Parsers

# DomainTools Iris Investigate for Microsoft Sentinel

Accelerate Analysis of Malicious Online Infrastructure. Analyze dozens of domain attributes including Risk Score, DNS, Whois, SSL, and more. Pivot through domain name attributes and expose meaningful connections between domains.

**Data Connectors:** 0**, Workbooks:** 0**, Analytic Rules:** 0**, Hunting Queries:** 0**, Watchlists:** 0**, Playbooks:** 7, Parsers: 0

## Data Connectors

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

### Domain Enrichment - DomainTools Iris Enrich

The DomainTools Iris Enrich API is more suited to high-volume API lookups than Iris Investigate and is able to provide domain infrastructure information for a domain or set of domains associated with an incident.

### Domain Enrichment - DomainTools Iris Investigate

Given a domain or set of domains associated with an incident return all Iris Investigate data for those domains as comments in the incident.

### Domain Risk Score - DomainTools Iris Investigate

Given a domain or set of domains associated with an incident return the risk scores and adjust the severity of the incident if a high risk domain is observed, adding the risk details in the comments of the incident.

### Guided Pivots - DomainTools Iris Investigate

Given a domain return all the Iris Investigate data, highlighting fields where < 200 domains share an attribute to clue investigators in to retrieve more data via Iris Investigate UI (or further queries using the Iris Investigate API).

### Malicious Tags - DomainTools Iris Investigate

Track the activities of malicious actors using the Iris Investigate UI, tagging domains of interest. Given a domain or set of domains associated with an incident, query Iris Investigate for information on those domains, and if a specified set of tags is observed, mark the incident as “severe” Sentinel and add a comment.

### URL Enrichment- DomainTools Iris Investigate

Given a URL or set of URLs associated with an incident return all Iris Investigate data for the extracted domains from the URL as comments in the incident.

### Domain Enrichment- DomainTools Iris Investigate With Farsight DNSDB

Given a domain or set of domains associated with an incident, enrich the domain using the DomainTools Iris Investigate API, returning whois and infrastructure details. Subsequently retrieve associated subdomains from passive DNS information seen in Farsight’s DNSDB.

## Parsers

# Dynamics 365 - Connector Only

The Dynamics 365 Dataverse Activity logs connector provides insight into admin and user activities.

This solution includes only the data connector.

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

## Data Connectors

### Dynamics365

The Dynamics 365 Common Data Service (CDS) activities connector provides insight into admin, user, and support activities, as well as Microsoft Social Engagement logging events. By connecting Dynamics 365 CRM logs into Microsoft Sentinel, you can view this data in workbooks, use it to create custom alerts, and improve your investigation process.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Dynatrace Software Intelligence Platform with Microsoft Sentinel

Secure your hybrid cloud environments at runtime with Dynatrace and Microsoft Sentinel leveraging runtime vulnerability analysis, AI-assisted prioritization, runtime application protection, as well as log audit and forensics.

**Data Connectors:** 4**, Workbooks:** 1**, Analytic Rules:** 5**, Hunting Queries:** 0**, Watchlists:** 0**, Playbooks:** 6, Parsers: 4

## Data Connectors

### Dynatrace Attacks

This connector uses the Dynatrace Attacks REST API to ingest detected attacks into Microsoft Sentinel Log Analytics

### Dynatrace Runtime Vulnerabilities

This connector uses the [Dynatrace Security Problem REST API](https://www.dynatrace.com/support/help/dynatrace-api/environment-api/application-security/security-problems) to ingest detected runtime vulnerabilities into Microsoft Sentinel Log Analytics.

### Dynatrace Problems

This connector uses the [Dynatrace Problem REST API](https://www.dynatrace.com/support/help/dynatrace-api/environment-api/problems-v2) to ingest problem events into Microsoft Sentinel Log Analytics

### Dynatrace Audit Logs

This connector uses the [Dynatrace Audit Logs REST API](https://www.dynatrace.com/support/help/dynatrace-api/environment-api/audit-logs) to ingest tenant audit logs into Microsoft Sentinel Log Analytics

## Workbooks

### Dynatrace

This workbook brings together queries and visualizations to assist you in identifying potential threats surfaced by Dynatrace.

**Required Data Types**

DynatraceAttacks\_CL

DynatraceAuditLogs\_CL

DynatraceProblems\_CL

DynatraceSecurityProblems\_CL

DynatraceAttacks

DynatraceAuditLogs

DynatraceProblems

DynatraceRuntimeVulnerabilities

## Analytic Rules

### Dynatrace Application Security - Attack detection

Dynatrace has detected an ongoing attack in your environment.

**Required Data Connectors**

DynatraceAttacks

### Dynatrace Application Security - Code-Level runtime vulnerability detection

Detect Code-level runtime vulnerabilities in your environment insights by snyk

**Required Data Connectors**

DynatraceRuntimeVulnerabilities

### Dynatrace Application Security - Third-Party runtime vulnerability detection

Detect Third-Party runtime vulnerabilities in your environment insights by snyk

**Required Data Connectors**

DynatraceRuntimeVulnerabilities

### Dynatrace Application Security - Non-critical runtime vulnerability detection

Detect runtime vulnerabilities in your environment insights by snyk

**Required Data Connectors**

DynatraceRuntimeVulnerabilities

### Dynatrace - Problem detection

Detect application & infrastructure problems in your environment

**Required Data Connectors**

DynatraceProblems

## Hunting Queries

## Watchlists

## Playbooks

### Add Dynatrace Application Security Attack Source IP Address to Threat Intelligence

This playbook will add an attackers source ip to Threat Intelligence when a new incident is opened in Microsoft Sentinel.

### Enrich Dynatrace Application Security Attack Incident

This playbook will enriche Dynatrace Application Security Attack Incidents with additional information when new incident is opened.

### Enrich Dynatrace Application Security Attack with related Microsoft Defender 365 insights

This playbook will enrich Dynatrace Application Security Attack with related Microsoft Defender 365 insights.

### Enrich Dynatrace Application Security Attack with related Microsoft Sentinel Security Alerts

This playbook will enrich Dynatrace Application Security Attack with related Microsoft Sentinel Security Alerts.

### Ingest Microsoft Defender 365 insights into Dynatrace

This playbook will ingest Microsoft Defender 365 insights into Dynatrace.

### Ingest Microsoft Sentinel Security Alerts into Dynatrace

This playbook will ingest Microsoft Sentinel Security Alerts into Dynatrace.

## Parsers

### DynatraceAttacks

Category: Samples

Function Alias: DynatraceAttacks

### DynatraceAuditLogs

Category: Samples

Function Alias: DynatraceAuditLogs

### DynatraceProblems

Category: Samples

Function Alias: DynatraceProblems

### DynatraceSecurityProblems

Category: Samples

Function Alias: DynatraceSecurityProblems

# Eaton Foreseer (Preview)

Stream application logs for Eaton Foreseer OT application into Microsoft Sentinel using MMA or AMA

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

## Data Connectors

## Workbooks

### EatonForeseerHealthAndAccess

This workbook gives an insight into the health of all the Windows VMs in this subscription running Eaton Foreseer and the unauthorized access into the Eaton Foreseer application running on these VMs.

**Required Data Types**

SecurityEvent

## Analytic Rules

### EatonForeseer - Unauthorized Logins

Detects Unauthorized Logins into Eaton Foreseer

**Required Data Connectors**

WindowsSecurityEvents

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Egress Defend Connector for Microsoft Sentinel

Egress Defend protects against data breaches with intelligent phishing protection, providing the information to ingest into Microsoft Sentinel via the Egress Defend rest API

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

## Data Connectors

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Elastic Agent Solution (Preview)

The Elastic Agent solution provides the capability to ingest Elastic Agent logs, metrics, and security data into Microsoft Sentinel.

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

## Data Connectors

### Elastic Agent (Standalone)

The [Elastic Agent](https://www.elastic.co/security) data connector provides the capability to ingest Elastic Agent logs, metrics, and security data into Microsoft Sentinel.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### ElasticAgent Data Parser

Category: Samples

Function Alias: ElasticAgentEvent

# Endpoint Threat Protection Essentials

The Endpoint Threat Protection Essentials solution provides content to monitor, detect and investigate threats related to windows machines.

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

## Data Connectors

## Workbooks

## Analytic Rules

### Base64 encoded Windows process command-lines

Identifies instances of a base64 encoded PE file header seen in the process command line parameter.

**Required Data Connectors**

SecurityEvents

WindowsSecurityEvents

WindowsSecurityEvents

WindowsForwardedEvents

### Dumping LSASS Process Into a File

Adversaries may attempt to access credential material stored in the process memory of the Local Security Authority Subsystem Service (LSASS).

After a user logs on, the system generates and stores a variety of credential materials in LSASS process memory.

These credential materials can be harvested by an administrative user or SYSTEM and used to conduct Lateral Movement using Use Alternate Authentication Material.

As well as in-memory techniques, the LSASS process memory can be dumped from the target host and analyzed on a local system.

Ref: https://attack.mitre.org/techniques/T1003/001/

**Required Data Connectors**

SecurityEvents

### Process executed from binary hidden in Base64 encoded file

Encoding malicious software is a technique used to obfuscate files from detection.

The first CommandLine component is looking for Python decoding base64.

The second CommandLine component is looking for Bash/sh command line base64 decoding.

The third one is looking for Ruby decoding base64.

**Required Data Connectors**

SecurityEvents

WindowsSecurityEvents

WindowsSecurityEvents

WindowsForwardedEvents

### Lateral Movement via DCOM

This query detects a fairly uncommon attack technique using the Windows Distributed Component Object Model (DCOM) to make a remote execution call to another computer system and gain lateral movement throughout the network.

Ref: http://thenegative.zone/incident%20response/2017/02/04/MMC20.Application-Lateral-Movement-Analysis.html

**Required Data Connectors**

SecurityEvents

### Detecting Macro Invoking ShellBrowserWindow COM Objects

This query detects a macro invoking ShellBrowserWindow COM Objects evade naive parent/child Office detection rules.

Ref: https://blog.menasec.net/2019/02/threat-hunting-doc-with-macro-invoking.html

**Required Data Connectors**

SecurityEvents

### Malware in the recycle bin

The query detects Windows binaries, that can be used for executing malware, that have been hidden in the recycle bin.

The list of these binaries are sourced from https://lolbas-project.github.io/

References: https://azure.microsoft.com/blog/how-azure-security-center-helps-reveal-a-cyberattack/.

**Required Data Connectors**

SecurityEvents

WindowsSecurityEvents

WindowsSecurityEvents

WindowsForwardedEvents

### Potential Remote Desktop Tunneling

This query detects remote desktop authentication attempts with a localhost source address which can indicate a tunneled login.

Ref: https://www.mandiant.com/resources/bypassing-network-restrictions-through-rdp-tunneling

**Required Data Connectors**

SecurityEvents

### Registry Persistence via AppCert DLL Modification

Adversaries may establish persistence and/or elevate privileges by executing malicious content triggered by AppCert DLLs loaded into processes.

Dynamic-link libraries (DLLs) that are specified in the AppCertDLLs Registry key under HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\Session Manager\ are loaded into every process that calls the ubiquitously used application programming interface (API) functions CreateProcess, CreateProcessAsUser, CreateProcessWithLoginW, CreateProcessWithTokenW, or WinExec.

Ref: https://attack.mitre.org/techniques/T1546/009/

**Required Data Connectors**

SecurityEvents

### Registry Persistence via AppInit DLLs Modification

Adversaries may establish persistence and/or elevate privileges by executing malicious content triggered by AppInit DLLs loaded into processes.

Dynamic-link libraries (DLLs) that are specified in the AppInit\_DLLs value in the Registry keys HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows or HKEY\_LOCAL\_MACHINE\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows are loaded by user32.dll into every process that loads user32.dll. In practice this is nearly every program, since user32.dll is a very common library.

Ref: https://attack.mitre.org/techniques/T1546/010/

**Required Data Connectors**

SecurityEvents

### Security Event log cleared

Checks for event id 1102 which indicates the security event log was cleared.

It uses Event Source Name "Microsoft-Windows-Eventlog" to avoid generating false positives from other sources, like AD FS servers for instance.

**Required Data Connectors**

SecurityEvents

WindowsSecurityEvents

WindowsForwardedEvents

### WDigest downgrade attack

When the WDigest Authentication protocol is enabled, plain text passwords are stored in the Local Security Authority Subsystem Service (LSASS) exposing them to theft. This setting will prevent WDigest from storing credentials in memory.

Ref: https://www.stigviewer.com/stig/windows\_7/2016-12-19/finding/V-72753

**Required Data Connectors**

SecurityEvents

### Windows Binaries Executed from Non-Default Directory

The query detects Windows binaries, that can be executed from a non-default directory (e.g. C:\Windows\, C:\Windows\System32 etc.).

Ref: https://lolbas-project.github.io/

**Required Data Connectors**

SecurityEvents

### Windows Binaries Lolbins Renamed

This query detects the execution of renamed Windows binaries (Lolbins). This is a common technique used by adversaries to evade detection.

Ref: https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-analytics-alert-reference/cortex-xdr-analytics-alert-reference/execution-of-renamed-lolbin.html

**Required Data Connectors**

SecurityEvents

## Hunting Queries

### Backup Deletion

Endpoint Threat Protection Essentials Hunting Query 1

### Certutil (LOLBins and LOLScripts)

Endpoint Threat Protection Essentials Hunting Query 2

### Execution of File with One Character in the Name

Endpoint Threat Protection Essentials Hunting Query 3

### Persisting Via IFEO Registry Key

Endpoint Threat Protection Essentials Hunting Query 4

### Potential Microsoft security services tampering

Endpoint Threat Protection Essentials Hunting Query 5

### Remote Login Performed with WMI

Endpoint Threat Protection Essentials Hunting Query 6

### Remote Scheduled Task Creation or Update using ATSVC Named Pipe

Endpoint Threat Protection Essentials Hunting Query 7

### Scheduled Task Creation or Update from User Writable Directory

Endpoint Threat Protection Essentials Hunting Query 8

### Rundll32 (LOLBins and LOLScripts)

Endpoint Threat Protection Essentials Hunting Query 9

### Unicode Obfuscation in Command Line

Endpoint Threat Protection Essentials Hunting Query 10

## Watchlists

## Playbooks

## Parsers

# ESET Inspect integration for Microsoft Sentinel

Use the ESET Inspect REST API to grab all detections and ingest them into Microsoft Sentinel.

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

## Data Connectors

### ESET Inspect (using Azure Function)

This connector will ingest detections from [ESET Inspect](https://www.eset.com/int/business/solutions/xdr-extended-detection-and-response/) using the provided [REST API](https://help.eset.com/ei\_navigate/latest/en-US/api.html). This API is present in ESET Inspect version 1.4 and later.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# ESET PROTECT integration for Azure Sentinel

This integration offers a custom KQL function that maps the fields received though ESET PROTECT syslog output to standard fields.

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

## Data Connectors

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Exabeam Advanced Analytics

The Exabeam Advanced Analytics data connector provides the capability to ingest Exabeam Advanced Analytics events into Microsoft Sentinel.

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

## Data Connectors

### Exabeam Advanced Analytics

The [Exabeam Advanced Analytics](https://www.exabeam.com/ueba/advanced-analytics-and-mitre-detect-and-stop-threats/) data connector provides the capability to ingest Exabeam Advanced Analytics events into Azure Sentinel. Refer to [Exabeam Advanced Analytics documentation](https://docs.exabeam.com/) for more information.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### ExabeamEvent

Category: Samples

Function Alias: ExabeamEvent

# ExtraHop Reveal(x) for Microsoft Sentinel

The ExtraHop Reveal(x) Integration to Microsoft Sentinel allows you to view your essential Network Detection & Response (NDR) data in new ways utilizing Microsoft Sentinel.

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

## Data Connectors

### ExtraHop Reveal(x)

The ExtraHop Reveal(x) data connector enables you to easily connect your Reveal(x) system with Microsoft Sentinel to view dashboards, create custom alerts, and improve investigation. This integration gives you the ability to gain insight into your organization's network and improve your security operation capabilities.

## Workbooks

### ExtraHop

Gain insights into ExtraHop Reveal(x) detections by analyzing traffic and activities.

This workbook provides an overview of security detections in your organization's network, including high-risk detections and top participants.

**Required Data Types**

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# F5 Advanced WAF Integration via Syslog/CEF for Microsoft Sentinel

F5’s industry-leading BIG-IP Advanced Web Application Firewall (WAF) provides comprehensive application protection against threats and can be integrated with Microsoft Sentinel to analyze attack events and data in real-time.

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

## Data Connectors

### F5 Networks

The F5 firewall connector allows you to easily connect your F5 logs with Microsoft Sentinel, to view dashboards, create custom alerts, and improve investigation. This gives you more insight into your organization's network and improves your security operation capabilities.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# F5 Advanced WAF Integration via Telemetry Streaming for Microsoft Sentinel

F5’s industry-leading BIG-IP Advanced Web Application Firewall (WAF) provides comprehensive application protection against threats and can be integrated with Microsoft Sentinel to analyze attack events and data in real-time.

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

## Data Connectors

### F5 BIG-IP

The F5 firewall connector allows you to easily connect your F5 logs with Microsoft Sentinel, to view dashboards, create custom alerts, and improve investigation. This gives you more insight into your organization's network and improves your security operation capabilities.

## Workbooks

### F5 BIG-IP System Metrics

Gain insight into F5 BIG-IP health and performance. This workbook provides visibility of various metrics including CPU, memory, connectivity, throughput and disk utilization.

**Required Data Types**

F5Telemetry\_system\_CL

F5Telemetry\_AVR\_CL

F5BigIp

### F5 BIG-IP ASM

Gain insights into F5 BIG-IP Application Security Manager (ASM), by analyzing traffic and activities.

This workbook provides insight into F5's web application firewall events and identifies attack traffic patterns across multiple ASM instances as well as overall BIG-IP health.

**Required Data Types**

F5Telemetry\_LTM\_CL

F5Telemetry\_system\_CL

F5Telemetry\_ASM\_CL

F5BigIp

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# FalconForce FalconFriday Analytics for Microsoft Sentinel

This content is free and developed by FalconForce. These rules are published together with blog posts explaining their focus and how to work with them

You can find these posts here: https://medium.com/falconforce

**Data Connectors:** 0**, Workbooks:** 0**, Analytic Rules:** 30**, Hunting Queries:** 0**, Watchlists:** 0**, Playbooks:** 0, Parsers: 0

## Data Connectors

## Workbooks

## Analytic Rules

### ASR Bypassing Writing Executable Content

The query checks for any file which has been created/written by an Office application and shortly after renamed to one of the deny-listed "executable extensions" which are text files. (e.g. ps1, .js, .vbs).

**Required Data Connectors**

MicrosoftThreatProtection

### Azure AD Rare UserAgent App Sign-in

This query establishes a baseline of the type of UserAgent (i.e. browser, office application, etc) that is typically used for a particular application by looking back for a number of days.

It then searches the current day for any deviations from this pattern, i.e. types of UserAgents not seen before in combination with this application.

**Required Data Connectors**

AzureActiveDirectory

AzureActiveDirectory

### Azure AD UserAgent OS Missmatch

This query extracts the operating system from the UserAgent header and compares this to the DeviceDetail information present in Azure Active Directory.

**Required Data Connectors**

AzureActiveDirectory

AzureActiveDirectory

### Component Object Model Hijacking - Vault7 trick

This detection looks for the very specific value of "Attribute" in the "ShellFolder" CLSID of a COM object. This value (0xf090013d) seems to only link back to this specific persistence method.

The blog post linked here (https://www.ired.team/offensive-security/code-execution/forcing-iexplore.exe-to-load-a-malicious-dll-via-com-abuse) provides more background on the meaning of this value.

**Required Data Connectors**

MicrosoftThreatProtection

### Certified Pre-Owned - TGTs requested with certificate authentication

This query identifies someone using machine certificates to request Kerberos Ticket Granting Tickets (TGTs).

**Required Data Connectors**

SecurityEvents

### Certified Pre-Owned - backup of CA private key - rule 1

This query identifies someone that performs a read operation of they CA key from the file.

**Required Data Connectors**

SecurityEvents

### Certified Pre-Owned - backup of CA private key - rule 2

This query identifies someone that performs a backup of they CA key.

**Required Data Connectors**

SecurityEvents

### Ingress Tool Transfer - Certutil

This detection addresses most of the known ways to utilize this binary for malicious/unintended purposes.

It attempts to accommodate for most detection evasion techniques, like commandline obfuscation and binary renaming.

**Required Data Connectors**

MicrosoftThreatProtection

### Access Token Manipulation - Create Process with Token

This query detects the use of the 'runas' command and checks whether the account used to elevate privileges isn't the user's own admin account.

Additionally, it will match this event to the logon events - to check whether it has been successful as well as augment the event with the new SID.

**Required Data Connectors**

MicrosoftThreatProtection

### DCOM Lateral Movement

This detection looks for cases of close-time proximity between incoming network traffic on RPC/TCP, followed by the creation of a DCOM object, followed by the creation of a child process of the DCOM object.

The query first identifies incoming network traffic over RPC/TCP, followed by the creation of a DCOM object (process) within 2 seconds, followed by the creation of a child process of this DCOM object.

**Required Data Connectors**

MicrosoftThreatProtection

### Hijack Execution Flow - DLL Side-Loading

This detection tries to identify all DLLs loaded by "high integrity" processes and cross-checks the DLL paths against FileCreate/FileModify events of the same DLL by a medium integrity process.

Of course, we need to do some magic to filter out false positives as much as possible. So any FileCreate/FileModify done by "NT Authoriy\System" and the "RID 500" users aren't interesting.

Also, we only want to see the FileCreate/FileModify actions which are performed with a default or limited token elevation. If done with a full elevated token, the user is apparently admin already.

**Required Data Connectors**

MicrosoftThreatProtection

### Disable or Modify Windows Defender

This detection watches the commandline logs for known commands that are used to disable the Defender AV. This is based on research performed by @olafhartong on a large sample of malware for varying purposes.

Note that this detection is imperfect and is only meant to serve as basis for building a more resilient detection rule.

Make the detection more resilient, currently the order of parameters matters. You don't want that for a production rule.

See blogpost (https://medium.com/falconforce/falconfriday-av-manipulation-0xff0e-67ed4387f9ab?source=friends\_link&sk=3c7c499797bbb4d74879e102ef3ecf8f)

for more resilience considerations. The current approach can easily be bypassed by not using the powershell.exe executable.

Consider adding more ways to detect this behavior.

**Required Data Connectors**

MicrosoftThreatProtection

### Detect .NET runtime being loaded in JScript for code execution

This query detects .NET being loaded from wscript or cscript to run .NET code, such as cactustorch and sharpshooter.

All based on the DotNetToJScript by James Foreshaw documented here https://github.com/tyranid/DotNetToJScript.

**Required Data Connectors**

MicrosoftThreatProtection

### Excessive share permissions

The query searches for event 5143, which is triggered when a share is created or changed and includes de share permissions.

First it checks to see if this is a whitelisted share for the system (e.g. domaincontroller netlogon, printserver print$ etc.).

The share permissions are then checked against 'allow' rule (A) for a number of well known overly permissive groups, like all users, guests, authenticated users etc.

If these are found, an alert is raised so the share creation may be audited.

Note: this rule only checks for changed permissions, to prevent repeat alerts if for example a comment is changed, but the permissions are not altered.

**Required Data Connectors**

SecurityEvents

### Expired access credentials being used in Azure

This query searches for logins with an expired access credential (for example an expired cookie). It then matches the IP address from which the expired credential access occurred with the IP addresses of successful logins.

If there are logins with expired credentials, but no successful logins from an IP, this might indicate an attacker has copied the authentication cookie and is re-using it on another machine.

**Required Data Connectors**

AzureActiveDirectory

### Match Legitimate Name or Location - 2

Attackers often match or approximate the name or location of legitimate files to avoid detection rules that are based trust of certain operating system processes.

This query detects mismatches in the parent-child relationship of core operating system processes to uncover different masquerading attempts.

**Required Data Connectors**

MicrosoftThreatProtection

### Office ASR rule triggered from browser spawned office process.

The attacker sends a spearphishing email to a user. The email contains a link which points to a website that eventually

presents the user a download of an MS Office document. This document contains a malicious macro. The macro triggers one of the ASR rules.

This detection looks for Office ASR violations triggered by an Office document opened from a browser.

Note: be aware that you need to have the proper ASR rules enabled for this detection to work.

**Required Data Connectors**

MicrosoftThreatProtection

### Suspicious Process Injection from Office application

This query detects process injections using CreateRemoteThread, QueueUserAPC or SetThread context APIs, originating from an Office process (only Word/Excel/PowerPoint)

that might contains macros. Performing process injection from a macro is a common technique by attackers to escape out of the Office process into something

longer running.

**Required Data Connectors**

MicrosoftThreatProtection

### Oracle suspicious command execution

The query searches process creation events that are indicative of an attacker spawning OS commands from an Oracle database.

**Required Data Connectors**

MicrosoftThreatProtection

### Password Spraying

This query detects a password spraying attack, where a single machine has performed a large number of failed login attempts, with a large number of different accounts.

For each account, the attacker uses just a few attempts to prevent account lockout. This query uses the DeviceLogonEvents per machine to detect a password spraying attacks.

The machine against which the password spraying is performed (can be DC, a server or even an endpoint) needs to be enrolled in Microsoft Defender for Endpoint.

**Required Data Connectors**

MicrosoftThreatProtection

### Beacon Traffic Based on Common User Agents Visiting Limited Number of Domains

This query searches web proxy logs for a specific type of beaconing behavior by joining a number of sources together:

- Traffic by actual web browsers - by looking at traffic generated by a UserAgent that looks like a browser and is used by multiple users

to visit a large number of domains.

- Users that make requests using one of these actual browsers, but only to a small set of domains, none of which are common domains.

- The traffic is beacon-like; meaning that it occurs during many different hours of the day (i.e. periodic).

**Required Data Connectors**

Zscaler

### Remote Desktop Protocol - SharpRDP

This detection monitors for the behavior that SharpRDP exhibits on the target system. The most relevant is leveraging taskmgr.exe to gain elevated execution, which means that taskmgr.exe is creating unexpected child processes.

**Required Data Connectors**

MicrosoftThreatProtection

### Rename System Utilities

Attackers often use LOLBINs that are renamed to avoid detection rules that are based on filenames.

This rule detects renamed LOLBINs by first searching for all the known SHA1 hashes of the LOLBINs in your DeviceProcessEvents. This list is then used as reference to find other files executed which have a name that doesn't match the original filename.

This query is really heavy on resources. Use it with care.

**Required Data Connectors**

MicrosoftThreatProtection

### SMB/Windows Admin Shares

This query is based on detecting incoming RPC/TCP on the SCM, followed by the start of a child process of services.exe. Remotely interacting with the SCM triggers the RPC/TCP traffic on services.exe, and the creation of the child processes is a result of starting the service.

The query might look intimidating given its size. That's why we've commented the query per logic block to walk you through the details.

**Required Data Connectors**

MicrosoftThreatProtection

### Suspicious named pipes

This query looks for Named Pipe events that either contain one of the known IOCs or make use of patterns that can be linked to CobaltStrike usage.

**Required Data Connectors**

MicrosoftThreatProtection

### Suspicious parentprocess relationship - Office child processes.

The attacker sends a spearphishing email to a user. The email contains a link, which points to a website that eventually

presents the user a download of an MS Office document. This document contains a malicious macro. The macro spawns a new child process providing initial access.

This detection looks for suspicious parent-process chains starting with a browser which spawns an Office application which spawns something else.

**Required Data Connectors**

MicrosoftThreatProtection

### Trusted Developer Utilities Proxy Execution

This detection looks at process executions - in some cases with specific command line attributes to filter a lot of common noise.

**Required Data Connectors**

MicrosoftThreatProtection

### Detecting UAC bypass - elevated COM interface

This query identifies processes spawned with high integrity from dllhost.exe with a command line that contains one of three specific CLSID GUIDs.

**Required Data Connectors**

MicrosoftThreatProtection

### Detecting UAC bypass - modify Windows Store settings

This query identifies modification a specific registry key and then launching wsreset.exe that resets the Windows Store settings.

**Required Data Connectors**

MicrosoftThreatProtection

### Detecting UAC bypass - ChangePK and SLUI registry tampering

This query identifies setting a registry key under HKCU, launching slui.exe and then ChangePK.exe.

**Required Data Connectors**

MicrosoftThreatProtection

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Farsight DNSDB for Microsoft Sentinel

Farsight Security DNSDB is the world's largest DNS intelligence database that provides a fact-based view of the configuration of the global Internet infrastructure. Farsight collects, filters, and verifies Passive DNS data from its global sensor array.

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

## Data Connectors

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# FireEye Network Security

FireEye Network Security supplements these solutions by rapidly detecting both known and unknown attacks with high accuracy and few false positives, while facilitating an efficient response for each alert

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

## Data Connectors

### FireEye Network Security (NX)

The [FireEye Network Security (NX)](https://www.fireeye.com/products/network-security.html) data connector provides the capability to ingest FireEye Network Security logs into Microsoft Sentinel.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### FireEyeNXEvent

Category: Samples

Function Alias: FireEyeNXEvent

# Flare for Microsoft Sentinel

Flare identifies your company’s digital assets made publicly available due to human error or malicious attacks.

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

## Data Connectors

### Flare

[Flare](https://flare.systems/platform/) connector allows you to receive data and intelligence from Flare on Microsoft Sentinel.

## Workbooks

### FlareSystemsFirework

Select the time range for this Overview.

**Required Data Types**

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

### credential-warning

This playbook monitors all data received from Firework looking for leaked credentials (email:password combinations). When found, this playbook will send an email to the email address warning their password has been leaked, recommending appropriate measures if necessary. To learn more about how to connect Firework to Microsoft Sentinel, see the [API documentation](https://docs.flared.io/azure-sentinel-integration).

## Parsers

# Forcepoint CASB

The Forcepoint CASB (Cloud Access Security Broker) Solution for Microsoft Sentinel allows you to automatically export CASB logs and events into Microsoft Sentinel in real-time.

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

## Data Connectors

### Forcepoint CASB

The Forcepoint CASB (Cloud Access Security Broker) Connector allows you to automatically export CASB logs and events into Microsoft Sentinel in real-time. This enriches visibility into user activities across locations and cloud applications, enables further correlation with data from Azure workloads and other feeds, and improves monitoring capability with Workbooks inside Microsoft Sentinel.

## Workbooks

### Forcepoint Cloud Access Security Broker (CASB)

Get insights on user risk with the Forcepoint CASB (Cloud Access Security Broker) workbook.

**Required Data Types**

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Forcepoint CSG

Forcepoint Cloud Security Gateway (CSG) Solution for Microsoft Sentinel exports web and/or email logs so that custom dashboards can be created using Workbooks to visualize events and insights on activities of Forcepoint Cloud Security Gateway.

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

## Data Connectors

### Forcepoint CSG

Forcepoint Cloud Security Gateway is a converged cloud security service that provides visibility, control, and threat protection for users and data, wherever they are. For more information visit: https://www.forcepoint.com/product/cloud-security-gateway

## Workbooks

### Forcepoint Cloud Security Gateway Workbook

Use this report to understand query runs across your workspace.

**Required Data Types**

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Forcepoint DLP

The Forcepoint DLP (Data Loss Prevention) Solution for Microsoft Sentinel allows you to automatically export DLP incident data from Forcepoint DLP into Microsoft Sentinel in real-time.

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

## Data Connectors

### Forcepoint DLP

The Forcepoint DLP (Data Loss Prevention) connector allows you to automatically export DLP incident data from Forcepoint DLP into Microsoft Sentinel in real-time. This enriches visibility into user activities and data loss incidents, enables further correlation with data from Azure workloads and other feeds, and improves monitoring capability with Workbooks inside Microsoft Sentinel.

## Workbooks

### Forcepoint Data Loss Prevention (DLP)

Get insights on DLP incidents with the Forcepoint DLP (Data Loss Prevention) workbook.

**Required Data Types**

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Forcepoint NGFW

The Forcepoint NGFW (Next Generation Firewall) Solution for Microsoft Sentinel allows you to automatically export user defined Forcepoint NGFW logs into Microsoft Sentinel in real-time.

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

## Data Connectors

### Forcepoint NGFW

The Forcepoint NGFW (Next Generation Firewall) connector allows you to automatically export user-defined Forcepoint NGFW logs into Microsoft Sentinel in real-time. This enriches visibility into user activities recorded by NGFW, enables further correlation with data from Azure workloads and other feeds, and improves monitoring capability with Workbooks inside Microsoft Sentinel.

## Workbooks

### Forcepoint Next Generation Firewall (NGFW)

Get insights on firewall activities with the Forcepoint NGFW (Next Generation Firewall) workbook.

**Required Data Types**

### Forcepoint Next Generation Firewall (NGFW) Advanced Workbook

Gain threat intelligence correlated security and application insights on Forcepoint NGFW (Next Generation Firewall). Monitor Forcepoint logging servers health.

**Required Data Types**

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Forescout

The Forescout solution provides the capability to ingest Forescout events into Microsoft Sentinel.

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

## Data Connectors

### Forescout

The [Forescout](https://www.forescout.com/) data connector provides the capability to ingest [Forescout events](https://docs.forescout.com/bundle/syslog-3-6-1-h/page/syslog-3-6-1-h.How-to-Work-with-the-Syslog-Plugin.html) into Microsoft Sentinel. Refer to [Forescout documentation](https://docs.forescout.com/bundle/syslog-msg-3-6-tn/page/syslog-msg-3-6-tn.About-Syslog-Messages-in-Forescout.html) for more information.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### Forescout Data Parser

Category: Samples

Function Alias: ForescoutEvent

# Forescout eyeExtend for Microsoft Sentinel

Forescout eyeExtend for Microsoft Sentinel integration reports IP addresses of the hosts that are involved in various categories of malicious attacks. Microsoft Sentinel then determines the severity & triggers Forescout to perform network-based mitigation.

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

## Data Connectors

### Forescout Host Property Monitor

The Forescout Host Property Monitor connector allows you to connect host properties from Forescout platform with Microsoft Sentinel, to view, create custom incidents, and improve investigation. This gives you more insight into your organization network and improves your security operation capabilities.

## Workbooks

## Analytic Rules

### Forescout-DNS\_Sniff\_Event\_Monitor

This rule creates an incident when more than certain number of Dnsniff events are generated from a host

**Required Data Connectors**

(none listed)

## Hunting Queries

## Watchlists

## Playbooks

### Forescout-DNS\_Sniff\_Event\_Playbook

This playbook will update incident with action to perform on endpoint

## Parsers

# Fortinet FortiGate

The Fortinet FortiGate Next-generation Firewall Solution for Microsoft Sentinel allows you to easily connect your FortiGate logs with Microsoft Sentinel, to view dashboards, create custom alerts, and improve investigation.

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

## Data Connectors

### Fortinet

The Fortinet firewall connector allows you to easily connect your Fortinet logs with Microsoft Sentinel, to view dashboards, create custom alerts, and improve investigation. This gives you more insight into your organization's network and improves your security operation capabilities.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

### Fortinet-FortiGate-IPEnrichment

This playbook enriches the incident with address object and address group.When a new Microsoft Sentinel is created, this playbook gets triggered and performs below actions:

- It fetches details of the address object.

- It retrieve the details of address groups which address object is belongs to.

- Add the Summary of address object and its groups details to an incident.

### Fortinet-FortiGate-ResponseOnBlockIP

This playbook allows the SOC users to automatically response to Microsoft Sentinel incidents which includes IPs, by adding/removing the IPs to the Sentinel IP blocked group.

### Fortinet-FortiGate-ResponseOnBlockURL

This playbook allows the SOC users to automatically response to Microsoft Sentinel incidents which includes URL's, by adding the URLs to the Sentinel URL blocked group.

## Parsers

# Fortinet FortiWeb Cloud

The Fortinet FortiWeb Cloud solution for Microsoft Sentinel provides an automated approach for SecOps

**Data Connectors:** 0**, Workbooks:** 0**, Analytic Rules:** 0**, Hunting Queries:** 0**, Watchlists:** 0**, Playbooks:** 2, Parsers: 0

## Data Connectors

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

### Block IP & URL on fortiweb cloud

This Playbook Provides the automation on blocking the suspicious/malicious IP and URL on fortiweb cloud waf

### Fetch Threat Intel from fortiwebcloud

This playbook provides/updates the threat intel and essential details in comments section of triggered incident so that SOC analysts can directly take corrective measure to stop the attack

## Parsers

# Gitlab

The GitLab connector allows you to easily connect your GitLab (GitLab Enterprise Edition - Standalone) logs with Microsoft Sentinel. This gives you more security insight into your organization's DevOps pipelines.

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

## Data Connectors

### GitLab

The [GitLab](https://about.gitlab.com/solutions/devops-platform/) connector allows you to easily connect your GitLab (GitLab Enterprise Edition - Standalone) logs with Microsoft Sentinel. This gives you more security insight into your organization's DevOps pipelines.

## Workbooks

## Analytic Rules

### GitLab - Brute-force Attempts

This query relies on GitLab Application Logs to get failed logins to highlight brute-force attempts from different IP addresses in a short space of time.

**Required Data Connectors**

Syslog

### GitLab - External User Added to GitLab

This queries GitLab Application logs to list external user accounts (i.e.: account not in allow-listed domains) which have been added to GitLab users.

**Required Data Connectors**

Syslog

### GitLab - User Impersonation

This queries GitLab Audit Logs for user impersonation. A malicious operator or a compromised admin account could leverage the impersonation feature of GitLab to change code or

repository settings bypassing usual processes. This hunting queries allows you to track the audit actions done under impersonation.

**Required Data Connectors**

Syslog

### GitLab - Local Auth - No MFA

This query checks GitLab Audit Logs to see if a user authenticated without MFA. Ot might mean that MFA was disabled for the GitLab server or that an external authentication provider was bypassed. This rule focuses on 'admin' privileges but the parameter can be adapted to also include all users.

**Required Data Connectors**

Syslog

### GitLab - TI - Connection from Malicious IP

This query correlates Threat Intelligence data from Sentinel with GitLab NGINX Access Logs (available in GitLab CE as well) to identify access from potentially TI-flagged IPs.

**Required Data Connectors**

ThreatIntelligence

ThreatIntelligenceTaxii

Syslog

### GitLab - Personal Access Tokens creation over time

This queries GitLab Audit Logs for access tokens. Attacker can exfiltrate data from you GitLab repository after gaining access to it by generating or hijacking access tokens.

This hunting queries allows you to track the personal access tokens creation for each of your repositories.

The visualization allow you to quickly identify anomalies/excessive creation, to further investigate repo access & permissions.

**Required Data Connectors**

Syslog

### GitLab - Repository visibility to Public

This query leverages GitLab Audit Logs. A repository in GitLab changed visibility from Private or Internal to Public which could indicate compromise, error or misconfiguration leading to exposing the repository to the public.

**Required Data Connectors**

Syslog

### GitLab - Abnormal number of repositories deleted

This hunting queries identify an unusual increase of repo deletion activities adversaries may want to disrupt availability or compromise integrity by deleting business data.

**Required Data Connectors**

Syslog

### GitLab - SSO - Sign-Ins Burst

This query relies on Azure Active Directory sign-in activity when Azure AD is used for SSO with GitLab to highlights GitLab accounts associated with multiple authentications from different geographical locations in a short space of time.

**Required Data Connectors**

AzureActiveDirectory

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### GitLabAccess

Category: Samples

Function Alias: GitLabAccess

### GitLabApp

Category: Samples

Function Alias: GitLabApp

### GitLabAudit

Category: Samples

Function Alias: GitLabAudit

# Google ApigeeX

The Google ApigeeX solution provides the capability to ingest ApigeeX audit logs into Azure Sentinel using the GCP Logging API. Refer to GCP Logging API documentation for more information.

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

## Data Connectors

### Google ApigeeX (using Azure Function)

The [Google ApigeeX](https://cloud.google.com/apigee/docs) data connector provides the capability to ingest ApigeeX audit logs into Microsoft Sentinel using the GCP Logging API. Refer to [GCP Logging API documentation](https://cloud.google.com/logging/docs/reference/v2/rest) for more information.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### ApigeeX

Category: Samples

Function Alias: ApigeeX

# Google Cloud Platform Cloud Monitoring Solution

Monitor hybrid and multicloud environments, and gain visibility into the performance, availability, and health of your applications and infrastructure.

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

## Data Connectors

### Google Cloud Platform Cloud Monitoring (using Azure Function)

The Google Cloud Platform Cloud Monitoring data connector provides the capability to ingest [GCP Monitoring metrics](https://cloud.google.com/monitoring/api/metrics\_gcp) into Microsoft Sentinel using the GCP Monitoring API. Refer to [GCP Monitoring API documentation](https://cloud.google.com/monitoring/api/v3) for more information.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### Google Cloud Platform Cloud Monitoring Data Parser

Category: Samples

Function Alias: GCP\_MONITOR

# Google Cloud Platform DNS Solution

Google Cloud Platform Domain Name System (DNS) is a high-performance, resilient, global Domain Name System (DNS) service.

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 11**, Hunting Queries:** 10**, Watchlists:** 0**, Playbooks:** 0, Parsers: 1

## Data Connectors

### Google Cloud Platform DNS (using Azure Function)

The Google Cloud Platform DNS data connector provides the capability to ingest [Cloud DNS query logs](https://cloud.google.com/dns/docs/monitoring#using\_logging) and [Cloud DNS audit logs](https://cloud.google.com/dns/docs/audit-logging) into Microsoft Sentinel using the GCP Logging API. Refer to [GCP Logging API documentation](https://cloud.google.com/logging/docs/api) for more information.

## Workbooks

### Google Cloud Platform DNS

Sets the time name for analysis

**Required Data Types**

GCPCloudDNS

GCPDNSDataConnector

## Analytic Rules

### Google DNS - Possible data exfiltration

Detects possible data exfiltration.

**Required Data Connectors**

GCPDNSDataConnector

### Google DNS - Exchange online autodiscover abuse

Detects possible Exchange online autodiscover abuse.

**Required Data Connectors**

GCPDNSDataConnector

### Google DNS - CVE-2021-40444 exploitation

Detects CVE-2021-40444 exploitation.

**Required Data Connectors**

GCPDNSDataConnector

### Google DNS - IP check activity

Detects requests to ip lookup resources.

**Required Data Connectors**

GCPDNSDataConnector

### Google DNS - Request to dynamic DNS service

Detects requests to ip lookup resources.

**Required Data Connectors**

GCPDNSDataConnector

### Google DNS - Malicous Python packages

Detects requests to resources with malicious Python packages.

**Required Data Connectors**

GCPDNSDataConnector

### Google DNS - Multiple errors for source

Detects multiple errors for the same source IP address.

**Required Data Connectors**

GCPDNSDataConnector

### Google DNS - Multiple errors to same domain

Detects multiple errors to same domain.

**Required Data Connectors**

GCPDNSDataConnector

### Google DNS - CVE-2021-34527 (PrintNightmare) external exploit

Detects CVE-2021-34527 (PrintNightmare) external exploit

**Required Data Connectors**

GCPDNSDataConnector

### Google DNS - CVE-2020-1350 (SIGRED) exploitation pattern

Detects exploitation pattern of CVE-2020-1350 (SIGRED) vulnerability.

**Required Data Connectors**

GCPDNSDataConnector

### Google DNS - UNC2452 (Nobelium) APT Group activity

Detects UNC2452 (Nobelium) APT Group activity.

**Required Data Connectors**

GCPDNSDataConnector

## Hunting Queries

### Google DNS - Errors

GoogleCloudPlatformDNS Hunting Query 1

### Google DNS - Requests to IP lookup resources

GoogleCloudPlatformDNS Hunting Query 2

### Google DNS - Requests to online shares

GoogleCloudPlatformDNS Hunting Query 3

### Google DNS - Rare domains

GoogleCloudPlatformDNS Hunting Query 4

### Google DNS - Domains with rare errors

GoogleCloudPlatformDNS Hunting Query 5

### Google DNS - Requests to TOR resources

GoogleCloudPlatformDNS Hunting Query 6

### Google DNS - Server latency

GoogleCloudPlatformDNS Hunting Query 7

### Google DNS - Sources with high number of errors

GoogleCloudPlatformDNS Hunting Query 8

### Google DNS - Unexpected top level domains

GoogleCloudPlatformDNS Hunting Query 9

### Google DNS - Unusual top level domains

GoogleCloudPlatformDNS Hunting Query 10

## Watchlists

## Playbooks

## Parsers

### GoogleCloudPlatformDNS Data Parser

Category: Samples

Function Alias: imDNSGCPCloudDNS

# Google Cloud Platform IAM

Google Cloud Platform Identity and Access Management (IAM) lets administrators authorize who can act on specific resources, giving full control and visibility to manage Google Cloud resources centrally.

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 10**, Hunting Queries:** 10**, Watchlists:** 0**, Playbooks:** 0, Parsers: 1

## Data Connectors

### Google Cloud Platform IAM (using Azure Function)

The Google Cloud Platform Identity and Access Management (IAM) solution provides the capability to ingest [GCP IAM logs](https://cloud.google.com/iam/docs/audit-logging) into Microsoft Sentinel using the GCP Logging API. Refer to [GCP Logging API documentation](https://cloud.google.com/logging/docs/api) for more information.

## Workbooks

### Google Cloud Platform IAM

Sets the time name for analysis

**Required Data Types**

GCP\_IAM\_CL

GCPIAMDataConnector

## Analytic Rules

### GCP IAM - Disable Data Access Logging

Detects when Data Access Logging is disabled.

**Required Data Connectors**

GCPIAMDataConnector

### GCP IAM - Empty user agent

Detects requests where user agent is empty.

**Required Data Connectors**

GCPIAMDataConnector

### GCP IAM - High privileged role added to service account

Detects when high privileged role was added to service account.

**Required Data Connectors**

GCPIAMDataConnector

### GCP IAM - New Authentication Token for Service Account

Detects when new authentication token is created for service account.

**Required Data Connectors**

GCPIAMDataConnector

### GCP IAM - New Service Account

Detects new service account creation.

**Required Data Connectors**

GCPIAMDataConnector

### GCP IAM - New Service Account Key

Detects new service account key creation.

**Required Data Connectors**

GCPIAMDataConnector

### GCP IAM - Privileges Enumeration

Detects possible privileges enumeration.

**Required Data Connectors**

GCPIAMDataConnector

### GCP IAM - Publicly exposed storage bucket

Detects possible misconfiguration for bucket policy making it publicly available.

**Required Data Connectors**

GCPIAMDataConnector

### GCP IAM - Service Account Enumeration

Detects possible service account enumeration.

**Required Data Connectors**

GCPIAMDataConnector

### GCP IAM - Service Account Keys Enumeration

Detects possible service account keys enumeration.

**Required Data Connectors**

GCPIAMDataConnector

## Hunting Queries

### GCP IAM - Changed roles

GoogleCloudPlatformIAM Hunting Query 1

### GCP IAM - Deleted service accounts

GoogleCloudPlatformIAM Hunting Query 2

### GCP IAM - Disabled service accounts

GoogleCloudPlatformIAM Hunting Query 3

### GCP IAM - New custom roles

GoogleCloudPlatformIAM Hunting Query 4

### GCP IAM - New service accounts

GoogleCloudPlatformIAM Hunting Query 5

### GCP IAM - New service account keys

GoogleCloudPlatformIAM Hunting Query 6

### GCP IAM - Rare IAM actions

GoogleCloudPlatformIAM Hunting Query 7

### GCP IAM - Rare user agent

GoogleCloudPlatformIAM Hunting Query 8

### GCP IAM - Top service accounts by failed actions

GoogleCloudPlatformIAM Hunting Query 9

### GCP IAM - Top source IP addresses with failed actions

GoogleCloudPlatformIAM Hunting Query 10

## Watchlists

## Playbooks

## Parsers

### GoogleCloudPlatformIAM Data Parser

Category: Samples

Function Alias: GCP\_IAM

# Google Workspace Reports

This feature is provided without a service level agreement, and it's not recommended for production workloads.

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 10**, Hunting Queries:** 12**, Watchlists:** 0**, Playbooks:** 0, Parsers: 1

## Data Connectors

### Google Workspace (G Suite) (using Azure Function)

The [Google Workspace](https://workspace.google.com/) data connector provides the capability to ingest Google Workspace Activity events into Microsoft Sentinel through the REST API. The connector provides ability to get [events](https://developers.google.com/admin-sdk/reports/v1/reference/activities) which helps to examine potential security risks, analyze your team's use of collaboration, diagnose configuration problems, track who signs in and when, analyze administrator activity, understand how users create and share content, and more review events in your org.

## Workbooks

### GoogleWorkspaceReports

Sets the time name for analysis

**Required Data Types**

GWorkspace\_ReportsAPI\_admin\_CL

GWorkspace\_ReportsAPI\_calendar\_CL

GWorkspace\_ReportsAPI\_drive\_CL

GWorkspace\_ReportsAPI\_login\_CL

GWorkspace\_ReportsAPI\_login\_CL

GWorkspace\_ReportsAPI\_mobile\_CL

GoogleWorkspaceReportsAPI

## Analytic Rules

### GWorkspace - Admin permissions granted

Triggers on admin permissions granted.

**Required Data Connectors**

GoogleWorkspaceReportsAPI

### GWorkspace - Alert events

Detects alert events.

**Required Data Connectors**

GoogleWorkspaceReportsAPI

### GWorkspace - API Access Granted

Triggers when API Access has been granted to a new client.

**Required Data Connectors**

GoogleWorkspaceReportsAPI

### GWorkspace - User access has been changed

Detects user access change.

**Required Data Connectors**

GoogleWorkspaceReportsAPI

GWorkspace - Multiple user agents for single source

Detects requests with different user agents from one source in short timeframe.

**Required Data Connectors**

GoogleWorkspaceReportsAPI

### GWorkspace - An Outbound Relay has been added to a G Suite Domain

Detects outbound relays may be added to collect email.

**Required Data Connectors**

GoogleWorkspaceReportsAPI

### GWorkspace - Possible brute force attack

Detects possible brute force attack.

**Required Data Connectors**

GoogleWorkspaceReportsAPI

### GWorkspace - Possible maldoc file name in Google drive

Detects possible maldoc file name in Google drive.

**Required Data Connectors**

GoogleWorkspaceReportsAPI

### GWorkspace - Two-step authentification disabled for a user

Triggers on two-step authentification disabled for a user.

**Required Data Connectors**

GoogleWorkspaceReportsAPI

### GWorkspace - Unexpected OS update

Detects unexpected OS update.

**Required Data Connectors**

GoogleWorkspaceReportsAPI

## Hunting Queries

### GWorkspace - Document shared externally

GoogleWorkspaceReports Hunting Query 1

### GWorkspace - Document shared publicy in web

GoogleWorkspaceReports Hunting Query 2

### GWorkspace - Document shared publicy with link

GoogleWorkspaceReports Hunting Query 3

### GWorkspace - Multi IP addresses by user

GoogleWorkspaceReports Hunting Query 4

### GWorkspace - Possible SCAM/SPAM or Phishing via Calendar

GoogleWorkspaceReports Hunting Query 5

### GWorkspace - Rare document types by users

GoogleWorkspaceReports Hunting Query 6

### GWorkspace - Shared private document

GoogleWorkspaceReports Hunting Query 7

### GWorkspace - Suspended users

GoogleWorkspaceReports Hunting Query 8

### GWorkspace - Uncommon user agent strings

GoogleWorkspaceReports Hunting Query 9

### GWorkspace - Unknown login type

GoogleWorkspaceReports Hunting Query 10

### GWorkspace - User reported calendar invite as spam

GoogleWorkspaceReports Hunting Query 11

### GWorkspace - Users with several devices

GoogleWorkspaceReports Hunting Query 12

## Watchlists

## Playbooks

## Parsers

### GWorkspaceActivityReports

Category: Samples

Function Alias: GWorkspaceActivityReports

# Holm Security for Azure Sentinel

Holm Security connector allows you to easily connect your account at Holm Security Security Center with your Azure Sentinel. Asset and vulnerability severities will be automatically available in Azure Sentinel.

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

## Data Connectors

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# HYAS Insight

A threat or fraud investigation solution that improves visibility and productivity for analysts

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

## Data Connectors

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# HYAS Insight for Microsoft Sentinel

HYAS Insight is a threat investigation and attribution solution that uses exclusive data sources and non-traditional mechanisms to improve visibility and productivity for analysts, researchers, and investigators while increasing the accuracy of findings.

**Data Connectors:** 0**, Workbooks:** 0**, Analytic Rules:** 0**, Hunting Queries:** 0**, Watchlists:** 0**, Playbooks:** 17, Parsers: 0

## Data Connectors

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

### HYAS-Insight-Domain-Current-WHOIS

This playbook uses the HYAS Insight connector to automatically enrich incidents generated by Sentinel with current WHOIS information. You need a valid subscription in order to use the connector and playbook. Learn more about the integration via the [connector documentation](https://docs.microsoft.com/connectors/hyasinsight/) or visit [HYAS Insight](https://www.hyas.com/contact) to request a trial key.

### Insight-Domain-Historic-WHOIS

This playbook uses the HYAS Insight connector to automatically enrich incidents generated by Sentinel with historic WHOIS information. You need a valid subscription in order to use the connector and playbook. Learn more about the integration via the [connector documentation](https://docs.microsoft.com/connectors/hyasinsight/) or visit [HYAS Insight](https://www.hyas.com/contact) to request a trial key.

### HYAS-Insight-Domain-Passive-DNS

This playbook uses the HYAS Insight connector to automatically enrich incidents generated by Sentinel with recent passive DNS records. You need a valid subscription in order to use the connector and playbook. Learn more about the integration via the [connector documentation](https://docs.microsoft.com/connectors/hyasinsight/) or visit [HYAS Insight](https://www.hyas.com/contact) to request a trial key.

### HYAS-Insight-Email-C2-Attribution

This playbook uses the HYAS Insight connector to automatically enrich incidents generated by Sentinel with C2 Attribution information. You need a valid subscription in order to use the connector and playbook. Learn more about the integration via the [connector documentation](https://docs.microsoft.com/connectors/hyasinsight/) or visit [HYAS Insight](https://www.hyas.com/contact) to request a trial key.

### HYAS-Insight-Email-Dynamic-DNS

This playbook uses the HYAS Insight connector to automatically enrich incidents generated by Sentinel with Dynamic DNS information. You need a valid subscription in order to use the connector and playbook. Learn more about the integration via the [connector documentation](https://docs.microsoft.com/connectors/hyasinsight/) or visit [HYAS Insight](https://www.hyas.com/contact) to request a trial key.

### HYAS-Insight-Email-Historic-WHOIS

This playbook uses the HYAS Insight connector to automatically enrich incidents generated by Sentinel with historic WHOIS information. You need a valid subscription in order to use the connector and playbook. Learn more about the integration via the [connector documentation](https://docs.microsoft.com/connectors/hyasinsight/) or visit [HYAS Insight](https://www.hyas.com/contact) to request a trial key.

### HYAS-Insight-IP-C2-Attribution

This playbook uses the HYAS Insight connector to automatically enrich incidents generated by Sentinel with historic WHOIS information. You need a valid subscription in order to use the connector and playbook. Learn more about the integration via the [connector documentation](https://docs.microsoft.com/connectors/hyasinsight/) or visit [HYAS Insight](https://www.hyas.com/contact) to request a trial key.

### HYAS-Insight-IP-Dynamic-DNS

This playbook uses the HYAS Insight connector to automatically enrich incidents generated by Sentinel with recent Dynamic DNS information. You need a valid subscription in order to use the connector and playbook. Learn more about the integration via the [connector documentation](https://docs.microsoft.com/connectors/hyasinsight/) or visit [HYAS Insight](https://www.hyas.com/contact) to request a trial key.

### HYAS-Insight-IP-Passive-DNS

This playbook uses the HYAS Insight connector to automatically enrich incidents generated by Sentinel with geolocation information. You need a valid subscription in order to use the connector and playbook. Learn more about the integration via the [connector documentation](https://docs.microsoft.com/connectors/hyasinsight/) or visit [HYAS Insight](https://www.hyas.com/contact) to request a trial key.

### HYAS-Insight-IP-Passive-Hash

This playbook uses the HYAS Insight connector to automatically enrich incidents generated by Sentinel with Passive Hash information. You need a valid subscription in order to use the connector and playbook. Learn more about the integration via the [connector documentation](https://docs.microsoft.com/connectors/hyasinsight/) or visit [HYAS Insight](https://www.hyas.com/contact) to request a trial key.

### HYAS-Insight-IP-Sinkhole

This playbook uses the HYAS Insight connector to automatically enrich incidents generated by Sentinel with Sinkhole information. You need a valid subscription in order to use the connector and playbook. Learn more about the integration via the [connector documentation](https://docs.microsoft.com/connectors/hyasinsight/) or visit [HYAS Insight](https://www.hyas.com/contact) to request a trial key.

### HYAS-Insight-IP-SSL-Certificate

This playbook uses the HYAS Insight connector to automatically enrich incidents generated by Sentinel with SSL certificate information. You need a valid subscription in order to use the connector and playbook. Learn more about the integration via the [connector documentation](https://docs.microsoft.com/connectors/hyasinsight/) or visit [HYAS Insight](https://www.hyas.com/contact) to request a trial key.

### HYAS-Insight-IPv4-Device-Geo

This playbook uses the HYAS Insight connector to automatically enrich incidents generated by Sentinel with geolocation information. You need a valid subscription in order to use the connector and playbook. Learn more about the integration via the [connector documentation](https://docs.microsoft.com/connectors/hyasinsight/) or visit [HYAS Insight](https://www.hyas.com/contact) to request a trial key.

### HYAS-Insight-IPv6-Device-Geo

This playbook uses the HYAS Insight connector to automatically enrich incidents generated by Sentinel with geolocation information. You need a valid subscription in order to use the connector and playbook. Learn more about the integration via the [connector documentation](https://docs.microsoft.com/connectors/hyasinsight/) or visit [HYAS Insight](https://www.hyas.com/contact) to request a trial key.

### Insight-Phone-Number-Historic-WHOIS

This playbook uses the HYAS Insight connector to automatically enrich incidents generated by Sentinel with historic WHOIS information. You need a valid subscription in order to use the connector and playbook. Learn more about the integration via the [connector documentation](https://docs.microsoft.com/connectors/hyasinsight/) or visit [HYAS Insight](https://www.hyas.com/contact) to request a trial key.

### HYAS-Insight-SHA256-C2-Attribution

This playbook uses the HYAS Insight connector to automatically enrich incidents generated by Sentinel with historic WHOIS information. You need a valid subscription in order to use the connector and playbook. Learn more about the integration via the [connector documentation](https://docs.microsoft.com/connectors/hyasinsight/) or visit [HYAS Insight](https://www.hyas.com/contact) to request a trial key.

### Insight-Domain-C2-Attribution

This playbook uses the HYAS Insight connector to automatically enrich incidents generated by Sentinel with C2 Attribution information. You need a valid subscription in order to use the connector and playbook. Learn more about the integration via the [connector documentation](https://docs.microsoft.com/connectors/hyasinsight/) or visit [HYAS Insight](https://www.hyas.com/contact) to request a trial key.

## Parsers

# iboss Connector for Microsoft Sentinel

iboss Zero Trust Edge secures all resource access from any location with consistent security features and visibility. Realtime stream of iboss logs into Sentinel with parser functions and custom workbooks.

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

## Data Connectors

### iboss

The [iboss](https://www.iboss.com) data connector enables you to seamlessly connect your Threat Console to Microsoft Sentinel and enrich your instance with iboss URL event logs. Our logs are forwarded in Common Event Format (CEF) over Syslog and the configuration required can be completed on the iboss platform without the use of a proxy. Take advantage of our connector to garner critical data points and gain insight into security threats.

## Workbooks

### iboss Malware and C2

A workbook providing insights into malware and C2 activity detected by iboss.

**Required Data Types**

### iboss Web Usage

A workbook providing insights into web usage activity detected by iboss.

**Required Data Types**

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### ibossUrlEvent

Category: Samples

Function Alias: ibossUrlEvent

# Illumio Core

Ingest Illumio Core logs into Microsoft Sentinel

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

## Data Connectors

### Illumio Core

The [Illumio Core](https://www.illumio.com/products/core) data connector provides the capability to ingest Illumio Core logs into Microsoft Sentinel.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### IllumioCoreEvent

Category: Samples

Function Alias: IllumioCoreEvent

# Illusive Attack Surface Analysis and Incident Logs for Microsoft Sentinel

The Illusive data connector allows to share Illusive’s attack surface analysis data & incidents with Microsoft Sentinel and view this data in dedicated dashboards that offer insight to your org’s attack surface risk and track unauthorized lateral movement

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

## Data Connectors

### Illusive Platform

The Illusive Platform Connector allows you to share Illusive's attack surface analysis data and incident logs with Microsoft Sentinel and view this information in dedicated dashboards that offer insight into your organization's attack surface risk (ASM Dashboard) and track unauthorized lateral movement in your organization's network (ADS Dashboard).

## Workbooks

### Illusive ADS Dashboard

Gain insights into unauthorized lateral movement in your organization's network.

Illusive ADS is designed to paralyzes attackers and eradicates in-network threats by creating a hostile environment for the attackers across all the layers of the attack surface.

**Required Data Types**

### Illusive ASM Dashboard

Gain insights into your organization's Cyber Hygiene and Attack Surface risk.

Illusive ASM automates discovery and clean-up of credential violations, allows drill-down inspection of pathways to critical assets, and provides risk insights that inform intelligent decision-making to reduce attacker mobility.

**Required Data Types**

## Analytic Rules

### Illusive Incidents Analytic Rule

Create a Sentinel incident upon a new Illusive alert (incident) and associate all related Illusive events to the relevant Sentinel alert. This is done by filtering and processing Illusive Syslog messages.

**Required Data Connectors**

Illusive

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Imperva WAF Cloud Solution

Imperva Cloud WAF offers the industry’s leading web application security firewall, providing enterprise-class protection against the most sophisticated security threats.

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 10**, Hunting Queries:** 10**, Watchlists:** 0**, Playbooks:** 0, Parsers: 1

## Data Connectors

### Imperva Cloud WAF (using Azure Function)

The [Imperva Cloud WAF](https://www.imperva.com/resources/resource-library/datasheets/imperva-cloud-waf/) data connector provides the capability to integrate and ingest Web Application Firewall events into Microsoft Sentinel through the REST API. Refer to Log integration [documentation](https://docs.imperva.com/bundle/cloud-application-security/page/settings/log-integration.htm#Download) for more information. The connector provides ability to get events which helps to examine potential security risks, analyze your team's use of collaboration, diagnose configuration problems and more.

## Workbooks

### Imperva WAF Cloud Overview

Sets the time name for analysis.

**Required Data Types**

## Analytic Rules

### Imperva - Abnormal protocol usage

Detects abnormal protocol usage.

**Required Data Connectors**

ImpervaWAFCloudAPI

### Imperva - Request from unexpected IP address to admin panel

Detects requests from unexpected IP addresses to admin panel.

**Required Data Connectors**

ImpervaWAFCloudAPI

### Imperva - Critical severity event not blocked

Detects when critical severity event was not blocked.

**Required Data Connectors**

ImpervaWAFCloudAPI

### Imperva - Possible command injection

Detects requests with commands in URI.

**Required Data Connectors**

ImpervaWAFCloudAPI

### Imperva - Request from unexpected countries

Detects request attempts from unexpected countries.

**Required Data Connectors**

ImpervaWAFCloudAPI

### Imperva - Forbidden HTTP request method in request

Detects connections with unexpected HTTP request method.

**Required Data Connectors**

ImpervaWAFCloudAPI

### Imperva - Malicious Client

Detects connections from known malicious clients.

**Required Data Connectors**

ImpervaWAFCloudAPI

### Imperva - Malicious user agent

Detects requests containing known malicious user agent strings.

**Required Data Connectors**

ImpervaWAFCloudAPI

### Imperva - Multiple user agents from same source

'Detects suspicious number of user agents from the same IP address.

**Required Data Connectors**

ImpervaWAFCloudAPI

### Imperva - Request to unexpected destination port

Detects request attempts to unexpected destination ports.

**Required Data Connectors**

ImpervaWAFCloudAPI

## Hunting Queries

### Imperva - Top destinations with blocked requests

ImpervaCloudWAF Hunting Query 1

### Imperva - Applications with insecure web protocol version

ImpervaCloudWAF Hunting Query 2

### Imperva - Non HTTP/HTTPs applications

ImpervaCloudWAF Hunting Query 3

### Imperva - Rare applications

ImpervaCloudWAF Hunting Query 4

### Imperva - Rare client applications

ImpervaCloudWAF Hunting Query 5

### Imperva - Rare destination ports

ImpervaCloudWAF Hunting Query 6

### Imperva - request from known bots

ImpervaCloudWAF Hunting Query 7

### Imperva - Top sources with blocked requests

ImpervaCloudWAF Hunting Query 8

### Imperva - Top applications with error requests

ImpervaCloudWAF Hunting Query 9

### Imperva - Top sources with error requests

ImpervaCloudWAF Hunting Query 10

## Watchlists

## Playbooks

## Parsers

### ImpervaCloudWAF Data Parser

Category: Samples

Function Alias: ImpervaWAFCloud

# Infoblox Cloud for Microsoft Sentinel

This solution allows you to easily connect Infoblox Cloud to Microsoft Sentinel via an Infoblox Cloud Data Connector.

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

## Data Connectors

### Infoblox Cloud Data Connector

The Infoblox Cloud Data Connector allows you to easily connect your Infoblox BloxOne data with Microsoft Sentinel. By connecting your logs to Microsoft Sentinel, you can take advantage of search & correlation, alerting, and threat intelligence enrichment for each log.

## Workbooks

### Infoblox Cloud Data Connector

Sets the time name for analysis

**Required Data Types**

CommonSecurityLog

InfobloxCloudDataConnector

## Analytic Rules

### Infoblox - High Number of High Threat Level Queries Detected

This creates an incident in the event a single host generates at least 200 high threat level RPZ queries (Threat Defense security hits) in 1 hour. Query count threshold and scheduling is customizable. This rule depends on a parser based on a Kusto Function to work as expected called [\*\*InfobloxCDC\*\*](https://aka.ms/sentinel-InfobloxCloudDataConnector-parser).

**Required Data Connectors**

InfobloxCloudDataConnector

### Infoblox - High Number of NXDOMAIN DNS Responses Detected

This creates an incident in the event a single host generates at least 200 DNS responses for non-existent domains in 1 hour. Query count threshold and scheduling is customizable. This rule depends on a parser based on a Kusto Function to work as expected called [\*\*InfobloxCDC\*\*](https://aka.ms/sentinel-InfobloxCloudDataConnector-parser).

**Required Data Connectors**

InfobloxCloudDataConnector

### Infoblox - High Threat Level Query Not Blocked Detected

This creates an incident in the event a single host generates at least 1 high threat level query (Threat Defense security hit) that is not blocked or redirected in 1 hour. Query count threshold and scheduling is customizable. This rule depends on a parser based on a Kusto Function to work as expected called [\*\*InfobloxCDC\*\*](https://aka.ms/sentinel-InfobloxCloudDataConnector-parser).

**Required Data Connectors**

InfobloxCloudDataConnector

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### Infoblox Cloud Data Connector Data Parser

Category: Samples

Function Alias: InfobloxCDC

# Infoblox NIOS

The Infoblox Network Identity Operating System (NIOS) solution for Microsoft Sentinel enables you to easily connect your Infoblox NIOS logs with Microsoft Sentinel, to view dashboards, create custom alerts, and improve investigation.

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 2**, Hunting Queries:** 0**, Watchlists:** 1**, Playbooks:** 0, Parsers: 22

## Data Connectors

### Infoblox NIOS

The [Infoblox Network Identity Operating System (NIOS)](https://www.infoblox.com/glossary/network-identity-operating-system-nios/) connector allows you to easily connect your Infoblox NIOS logs with Microsoft Sentinel, to view dashboards, create custom alerts, and improve investigation. This gives you more insight into your organization's network and improves your security operation capabilities.

## Workbooks

### Infoblox NIOS

Gain insight into Infoblox NIOS by analyzing, collecting and correlating DHCP and DNS data.

This workbook provides visibility into DHCP and DNS traffic

**Required Data Types**

Syslog

InfobloxNIOS

## Analytic Rules

### Excessive NXDOMAIN DNS Queries

This creates an incident in the event a client generates excessive amounts of DNS queries for non-existent domains.

**Required Data Connectors**

InfobloxNIOS

### Potential DHCP Starvation Attack

This creates an incident in the event that an excessive amount of DHCPREQUEST have been recieved by a DHCP Server and could potentially be an indication of a DHCP Starvation Attack.

**Required Data Connectors**

InfobloxNIOS

## Hunting Queries

## Watchlists

### Sources\_by\_SourceType

The watchlist is used by parsers to specify Sources and their types.

## Playbooks

## Parsers

### Infoblox

Category: Samples

Function Alias: Infoblox

### Infoblox\_allotherdhcpdTypes

Category: Samples

Function Alias: Infoblox\_allotherdhcpdTypes

### Infoblox\_allotherdnsTypes

Category: Samples

Function Alias: Infoblox\_allotherdnsTypes

### Infoblox\_allotherlogTypes

Category: Samples

Function Alias: Infoblox\_allotherlogTypes

### Infoblox\_dhcp\_consolidated

Category: Samples

Function Alias: Infoblox\_dhcp\_consolidated

### Infoblox\_dhcpack

Category: Samples

Function Alias: Infoblox\_dhcpack

### Infoblox\_dhcpadded

Category: Samples

Function Alias: Infoblox\_dhcpadded

### Infoblox\_dhcpbindupdate

Category: Samples

Function Alias: Infoblox\_dhcpbindupdate

### Infoblox\_dhcpdiscover

Category: Samples

Function Alias: Infoblox\_dhcpdiscover

### Infoblox\_dhcpexpire

Category: Samples

Function Alias: Infoblox\_dhcpexpire

### Infoblox\_dhcpinform

Category: Samples

Function Alias: Infoblox\_dhcpinform

### Infoblox\_dhcpoffer

Category: Samples

Function Alias: Infoblox\_dhcpoffer

### Infoblox\_dhcpoption

Category: Samples

Function Alias: Infoblox\_dhcpoption

### Infoblox\_dhcpother

Category: Samples

Function Alias: Infoblox\_dhcpother

### Infoblox\_dhcprelease

Category: Samples

Function Alias: Infoblox\_dhcprelease

### Infoblox\_dhcpremoved

Category: Samples

Function Alias: Infoblox\_dhcpremoved

### Infoblox\_dhcprequest

Category: Samples

Function Alias: Infoblox\_dhcprequest

### Infoblox\_dhcpsession

Category: Samples

Function Alias: Infoblox\_dhcpsession

### Infoblox\_dns\_consolidated

Category: Samples

Function Alias: Infoblox\_dns\_consolidated

### Infoblox\_dnsclient

Category: Samples

Function Alias: Infoblox\_dnsclient

### Infoblox\_dnsgss

Category: Samples

Function Alias: Infoblox\_dnsgss

### Infoblox\_dnszone

Category: Samples

Function Alias: Infoblox\_dnszone

# InsightVM CloudAPI

The Rapid7 Insight platform brings together Rapid7’s library of vulnerability research, exploit knowledge, global attacker behavior, Internet-wide scanning data, exposure analytics, and real-time reporting to provide a fully available and scalable.

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

## Data Connectors

### Rapid7 Insight Platform Vulnerability Management Reports (using Azure Function)

The [Rapid7 Insight VM](https://www.rapid7.com/products/insightvm/) Report data connector provides the capability to ingest Scan reports and vulnerability data into Microsoft Sentinel through the REST API from the Rapid7 Insight platform (Managed in the cloud). Refer to [API documentation](https://docs.rapid7.com/insight/api-overview/) for more information. The connector provides ability to get events which helps to examine potential security risks, analyze your team's use of collaboration, diagnose configuration problems and more.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

### Rapid7 Insight VM - Enrich incident with asset info

Once a new Microsoft Sentinel incident is created, this playbook gets triggered and performs the following actions:

1. Obtains IPs from the incident.

2. Searches asset ids by the IPs.

3. Gets assets information.

4. Adds obtained information as a comment to the incident.

### Rapid7 Insight VM - Enrich vulnerability info

Once a new Microsoft Sentinel incident is created, this playbook gets triggered and performs the following actions:

1. Obtains IPs from the incident.

2. Searches asset ids by the IPs.

3. Gets vulnerability ids.

4. Gets vulnerability information.

5. Adds obtained information as a comment to the incident.

### Rapid7 Insight VM - Run scan

Once a new Microsoft Sentinel incident is created, this playbook gets triggered and performs the following actions:

1. Obtains IPs from the incident.

2. Searches asset ids by the IPs.

3. Obtains a list of scan engines.

4. Sends an adaptive card to the Teams channel where the user can choose an action to be taken.

5. Runs scans for selected IPs using chosen scan engines.

6. Add inforamtions about launched scans as a comment to the incident.

## Parsers

### InsightVMAssets

Category: Samples

Function Alias: InsightVMAssets

### InsightVMVulnerabilities

Category: Samples

Function Alias: InsightVMVulnerabilities

# ISC Bind

The ISC Bind solution for Microsoft sentinel allows you to ingest ISC Bind logs to get better insights into your organization's network traffic data, DNS query data, traffic statistics and improves your security operation capabilities.

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

## Data Connectors

### ISC Bind

The [ISC Bind](https://www.isc.org/bind/) connector allows you to easily connect your ISC Bind logs with Microsoft Sentinel. This gives you more insight into your organization's network traffic data, DNS query data, traffic statistics and improves your security operation capabilities.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### ISCBind

Category: Samples

Function Alias: ISCBind

# Ivanti Unified Endpoint Management

The Ivanti Unified Endpoint Management gives you the ability to enforce policy and privileges everywhere in a few clicks, and discover and patch threats predictively and quickly.The result is better user experiences, and zero compromise on protection.

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

## Data Connectors

### Ivanti Unified Endpoint Management

The [Ivanti Unified Endpoint Management](https://www.ivanti.com/products/unified-endpoint-manager) data connector provides the capability to ingest [Ivanti UEM Alerts](https://help.ivanti.com/ld/help/en\_US/LDMS/11.0/Windows/alert-c-monitoring-overview.htm) into Microsoft Sentinel.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### IvantiUEMEvent

Category: Samples

Function Alias: IvantiUEMEvent

# Jamf Protect for Microsoft Sentinel

Provide complete insight and visibility into your protected macOS endpoints, alongside other managed endpoints, all within a single Microsoft Sentinel workspace.

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

## Data Connectors

### Jamf Protect

The [Jamf Protect](https://www.jamf.com/products/jamf-protect/) connector provides the capability to read raw event data from Jamf Protect in Microsoft Sentinel.

## Workbooks

### Jamf Protect Workbook

This Jamf Protect Workbook for Microsoft Sentinel enables you to ingest Jamf Protect events forwarded into Microsoft Sentinel.

Providing reports into all alerts, device controls and Unfied Logs.

**Required Data Types**

jamfprotect\_CL

## Analytic Rules

### Jamf Protect - Alerts

Creates an incident based on Jamf Protect Alert data in Microsoft Sentinel

**Required Data Connectors**

JamfProtect

### Jamf Protect - Network Threats

Creates an incident based based on Jamf Protect's Network Threat Event Stream alerts.

**Required Data Connectors**

JamfProtect

### Jamf Protect - Unified Logs

Creates an informational incident based on Jamf Protect Unified Log data in Microsoft Sentinel

**Required Data Connectors**

JamfProtect

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Jboss

JBoss delivers enterprise-grade security, performance, and scalability in any environment. Whether on-premise; virtual; or in private, public, or hybrid clouds, JBoss EAP can help you deliver apps faster, everywhere.

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

## Data Connectors

### JBoss Enterprise Application Platform

The JBoss Enterprise Application Platform data connector provides the capability to ingest [JBoss](https://www.redhat.com/en/technologies/jboss-middleware/application-platform) events into Azure Sentinel. Refer to [Red Hat documentation](https://access.redhat.com/documentation/en-us/red\_hat\_jboss\_enterprise\_application\_platform/7.0/html/configuration\_guide/logging\_with\_jboss\_eap) for more information.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### JBossEvent

Category: Samples

Function Alias: JBossEvent

# Joshua Cyberisk Vision

Joshua Cyberiskvision enables organizations to define, monitor, analyze and improve their level of Global Cybersecurity following a predictive and context-aware approach that uses a broad-spectrum cyber intelligence-driven logic.

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

## Data Connectors

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Juniper IDP Solution

The Juniper IDP solution provides the capability to ingest Juniper IDP events into Microsoft Sentinel.

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

## Data Connectors

### Juniper IDP

The [Juniper](https://www.juniper.net/) IDP data connector provides the capability to ingest [Juniper IDP](https://www.juniper.net/documentation/us/en/software/junos/idp-policy/topics/topic-map/security-idp-overview.html) events into Microsoft Sentinel.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### Juniper IDP Data Parser

Category: Samples

Function Alias: JuniperIDP

# Juniper SRX

The Juniper SRX solution for Microsoft Sentinel enables you to ingest Juniper SRX traffic and system logs into Microsoft Sentinel.

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

## Data Connectors

### Juniper SRX

The [Juniper SRX](https://www.juniper.net/us/en/products-services/security/srx-series/) connector allows you to easily connect your Juniper SRX logs with Microsoft Sentinel. This gives you more insight into your organization's network and improves your security operation capabilities.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### JuniperSRX

Category: Samples

Function Alias: JuniperSRX

# Kaspersky Security Center

The Kaspersky Security Center data connector provides the capability to ingest Kaspersky Security Center logs into Microsoft Sentinel.

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

## Data Connectors

### Kaspersky Security Center

The [Kaspersky Security Center](https://support.kaspersky.com/KSC/13/en-US/3396.htm) data connector provides the capability to ingest [Kaspersky Security Center logs](https://support.kaspersky.com/KSC/13/en-US/151336.htm) into Microsoft Sentinel.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### KasperskySecurityCenter Data Parser

Category: Samples

Function Alias: KasperskySCEvent

# KQL Training

The KQL Training solution for Microsoft Sentinel contains resources that can help up – skill on understanding the fundamentals and using KQL in advanced scenarios like authoring effective and optimized queries used in Sentinel Analytics, Hunting Queries.

**Data Connectors:** 0**, Workbooks:** 2**, Analytic Rules:** 0**, Hunting Queries:** 0**, Watchlists:** 0**, Playbooks:** 0, Parsers: 0

## Data Connectors

## Workbooks

### Advanced KQL for Microsoft Sentinel

This interactive Workbook is designed to improve your KQL proficiency by using a use-case driven approach.

**Required Data Types**

### Intro to KQL

Learn and practice the Kusto Query Language. This workbook introduces and provides 100 to 200 level content for new and existing users looking to learn KQL. This workbook will be updated with content over time.

**Required Data Types**

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Lastpass Enterprise Activity Monitoring

By leveraging Microsoft technologies, your LastPass Enterprise solution will be enriched with activity monitoring and alerts for a better password management and increased security posture.

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 5**, Hunting Queries:** 3**, Watchlists:** 1**, Playbooks:** 0, Parsers: 0

## Data Connectors

### LastPass Enterprise - Reporting (Polling CCP)

The [LastPass Enterprise](https://www.lastpass.com/products/enterprise-password-management-and-sso) connector provides the capability to LastPass reporting (audit) logs into Microsoft Sentinel. The connector provides visibility into logins and activity within LastPass (such as reading and removing passwords).

## Workbooks

### Lastpass Enterprise Activity Monitoring

Sets the time name for analysis

**Required Data Types**

## Analytic Rules

### Employee account deleted

This rule will monitor for any employee accounts being deleted.

Deleting an employee account can have a big potential impact as all of the data for that user will be removed.

**Required Data Connectors**

LastPass

### Failed sign-ins into LastPass due to MFA

This rule will check if a sign-in failed into LastPass due to MFA.

An incident can indicate the potential brute forcing of a LastPass account.

The use of MFA is identified by combining the sign-in logs, this rule assumes LastPass is federated to AAD.

**Required Data Connectors**

LastPass

AzureActiveDirectory

### Highly Sensitive Password Accessed

This rule will monitor access to highly sensitive passwords.

Within the Watchlist called 'LastPass' define passwords which are deemed highly sensitive (such as password to a high privileged application).

When an activity is observed against such password, an incident is created.

**Required Data Connectors**

LastPass

### TI map IP entity to LastPass data

Identifies a match in LastPass table from any IP IOC from TI

**Required Data Connectors**

LastPass

ThreatIntelligence

### Unusual Volume of Password Updated or Removed

This rule will check if there is an unnormal activity of sites that are deleted or changed per user.

The normal amount of actions is calculated based on the previous 14 days of activity. If there is a significant increase, an incident will be created.

**Required Data Connectors**

LastPass

## Hunting Queries

### Failed sign-ins into LastPass due to MFA.

Lastpass Enterprise Activity Monitoring Hunting Query 1

### Login into LastPass from a previously unknown IP.

Lastpass Enterprise Activity Monitoring Hunting Query 2

### Password moved to shared folders

Lastpass Enterprise Activity Monitoring Hunting Query 3

## Watchlists

### Last Pass High Sensitive Passwords

Used to maintain list of high sensitive accounts in LastPass.

## Playbooks

## Parsers

# Legacy IOC based Threat Protection

Microsoft Security Research, based on ongoing trends and exploits creates content that help identify existence of known IOCs based on known prevalent attacks and threat actor tactics/techniques, such as Nobelium, Gallium, Solorigate, etc.

**Data Connectors:** 0**, Workbooks:** 0**, Analytic Rules:** 35**, Hunting Queries:** 10**, Watchlists:** 0**, Playbooks:** 0, Parsers: 0

## Data Connectors

## Workbooks

## Analytic Rules

### ACTINIUM Actor IOCs - Feb 2022

Identifies a match across various data feeds for domains, hashes and commands related to an actor tracked by Microsoft as Actinium.

**Required Data Connectors**

DNS

AzureMonitor(VMInsights)

F5

CiscoASA

PaloAltoNetworks

Fortinet

CheckPoint

CEF

MicrosoftThreatProtection

SecurityEvents

AzureFirewall

### Known Barium domains

Identifies a match across various data feeds for domains IOCs related to the Barium activity group.

References: https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer

**Required Data Connectors**

SquidProxy

DNS

AzureMonitor(VMInsights)

CiscoASA

PaloAltoNetworks

MicrosoftThreatProtection

AzureFirewall

Zscaler

InfobloxNIOS

GCPDNSDataConnector

NXLogDnsLogs

CiscoUmbrellaDataConnector

Corelight

### Known Barium IP

Identifies a match across various data feeds for IP IOCs related to the Barium activity group.

References: https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer

**Required Data Connectors**

AWSS3

WindowsForwardedEvents

MicrosoftSysmonForLinux

Office365

DNS

AzureMonitor(VMInsights)

CiscoASA

PaloAltoNetworks

SecurityEvents

AzureActiveDirectory

AzureActiveDirectory

AzureMonitor(WireData)

AzureMonitor(IIS)

AzureActivity

AWS

MicrosoftThreatProtection

AzureFirewall

Zscaler

InfobloxNIOS

GCPDNSDataConnector

NXLogDnsLogs

CiscoUmbrellaDataConnector

Corelight

### Known CERIUM domains and hashes

CERIUM malicious webserver and hash values for maldocs and malware.

Matches domain name IOCs related to the CERIUM activity group with CommonSecurityLog, DnsEvents, and VMConnection dataTypes.

**Required Data Connectors**

SquidProxy

DNS

AzureMonitor(VMInsights)

CiscoASA

PaloAltoNetworks

AzureFirewall

Zscaler

InfobloxNIOS

GCPDNSDataConnector

NXLogDnsLogs

CiscoUmbrellaDataConnector

Corelight

### Chia\_Crypto\_Mining - Domain, Process, Hash and IP IOCs - June 2021

Identifies a match across various data feeds for domains, process, hashes and IP IOC related to Chia cryptocurrency farming/plotting activity.

**Required Data Connectors**

DNS

AzureMonitor(VMInsights)

F5

CiscoASA

PaloAltoNetworks

Fortinet

CheckPoint

CEF

MicrosoftThreatProtection

SecurityEvents

Office365

AzureFirewall

WindowsFirewall

### DEV-0322 Serv-U related IOCs - July 2021

Identifies a match across IOC's related to DEV-0322 targeting SolarWinds Serv-U software.

**Required Data Connectors**

DNS

AzureMonitor(VMInsights)

F5

CiscoASA

PaloAltoNetworks

Fortinet

CheckPoint

CEF

MicrosoftThreatProtection

SecurityEvents

Office365

AzureFirewall

WindowsFirewall

### Dev-0530 IOC - July 2022

Identifies a IOC match related to Dev-0530 actor across various data sources.

**Required Data Connectors**

CiscoASA

PaloAltoNetworks

MicrosoftThreatProtection

SecurityEvents

Office365

AzureActiveDirectory

AzureActiveDirectory

AzureMonitor(IIS)

AzureActivity

AWS

AzureFirewall

### DEV-0586 Actor IOC - January 2022

Identifies a match across IOC's related to an actor tracked by Microsoft as DEV-0586

Reference: https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/

**Required Data Connectors**

CiscoASA

PaloAltoNetworks

MicrosoftThreatProtection

SecurityEvents

WindowsSecurityEvents

### Exchange Server Vulnerabilities Disclosed March 2021 IoC Match

This detection look for IoCs shared by Microsoft relating to attacks exploiting the Exchange Server vulnerabilities disclosed in March 2021. It looks for SHA256 file hashes, IP addresses and file paths in a number of data sources. This query can also be customized with additional data sources that may include these elements.

Ref: https://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server/

**Required Data Connectors**

AWSS3

WindowsForwardedEvents

AzureMonitor(IIS)

AzureMonitor(WireData)

CheckPoint

CiscoASA

CEF

F5

Fortinet

PaloAltoNetworks

SecurityEvents

WindowsFirewall

DNS

Zscaler

InfobloxNIOS

MicrosoftSysmonForLinux

GCPDNSDataConnector

WindowsForwardedEvents

NXLogDnsLogs

CiscoUmbrellaDataConnector

Corelight

### Known GALLIUM domains and hashes

GALLIUM command and control domains and hash values for tools and malware used by GALLIUM.

Matches domain name IOCs related to the GALLIUM activity group with CommonSecurityLog, DnsEvents, VMConnection and SecurityEvents dataTypes.

References: https://www.microsoft.com/security/blog/2019/12/12/gallium-targeting-global-telecom/

**Required Data Connectors**

DNS

AzureMonitor(VMInsights)

CiscoASA

PaloAltoNetworks

SecurityEvents

AzureFirewall

Zscaler

InfobloxNIOS

GCPDNSDataConnector

NXLogDnsLogs

CiscoUmbrellaDataConnector

Corelight

### HAFNIUM UM Service writing suspicious file

This query looks for the Exchange server UM process writing suspicious files that may be indicative of webshells.

Reference: https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

**Required Data Connectors**

SecurityEvents

MicrosoftThreatProtection

WindowsSecurityEvents

WindowsForwardedEvents

### Hive Ransomware IOC - July 2022

Identifies a hash match related to Hive Ransomware across various data sources.

**Required Data Connectors**

CiscoASA

PaloAltoNetworks

MicrosoftThreatProtection

SecurityEvents

### Known IRIDIUM IP

IRIDIUM command and control IP. Identifies a match across various data feeds for IP IOCs related to the IRIDIUM activity group.

**Required Data Connectors**

AWSS3

WindowsForwardedEvents

SquidProxy

MicrosoftThreatProtection

SecurityEvents

MicrosoftSysmonForLinux

Office365

DNS

AzureMonitor(VMInsights)

CiscoASA

PaloAltoNetworks

SecurityEvents

AzureActiveDirectory

AzureActiveDirectory

AzureMonitor(IIS)

AzureActivity

AWS

AzureFirewall

Zscaler

InfobloxNIOS

GCPDNSDataConnector

NXLogDnsLogs

CiscoUmbrellaDataConnector

Corelight

### KNOTWEED AV Detection

This query looks for Microsoft Defender AV detections related to the KNOTWEED threat actor and the Corelump and Jumplump malware.

Ref: https://www.microsoft.com/security/blog/2022/07/27/untangling-knotweed-european-private-sector-offensive-actor-using-0-day-exploits/

**Required Data Connectors**

MicrosoftThreatProtection

SecurityEvents

### KNOTWEED C2 Domains July 2022

This query looks for references to known KNOTWEED Domains in network logs.

This query was published July 2022.

Ref: https://www.microsoft.com/security/blog/2022/07/27/untangling-knotweed-european-private-sector-offensive-actor-using-0-day-exploits/

**Required Data Connectors**

AzureMonitor(VMInsights)

DNS

MicrosoftThreatProtection

### KNOTWEED File Hashes July 2022

This query looks for references to known KNOTWEED file hashes in various logs.

This query was published July 2022.

Ref: https://www.microsoft.com/security/blog/2022/07/27/untangling-knotweed-european-private-sector-offensive-actor-using-0-day-exploits/

**Required Data Connectors**

MicrosoftThreatProtection

SecurityEvents

WindowsFirewall

### Known PHOSPHORUS group domains/IP - October 2020

Matches IOCs related to PHOSPHORUS group activity published October 2020 with CommonSecurityLog, DnsEvents, OfficeActivity and VMConnection dataTypes.

References:

**Required Data Connectors**

DNS

AzureMonitor(VMInsights)

CiscoASA

PaloAltoNetworks

Zscaler

Fortinet

OfficeATP

AzureFirewall

### Known Manganese IP and UserAgent activity

Matches IP plus UserAgent IOCs in OfficeActivity data, along with IP plus Connection string information in the CommonSecurityLog data related to Manganese group activity.

References:

https://kb.pulsesecure.net/articles/Pulse\_Security\_Advisories/SA44101/

https://fortiguard.com/psirt/FG-IR-18-384

**Required Data Connectors**

Office365

### MSHTML vulnerability CVE-2021-40444 attack

This query detects attacks that exploit the CVE-2021-40444 MSHTML vulnerability using specially crafted Microsoft Office documents.

The detection searches for relevant files used in the attack along with regex matches in commnadline to look for pattern similar to : ".cpl:../../msword.inf"

Refrence: https://www.microsoft.com/security/blog/2021/09/15/analyzing-attacks-that-exploit-the-mshtml-cve-2021-40444-vulnerability/

**Required Data Connectors**

SecurityEvents

MicrosoftThreatProtection

### Known NICKEL domains and hashes

IOC domains and hash values for tools and malware used by NICKEL.

Matches domain name, hash IOCs and M365 Defender sigs related to the NICKEL activity group with CommonSecurityLog, DnsEvents, VMConnection and SecurityEvents dataTypes.

**Required Data Connectors**

SquidProxy

DNS

AzureMonitor(VMInsights)

CiscoASA

PaloAltoNetworks

MicrosoftThreatProtection

MicrosoftThreatProtection

SecurityEvents

AzureFirewall

Zscaler

InfobloxNIOS

GCPDNSDataConnector

NXLogDnsLogs

CiscoUmbrellaDataConnector

Corelight

### NOBELIUM - Domain and IP IOCs - March 2021

Identifies a match across various data feeds for domains and IP IOCs related to NOBELIUM.

References: https://www.microsoft.com/security/blog/2021/03/04/goldmax-goldfinder-sibot-analyzing-nobelium-malware/

**Required Data Connectors**

SquidProxy

DNS

AzureMonitor(VMInsights)

CiscoASA

PaloAltoNetworks

MicrosoftThreatProtection

Office365

AzureFirewall

Zscaler

InfobloxNIOS

GCPDNSDataConnector

NXLogDnsLogs

CiscoUmbrellaDataConnector

Corelight

### NOBELIUM IOCs related to FoggyWeb backdoor

Identifies a match across various data feeds for IOCs related to FoggyWeb backdoor by the threat actor NOBELIUM.

FoggyWeb is a passive and highly targeted backdoor capable of remotely exfiltrating sensitive information from a compromised AD FS server.

It can also receive additional malicious components from a command-and-control (C2) server and execute them on the compromised server.

Reference: https://aka.ms/nobelium-foggy-web

**Required Data Connectors**

F5

CiscoASA

PaloAltoNetworks

Fortinet

CheckPoint

CEF

MicrosoftThreatProtection

SecurityEvents

WindowsSecurityEvents

AzureMonitor(IIS)

WindowsSecurityEvents

WindowsForwardedEvents

### NOBELIUM - Domain, Hash and IP IOCs - May 2021

Identifies a match across various data feeds for domains, hashes and IP IOCs related to NOBELIUM.

Ref: https://www.microsoft.com/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/

**Required Data Connectors**

AWSS3

WindowsForwardedEvents

SquidProxy

MicrosoftSysmonForLinux

DNS

AzureMonitor(VMInsights)

F5

CiscoASA

PaloAltoNetworks

Fortinet

CheckPoint

CEF

MicrosoftThreatProtection

SecurityEvents

Office365

AzureFirewall

WindowsFirewall

Zscaler

InfobloxNIOS

GCPDNSDataConnector

NXLogDnsLogs

CiscoUmbrellaDataConnector

Corelight

### Known Phosphorus group domains/IP

Matches domain name IOCs related to Phosphorus group activity with CommonSecurityLog, DnsEvents, OfficeActivity and VMConnection dataTypes.

References: https://blogs.microsoft.com/on-the-issues/2019/03/27/new-steps-to-protect-customers-from-hacking/.

**Required Data Connectors**

SquidProxy

DNS

AzureMonitor(VMInsights)

CiscoASA

PaloAltoNetworks

Office365

AzureFirewall

Zscaler

InfobloxNIOS

GCPDNSDataConnector

NXLogDnsLogs

CiscoUmbrellaDataConnector

Corelight

### Known POLONIUM IP

Identifies a match across various data feeds for IP IOCs related to the POLONIUM activity group.

References: BLOGURL

**Required Data Connectors**

AWSS3

WindowsForwardedEvents

MicrosoftSysmonForLinux

Office365

DNS

AzureMonitor(VMInsights)

CiscoASA

PaloAltoNetworks

SecurityEvents

AzureActiveDirectory

AzureActiveDirectory

AzureMonitor(WireData)

AzureMonitor(IIS)

AzureActivity

AWS

MicrosoftThreatProtection

AzureFirewall

Zscaler

InfobloxNIOS

GCPDNSDataConnector

NXLogDnsLogs

CiscoUmbrellaDataConnector

Corelight

### Solorigate Network Beacon

Identifies a match across various data feeds for domains IOCs related to the Solorigate incident.

References: https://blogs.microsoft.com/on-the-issues/2020/12/13/customers-protect-nation-state-cyberattacks/,

https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html?1

**Required Data Connectors**

DNS

AzureMonitor(VMInsights)

CiscoASA

PaloAltoNetworks

MicrosoftThreatProtection

AzureFirewall

Zscaler

InfobloxNIOS

GCPDNSDataConnector

NXLogDnsLogs

CiscoUmbrellaDataConnector

Corelight

### Solorigate Domains Found in VM Insights

Identifies connections to Solorigate-related DNS records based on VM insights data

**Required Data Connectors**

AzureMonitor(VMInsights)

AzureMonitor(VMInsights)

AzureMonitor(VMInsights)

### SOURGUM Actor IOC - July 2021

Identifies a match across IOC's related to an actor tracked by Microsoft as SOURGUM

**Required Data Connectors**

DNS

AzureMonitor(VMInsights)

F5

CiscoASA

PaloAltoNetworks

Fortinet

CheckPoint

CEF

MicrosoftThreatProtection

SecurityEvents

Office365

AzureFirewall

WindowsFirewall

WindowsSecurityEvents

WindowsForwardedEvents

### Possible STRONTIUM attempted credential harvesting - Oct 2020

Surfaces potential STRONTIUM group Office365 credential harvesting attempts within OfficeActivity Logon events.

**Required Data Connectors**

Office365

### SUNSPOT log file creation

This query uses Microsoft Defender for Endpoint data and Windows Event Logs to look for IoCs associated with the SUNSPOT malware shared by Crowdstrike.

More details:

- https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/

- https://techcommunity.microsoft.com/t5/azure-sentinel/monitoring-your-software-build-process-with-azure-sentinel/ba-p/2140807

**Required Data Connectors**

MicrosoftThreatProtection

SecurityEvents

WindowsSecurityEvents

WindowsForwardedEvents

### Tarrask malware IOC - April 2022

Identifies a hash match related to Tarrask malware across various data sources.

Reference: https://www.microsoft.com/security/blog/2022/04/12/tarrask-malware-uses-scheduled-tasks-for-defense-evasion/

**Required Data Connectors**

CiscoASA

PaloAltoNetworks

MicrosoftThreatProtection

SecurityEvents

### THALLIUM domains included in DCU takedown

THALLIUM spearphishing and command and control domains included in December 2019 DCU/MSTIC takedown.

Matches domain name IOCs related to the THALLIUM activity group with CommonSecurityLog, DnsEvents, VMConnection and SecurityEvents dataTypes.

References: https://blogs.microsoft.com/on-the-issues/2019/12/30/microsoft-court-action-against-nation-state-cybercrime/

**Required Data Connectors**

DNS

AzureMonitor(VMInsights)

CiscoASA

PaloAltoNetworks

AzureFirewall

Zscaler

InfobloxNIOS

GCPDNSDataConnector

NXLogDnsLogs

CiscoUmbrellaDataConnector

Corelight

### Alert for IOCs related to Windows/ELF malware - IP, Hash IOCs - September 2021

Identifies a match across various data feeds for IP,hashes and IOCs related to Windows/ELF malware published by Black Lotus Labs

Reference:

https://blog.lumen.com/no-longer-just-theory-black-lotus-labs-uncovers-linux-executables-deployed-as-stealth-windows-loaders

https://github.com/ManuelBerrueta/YARA-rules/blob/master/BlackLotusLabs-WSLMalware/BLL\_SneakyWSL.yar

**Required Data Connectors**

F5

CiscoASA

PaloAltoNetworks

Fortinet

CheckPoint

CEF

MicrosoftThreatProtection

SecurityEvents

AzureFirewall

WindowsFirewall

WindowsSecurityEvents

WindowsForwardedEvents

### Known ZINC Comebacker and Klackring malware hashes

ZINC attacks against security researcher campaign malware hashes.

**Required Data Connectors**

DNS

AzureMonitor(VMInsights)

CiscoASA

PaloAltoNetworks

SecurityEvents

MicrosoftThreatProtection

MicrosoftThreatProtection

MicrosoftThreatProtection

AzureFirewall

Zscaler

InfobloxNIOS

GCPDNSDataConnector

NXLogDnsLogs

CiscoUmbrellaDataConnector

Corelight

WindowsForwardedEvents

### Known ZINC related maldoc hash

Document hash used by ZINC in highly targeted spear phishing campaign.

**Required Data Connectors**

CiscoASA

PaloAltoNetworks

SecurityEvents

## Hunting Queries

### Dev-0056 Command Line Activity November 2021

Legacy IOC based Threat Protection Hunting Query 1

### Dev-0322 Command Line Activity November 2021 (ASIM Version)

Legacy IOC based Threat Protection Hunting Query 2

### Dev-0322 Command Line Activity November 2021

Legacy IOC based Threat Protection Hunting Query 3

### Dev-0322 File Drop Activity November 2021 (ASIM Version)

Legacy IOC based Threat Protection Hunting Query 4

### Dev-0322 File Drop Activity November 2021

Legacy IOC based Threat Protection Hunting Query 5

### Connection from external IP to OMI related Ports

Legacy IOC based Threat Protection Hunting Query 6

### NICKEL Command Line Activity November 2021

Legacy IOC based Threat Protection Hunting Query 7

### Known NICKEL Registry modifications patterns

Legacy IOC based Threat Protection Hunting Query 8

### SolarWinds Inventory

Legacy IOC based Threat Protection Hunting Query 9

### Retrospective hunt for STRONTIUM IP IOCs

Legacy IOC based Threat Protection Hunting Query 10

## Watchlists

## Playbooks

## Parsers

# Log4j Vulnerability Detection

This solution provides content to monitor, detect and investigate signals related to exploitation of a remote code execution (RCE) vulnerability in Apache Log4j 2 thru Microsoft Sentinel.

**Data Connectors:** 0**, Workbooks:** 2**, Analytic Rules:** 4**, Hunting Queries:** 10**, Watchlists:** 1**, Playbooks:** 2, Parsers: 0

## Data Connectors

## Workbooks

### Log4j Post Compromise Hunting

This hunting workbook is intended to help identify activity related to the Log4j compromise discovered in December 2021.

**Required Data Types**

SecurityNestedRecommendation

AzureDiagnostics

OfficeActivity

W3CIISLog

AWSCloudTrail

SigninLogs

AADNonInteractiveUserSignInLogs

imWebSessions

imNetworkSession

### Log4j Impact Assessment

This hunting workbook is intended to help identify activity related to the Log4j compromise discovered in December 2021.

**Required Data Types**

SecurityIncident

SecurityAlert

AzureSecurityCenter

MDfESecureScore\_CL

MDfEExposureScore\_CL

MDfERecommendations\_CL

MDfEVulnerabilitiesList\_CL

## Analytic Rules

### Vulnerable Machines related to log4j CVE-2021-44228

This query uses the Azure Defender Security Nested Recommendations data to find machines vulnerable to log4j CVE-2021-44228. Log4j is an open-source Apache logging library that is used in

many Java-based applications. Security Nested Recommendations data is sent to Microsoft Sentinel using the continuous export feature of Azure Defender(refrence link below).

Reference: https://msrc-blog.microsoft.com/2021/12/11/microsofts-response-to-cve-2021-44228-apache-log4j2/

Reference: https://docs.microsoft.com/azure/security-center/continuous-export?tabs=azure-portal

Reference: https://techcommunity.microsoft.com/t5/microsoft-defender-for-cloud/how-defender-for-cloud-displays-machines-affected-by-log4j/ba-p/3037271

**Required Data Connectors**

(none listed)

### Azure WAF matching for Log4j vuln(CVE-2021-44228)

This query will alert on a positive pattern match by Azure WAF for CVE-2021-44228 log4j vulnerability exploitation attempt. If possible, it then decodes the malicious command for further analysis.

Refrence: https://www.microsoft.com/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation/

**Required Data Connectors**

WAF

### Log4j vulnerability exploit aka Log4Shell IP IOC

Identifies a match across various data feeds for IP IOCs related to the Log4j vulnerability exploit aka Log4Shell described in CVE-2021-44228.

References: https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-44228

**Required Data Connectors**

Office365

DNS

AzureMonitor(VMInsights)

CiscoASA

PaloAltoNetworks

SecurityEvents

AzureActiveDirectory

AzureActiveDirectory

AzureMonitor(WireData)

AzureMonitor(IIS)

AzureActivity

AWS

MicrosoftThreatProtection

AzureFirewall

### User agent search for log4j exploitation attempt

This query uses various log sources having user agent data to look for log4j CVE-2021-44228 exploitation attempt based on user agent pattern. Log4j is an open-source Apache logging library that is used in

many Java-based applications. The regex and the string matching look for the most common attacks. This might not be comprehensive to detect every possible user agent variation.

Reference: https://msrc-blog.microsoft.com/2021/12/11/microsofts-response-to-cve-2021-44228-apache-log4j2/

**Required Data Connectors**

SquidProxy

Zscaler

WAF

Office365

AzureActiveDirectory

AzureActiveDirectory

AWS

AzureMonitor(IIS)

## Hunting Queries

### Azure WAF Log4j CVE-2021-44228 hunting

Apache Log4j Vulnerability Detection Hunting Query 1

### Malicious Connection to LDAP port for CVE-2021-44228 vulnerability

Apache Log4j Vulnerability Detection Hunting Query 2

### Suspicious manipulation of firewall detected via Syslog data

Apache Log4j Vulnerability Detection Hunting Query 3

### Possible exploitation of Apache log4j component detected

Apache Log4j Vulnerability Detection Hunting Query 4

### Linux security related process termination activity detected

Apache Log4j Vulnerability Detection Hunting Query 5

### Suspicious Shell script detected

Apache Log4j Vulnerability Detection Hunting Query 6

### Suspicious Base64 download activity detected

Apache Log4j Vulnerability Detection Hunting Query 7

### Possible Container Miner related artifacts detected

Apache Log4j Vulnerability Detection Hunting Query 8

### Possible Linux attack toolkit detected via Syslog data

Apache Log4j Vulnerability Detection Hunting Query 9

### Network Connection to New External LDAP Server

Apache Log4j Vulnerability Detection Hunting Query 10

## Watchlists

### Campaign

Watchlist provide lookup for IOC of different sources.

## Playbooks

### BatchImportToSentinel

These playbooks automate the ingest of threat indicators into the ThreatIntelligenceIndicator table of an Microsoft Sentinel workspace. Sample data for Log4j IOC can be found at https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/Sample%20Data/Feeds/Log4j\_IOC\_List.csv.1. You must deploy the BatchImportToSentinel playbook before deploying the Log4jIndicatorProcessor playbook. 2. During the deployment of Log4jIndicatorProcessor playbook, Playbook2 parameter name should be that of BatchImportToSentinel(default).

### Log4jIndicatorProcessor

These playbooks automate the ingest of threat indicators into the ThreatIntelligenceIndicator table of an Microsoft Sentinel workspace. Sample data for Log4j IOC can be found at https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/Sample%20Data/Feeds/Log4j\_IOC\_List.csv.1. You must deploy the BatchImportToSentinel playbook before deploying the Log4jIndicatorProcessor playbook. 2. During the deployment of Log4jIndicatorProcessor playbook, Playbook2 parameter name should be that of BatchImportToSentinel(default).

## Parsers

# Lookout Cloud Security Platform for Microsoft Sentinel

Deploy the Lookout connector and associated Workbook to receive Lookout Cloud Security data protection compliance violations and threat alerts in Microsoft Sentinel SIEM to enable integrated security visibility and response.

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

## Data Connectors

### Lookout Cloud Security for Microsoft Sentinel (using Azure Function)

This connector uses a Agari REST API connection to push data into Microsoft Sentinel Log Analytics.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### LookoutCSActivities

Category: Samples

Function Alias: LookoutCSActivities

### LookoutCSAnomalies

Category: Samples

Function Alias: LookoutCSAnomalies

### LookoutCSViolations

Category: Samples

Function Alias: LookoutCSViolations

# Lookout Mobile Threat Defense for Microsoft Sentinel

Deploy the Lookout connector and associated Workbook to receive Lookout mobile security threat alerts and device status updates in Microsoft Sentinel SIEM for integrated security visibility and response.

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

## Data Connectors

### Lookout (using Azure Function)

The [Lookout](https://lookout.com) data connector provides the capability to ingest [Lookout](https://enterprise.support.lookout.com/hc/en-us/articles/115002741773-Mobile-Risk-API-Guide#commoneventfields) events into Microsoft Sentinel through the Mobile Risk API. Refer to [API documentation](https://enterprise.support.lookout.com/hc/en-us/articles/115002741773-Mobile-Risk-API-Guide) for more information. The [Lookout](https://lookout.com) data connector provides ability to get events which helps to examine potential security risks and more.

## Workbooks

### Lookout

Sets the time name for analysis

**Required Data Types**

Lookout\_CL

LookoutAPI

## Analytic Rules

### Lookout - New Threat events found.

Created to detect new Threat events from the data which is recently synced by Lookout Solution.

**Required Data Connectors**

LookoutAPI

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### Lookout Data Parser

Category: Samples

Function Alias: LookoutEvents

# MarkLogic Audit

The MarkLogic Solution provides the capability to ingest MarkLogic Audit logs into Microsoft Sentinel. Refer to MarkLogic documentation for more information.

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

## Data Connectors

### MarkLogic Audit

MarkLogic data connector provides the capability to ingest [MarkLogicAudit](https://www.marklogic.com/) logs into Microsoft Sentinel. Refer to [MarkLogic documentation](https://docs.marklogic.com/guide/getting-started) for more information.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### MarkLogicAudit

Category: Samples

Function Alias: MarkLogicAudit

# Maturity Model For Event Log Management M2131

This solution is designed to enable Cloud Architects, Security Engineers, and Governance Risk Compliance Professionals to increase visibility before, during, and after a cybersecurity incident.

**Data Connectors:** 0**, Workbooks:** 1**, Analytic Rules:** 8**, Hunting Queries:** 4**, Watchlists:** 0**, Playbooks:** 3, Parsers: 0

## Data Connectors

## Workbooks

### MaturityModelForEventLogManagementM2131

Select the time range for this Overview.

**Required Data Types**

## Analytic Rules

### M2131\_AssetStoppedLogging

This alert is designed to monitor assets within the Maturity Model for Event Log Management (M-21-31) standard. The alert triggers when a monitored asset fails to provide a heartbeat within 24 hours.

**Required Data Connectors**

(none listed)

### M2131\_DataConnectorAddedChangedRemoved

This alert is designed to monitor data connector configurations. This alert is triggered when a data connector is added, updated, or deleted.

**Required Data Connectors**

(none listed)

### M2131\_EventLogManagementPostureChanged\_EL0

This alert is desinged to monitor Azure policies aligned with the Maturity Model for Event Log Management (M-21-31) standard. The alert triggers when EL0 policy compliance falls below 70% within a 1 week timeframe.

**Required Data Connectors**

(none listed)

### M2131\_EventLogManagementPostureChanged\_EL1

This alert is desinged to monitor Azure policies aligned with the Maturity Model for Event Log Management (M-21-31) standard. The alert triggers when EL1 policy compliance falls below 70% within a 1 week timeframe.

**Required Data Connectors**

(none listed)

### M2131\_EventLogManagementPostureChanged\_EL2

This alert is desinged to monitor Azure policies aligned with the Maturity Model for Event Log Management (M-21-31) standard. The alert triggers when EL2 policy compliance falls below 70% within a 1 week timeframe.

**Required Data Connectors**

(none listed)

### M2131\_EventLogManagementPostureChanged\_EL3

This alert is desinged to monitor Azure policies aligned with the Maturity Model for Event Log Management (M-21-31) standard. The alert triggers when EL3 policy compliance falls below 70% within a 1 week timeframe.

**Required Data Connectors**

(none listed)

### M2131\_LogRetentionLessThan1Year

This alert is designed to monitor log retention within the Maturity Model for Event Log Management (M-21-31) standard. The alert triggers when a log analytics workspace in active storage is configured for less than 1 year.

**Required Data Connectors**

(none listed)

### M2131\_RecommendedDatatableUnhealthy

This alert is designed to monitor recommended data tables aligned to the Maturity Model for Event Log Management (M-21-31) standard. The alert triggers when a recommended data table hasn't been observed in over 48 hours.

**Required Data Connectors**

(none listed)

## Hunting Queries

### M2131\_RecommendedDatatableNotLogged\_EL0

MaturityModelForEventLogManagementM2131 Hunting Query 1

### M2131\_RecommendedDatatableNotLogged\_EL1

MaturityModelForEventLogManagementM2131 Hunting Query 2

### M2131\_RecommendedDatatableNotLogged\_EL2

MaturityModelForEventLogManagementM2131 Hunting Query 3

### M2131\_RecommendedDatatableNotLogged\_EL3

MaturityModelForEventLogManagementM2131 Hunting Query 4

## Watchlists

## Playbooks

### Notify-LogManagementTeam

This Security Orchestration, Automation, & Response (SOAR) capability is designed for configuration with the solution's analytics rules. When analytics rules trigger this automation notifies the log management team of respective details via Teams chat and exchange email. this automation reduces requirements to manually monitor the workbook or analytics rules while increasing response times.

### Create-AzureDevOpsTask

This playbook will create the Azure DevOps task filled with the Microsoft Sentinel incident details.

### Create Jira Issue

This playbook will open a Jira Issue when a new incident is opened in Microsoft Sentinel.

## Parsers

# McAfee ePolicy Orchestrator Solution

The McAfee ePO is a centralized policy management and enforcement for your endpoints and enterprise security products. McAfee ePO monitors and manages your network, detecting threats and protecting endpoints against these threats.

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 14**, Hunting Queries:** 10**, Watchlists:** 0**, Playbooks:** 0, Parsers: 1

## Data Connectors

### McAfee ePolicy Orchestrator (ePO)

The McAfee ePolicy Orchestrator data connector provides the capability to ingest [McAfee ePO](https://www.mcafee.com/enterprise/en-us/products/epolicy-orchestrator.html) events into Microsoft Sentinel through the syslog. Refer to [documentation](https://docs.mcafee.com/bundle/epolicy-orchestrator-landing/page/GUID-0C40020F-5B7F-4549-B9CC-0E017BC8797F.html) for more information.

## Workbooks

### McAfee ePolicy Orchestrator

Sets the time name for analysis

**Required Data Types**

## Analytic Rules

### McAfee ePO - Agent Handler down

Detects when AgentHandler is down.

**Required Data Connectors**

McAfeeePO

### McAfee ePO - Error sending alert

Detects when error sending alert occurs.

**Required Data Connectors**

McAfeeePO

### McAfee ePO - Attempt uninstall McAfee agent

Detects attempts uninstalling McAfee agent on host.

**Required Data Connectors**

McAfeeePO

### McAfee ePO - Deployment failed

Detects when errors occur during deployment new changes/policies.

**Required Data Connectors**

McAfeeePO

### McAfee ePO - File added to exceptions

Detects when file was added to exception list on a host.

**Required Data Connectors**

McAfeeePO

### McAfee ePO - Firewall disabled

Detects when firewall was disabled from Mctray.

**Required Data Connectors**

McAfeeePO

### McAfee ePO - Logging error occurred

Detects when logging errors on agent.

**Required Data Connectors**

McAfeeePO

### McAfee ePO - Multiple threats on same host

Rule fires when multiple threat events were detected on the same host.

**Required Data Connectors**

McAfeeePO

### McAfee ePO - Scanning engine disabled

Detects when OAS scanning engine was disabled.

**Required Data Connectors**

McAfeeePO

### McAfee ePO - Spam Email detected

Detects when email was marked as spam.

**Required Data Connectors**

McAfeeePO

### McAfee ePO - Task error

Detects when task error occurs.

**Required Data Connectors**

McAfeeePO

### McAfee ePO - Threat was not blocked

Detects when a threat was not blocked on a host.

**Required Data Connectors**

McAfeeePO

### McAfee ePO - Unable to clean or delete infected file

Detects when McAfee failed to clean or delete infected file.

**Required Data Connectors**

McAfeeePO

### McAfee ePO - Update failed

Detects when update failed event occurs on agent.

**Required Data Connectors**

McAfeeePO

## Hunting Queries

### McAfee ePO - Agent Errors

McAfee ePolicy Orchestrator Hunting Query 1

### McAfee ePO - Applications blocked or contained

McAfee ePolicy Orchestrator Hunting Query 2

### McAfee ePO - Email Treats

McAfee ePolicy Orchestrator Hunting Query 3

### McAfee ePO - Infected files by source

McAfee ePolicy Orchestrator Hunting Query 4

### McAfee ePO - Infected Systems

McAfee ePolicy Orchestrator Hunting Query 5

### McAfee ePO - Long term infected systems

McAfee ePolicy Orchestrator Hunting Query 6

### McAfee ePO - Sources with multiple threats

McAfee ePolicy Orchestrator Hunting Query 7

### McAfee ePO - Objects not scanned

McAfee ePolicy Orchestrator Hunting Query 8

### McAfee ePO - Scan Errors

McAfee ePolicy Orchestrator Hunting Query 9

### McAfee ePO - Threats detected and not blocked, cleaned or deleted

McAfee ePolicy Orchestrator Hunting Query 10

## Watchlists

## Playbooks

## Parsers

### McAfeeePO Data Parser

Category: Samples

Function Alias: McAfeeEPOEvent

# McAfee Network Security Platform Solution

McAfee Network Security Platform expands network protection across virtualized environments to provide intelligent threat protection for virtual networks.

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

## Data Connectors

### McAfee Network Security Platform

The [McAfee® Network Security Platform](https://www.mcafee.com/enterprise/en-us/products/network-security-platform.html) data connector provides the capability to ingest [McAfee® Network Security Platform events](https://docs.mcafee.com/bundle/network-security-platform-10.1.x-integration-guide-unmanaged/page/GUID-8C706BE9-6AC9-4641-8A53-8910B51207D8.html) into Microsoft Sentinel. Refer to [McAfee® Network Security Platform](https://docs.mcafee.com/bundle/network-security-platform-10.1.x-integration-guide-unmanaged/page/GUID-F7D281EC-1CC9-4962-A7A3-5A9D9584670E.html) for more information.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### McAfee Network Security Platform Data Parser

Category: Samples

Function Alias: McAfeeNSPEvent

# Microsoft 365 Defender solution for Sentinel

The Microsoft 365 Defender solution for Microsoft Sentinel enables you to ingest Security Alerts/Incidents and raw logs from the products within Microsoft 365 Defender suite into Microsoft Sentinel.

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

## Data Connectors

### Microsoft 365 Defender

Microsoft 365 Defender​ is a unified, natively integrated, pre- and post-breach enterprise defense suite that protects endpoint, identity, email, and applications and helps you detect, prevent, investigate, and automatically respond to sophisticated threats.

Microsoft 365 Defender suite includes:

- Microsoft Defender for Endpoint

- Microsoft Defender for Identity

- Microsoft Defender for Office 365

- Threat & Vulnerability Management

- Microsoft Defender for Cloud Apps

For more information, see the [Microsoft Sentinel documentation](https://go.microsoft.com/fwlink/p/?linkid=2220004&wt.mc\_id=sentinel\_dataconnectordocs\_content\_cnl\_csasci).

## Workbooks

### Microsoft 365 Defender MDOWorkbook

Gain extensive insight into your organization's Microsoft Defender for Office Activity by analyzing, and correlating events.

You can track malware and phishing detection over time.

**Required Data Types**

SecurityAlert

MicrosoftThreatProtection

## Analytic Rules

### SUNSPOT malware hashes

This query uses Microsoft Defender for Endpoint data to look for IoCs associated with the SUNSPOT malware shared by Crowdstrike.

More details:

- https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/

- https://techcommunity.microsoft.com/t5/azure-sentinel/monitoring-your-software-build-process-with-azure-sentinel/ba-p/2140807

**Required Data Connectors**

MicrosoftThreatProtection

### Potential Build Process Compromise - MDE

The query looks for source code files being modified immediately after a build process is started. The purpose of this is to look for malicious code injection during the build process. This query uses Microsoft Defender for Endpoint telemetry.

More details: https://techcommunity.microsoft.com/t5/azure-sentinel/monitoring-the-software-supply-chain-with-azure-sentinel/ba-p/2176463

**Required Data Connectors**

MicrosoftThreatProtection

### TEARDROP memory-only dropper

Identifies SolarWinds TEARDROP memory-only dropper IOCs in Window's defender Exploit Guard activity

References:

- https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

- https://gist.github.com/olafhartong/71ffdd4cab4b6acd5cbcd1a0691ff82f

**Required Data Connectors**

MicrosoftThreatProtection

### SUNBURST network beacons

Identifies SolarWinds SUNBURST domain beacon IOCs in DeviceNetworkEvents

References:

- https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

- https://gist.github.com/olafhartong/71ffdd4cab4b6acd5cbcd1a0691ff82f

**Required Data Connectors**

MicrosoftThreatProtection

### SUNBURST and SUPERNOVA backdoor hashes

Identifies SolarWinds SUNBURST and SUPERNOVA backdoor file hash IOCs in DeviceFileEvents

References:

- https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

- https://gist.github.com/olafhartong/71ffdd4cab4b6acd5cbcd1a0691ff82f

**Required Data Connectors**

MicrosoftThreatProtection

### AV detections related to Ukraine threats

This query looks for Microsoft Defender AV detections for malware observed in relation to the war in Ukraine.

Ref: https://msrc-blog.microsoft.com/2022/02/28/analysis-resources-cyber-threat-activity-ukraine/

**Required Data Connectors**

MicrosoftThreatProtection

### AV detections related to Tarrask malware

This query looks for Microsoft Defender AV detections related to Tarrask malware. In Microsoft Sentinel the SecurityAlerts table

includes only the Device Name of the affected device, this query joins the DeviceInfo table to clearly connect other information such as Device group, ip, logged on users etc.

This would allow the Microsoft Sentinel analyst to have more context related to the alert, if available.

Reference: https://www.microsoft.com/security/blog/2022/04/12/tarrask-malware-uses-scheduled-tasks-for-defense-evasion/

**Required Data Connectors**

MicrosoftThreatProtection

### AV detections related to SpringShell Vulnerability

This query looks for Microsoft Defender AV detections related to SpringShell Vulnerability. In Microsoft Sentinel the SecurityAlerts table includes only the Device Name of the affected device,

this query joins the DeviceInfo table to clearly connect other information such as Device group, ip, logged on users etc. This would allow the Microsoft Sentinel analyst to have more context related to the alert, if available.

Reference: https://www.microsoft.com/security/blog/2022/04/04/springshell-rce-vulnerability-guidance-for-protecting-against-and-detecting-cve-2022-22965/

**Required Data Connectors**

MicrosoftThreatProtection

## Hunting Queries

Appspot Phishing Abuse

Microsoft 365 Defender Hunting Query 1

### Check for spoofing attempts on the domain with Authentication failures

Microsoft 365 Defender Hunting Query 2

### Determines emails sent by top malicious/bad IP addresses.

Microsoft 365 Defender Hunting Query 3

### Determines phising emails sent delivered to Inbox/Junk folder.

Microsoft 365 Defender Hunting Query 4

## Watchlists

## Playbooks

## Parsers

# Microsoft 365 solution for Sentinel

The Microsoft 365 solution for Microsoft Sentinel enables you to ingest operational logs from Microsoft 365 to gain insights into user and admin activity across your collaboration platforms such as Teams, SharePoint and Exchange.

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

## Data Connectors

### Office 365

The Office 365 activity log connector provides insight into ongoing user activities. You will get details of operations such as file downloads, access requests sent, changes to group events, set-mailbox and details of the user who performed the actions. By connecting Office 365 logs into Microsoft Sentinel you can use this data to view dashboards, create custom alerts, and improve your investigation process. For more information, see the [Microsoft Sentinel documentation](https://go.microsoft.com/fwlink/p/?linkid=2219943&wt.mc\_id=sentinel\_dataconnectordocs\_content\_cnl\_csasci).

## Workbooks

### SharePoint & OneDrive

Gain insights into SharePoint and OneDrive by tracing and analyzing all operations and activities.

You can view trends across user operation, find correlations between users and files, and identify interesting information such as user IP addresses.

**Required Data Types**

OfficeActivity

Office365

### Office 365

Gain insights into Office 365 by tracing and analyzing all operations and activities. You can drill down into your SharePoint, OneDrive, and Exchange.

This workbook lets you find usage trends across users, files, folders, and mailboxes, making it easier to identify anomalies in your network.

**Required Data Types**

OfficeActivity

Office365

### Exchange Online

Gain insights into Microsoft Exchange online by tracing and analyzing all Exchange operations and user activities.

This workbook let you monitor user activities, including logins, account operations, permission changes, and mailbox creations to discover suspicious trends among them.

**Required Data Types**

OfficeActivity

Office365

## Analytic Rules

### Accessed files shared by temporary external user

This detection identifies an external user is added to a Team or Teams chat

and shares a files which is accessed by many users (>10) and the users is removed within short period of time. This might be

an indicator of suspicious activity.

**Required Data Connectors**

Office365

### External user added and removed in short timeframe

This detection flags the occurances of external user accounts that are added to a Team and then removed within

one hour.

**Required Data Connectors**

Office365

### Exchange workflow MailItemsAccessed operation anomaly

Identifies anomalous increases in Exchange mail items accessed operations.

The query leverages KQL built-in anomaly detection algorithms to find large deviations from baseline patterns.

Sudden increases in execution frequency of sensitive actions should be further investigated for malicious activity.

Manually change scorethreshold from 1.5 to 3 or higher to reduce the noise based on outliers flagged from the query criteria.

Read more about MailItemsAccessed- https://docs.microsoft.com/microsoft-365/compliance/advanced-audit?view=o365-worldwide#mailitemsaccessed

**Required Data Connectors**

Office365

### Mail redirect via ExO transport rule

Identifies when Exchange Online transport rule configured to forward emails.

This could be an adversary mailbox configured to collect mail from multiple user accounts.

**Required Data Connectors**

Office365

### Malicious Inbox Rule

Often times after the initial compromise the attackers create inbox rules to delete emails that contain certain keywords.

This is done so as to limit ability to warn compromised users that they've been compromised. Below is a sample query that tries to detect this.

Reference: https://www.reddit.com/r/sysadmin/comments/7kyp0a/recent\_phishing\_attempts\_my\_experience\_and\_what/

**Required Data Connectors**

Office365

### Multiple Teams deleted by a single user

This detection flags the occurrences of deleting multiple teams within an hour.

This data is a part of Office 365 Connector in Microsoft Sentinel.

**Required Data Connectors**

Office365

### Multiple users email forwarded to same destination

Identifies when multiple (more than one) users mailboxes are configured to forward to the same destination.

This could be an attacker-controlled destination mailbox configured to collect mail from multiple compromised user accounts.

**Required Data Connectors**

Office365

### New executable via Office FileUploaded Operation

Identifies when executable file types are uploaded to Office services such as SharePoint and OneDrive.

List currently includes 'exe', 'inf', 'gzip', 'cmd', 'bat' file extensions.

Additionally, identifies when a given user is uploading these files to another users workspace.

This may be indication of a staging location for malware or other malicious activity.

**Required Data Connectors**

Office365

### Rare and potentially high-risk Office operations

Identifies Office operations that are typically rare and can provide capabilities useful to attackers.

**Required Data Connectors**

Office365

### SharePointFileOperation via previously unseen IPs

Identifies when the volume of documents uploaded to or downloaded from Sharepoint by new IP addresses

exceeds a threshold (default is 50).

**Required Data Connectors**

Office365

### SharePointFileOperation via devices with previously unseen user agents

Identifies if the number of documents uploaded or downloaded from device(s) associated

with a previously unseen user agent exceeds a threshold (default is 5).

**Required Data Connectors**

Office365

### Possible STRONTIUM attempted credential harvesting - Sept 2020

Surfaces potential STRONTIUM group Office365 credential harvesting attempts within OfficeActivity Logon events.

References: https://www.microsoft.com/security/blog/2020/09/10/strontium-detecting-new-patters-credential-harvesting/.

**Required Data Connectors**

Office365

### Exchange AuditLog disabled

Identifies when the exchange audit logging has been disabled which may be an adversary attempt

to evade detection or avoid other defenses.

**Required Data Connectors**

Office365

### Office policy tampering

Identifies if any tampering is done to either auditlog, ATP Safelink, SafeAttachment, AntiPhish or Dlp policy.

An adversary may use this technique to evade detection or avoid other policy based defenses.

References: https://docs.microsoft.com/powershell/module/exchange/advanced-threat-protection/remove-antiphishrule?view=exchange-ps.

**Required Data Connectors**

Office365

## Hunting Queries

### Anomalous access to other user's mailboxes

Microsoft 365 Hunting Query 1

### External user added and removed in a short timeframe - Hunt Version

Microsoft 365 Hunting Query 2

### External user from a new organisation added to Teams

Microsoft 365 Hunting Query 3

### Mail redirect via ExO transport rule

Microsoft 365 Hunting Query 4

### Bots added to multiple teams

Microsoft 365 Hunting Query 5

### User made Owner of multiple teams

Microsoft 365 Hunting Query 6

### Multiple Teams deleted by a single user

Microsoft 365 Hunting Query 7

### Previously unseen bot or application added to Teams

Microsoft 365 Hunting Query 8

### New Windows Reserved Filenames staged on Office file services

Microsoft 365 Hunting Query 9

### Office Mail Forwarding - Hunting Version

Microsoft 365 Hunting Query 10

### Files uploaded to teams and access summary

Microsoft 365 Hunting Query 11

### User added to Team and immediately uploads file

Microsoft 365 Hunting Query 12

### Windows Reserved Filenames staged on Office file services

Microsoft 365 Hunting Query 13

### Exes with double file extension and access summary

Microsoft 365 Hunting Query 14

### New Admin account activity seen which was not seen historically

Microsoft 365 Hunting Query 15

### SharePointFileOperation via previously unseen IPs

Microsoft 365 Hunting Query 16

### SharePointFileOperation via devices with previously unseen user agents

Microsoft 365 Hunting Query 17

### Non-owner mailbox login activity

Microsoft 365 Hunting Query 18

### Powershell or non-browser mailbox login activity

Microsoft 365 Hunting Query 19

### SharePointFileOperation via clientIP with previously unseen user agents

Microsoft 365 Hunting Query 20

## Watchlists

## Playbooks

## Parsers

# Microsoft Defender for Cloud Apps solution for Sentinel

Microsoft Defender for Cloud Apps

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

## Data Connectors

### Microsoft Defender for Cloud Apps

By connecting with [Microsoft Defender for Cloud Apps](https://aka.ms/asi-mcas-connector-description) you will gain visibility into your cloud apps, get sophisticated analytics to identify and combat cyberthreats, and control how your data travels.

- Identify shadow IT cloud apps on your network.

- Control and limit access based on conditions and session context.

- Use built-in or custom policies for data sharing and data loss prevention.

- Identify high-risk use and get alerts for unusual user activities with Microsoft behavioral analytics and anomaly detection capabilities, including ransomware activity, impossible travel, suspicious email forwarding rules, and mass download of files.

- Mass download of files

[Deploy now >](https://aka.ms/asi-mcas-connector-deploynow)

## Workbooks

### Microsoft Cloud App Security - discovery logs

Using this workbook, you can identify which cloud apps are being used in your organization, gain insights from usage trends and drill down to a specific user and application

**Required Data Types**

McasShadowItReporting

MicrosoftCloudAppSecurity

## Analytic Rules

### Linked Malicious Storage Artifacts

An IP address which uploaded malicious content to an Azure Blob or File Storage container (triggering a malware alert) also uploaded additional files.

**Required Data Connectors**

MicrosoftCloudAppSecurity

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Microsoft Defender for Cloud solution for Sentinel

The Microsoft Defender for Cloud solution for Microsoft Sentinel allows you to ingest Security alerts reported in Microsoft Defender for Cloud on assessing your hybrid cloud workload's security posture.

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

## Data Connectors

### Microsoft Defender for Cloud

Microsoft Defender for Cloud is a security management tool that allows you to detect and quickly respond to threats across Azure, hybrid, and multi-cloud workloads. This connector allows you to stream your security alerts from Microsoft Defender for Cloud into Microsoft Sentinel, so you can view Defender data in workbooks, query it to produce alerts, and investigate and respond to incidents.

[For more information>](https://aka.ms/ASC-Connector)

## Workbooks

## Analytic Rules

### CoreBackUp Deletion in correlation with other related security alerts

This query will help detect attackers attempt to delete backup containers in correlation with other alerts that could have triggered to help possibly reveal more details of attacker activity.

Though such an activity could be legitimate as part of business operation, some ransomware actors may perform such operation to cause interruption to regular business services.

**Required Data Connectors**

AzureSecurityCenter

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Microsoft Defender for Endpoint

Microsoft Defender for Endpoint is an enterprise endpoint security platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats .

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 1**, Hunting Queries:** 2**, Watchlists:** 0**, Playbooks:** 20, Parsers: 2

## Data Connectors

### Microsoft Defender for Endpoint

Microsoft Defender for Endpoint is a security platform designed to prevent, detect, investigate, and respond to advanced threats. The platform creates alerts when suspicious security events are seen in an organization. Fetch alerts generated in Microsoft Defender for Endpoint to Microsoft Sentinel so that you can effectively analyze security events. You can create rules, build dashboards and author playbooks for immediate response. For more information, see the [Microsoft Sentinel documentation >](https://go.microsoft.com/fwlink/p/?linkid=2220128&wt.mc\_id=sentinel\_dataconnectordocs\_content\_cnl\_csasci).

## Workbooks

### MicrosoftDefenderForEndPoint

A wokbook to provide details about Microsoft Defender for Endpoint Advance Hunting to Overview & Analyse data brought through M365 Defender Connector.

**Required Data Types**

## Analytic Rules

### ACTINIUM AV hits - Feb 2022

Identifies a match in the Security Alert table for MDATP hits related to the ACTINIUM actor

**Required Data Connectors**

MicrosoftDefenderAdvancedThreatProtection

## Hunting Queries

### Probable AdFind Recon Tool Usage

MicrosoftDefenderForEndpoint Hunting Query 1

### SUNBURST suspicious SolarWinds child processes

MicrosoftDefenderForEndpoint Hunting Query 2

## Watchlists

## Playbooks

### Isolate MDE Machine - Alert Triggered

This playbook will isolate (full) the machine in Microsoft Defender for Endpoint.

### Isolate endpoint - MDE - Incident Triggered

This playbook will isolate (full) the machine in Microsoft Defender for Endpoint.

### Restrict MDE App Execution - Alert Triggered

This playbook will restrict app execution on the machine in Microsoft Defender for Endpoint.

### Restrict MDE App Execution - Incident Triggered

This playbook will restrict app execution on the machine in Microsoft Defender for Endpoint.

### Restrict MDE Domain - Alert Triggered

This play book will take DNS entities and generate alert and block threat indicators for each domain in Microsoft Defender for Endpoint for 90 days.

### Restrict MDE Domain - Incident Triggered

This play book will take DNS entities and generate alert and block threat indicators for each domain in Microsoft Defender for Endpoint for 90 days.

### Restrict MDE FileHash - Alert Triggered

This playbook will take FileHash entities and generate alert and block threat indicators for each file hash in MDE for 90 days.

### Restrict MDE FileHash - Incident Triggered

This playbook will take FileHash entities and generate alert and block threat indicators for each file hash in MDE for 90 days.

### Restrict MDE Ip Address - Alert Triggered

This playbook will take IP entities and generate alert and block threat indicators for each IP in MDE for 90 days.

### Restrict MDE Ip Address - Incident Triggered

This playbook will take IP entities and generate alert and block threat indicators for each IP in MDE for 90 days.

### Restrict MDE Url - Alert Triggered

This playbook will take Url entities and generate alert and block threat indicators for each IP in MDE for 90 days.

### Restrict MDE Url - Incident Triggered

This playbook will take Url entities and generate alert and block threat indicators for each IP in MDE for 90 days.

### Run MDE Antivirus - Alert Triggered

This playbook will run a antivirus (full) scan on the machine in Microsoft Defender for Endpoint.

### Run MDE Antivirus - Incident Triggered

This playbook will run a antivirus (full) scan on the machine in Microsoft Defender for Endpoint.

### Unisolate MDE Machine - Alert Triggered

This playbook will release a machine from isolation in Microsoft Defender for Endpoint.

### Unisolate MDE Machine - Incident Triggered

This playbook will release a machine from isolation in Microsoft Defender for Endpoint.

### Restrict MDE Domain - Entity Triggered

This playbook will take the triggering entity and generate an alert and block threat indicator for the domain in MDE for 90 days.

### Restrict MDE FileHash - Entity Triggered

This playbook will take the triggering FileHash entity and generate an alert and block threat indicator for the file hash in MDE for 90 days.

### Restrict MDE Ip Address - Entity Triggered

This playbook will and generate alert and block threat indicators for the IP entity in MDE for 90 days.

### Restrict MDE URL - Entity Triggered

This playbook will take the triggering entity and generate an alert and block threat indicator for the URL in MDE for 90 days.

## Parsers

### AssignedIPAddress

Category: Samples

Function Alias: AssignedIPAddress

### Devicefromip

Category: Samples

Function Alias: Devicefromip

# Microsoft Defender for Identity solution for Sentinel

The Microsoft Defender for Identity solution for Microsoft Sentinel allows you to ingest security alerts reported in the Microsoft Defender for Identity platform to get better insights into the identity posture of your organization’s Active Directory envir

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

## Data Connectors

### Microsoft Defender for Identity

Connect Microsoft Defender for Identity to gain visibility into the events and user analytics. Microsoft Defender for Identity identifies, detects, and helps you investigate advanced threats, compromised identities, and malicious insider actions directed at your organization. Microsoft Defender for Identity enables SecOp analysts and security professionals struggling to detect advanced attacks in hybrid environments to:

- Monitor users, entity behavior, and activities with learning-based analytics​

- Protect user identities and credentials stored in Active Directory

- Identify and investigate suspicious user activities and advanced attacks throughout the kill chain

- Provide clear incident information on a simple timeline for fast triage

[Try now >](https://aka.ms/AtpTryNow)

[Deploy now >](https://aka.ms/AzureATP\_Deploy)

For more information, see the [Microsoft Sentinel documentation](https://go.microsoft.com/fwlink/p/?linkid=2220069&wt.mc\_id=sentinel\_dataconnectordocs\_content\_cnl\_csasci).

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Microsoft Defender for IoT solution for Microsoft Sentinel

The Microsoft Defender for IoT solution for Microsoft Sentinel allows you to ingest Security alerts reported in Microsoft Defender for IoT on assessing your Internet of Things (IoT)/Operational Technology (OT) infrastructure.

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 15**, Hunting Queries:** 0**, Watchlists:** 0**, Playbooks:** 7, Parsers: 0

## Data Connectors

### Microsoft Defender for IoT

Gain insights into your IoT security by connecting Microsoft Defender for IoT alerts to Microsoft Sentinel.

You can get out-of-the-box alert metrics and data, including alert trends, top alerts, and alert breakdown by severity.

You can also get information about the recommendations provided for your IoT hubs including top recommendations and recommendations by severity. For more information, see the [Microsoft Sentinel documentation >](https://go.microsoft.com/fwlink/p/?linkid=2224002&wt.mc\_id=sentinel\_dataconnectordocs\_content\_cnl\_csasci).

## Workbooks

### Microsoft Defender for IoT

The OT Threat Monitoring with Defender for IoT Workbook features OT filtering for Security Alerts, Incidents, Vulnerabilities and Asset Inventory. The workbook features a dynamic assessment of the MITRE ATT&CK for ICS matrix across your environment to analyze and respond to OT-based threats. This workbook is designed to enable SecOps Analysts, Security Engineers, and MSSPs to gain situational awareness for IT/OT security posture.

**Required Data Types**

SecurityAlert

SecurityIncident

## Analytic Rules

### Denial of Service (Microsoft Defender for IoT)

This alert leverages Defender for IoT to detect attacks that would prevent the use or proper operation of a DCS system including Denial of Service events.

**Required Data Connectors**

IoT

### Excessive Login Attempts (Microsoft Defender for IoT)

This alert leverages Defender for IoT to detect excessive login attempts that may indicate improper service configuration, human error, or malicious activity on the network such as a cyber threat attempting to manipulate the SCADA network.

**Required Data Connectors**

IoT

### Firmware Updates (Microsoft Defender for IoT)

This alert leverages Defender for IoT to detect unauthorized firmware updates that may indicate malicious activity on the network such as a cyber threat that attempts to manipulate PLC firmware to compromise PLC function.

**Required Data Connectors**

IoT

### High bandwidth in the network (Microsoft Defender for IoT)

This alert leverages Defender for IoT to detect an unusually high bandwidth which may be an indication of a new service/process or malicious activity on the network. An example scenario is a cyber threat attempting to manipulate the SCADA network.

**Required Data Connectors**

IoT

### No traffic on Sensor Detected (Microsoft Defender for IoT)

This alert leverages Defender for IoT to detect that a sensor can no longer detect the network traffic, which indicates that the system is potentially insecure.

**Required Data Connectors**

IoT

### Illegal Function Codes for ICS traffic (Microsoft Defender for IoT)

This alert leverages Defender for IoT to detect Illegal function codes in SCADA equipment indicating improper application configuration or malicious activity such using illegal values within a protocol to exploit a PLC vulnerability.

**Required Data Connectors**

IoT

### PLC unsecure key state (Microsoft Defender for IoT)

This alert leverages Defender for IoT to detect PLC operating mode changes indicating the PLC is potentially insecure. If the PLC is compromised, devices that interact with it may be impacted. This may affect overall system security and safety.

**Required Data Connectors**

IoT

### Internet Access (Microsoft Defender for IoT)

This alert leverages Defender for IoT to detect an OT device communicating with Internet which is possibly an indication of improper configuration of an application or malicious activity on the network.

**Required Data Connectors**

IoT

### Suspicious malware found in the network (Microsoft Defender for IoT)

This alert leverages Defender for IoT to detect IoT/OT malware found on the network indicating possible attempts to compromise production systems.

**Required Data Connectors**

IoT

### Multiple scans in the network (Microsoft Defender for IoT)

This alert leverages Defender for IoT to detect multiple scans on the network indicating new devices, functionality, application misconfiguration, or malicious reconnaissance activity on the network.

**Required Data Connectors**

IoT

### PLC Stop Command (Microsoft Defender for IoT)

This alert leverages Defender for IoT to detect PLC stop commands which could indicate improper configuration or malicious activity on the network such as a threat manipulating PLC programming to affect the function of the network.

**Required Data Connectors**

IoT

### Unauthorized device in the network (Microsoft Defender for IoT)

This alert leverages Defender for IoT to detect a new device indicating a legitimate device recently installed on the network or an indication of malicious activity such as a cyber threat attempting to manipulate the SCADA network.

**Required Data Connectors**

IoT

### Unauthorized DHCP configuration in the network (Microsoft Defender for IoT)

This alert leverages Defender for IoT to detect an unauthorized DHCP configuration indicating a possible unauthorized device configuration.

**Required Data Connectors**

IoT

### Unauthorized PLC changes (Microsoft Defender for IoT)

This alert leverages Defender for IoT to detect unauthorized changes to PLC ladder logic code indicating new functionality in the PLC, improper configuration of an application, or malicious activity on the network.

**Required Data Connectors**

IoT

### Unauthorized remote access to the network (Microsoft Defender for IoT)

This alert leverages Defender for IoT to detect unauthorized remote access to network devices, if another device on the network is compromised, target devices can be accessed remotely, increasing the attack surface.

**Required Data Connectors**

IoT

## Hunting Queries

## Watchlists

## Playbooks

### AD4IoT-AutoCloseIncidents

In some cases, maintenance activities generate alerts in Sentinel which distracts the SOC team from handling the real problems. This playbook allows to input the time period in which the maintenance is expected and the assets IP (Excel file can be found). The playbook requires a watchlist which includes all the IP addresses of the assets on which alerts will handled automatically. This playbook parses explicitly the IoT device entity fields. For more information, see [AD4IoT-AutoCloseIncidents](https://github.com/Azure/Azure-Sentinel/tree/master/Playbooks/AD4IoT-AutoCloseIncidents)

### AD4IoT-MailByProductionLine

The following playbook will send mail to notify specific stake holders. One example can be in the case of specific security team per product line or per physical location. This playbook requires a watchlist which maps between the sensors name and the mail addresses of the alerts stockholders. For more information, see [AD4IoT-MailbyProductionLine](https://github.com/Azure/Azure-Sentinel/tree/master/Playbooks/AD4IoT-MailbyProductionLine)

### AD4IoT-NewAssetServiceNowTicket

Normally, the authorized entity to program a PLC is the Engineering Workstation, to program a PLC attackers might create a new Engineering Workstation to create malicious programing. The following playbook will open a ticket in ServiceNow each time a new Engineering Workstation is detected. This playbook parses explicitly the IoT device entity fields. For more information, see [AD4IoT-NewAssetServiceNowTicket](https://github.com/Azure/Azure-Sentinel/blob/master/Playbooks/AD4IoT-NewAssetServiceNowTicket/readme.md)

### AD4IoT-AutoAlertStatusSync

This playbook updates alert statuses in Defender for IoT whenever a related alert in Microsoft Sentinel has a Status update.

### AD4IoT-SendEmailtoIoTOwner

The playbooks automate the SOC workflow by automatically emailing the incident details to the right IoT/OT device owner (based on Defender for IoT dafinition) and allowing him to respond by email. The incident is automatically updated based on the email response from the device owner

### AD4IoT-AutoTriageIncident

SOC and OT engineers can stream their workflows using the playbook, which automatically updates the incident severity based on the devices involved in the incident and their importance.

### AD4IoT-CVEAutoWorkflow

The playbook automates the SOC workflow by automatically enriching incident comments with the CVEs of the involved devices based on Defender for IoT data. An automated triage is performed if the CVE is critical, and the asset owner is automatically notified by email.

## Parsers

# Microsoft Defender for Office 365

The Microsoft Defender for Office 365 solution for Microsoft Sentinel enables you to ingest security alerts from the Defender for Office 365 platform, providing visibility into threats within email messages, links (URLs) and collaboration tools.

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

## Data Connectors

### Microsoft Defender for Office 365

Microsoft Defender for Office 365 safeguards your organization against malicious threats posed by email messages, links (URLs) and collaboration tools. By ingesting Microsoft Defender for Office 365 alerts into Microsoft Sentinel, you can incorporate information about email- and URL-based threats into your broader risk analysis and build response scenarios accordingly.

The following types of alerts will be imported:

- A potentially malicious URL click was detected

- Email messages containing malware removed after delivery

- Email messages containing phish URLs removed after delivery

- Email reported by user as malware or phish

- Suspicious email sending patterns detected

- User restricted from sending email

These alerts can be seen by Office customers in the \*\* Office Security and Compliance Center\*\*.

For more information, see the [Microsoft Sentinel documentation](https://go.microsoft.com/fwlink/p/?linkid=2219942&wt.mc\_id=sentinel\_dataconnectordocs\_content\_cnl\_csasci).

## Workbooks

### Microsoft Defender For Office 365

Gain insights into your Microsoft Defender for Office 365 raw data logs. This workbook lets you look at trends in email senders, attachments and embedded URL data to find anomalies. You can also search by, sender, recipient, subject, attachment or embedded URL to find where the related messages have been sent.

**Required Data Types**

EmailEvents

EmailUrlInfo

EmailAttachmentInfo

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Microsoft PowerBI solution for Sentinel

The Microsoft PowerBI solution enables you to track user activities in your PowerBI environment

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

## Data Connectors

### Microsoft PowerBI

Microsoft PowerBI is a collection of software services, apps, and connectors that work together to turn your unrelated sources of data into coherent, visually immersive, and interactive insights. Your data may be an Excel spreadsheet, a collection of cloud-based and on-premises hybrid data warehouses, or a data store of some other type. This connector lets you stream PowerBI audit logs into Microsoft Sentinel, allowing you to track user activities in your PowerBI environment. You can filter the audit data by date range, user, dashboard, report, dataset, and activity type.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Microsoft Project solution for Sentinel

Stream your Microsoft Project audit logs into Microsoft Sentinel

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

## Data Connectors

### Microsoft Project

Microsoft Project (MSP) is a project management software solution. Depending on your plan, Microsoft Project lets you plan projects, assign tasks, manage resources, create reports and more. This connector allows you to stream your Azure Project audit logs into Microsoft Sentinel in order to track your project activities.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Microsoft Purview Information Protection

The Microsoft Information Protection Solution for Microsoft Sentinel integrates Microsoft Purview Information Protection logs for security monitoring in Microsoft Sentinel.

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

## Data Connectors

### Microsoft Purview Information Protection

Microsoft Purview Information Protection helps you discover, classify, protect, and govern sensitive information wherever it lives or travels. Using these capabilities enable you to know your data, identify items that are sensitive and gain visibility into how they are being used to better protect your data. Sensitivity labels are the foundational capability that provide protection actions, applying encryption, access restrictions and visual markings.

Integrate Microsoft Purview Information Protection logs with Microsoft Sentinel to view dashboards, create custom alerts and improve investigation. For more information, see the [Microsoft Sentinel documentation](https://go.microsoft.com/fwlink/p/?linkid=2223811&wt.mc\_id=sentinel\_dataconnectordocs\_content\_cnl\_csasci).

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Microsoft Purview Insider Risk Management

This solution enables insider risk management teams to investigate risk-based behavior across 25+ Microsoft products. This solution is a better-together story between Microsoft Sentinel and Microsoft Purview Insider Risk Management.

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

## Data Connectors

### Microsoft 365 Insider Risk Management

Microsoft 365 Insider Risk Management is a compliance solution in Microsoft 365 that helps minimize internal risks by enabling you to detect, investigate, and act on malicious and inadvertent activities in your organization. Risk analysts in your organization can quickly take appropriate actions to make sure users are compliant with your organization's compliance standards.

Insider risk policies allow you to:

- define the types of risks you want to identify and detect in your organization.

- decide on what actions to take in response, including escalating cases to Microsoft Advanced eDiscovery if needed.

This solution produces alerts that can be seen by Office customers in the Insider Risk Management solution in Microsoft 365 Compliance Center.

[Learn More](https://aka.ms/OfficeIRMConnector) about Insider Risk Management.

These alerts can be imported into Microsoft Sentinel with this connector, allowing you to see, investigate, and respond to them in a broader organizational threat context. For more information, see the [Microsoft Sentinel documentation](https://go.microsoft.com/fwlink/p/?linkid=2223721&wt.mc\_id=sentinel\_dataconnectordocs\_content\_cnl\_csasci).

## Workbooks

### Insider Risk Management

The Microsoft Insider Risk Management Workbook integrates telemetry from 25+ Microsoft security products to provide actionable insights into insider risk management. Reporting tools provide “Go to Alert” links to provide deeper integration between products and a simplified user experience for exploring alerts.

**Required Data Types**

SigninLogsSigninLogs

AuditLogs

AzureActivity

OfficeActivity

InformationProtectionLogs\_CL

SecurityIncident

## Analytic Rules

### Insider Risk\_High User Security Alert Correlations

This alert joins SecurityAlerts from Microsoft Products with SecurityIncidents from Microsoft Sentinel and Microsoft 365 Defender. This join allows for identifying patterns in user principal names associated with respective security alerts. A machine learning function (Basket) is leveraged with a .001 threshold. Baset finds all frequent patterns of discrete attributes (dimensions) in the data. It returns the frequent patterns passed the frequency threshold. This query evaluates UserPrincipalName for patterns in SecurityAlerts and Reporting Security Tools. This query can be further tuned/configured for higher confidence percentages, security products, or alert severities pending the needs of the organization. There is an option for configuration of correlations against Microsoft Sentinel watchlists. For more information on the basket plugin, see [basket plugin](https://docs.microsoft.com/azure/data-explorer/kusto/query/basketplugin)

**Required Data Connectors**

MicrosoftDefenderAdvancedThreatProtection

AzureActiveDirectoryIdentityProtection

AzureSecurityCenter

IoT

MicrosoftCloudAppSecurity

IoT

OfficeATP

### Insider Risk\_High User Security Incidents Correlation

This alert joins SecurityAlerts to SecurityIncidents to associate Security Alerts and Incidents with user accounts. This aligns all Microsoft Alerting Products with Microsoft Incident Generating Products (Microsoft Sentinel, M365 Defender) for a count of user security incidents over time. The default threshold is 5 security incidents, and this is customizable per the organization's requirements. Results include UserPrincipalName (UPN), SecurityIncident, LastIncident, ProductName, LastObservedTime, and Previous Incidents. There is an option for configuration of correlations against Microsoft Sentinel watchlists. For more information, see [Investigate incidents with Microsoft Sentinel]( https://docs.microsoft.com/azure/sentinel/investigate-cases).

**Required Data Connectors**

MicrosoftDefenderAdvancedThreatProtection

AzureActiveDirectoryIdentityProtection

AzureSecurityCenter

IoT

MicrosoftCloudAppSecurity

IoT

OfficeATP

### Insider Risk\_Microsoft Purview Insider Risk Management Alert Observed

This alert is triggered when a Microsoft Purview Insider Risk Management alert is recieved in Microsoft Sentinel via the Microsoft Purview Insider Risk Management Connector. The alert extracts usernames from security alerts to provide UserPrincipalName, Alert Name, Reporting Product Name, Status, Alert Link, Previous Alerts Links, Time Generated. There is an option for configuration of correlations against Microsoft Sentinel watchlists. For more information, see [Learn about insider risk management](https://docs.microsoft.com/microsoft-365/compliance/insider-risk-management)

**Required Data Connectors**

OfficeATP

### Insider Risk\_Sensitive Data Access Outside Organizational Geo-location

This alert joins Azure Information Protection Logs (InformationProtectionLogs\_CL) with Azure Active Directory Sign in Logs (SigninLogs) to provide a correlation of sensitive data access by geo-location. Results include User Principal Name, Label Name, Activity, City, State, Country/Region, and Time Generated. Recommended configuration is to include (or exclude) Sign in geo-locations (City, State, Country and/or Region) for trusted organizational locations. There is an option for configuration of correlations against Microsoft Sentinel watchlists. Accessing sensitive data from a new or unauthorized geo-location warrants further review. For more information see [Sign-in logs in Azure Active Directory: Location Filtering](https://docs.microsoft.com/azure/active-directory/reports-monitoring/concept-sign-ins)

**Required Data Connectors**

AzureInformationProtection

AzureActiveDirectory

### Insider Risk\_Risky User Access By Application

This alert evaluates Azure Active Directory Sign in risk via Machine Learning correlations in the basket operator. The basket threshold is adjustable, and the default is set to .01. There is an optional configuration to configure the percentage rates. The correlations are designed to leverage machine learning to identify patterns of risky user application access. There is an option for configuration of correlations against Microsoft Sentinel watchlists. For more information, see [Tutorial: Use risk detections for user sign-ins to trigger Azure AD Multi-Factor Authentication or password changes](https://docs.microsoft.com/azure/active-directory/authentication/tutorial-risk-based-sspr-mfa)

**Required Data Connectors**

AzureActiveDirectory

## Hunting Queries

### Insider Risk\_Entity Anomaly Followed by IRM Alert

MicrosoftPurviewInsiderRiskManagement Hunting Query 1

### Insider Risk\_ISP Anomaly to Exfil

MicrosoftPurviewInsiderRiskManagement Hunting Query 2

### Insider Risk\_Multiple Entity-Based Anomalies

MicrosoftPurviewInsiderRiskManagement Hunting Query 3

### Insider Risk\_Possible Sabotage

MicrosoftPurviewInsiderRiskManagement Hunting Query 4

### Insider Risk\_Sign In Risk Followed By Sensitive Data Access

MicrosoftPurviewInsiderRiskManagement Hunting Query 5

## Watchlists

## Playbooks

### Notify-InsiderRiskTeam

This playbook should be configured as an automation action with the Insider Risk Management Analytics Rules. Upon triggering an Analytic Rule, this playbook captures respective details and both emails and posts a message in a Teams chat to the Insider Risk Management team.

## Parsers

# Microsoft Purview solution for Sentinel

The Microsoft Purview Solution enables data sensitivity enrichment of Microsoft Sentinel.

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

## Data Connectors

### Microsoft Purview (Preview)

Connect to Microsoft Purview to enable data sensitivity enrichment of Microsoft Sentinel. Data classification and sensitivity label logs from Microsoft Purview scans can be ingested and visualized through workbooks, analytical rules, and more. For more information, see the [Microsoft Sentinel documentation](https://go.microsoft.com/fwlink/p/?linkid=2224125&wt.mc\_id=sentinel\_dataconnectordocs\_content\_cnl\_csasci).

## Workbooks

### Microsoft Purview

Sets the time name for analysis

**Required Data Types**

AzureDiagnostics

MicrosoftAzurePurview

## Analytic Rules

### Sensitive Data Discovered in the Last 24 Hours

Identifies all classifications that have been detected on assets during a scan by Microsoft Purview within the last 24 hours.

**Required Data Connectors**

MicrosoftAzurePurview

### Sensitive Data Discovered in the Last 24 Hours - Customized

Customized query used to identify specific classifications and parameters that have been discovered on assets in the last 24 hours by Microsoft Purview. By default, the query identifies Social Security Numbers detected, but the specific classification monitored along with other data fields can be adjusted. A list of supported Microsoft Purview classifications can be found here: https://docs.microsoft.com/azure/purview/supported-classifications

**Required Data Connectors**

MicrosoftAzurePurview

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Microsoft Sentinel - Continuous Threat Monitoring for GitHub (Preview)

The GitHub connector provides the capability to ingest GitHub logs into Microsoft Sentinel.

**Data Connectors:** 2**, Workbooks:** 2**, Analytic Rules:** 12**, Hunting Queries:** 8**, Watchlists:** 0**, Playbooks:** 0, Parsers: 4

## Data Connectors

### GitHub Enterprise Audit Log

The GitHub audit log connector provides the capability to ingest GitHub logs into Microsoft Sentinel. By connecting GitHub audit logs into Microsoft Sentinel, you can view this data in workbooks, use it to create custom alerts, and improve your investigation process.

\*\*Note:\*\* If you are intended to ingest GitHub subscribed events into Microsoft Sentinel , Please refer to GitHub (using Webhooks) Connector from "\*\*Data Connectors\*\*" gallery.

### GitHub (using Webhooks) (using Azure Function)

The [GitHub](https://www.github.com) webhook data connector provides the capability to ingest GitHub subscribed events into Microsoft Sentinel using [GitHub webhook events](https://docs.github.com/en/developers/webhooks-and-events/webhooks/webhook-events-and-payloads). The connector provides ability to get events into Sentinel which helps to examine potential security risks, analyze your team's use of collaboration, diagnose configuration problems and more.

\*\*Note:\*\* If you are intended to ingest Github Audit logs, Please refer to GitHub Enterprise Audit Log Connector from "\*\*Data Connectors\*\*" gallery.

## Workbooks

### GitHub Security

Gain insights to GitHub activities that may be interesting for security.

**Required Data Types**

### GithubWorkbook

Gain insights to GitHub activities that may be interesting for security.

**Required Data Types**

## Analytic Rules

### (Preview) GitHub - A payment method was removed

Detect activities when a payment method was removed. This query runs every day and its severity is Medium.

**Required Data Connectors**

(none listed)

### GitHub Activites from a New Country

Detect activities from a location that was not recently or was never visited by the user or by any user in your organization.

**Required Data Connectors**

(none listed)

### (Preview) GitHub - Oauth application - a client secret was removed

Detect activities when a client secret was removed. This query runs every day and its severity is Medium.

**Required Data Connectors**

(none listed)

### (Preview) GitHub - Repository was created

Detect activities when a repository was created. This query runs every day and its severity is Medium.

**Required Data Connectors**

(none listed)

### (Preview) GitHub - Repository was destroyed

Detect activities when a repository was destroyed. This query runs every day and its severity is Medium.

**Required Data Connectors**

(none listed)

### GitHub Two Factor Auth Disable

Two-factor authentication is a process where a user is prompted during the sign-in process for an additional form of identification, such as to enter a code on their cellphone or to provide a fingerprint scan. Two factor authentication reduces the risk of account takeover. Attacker will want to disable such security tools in order to go undetected.

**Required Data Connectors**

(none listed)

### (Preview) GitHub - User visibility Was changed

Detect activities when a user visibility Was changed. This query runs every day and its severity is Medium.

**Required Data Connectors**

(none listed)

### (Preview) GitHub - User was added to the organization

Detect activities when a user was added to the organization. This query runs every day and its severity is Medium.

**Required Data Connectors**

(none listed)

### (Preview) GitHub - User was blocked

Detect activities when a user was blocked on the repository. This query runs every day and its severity is Medium.

**Required Data Connectors**

(none listed)

### (Preview) GitHub - User was invited to the repository

Detect activities when a user was invited to the repository. This query runs every day and its severity is Medium.

**Required Data Connectors**

(none listed)

### (Preview) GitHub - pull request was created

Detect activities when a pull request was created. This query runs every day and its severity is Medium.

**Required Data Connectors**

(none listed)

### (Preview) GitHub - pull request was merged

Detect activities when a pull request was merged. This query runs every day and its severity is Medium.

**Required Data Connectors**

(none listed)

## Hunting Queries

### GitHub First Time Invite Member and Add Member to Repo

GitHub Hunting Query 1

### GitHub Inactive or New Account Access or Usage

GitHub Hunting Query 2

### GitHub Mass Deletion of repos or projects

GitHub Hunting Query 3

### GitHub OAuth App Restrictions Disabled

GitHub Hunting Query 4

### GitHub Update Permissions

GitHub Hunting Query 5

GitHub Repo switched from private to public

GitHub Hunting Query 6

### GitHub First Time Repo Delete

GitHub Hunting Query 7

### GitHub User Grants Access and Other User Grants Access

GitHub Hunting Query 8

## Watchlists

## Playbooks

## Parsers

### GitHub Data Parser

Category: Samples

Function Alias: GitHubAuditData

### GitHubCodeScanningData

Category: Samples

Function Alias: GitHubCodeScanningData

### GitHubDependabotData

Category: Samples

Function Alias: GitHubDependabotData

### GithubSecretScanningData

Category: Samples

Function Alias: GithubSecretScanningData

# Microsoft Sentinel Deception (Honey Tokens) Solution

HoneyTokens aim to deceive attackers by distributing a collection of traps and decoys across the infrastructure to imitate genuine assets.

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

## Data Connectors

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

### [variables('WatchListName')]

HoneyTokens' solution watchlist

## Playbooks

## Parsers

# Microsoft Sentinel for Teams (Preview)

Microsoft Sentinel for Teams provides Teams security logs visibility and threat protection.

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

## Data Connectors

## Workbooks

### Microsoft Teams

This workbook is intended to identify the activities on Microrsoft Teams.

**Required Data Types**

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

### Send Teams Adaptive Card on incident creation

This playbook will send Microsoft Teams Adaptive Card on incident creation, with the option to change the incident's severity and/or status.

### Advanced SNOW Teams Integration Playbook

This playbook showcases an example of triggering an incident within a targeted Teams channel and opening up a ticket within Service Now. Additionally The playbook will also list playbooks that can be initiated from teams using an adaptive card and callbacks that will take action upon certain entities identified in the incident.

### Post Message Teams

This playbook will post a message in a Microsoft Teams channel when an Alert is created in Microsoft Sentinel.

### Post Message Teams

This playbook will post a message in a Microsoft Teams channel when an Incident is created in Microsoft Sentinel.

## Parsers

# Microsoft Sentinel Solution for Dynamics 365 CE Apps (Preview)

The Microsoft Sentinel solution for Dynamics 365 CE apps provides threat monitoring, detection and incident response capabilities for Dynamics 365 CE apps.

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

## Data Connectors

## Workbooks

### Dynamics 365 Activity

This workbook brings together queries and visualizations to assist you in identifying potential threats in your Dynamics 365 audit data. This workbook is separated into 5 distinct sections and within each section there are several queries and visualizations. Many of the queries build on data from previous queries so may not appear if no data is present.

To begin select the desired TimeRange to filter the data to the timeframe you want to focus on. Note if you have a large amount of Dynamics 365 data queries may timeout with a large time range, if this is the case simply select a smaller time range.

**Required Data Types**

Dynamics365

Dynamics365

## Analytic Rules

### D365 - Audit log configuration change

Identifies change in Security Audit Configuration

Source Action: Checking or un-checking below options on Entity level in CRM.

- Single record auditing.

- Multiple record auditing.

- Log all records displayed on an opened page.

**Required Data Connectors**

Dynamics365

### D365 - Audit log data deletion

Identifies audit log data deletion activity in Dynamics 365.

Source Action:

- Deletion of Audit Logs from Audit Summary View.

- Deleting Audit History on Record from Related Tab Data.

**Required Data Connectors**

Dynamics365

### D365 - Dormant admin or previously non-admin user conducting admin activity

Monitors and detects dormant admins or previously non-admin users

currently conducting admin activities in Dynamics 365.

**Required Data Connectors**

Dynamics365

### D365 - Encryption settings changed

This query looks for changes to the Data Encryption settings for Dynamics 365.

Reference: https://docs.microsoft.com/microsoft-365/compliance/office-365-encryption-in-microsoft-dynamics-365'

**Required Data Connectors**

Dynamics365

### D365 - Login by a sensitive privileged user

This query identifies users tagged ["D365 Sensitive"] using the built-in VIP Users watchlist template and searches Dynamics 365 logs for any corresponding authentication events.

**Required Data Connectors**

Dynamics365

### D365 - Login from IP in the block list

Identifies logons from IPv4 address maintained on a block list. The block list

is maintained within the query as well as using the built in NetworkAddresses

watchlist template using "D365 Block" tag.

**Required Data Connectors**

Dynamics365

### D365 - Login from IP not in the allow list

Identifies logons from IPv4 addresses not matching IPv4 subnets maintained on an allow list.

The allow list is maintained within the query as well as using the built in

NetworkAddresses watchlist template using "D365 Allow" tag.

**Required Data Connectors**

Dynamics365

### D365 - Mass deletion of records

This query identifies large scale delete operations where the number of delete entries exceeds a

query defined threshold within the last period. The scheduling of bulk delete jobs in

Dynamics 365 is also detected.

**Required Data Connectors**

Dynamics365

### D365 - Mass export of records to Excel

The query detects user exporting a large amount of records from Dynamics 365

to Excel, significantly more records exported than any other recent activity

by that user.

**Required Data Connectors**

Dynamics365

### D365 - Monitored Security configuration changed

Identifies security configuration changes in Dynamics 365 based on a

watchlist. The watchlist deployed as part of the Dynamics 355 Continuous Threat

Montioring Solution contains common security configuration related changes and

can be modified to tune which events generate an alert.

**Required Data Connectors**

Dynamics365

### D365 - Monitored User configuration changed

Identifies User configuration changes made done in the D365 like Add/Removing

Business Units, Teams, Enable/Disable Users, Change the Access Mode field for

any user in the "D365-UserConfig" watchlist. The watchlist deployed as part of

the Dynamics 355 Continuous Threat Montioring Solution contains common security

configuration related changes and can be modified to tune which events generate

an alert.

**Required Data Connectors**

Dynamics365

### D365 - New Office user agent detected

Identifies users accessing Dynamics from a User Agent that has not been

seen in any Office 365 workloads in the last 7 days. Has configurable filter for

known good user agents such as PowerApps.

**Required Data Connectors**

Dynamics365

### D365 - New user agent detected

Identifies users accessing Dynamics from a User Agent that has not been

seen the 14 days. Has configurable filter for known good user agents such as PowerApps.

Also includes optional section to exclude User Agents to indicate a browser being

used.

**Required Data Connectors**

Dynamics365

### D365 - Permissions granted to an application identity

This query identifies API level permission grants, either via the delegated

permissions of an Azure AD Application or direct assignment within Dynamics 365

as an application user.

**Required Data Connectors**

Dynamics365

AzureActiveDirectory

### D365 - Sign-in from an unauthorized domain

This query identifies user authentication events originating from a user

domain that is not found on an allow list. Common internal Dynamics 365 system

names are excluded.

**Required Data Connectors**

Dynamics365

### D365 - User bulk retrieval outside normal activity

This query detects users retrieving significantly more records from Dynamics

365 than they have in the past 2 weeks. This could indicate potentially unauthorized

access to data within Dynamics 365.

**Required Data Connectors**

Dynamics365

## Hunting Queries

### Dynamics 365 Activity After Azure AD Alerts

Dynamics 365 Hunting Query 1

### Dynamics 365 Activity After Failed Logons

Dynamics 365 Hunting Query 2

## Watchlists

### D365-SecurityConfig

D365 Security Config Changes.

### D365-UserConfig

D365 User Config Changes.

## Playbooks

## Parsers

# Microsoft Sentinel solution for SAP® applications

Continuous Threat Monitoring for SAP ABAP/NetWeaver and S/4 systems

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 61**, Hunting Queries:** 0**, Watchlists:** 18**, Playbooks:** 0, Parsers: 0

## Data Connectors

### SAP

SAP systems and applications handle massive volumes of business-critical data, hosted on cloud/on-premises infrastructure. Due to the complexity of the SAP ecosystem, security operations (SecOps) teams face the challenge of effectively monitoring and protecting their organization against growing threats. A breach of the SAP system could result in data loss, disruption to business processes, loss of revenue, and major reputation damage.

The Microsoft Sentinel SAP connector, part of the Microsoft Sentinel Solution for SAP® Applications, ingests SAP logs to Microsoft Sentinel workspaces. You can access raw data using the built-in Microsoft Sentinel Solution for SAP content or using custom content. The connector ingests SAP NetWeaver (RFC) application layer logs, including Security Auditlogs, Application logs, ChangeDocuments, Spool Logs, Change Request data, User masterdata, and more.

The Microsoft Sentinel solution for SAP will be generally available with a six-month free promotion starting in August 2022. Billing will start in February 2023, as an add-on charge in addition to the existing Microsoft Sentinel consumption-billing model for monitoring SAP production systems.

## Workbooks

### SAP -Security Audit log and Initial Access

SAP -Security Audit log and Initial Access

**Required Data Types**

SAPAuditLog

SAP

## Analytic Rules

### SAP - (Preview) Capture-replay vulnerability in SAP NetWeaver [CVE-2023-0014]

SAP NetWeaver ABAP Server and ABAP Platform creates information about system identity in an ambiguous format. <br/> This may be exploited by malicious users to obtain illegitimate access to the system. <br/> Read SAP note 3281854 - FAQ for Security Note 3089413 for more details. This alert rule helps to identify current risks for systems in the landscape.

**Required Data Connectors**

SAP

### SAP - (Preview) Critical authorizations assignment - New Authorization Value

Identifies assignment of a critical authorization object value to a new user.

Source Action: Assign a new authorization object / update existing one in a role using PFCG.

Critical authorization objects should be maintained in watchlist ""SAP - Critical Authorization Objects""

\*Data Sources: SAPcon - Change Documents Log\*

\*Data Sources: SAPcon - User MD\*

**Required Data Connectors**

SAP

### SAP - (Preview) Data collection health check

Produces insights on potential SAP agent connectivity issues.

**Required Data Connectors**

SAP

### SAP - (Preview) Data exported from a production system using a transport

Transports are like pull requests and are normally created in a developement system. This alert rule is triggered when a transport is released from a production system, with data coming from a sensitive table.

**Required Data Connectors**

SAP

### SAP - (Preview) Dynamic Anomaly based Audit Log Monitor Alerts

SAP Audit log events with message IDs preconfigured in Watchlist SAP\_Dynamic\_Audit\_Log\_Monitor\_Configuration and with RuleType = "AnomaliesOnly" will be shown here.

<br/>

See [Sentinel4SAP Dcoumentation](https://aka.ms/sapsecdocs) for further information

**Required Data Connectors**

SAP

### SAP - (Preview) File Downloaded From a Malicious IP Address

User has downloaded a file from an SAP system using an IP address known to be malicious.

Malicious IP addresses are obtained from threat intelligence services. For additional information visit the [Connect your threat intelligence platform to Microsoft Sentinel]( https://learn.microsoft.com/Azure/sentinel/connect-threat-intelligence-tip) how-to page.

This Alert rule allows for a cross-workspace query to accommodate an architecture where the threat intelligence data resides in a different workspace than the one which holds the SAP data.

**Required Data Connectors**

SAP

### SAP - (Preview) HANA DB - Assign Admin Authorizations

Identifies admin privileges/roles assignment.

Source Action: Assign a user with any Admin role / privileges.

\*Data Sources: Linux Agent - Syslog\*

**Required Data Connectors**

### SAP - (Preview) HANA DB - Audit Trail Policy Changes

Identifies changes for HANA DB audit trail policies.

Source Action: Create / update existing audit policy in security definitions.

\*Data Sources: Linux Agent - Syslog\*

**Required Data Connectors**

### SAP - (Preview) HANA DB - Deactivation of Audit Trail

Identifies deactivation of HANA DB audit log.

Source Action: Deactivate Audit Log in HANA DB security defnitions.

\*Data Sources: Linux Agent - Syslog\*

**Required Data Connectors**

### SAP - (Preview) HANA DB - User Admin actions

Identifies user administration actions.

Souirce Action: Create/Update/Delete a DB User.

\*Data Sources: Linux Agent - Syslog\*

**Required Data Connectors**

### SAP - (Preview) High volume of potentially sensitive data exported

High volume of data exported via files in proximity to an execution of a sensitive transaction, a sensitive program or direct access to sensitive table.

**Required Data Connectors**

SAP

### SAP - (Preview) New trusted RFC connection capture-replay vulnerability in SAP NetWeaver [CVE-2023-0014]

SAP NetWeaver ABAP Server and ABAP Platform creates information about system identity in an ambiguous format. <br/> This may be exploited by malicious users to obtain illegitimate access to the system. <br/> Read SAP note 3281854 - FAQ for Security Note 3089413 for more details. This alert rule helps to identify newly added trusted RFC relationships.

**Required Data Connectors**

SAP

### SAP - (Preview) Printing of potentially sensitive data

The alert rule was disabled due to too many consecutive failures. Reason: Server is failing to execute the query of this rule, please verify the query. User has requested printing or has printed data which is potentially sensitive.

Data is considered sensitive if it is obtained by using a sensitive transaction, by executing a sensitive program or by directly accessing a sensitive table.

**Required Data Connectors**

SAP

### SAP - (Preview) Sensitive data saved into a USB drive

SAP data exported via files and saved into a recently mounted USB drive in proximity to an execution of a sensitive transaction, a sensitive program or direct access to a sensitive table.

**Required Data Connectors**

SAP

### SAP - Activation or Deactivation of ICF Service

Identifies activation or deactivation of ICF Services.

Source Action: Activate or deactivate a service using SICF.

\*Data Sources: SAPcon - Table Data Log\*

**Required Data Connectors**

SAP

### SAP - Assignment of a sensitive profile

Identifies new assignments of a sensitive profile to a user.

Source Action: Assign a profile to a User using SU01.

Sensitive profiles can be maintained using the "SAP - Sensitive Profiles" watchlist

\*Data Sources: SAPcon - Change Documents Log\*

**Required Data Connectors**

SAP

### SAP - Assignment of a sensitive role

Identifies new assignments for a sensitive role to a user.

Source Action: Assign a role to a User using SU01 / PFCG.

Sensitive roles should be maintained in watchlist "SAP - Sensitive Roles"

\*Data Sources: SAPcon - Change Documents Log, Audit Log\*

**Required Data Connectors**

SAP

### SAP - Brute Force (RFC)

Identifies brute force attacks on the SAP system using RFC logons

Source Action: Attempt to login from the same IP to several systems/clients within the scheduled time interval using RFC

\*Data Sources: SAPcon - Audit Log\*

**Required Data Connectors**

SAP

### SAP - Change in a Sensitive Privileged User

Identifies changes of sensitive privileged users.

Source Action: Change user details / authorizations using SU01.

<p>Users are considered as Privileged when one of these conditions apply: </p>

<li>If they are named in the SAP - Privileged Users Watchlist

<li>If they have a profile which is included in the SAP - Sensitive Profiles watchlist

<li>If they have a role which is included in the SAP - Sensitive Roles watchlist

This Rule requires a fresh full reload of SAP user master data to be performed daily.

\*Data Sources: SAPcon - Audit Log\*

\*Data Sources: SAPcon - User MD\*

**Required Data Connectors**

SAP

### SAP - Client Configuration Change

Identifies changes for client configuration such as: Client role, Changes recording mode.

Source Action: Perofrm client configurations changes using SCC4 transaction code.

\*Data Sources: SAPcon - Audit Log\*

**Required Data Connectors**

SAP

### SAP - Critical authorizations assignment - New User Assignment

Identifies assignment of a critical authorization object value to a new user.

Source Action: Assign a new user to a role which holds critical authorization values using SU01/PFCG.

Critical authorization objects should be maintained in watchlist ""SAP - Critical Authorization Objects""

\*Data Sources: SAPcon - Change Documents Log\*

**Required Data Connectors**

SAP

### SAP - Data has Changed during Debugging Activity

Identifies changes for runtime data during a debugging activity.

Source Action: Activate Debug ("/h"), Select a field for change and update it's value.

\*\*Recommended for Production only\*\*

\*Data Sources: SAPcon - Audit Log\*

**Required Data Connectors**

SAP

### SAP - Deactivation of Security Audit Log

Identifies deactivation of Security Audit Log

Source Action: Disable secruity Audit Log using SM19/RSAU\_CONFIG.

\*Data Sources: SAPcon - Audit Log\*

**Required Data Connectors**

SAP

### SAP - Debugging Activities

Identifies all debugging related activities.

Source Action: Activate Debug ("/h") in system, debug an active process, add breakpoint to source code etc.

\*\*Recommended for Production only\*\*

\*Data Sources: SAPcon - Audit Log\*

**Required Data Connectors**

SAP

### SAP - Dialog logon attempt from a privileged user

Identifies dialog logon (Type AUM) attempts by priviledged users (See Function SAPUsersGetPrivileged) on SAP system .

Source Action: Attempt to login from the same IP to several systems/clients within the scheduled time interval.

\*Data Sources: SAPcon - Audit Log\*

**Required Data Connectors**

SAP

### SAP - Dynamic ABAP Program

Identifies execution of dynamic ABAP programming. For example, ABAP code was dynamically created/changed/deleted. Source Action: Create an ABAP Report which uses ABAP program generation commands such as "INSERT REPORT" and execute it. Excluded Transaction Codes can be maintained in "SAP - Transactions for ABAP Generations" watchlist. \*Data Sources: SAPcon - Audit Log\*

**Required Data Connectors**

SAP

### SAP - Dynamic Deterministic Audit Log Monitor

SAP Audit log events with message IDs preconfigured in Watchlist SAP\_Dynamic\_Audit\_Log\_Monitor\_Configuration

will be shown here.

<br/>

See [Sentinel4SAP Dcoumentation](https://aka.ms/sapsecdocs) for further information

**Required Data Connectors**

SAP

### SAP - Dynamic RFC Destination

Identifies execution of RFC using dynamic destinations. Source Action: Execute an ABAP report which is using dynamic destinations (cl\_dynamic\_destination). Sample report: DEMO\_RFC\_DYNAMIC\_DEST. \*Data Sources: SAPcon - Audit Log\*

**Required Data Connectors**

SAP

### SAP - Execution of a Sensitive ABAP Program

Identifies direct execution of a sensitive ABAP program.

Source Action: Execute a program directly using SE38/SA38/SE80.

\*\*Recommended for Production only\*\*

ABAP Programs should be maintained in watchlist "SAP - Sensitive ABAP Programs"

\*Data Sources: SAPcon - Audit Log\*

**Required Data Connectors**

SAP

### SAP - Execution of a Sensitive Transaction Code

Identifies execution of a sensitive Transaction Code.

Source Action: Execute a sensitive Transaction Code.

\*\*Recommended for Production only\*\*

Transaction Codes should be maintained in watchlist ""SAP - Sensitive Transaction Codes""

\*Data Sources: SAPcon - Audit Log\*

**Required Data Connectors**

SAP

### SAP - Execution of an Obsolete or an Insecure Function Module

Identifies execution of an obsolete/insecure ABAP Function Module.

Source Action: Execute an obsolete/insecure function module directly using SE37.

\*\*Recommended for Production only\*\*

Obsolete functions should be maintained in "SAP - Obsolete Function Modules" Watchlist.

**Required Data Connectors**

SAP

### SAP - Execution of an Obsolete or an Insecure Program

Identifies execution of an obsolete insecure ABAP program.

Source Action: Execute a program directly using SE38/SA38/SE80 or by using a background job.

\*\*Recommended for Production only\*\*

Obsolete programs should be maintained in "SAP - Obsolete Programs" Watchlist

\*Data Sources: SAPcon - Audit Log\*

**Required Data Connectors**

SAP

### SAP - Execution of Sensitive Function Module

Identifies execution of a sensitive ABAP Function Module.

Source Action: Execute a sensitive function module directly using SE37.

\*\*Recommended for Production only\*\*

Sensitive functions should be maintained in "SAP - Sensitive Function Modules" Watchlist.

Table logging changes should be activated for table "EUFUNC" in backend. (SE13)

\*Data Sources: SAPcon - Table Data Log\*

**Required Data Connectors**

SAP

### SAP - FTP for non authorized servers

Identifies FTP connection for non authorized server.

Maintain new Watchlist, similar to SAPFTP\_SERVERS

Source Action: Create a new FTP connection e.g. by using Function Module FTP\_CONNECT.

\*Data Sources: SAPcon - Audit Log\*

**Required Data Connectors**

SAP

### SAP - Function Module tested

Identifies testing of a function module.

Source Action: Test a function module using SE37 / SE80.

\*\*Recommended for Production only\*\*

\*Data Sources: SAPcon - Audit Log\*

**Required Data Connectors**

SAP

### SAP - Insecure FTP servers configuration

Identifies Insecure FTP servers configuration - FTP Whitelist is empty / Contains Placeholders.

Source Action: Do not maintain / maintain values which contains placeholders in table SAPFTP\_SERVERS using maintenance view SAPFTP\_SERVERS\_V. (SM30)

\*Data Sources: SAPcon - Audit Log\*

**Required Data Connectors**

SAP

### SAP - Lifecycle - SAP Notes were implemented in system

Identifies SAP Notes implementation in the system.

Source Action: Implement SAP Note using SNOTE/TCI.

\*Data Sources: SAPcon - Change Requests\*

**Required Data Connectors**

SAP

### SAP - Login from unexpected network

Identifies logons from an unexpected network.

Source Action: Logon to the backend system from an IP address which is not assigned to one of the netwroks.

Networks should be maintained in watchlist "SAP - Networks"

\*Data Sources: SAPcon - Audit Log\*

**Required Data Connectors**

SAP

### SAP - Missing configuration in the Dynamic Security Audit Log Monitor

An SAP audit log event has occurred bearing a message ID which was not maintained in the SAP\_Dynamic\_Audit\_Log\_Monitor\_Configuration watchlist.

The SAP\_Dynamic\_Audit\_Log\_Monitor\_Configuration watchlist allows for dynamically alerting on SAP audit log events.

Recommended solution - go to the SAP\_Dynamic\_Audit\_Log\_Monitor\_Configuration and add the missing SAP audit log message ID. Specify a severity level of medium or high to have this message ID covered by the alerts based on rule "Dynamic Security Audit Log Monitor".

**Required Data Connectors**

SAP

### SAP - Multiple Files Download

Identifies multiple files downloads for a user within a specific timerange.

Source Action: Download multiple files while using SAPGui to Excel/Lists etc.

\*Data Sources: SAPcon - Audit Log\*

**Required Data Connectors**

SAP

### SAP - Multiple Logons by IP

Identifies logon of several users from same IP within scheduled time interval.

Source Action: Logon using several users thorugh the same IP.

Networks can be excluded from this alert by specifying ranges in the 'SAP - Excluded Networks' watchlist.

This rule alerts on "empty" IP addresses as well- Add an entry with serachkey= 000.00.000.0 and Description= EmptyIPAddressesShouldBeExcluded in the 'SAP - Excluded Networks' watchlist to avoid alerting on empty IP addresses

\*Data Sources: SAPcon - Audit Log\*

**Required Data Connectors**

SAP

### SAP - Multiple Password Changes

Identifies multiple password changes at different levels:

1. Users across systems

2. Per user performing the password change

3. Per user who's password is being changed

Source Action: Change user password

**Required Data Connectors**

SAP

### SAP - Multiple Spool Executions

Identifies multiple spools for a user within a specific timerange.

Source Action: Create and execute multiple Spool Jobs from any type by a user. (SP01)

\*Data Sources: SAPcon - Spool Log\*

**Required Data Connectors**

SAP

### SAP - Multiple Spool Output Executions

Identifies multiple spools for a user within a specific timerange.

Source Action: Create and execute multiple Spool Jobs from any type by a user. (SP01)

\*Data Sources: SAPcon - Spool Log\*

**Required Data Connectors**

SAP

### SAP - Multiple Subnets by User

Identifies logon of the same user from several subnets within scheduled time interval.

Multiple configuration options available within the query.

Source Action: Logon using the same user thorugh different IP's.

\*Data Sources: SAPcon - Audit Log\*

**Required Data Connectors**

SAP

### SAP - New ICF Service Handlers

Identifies creation of ICF Handlers.

Source Action: Assign a new handler to a service using SICF.

\*Data Sources: SAPcon - Table Data Log\*

**Required Data Connectors**

SAP

### SAP - New ICF Services

Identifies creation of ICF Services.

Source Action: Create a service using SICF.

\*Data Sources: SAPcon - Table Data Log\*

**Required Data Connectors**

SAP

### SAP - RFC Execution of a Sensitive Function Module

Identifies execution of a sensitive function module using RFC.

Source Action: Execute a function module using RFC.

\*\*Recommended for Production only\*\*

Function Modules should be maintained in watchlist "SAP - Sensitive Function Modules"

\*Data Sources: SAPcon - Audit Log\*

**Required Data Connectors**

SAP

### SAP - Security Audit Log Configuration Change

Idenitifes changes for configuration in Securiy Audit Log

Source Action: change any Security Audit Log Configuration using SM19/RSAU\_CONFIG. (Filters/Status/Recording mode etc..)

\*Data Sources: SAPcon - Audit Log\*

**Required Data Connectors**

SAP

### SAP - Sensitive Privileged User Logged in

Identifies Dialog logon of a sensitive privileged user.

Source Action: Logon to the backend system using SAP\* or anoter privileged user.

Priveleged users should be maintained in "SAP - Privileged Users" Watchlist

This rule requires a fresh full reload of the SAP user master data to be performed daily.

\*Data Sources: SAPcon - Audit Log\*

\*Data Sources: SAPcon - User MD\*

**Required Data Connectors**

SAP

### SAP - Sensitive privileged user makes a change in another user

Identifies changes of sensitive privileged users in other users.

Source Action: Change user details / authorizations using SU01.

Priveleged users should be maintained in "SAP - Privileged Users" Watchlist

This rule requires a fresh full reload of SAP user master data to be performed daily.

\*Data Sources: SAPcon - Audit Log\*

\*Data Sources: SAPcon - User MD\*

**Required Data Connectors**

SAP

### SAP - Sensitive Role Changes

Identifies changes in sensitive roles.

Source Action: Change a role using PFCG.

Sensitive roles should be maintained in "SAP - Sensitive Roles" Watchlist

\*Data Sources: SAPcon - Change Documents Log\*

**Required Data Connectors**

SAP

### SAP - Sensitive Tables Direct Access By Dialog Logon

Identifies generic table access by dialog logon

Source Action: Open table contents using SE11/SE16/SE16N.

\*\*Recommended for Production only\*\*

Tables should be maintained in ""SAP - Sensitive Tables"" Watchlist.

\*Data Sources: SAPcon - Audit Log\*

**Required Data Connectors**

SAP

### SAP - Sensitive Tables Direct Access By RFC Logon

Identifies generic table access by RFC logon

Source Action: Open table contents using SE11/SE16/SE16N.

\*\*Recommended for Production only\*\*

Tables should be maintained in "SAP - Sensitive Tables" Watchlist.

\*Data Sources: SAPcon - Audit Log\*

**Required Data Connectors**

SAP

### SAP - Sensitive User's Password Change and Log in

Identifies password changes for privileged users.

Source Action: Change Password for a user and login to the system.

Priveleged users should be maintained in "SAP - Privileged Users" Watchlist

This rule requires a fresh full reload of SAP user master data to be performed daily.

\*Data Sources: SAPcon - Audit Log\*

\*Data Sources: SAPcon - User MD\*

**Required Data Connectors**

SAP

### SAP - SPNego Attack

Identifies SPNego Replay Attack.

\*Data Sources: SAPcon - Audit Log\*

**Required Data Connectors**

SAP

### SAP - Spool Takeover

Identifies a user printing a spool request which was created by someone else.

Source Action: Create a Spool Request using one user, Output it in using another user.

\*Data Sources: SAPcon - Spool Log\*

\*Data Sources: SAPcon - Spool Output Log\*

**Required Data Connectors**

SAP

### SAP - System Configuration Change

Identifies changes for system configuration.

Source Action: Adapt system change options or software components modifcation using SE06 transaction code.

\*Data Sources: SAPcon - Audit Log\*

**Required Data Connectors**

SAP

### SAP - Transaction is unlocked

Identifies unlocking of a transaction.

Source Action: Unlock a transaction code using SM01/SM01\_DEV/SM01\_CUS.

\*Data Sources: SAPcon - Audit Log\*

**Required Data Connectors**

SAP

### SAP - User Creates and uses new user

Identifies a user creating and using other users.

Source Action: Create a user using SU01. Login using the newly created user from the same IP.

\*Data Sources: SAPcon - Audit Log\*

**Required Data Connectors**

SAP

### SAP - User Unlocks and uses other users

A user unlocked another, and then used the other's user credentials.

Source Action: Unlock a user using SU01. Login using the unlocked user from the same IP.

\*Data Sources: SAPcon - Audit Log\*

\*Data Sources: SAPcon - Change Documents Log\*

**Required Data Connectors**

SAP

## Hunting Queries

## Watchlists

### SAP - Critical Authorizations

Critical Authorizations object which their assignment should be governed.

### SAP - Excluded Networks

Internal and maintenance of excluded networks for ignoring web dispatchers, terminal servers etc.

### SAP - Excluded Users

System users which are logged in the systems need to be ignored. (for example Multiple logons by user alert)

### SAP - FTP Servers

FTP Servers for identification of unauthorized connections.

### SAP - Networks

Internal and maintenance networks for identification of unauthorized logins.

### SAP - Obsolete Function Modules

Obsolete Function Modules which their execution should be governed.

### SAP - Obsolete Programs

Obsolete ABAP programs (reports) which their execution should be governed.

### SAP - Privileged Users

Privileged users which are under extra restrictions.

### SAP - Sensitive ABAP Programs

Sensitive ABAP programs (reports) which their execution should be governed.

### SAP - Sensitive Function Modules

Sensitive Function Modules which their execution should be governed.

### SAP - Sensitive Profiles

Sensitive profiles which their assignment should be governed.

### SAP - Sensitive Roles

Sensitive roles which their assignment should be governed.

### SAP - Sensitive Tables

Sensitive tables which their access should be governed.

### SAP - Sensitive Transactions

Sensitive transactions which their execution should be governed.

### SAP - Systems

Describes the landscape of SAP systems according to role and usage.

### SAP - Transactions for ABAP Generations

Transactions for ABAP generations which their execution should be governed.

### SAP\_Dynamic\_Audit\_Log\_Monitor\_Configuration

Configure the SAP audit log alerts by assigning each message ID a severity level as required by you, per system role (production, non-production). This watchlist also allows for configuring a designated team to handle each of the messages. Configure the SAP audit log alerts by assigning each message ID a severity level as required by you, per system role (production, non-production). This watchlist also allows for configuring a designated team to handle each of the messages, and excluding users by SAP roles or by tags from the SAPVIPUsers watchlist.

### SAP\_User\_Config

SAP VIP Users allows for fine tunning alerts by excluding users and including users in specific contexts.

## Playbooks

## Parsers

# Microsoft Sentinel Training Lab Solution (Preview)

Microsoft Sentinel Training Lab helps you get ramped up with Microsoft Sentinel providing hands-on practical experience for product features, capabilities, and scenarios.

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

## Data Connectors

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Microsoft Sysmon For Linux Solution

Sysmon for Linux provides detailed information about process creations, network connections and other system events.

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

## Data Connectors

### Microsoft Sysmon For Linux

[Sysmon for Linux](https://github.com/Sysinternals/SysmonForLinux) provides detailed information about process creations, network connections and other system events.

[Sysmon for linux link:]. The Sysmon for Linux connector uses [Syslog](https://aka.ms/sysLogInfo) as its data ingestion method. This solution depends on ASIM to work as expected. [Deploy ASIM](https://aka.ms/DeployASIM) to get the full value from the solution.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Microsoft Windows SQL Server Database Audit

The Microsoft Windows SQL Server Database Audit solution for Microsoft Sentinel enables security monitoring scenarios using Windows events.

**Data Connectors:** 0**, Workbooks:** 0**, Analytic Rules:** 0**, Hunting Queries:** 9**, Watchlists:** 0**, Playbooks:** 0, Parsers: 0

## Data Connectors

## Workbooks

## Analytic Rules

## Hunting Queries

### Failed Logon Attempts on SQL Server

Microsoft Windows SQL Server Database Audit Hunting Query 1

### Failed Logon on SQL Server from Same IPAddress in Short time Span

Microsoft Windows SQL Server Database Audit Hunting Query 2

### Multiple Failed Logon on SQL Server in Short time Span

Microsoft Windows SQL Server Database Audit Hunting Query 3

### New User created on SQL Server

Microsoft Windows SQL Server Database Audit Hunting Query 4

### User added to SQL Server SecurityAdmin Group

Microsoft Windows SQL Server Database Audit Hunting Query 5

### SQL User deleted from Database

Microsoft Windows SQL Server Database Audit Hunting Query 6

### User removed from SQL Server SecurityAdmin Group

Microsoft Windows SQL Server Database Audit Hunting Query 7

### User removed from SQL Server Roles

Microsoft Windows SQL Server Database Audit Hunting Query 8

### User Role altered on SQL Server

Microsoft Windows SQL Server Database Audit Hunting Query 9

## Watchlists

## Playbooks

## Parsers

# Minemeld

The Minemeld solution for Microsoft Sentinel has SOAR Connector and Playbooks, which helps to add indicators to Minemeld platform, enrich Microsoft Sentinel incident using Minemeld indicators data.

**Data Connectors:** 0**, Workbooks:** 0**, Analytic Rules:** 0**, Hunting Queries:** 0**, Watchlists:** 0**, Playbooks:** 2, Parsers: 0

## Data Connectors

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

### Create Indicator - Minemeld

This playbook search for indicators in Minemeld related to the entities(IP, filehash, URL) gathered from Sentinel incident. If the search result is positive a comment stating the indicator is already present or it creates a new indicator in Minemeld.

### Entity (IP, URL, FileHash) Enrichment - Minemeld

This playbook search for indicators in Minemeld related to the entities(IP, filehash, URL) gathered from Sentinel incident. If the search result is positive a comment will be added to enrich the incident, if not a comment stating no information available on Minemeld for searched indicator will be added to the incident.

## Parsers

# MongoDB Audit

The MongoDBAudit solution allows you to ingest Mongo DB audit information into Microsoft Sentinel. Refer to MongoDB documentation for more information.

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

## Data Connectors

### MongoDB Audit

MongoDB data connector provides the capability to ingest [MongoDBAudit](https://www.mongodb.com/) into Microsoft Sentinel. Refer to [MongoDB documentation](https://www.mongodb.com/docs/manual/tutorial/getting-started/) for more information.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### MongoDBAudit

Category: Samples

Function Alias: MongoDBAudit

# Morphisec UTPP

This parser will create new fields and terms to support improved queries and investigation of Morphisec threat logs.

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

## Data Connectors

### Morphisec UTPP

Integrate vital insights from your security products with the Morphisec Data Connector for Microsoft Sentinel and expand your analytical capabilities with search and correlation, threat intelligence, and customized alerts. Morphisec's Data Connector provides visibility into today's most advanced threats including sophisticated fileless attacks, in-memory exploits and zero days. With a single, cross-product view, you can make real-time, data-backed decisions to protect your most important assets

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### Morphisec

Category: Samples

Function Alias: Morphisec

# Mulesoft

The MuleSoft Cloudhub solution provides the capability to retrieve logs from Cloudhub applications using the Cloudhub API and more events into Microsoft Sentinel through the REST API.

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

## Data Connectors

### MuleSoft Cloudhub (using Azure Function)

The [MuleSoft Cloudhub](https://www.mulesoft.com/platform/saas/cloudhub-ipaas-cloud-based-integration) data connector provides the capability to retrieve logs from Cloudhub applications using the Cloudhub API and more events into Microsoft Sentinel through the REST API. The connector provides ability to get events which helps to examine potential security risks, analyze your team's use of collaboration, diagnose configuration problems and more.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### MuleSoftCloudhub

Category: Samples

Function Alias: MuleSoftCloudhub

# NC Protect Data Connector for Microsoft Sentinel

NC Protect Data Connector for Microsoft Sentinel enables customers to easily ingest user activity and logs collected in NC Protect and push it into Microsoft Sentinel to analyze the data at cloud scale using pre-built workbooks, as well as trigger alerts.

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

## Data Connectors

### NC Protect

[NC Protect Data Connector (archtis.com)](https://info.archtis.com/get-started-with-nc-protect-sentinel-data-connector) provides the capability to ingest user activity logs and events into Microsoft Sentinel. The connector provides visibility into NC Protect user activity logs and events in Microsoft Sentinel to improve monitoring and investigation capabilities

## Workbooks

### NCProtect

Sets the time name for analysis

**Required Data Types**

NCProtectUAL\_CL

NCProtect

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Netskope Data Connector for Microsoft Sentinel

This connector uses Azure Functions to connect to Netskope to pull logs into Microsoft Sentinel.

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

## Data Connectors

### Netskope (using Azure Function)

The [Netskope Cloud Security Platform](https://www.netskope.com/platform) connector provides the capability to ingest Netskope logs and events into Microsoft Sentinel. The connector provides visibility into Netskope Platform Events and Alerts in Microsoft Sentinel to improve monitoring and investigation capabilities.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

Parsers

### Netskope

Category: Samples

Function Alias: Netskope

# Network Threat Protection Essentials

The Network Threat Protection Essentials solution contains queries that identifies suspicious network behavior based on various data sources ingested in Sentinel.

**Data Connectors:** 0**, Workbooks:** 0**, Analytic Rules:** 2**, Hunting Queries:** 3**, Watchlists:** 0**, Playbooks:** 0, Parsers: 0

## Data Connectors

## Workbooks

## Analytic Rules

### Network endpoint to host executable correlation

Correlates blocked URLs hosting [malicious] executables with host endpoint data

to identify potential instances of executables of the same name having been recently run.

**Required Data Connectors**

TrendMicro

SecurityEvents

WindowsSecurityEvents

WindowsForwardedEvents

### New UserAgent observed in last 24 hours

Identifies new UserAgents observed in the last 24 hours versus the previous 14 days. This detection

extracts words from user agents to build the baseline and determine rareity rather than perform a

direct comparison. This avoids FPs caused by version numbers and other high entropy user agent components.

These new UserAgents could be benign. However, in normally stable environments,

these new UserAgents could provide a starting point for investigating malicious activity.

Note: W3CIISLog can be noisy depending on the environment, however OfficeActivity and AWSCloudTrail are

usually stable with low numbers of detections.

**Required Data Connectors**

AWS

Office365

AzureMonitor(IIS)

## Hunting Queries

### Exploit and Pentest Framework User Agent

Network Threat Protection Essentials Hunting Query 1

### Base64 encoded IPv4 address in request url

Network Threat Protection Essentials Hunting Query 2

### Risky base64 encoded command in URL

Network Threat Protection Essentials Hunting Query 3

## Watchlists

## Playbooks

## Parsers

# Netwrix Auditor (Preview)

The Netwrix Auditor solution provides the capability to ingest Netwrix Auditor (formerly Stealthbits Privileged Activity Manager) events into Microsoft Sentinel. Refer to Netwrix documentation for more information.

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

## Data Connectors

### Netwrix Auditor (formerly Stealthbits Privileged Activity Manager)

Netwrix Auditor data connector provides the capability to ingest [Netwrix Auditor (formerly Stealthbits Privileged Activity Manager)](https://www.netwrix.com/auditor.html) events into Microsoft Sentinel. Refer to [Netwrix documentation](https://helpcenter.netwrix.com/) for more information.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### NetwrixAuditor

Category: Samples

Function Alias: NetwrixAuditor

# Neustar IP GeoPoint

Solution for Microsoft Sentinel contains playbook to allows you to easily lookup for IP address to enrich Microsoft Sentinel's incident and to help auto remediation scenarios

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

## Data Connectors

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

### EnrichIP-GetIPGeoInfo-Neustar

When a new sentinel incident is created, this playbook gets triggered and performs the following actions:

1. Gets IP Addresses from incident.

2. Gets Geographical location information from Neustart IP GeoPoint API.

3. Summarize the details and add as a comment to the incident.

## Parsers

# Nginx

NGINX, is the company behind the popular open source project, NGINX. It offer a suite of technologies for developing and delivering modern applications.

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 10**, Hunting Queries:** 10**, Watchlists:** 0**, Playbooks:** 0, Parsers: 1

## Data Connectors

### NGINX HTTP Server

The NGINX HTTP Server data connector provides the capability to ingest [NGINX](https://nginx.org/en/) HTTP Server events into Microsoft Sentinel. Refer to [NGINX Logs documentation](https://nginx.org/en/docs/http/ngx\_http\_log\_module.html) for more information.

## Workbooks

### NGINX HTTP Server

Sets the time name for analysis

**Required Data Types**

## Analytic Rules

### NGINX - Command in URI

Detects command in URI

**Required Data Connectors**

NGINXHTTPServer

### NGINX - Core Dump

Detects a core dump of a crashing Nginx worker process, which could be a signal of a serious problem or exploitation attempts.

**Required Data Connectors**

NGINXHTTPServer

### NGINX - Multiple user agents for single source

Detects requests with different user agents from one source in short timeframe.

**Required Data Connectors**

NGINXHTTPServer

### NGINX - Known malicious user agent

Detects known malicious user agents

**Required Data Connectors**

NGINXHTTPServer

### NGINX - Multiple client errors from single IP address

Detects multiple client errors from one source in short timeframe

**Required Data Connectors**

NGINXHTTPServer

### NGINX - Multiple server errors from single IP address

Detects multiple server errors from one source in short timeframe

**Required Data Connectors**

NGINXHTTPServer

### NGINX - Private IP address in URL

Detects requests to unusual URL

**Required Data Connectors**

NGINXHTTPServer

### NGINX - Put file and get file from same IP address

Detects put or get files from one source in short timeframe

**Required Data Connectors**

NGINXHTTPServer

### NGINX - Request to sensitive files

Detects request to sensitive files.

**Required Data Connectors**

NGINXHTTPServer

### NGINX - Sql injection patterns

Detects possible sql injection patterns

**Required Data Connectors**

NGINXHTTPServer

## Hunting Queries

### NGINX - Uncommon user agent strings

NGINX HTTP Server Hunting Query 1

### NGINX - Abnormal request size

NGINX HTTP Server Hunting Query 2

### NGINX - Rare files requested

NGINX HTTP Server Hunting Query 3

### NGINX - Rare URLs requested

NGINX HTTP Server Hunting Query 4

### NGINX - Requests from bots and crawlers

NGINX HTTP Server Hunting Query 5

### NGINX - Requests to unexisting files

NGINX HTTP Server Hunting Query 6

### NGINX - Top files requested

NGINX HTTP Server Hunting Query 7

### NGINX - Top files with error requests

NGINX HTTP Server Hunting Query 8

### NGINX - Top URLs client errors

NGINX HTTP Server Hunting Query 9

### NGINX - Top URLs server errors

NGINX HTTP Server Hunting Query 10

## Watchlists

## Playbooks

## Parsers

### Nginx Data Parser

Category: Samples

Function Alias: NGINXHTTPServer

# NIST SP 800-53

This solution enables Compliance Teams, Architects, SecOps Analysts, and Consultants to gain situational awareness for cloud workload security posture.

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

## Data Connectors

## Workbooks

### NISTSP80053workbook

None

**Required Data Types**

## Analytic Rules

### NIST SP 800-53 Posture Changed

This alert is desinged to monitor Azure policies aligned with the NIST SP 800-53 Regulatory Compliance initative. The alert triggers when policy compliance falls below 70% within a 1 week timeframe.

**Required Data Connectors**

(none listed)

## Hunting Queries

## Watchlists

## Playbooks

### Notify\_GovernanceComplianceTeam

This playbook will create the Azure DevOps task filled with the Microsoft Sentinel incident details.

### Create-AzureDevOpsTask

This playbook will create the Azure DevOps task filled with the Microsoft Sentinel incident details.

### Create Jira Issue

This playbook will open a Jira Issue when a new incident is opened in Microsoft Sentinel.

## Parsers

# Noname Security for Microsoft Sentinel

Noname Security for Microsoft Sentinel

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

## Data Connectors

### Noname Security for Microsoft Sentinel

Noname Security solution to POST data into a Microsoft Sentinel SIEM workspace via the Azure Monitor REST API

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Nozomi Networks

The Nozomi Networks solution provides the capability to ingest Nozomi Networks Events into Microsoft Sentinel. Refer to the Nozomi Networks PDF documentation for more information.

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

## Data Connectors

### Nozomi Networks N2OS

The [Nozomi Networks](https://www.nozominetworks.com/) data connector provides the capability to ingest Nozomi Networks Events into Microsoft Sentinel. Refer to the Nozomi Networks [PDF documentation](https://www.nozominetworks.com/resources/data-sheets-brochures-learning-guides/) for more information.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### NozomiNetworksEvents

Category: Samples

Function Alias: NozomiNetworksEvents

# NXLog AIX Audit for Azure Sentinel

Collect and send AIX audit events with NXLog Enterprise Edition to Azure Sentinel.

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

## Data Connectors

### NXLog AIX Audit

The NXLog [AIX Audit](https://nxlog.co/documentation/nxlog-user-guide/im\_aixaudit.html) data connector uses the AIX Audit subsystem to read events directly from the kernel for capturing audit events on the AIX platform. This REST API connector can efficiently export AIX Audit events to Microsoft Sentinel in real time.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### NXLogAixAudit Data Parser

Category: Samples

Function Alias: NXLog\_parsed\_AIX\_Audit\_view

# NXLog BSM macOS for Microsoft Sentinel

Collect and send macOS BSM events with NXLog Enterprise Edition to Microsoft Sentinel.

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

## Data Connectors

### NXLog BSM macOS

The NXLog [BSM](https://nxlog.co/documentation/nxlog-user-guide/im\_bsm.html) macOS data connector uses Sun's Basic Security Module (BSM) Auditing API to read events directly from the kernel for capturing audit events on the macOS platform. This REST API connector can efficiently export macOS audit events to Azure Sentinel in real-time.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# NXLog DNS Logs for Azure Sentinel

Collect and send Windows DNS Server events with NXLog Enterprise Edition to Microsoft Sentinel.

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

## Data Connectors

### NXLog DNS Logs

The NXLog DNS Logs data connector uses Event Tracing for Windows ([ETW](https://docs.microsoft.com/windows/apps/trace-processing/overview)) for collecting both Audit and Analytical DNS Server events. The [NXLog \*im\_etw\* module](https://nxlog.co/documentation/nxlog-user-guide/im\_etw.html) reads event tracing data directly for maximum efficiency, without the need to capture the event trace into an .etl file. This REST API connector can forward DNS Server events to Microsoft Sentinel in real time.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### ASimDnsMicrosoftNXLog

Category: Samples

Function Alias: ASimDnsMicrosoftNXLog

# NXLog LinuxAudit for Microsoft Sentinel

Collect and send Linux Audit events with NXLog Enterprise Edition to Azure Sentinel.

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

## Data Connectors

### NXLog LinuxAudit

The NXLog [LinuxAudit](https://nxlog.co/documentation/nxlog-user-guide/im\_linuxaudit.html) data connector supports custom audit rules and collects logs without auditd or any other user-space software. IP addresses and group/user ids are resolved to their respective names making [Linux audit](https://nxlog.co/documentation/nxlog-user-guide/linux-audit.html) logs more intelligible to security analysts. This REST API connector can efficiently export Linux security events to Azure Sentinel in real-time.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Okta Single Sign-On Solution

Okta is an enterprise-grade, identity management service, built for the cloud, but compatible with many on-premises applications.

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 3**, Hunting Queries:** 5**, Watchlists:** 0**, Playbooks:** 3, Parsers: 0

## Data Connectors

### Okta Single Sign-On (using Azure Function)

The [Okta Single Sign-On (SSO)](https://www.okta.com/products/single-sign-on/) connector provides the capability to ingest audit and event logs from the Okta API into Microsoft Sentinel. The connector provides visibility into these log types in Microsoft Sentinel to view dashboards, create custom alerts, and to improve monitoring and investigation capabilities.

## Workbooks

### Okta Single Sign-On

Gain extensive insight into Okta Single Sign-On (SSO) by analyzing, collecting and correlating Audit and Event events.

This workbook provides visibility into message and click events that were permitted, delivered, or blocked

**Required Data Types**

Okta\_CL

OktaSSO

## Analytic Rules

### Failed Logins from Unknown or Invalid User

This query searches for numerous login attempts to the management console with an unknown or invalid user name

**Required Data Connectors**

OktaSSO

### User Login from Different Countries within 3 hours

This query searches for successful user logins to the Okta Console from different countries within 3 hours

**Required Data Connectors**

OktaSSO

### Potential Password Spray Attack

This query searches for failed attempts to log into the Okta console from more than 15 various users within a 5 minute timeframe from the same source. This is a potential indication of a password spray attack

**Required Data Connectors**

OktaSSO

## Hunting Queries

### Admin privilege granted (Okta)

Okta Single Sign-On Hunting Query 1

### Create API Token (Okta)

Okta Single Sign-On Hunting Query 2

### Initiate impersonation session (Okta)

Okta Single Sign-On Hunting Query 3

### Rare MFA Operations (Okta)

Okta Single Sign-On Hunting Query 4

### User password reset(Okta)

Okta Single Sign-On Hunting Query 5

## Watchlists

## Playbooks

### User enrichment - Okta

This playbook will collect user information from Okta and post a report on the incident.

### Prompt Okta user

This playbook uses the OKTA connector to prompt the risky user on Teams. User is asked action was taken by them. Based on the user confirmation the SOC admin is notified to investige on the user account. Also, comment is added to the incident with user information and summary of actions taken.

### Response on Okta user from Teams

This playbooks sends an adaptive card to the SOC Teams channel with information about the Okta user and incident details. The SOC is allowed to take action such suspend, reset password, expire password, add to group. An informative comment will be posted to the incident.

## Parsers

# One Identity Safeguard On Demand

Safeguard On Demand combines a session management and monitoring solution delivered from the cloud.

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

## Data Connectors

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# OneLogin IAM

The OneLogin solution for Microsoft Sentinel provides the capability to ingest common OneLogin IAM Platform events into Microsoft Sentinel through Webhooks.

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

## Data Connectors

### OneLogin IAM Platform (using Azure Function)

The [OneLogin](https://www.onelogin.com/) data connector provides the capability to ingest common OneLogin IAM Platform events into Microsoft Sentinel through Webhooks. The OneLogin Event Webhook API which is also known as the Event Broadcaster will send batches of events in near real-time to an endpoint that you specify. When a change occurs in the OneLogin, an HTTPS POST request with event information is sent to a callback data connector URL. Refer to [Webhooks documentation](https://developers.onelogin.com/api-docs/1/events/webhooks) for more information. The connector provides ability to get events which helps to examine potential security risks, analyze your team's use of collaboration, diagnose configuration problems and more.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### OneLogin

Category: Samples

Function Alias: OneLogin

# OpenCTI

The OpenCTI for Microsoft Sentinel enables you to ingest threat intelligence data from OpenCTI platform into Microsoft Sentinel. This solution also includes SOAR Connector and Playbooks, which helps in enriching Sentinel incidents and also adding indicator

**Data Connectors:** 0**, Workbooks:** 0**, Analytic Rules:** 0**, Hunting Queries:** 0**, Watchlists:** 0**, Playbooks:** 4, Parsers: 0

## Data Connectors

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

### Send to Security Graph API - Batch Import (OpenCTI)

This playbook sends messages to Security GraphAPI in batches

### Create Indicator - OpenCTI

This playbook adds new indicator in OpenCTI based on the entities info present in Sentinel incident. This playbook search in OpenCTI for indicatoes based on the entities (Account, Host, IP, FileHash, URL) present in Microsoft Sentinel incident. If it presnts in OpenCTI, information will be added to incident comment otherwise it creates new indicator in OpenCTI

### Entity (IP, URL, FileHash, Account, Host) Enrichment - OpenCTI

This playbook search in OpenCTI for indicatoes based on the entities (Account, Host, IP, FileHash, URL) present in Microsoft Sentinel incident. If it presnts in OpenCTI, information will be added to incident comment.

### Read Stream- OpenCTI Indicators

This playbook fetches indicators from OpenCTI and send to Sentinel. Supported types are Domain, File, IPv4, IPv6, Account, Url. This runs for every 10 minutes

## Parsers

# OpenVPN

The OpenVPN solution for Microsoft Sentinel provides the capability to ingest OpenVPN Server logs into Microsoft Sentinel.

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

## Data Connectors

### OpenVPN Server

The [OpenVPN](https://github.com/OpenVPN) data connector provides the capability to ingest OpenVPN Server logs into Microsoft Sentinel.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### OpenVPNEvent

Category: Samples

Function Alias: OpenVPNEvent

# Oracle Cloud Infrastructure

The Oracle Cloud Infrastructure (OCI) solution provides the capability to ingest OCI Logs from OCI Stream into Microsoft Sentinel using the OCI Streaming REST API.

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 10**, Hunting Queries:** 10**, Watchlists:** 0**, Playbooks:** 0, Parsers: 1

## Data Connectors

### Oracle Cloud Infrastructure (using Azure Function)

The Oracle Cloud Infrastructure (OCI) data connector provides the capability to ingest OCI Logs from [OCI Stream](https://docs.oracle.com/iaas/Content/Streaming/Concepts/streamingoverview.htm) into Microsoft Sentinel using the [OCI Streaming REST API](https://docs.oracle.com/iaas/api/#/streaming/streaming/20180418).

## Workbooks

### Oracle Cloud Infrastructure

Sets the time name for analysis

**Required Data Types**

## Analytic Rules

### OCI - Discovery activity

Detects possible discovery activity.

**Required Data Connectors**

OracleCloudInfrastructureLogsConnector

### OCI - Event rule deleted

Detects when event rule was deleted.

**Required Data Connectors**

OracleCloudInfrastructureLogsConnector

### OCI - Inbound SSH connection

Detects inbound SSH connection.

**Required Data Connectors**

OracleCloudInfrastructureLogsConnector

### OCI - Insecure metadata endpoint

Detects insecure metadata endpoint.

**Required Data Connectors**

OracleCloudInfrastructureLogsConnector

### OCI - Instance metadata access

Detects instance metadata access.

**Required Data Connectors**

OracleCloudInfrastructureLogsConnector

### OCI - Multiple instances launched

Detects when multiple instances were launched.

**Required Data Connectors**

OracleCloudInfrastructureLogsConnector

### OCI - Multiple instances terminated

Detects when multiple instances were terminated.

**Required Data Connectors**

OracleCloudInfrastructureLogsConnector

### OCI - Multiple rejects on rare ports

Detects multiple rejects on rare ports.

**Required Data Connectors**

OracleCloudInfrastructureLogsConnector

### OCI - SSH scanner

Detects possible SSH scanning activity.

**Required Data Connectors**

OracleCloudInfrastructureLogsConnector

### OCI - Unexpected user agent

Detects unexpected user agent strings.

**Required Data Connectors**

OracleCloudInfrastructureLogsConnector

## Hunting Queries

### OCI - Destination ports (inbound traffic)

Oracle Cloud Infrastructure Hunting Query 1

### OCI - Destination ports (outbound traffic)

Oracle Cloud Infrastructure Hunting Query 2

### OCI - Launched instances

Oracle Cloud Infrastructure Hunting Query 3

### OCI - Update activities

Oracle Cloud Infrastructure Hunting Query 4

### OCI - Delete operations

Oracle Cloud Infrastructure Hunting Query 5

### OCI - Deleted users

Oracle Cloud Infrastructure Hunting Query 6

### OCI - New users

Oracle Cloud Infrastructure Hunting Query 7

### OCI - User source IP addresses

Oracle Cloud Infrastructure Hunting Query 8

### OCI - Terminated instances

Oracle Cloud Infrastructure Hunting Query 9

### OCI - Updated instances

Oracle Cloud Infrastructure Hunting Query 10

## Watchlists

## Playbooks

## Parsers

### OCILogs

Category: Samples

Function Alias: OCILogs

# Oracle Database Audit Solution

The Oracle Database Audit solution provides the capability to ingest Oracle Database audit events into Microsoft Sentinel through the syslog.

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 10**, Hunting Queries:** 10**, Watchlists:** 0**, Playbooks:** 0, Parsers: 1

## Data Connectors

### Oracle Database Audit

The Oracle DB Audit data connector provides the capability to ingest [Oracle Database](https://www.oracle.com/database/technologies/) audit events into Microsoft Sentinel through the syslog. Refer to [documentation](https://docs.oracle.com/en/database/oracle/oracle-database/21/dbseg/introduction-to-auditing.html#GUID-94381464-53A3-421B-8F13-BD171C867405) for more information.

## Workbooks

### Oracle Database Audit

Sets the time name for analysis

**Required Data Types**

Syslog

OracleDatabaseAudit

## Analytic Rules

### OracleDBAudit - Connection to database from external IP

Detects when connection to database is from external IP source.

**Required Data Connectors**

OracleDatabaseAudit

### OracleDBAudit - Multiple tables dropped in short time

Detects when user drops many tables in short period of time.

**Required Data Connectors**

OracleDatabaseAudit

### OracleDBAudit - Connection to database from unknown IP

Detects when user connects to a database from IP address which is not present in AllowList.

**Required Data Connectors**

OracleDatabaseAudit

### OracleDBAudit - User connected to database from new IP

Detects when a user connects to database from new IP address.

**Required Data Connectors**

OracleDatabaseAudit

### OracleDBAudit - New user account

Detects when an action was made by new user.

**Required Data Connectors**

OracleDatabaseAudit

### OracleDBAudit - Query on Sensitive Table

Detects when user queries sensitive tables.

**Required Data Connectors**

OracleDatabaseAudit

### OracleDBAudit - User activity after long inactivity time

Detects when an action was made by a user which last activity was observed more than 30 days ago.

**Required Data Connectors**

OracleDatabaseAudit

### OracleDBAudit - Unusual user activity on multiple tables

Detects when user queries many tables in short period of time.

**Required Data Connectors**

OracleDatabaseAudit

### OracleDBAudit - Shutdown Server

Detects when "SHUTDOWN" command was sent to server.

**Required Data Connectors**

OracleDatabaseAudit

### OracleDBAudit - SQL injection patterns

Detects common known SQL injection patterns used in automated scripts.

**Required Data Connectors**

OracleDatabaseAudit

## Hunting Queries

### OracleDBAudit - Action by Ip

OracleDatabaseAudit Hunting Query 1

### OracleDBAudit - Action by user

OracleDatabaseAudit Hunting Query 2

### OracleDBAudit - Active Users

OracleDatabaseAudit Hunting Query 3

### OracleDBAudit - Users connected to databases during non-operational hours.

OracleDatabaseAudit Hunting Query 4

### OracleDBAudit - Dropped Tables

OracleDatabaseAudit Hunting Query 5

### OracleDBAudit - Inactive Users

OracleDatabaseAudit Hunting Query 6

### OracleDBAudit - Audit large queries

OracleDatabaseAudit Hunting Query 7

### OracleDBAudit - Top tables queries

OracleDatabaseAudit Hunting Query 8

### OracleDBAudit - Users with new privileges

OracleDatabaseAudit Hunting Query 9

### OracleDBAudit - Users Privileges Review

OracleDatabaseAudit Hunting Query 10

## Watchlists

## Playbooks

## Parsers

### OracleDatabaseAudit Data Parser

Category: Samples

Function Alias: OracleDatabaseAuditEvent

# Oracle WebLogic Server

The Oracle WebLogic Server solution for Microsoft Sentinel provides the capability to ingest Oracle Web Logic Server events into Microsoft Sentinel

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 10**, Hunting Queries:** 10**, Watchlists:** 0**, Playbooks:** 0, Parsers: 1

## Data Connectors

### Oracle WebLogic Server

OracleWebLogicServer data connector provides the capability to ingest [OracleWebLogicServer](https://docs.oracle.com/en/middleware/standalone/weblogic-server/index.html) events into Microsoft Sentinel. Refer to [OracleWebLogicServer documentation](https://docs.oracle.com/en/middleware/standalone/weblogic-server/14.1.1.0/index.html) for more information.

## Workbooks

### Oracle WebLogic Server

Sets the time name for analysis

**Required Data Types**

OracleWebLogicServer\_CL

OracleWebLogicServer

## Analytic Rules

### Oracle - Command in URI

Detects command in URI

**Required Data Connectors**

OracleWebLogicServer

### Oracle - Multiple user agents for single source

Detects requests with different user agents from one source in short timeframe.

**Required Data Connectors**

OracleWebLogicServer

### Oracle - Oracle WebLogic Exploit CVE-2021-2109

Detects exploitation of Oracle WebLogic vulnerability CVE-2021-2109

**Required Data Connectors**

OracleWebLogicServer

### Oracle - Malicious user agent

Detects known malicious user agent strings

**Required Data Connectors**

OracleWebLogicServer

### Oracle - Multiple client errors from single IP

Detects multiple client errors from one source in short timeframe

**Required Data Connectors**

OracleWebLogicServer

### Oracle - Multiple server errors from single IP

Detects multiple server errors from one source in short timeframe

**Required Data Connectors**

OracleWebLogicServer

### Oracle - Private IP in URL

Detects requests to unusual URL

**Required Data Connectors**

OracleWebLogicServer

### Oracle - Put file and get file from same IP address

Detects put or get files from one source in short timeframe

**Required Data Connectors**

OracleWebLogicServer

### Oracle - Put suspicious file

Detects PUT or POST of suspicious file

**Required Data Connectors**

OracleWebLogicServer

### Oracle - Request to sensitive files

Detects request to sensitive files.

**Required Data Connectors**

OracleWebLogicServer

## Hunting Queries

### Oracle - Request to forbidden files

OracleWebLogicServer Hunting Query 1

### Oracle - Abnormal request size

OracleWebLogicServer Hunting Query 2

### Oracle - Critical event severity

OracleWebLogicServer Hunting Query 3

### Oracle - Error messages

OracleWebLogicServer Hunting Query 4

### Oracle - Top files requested by users with error

OracleWebLogicServer Hunting Query 5

### Oracle - Rare user agents with client errors

OracleWebLogicServer Hunting Query 6

### Oracle - Rare URLs requested

OracleWebLogicServer Hunting Query 7

### Oracle - Rare user agents

OracleWebLogicServer Hunting Query 8

### Oracle - Top URLs client errors

OracleWebLogicServer Hunting Query 9

### Oracle - Top URLs server errors

OracleWebLogicServer Hunting Query 10

## Watchlists

## Playbooks

## Parsers

### OracleWebLogicServer Data Parser

Category: Samples

Function Alias: OracleWebLogicServerEvent

# Orca Security Alerts

Search and Discover Orca Alerts in Azure Sentinel.

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

## Data Connectors

### Orca Security Alerts

The Orca Security Alerts connector allows you to easily export Alerts logs to Azure Sentinel.

## Workbooks

### Orca alerts overview

A visualized overview of Orca security alerts.

Explore, analize and learn about your security posture using Orca alerts Overview

**Required Data Types**

OrcaAlerts\_CL

OrcaSecurityAlerts

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# OSSEC

The OSSEC solution provides the capability to ingest OSSEC events into Microsoft Sentinel. Refer to OSSEC documentation for more information.

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

## Data Connectors

### OSSEC

OSSEC data connector provides the capability to ingest [OSSEC](https://www.ossec.net/) events into Azure Sentinel. Refer to [OSSEC documentation](https://www.ossec.net/docs) for more information.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### OSSECEvent

Category: Samples

Function Alias: OSSECEvent

# Palo Alto Networks Cortex Data Lake Solution

The Palo Alto Networks CDL solution provides the capability to ingest CDL logs into Microsoft Sentinel.

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 10**, Hunting Queries:** 10**, Watchlists:** 0**, Playbooks:** 0, Parsers: 1

## Data Connectors

### Palo Alto Networks Cortex Data Lake (CDL)

The [Palo Alto Networks CDL](https://www.paloaltonetworks.com/cortex/cortex-data-lake) data connector provides the capability to ingest [CDL logs](https://docs.paloaltonetworks.com/cortex/cortex-data-lake/log-forwarding-schema-reference/log-forwarding-schema-overview.html) into Microsoft Sentinel.

## Workbooks

### Palo Alto Networks Cortex Data Lake

Sets the time name for analysis

**Required Data Types**

CommonSecurityLog

PaloAltoCDL

## Analytic Rules

### PaloAlto - MAC address conflict

Detects several users with the same MAC address.

**Required Data Connectors**

PaloAltoCDL

### PaloAlto - Dropping or denying session with traffic

Detects dropping or denying session with traffic.

**Required Data Connectors**

PaloAltoCDL

### PaloAlto - File type changed

Detects when file type changed.

**Required Data Connectors**

PaloAltoCDL

### PaloAlto - Inbound connection to high risk ports

Detects inbound connection to high risk ports.

**Required Data Connectors**

PaloAltoCDL

### PaloAlto - Possible attack without response

Detects possible attack without response.

**Required Data Connectors**

PaloAltoCDL

### PaloAlto - Possible flooding

Detects possible flooding.

**Required Data Connectors**

PaloAltoCDL

### PaloAlto - Possible port scan

Detects possible port scan.

**Required Data Connectors**

PaloAltoCDL

### PaloAlto - User privileges was changed

Detects changing of user privileges.

**Required Data Connectors**

PaloAltoCDL

### PaloAlto - Put and post method request in high risk file type

Detects put and post method request in high risk file type.

**Required Data Connectors**

PaloAltoCDL

### PaloAlto - Forbidden countries

Detects suspicious connections from forbidden countries.

**Required Data Connectors**

PaloAltoCDL

## Hunting Queries

### PaloAlto - Critical event result

PaloAltoCDL Hunting Query 1

### PaloAlto - File permission with PUT or POST request

PaloAltoCDL Hunting Query 2

### PaloAlto - Destination ports by IPs

PaloAltoCDL Hunting Query 3

### PaloAlto - Incomplete application protocol

PaloAltoCDL Hunting Query 4

### PaloAlto - Multiple Deny result by user

PaloAltoCDL Hunting Query 5

### PaloAlto - Agent versions

PaloAltoCDL Hunting Query 6

### PaloAlto - Outdated config vesions

PaloAltoCDL Hunting Query 7

### PaloAlto - Rare application layer protocols

PaloAltoCDL Hunting Query 8

### PaloAlto - Rare files observed

PaloAltoCDL Hunting Query 9

### PaloAlto - Rare ports by user

PaloAltoCDL Hunting Query 10

## Watchlists

## Playbooks

## Parsers

### PaloAltoCDLEvent

Category: Samples

Function Alias: PaloAltoCDLEvent

# Palo Alto PAN-OS Solution (Preview)

By leveraging the key technologies that are built into PAN‑OS natively—App‑ID, Content‑ID, Device-ID, and User‑ID can have complete visibility and control of the applications in use across all users and devices in all locations all the time.

**Data Connectors:** 1**, Workbooks:** 2**, Analytic Rules:** 4**, Hunting Queries:** 1**, Watchlists:** 0**, Playbooks:** 5, Parsers: 0

## Data Connectors

### Palo Alto Networks (Firewall)

The Palo Alto Networks firewall connector allows you to easily connect your Palo Alto Networks logs with Microsoft Sentinel, to view dashboards, create custom alerts, and improve investigation. This gives you more insight into your organization's network and improves your security operation capabilities.

## Workbooks

### Palo Alto overview

Gain insights and comprehensive monitoring into Palo Alto firewalls by analyzing traffic and activities.

This workbook correlates all Palo Alto data with threat events to identify suspicious entities and relationships.

You can learn about trends across user and data traffic, and drill down into Palo Alto Wildfire and filter results.

**Required Data Types**

CommonSecurityLog

PaloAltoNetworks

### Palo Alto Network Threat

Gain insights into Palo Alto network activities by analyzing threat events.

You can extract meaningful security information by correlating data between threats, applications, and time.

This workbook makes it easy to track malware, vulnerability, and virus log events.

**Required Data Types**

CommonSecurityLog

PaloAltoNetworks

## Analytic Rules

### Palo Alto Threat signatures from Unusual IP addresses

Identifies Palo Alto Threat signatures from unusual IP addresses which are not historically seen.

This detection is also leveraged and required for MDE and PAN Fusion scenario

https://docs.microsoft.com/Azure/sentinel/fusion-scenario-reference#network-request-to-tor-anonymization-service-followed-by-anomalous-traffic-flagged-by-palo-alto-networks-firewall

**Required Data Connectors**

PaloAltoNetworks

### Microsoft COVID-19 file hash indicator matches

Identifies a match in CommonSecurityLog Event data from any FileHash published in the Microsoft COVID-19 Threat Intel Feed - as described at https://www.microsoft.com/security/blog/2020/05/14/open-sourcing-covid-threat-intelligence/

**Required Data Connectors**

PaloAltoNetworks

### Palo Alto - potential beaconing detected

Identifies beaconing patterns from Palo Alto Network traffic logs based on recurrent timedelta patterns.

The query leverages various KQL functions to calculate time deltas and then compares it with total events observed in a day to find percentage of beaconing.

This outbound beaconing pattern to untrusted public networks should be investigated for any malware callbacks or data exfiltration attempts.

Reference Blog:

http://www.austintaylor.io/detect/beaconing/intrusion/detection/system/command/control/flare/elastic/stack/2017/06/10/detect-beaconing-with-flare-elasticsearch-and-intrusion-detection-systems/

https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/detect-network-beaconing-via-intra-request-time-delta-patterns/ba-p/779586

**Required Data Connectors**

PaloAltoNetworks

### Palo Alto - possible internal to external port scanning

Identifies a list of internal Source IPs (10.x.x.x Hosts) that have triggered 10 or more non-graceful tcp server resets from one or more Destination IPs which

results in an "ApplicationProtocol = incomplete" designation. The server resets coupled with an "Incomplete" ApplicationProtocol designation can be an indication

of internal to external port scanning or probing attack.

References: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClUvCAK and

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClTaCAK

**Required Data Connectors**

PaloAltoNetworks

## Hunting Queries

### Palo Alto - high-risk ports

PaloAlto-PAN-OS Hunting Query 1

## Watchlists

## Playbooks

### Get System Info - Palo Alto PAN-OS XML API

This playbook allows us to get System Info of a Palo Alto device for a Sentinel alert.When a new Sentinel incident is created, this playbook gets triggered and performs below actions:

1. Gets the various parameters from the alert

2. Gets the System Info for the device in the alert.

3. Creates a Sentinel Incident and updates it with the system info.

### Get Threat PCAP - Palo Alto PAN-OS XML API

This playbook allows us to get a threat PCAP for a given PCAP ID.When a new Sentinel incident is created, this playbook gets triggered and performs below actions:

1. Gets the various parameters from the alert

2. Gets the PCAP from the device.

3. Puts the PCAP in Blob Storage

4. Creates a Sentinel Incident and updates it with a link to the blob.

### PaloAlto-PAN-OS-GetURLCategoryInfo

When a new sentinal incident is created, this playbook gets triggered and performs below actions:1. Fetches the address group details and URL filtering category information from PAN-OS

2. Updates all the collected information in incident

![PaloAlto-PAN-OS-GetURLCategoryInfo](https://github.com/Azure/Azure-Sentinel/blob/master/Solutions/PaloAlto-PAN-OS/Playbooks/PaloAlto-PAN-OS-GetURLCategoryInfo/designerscreenshot.PNG?raw=true)

### PaloAlto-PAN-OS-BlockIP

This playbook allows blocking/unblocking IPs in PaloAlto, using \*\*Address Object Groups\*\*. This allows to make changes on predefined address group, which is attached to predefined security policy rule.When a new Sentinel incident is created, this playbook gets triggered and performs below actions:

1. An adaptive card is sent to the SOC channel providing Incident information, IP address, list of existing security policy rules in which IP is a member of and provides an option to Block/Unblock IP Address to predefined address group or Ignore.

2. The SOC can take action on risky IP based on the information provided in the adaptive card.

![PaloAlto-PAN-OS-BlockIP](https://github.com/Azure/Azure-Sentinel/blob/master/Solutions/PaloAlto-PAN-OS/Playbooks/PaloAlto-PAN-OS-BlockIP/designerscreenshot.PNG?raw=true)

\*\*This is the adaptive card SOC will receive when playbook is triggered for each risky IP for taking actions like block/unblock/ignore:\*\*

![Adaptive Card example](https://github.com/Azure/Azure-Sentinel/blob/master/Solutions/PaloAlto-PAN-OS/Playbooks/PaloAlto-PAN-OS-BlockIP/AdaptiveCardtoBlockorUnblock.PNG?raw=true)

\*\*This is the consolidate adaptive card about the summary of actions taken on IP and the incident configuration:\*\*

![Consolidated Adaptive Card example](https://github.com/Azure/Azure-Sentinel/blob/master/Solutions/PaloAlto-PAN-OS/Playbooks/PaloAlto-PAN-OS-BlockIP/SummarizedAdaptiveCard.PNG?raw=true)

### PaloAlto-PAN-OS-BlockURL

This playbook allows blocking/unblocking URLs in PaloAlto, using \*\*predefined address group\*\*. This allows to make changes on predefined address group, which is attached to security policy rule.When a new Sentinel incident is created, this playbook gets triggered and performs below actions:

1. An adaptive card is sent to the SOC channel providing Incident information, URL address, list of existing security policy rules in which URL is a member of and provides an option to Block/Unblock URL Address by adding/removing it to/from the predefined address group.

2. The SOC can act on risky URL based on the information provided in the adaptive card, or ignore.

![PaloAlto-PAN-OS-BlockURL](https://github.com/Azure/Azure-Sentinel/blob/master/Solutions/PaloAlto-PAN-OS/Playbooks/PaloAlto-PAN-OS-BlockURL/designerscreenshot.PNG?raw=true)

\*\*This is the adaptive card SOC will receive when playbook is triggered for each risky URL for taking actions like block/unblock/ignore ::\*\*

![Adaptive Card example](https://github.com/Azure/Azure-Sentinel/blob/master/Solutions/PaloAlto-PAN-OS/Playbooks/PaloAlto-PAN-OS-BlockURL/AdaptiveCardtoBlockorUnblock.PNG?raw=true)

\*\*This is the consolidate adaptive card about the summary of actions taken on URL and the incident configuration ::\*\*

![Consolidated Adaptive Card example](https://github.com/Azure/Azure-Sentinel/blob/master/Solutions/PaloAlto-PAN-OS/Playbooks/PaloAlto-PAN-OS-BlockURL/SummarizedAdaptiveCard.PNG?raw=true)

## Parsers

# Palo Alto Prisma Cloud CSPM Solution

Prisma Cloud is the industry's only comprehensive Cloud Native Security Platform that delivers full lifecycle security and full stack protection for multi- and hybrid-cloud environments.

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 11**, Hunting Queries:** 9**, Watchlists:** 0**, Playbooks:** 2, Parsers: 1

## Data Connectors

### Palo Alto Prisma Cloud CSPM (using Azure Function)

The Palo Alto Prisma Cloud CSPM data connector provides the capability to ingest [Prisma Cloud CSPM alerts](https://prisma.pan.dev/api/cloud/cspm/alerts#operation/get-alerts) and [audit logs](https://prisma.pan.dev/api/cloud/cspm/audit-logs#operation/rl-audit-logs) into Microsoft sentinel using the Prisma Cloud CSPM API. Refer to [Prisma Cloud CSPM API documentation](https://prisma.pan.dev/api/cloud/cspm) for more information.

## Workbooks

### Palo Alto Prisma

Sets the time name for analysis.

**Required Data Types**

PaloAltoPrismaCloudAlert\_CL

PaloAltoPrismaCloudAudit\_CL

PaloAltoPrismaCloud

## Analytic Rules

### Palo Alto Prisma Cloud - Access keys are not rotated for 90 days

Detects access keys which were not rotated for 90 days.

**Required Data Connectors**

PaloAltoPrismaCloud

### Palo Alto Prisma Cloud - Network ACL allow all outbound traffic

Detects network ACLs with outbound rule to allow all traffic.

**Required Data Connectors**

PaloAltoPrismaCloud

### Palo Alto Prisma Cloud - Network ACL allow ingress traffic to server administration ports

Detects Network ACLs allow ingress traffic to server administration ports.

**Required Data Connectors**

PaloAltoPrismaCloud

### Palo Alto Prisma Cloud - Network ACLs Inbound rule to allow All Traffic

Detects Network ACLs with Inbound rule to allow All Traffic.

**Required Data Connectors**

PaloAltoPrismaCloud

### Palo Alto Prisma Cloud - Anomalous access key usage

Detects anomalous API key usage activity.

**Required Data Connectors**

PaloAltoPrismaCloud

### Palo Alto Prisma Cloud - High risk score alert

Detects alerts with high risk score value.

**Required Data Connectors**

PaloAltoPrismaCloud

### Palo Alto Prisma Cloud - High severity alert opened for several days

Detects high severity alert which is opened for several days.

**Required Data Connectors**

PaloAltoPrismaCloud

### Palo Alto Prisma Cloud - IAM Group with Administrator Access Permissions

Detects IAM Groups with Administrator Access Permissions.

**Required Data Connectors**

PaloAltoPrismaCloud

### Palo Alto Prisma Cloud - Inactive user

Detects users inactive for 30 days.

**Required Data Connectors**

PaloAltoPrismaCloud

### Palo Alto Prisma Cloud - Maximum risk score alert

Detects alerts with maximum risk score value.

**Required Data Connectors**

PaloAltoPrismaCloud

### Palo Alto Prisma Cloud - Multiple failed logins for user

Detects multiple failed logins for the same user account.

**Required Data Connectors**

PaloAltoPrismaCloud

## Hunting Queries

### Palo Alto Prisma Cloud - Access keys used

PaloAltoPrismaCloud Hunting Query 1

### Palo Alto Prisma Cloud - Top sources of failed logins

PaloAltoPrismaCloud Hunting Query 2

### Palo Alto Prisma Cloud - Top users by failed logins

PaloAltoPrismaCloud Hunting Query 3

### Palo Alto Prisma Cloud - High risk score opened alerts

PaloAltoPrismaCloud Hunting Query 4

### Palo Alto Prisma Cloud - High severity alerts

PaloAltoPrismaCloud Hunting Query 5

### Palo Alto Prisma Cloud - New users

PaloAltoPrismaCloud Hunting Query 6

### Palo Alto Prisma Cloud - Opened alerts

PaloAltoPrismaCloud Hunting Query 7

### Palo Alto Prisma Cloud - Top recources with alerts

PaloAltoPrismaCloud Hunting Query 8

### Palo Alto Prisma Cloud - Updated resources

PaloAltoPrismaCloud Hunting Query 9

## Watchlists

## Playbooks

### Fetch Security Posture from Prisma Cloud

This playbook provides/updates the compliance security posture details of asset in comments section of triggered incident so that SOC analysts can directly take corrective measure to prevent the attack

### Remediate assets on prisma cloud

This playbook provides/updates the compliance security posture details of asset in comments section of triggered incident so that SOC analysts can directly take corrective measure to prevent the attack

## Parsers

### PaloAltoPrismaCloud Data Parser

Category: Samples

Function Alias: PaloAltoPrismaCloud

# PCI DSS Compliance

This Solution enables Microsoft Sentinel users to harness the power of their SIEM to assist in meeting PCI-DSS 3.2.1 requirements.

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

## Data Connectors

## Workbooks

### PCI DSS Compliance

Choose your subscription and workspace in which PCI assets are deployed

**Required Data Types**

AzureDaignostics

SecurityEvent

SecurityAlert

OracleDatabaseAuditEvent

Syslog

Anomalies

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Perimeter 81

Perimeter 81 offers robust logging which provides administrators with information crucial to managing and securing network access. View this data inside Microsoft Sentinel.

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

## Data Connectors

### Perimeter 81 Activity Logs

The Perimeter 81 Activity Logs connector allows you to easily connect your Perimeter 81 activity logs with Azure Sentinel, to view dashboards, create custom alerts, and improve investigation.

## Workbooks

### Perimeter 81 Overview

Gain insights and comprehensive monitoring into your Perimeter 81 account by analyzing activities.

**Required Data Types**

Perimeter81\_CL

Perimeter81ActivityLogs

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# PingFederate

PingFederate is the leading enterprise federation server for user authentication and standards-based single sign-on (SSO) for employee, partner and customer identity types.

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 11**, Hunting Queries:** 10**, Watchlists:** 0**, Playbooks:** 0, Parsers: 1

## Data Connectors

### PingFederate

The [PingFederate](https://www.pingidentity.com/en/software/pingfederate.html) data connector provides the capability to ingest [PingFederate events](https://docs.pingidentity.com/bundle/pingfederate-102/page/lly1564002980532.html) into Microsoft Sentinel. Refer to [PingFederate documentation](https://docs.pingidentity.com/bundle/pingfederate-102/page/tle1564002955874.html) for more information.

## Workbooks

### PingFederate

Sets the time name for analysis

**Required Data Types**

PingFederateEvent

PingFederate

## Analytic Rules

### Ping Federate - Abnormal password reset attempts

Detects abnormal password reset attempts for user in short period of time.

**Required Data Connectors**

PingFederate

### Ping Federate - Authentication from new IP.

Detects authentication requests from new IP address.

**Required Data Connectors**

PingFederate

### Ping Federate - Forbidden country

Detects requests from forbidden countries.

**Required Data Connectors**

PingFederate

### Ping Federate - Abnormal password resets for user

Detects multiple password reset for user.

**Required Data Connectors**

PingFederate

### Ping Federate - New user SSO success login

Detects new user SSO success login.

**Required Data Connectors**

PingFederate

### Ping Federate - OAuth old version

Detects requests using not the latest version of OAuth protocol.

**Required Data Connectors**

PingFederate

### Ping Federate - Password reset request from unexpected source IP address..

Detects password reset requests from unexpected source IP address.

**Required Data Connectors**

PingFederate

### Ping Federate - SAML old version

Detects requests using not the latest version of SAML protocol.

**Required Data Connectors**

PingFederate

### Ping Federate - Unexpected authentication URL.

Detects unexpected authentication URL.

**Required Data Connectors**

PingFederate

### Ping Federate - Unexpected country for user

Detects requests from different countries for user in shotr term.

**Required Data Connectors**

PingFederate

### Ping Federate - Unusual mail domain.

Detects unusual mail domain in authentication requests.

**Required Data Connectors**

PingFederate

## Hunting Queries

### Ping Federate - Authentication URLs

PingFederate Hunting Query 1

### Ping Federate - Failed Authentication

PingFederate Hunting Query 2

### Ping Federate - New users

PingFederate Hunting Query 3

### Ping Federate - Password reset requests

PingFederate Hunting Query 4

### Ping Federate - Rare source IP addresses

PingFederate Hunting Query 5

### Ping Federate - SAML subjects

PingFederate Hunting Query 6

### Ping Federate - Top source IP addresses

PingFederate Hunting Query 7

### Ping Federate - Requests from unusual countries

PingFederate Hunting Query 8

### Ping Federate - Authentication from unusual sources

PingFederate Hunting Query 9

### Ping Federate - Users recently reseted password

PingFederate Hunting Query 10

## Watchlists

## Playbooks

## Parsers

### PingFederate Data Parser

Category: Samples

Function Alias: PingFederateEvent

# PostgreSQL

The PostgreSQL solution provides the capability to ingest PostgreSQL events into Microsoft Sentinel. Refer to PostgreSQL documentation for more information.

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

## Data Connectors

### PostgreSQL Events

PostgreSQL data connector provides the capability to ingest [PostgreSQL](https://www.postgresql.org/) events into Microsoft Sentinel. Refer to [PostgreSQL documentation](https://www.postgresql.org/docs/current/index.html) for more information.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### PostgreSQLEvent

Category: Samples

Function Alias: PostgreSQLEvent

# Proofpoint On demand (POD) Email Security

Proofpoint on Demand Email Security accurately classifies various types of email, while detecting and blocking threats without malicious payload. You can automatically tag suspicious email to raise end-user awareness, and track down any email in seconds.

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 8**, Hunting Queries:** 10**, Watchlists:** 0**, Playbooks:** 0, Parsers: 1

## Data Connectors

### Proofpoint On Demand Email Security (using Azure Function)

Proofpoint On Demand Email Security data connector provides the capability to get Proofpoint on Demand Email Protection data, allows users to check message traceability, monitoring into email activity, threats,and data exfiltration by attackers and malicious insiders. The connector provides ability to review events in your org on an accelerated basis, get event log files in hourly increments for recent activity.

## Workbooks

### Proofpoint On-Demand Email Security

Gain insights into your Proofpoint on Demand Email Security activities, including maillog and messages data. The Workbook provides users with an executive dashboard showing the reporting capabilities, message traceability and monitoring.

**Required Data Types**

ProofpointPOD\_maillog\_CL

ProofpointPOD\_message\_CL

ProofpointPOD

## Analytic Rules

### ProofpointPOD - Binary file in attachment

Detects when email received with binary file as attachment.

**Required Data Connectors**

ProofpointPOD

### ProofpointPOD - Possible data exfiltration to private email

Detects when sender sent email to the non-corporate domain and recipient's username is the same as sender's username.

**Required Data Connectors**

ProofpointPOD

### ProofpointPOD - High risk message not discarded

Detects when email with high risk score was not rejected or discarded by filters.

**Required Data Connectors**

ProofpointPOD

### ProofpointPOD - Multiple archived attachments to the same recipient

Detects when multiple emails where sent to the same recipient with large archived attachments.

**Required Data Connectors**

ProofpointPOD

### ProofpointPOD - Multiple large emails to the same recipient

Detects when multiple emails with large size where sent to the same recipient.

**Required Data Connectors**

ProofpointPOD

### ProofpointPOD - Multiple protected emails to unknown recipient

Detects when multiple protected messages where sent to early not seen recipient.

**Required Data Connectors**

ProofpointPOD

### ProofpointPOD - Suspicious attachment

Detects when email contains suspicious attachment (file type).

**Required Data Connectors**

ProofpointPOD

### ProofpointPOD - Weak ciphers

Detects when weak TLS ciphers are used.

**Required Data Connectors**

ProofpointPOD

## Hunting Queries

### ProofpointPOD - Emails with high score of 'adult' filter classifier value

Proofpoint On demand(POD) Email Security Hunting Query 1

### ProofpointPOD - Emails with high score of 'malware' filter classifier value

Proofpoint On demand(POD) Email Security Hunting Query 2

### ProofpointPOD - Emails with high score of 'phish' filter classifier value

Proofpoint On demand(POD) Email Security Hunting Query 3

### ProofpointPOD - Emails with high score of 'spam' filter classifier value

Proofpoint On demand(POD) Email Security Hunting Query 4

### ProofpointPOD - Emails with high score of 'suspect' filter classifier value

Proofpoint On demand(POD) Email Security Hunting Query 5

### ProofpointPOD - Large size outbound emails

Proofpoint On demand(POD) Email Security Hunting Query 6

### ProofpointPOD - Recipients with high number of discarded or rejected emails

Proofpoint On demand(POD) Email Security Hunting Query 7

### ProofpointPOD - Recipients with large number of corrupted emails

Proofpoint On demand(POD) Email Security Hunting Query 8

### ProofpointPOD - Senders with large number of corrupted messages

Proofpoint On demand(POD) Email Security Hunting Query 9

### ProofpointPOD - Suspicious file types in attachments

Proofpoint On demand(POD) Email Security Hunting Query 10

## Watchlists

## Playbooks

## Parsers

### ProofpointPOD Data Parser

Category: Samples

Function Alias: ProofpointPOD

# Proofpoint TAP Solution

Proofpoint TAP helps detect, mitigate and block advanced threats that target people through email.

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

## Data Connectors

### Proofpoint TAP (using Azure Function)

The [Proofpoint Targeted Attack Protection (TAP)](https://www.proofpoint.com/us/products/advanced-threat-protection/targeted-attack-protection) connector provides the capability to ingest Proofpoint TAP logs and events into Microsoft Sentinel. The connector provides visibility into Message and Click events in Microsoft Sentinel to view dashboards, create custom alerts, and to improve monitoring and investigation capabilities.

## Workbooks

### Proofpoint TAP

Gain extensive insight into Proofpoint Targeted Attack Protection (TAP) by analyzing, collecting and correlating TAP log events.

This workbook provides visibility into message and click events that were permitted, delivered, or blocked

**Required Data Types**

ProofPointTAPMessagesBlocked\_CL

ProofPointTAPMessagesDelivered\_CL

ProofPointTAPClicksPermitted\_CL

ProofPointTAPClicksBlocked\_CL

ProofpointTAP

## Analytic Rules

### Malware attachment delivered

This query identifies a message containing a malware attachment that was delivered.

**Required Data Connectors**

ProofpointTAP

### Malware Link Clicked

This query identifies a user clicking on an email link whose threat category is classified as a malware

**Required Data Connectors**

ProofpointTAP

## Hunting Queries

## Watchlists

## Playbooks

### Get-ProofpointTapEvents

This playbook ingests events from ProofPoint TAP to Log Analytics/MicroSoft Sentinel.

### ProofpointTAP-AddForensicsInfoToIncident

Once a new sentinel incident is created, this playbook gets triggered and performs the following actions:

1. [Gets Forensics](https://help.proofpoint.com/Threat\_Insight\_Dashboard/API\_Documentation/Forensics\_API) by the \*campaignId\*, provided in the alert custom entities.

2. Enriches the incident with Forensics info.

### ProofpointTAP-CheckAccountInVAP

Once a new sentinel incident is created, this playbook gets triggered and performs the following actions:

1. Gets [Very Attacked People](https://help.proofpoint.com/Threat\_Insight\_Dashboard/API\_Documentation/People\_API#.2Fv2.2Fpeople.2Fvap) for the latest 14 days.

2. Enriches the incident with information whether incident's users are in VAP list and changes incident severity.

## Parsers

### ProofpointTAPEvent

Category: Samples

Function Alias: ProofpointTAPEvent

# Pulse Connect Secure

Pulse Connect Secure

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

## Data Connectors

### Pulse Connect Secure

The [Pulse Connect Secure](https://www.pulsesecure.net/products/pulse-connect-secure/) connector allows you to easily connect your Pulse Connect Secure logs with Microsoft Sentinel, to view dashboards, create custom alerts, and improve investigations. Integrating Pulse Connect Secure with Microsoft Sentinel provides more insight into your organization's network and improves your security operation capabilities.

## Workbooks

### Pulse Connect Secure

Gain insight into Pulse Secure VPN by analyzing, collecting and correlating vulnerability data.

This workbook provides visibility into user VPN activities

**Required Data Types**

## Analytic Rules

### PulseConnectSecure - Potential Brute Force Attempts

This query identifies evidence of potential brute force attack by looking at multiple failed attempts to log into the VPN server

**Required Data Connectors**

PulseConnectSecure

PulseConnectSecure - Large Number of Distinct Failed User Logins

This query identifies evidence of failed login attempts from a large number of distinct users on a Pulse Connect Secure VPN server

**Required Data Connectors**

PulseConnectSecure

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### PulseConnectSecure

Category: Samples

Function Alias: PulseConnectSecure

# Qualys VM Knowledgebase

The Qualys Vulnerability Management KB solution for Microsoft Sentinel enables you to ingest Qualys VM KB logs into Microsoft Sentinel.

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

## Data Connectors

### Qualys VM KnowledgeBase (using Azure Function)

The [Qualys Vulnerability Management (VM)](https://www.qualys.com/apps/vulnerability-management/) KnowledgeBase (KB) connector provides the capability to ingest the latest vulnerability data from the Qualys KB into Azure Sentinel.

This data can used to correlate and enrich vulnerability detections found by the [Qualys Vulnerability Management (VM)](https://docs.microsoft.com/azure/sentinel/connect-qualys-vm) data connector.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### QualysKB

Category: Samples

Function Alias: QualysKB

# Qualys VM Solution

The Qualys Vulnerability Management solution for Microsoft Sentinel enables you to ingest host vulnerability detection data into Microsoft Sentinel.

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 2**, Hunting Queries:** 0**, Watchlists:** 0**, Playbooks:** 4, Parsers: 0

## Data Connectors

### Qualys Vulnerability Management (using Azure Function)

The [Qualys Vulnerability Management (VM)](https://www.qualys.com/apps/vulnerability-management/) data connector provides the capability to ingest vulnerability host detection data into Microsoft Sentinel through the Qualys API. The connector provides visibility into host detection data from vulerability scans. This connector provides Microsoft Sentinel the capability to view dashboards, create custom alerts, and improve investigation

## Workbooks

### Qualys Vulnerability Management

Gain insight into Qualys Vulnerability Management by analyzing, collecting and correlating vulnerability data.

This workbook provides visibility into vulnerabilities detected from vulnerability scans

**Required Data Types**

## Analytic Rules

### High Number of Urgent Vulnerabilities Detected

This Creates an incident when a host has a high number of Urgent, severity 5, vulnerabilities detected.

**Required Data Connectors**

QualysVulnerabilityManagement

### New High Severity Vulnerability Detected Across Multiple Hosts

This creates an incident when a new high severity vulnerability is detected across multilple hosts

**Required Data Connectors**

QualysVulnerabilityManagement

## Hunting Queries

## Watchlists

## Playbooks

### QualysVM-GetAssetDetails

When a new sentinel incident is created, this playbook gets triggered and performs the following actions:

1. Get IP Addresses from incident.

2. Get Asset Details for all IP Addresses.

3. Add asset details as a comment to the incident.

### QualysVM-GetAssets-ByCVEID

When a new sentinel incident is created, this playbook gets triggered and performs the following actions:

1. Get CVE IDs from incident.

2. Create a Dynamic Search List with CVE IDs as filter criteria.

3. Generate the Vulnerability Report based on Dynamic Search List.

4. Download the report and store it to a blob storage. This report has details about assets which are vulnerable to CVE.

5. Add the link of report as a comment to the incident.

### QualysVM-GetAssets-ByOpenPort

When a new sentinel incident is created, this playbook gets triggered and performs the following actions:

1. Gets Port from incident. (Only one port)

2. Search the Qualys platform and get the asset count with open port.

3. Search the Qualys platform and get the asset details as well. (Asset details limited to 50 assets, since incident comment has limitaion of 30000 characters.)

4. Combine both the results.

5. Add the info as comment to the incident.

### QualysVM-LaunchVMScan-GenerateReport

When a new sentinel incident is created, this playbook gets triggered and performs the following actions:

1. Get IP Addresses from incident.

2. Scan IP Addresses with Qualys Scanner.

3. Generate the Scan Report.

4. Download the report and store it to a blob storage.

5. Add the link of report as a comment to the incident.

## Parsers

# Recorded Future Intelligence for Microsoft Sentinel

Recorded Future’s unprecedented intelligence reduces security risk by automatically positioning threat intelligence data in your Microsoft Sentinel environment.

**Data Connectors:** 0**, Workbooks:** 2**, Analytic Rules:** 6**, Hunting Queries:** 0**, Watchlists:** 0**, Playbooks:** 7, Parsers: 0

## Data Connectors

## Workbooks

### Recorded Future - C&C DNS Name to DNS Events - Correlation&Threat Hunting

**Required Data Types**

### Recorded Future - Actively Communicating C&C IPs to DNS Events - Correlation&Threat Hunting

Sets the time name for DNS Events and Threat Intelligence Time Range

**Required Data Types**

ThreatIntelligenceIndicator

## Analytic Rules

### Detection of Malware C2 Domains in DNS Events

Identifies a match in DNSEvents from Recorded Future C2 DNS Name Domains Risklist.

**Required Data Connectors**

DNS

### Detection of Malware C2 Domains in Syslog Events

Identifies a match in Syslog from Recorded Future C2 DNS Name Domains Risklist.

**Required Data Connectors**

Syslog

### Detection of Specific Hashes in CommonSecurityLog

Identifies a match in CommonSecurityLog from Recorded Future Hash Observed in Underground Virus Testing Sites RiskList.

**Required Data Connectors**

CEF

### Detection of Malware C2 IPs in Azure Act. Events

Identifies a match in Azure Activity Events from Recorded Future Actively Communicating C&C Server Risklist.

**Required Data Connectors**

AzureActivity

### Detection of Malware C2 IPs in DNS Events

Identifies a match in DnsEvents from Recorded Future Actively Communicating C&C Server Risklist.

**Required Data Connectors**

DNS

### Detection of Malicious URLs in Syslog Events

Identifies a match in Syslog from Recorded Future URLs Recently Reported as malicious by Insikt Group.

**Required Data Connectors**

Syslog

## Hunting Queries

## Watchlists

## Playbooks

### RecordedFuture-ImportToSentinel

This playbook is purposed to listen (via batching mechanism provided by Microsoft Azure) for incoming messages from the IndicatorProcessor Playbooks and create submit the indicators for creation

### RecordedFuture-DOMAIN-C2\_DNS\_Name-TIProcessor

This playbook leverages the Recorded Future API and automatically imports the C&C DNS Name Domain RiskList, as Threat Intelligence Indicators, for detection purposes in Microsoft Sentinel.

This playbook depends on RecordedFuture-ImportToSentinel that need to be installed \*\*manually\*\* before installing current playbook.

### RecordedFuture-HASH-Obs\_in\_Underground-TIProcessor

This playbook leverages the Recorded Future API and automatically imports the Observed in Underground Virus Testing Sites Hash RiskList, as Threat Intelligence Indicators, for detection purposes in Microsoft Sentinel.

This playbook depends on RecordedFuture-ImportToSentinel that need to be installed \*\*manually\*\* before installing current playbook.

### RecordedFuture-IOC\_Enrichment-IP\_Domain\_URL\_Hash

This playbook leverages the Recorded Future API to enrich IP, Domain, Url & Hash indicators, found in Sentinel incidents, with the following context: Risk Score, Risk Rules and Link to Intelligence Card. The enrichment content will be posted as a comment in the Sentinel incident <img alt="Sentinel incident comment" src="https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/Solutions/Recorded%20Future/Playbooks/RecordedFuture-IOC\_Enrichment-IP\_Domain\_URL\_Hash/images/EnrichmentExampleDark.png"/>.

### RecordedFuture-IP-Actively\_Comm\_C2\_Server-TIProcessor

This playbook leverages the Recorded Future API and automatically imports the Actively Communicating C&C Server IP RiskList, as Threat Intelligence Indicators, for detection purposes in Microsoft Sentinel.

This playbook depends on RecordedFuture-ImportToSentinel that need to be installed \*\*manually\*\* before installing current playbook.

### RecordedFuture-URL-Recent\_Rep\_by\_Insikt-TIProcessor

This playbook leverages the Recorded Future API and automatically imports the Recently Reported by Insikt Group URL RiskList, as Threat Intelligence Indicators, for detection purposes in Microsoft Sentinel.

This playbook depends on RecordedFuture-ImportToSentinel that need to be installed \*\*manually\*\* before installing current playbook.

### RecordedFuture-Ukraine-IndicatorProcessor

This playbook leverages the Recorded Future API and automatically imports the Ukraine RiskLists, as Threat Intelligence Indicators, for detection purposes in Microsoft Sentinel.

This playbook depends on RecordedFuture-ImportToSentinel that need to be installed \*\*manually\*\* before installing current playbook.

## Parsers

# Red Canary Connector for Microsoft Sentinel

This application enables integration of Red Canary services with Microsoft Sentinel.

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

## Data Connectors

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# ReversingLabs Content Pack

ReversingLabs has made this rich collection of content available for the best results when enabling the ReversingLabs TitaniumCloud platform with Microsoft Sentinel to leverage the benefits of both solutions.

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

## Data Connectors

## Workbooks

### ReversingLabs-CapabilitiesOverview

The ReversingLabs-CapabilitiesOverview workbook provides a high level look at your threat intelligence capabilities and how they relate to your operations.

**Required Data Types**

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

### ReversingLabs-EnrichFileHash

This playbook will enrich a Sentinel Incident with file hash information from ReversingLabs TitaniumCloud. A comment will be added to the incident with details about the file.

### ReversingLabs-CheckQuota

This playbook will check your ReversingLabs TitaniumCloud API quota and provide usage details. To be used in conjunction with the ReversingLabs-CapabilitiesOverview workbook.

## Parsers

# RiskIQ Illuminate Solution

RiskIQ Illuminate is a complete security intelligence offering, blending attack surface visibility with detailed threat intelligence. With RiskIQ Illuminate, security teams will accelerate their investigations, increase their visibility, respond more effec

**Data Connectors:** 0**, Workbooks:** 0**, Analytic Rules:** 0**, Hunting Queries:** 0**, Watchlists:** 0**, Playbooks:** 27, Parsers: 0

## Data Connectors

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

### RiskIQ-Base

This playbook creates a shared API Connection for all RiskIQ playbooks to leverage. This eases the configuration process for a user during deployment of the RiskIQ solution. In time, this base playbook may be extended to set more functionality. You will need your API credentials (email/secret) when configuring this playbook. Those can be found on your [account settings](https://community.riskiq.com/settings) page. For enterprise customers, it's preferred to use the 'organization' credential pair, not the user. If you have trouble accessing your account or your credentials contact your account representative (support[@]riskiq.com).

### RiskIQ-Automated-Triage-Alert

This playbook uses the RiskIQ PassiveTotal connector to automatically enrich incidents generated by Microsoft Sentinel. Indicators from an incident will be evaluated with RiskIQ reputation data. If any indicators are labeled as 'suspicious', the incident will be tagged as such and its severity will be marked as 'medium'. If any indicators are labeled as 'malicious', the incident will be tagged as such and its severity will be marked as 'high'. Regardless of the reputation state, comments will be added to the incident outlining the reputation details with links to further information if applicable.

### RiskIQ-Automated-Triage-Incident

This playbook uses the RiskIQ PassiveTotal connector to automatically enrich incidents generated by Microsoft Sentinel. Indicators from an incident will be evaluated with RiskIQ reputation data. If any indicators are labeled as 'suspicious', the incident will be tagged as such and its severity will be marked as 'medium'. If any indicators are labeled as 'malicious', the incident will be tagged as such and its severity will be marked as 'high'. Regardless of the reputation state, comments will be added to the incident outlining the reputation details with links to further information if applicable.

### RiskIQ-Data-PassiveDns-Domain

This playbook uses the RiskIQ PassiveTotal connector to automatically enrich incidents generated by Microsoft Sentinel. Passive DNS provides analysts with a means to see DNS data in a historic manner. This history can aid in creating analytical connections, especially if the operational security of a threat actor is poor. Leverage this playbook in order to enrich your incidents with raw passive DNS data related to indicators found within the incident.

### RiskIQ-Data-PassiveDns-Ip

This playbook uses the RiskIQ PassiveTotal connector to automatically enrich incidents generated by Microsoft Sentinel. Passive DNS provides analysts with a means to see DNS data in a historic manner. This history can aid in creating analytical connections, especially if the operational security of a threat actor is poor. Leverage this playbook in order to enrich your incidents with raw passive DNS data related to indicators found within the incident.

### RiskIQ-Data-PassiveDns

This playbook uses the RiskIQ PassiveTotal connector to automatically enrich incidents generated by Microsoft Sentinel. Passive DNS provides analysts with a means to see DNS data in a historic manner. This history can aid in creating analytical connections, especially if the operational security of a threat actor is poor. Leverage this playbook in order to enrich your incidents with raw passive DNS data related to indicators found within the incident.

### RiskIQ-Data-Summary-Domain-alert

This playbook uses the RiskIQ PassiveTotal connector to automatically enrich incidents generated by Microsoft Sentinel. The RiskIQ summary data will provide analysts with an understanding of what RiskIQ knows about a given indicator extracted from the incident in the form of result counts with corresponding data sets. Each data set will be linked, making it easy for an analyst to one-click pivot into a deeper investigation.

### RiskIQ-Data-Summary-Domain-incident

This playbook uses the RiskIQ PassiveTotal connector to automatically enrich incidents generated by Microsoft Sentinel. The RiskIQ summary data will provide analysts with an understanding of what RiskIQ knows about a given indicator extracted from the incident in the form of result counts with corresponding data sets. Each data set will be linked, making it easy for an analyst to one-click pivot into a deeper investigation.

### RiskIQ-Data-Summary-Ip-Alert

This playbook uses the RiskIQ PassiveTotal connector to automatically enrich incidents generated by Microsoft Sentinel. The RiskIQ summary data will provide analysts with an understanding of what RiskIQ knows about a given indicator extracted from the incident in the form of result counts with corresponding data sets. Each data set will be linked, making it easy for an analyst to one-click pivot into a deeper investigation.

### RiskIQ-Data-Summary-Ip-Incident

This playbook uses the RiskIQ PassiveTotal connector to automatically enrich incidents generated by Microsoft Sentinel. The RiskIQ summary data will provide analysts with an understanding of what RiskIQ knows about a given indicator extracted from the incident in the form of result counts with corresponding data sets. Each data set will be linked, making it easy for an analyst to one-click pivot into a deeper investigation.

### RiskIQ Data Summary Alert

This playbook uses the RiskIQ PassiveTotal connector to automatically enrich incidents generated by Microsoft Sentinel. The RiskIQ summary data will provide analysts with an understanding of what RiskIQ knows about a given indicator extracted from the incident in the form of result counts with corresponding data sets. Each data set will be linked, making it easy for an analyst to one-click pivot into a deeper investigation.

### RiskIQ Data Summary Incident

This playbook uses the RiskIQ PassiveTotal connector to automatically enrich incidents generated by Microsoft Sentinel. The RiskIQ summary data will provide analysts with an understanding of what RiskIQ knows about a given indicator extracted from the incident in the form of result counts with corresponding data sets. Each data set will be linked, making it easy for an analyst to one-click pivot into a deeper investigation.

### RiskIQ-Data-Whois-Domain

This playbook uses the RiskIQ PassiveTotal connector to automatically enrich incidents generated by Microsoft Sentinel. WHOIS is akin to a phone book for the Internet; it reveals the owners behind domain registrations and IP address hosting. Analysts can leverage WHOIS, both active and historic, in order to identify analytical leads. This data can sometimes reveal the threat actor behind a given set of infrastructure or provide deeper context as to what else may be related. This playbook will query for WHOIS data from indicators contained within the incident and post the results in the form of a comment.

### RiskIQ-Data-Whois-Ip

This playbook uses the RiskIQ PassiveTotal connector to automatically enrich incidents generated by Microsoft Sentinel. WHOIS is akin to a phone book for the Internet; it reveals the owners behind domain registrations and IP address hosting. Analysts can leverage WHOIS, both active and historic, in order to identify analytical leads. This data can sometimes reveal the threat actor behind a given set of infrastructure or provide deeper context as to what else may be related. This playbook will query for WHOIS data from indicators contained within the incident and post the results in the form of a comment.

### RiskIQ-Data-Whois

This playbook uses the RiskIQ PassiveTotal connector to automatically enrich incidents generated by Microsoft Sentinel. WHOIS is akin to a phone book for the Internet; it reveals the owners behind domain registrations and IP address hosting. Analysts can leverage WHOIS, both active and historic, in order to identify analytical leads. This data can sometimes reveal the threat actor behind a given set of infrastructure or provide deeper context as to what else may be related. This playbook will query for WHOIS data from indicators contained within the incident and post the results in the form of a comment.

### RiskIQ-Intel-Reputation-Domain-Alert

This playbook uses the RiskIQ PassiveTotal connector to automatically enrich incidents generated by Microsoft Sentinel. Reputation information provides analyst with a decision as to whether an indicator is considered benign, suspicious or malicious. Analysts can leverage this playbook in order to enrich indicators found within an incident. Each reputation result is contained within a comment and will include detailed scoring information noting why a given indicator is considered suspicious or malicious with links back to the RiskIQ platform for more information.

### RiskIQ-Intel-Reputation-Domain-Incident

This playbook uses the RiskIQ PassiveTotal connector to automatically enrich incidents generated by Microsoft Sentinel. Reputation information provides analyst with a decision as to whether an indicator is considered benign, suspicious or malicious. Analysts can leverage this playbook in order to enrich indicators found within an incident. Each reputation result is contained within a comment and will include detailed scoring information noting why a given indicator is considered suspicious or malicious with links back to the RiskIQ platform for more information.

### RiskIQ-Intel-Reputation-Ip-Alert

This playbook uses the RiskIQ PassiveTotal connector to automatically enrich incidents generated by Microsoft Sentinel. Reputation information provides analyst with a decision as to whether an indicator is considered benign, suspicious or malicious. Analysts can leverage this playbook in order to enrich indicators found within an incident. Each reputation result is contained within a comment and will include detailed scoring information noting why a given indicator is considered suspicious or malicious with links back to the RiskIQ platform for more information.

### RiskIQ-Intel-Reputation-Ip-Incident

This playbook uses the RiskIQ PassiveTotal connector to automatically enrich incidents generated by Microsoft Sentinel. Reputation information provides analyst with a decision as to whether an indicator is considered benign, suspicious or malicious. Analysts can leverage this playbook in order to enrich indicators found within an incident. Each reputation result is contained within a comment and will include detailed scoring information noting why a given indicator is considered suspicious or malicious with links back to the RiskIQ platform for more information.

### RiskIQ-Intel-Reputation-Alert

This playbook uses the RiskIQ PassiveTotal connector to automatically enrich incidents generated by Microsoft Sentinel. Reputation information provides analyst with a decision as to whether an indicator is considered benign, suspicious or malicious. Analysts can leverage this playbook in order to enrich indicators found within an incident. Each reputation result is contained within a comment and will include detailed scoring information noting why a given indicator is considered suspicious or malicious with links back to the RiskIQ platform for more information.

### RiskIQ-Intel-Reputation-Incident

This playbook uses the RiskIQ PassiveTotal connector to automatically enrich incidents generated by Microsoft Sentinel. Reputation information provides analyst with a decision as to whether an indicator is considered benign, suspicious or malicious. Analysts can leverage this playbook in order to enrich indicators found within an incident. Each reputation result is contained within a comment and will include detailed scoring information noting why a given indicator is considered suspicious or malicious with links back to the RiskIQ platform for more information.

### RiskIQ-Intel-Summary-Domain-Alert

This playbook uses the RiskIQ PassiveTotal connector to automatically enrich incidents generated by Microsoft Sentinel. RiskIQ intelligence provides analyst with deeper context around vulnerabilities, threat actors, their campaigns or other noteworthy context found from analyzing the Internet. Analysts can leverage this playbook to add context to indicators found within incidents. Each comment added to the incident will link to a more detailed intelligence card from RiskIQ.

### RiskIQ-Intel-Summary-Domain-Incident

This playbook uses the RiskIQ PassiveTotal connector to automatically enrich incidents generated by Microsoft Sentinel. RiskIQ intelligence provides analyst with deeper context around vulnerabilities, threat actors, their campaigns or other noteworthy context found from analyzing the Internet. Analysts can leverage this playbook to add context to indicators found within incidents. Each comment added to the incident will link to a more detailed intelligence card from RiskIQ.

### RiskIQ-Intel-Summary-Ip-Alert

This playbook uses the RiskIQ PassiveTotal connector to automatically enrich incidents generated by Microsoft Sentinel. RiskIQ intelligence provides analyst with deeper context around vulnerabilities, threat actors, their campaigns or other noteworthy context found from analyzing the Internet. Analysts can leverage this playbook to add context to indicators found within incidents. Each comment added to the incident will link to a more detailed intelligence card from RiskIQ.

### RiskIQ-Intel-Summary-Ip-Incident

This playbook uses the RiskIQ PassiveTotal connector to automatically enrich incidents generated by Microsoft Sentinel. RiskIQ intelligence provides analyst with deeper context around vulnerabilities, threat actors, their campaigns or other noteworthy context found from analyzing the Internet. Analysts can leverage this playbook to add context to indicators found within incidents. Each comment added to the incident will link to a more detailed intelligence card from RiskIQ.

### RiskIQ-Intel-Summary-Alert

This playbook uses the RiskIQ PassiveTotal connector to automatically enrich incidents generated by Microsoft Sentinel. RiskIQ intelligence provides analyst with deeper context around vulnerabilities, threat actors, their campaigns or other noteworthy context found from analyzing the Internet. Analysts can leverage this playbook to add context to indicators found within incidents. Each comment added to the incident will link to a more detailed intelligence card from RiskIQ.

### RiskIQ-Intel-Summary-Incident

This playbook uses the RiskIQ PassiveTotal connector to automatically enrich incidents generated by Microsoft Sentinel. RiskIQ intelligence provides analyst with deeper context around vulnerabilities, threat actors, their campaigns or other noteworthy context found from analyzing the Internet. Analysts can leverage this playbook to add context to indicators found within incidents. Each comment added to the incident will link to a more detailed intelligence card from RiskIQ.

## Parsers

# RSA SecurID Solution (Preview)

SecurID provides powerful identity and access management capabilities to fully protect organizations in a perimeterless world—without compromising ease and convenience for users.

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

## Data Connectors

### RSA® SecurID (Authentication Manager)

The [RSA® SecurID Authentication Manager](https://www.securid.com/) data connector provides the capability to ingest [RSA® SecurID Authentication Manager events](https://community.rsa.com/t5/rsa-authentication-manager/log-messages/ta-p/571404) into Microsoft Sentinel. Refer to [RSA® SecurID Authentication Manager documentation](https://community.rsa.com/t5/rsa-authentication-manager/getting-started-with-rsa-authentication-manager/ta-p/569582) for more information.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### RSASecurIDAMEvent

Category: Samples

Function Alias: RSASecurIDAMEvent

# Rubrik Integration with Sentinel for Ransomware Protection

Rubrik’s integration enables Microsoft Sentinel users to accelerate and enrich threat investigations with more insights into potential security incidents and speed up remediation with automated responses and malware-free backups.

**Data Connectors:** 1**, Workbooks:** 0**, Analytic Rules:** 0**, Hunting Queries:** 0**, Watchlists:** 0**, Playbooks:** 8, Parsers: 0

## Data Connectors

### Rubrik Security Cloud data connector (using Azure Function)

The Rubrik Security Cloud data connector enables security operations teams to integrate insights from Rubrik’s Data Observability services into Microsoft Sentinel. The insights include identification of anomalous filesystem behavior associated with ransomware and mass deletion, assess the blast radius of a ransomware attack, and sensitive data operators to prioritize and more rapidly investigate potential incidents.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

### Rubrik Anomaly Analysis

This playbook queries Rubrik Security Cloud to enrich the Anomaly event with additional information regarding the Ransomware analysis, results from sensitive data scans, (to aid in incident prioritization), and additional information about the Rubrik cluster.

### Rubrik Anomaly Incident Response

This playbook provides an end to end example of the collection of Ransomware Anomaly information from Rubrik, its enrichment with Data Classification insights (to aid in incident prioritization), and the options to optionally perform various recovery operations. It uses several other playbooks defined in this solution to perform these tasks.

### Rubrik Data Object Discovery

This playbook queries Rubrik Security Cloud to enrich the incoming event with additional information from Rubrik about the object and it’s snapshots that the event refers to.

### Rubrik Fileset Ransomware Discovery

This playbook queries Rubrik Security Cloud to enrich the incoming event with additional information from Rubrik about the fileset object and perform an IOC scan against the fileset.

### Rubrik IOC Scan

This playbook interacts with Rubrik Security Cloud to scan backups for specified IOCs. This playbook is used by other playbooks that leverage this capability.

### Rubrik Poll Async Result

This playbook is used by other playbooks to poll for results from some of the asynchronous API calls that are invoked by other playbooks.

### Rubrik Ransomware Discovery and File Recovery

This playbook interacts with Rubrik Security Cloud to (1) optionally preserve evidence by creating an on-demand snapshot of the object, (2) identify a potential recovery point by scanning backups for specified IOCs, and (3) supporting file level recovery.

### Rubrik Ransomware Discovery and VM Recovery

This playbook interacts with Rubrik Security Cloud to (1) optionally preserve evidence by creating an on-demand snapshot of the object, (2) identify a potential recovery point by scanning backups for specified IOCs, and (3) supporting VM image level recovery.

## Parsers

# SailPoint for Microsoft Sentinel

SailPoint for Microsoft Sentinel solution exists as a listing within Microsoft Sentinel for customers to install.

**Data Connectors:** 1**, Workbooks:** 0**, Analytic Rules:** 6**, Hunting Queries:** 0**, Watchlists:** 0**, Playbooks:** 0, Parsers: 0

## Data Connectors

### SailPoint IdentityNow (using Azure Function)

The [SailPoint](https://www.sailpoint.com/) IdentityNow data connector provides the capability to ingest [SailPoint IdentityNow] search events into Microsoft Sentinel through the REST API. The connector provides customers the ability to extract audit information from their IdentityNow tenant. It is intended to make it even easier to bring IdentityNow user activity and governance events into Microsoft Sentinel to improve insights from your security incident and event monitoring solution.

## Workbooks

## Analytic Rules

### SailPointIdentityNowAlertForTriggers

Create alerts for SailPoint IdentityNow Event Trigger Service.

**Required Data Connectors**

SailPointIdentityNow

### SailPointIdentityNowEventType

Created to detect failed events of particular type from SailPointIDN\_Events.

**Required Data Connectors**

SailPointIdentityNow

### SailPointIdentityNowEventTypeTechnicalName

Created to detect new threat events from the data in SailPointIDN\_Events.

**Required Data Connectors**

SailPointIdentityNow

### SailPointIdentityNowFailedEvents

Detects all events with status failed.

**Required Data Connectors**

SailPointIdentityNow

### SailPointIdentityNowFailedEventsBasedOnTime

Detects failed events based on created time.

**Required Data Connectors**

SailPointIdentityNow

### SailPointIdentityNowUserWithFailedEvent

Detects any failed event for a particular user.

**Required Data Connectors**

SailPointIdentityNow

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Salesforce Service Cloud

The Salesforce Service Cloud solution for Microsoft Sentinel enables you to ingest Service Cloud events into Microsoft Sentinel.

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

## Data Connectors

### Salesforce Service Cloud (using Azure Function)

The Salesforce Service Cloud data connector provides the capability to ingest information about your Salesforce operational events into Microsoft Sentinel through the REST API. The connector provides ability to review events in your org on an accelerated basis, get [event log files](https://developer.salesforce.com/docs/atlas.en-us.api\_rest.meta/api\_rest/event\_log\_file\_hourly\_overview.htm) in hourly increments for recent activity.

## Workbooks

### Salesforce Service Cloud

Sets the time name for analysis.

**Required Data Types**

SalesforceServiceCloud

SalesforceServiceCloud\_CL

## Analytic Rules

### Brute force attack against user credentials

Identifies evidence of brute force activity against a user based on multiple authentication failures

and at least one successful authentication within a given time window. This query limits IPAddresses to 100 and may not potentially cover all IPAddresses

The default failure threshold is 10, success threshold is 1, and the default time window is 20 minutes.

**Required Data Connectors**

SalesforceServiceCloud

### Potential Password Spray Attack

This query searches for failed attempts to log in from more than 15 various users within a 5 minute timeframe from the same source. This is a potential indication of a password spray attack.

**Required Data Connectors**

SalesforceServiceCloud

### User Sign in from different countries

This query searches for successful user logins from different countries within 30min.

**Required Data Connectors**

SalesforceServiceCloud

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### SalesforceServiceCloud

Category: Samples

Function Alias: SalesforceServiceCloud

# Security Threat Essentials

This solution published by Microsoft is based on the continuous evaluation of threat campaigns and provides out-of-the-box security content that helps you to enhance your security posture.

**Data Connectors:** 0**, Workbooks:** 0**, Analytic Rules:** 6**, Hunting Queries:** 2**, Watchlists:** 0**, Playbooks:** 0, Parsers: 0

## Data Connectors

## Workbooks

## Analytic Rules

### Threat Essentials - Mail redirect via ExO transport rule

Identifies when Exchange Online transport rule configured to forward emails.

This could be an adversary mailbox configured to collect mail from multiple user accounts.

**Required Data Connectors**

Office365

### Threat Essentials - Multiple admin membership removals from newly created admin.

This query detects when newly created Global admin removes multiple existing global admins which can be an attempt by adversaries to lock down organization and retain sole access.

Investigate reasoning and intention of multiple membership removal by new Global admins and take necessary actions accordingly.

**Required Data Connectors**

AzureActiveDirectory

### Threat Essentials - NRT User added to Azure Active Directory Privileged Groups

This will alert when a user is added to any of the Privileged Groups.

For further information on AuditLogs please see https://docs.microsoft.com/azure/active-directory/reports-monitoring/reference-audit-activities.

For Administrator role permissions in Azure Active Directory please see https://docs.microsoft.com/azure/active-directory/users-groups-roles/directory-assign-admin-roles

**Required Data Connectors**

AzureActiveDirectory

### Threat Essentials - Mass Cloud resource deletions Time Series Anomaly

This query generates baseline pattern of cloud resource deletions by an user and generated anomaly

when any unusual spike is detected.

These anomalies from unusual or privileged users could be an indication of cloud infrastructure

take-down by an adversary

**Required Data Connectors**

AzureActivity

### Threat Essentials - Time series anomaly for data size transferred to public internet

Identifies anomalous data transfer to public networks. The query leverages built-in KQL anomaly detection algorithms that detects large deviations from a baseline pattern.

A sudden increase in data transferred to unknown public networks is an indication of data exfiltration attempts and should be investigated.

The higher the score, the further it is from the baseline value.

The output is aggregated to provide summary view of unique source IP to destination IP address and port bytes sent traffic observed in the flagged anomaly hour.

The source IP addresses which were sending less than bytessentperhourthreshold have been exluded whose value can be adjusted as needed .

You may have to run queries for individual source IP addresses from SourceIPlist to determine if anything looks suspicious

**Required Data Connectors**

CiscoASA

PaloAltoNetworks

AzureMonitor(VMInsights)

### Threat Essentials - User Assigned Privileged Role

Identifies when a new privileged role is assigned to a user. Any account eligible for a role is now being given privileged access. If the assignment is unexpected or into a role that isn't the responsibility of the account holder, investigate.

Ref : https://docs.microsoft.com/azure/active-directory/fundamentals/security-operations-privileged-accounts#things-to-monitor-1

**Required Data Connectors**

AzureActiveDirectory

## Hunting Queries

### Threat Essentials - Signins from Nord VPN Providers

SecurityThreatEssentialSolution Hunting Query 1

### Threat Essentials - Signins From VPS Providers

SecurityThreatEssentialSolution Hunting Query 2

## Watchlists

## Playbooks

## Parsers

# SecurityBridge App for Microsoft Sentinel

SecurityBridge is the most innovative and complete security solution available for organizations running SAP©.

It is an SAP-certified add-on solution developed on ABAP Netweaver and S/4HANA.

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

## Data Connectors

### SecurityBridge Threat Detection for SAP

SecurityBridge is the first and only holistic, natively integrated security platform, addressing all aspects needed to protect organizations running SAP from internal and external threats against their core business applications. The SecurityBridge platform is an SAP-certified add-on, used by organizations around the globe, and addresses the clients’ need for advanced cybersecurity, real-time monitoring, compliance, code security, and patching to protect against internal and external threats.This Microsoft Sentinel Solution allows you to integrate SecurityBridge Threat Detection events from all your on-premise and cloud based SAP instances into your security monitoring.Use this Microsoft Sentinel Solution to receive normalized and speaking security events, pre-built dashboards and out-of-the-box templates for your SAP security monitoring.

## Workbooks

### SecurityBridge App

Sets the time name for analysis

**Required Data Types**

SecurityBridgeLogs

SecurityBridgeSAP

## Analytic Rules

### SecurityBridge: A critical event occured

This rule alerts if there is any critical event occured in the SAP system

**Required Data Connectors**

SecurityBridge

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### SecurityBridge Threat Detection for SAP Data Parser

Category: Samples

Function Alias: SecurityBridgeLogs

# SecurityScorecard Ratings for Microsoft Sentinel

SecurityScorecard uses non-intrusive and proprietary data collection methods, as well as trusted commercial and open-source threat feeds, to quantitatively evaluate the cybersecurity posture of any organization.

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

## Data Connectors

### SecurityScorecard Cybersecurity Ratings (using Azure Function)

SecurityScorecard is the leader in cybersecurity risk ratings. The [SecurityScorecard](https://www.SecurityScorecard.com/) data connector provides the ability for Sentinel to import SecurityScorecard ratings as logs. SecurityScorecard provides ratings for over 12 million companies and domains using countless data points from across the internet. Maintain full awareness of any company's security posture and be able to receive timely updates when scores change or drop. SecurityScorecard ratings are updated daily based on evidence collected across the web.

### SecurityScorecard Factor (using Azure Function)

SecurityScorecard is the leader in cybersecurity risk ratings. The [SecurityScorecard](https://www.SecurityScorecard.com/) Factors data connector provides the ability for Sentinel to import SecurityScorecard factor ratings as logs. SecurityScorecard provides ratings for over 12 million companies and domains using countless data points from across the internet. Maintain full awareness of any company's security posture and be able to receive timely updates when factor scores change or drop. SecurityScorecard factor ratings are updated daily based on evidence collected across the web.

### SecurityScorecard Issue (using Azure Function)

SecurityScorecard is the leader in cybersecurity risk ratings. The [SecurityScorecard](https://www.SecurityScorecard.com/) Issues data connector provides the ability for Sentinel to import SecurityScorecard issue data as logs. SecurityScorecard provides ratings for over 12 million companies and domains using countless data points from across the internet. Maintain full awareness of any company's security posture and be able to receive timely updates when new cybersecurity issues are discovered.

## Workbooks

### SecurityScorecard

This Workbook provides immediate insight into the data coming from SecurityScorecard’s three Sentinel data connectors: SecurityScorecard Cybersecurity Ratings, SecurityScorecard Cybersecurity Ratings - Factors, and SecurityScorecard Cybersecurity Ratings - Issues.

**Required Data Types**

SecurityScorecardFactor\_CL

SecurityScorecardIssues\_CL

SecurityScorecardRatings\_CL

SecurityScorecardFactorAzureFunctions

SecurityScorecardIssueAzureFunctions

SecurityScorecardRatingsAzureFunctions

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Semperis Directory Services Protector

One platform for peace of mind. Semperis Directory Services Protector(DSP) is a comprehensive platform that continuously monitors Active Directory and Azure Active Directory for indicators of exposure, detects advanced threats, and enables rapid response.

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

## Data Connectors

### Semperis Directory Services Protector

Semperis Directory Services Protector data connector allows for the export of its Windows event logs (i.e. Indicators of Exposure and Indicators of Compromise) to Microsoft Sentinel in real time.

It provides a data parser to manipulate the Windows event logs more easily. The different workbooks ease your Active Directory security monitoring and provide different ways to visualize the data. The analytic templates allow to automate responses regarding different events, exposures, or attacks.

## Workbooks

### Semperis Directory Services Protector

Specify the time range on which to query the data

**Required Data Types**

## Analytic Rules

### Semperis DSP Mimikatz's DCShadow Alert

Mimikatz's DCShadow switch allows a user who has compromised an AD domain, to inject arbitrary changes into AD using a "fake" domain controller. These changes bypass the security event log and can't be spotted using normal AD tools. This rule looks for evidence that a machine has been used in this capacity.

**Required Data Connectors**

SemperisDSP

### Semperis DSP Kerberos krbtgt account with old password

The krbtgt user account is a special (disabled) user account in every Active Directory domain that has a special role in Kerberos function. If this account's password is compromised, Golden Ticket attacks can be performed to get access to any resource in the AD domain. This indicator looks for a krbtgt user account whose password hasn't been changed in the past 180 days. While Microsoft recommends changing the password every year, STIG recommends changing it every 180 days.

**Required Data Connectors**

SemperisDSP

### Semperis DSP Recent sIDHistory changes on AD objects

This indicator detects any recent changes to sIDHistory on AD objects, including changes to non-privileged accounts where privileged SIDs are added.

**Required Data Connectors**

SemperisDSP

### Semperis DSP Well-known privileged SIDs in sIDHistory

This indicator looks for security principals that contain specific SIDs of accounts from built-in privileged groups within their sIDHistory attribute. This would allow those security principals to have the same privileges as those privileged accounts, but in a way that is not obvious to monitor (e.g. through group membership).

**Required Data Connectors**

SemperisDSP

### Semperis DSP Zerologon vulnerability

This indicator looks for security vulnerability to CVE-2020-1472, which was patched by Microsoft in August 2020. Without this patch, an unauthenticated attacker can exploit CVE-2020-1472 to elevate their privileges and get administrative access on the domain.

**Required Data Connectors**

SemperisDSP

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### SemperisDSP Data Parser

Category: Samples

Function Alias: dsp\_parser

# Senserva Offer for Microsoft Sentinel

MSSP focused, Senserva integrates with Microsoft Sentinel to provide automated, detailed insights about user and application security for enriched correlation of high-risk events. Senserva has a low Azure Cost.

**Data Connectors:** 1**, Workbooks:** 3**, Analytic Rules:** 15**, Hunting Queries:** 15**, Watchlists:** 0**, Playbooks:** 0, Parsers: 0

## Data Connectors

### SenservaPro (Preview)

The SenservaPro data connector provides a viewing experience for your SenservaPro scanning logs. View dashboards of your data, use queries to hunt & explore, and create custom alerts.

## Workbooks

### SenservaProAnalytics

Sets the time name for analysis

**Required Data Types**

SenservaPro\_CL

SenservaPro

### SenservaProMultipleWorkspace

Sets the time name for analysis

**Required Data Types**

SenservaPro\_CL

SenservaPro

### SenservaProSecureScoreMultiTenant

Sets the time name for analysis

**Required Data Types**

SenservaPro\_CL

SenservaPro

## Analytic Rules

### Azure secure score admin MFA

This query searches for requiring multi-factor authentication (MFA) for all administrative roles makes it harder

for attackers to access accounts. Administrative roles have higher permissions than typical users.

If any of those accounts are compromised, critical devices and data is open to attack.

**Required Data Connectors**

SenservaPro

### SenservaPro AD Applications Not Using Client Credentials

Searches for logs of AD Applications without Client Credentials (Key or Secret)

**Required Data Connectors**

SenservaPro

### Azure secure score block legacy authentication

This query searches for most compromising sign-in attempts come from legacy authentication.

Older office clients such as Office 2010 do not support modern authentication

and use legacy protocols such as IMAP, SMTP, and POP3.

Legacy authentication does not support multi-factor authentication (MFA).

Even if an MFA policy is configured in your environment, bad actors can

bypass these enforcements through legacy protocols.

**Required Data Connectors**

SenservaPro

### Azure secure score role overlap

This query searches for accounts that have been assigned Global Administrator do not need other roles assigned.

Global Administrators have access to all aspects of Azure

**Required Data Connectors**

SenservaPro

### Azure secure score MFA registration V2

This query searches for multi-factor authentication (MFA) helps protect devices and data

that are accessible to these users. Adding more authentication methods,

such as the Microsoft Authenticator app or a phone number, increases the level of protection

if one factor is compromised.

**Required Data Connectors**

SenservaPro

### Non-admin guest

This query searches for guest is not an admin in Azure

**Required Data Connectors**

SenservaPro

### Service principal not using client credentials

This query searches for an service principal is not using a client certificate or secret is not secure.

It is recommended that you review your needs and use an Authentication method

for sign-in.

**Required Data Connectors**

SenservaPro

### Azure secure score one admin

This query searches for having 1 Global Administrator reduces the surface area of attack for your Azure tenant,

but sets up a single point of failure for the whole tenant. Global Administrators have access

to all aspects of Azure

**Required Data Connectors**

SenservaPro

### Azure secure score PW age policy new

This query searches for having found that when periodic password resets are enforced,

passwords become less secure. Users tend to pick a weaker password and vary it slightly for each reset.

If a user creates a strong password (long, complex and without any pragmatic words present)

it should remain just as strong in the future as it is today. It is Microsoft's official security position

to not expire passwords periodically without a specific reason, and recommends

that cloud-only tenants set the password policy to never expire.

**Required Data Connectors**

SenservaPro

### Stale last password change

This query searches for stale last password change

**Required Data Connectors**

SenservaPro

### Azure Secure Score Self Service Password Reset

This query searches for requires you to setup Azure AD Connect.

Azure AD Connect is free with all Azure Subscriptions

**Required Data Connectors**

SenservaPro

### Azure secure score sign in risk policy

This query searches for an active Azure Premium P2 license is required to use and edit this policy.

You will be required to have setup the MFA Policy before activating this policy

**Required Data Connectors**

SenservaPro

### Third party integrated apps

This query searches for your services by regulating the access of third-party integrated apps.

Only allow access to necessary apps that support robust security controls.

Third-party applications are not created by Microsoft,

so there is a possibility they could be used for malicious purposes like exfiltrating data from your tenancy.

Attackers can maintain persistent access to your services through these integrated apps, without relying on compromised accounts.

**Required Data Connectors**

SenservaPro

### UserAccountDisabled

This query searches for account is Disabled. Does not effect score as its easily enabled.

**Required Data Connectors**

SenservaPro

### Azure secure score user risk policy

This query searches for an active Azure Premium P2 license is required to use and edit this policy.

You will be required to have setup the MFA Policy before activating this policy

**Required Data Connectors**

SenservaPro

## Hunting Queries

### Application not using client credentials

SenservaPro Hunting Query 1

### Azure secure score admin MFA V2

SenservaPro Hunting Query 2

### Azure secure score block legacy authentication

SenservaPro Hunting Query 3

### Azure secure score integrated apps

SenservaPro Hunting Query 4

### Azure secure score MFA registration V2

SenservaPro Hunting Query 5

### Azure secure score one admin

SenservaPro Hunting Query 6

### Azure secure score PW age policy new

SenservaPro Hunting Query 7

### Azure secure score role overlap

SenservaPro Hunting Query 8

Azure Secure Score Self Service Password Reset

SenservaPro Hunting Query 9

### Azure secure score sign in risk policy

SenservaPro Hunting Query 10

### Azure secure score user risk policy

SenservaPro Hunting Query 11

### Non-admin guest

SenservaPro Hunting Query 12

### Service principal not using client credentials

SenservaPro Hunting Query 13

### Stale last password change

SenservaPro Hunting Query 14

### UserAccountDisabled

SenservaPro Hunting Query 15

## Watchlists

## Playbooks

## Parsers

# Sentinel SOAR Essentials

The Sentinel SOAR Essentials solution for Microsoft Sentinel contains Playbooks that can help you get started with basic notification and orchestration scenarios for common use cases.

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

## Data Connectors

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

### Incident Assignment Shifts

This playbook will assign an Incident to an owner based on the Shifts schedule in Microsoft Teams. When an incident is assigned, the incident owner will be notified via email. Incidents are assigned to users based on the following criteria:<br> \*Only users who have started their shifts during the time the Logic App runs will be considered. \*Users who still have at least 1 hours left before going off shift (can be configured in playbook) \*User with the least incidents assigned on the current Shift will be assigned incident first. <br> Refer to [Automate Incident Assignment with Shifts for Teams](https://techcommunity.microsoft.com/t5/azure-sentinel/automate-incident-assignment-with-shifts-for-teams/ba-p/2297549) for more details.

### Notify When Incident Is Closed

This playbook is utilizing new update trigger to notify person/group on Microsoft Teams/Outlook when incident is closed.

### Notify When Incident Is Reopened

This playbook is utilizing new update trigger to notify person/group on Microsoft Teams/Outlook when incident is reopened.

### Notify When Incident Severity Changed

This playbook is utilizing new update trigger to notify person/group on Microsoft Teams/Outlook when incident severity change.

### Notify Incident Owner in Microsoft Teams

This playbook sends a Teams message to the new incident owner.

### Post Message Slack

This playbook will post a message in a Slack channel when an alert is created in Microsoft Sentinel

### Post Message Teams

This playbook will post a message in a Microsoft Teams channel when an Alert is created in Microsoft Sentinel.

### Post Message Teams

This playbook will post a message in a Microsoft Teams channel when an Incident is created in Microsoft Sentinel.

### Post Message Slack

This playbook will post a message in a Slack channel when an Incident is created in Microsoft Sentinel

### Relate alerts to incident by IP

This playbook looks for other alerts with the same IP as the triggered incident. When such an alert is found, this playbook will add the alert to the incident (only if it isn't related to another incident).When a new incident is created: 1. Get the first IP entity of the incident 2. Make a list of alerts with the IP fetched in the previous step. Please note we exclude all the alerts with the same IP already related to the triggered incident. 3. For each alert in the list: 3.1 Get the incident of the alert 3.2 If the last step fails (meaning the current alert is not related to another incident): add this alert to the incident. 4. Add a comment to the incident specifying all the alerts added to it by listing their "SystemAlertId" field.

### Send basic email

This playbook will be sending email with basic incidents details (Incident title, severity, tactics, link,…) when incident is created in Microsoft Sentinel.

### Send email with formatted incident report

This playbook will be sending email with formated incidents report (Incident title, severity, tactics, link,…) when incident is created in Microsoft Sentinel. Email notification is made in HTML.

## Parsers

# SentinelOne

The SentinelOne solution provides ability to bring SentinelOne events to your Microsoft Sentinel Workspace to inform and to examine potential security risks, analyze your team's use of collaboration, diagnose configuration problems and more.

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 11**, Hunting Queries:** 10**, Watchlists:** 0**, Playbooks:** 0, Parsers: 1

## Data Connectors

### SentinelOne (using Azure Function)

The [SentinelOne](https://www.sentinelone.com/) data connector provides the capability to ingest common SentinelOne server objects such as Threats, Agents, Applications, Activities, Policies, Groups, and more events into Microsoft Sentinel through the REST API. Refer to API documentation: `https://<SOneInstanceDomain>.sentinelone.net/api-doc/overview` for more information. The connector provides ability to get events which helps to examine potential security risks, analyze your team's use of collaboration, diagnose configuration problems and more.

## Workbooks

### SentinelOneWorkbook

Sets the time name for analysis.

**Required Data Types**

SentinelOne\_CL

SentinelOne

## Analytic Rules

### Sentinel One - Admin login from new location

Detects admin user login from new location (IP address).

**Required Data Connectors**

SentinelOne

### Sentinel One - Agent uninstalled from multiple hosts

Detects when agent was uninstalled from multiple hosts.

**Required Data Connectors**

SentinelOne

### Sentinel One - Alert from custom rule

Detects when alert from custom rule received.

**Required Data Connectors**

SentinelOne

### Sentinel One - Blacklist hash deleted

Detects when blacklist hash was deleted.

**Required Data Connectors**

SentinelOne

### Sentinel One - Exclusion added

Detects when new exclusion added.

**Required Data Connectors**

SentinelOne

### Sentinel One - Multiple alerts on host

Detects when multiple alerts received from same host.

**Required Data Connectors**

SentinelOne

### Sentinel One - New admin created

Detects when new admin user is created.

**Required Data Connectors**

SentinelOne

### Sentinel One - Rule deleted

Detects when a rule was deleted.

**Required Data Connectors**

SentinelOne

### Sentinel One - Rule disabled

Detects when a rule was disabled.

**Required Data Connectors**

SentinelOne

### Sentinel One - Same custom rule triggered on different hosts

Detects when same custom rule was triggered on different hosts.

**Required Data Connectors**

SentinelOne

### Sentinel One - User viewed agent's passphrase

Detects when a user viewed agent's passphrase.

**Required Data Connectors**

SentinelOne

## Hunting Queries

### Sentinel One - Agent not updated

SentinelOne Hunting Query 1

### Sentinel One - Agent status

SentinelOne Hunting Query 2

### Sentinel One - Alert triggers (files, processes, strings)

SentinelOne Hunting Query 3

### Sentinel One - Hosts not scanned recently

SentinelOne Hunting Query 4

### Sentinel One - New rules

SentinelOne Hunting Query 5

### Sentinel One - Deleted rules

SentinelOne Hunting Query 6

### Sentinel One - Scanned hosts

SentinelOne Hunting Query 7

### Sentinel One - Sources by alert count

SentinelOne Hunting Query 8

### Sentinel One - Uninstalled agents

SentinelOne Hunting Query 9

### Sentinel One - Users by alert count

SentinelOne Hunting Query 10

## Watchlists

## Playbooks

## Parsers

### SentinelOne

Category: Samples

Function Alias: SentinelOne

# ServiceNow

Unidirectional incident are sync from Microsoft Sentinel and Bi-directional incident sync using app hosted on ServiceNow store.

**Data Connectors:** 0**, Workbooks:** 0**, Analytic Rules:** 0**, Hunting Queries:** 0**, Watchlists:** 0**, Playbooks:** 3, Parsers: 0

## Data Connectors

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

### Create SNOW record - Alert trigger

This playbook will open a Service Now incident when a new incident is opened in Microsoft Sentinel.

### Create SNOW record - Incident trigger

This playbook will open a Service Now incident when a new incident is opened in Microsoft Sentinel.

### Create And Update Service Now Record

This playbook will create or update incident in SNOW. When incident is created, playbook will run and create incident in SNOW. When incident is updated, playbook will run and add update to comment section. When incident is closed, playbook will run and close incident in SNOW.

## Parsers

# Shadowbyte's Threat Intelligence for Sentinel

Shadowbyte's ARIA platform provides data breach and data leak detection, and account takeover protection. Shadowbyte is designed to detect breaches before they happen.

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

## Data Connectors

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# SIGNL4 – Mobile Alerting for Microsoft Sentinel

SIGNL4 offers critical alerting, incident response and service dispatching for operating critical infrastructure.

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

## Data Connectors

### Derdack SIGNL4

When critical systems fail or security incidents happen, SIGNL4 bridges the ‘last mile’ to your staff, engineers, IT admins and workers in the field. It adds real-time mobile alerting to your services, systems, and processes in no time. SIGNL4 notifies through persistent mobile push, SMS text and voice calls with acknowledgement, tracking and escalation. Integrated duty and shift scheduling ensure the right people are alerted at the right time.

[Learn more >](https://www.signl4.com)

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

### SIGNL4 Alerting and Response

This playbook will be sending alerts with basic incidents to SIGNL4 teams when an incident is created in Microsoft Sentinel.

## Parsers

# Slack Audit Solution

The connector provides ability to get events which helps to examine potential security risks, analyze your team's use of collaboration, diagnose configuration problems and more.

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 9**, Hunting Queries:** 10**, Watchlists:** 0**, Playbooks:** 0, Parsers: 1

## Data Connectors

### Slack Audit (using Azure Function)

The [Slack](https://slack.com) Audit data connector provides the capability to ingest [Slack Audit Records](https://api.slack.com/admins/audit-logs) events into Microsoft Sentinel through the REST API. Refer to [API documentation](https://api.slack.com/admins/audit-logs#the\_audit\_event) for more information. The connector provides ability to get events which helps to examine potential security risks, analyze your team's use of collaboration, diagnose configuration problems and more.

## Workbooks

### SlackAudit

Sets the time name for analysis

**Required Data Types**

SlackAudit\_CL

SlackAuditAPI

## Analytic Rules

### SlackAudit - Empty User Agent

This query shows connections to the Slack Workspace with empty User Agent.

**Required Data Connectors**

SlackAuditAPI

### SlackAudit - Multiple archived files uploaded in short period of time

This query helps to detect when a user uploads multiple archived files in short period of time.

**Required Data Connectors**

SlackAuditAPI

### SlackAudit - Multiple failed logins for user

This query helps to detect bruteforce of a user account.

**Required Data Connectors**

SlackAuditAPI

### SlackAudit - Public link created for file which can contain sensitive information.

Detects public links for files which potentialy may contain sensitive data such as passwords, authentication tokens, secret keys.

**Required Data Connectors**

SlackAuditAPI

### SlackAudit - Suspicious file downloaded.

Detects potentialy suspicious downloads.

**Required Data Connectors**

SlackAuditAPI

### SlackAudit - Unknown User Agent

This query helps to detect who trying to connect to the Slack Workspace with unknown User Agent.

**Required Data Connectors**

SlackAuditAPI

### SlackAudit - User role changed to admin or owner

This query helps to detect a change in the users role to admin or owner.

**Required Data Connectors**

SlackAuditAPI

### SlackAudit - User email linked to account changed.

Detects when user email linked to account changes.

**Required Data Connectors**

SlackAuditAPI

### SlackAudit - User login after deactivated.

Detects when user email linked to account changes.

**Required Data Connectors**

SlackAuditAPI

## Hunting Queries

### SlackAudit - Applications installed

SlackAudit Hunting Query 1

### SlackAudit - Deactivated users

SlackAudit Hunting Query 2

### SlackAudit - Downloaded files stats

SlackAudit Hunting Query 3

### SlackAudit - Failed logins with unknown username

SlackAudit Hunting Query 4

### SlackAudit - New User created

SlackAudit Hunting Query 5

### SlackAudit - Suspicious files downloaded

SlackAudit Hunting Query 6

### SlackAudit - Uploaded files stats

SlackAudit Hunting Query 7

### SlackAudit - User logins by IP

SlackAudit Hunting Query 8

### SlackAudit - User Permission Changed

SlackAudit Hunting Query 9

### SlackAudit - Users joined channels without invites

SlackAudit Hunting Query 10

## Watchlists

## Playbooks

## Parsers

### SlackAudit Data Parser

Category: Samples

Function Alias: SlackAudit

# SlashNext URL Threat Analysis and IR for Microsoft Sentinel

SlashNext for Microsoft Sentinel delivers instant value by automatically identifying malicious URLs, BEC phishing, scams, attachment exploits in email, mobile and web messaging apps with precision 99.9% detection and low false positives.

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

## Data Connectors

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Snowflake

The Snowflake solution provides the capability to ingest Snowflake login logs and query logs into Microsoft Sentinel using the Snowflake Python Connector. Refer to Snowflake documentation for more information.

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 10**, Hunting Queries:** 10**, Watchlists:** 0**, Playbooks:** 0, Parsers: 1

## Data Connectors

### Snowflake (using Azure Function)

The Snowflake data connector provides the capability to ingest Snowflake [login logs](https://docs.snowflake.com/en/sql-reference/account-usage/login\_history.html) and [query logs](https://docs.snowflake.com/en/sql-reference/account-usage/query\_history.html) into Microsoft Sentinel using the Snowflake Python Connector. Refer to [Snowflake documentation](https://docs.snowflake.com/en/user-guide/python-connector.html) for more information.

## Workbooks

### Snowflake

Sets the time name for analysis

**Required Data Types**

Snowflake\_CL

SnowflakeDataConnector

## Analytic Rules

### Snowflake - Possible discovery activity

Detects possible discovery activity.

**Required Data Connectors**

Snowflake

### Snowflake - Abnormal query process time

Detects query with abnormal proccess time.

**Required Data Connectors**

Snowflake

### Snowflake - Multiple failed queries

Detects multiple failed queries in short timeframe.

**Required Data Connectors**

Snowflake

### Snowflake - Multiple login failures by user

Detects multiple login failures by user.

**Required Data Connectors**

Snowflake

### Snowflake - Multiple login failures from single IP

Detects Mmltiple login failures from single IP.

**Required Data Connectors**

Snowflake

### Snowflake - Possible data destraction

Detects possible data destruction.

**Required Data Connectors**

Snowflake

### Snowflake - Possible privileges discovery activity

Detects possible privileges discovery activity.

**Required Data Connectors**

Snowflake

### Snowflake - Query on sensitive or restricted table

Detects query on sensitive or restricted table.

**Required Data Connectors**

Snowflake

### Snowflake - Unusual query

Detects unusual query.

**Required Data Connectors**

Snowflake

### Snowflake - User granted admin privileges

Detects when user asigned admin privileges.

**Required Data Connectors**

Snowflake

## Hunting Queries

### Snowflake - Privileged users' source IP addresses

Snowflake Hunting Query 1

### Snowflake - Deleted databases

Snowflake Hunting Query 2

### Snowflake - Deleted tables

Snowflake Hunting Query 3

### Snowflake - Rarely used account

Snowflake Hunting Query 4

### Snowflake - Failed logins

Snowflake Hunting Query 5

### Snowflake - Credit consuming queries

Snowflake Hunting Query 6

### Snowflake - Time consuming queries

Snowflake Hunting Query 7

### Snowflake - Unknown query type

Snowflake Hunting Query 8

### Snowflake - Rarely used privileged users

Snowflake Hunting Query 9

### Snowflake - Users' source IP addresses

Snowflake Hunting Query 10

## Watchlists

## Playbooks

## Parsers

### Snowflake Data Parser

Category: Samples

Function Alias: Snowflake

# SOC Handbook solution for Microsoft Sentinel

The SOC Handbook Microsoft Sentinel solution has a collection of resources that enable and empower SOC Analysts to get better visibility and understanding of point-in-time Security posture of organizational resources.

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

## Data Connectors

## Workbooks

### Analytics Efficiency

Gain insights into the efficacy of your analytics rules. In this workbook you can analyze and monitor the analytics rules found in your workspace to achieve better performance by your SOC.

**Required Data Types**

SecurityAlert

SecurityIncident

### AnomaliesVisulization

A workbook that provides contextual information to a user for better insight on Anomalies and their impact. The workbook will help with investigation of anomalies as well as identify patterns that can lead to a threat.

**Required Data Types**

Anomalies

### AnomalyData

A workbook providing details, related Incident, and related Hunting Workbook for a specific Anomaly.

**Required Data Types**

Anomalies

### Microsoft Sentinel Cost

This workbook provides an estimated cost across the main billed items in Microsoft Sentinel: ingestion, retention and automation. It also provides insight about the possible impact of the Microsoft 365 E5 offer.

**Required Data Types**

### Security Alerts

Security Alerts dashboard for alerts in your Microsoft Sentinel environment.

**Required Data Types**

SecurityAlert

### Incident overview

The Incident Overview workbook is designed to assist in triaging and investigation by providing in-depth information about the incident, including:

\* General information

\* Entity data

\* Triage time (time between incident creation and first response)

\* Mitigation time (time between incident creation and closing)

\* Comments

Customize this workbook by saving and editing it.

You can reach this workbook template from the incidents panel as well. Once you have customized it, the link from the incident panel will open the customized workbook instead of the template.

**Required Data Types**

SecurityAlert

SecurityIncident

### IntSights IOC Workbook

**Required Data Types**

ThreatIntelligenceIndicator

SecurityAlert

ThreatIntelligenceTaxii

### Investigation Insights

Help analysts gain insight into incident, bookmark and entity data through the Investigation Insights Workbook. This workbook provides common queries and detailed visualizations to help an analyst investigate suspicious activities quickly with an easy to use interface. Analysts can start their investigation from a Sentinel incident, bookmark, or by simply entering the entity data into the workbook manually.

**Required Data Types**

AuditLogs

AzureActivity

CommonSecurityLog

OfficeActivity

SecurityEvent

SigninLogs

ThreatIntelligenceIndicator

AzureActivity

SecurityEvents

Office365

AzureActiveDirectory

ThreatIntelligence

ThreatIntelligenceTaxii

WindowsSecurityEvents

### MITRE ATT&CK Workbook

Workbook to showcase MITRE ATT&CK Coverage for Microsoft Sentinel

**Required Data Types**

### Security Operations Efficiency

Security operations center managers can view overall efficiency metrics and measures regarding the performance of their team. They can find operations by multiple indicators over time including severity, MITRE tactics, mean time to triage, mean time to resolve and more. The SOC manager can develop a picture of the performance in both general and specific areas over time and use it to improve efficiency.

**Required Data Types**

SecurityAlert

SecurityIncident

### Security Status

This workbook gives an overview of Security Settings for VMs and Azure Arc.

**Required Data Types**

CommonSecurityLog

SecurityEvent

Syslog

### Sentinel Central

Use this report to view Incident (and Alert data) across many workspaces, this works with Azure Lighthouse and across any subscription you have access to.

**Required Data Types**

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# SOC Process Framework(Preview)

The Get-SOCActions Playbook with SocRA Watchlist gives SOCs the ability to onboard SOC Actions for their Analysts to follow that snap to the SOC Process Framework Workbook.

**Data Connectors:** 0**, Workbooks:** 7**, Analytic Rules:** 0**, Hunting Queries:** 0**, Watchlists:** 12**, Playbooks:** 1, Parsers: 0

## Data Connectors

## Workbooks

### SOC Process Framework

Built by Microsoft's Sentinel GBB's - This workbook contains years of SOC Best Practices and is intended to help SOCs mature and leverage industry standards in Operationalizing their SOC in using Microsoft Sentinel. It contains Processes and Procedures every SOC should consider and builds a high level of operational excellence.

**Required Data Types**

### SOC Large Staff

Built by Microsoft's Sentinel GBB's - This workbook contains years of SOC Best Practices and is intended to help SOCs mature and leverage industry standards in Operationalizing their SOC in using Microsoft Sentinel. It contains Processes and Procedures every SOC should consider and builds a high level of operational excellence.

**Required Data Types**

### SOC Medium Staff

Built by Microsoft's Sentinel GBB's - This workbook contains years of SOC Best Practices and is intended to help SOCs mature and leverage industry standards in Operationalizing their SOC in using Microsoft Sentinel. It contains Processes and Procedures every SOC should consider and builds a high level of operational excellence.

**Required Data Types**

### SOC Small Staff

Built by Microsoft's Sentinel GBB's - This workbook contains years of SOC Best Practices and is intended to help SOCs mature and leverage industry standards in Operationalizing their SOC in using Microsoft Sentinel. It contains Processes and Procedures every SOC should consider and builds a high level of operational excellence.

**Required Data Types**

### SOC Part Time Staff

Built by Microsoft's Sentinel GBB's - This workbook contains years of SOC Best Practices and is intended to help SOCs mature and leverage industry standards in Operationalizing their SOC in using Microsoft Sentinel. It contains Processes and Procedures every SOC should consider and builds a high level of operational excellence.

**Required Data Types**

### SOC IR Planning

Built by Microsoft's Sentinel GBB's - This workbook contains years of SOC Best Practices and is intended to help SOCs mature and leverage industry standards in Operationalizing their SOC in using Microsoft Sentinel. It contains Processes and Procedures every SOC should consider and builds a high level of operational excellence.

**Required Data Types**

### Update SOC Maturity Score

Built by Microsoft's Sentinel GBB's - This workbook contains years of SOC Best Practices and is intended to help SOCs mature and leverage industry standards in Operationalizing their SOC in using Microsoft Sentinel. It contains Processes and Procedures every SOC should consider and builds a high level of operational excellence.

**Required Data Types**

## Analytic Rules

## Hunting Queries

## Watchlists

### SOC Contacts

SOC Contacts within Org.

### SOC Departmental

SOC Departments within Org.

### SOC Email Distribution

SOC Email Distribution within Org.

### SOC External Contacts

SOC External Contacts within Org.

### SOC General IT

SOC General IT within Org.

### SOC Incident Response Planning

Use this table as a checklist to prepare your Security Operations Center (SOC) to respond to cybersecurity incidents.

### SOC Internal Contacts

SOC Internal Contacts within Org.

### SOC Maturity Assessment (CMMI)

The SOC CMMI model was created by evaluating scientific and non-scientific literature to determine characteristics and features of SOCs, such as specific technologies or processes. These characteristics and features were then aggregated into respective domains. Then, a survey was held among SOCs to determine the existence of identified theoretical elements in practical situations. The outcome of that survey, combined with the initial literature review and augmented with literature review on maturity models was used to create the SOC CMMI model.

### SOC Pager Contacts

SOC Pager Contacts within Org.

### SOC Recommended Actions

SOC Recommended Actions per Alert for Analyst's to action on and Follow.

### SOC Use Cases

A list of onboarded Analytic Rules Configured and Onboarded.

### SOC Workstations

SOC process framework Workstations list.

## Playbooks

### Get SOC Actions

This playbook uses the SOCRA Watchlist to automatically enrich incidents generated by Microsoft Sentinel with Actions to review and take. Actions will be evaluated per Customer Organization and edited/modified per their standards of conduct

## Parsers

# SonicWall Network Security for Microsoft Sentinel

SonicWall Firewall brings industry leading capabilities such as application intelligence and control, real-time monitoring, IPS, TLS/SSL decryption and inspection, advanced threat protection, VPN and network segmentation. SonicWall also includes the patent

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

## Data Connectors

### SonicWall Firewall

Common Event Format (CEF) is an industry standard format on top of Syslog messages, used by SonicWall to allow event interoperability among different platforms. By connecting your CEF logs to Microsoft Sentinel, you can take advantage of search & correlation, alerting, and threat intelligence enrichment for each log.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Sonrai Security for Microsoft Sentinel

Sonrai Dig brings context-rich insights into Microsoft Sentinel.

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 9**, Hunting Queries:** 0**, Watchlists:** 0**, Playbooks:** 0, Parsers: 0

## Data Connectors

### Sonrai Data Connector

Use this data connector to integrate with Sonrai Security and get Sonrai tickets sent directly to Microsoft Sentinel.

## Workbooks

### Sonrai

Sets the time name for analysis

**Required Data Types**

Sonrai\_Tickets\_CL

SonraiDataConnector

## Analytic Rules

### New Sonrai Ticket

Checks for new Sonrai tickets.

It uses the action type to check if a ticket has been created

**Required Data Connectors**

SonraiDataConnector

### Sonrai Ticket Assigned

Checks if Sonrai tickets have been assigned.

It uses the action type to check if a ticket has been assigned

**Required Data Connectors**

SonraiDataConnector

### Sonrai Ticket Closed

Checks if Sonrai tickets have been closed.

It uses the action type to check if a ticket has been closed

**Required Data Connectors**

SonraiDataConnector

### Sonrai Ticket Escalation Executed

Checks if Sonrai tickets have had a comment added.

It uses the action type to check if a ticket has had a comment added

**Required Data Connectors**

SonraiDataConnector

### Sonrai Ticket Escalation Executed

Checks if Sonrai tickets have had an escalation executed.

It uses the action type to check if a ticket has had an escalation executed

**Required Data Connectors**

SonraiDataConnector

### Sonrai Ticket Reopened

Checks if Sonrai tickets have been reopened.

It uses the action type to check if a ticket has been reopened

**Required Data Connectors**

SonraiDataConnector

### Sonrai Ticket Risk Accepted

Checks if Sonrai tickets have had their risk accepted.

It uses the action type to check if a ticket has had it's risk accepted

**Required Data Connectors**

SonraiDataConnector

### Sonrai Ticket Snoozed

Checks if Sonrai tickets have been snoozed.

It uses the action type to check if a ticket has been snoozed

**Required Data Connectors**

SonraiDataConnector

### Sonrai Ticket Updated

Checks if Sonrai tickets have been updated.

It uses the action type to check if a ticket has been updated

**Required Data Connectors**

SonraiDataConnector

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Sophos Cloud Optix

Continually monitor public cloud infrastructure for unsanctioned activity, vulnerabilities, and more

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

## Data Connectors

### Sophos Cloud Optix

The [Sophos Cloud Optix](https://www.sophos.com/products/cloud-optix.aspx) connector allows you to easily connect your Sophos Cloud Optix logs with Azure Sentinel, to view dashboards, create custom alerts, and improve investigation. This gives you more insight into your organization's cloud security and compliance posture and improves your cloud security operation capabilities.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

Parsers

# Sophos Endpoint Protection Solution

Sophos delivers a broad portfolio of advanced products and services to secure users, networks and endpoints against ransomware, malware, exploits, phishing and the wide range of other cyberattacks.

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

## Data Connectors

### Sophos Endpoint Protection (using Azure Function)

The [Sophos Endpoint Protection](https://www.sophos.com/en-us/products/endpoint-antivirus.aspx) data connector provides the capability to ingest [Sophos events](https://docs.sophos.com/central/Customer/help/en-us/central/Customer/common/concepts/Events.html) into Microsoft Sentinel. Refer to [Sophos Central Admin documentation](https://docs.sophos.com/central/Customer/help/en-us/central/Customer/concepts/Logs.html) for more information.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### Sophos Endpoint Protection Data Parser

Category: Samples

Function Alias: SophosEPEvent

# Sophos XG Firewall Solution

Sophos XG Firewall Solution for Azure Sentinel provides all-in-one protection for enterprises through visibility, synchronized security, and automated response. This includes exposing hidden risks, stopping unknown threats, and isolating infected systems.

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

## Data Connectors

### Sophos XG Firewall

The [Sophos XG Firewall](https://www.sophos.com/products/next-gen-firewall.aspx) allows you to easily connect your Sophos XG Firewall logs with Microsoft Sentinel, to view dashboards, create custom alerts, and improve investigations. Integrating Sophos XG Firewall with Microsoft Sentinel provides more visibility into your organization's firewall traffic and will enhance security monitoring capabilities.

## Workbooks

### Sophos XG Firewall

Gain insight into Sophos XG Firewall by analyzing, collecting and correlating firewall data.

This workbook provides visibility into network traffic

**Required Data Types**

Syslog

SophosXGFirewall

## Analytic Rules

### Excessive Amount of Denied Connections from a Single Source

This creates an incident in the event that a single source IP address generates a excessive amount of denied connections.

**Required Data Connectors**

SophosXGFirewall

### Port Scan Detected

This alert creates an incident when a source IP addresses attempt to communicate with a large amount of distinct ports within a short period.

**Required Data Connectors**

SophosXGFirewall

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### SophosXGFirewall

Category: Samples

Function Alias: SophosXGFirewall

# Squadra Technologies secRMM

Squadra Technologies security Removable Media Manager (secRMM) software is Windows security software that audits and controls removable media (mobile devices, USB flash drives, external hard drives, CD/DVD/Blu-Ray) on physical and virtual computers.

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

## Data Connectors

### Squadra Technologies secRMM

Use the Squadra Technologies secRMM Data Connector to push USB removable storage security event data into Azure Sentinel Log Analytics.

## Workbooks

### Squadra Technologies SecRMM - USB removable storage security

This workbook gives an overview of security data for removable storage activity such as USB thumb drives and USB connected mobile devices.

**Required Data Types**

secRMM\_CL

SquadraTechnologiesSecRmm

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# SquidProxy

The Squid Proxy solution for Microsoft Sentinel enables you to ingest Squid Proxy logs into Microsoft Sentinel.

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

## Data Connectors

### Squid Proxy

The [Squid Proxy](http://www.squid-cache.org/) connector allows you to easily connect your Squid Proxy logs with Azure Sentinel. This gives you more insight into your organization's network proxy traffic and improves your security operation capabilities.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### SquidProxy

Category: Samples

Function Alias: SquidProxy

# Symantec Endpoint Protection Solution

Symantec Endpoint Protection is a security software suite that consists of anti-malware, intrusion prevention and firewall features for server and desktop computers

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

## Data Connectors

### Symantec Endpoint Protection

The [Broadcom Symantec Endpoint Protection (SEP)](https://www.broadcom.com/products/cyber-security/endpoint/end-user/enterprise) connector allows you to easily connect your SEP logs with Microsoft Sentinel. This gives you more insight into your organization's network and improves your security operation capabilities.

## Workbooks

### Symantec Endpoint Protection

Sets the time name for analysis

**Required Data Types**

SymantecEndpointProtection

SymantecEndpointProtection

## Analytic Rules

### Excessive Blocked Traffic Events Generated by User

Creates an incident when a Symantec Endpoint Proection agent detects excessive amounts of blocked traffic generated by a single user.

**Required Data Connectors**

SymantecEndpointProtection

### Malware Detected

Creates an incident when a Symantec Endpoint Proection agent detects malware and the malware was not cleaned.

**Required Data Connectors**

SymantecEndpointProtection

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### SymantecEndpointProtection

Category: Samples

Function Alias: SymantecEndpointProtection

# Symantec Integrated Cyber Defense

The Symantec Integrated Cyber Defense Exchange (ICDx) solution allows you to easily connect your Symantec security solutions logs with Microsoft Sentinel, to view dashboards, create custom alerts, and improve investigation.

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

## Data Connectors

### Symantec Integrated Cyber Defense Exchange

Symantec ICDx connector allows you to easily connect your Symantec security solutions logs with Microsoft Sentinel, to view dashboards, create custom alerts, and improve investigation. This gives you more insight into your organization’s network and improves your security operation capabilities.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Symantec ProxySG Solution

Symantec Secure Web Gateway solutions draw on a unique proxy server architecture that allows organizations to effectively monitor, control, and secure traffic to ensure a safe web and cloud experience.

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

## Data Connectors

### Symantec ProxySG

The [Symantec ProxySG](https://www.broadcom.com/products/cyber-security/network/gateway/proxy-sg-and-advanced-secure-gateway) allows you to easily connect your Symantec ProxySG logs with Microsoft Sentinel, to view dashboards, create custom alerts, and improve investigations. Integrating Symantec ProxySG with Microsoft Sentinel provides more visibility into your organization's network proxy traffic and will enhance security monitoring capabilities.

## Workbooks

### Symantec ProxySG

Gain insight into Symantec ProxySG by analyzing, collecting and correlating proxy data.

This workbook provides visibility into ProxySG Access logs

**Required Data Types**

## Analytic Rules

### Excessive Denied Proxy Traffic

This alert creates an incident when a client generates an excessive amounts of denied proxy traffic.

**Required Data Connectors**

SymantecProxySG

### User Accessed Suspicious URL Categories

Creates an incident in the event the requested URL accessed by the user has been identified as Suspicious, Phishing, or Hacking.

**Required Data Connectors**

SymantecProxySG

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### SymantecProxySG

Category: Samples

Function Alias: SymantecProxySG

# Symantec VIP

The Symantec VIP solution for Microsoft Sentinel enables you to ingest Symantec VIP's authentication logs into Microsoft Sentinel.

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

## Data Connectors

### Symantec VIP

The [Symantec VIP](https://vip.symantec.com/) connector allows you to easily connect your Symantec VIP logs with Microsoft Sentinel, to view dashboards, create custom alerts, and improve investigation. This gives you more insight into your organization's network and improves your security operation capabilities.

## Workbooks

### Symantec VIP

Gain insight into Symantec VIP by analyzing, collecting and correlating strong authentication data.

This workbook provides visibility into user authentications

**Required Data Types**

Syslog

SymantecVIP

## Analytic Rules

### ClientDeniedAccess

Creates an incident in the event a Client has an excessive amounts of denied access requests.

**Required Data Connectors**

SymantecVIP

### Excessive Failed Authentication from Invalid Inputs

Creates an incident in the event that a user generates an excessive amount of failed authentications due to invalid inputs, indications of a potential brute force.

**Required Data Connectors**

SymantecVIP

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### SymantecVIP

Category: Samples

Function Alias: SymantecVIP

# Synack Integration for Microsoft Sentinel

Synack's security testing platform synchronizes exploitable vulnerability data into Microsoft Sentinel from the Synack Client Portal, streamlining the vulnerability management process.

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

## Data Connectors

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Syslog solution for Sentinel

The Syslog solution allows you to ingest events from applications or appliances that generate and can forward logs in the Syslog format to a Syslog Forwarder

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 5**, Hunting Queries:** 9**, Watchlists:** 0**, Playbooks:** 0, Parsers: 0

## Data Connectors

### Syslog

Syslog is an event logging protocol that is common to Linux. Applications will send messages that may be stored on the local machine or delivered to a Syslog collector. When the Agent for Linux is installed, it configures the local Syslog daemon to forward messages to the agent. The agent then sends the message to the workspace. For more information, see the [Microsoft Sentinel documentation](https://go.microsoft.com/fwlink/p/?linkid=2223807&wt.mc\_id=sentinel\_dataconnectordocs\_content\_cnl\_csasci).

## Workbooks

### Linux machines

Gain insights into your workspaces' Linux machines by connecting Microsoft Sentinel and using the logs to gather insights around Linux events and errors.

**Required Data Types**

Syslog

Syslog

## Analytic Rules

### Failed logon attempts in authpriv

Identifies failed logon attempts from unknown users in Syslog authpriv logs. The unknown user means the account that tried to log in

isn't provisioned on the machine. A few hits could indicate someone attempting to access a machine they aren't authorized to access.

If there are many of hits, especially from outside your network, it could indicate a brute force attack.

Default threshold for logon attempts is 15.

**Required Data Connectors**

Syslog

### NRT Squid proxy events related to mining pools

Checks for Squid proxy events in Syslog associated with common mining pools .This query presumes the default Squid log format is being used.

http://www.squid-cache.org/Doc/config/access\_log/

**Required Data Connectors**

Syslog

### Squid proxy events related to mining pools

Checks for Squid proxy events in Syslog associated with common mining pools .This query presumes the default Squid log format is being used.

http://www.squid-cache.org/Doc/config/access\_log/

**Required Data Connectors**

Syslog

### Squid proxy events for ToR proxies

Check for Squid proxy events associated with common ToR proxies. This query presumes the default squid log format is being used.

http://www.squid-cache.org/Doc/config/access\_log/

**Required Data Connectors**

Syslog

### SSH - Potential Brute Force

Identifies an IP address that had 15 failed attempts to sign in via SSH in a 4 hour block during a 24 hour time period.

**Required Data Connectors**

Syslog

## Hunting Queries

### Crypto currency miners EXECVE

Syslog Hunting Query 1

### SCX Execute RunAs Providers

Syslog Hunting Query 2

### Suspicious crytocurrency mining related threat activity detected

Syslog Hunting Query 3

### Rare process running on a Linux host

Syslog Hunting Query 4

### Linux scheduled task Aggregation

Syslog Hunting Query 5

### Editing Linux scheduled tasks through Crontab

Syslog Hunting Query 6

### Squid commonly abused TLDs

Syslog Hunting Query 7

### Squid malformed requests

Syslog Hunting Query 8

### Squid data volume timeseries anomalies

Syslog Hunting Query 9

## Watchlists

## Playbooks

## Parsers

# Talon Connector for Microsoft Sentinel

The Talon Security Logs connector lets you easily connect your Talon events and audit logs with Microsoft Sentinel, to view dashboards, create custom alerts, and improve security investigation.

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

## Data Connectors

### Talon Insights

The Talon Security Logs connector allows you to easily connect your Talon events and audit logs with Microsoft Sentinel, to view dashboards, create custom alerts, and improve investigation.

## Workbooks

### Talon Insights

This workbook provides Talon Security Insights on Log Analytics Query Logs

**Required Data Types**

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Tanium Microsoft Sentinel Connector

This enables organizations to enrich alerts in Microsoft Sentinel with real-time device posture information from Tanium. In addition, customers can remediate (e.g., quarantine, update config) - whether one time or via playbook - without switching context

**Data Connectors:** 0**, Workbooks:** 1**, Analytic Rules:** 1**, Hunting Queries:** 0**, Watchlists:** 0**, Playbooks:** 7, Parsers: 0

## Data Connectors

## Workbooks

### Tanium Workbook

Visualize Tanium endpoint and module data

**Required Data Types**

## Analytic Rules

### Tanium Threat Response Alerts

Alerts from Tanium Threat Response (THR) that can be acted upon by Microsoft Sentinel Playbook

**Required Data Connectors**

(none listed)

## Hunting Queries

## Watchlists

## Playbooks

### Tanium-ComplyFindings

This playbook starts with a Microsoft Sentinel incident, gets the hosts associated with that incident, queries the Tanium API Gateway for Comply Findings for those hosts, and then adds a comment to the incident with that information.

### Tanium-GeneralHostInfo

This playbook starts with a Microsoft Sentinel incident, gets the hosts associated with that incident, queries the Tanium API Gateway for general endpoint information for those hosts, and then adds a comment to the incident with that information.

### Tanium-MSDefenderHealth

This playbook starts with a Microsoft Sentinel incident, gets the hosts associated with that incident, queries the Tanium API Gateway for the Microsoft Defender Health for those hosts, and then adds a comment to the incident with that information.

### Tanium-QuarantineHosts

This playbook starts with a Microsoft Sentinel incident, gets the hosts associated with that incident, then directs Tanium to quarantine those hosts. The status of the quarantine operation is commented on the Sentinel incident.

### Tanium-ResolveThreatResponseAlert

This playbook will resolve any Tanium Threat Response alerts associated with a Microsoft Sentinel incident.

### Tanium-SCCMClientHealth

This playbook starts with a Microsoft Sentinel incident, gets the hosts associated with that incident, queries the Tanium API Gateway for the SCCM Client Health for those hosts, and then adds a comment to the incident with that information.

### Tanium-UnquarantineHosts

This playbook starts with a Microsoft Sentinel incident, gets the hosts associated with that incident, then directs Tanium to un-quarantine those hosts. The status of the un-quarantine operation is commented on the Sentinel incident.

## Parsers

# Tenable App for Microsoft Sentinel

This integration combines Tenable's Cyber Exposure insights with Microsoft Sentinel's collection, detection, and investigation capabilities. This integration supports exporting assets and vulnerability data from Tenable.io directly to Microsoft Sentinel.

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

## Data Connectors

### Tenable.io Vulnerability Management (using Azure Function)

The [Tenable.io](https://www.tenable.com/products/tenable-io) data connector provides the capability to ingest Asset and Vulnerability data into Microsoft Sentinel through the REST API from the Tenable.io platform (Managed in the cloud). Refer to [API documentation](https://developer.tenable.com/reference) for more information. The connector provides the ability to get data which helps to examine potential security risks, get insight into your computing assets, diagnose configuration problems and more

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

### Tenable.io - Enrich incident with asset info

Once a new Microsoft Sentinel incident is created, this playbook gets triggered and performs the following actions:

1. Obtains IPs from the incident.

2. Searches asset information by the IPs in Microsoft Sentinel.

3. Adds obtained information as a comment to the incident.

### Tenable.io - Enrich incident with vulnerability info

Once a new Microsoft Sentinel incident is created, this playbook gets triggered and performs the following actions:

1. Obtains IPs from the incident.

2. Searches asset IDs by the IPs in Microsoft Sentinel.

3. Gets vulnerabilities information in Microsoft Sentinel.

4. Adds obtained information as a comment to the incident.

### Tenable.io - Launch Scan

Once a new Microsoft Sentinel incident is created, this playbook gets triggered and performs the following actions:

1. Launches scan by scan id provided during the playbook deployment.

2. Adds information about launched scan as a comment to the incident.

## Parsers

### TenableIOAssets

Category: Samples

Function Alias: TenableIOAssets

### TenableIOVulnerabilities

Category: Samples

Function Alias: TenableIOVulnerabilities

# TheHive Solution

TheHive is a scalable, open source and free Security Incident Response Platform, tightly integrated with MISP (Malware Information Sharing Platform), designed to make life easier for any information security practitioner dealing with security incidents.

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

## Data Connectors

### TheHive Project - TheHive (using Azure Function)

The [TheHive](http://thehive-project.org/) data connector provides the capability to ingest common TheHive events into Microsoft Sentinel through Webhooks. TheHive can notify external system of modification events (case creation, alert update, task assignment) in real time. When a change occurs in the TheHive, an HTTPS POST request with event information is sent to a callback data connector URL. Refer to [Webhooks documentation](https://docs.thehive-project.org/thehive/legacy/thehive3/admin/webhooks/) for more information. The connector provides ability to get events which helps to examine potential security risks, analyze your team's use of collaboration, diagnose configuration problems and more.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

### The Hive - Create alert

Once a new Microsoft Sentinel incident is created, this playbook gets triggered and performs the following actions:

1. Parses alert extended properties.

2. Parses alert custom details.

3. Creates alert in TheHive with description, source, sourceRef, title and type passed.

### The Hive - Create case

Once a new Microsoft Sentinel incident is created, this playbook gets triggered and performs the following actions:

1. Creates case in TheHive instance with enriched description and title.

2. Gets Hosts, IPs entities.

3. Creates task and bind it to case.

4. Creates observables with hosts and IPs for created case.

### The Hive - Lock user

Once a new Microsoft Sentinel incident is created, this playbook gets triggered and performs the following actions:

1. Parses alerts custom details

2. Locks Users by UserId or UserLogin passed from alert.

## Parsers

### TheHive Data Parser

Category: Samples

Function Alias: TheHive

# Theom for Microsoft Sentinel Solution - Data Cloud and Data Lakehouse Attack Detection

Theom for Microsoft Sentinel Solution enables customers to detect and stop active threats to data clouds and data lakehouses. Sentinel customers can seamlessly apply Theom’s unique AI threat intelligence while using their trusted environment for alerting.

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 20**, Hunting Queries:** 0**, Watchlists:** 0**, Playbooks:** 0, Parsers: 0

## Data Connectors

### Theom

Theom Data Connector enables organizations to connect their Theom environment to Microsoft Sentinel. This solution enables users to receive alerts on data security risks, create and enrich incidents, check statistics and trigger SOAR playbooks in Microsoft Sentinel

## Workbooks

### Theom

Theom Alert Statistics

**Required Data Types**

TheomAlerts\_CL

Theom

## Analytic Rules

### Theom Critical Risks

Creates Microsoft Sentinel incidents for critical risk Theom alerts.

**Required Data Connectors**

Theom

### Theom High Risks

Creates Microsoft Sentinel incidents for high risk Theom alerts.

**Required Data Connectors**

Theom

### Theom Medium Risks

Creates Microsoft Sentinel incidents for medium risk Theom alerts.

**Required Data Connectors**

Theom

### Theom Low Risks

Creates Microsoft Sentinel incidents for low risk Theom alerts

**Required Data Connectors**

Theom

### Theom Insights

Creates Microsoft Sentinel incidents for Theom insight alerts.

**Required Data Connectors**

Theom

### Theom - Dev secrets unencrypted

Creates Sentinel incidents for critical/high Theom risks, associated with ruleId TRIS0001 (Developer secrets have been observed in unencrypted data stores. Encrypt data at rest to comply with this CIS requirement)

**Required Data Connectors**

Theom

### Theom - National IDs unencrypted

Creates Sentinel incidents for critical/high Theom risks, associated with ruleId TRIS0002 (National IDs have been observed in unencrypted data stores. Encrypt data at rest to comply with this CIS requirement)

**Required Data Connectors**

Theom

### Theom - Financial data unencrypted

Creates Sentinel incidents for critical/high Theom risks, associated with ruleId TRIS0003 (Financial data has been observed in unencrypted data stores. Encrypt data at rest to comply with this CIS requirement)

**Required Data Connectors**

Theom

### Theom - Healthcare data unencrypted

Creates Sentinel incidents for critical/high Theom risks, associated with ruleId TRIS0004 (Healthcare data has been observed in unencrypted data stores. Encrypt data at rest to comply with this CIS requirement)

**Required Data Connectors**

Theom

### Theom - Unencrypted public data stores

Creates Sentinel incidents for critical/high Theom risks, associated with ruleId TRIS0005 (Theom has observed data stores that are both unencrypted and publicly accessible. Review if the data store and the data within should be publicly accessible. Additionally, encrypt the data at rest to comply with these CIS requirements)

**Required Data Connectors**

Theom

### Theom - Critical data in API headers or body

Creates Sentinel incidents for critical/high Theom risks, associated with ruleId's TRIS0007 to TRIS0010 and TRIS0014

**Required Data Connectors**

Theom

### Theom - Dev secrets exposed

Creates Sentinel incidents for critical/high Theom risks, associated with ruleId TRIS0012 (Theom has observed developer secrets in a data store that is publicly exposed. As per this requirement, use this information to apply data access control lists or access permissions to secure your data)

**Required Data Connectors**

Theom

### Theom - Healthcare data exposed

Creates Sentinel incidents for critical/high Theom risks, associated with ruleId TRIS0015 (Theom has observed healthcare data in a data store that is publicly exposed. As per this requirement, use this information to apply data access control lists or access permissions to secure your data)

**Required Data Connectors**

Theom

### Theom - National IDs exposed

Creates Sentinel incidents for critical/high Theom risks, associated with ruleId TRIS0018 (Theom has observed National IDs in a data store that is publicly exposed. As per this requirement, use this information to apply data access control lists or access permissions to secure your data)

**Required Data Connectors**

Theom

### Theom - Financial data exposed

Creates Sentinel incidents for critical/high Theom risks, associated with ruleId TRIS0026 (Theom has observed financial data in a data store that is publicly exposed. As per this requirement, use this information to apply data access control lists or access permissions to secure your data)

**Required Data Connectors**

Theom

### Theom - Dark Data with large fin value

Creates Sentinel incidents for critical/high Theom risks, associated with ruleId TRIS0032 (Theom has observed data with a large financial value, but that has not been accessed recently. Use this information to enforce data retention policies)

**Required Data Connectors**

Theom

### Theom - Least priv large value shadow DB

Creates Sentinel incidents for critical/high Theom risks, associated with ruleId TRIS0032 (Theom has observed shadow (or clone) databases/tables that have a large financial value. Additionally, it has observed roles that are overprovisioned for these data stores. As per this requirement, use this information to apply data access control lists or access permissions and enforce data retention policies)

**Required Data Connectors**

Theom

### Theom - Overprovisioned Roles Shadow DB

Creates Sentinel incidents for critical/high Theom risks, associated with ruleId TRIS0034 (Theom has observed shadow (or clone) databases/tables. Additionally, it has observed roles that are overprovisioned for these data stores. As per this requirement, use this information to apply data access control lists or access permissions and enforce data retention policies)

**Required Data Connectors**

Theom

### Theom - Shadow DB large datastore value

Creates Sentinel incidents for critical/high Theom risks, associated with ruleId TRIS0035 (Theom has observed shadow (or clone) databases/tables with large financial value. As per this requirement, use this information to apply data access control lists or access permissions and enforce data retention policies)

**Required Data Connectors**

Theom

### Theom - Shadow DB with atypical accesses

Creates Sentinel incidents for critical/high Theom risks, associated with ruleId TRIS0036 (Theom has observed shadow or clone databases/tables. Additionally, it has observed atypical accesses to these data stores. As per this requirement, use this information to apply data access control lists or access permissions and enforce data retention policies)

**Required Data Connectors**

Theom

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Threat Analysis & Response

MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.

**Data Connectors:** 0**, Workbooks:** 2**, Analytic Rules:** 0**, Hunting Queries:** 0**, Watchlists:** 0**, Playbooks:** 0, Parsers: 0

## Data Connectors

## Workbooks

### Threat Analysis Response

Sets the time name for analysis

**Required Data Types**

### Dynamic Threat Modeling Response

Sets the time name for analysis

**Required Data Types**

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Threat Intelligence

The Threat Intelligence solution allows you to ingest threat indicators into Microsoft Sentinel.

**Data Connectors:** 2**, Workbooks:** 1**, Analytic Rules:** 35**, Hunting Queries:** 5**, Watchlists:** 0**, Playbooks:** 0, Parsers: 0

## Data Connectors

### Threat intelligence - TAXII

Microsoft Sentinel integrates with TAXII 2.0 and 2.1 data sources to enable monitoring, alerting, and hunting using your threat intelligence. Use this connector to send threat indicators from TAXII servers to Microsoft Sentinel. Threat indicators can include IP addresses, domains, URLs, and file hashes.

### Threat Intelligence Platforms

Microsoft Sentinel integrates with Microsoft Graph Security API data sources to enable monitoring, alerting, and hunting using your threat intelligence. Use this connector to send threat indicators to Microsoft Sentinel from your Threat Intelligence Platform (TIP), such as Threat Connect, Palo Alto Networks MindMeld, MISP, or other integrated applications. Threat indicators can include IP addresses, domains, URLs, and file hashes.

## Workbooks

### Threat Intelligence

Gain insights into threat indicators ingestion and search for indicators at scale across Microsoft 1st Party, 3rd Party, On-Premises, Hybrid, and Multi-Cloud Workloads. Indicators Search facilitates a simple interface for finding IP, File, Hash, Sender and more across your data. Seamless pivots to correlate indicators with Microsoft Sentinel: Incidents to make your threat intelligence actionable.

**Required Data Types**

ThreatIntelligenceIndicator

SecurityIncident

ThreatIntelligence

ThreatIntelligenceTaxii

## Analytic Rules

### TI map Domain entity to CommonSecurityLog

Identifies a match in CommonSecurityLog table from any Domain IOC from TI

**Required Data Connectors**

ThreatIntelligence

ThreatIntelligenceTaxii

### TI map Domain entity to DnsEvents

Identifies a match in DnsEvents from any Domain IOC from TI

**Required Data Connectors**

DNS

ThreatIntelligence

ThreatIntelligenceTaxii

### (Preview) TI map Domain entity to Web Session Events (ASIM Web Session schema)

This rule identifies Web Sessions for which the target URL hostname is a known IoC. <br><br>This rule uses the [Advanced Security Information Model (ASIM)](https://aka.ms/AboutSIM) and supports any web session source that complies with ASIM.

**Required Data Connectors**

SquidProxy

Zscaler

ThreatIntelligence

### TI map Domain entity to PaloAlto

Identifies a match in Palo Alto data in CommonSecurityLog table from any Domain IOC from TI

**Required Data Connectors**

PaloAltoNetworks

ThreatIntelligence

ThreatIntelligenceTaxii

### TI map Domain entity to SecurityAlert

Identifies a match in SecurityAlert table from any Domain IOC from TI

**Required Data Connectors**

ThreatIntelligence

ThreatIntelligenceTaxii

MicrosoftCloudAppSecurity

AzureSecurityCenter

### TI map Domain entity to Syslog

Identifies a match in Syslog table from any Domain IOC from TI

**Required Data Connectors**

Syslog

ThreatIntelligence

ThreatIntelligenceTaxii

### TI map Email entity to AzureActivity

Identifies a match in AzureActivity table from any Email IOC from TI

**Required Data Connectors**

AzureActivity

ThreatIntelligence

ThreatIntelligenceTaxii

### TI map Email entity to OfficeActivity

Identifies a match in OfficeActivity table from any Email IOC from TI

**Required Data Connectors**

Office365

ThreatIntelligence

ThreatIntelligenceTaxii

### TI map Email entity to CommonSecurityLog

Identifies a match in CommonSecurityLog table from any Email IOC from TI

**Required Data Connectors**

PaloAltoNetworks

ThreatIntelligence

ThreatIntelligenceTaxii

### TI map Email entity to SecurityAlert

Identifies a match in SecurityAlert table from any Email IOC from TI which will extend coverage to datatypes such as MCAS, StorageThreatProtection and many others

**Required Data Connectors**

AzureSecurityCenter

ThreatIntelligence

ThreatIntelligenceTaxii

### TI map Email entity to SecurityEvent

Identifies a match in SecurityEvent table from any Email IOC from TI

**Required Data Connectors**

ThreatIntelligence

ThreatIntelligenceTaxii

SecurityEvents

WindowsSecurityEvents

WindowsForwardedEvents

### TI map Email entity to SigninLogs

Identifies a match in SigninLogs table from any Email IOC from TI

**Required Data Connectors**

ThreatIntelligence

ThreatIntelligenceTaxii

AzureActiveDirectory

AzureActiveDirectory

### TI map File Hash to CommonSecurityLog Event

Identifies a match in CommonSecurityLog Event data from any FileHash IOC from TI

**Required Data Connectors**

PaloAltoNetworks

ThreatIntelligence

ThreatIntelligenceTaxii

### Microsoft COVID-19 file hash indicator matches

Identifies a match in CommonSecurityLog Event data from any FileHash published in the Microsoft COVID-19 Threat Intel Feed - as described at https://www.microsoft.com/security/blog/2020/05/14/open-sourcing-covid-threat-intelligence/

**Required Data Connectors**

PaloAltoNetworks

### TI map File Hash to Security Event

Identifies a match in Security Event data from any File Hash IOC from TI

**Required Data Connectors**

SecurityEvents

WindowsSecurityEvents

WindowsForwardedEvents

ThreatIntelligence

ThreatIntelligenceTaxii

### TI map IP entity to AppServiceHTTPLogs

Identifies a match in AppServiceHTTPLogs from any IP IOC from TI

**Required Data Connectors**

ThreatIntelligence

ThreatIntelligenceTaxii

### TI map IP entity to AWSCloudTrail

Identifies a match in AWSCloudTrail from any IP IOC from TI

**Required Data Connectors**

ThreatIntelligence

ThreatIntelligenceTaxii

AWS

### TI map IP entity to AzureActivity

Identifies a match in AzureActivity from any IP IOC from TI

**Required Data Connectors**

ThreatIntelligence

ThreatIntelligenceTaxii

AzureActivity

### TI map IP entity to AzureFirewall

Identifies a match in AzureFirewall (NetworkRule & ApplicationRule Logs) from any IP IOC from TI

**Required Data Connectors**

ThreatIntelligence

ThreatIntelligenceTaxii

AzureFirewall

### TI map IP entity to Azure Key Vault logs

Identifies a match in Azure Key Vault logsfrom any IP IOC from TI

**Required Data Connectors**

ThreatIntelligence

ThreatIntelligenceTaxii

AzureKeyVault

### TI map IP entity to AzureNetworkAnalytics\_CL (NSG Flow Logs)

Identifies a match in AzureNetworkAnalytics\_CL (NSG Flow Logs) from any IP IOC from TI that was Allowed

**Required Data Connectors**

ThreatIntelligence

ThreatIntelligenceTaxii

### TI map IP entity to Azure SQL Security Audit Events

Identifies a match in SQLSecurityAuditEvents from any IP IOC from TI

**Required Data Connectors**

ThreatIntelligence

ThreatIntelligenceTaxii

### TI map IP entity to CommonSecurityLog

Identifies a match in CommonSecurityLog from any IP IOC from TI

**Required Data Connectors**

ThreatIntelligence

ThreatIntelligenceTaxii

### TI map IP entity to DnsEvents

Identifies a match in DnsEvents from any IP IOC from TI

**Required Data Connectors**

ThreatIntelligence

ThreatIntelligenceTaxii

DNS

### (Preview) TI map IP entity to Web Session Events (ASIM Web Session schema)

This rule identifies Web Sessions for which the source IP address is a known IoC. <br><br>This rule uses the [Advanced Security Information Model (ASIM)](https://aka.ms/AboutASIM) and supports any web session source that complies with ASIM.

**Required Data Connectors**

SquidProxy

Zscaler

ThreatIntelligence

ThreatIntelligenceTaxii

### TI map IP entity to OfficeActivity

Identifies a match in OfficeActivity from any IP IOC from TI

**Required Data Connectors**

ThreatIntelligence

ThreatIntelligenceTaxii

Office365

### TI map IP entity to SigninLogs

Identifies a match in SigninLogs from any IP IOC from TI

**Required Data Connectors**

ThreatIntelligence

ThreatIntelligenceTaxii

AzureActiveDirectory

AzureActiveDirectory

### TI map IP entity to VMConnection

Identifies a match in VMConnection from any IP IOC from TI

**Required Data Connectors**

ThreatIntelligence

ThreatIntelligenceTaxii

AzureMonitor(VMInsights)

### TI map IP entity to W3CIISLog

Identifies a match in W3CIISLog from any IP IOC from TI

**Required Data Connectors**

ThreatIntelligence

ThreatIntelligenceTaxii

AzureMonitor(IIS)

### TI map IP entity to WireData

Identifies a match in WireData from any IP IOC from TI

**Required Data Connectors**

ThreatIntelligence

ThreatIntelligenceTaxii

AzureMonitor(WireData)

### TI map URL entity to AuditLogs

Identifies a match in AuditLogs from any URL IOC from TI

**Required Data Connectors**

AzureActiveDirectory

ThreatIntelligence

ThreatIntelligenceTaxii

### TI map URL entity to OfficeActivity data

Identifies a match in OfficeActivity data from any URL IOC from TI

**Required Data Connectors**

Office365

ThreatIntelligence

TI map URL entity to PaloAlto data

Identifies a match in PaloAlto data from any URL IOC from TI

**Required Data Connectors**

PaloAltoNetworks

ThreatIntelligence

ThreatIntelligenceTaxii

### TI map URL entity to SecurityAlert data

Identifies a match in SecurityAlert data from any URL IOC from TI

**Required Data Connectors**

MicrosoftCloudAppSecurity

AzureSecurityCenter

ThreatIntelligence

ThreatIntelligenceTaxii

### TI map URL entity to Syslog data

Identifies a match in Syslog data from any URL IOC from TI

**Required Data Connectors**

Syslog

ThreatIntelligence

ThreatIntelligenceTaxii

## Hunting Queries

### Preview - TI map File entity to OfficeActivity Event

Threat Intelligence Hunting Query 1

### Preview - TI map File entity to Security Event

Threat Intelligence Hunting Query 2

### Preview - TI map File entity to Syslog Event

Threat Intelligence Hunting Query 3

### Preview - TI map File entity to VMConnection Event

Threat Intelligence Hunting Query 4

### Preview - TI map File entity to WireData Event

Threat Intelligence Hunting Query 5

## Watchlists

## Playbooks

## Parsers

# ThreatX WAF

The ThreatX solution provides an automation approach to analyst for remediate the attacks happening at application level by blocking the suspicious IP and URL and also empowers them to gather the threat intelligence data for the malicious IP activity.

**Data Connectors:** 0**, Workbooks:** 0**, Analytic Rules:** 0**, Hunting Queries:** 0**, Watchlists:** 0**, Playbooks:** 2, Parsers: 0

## Data Connectors

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

### Block IP & URL on ThreatX-WAF cloud

This Playbook Provides the automation on blocking the suspicious/malicious IP and URL on ThreatX cloud waf

### Fetch Threat Intel from ThreatX

This playbook provides/updates the threat intel and essential details in comments section of triggered incident so that SOC analysts can directly take corrective measure to stop the attack

## Parsers

# Trend Micro Apex One Solution

Trend Micro Apex One protection offers advanced automated threat detection and response against an ever-growing variety of threats, including fileless and ransomware.

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 10**, Hunting Queries:** 10**, Watchlists:** 0**, Playbooks:** 0, Parsers: 1

## Data Connectors

### Trend Micro Apex One

The [Trend Micro Apex One](https://www.trendmicro.com/en\_us/business/products/user-protection/sps/endpoint.html) data connector provides the capability to ingest [Trend Micro Apex One events](https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/appendices/syslog-mapping-cef.aspx) into Microsoft Sentinel. Refer to [Trend Micro Apex Central](https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/preface\_001.aspx) for more information.

## Workbooks

### Trend Micro Apex One

Sets the time name for analysis.

**Required Data Types**

CommonSecurityLog

TrendMicroApexOne

## Analytic Rules

### ApexOne - Attack Discovery Detection

Detects Attack Discovery Detection events.

**Required Data Connectors**

TrendMicroApexOne

### ApexOne - Suspicious commandline arguments

Detects suspicious commandline arguments.

**Required Data Connectors**

TrendMicroApexOne

### ApexOne - Commands in Url

Detects commands in Url.

**Required Data Connectors**

TrendMicroApexOne

### ApexOne - Device access permissions was changed

Query shows device access permissions was changed.

**Required Data Connectors**

TrendMicroApexOne

### ApexOne - Inbound remote access connection

Detects inbound remote access connection.

**Required Data Connectors**

TrendMicroApexOne

### ApexOne - Multiple deny or terminate actions on single IP

Detects multiple deny or terminate actions on single IP.

**Required Data Connectors**

TrendMicroApexOne

### ApexOne - Possible exploit or execute operation

Detects possible exploit or execute operation.

**Required Data Connectors**

TrendMicroApexOne

### ApexOne - C&C callback events

Detects C&C callback events.

**Required Data Connectors**

TrendMicroApexOne

### ApexOne - Spyware with failed response

Detects spyware with failed response.

**Required Data Connectors**

TrendMicroApexOne

### ApexOne - Suspicious connections

Detects suspicious connections.

**Required Data Connectors**

TrendMicroApexOne

## Hunting Queries

### ApexOne - Behavior monitoring actions by files

Trend Micro Apex One Hunting Query 1

### ApexOne - Behavior monitoring operations by users

Trend Micro Apex One Hunting Query 2

### ApexOne - Behavior monitoring triggered policy by command line

Trend Micro Apex One Hunting Query 3

### ApexOne - Behavior monitoring event types by users

Trend Micro Apex One Hunting Query 4

### ApexOne - Channel type by users

Trend Micro Apex One Hunting Query 5

### ApexOne - Data loss prevention action by IP

Trend Micro Apex One Hunting Query 6

### ApexOne - Rare application protocols by Ip address

Trend Micro Apex One Hunting Query 7

### ApexOne - Spyware detection

Trend Micro Apex One Hunting Query 8

### ApexOne - Suspicious files events

Trend Micro Apex One Hunting Query 9

### ApexOne - Top sources with alerts

Trend Micro Apex One Hunting Query 10

## Watchlists

## Playbooks

## Parsers

### Trend Micro Apex One Data Parser

Category: Samples

Function Alias: TMApexOneEvent

# Trend Micro Cloud App Security

The Trend Micro Cloud App Security data connector provides the capability to retrieve security event logs of the services that Cloud App Security protects and more events into Microsoft Sentinel through the Log Retrieval API.

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 10**, Hunting Queries:** 10**, Watchlists:** 0**, Playbooks:** 0, Parsers: 1

## Data Connectors

### Trend Micro Cloud App Security (using Azure Function)

The [Trend Micro Cloud App Security](https://www.trendmicro.com/en\_be/business/products/user-protection/sps/email-and-collaboration/cloud-app-security.html) data connector provides the capability to retrieve security event logs of the services that Cloud App Security protects and more events into Microsoft Sentinel through the Log Retrieval API. Refer to API [documentation](https://docs.trendmicro.com/en-us/enterprise/cloud-app-security-integration-api-online-help/supported-cloud-app-/log-retrieval-api/get-security-logs.aspx) for more information. The connector provides ability to get events which helps to examine potential security risks, analyze your team's use of collaboration, diagnose configuration problems and more.

## Workbooks

### TrendMicroCAS

Sets the time name for analysis

**Required Data Types**

TrendMicroCAS\_CL

TrendMicroCAS

## Analytic Rules

### Trend Micro CAS - DLP violation

Detects when DLP policy violation occurs.

**Required Data Connectors**

TrendMicroCAS

### Trend Micro CAS - Possible phishing mail

Detects possible phishing mail.

**Required Data Connectors**

TrendMicroCAS

### Trend Micro CAS - Ransomware infection

Triggeres when ransomware was detected.

**Required Data Connectors**

TrendMicroCAS

### Trend Micro CAS - Ransomware outbreak

Triggeres when ransomware was detected on several accounts.

**Required Data Connectors**

TrendMicroCAS

### Trend Micro CAS - Suspicious filename

Detects unexpected filename.

**Required Data Connectors**

TrendMicroCAS

### Trend Micro CAS - Threat detected and not blocked

Detects when threat was not blocked by CAS solution.

**Required Data Connectors**

TrendMicroCAS

### Trend Micro CAS - Unexpected file via mail

Detects when unexpected file recieved via mail.

**Required Data Connectors**

TrendMicroCAS

### Trend Micro CAS - Unexpected file on file share

Detects unexpected files on file share.

**Required Data Connectors**

TrendMicroCAS

### Trend Micro CAS - Infected user

Detects when malware was detected for user account.

**Required Data Connectors**

TrendMicroCAS

### Trend Micro CAS - Multiple infected users

Detects when same malware was detected for multiple user account.

**Required Data Connectors**

TrendMicroCAS

## Hunting Queries

### Trend Micro CAS - Files stored on cloud fileshare services

Trend Micro Cloud App Security Hunting Query 1

### Trend Micro CAS - Infected files received via email

Trend Micro Cloud App Security Hunting Query 2

### Trend Micro CAS - Ransomware threats

Trend Micro Cloud App Security Hunting Query 3

### Trend Micro CAS - Rare files received via email services

Trend Micro Cloud App Security Hunting Query 4

### Trend Micro CAS - Risky users

Trend Micro Cloud App Security Hunting Query 5

### Trend Micro CAS - Security risk scan threats

Trend Micro Cloud App Security Hunting Query 6

### Trend Micro CAS - Suspicious files on sharepoint

Trend Micro Cloud App Security Hunting Query 7

### Trend Micro CAS - Files received via email services

Trend Micro Cloud App Security Hunting Query 8

### Trend Micro CAS - DLP violations

Trend Micro Cloud App Security Hunting Query 9

### Trend Micro CAS - Virtual Analyzer threats

Trend Micro Cloud App Security Hunting Query 10

## Watchlists

## Playbooks

## Parsers

### TrendMicroCAS

Category: Samples

Function Alias: TrendMicroCAS

# Trend Micro Deep Security for Microsoft Sentinel

The Trend Micro Deep Security connector allows you to easily connect your Deep Security logs with Microsoft Sentinel, to view dashboards, create custom alerts, and improve investigation.

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

## Data Connectors

### Trend Micro Deep Security

The Trend Micro Deep Security connector allows you to easily connect your Deep Security logs with Microsoft Sentinel, to view dashboards, create custom alerts, and improve investigation. This gives you more insight into your organization's networks/systems and improves your security operation capabilities.

## Workbooks

### Trend Micro Deep Security ATT&CK Related Activity

Visualize and gain insights into the MITRE ATT&CK related activity detected by Trend Micro Deep Security.

**Required Data Types**

### Trend Micro Deep Security Events

Gain insights into your Trend Micro Deep Security security event data by visualizing your Deep Security Anti-Malware, Firewall, Integrity Monitoring, Intrusion Prevention, Log Inspection, and Web Reputation event data.

**Required Data Types**

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### TrendMicroDeepSecurity

Category: Samples

Function Alias: TrendMicroDeepSecurity

# Trend Micro TippingPoint for Microsoft Sentinel

The Trend Micro TippingPoint connector allows you to easily connect your TippingPoint SMS IPS events with Microsoft Sentinel, to view dashboards, create custom alerts, and improve investigation.

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

## Data Connectors

### Trend Micro TippingPoint

The Trend Micro TippingPoint connector allows you to easily connect your TippingPoint SMS IPS events with Microsoft Sentinel, to view dashboards, create custom alerts, and improve investigation. This gives you more insight into your organization's networks/systems and improves your security operation capabilities.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### TrendMicroTippingPoint

Category: Samples

Function Alias: TrendMicroTippingPoint

# Trend Vision One for Microsoft Sentinel

The Trend Vision One connector provides the capability to ingest workbench alerts from the Trend Vision One API into Microsoft Sentinel.

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

## Data Connectors

### Trend Micro Vision One (using Azure Function)

The [Trend Micro Vision One](https://www.trendmicro.com/en\_us/business/products/detection-response/xdr.html) connector provides the capability to ingest workbench alerts from the Trend Micro Vision One API into Microsoft Sentinel. The connector provides visibility into these log types in Microsoft Sentinel to view dashboards, create custom alerts, and to improve monitoring and investigation capabilities.

## Workbooks

### Trend Micro Vision One Alert Overview

Gain insights from Trend Micro Vision One with this overview of the Alerts triggered.

**Required Data Types**

TrendMicro\_XDR\_WORKBENCH\_CL

TrendMicroXDR

## Analytic Rules

### TrendMicroXDRWorkbench

**Required Data Connectors**

(none listed)

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Ubiquiti UniFi

Ubiquiti Inc. is an American technology company that manufactures and sells wireless data communication and wired products for enterprises and homes under multiple brand names.

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 10**, Hunting Queries:** 10**, Watchlists:** 0**, Playbooks:** 0, Parsers: 1

## Data Connectors

### Ubiquiti UniFi (Preview)

The [Ubiquiti UniFi](https://www.ui.com/) data connector provides the capability to ingest [Ubiquiti UniFi firewall, dns, ssh, AP events](https://help.ui.com/hc/en-us/articles/204959834-UniFi-How-to-View-Log-Files) into Microsoft Sentinel.

## Workbooks

### Ubiquiti UniFi

Sets the time name for analysis

**Required Data Types**

Ubiquiti\_CL

UbiquitiUnifi

## Analytic Rules

### Ubiquiti - Possible connection to cryptominning pool

Detects connections which may indicate that device is infected with cryptominer.

**Required Data Connectors**

UbiquitiUnifi

### Ubiquiti - Connection to known malicious IP or C2

Detects allowed connections to IP addresses which are in TI list and are known to be malicious.

**Required Data Connectors**

UbiquitiUnifi

### Ubiquiti - Unusual FTP connection to external server

Detects local to remote (L2R) FTP connections.

**Required Data Connectors**

UbiquitiUnifi

### Ubiquiti - Large ICMP to external server

Detects large ICMP packets to external host.

**Required Data Connectors**

UbiquitiUnifi

### Ubiquiti - connection to non-corporate DNS server

Detects connections to non-corporate DNS servers.

**Required Data Connectors**

UbiquitiUnifi

### Ubiquiti - Unusual DNS connection

Detects unusual remote to local (R2L) DNS connections.

**Required Data Connectors**

UbiquitiUnifi

### Ubiquiti - RDP from external source

Detects remote to local (R2L) RDP connection.

**Required Data Connectors**

UbiquitiUnifi

### Ubiquiti - SSH from external source

Detects remote to local (R2L) SSH connection to internal host.

**Required Data Connectors**

UbiquitiUnifi

### Ubiquiti - Unknown MAC Joined AP

Detects when device with unseen MAC Address joined AP.

**Required Data Connectors**

UbiquitiUnifi

### Ubiquiti - Unusual traffic

Detects unusual traffic masking as HTTP(S).

**Required Data Connectors**

UbiquitiUnifi

## Hunting Queries

### Ubiquiti - DNS requests timed out

Ubiquiti UniFi Hunting Query 1

### Ubiquiti - Hidden internal DNS server

Ubiquiti UniFi Hunting Query 2

### Ubiquiti - Rare internal ports

Ubiquiti UniFi Hunting Query 3

### Ubiquiti - Top blocked destinations

Ubiquiti UniFi Hunting Query 4

### Ubiquiti - Top blocked external services

Ubiquiti UniFi Hunting Query 5

### Ubiquiti - Top blocked internal services

Ubiquiti UniFi Hunting Query 6

### Ubiquiti - Top blocked sources

Ubiquiti UniFi Hunting Query 7

### Ubiquiti - Top firewall rules

Ubiquiti UniFi Hunting Query 8

### Ubiquiti - Unusual number of subdomains for top level domain (TLD)

Ubiquiti UniFi Hunting Query 9

### Ubiquiti - Vulnerable devices

Ubiquiti UniFi Hunting Query 10

## Watchlists

## Playbooks

## Parsers

### Ubiquiti Data Parser

Category: Samples

Function Alias: UbiquitiAuditEvent

# UEBA Essentials

The Sentinel UEBA content package will provide you with various queries based on UEBA tables, that allows you to hunt for tailored threat scenarios.

**Data Connectors:** 0**, Workbooks:** 0**, Analytic Rules:** 0**, Hunting Queries:** 23**, Watchlists:** 0**, Playbooks:** 0, Parsers: 0

## Data Connectors

## Workbooks

## Analytic Rules

## Hunting Queries

### Anomalies on users tagged as VIP

UEBA Essentials Hunting Query 1

### Anomalous action performed in tenant by privileged user

UEBA Essentials Hunting Query 2

### Dormant account activity from uncommon country

UEBA Essentials Hunting Query 3

### Anomalous connection from highly privileged user

UEBA Essentials Hunting Query 4

### Anomalous login activity originated from Botnet, Tor proxy or C2

UEBA Essentials Hunting Query 5

### New account added to admin group

UEBA Essentials Hunting Query 6

### Terminated employee accessing High Value Asset

UEBA Essentials Hunting Query 7

### Activity from terminated employees after their termination date

UEBA Essentials Hunting Query 8

### Anomalous update Key Vault activity by high blast radius user

UEBA Essentials Hunting Query 9

### Anomalous AAD Account Manipulation

UEBA Essentials Hunting Query 10

### Anomalous AAD Account Creation

UEBA Essentials Hunting Query 11

### Anomalous Activity Role Assignment

UEBA Essentials Hunting Query 12

### Anomalous Code Execution

UEBA Essentials Hunting Query 13

### Anomalous Data Access

UEBA Essentials Hunting Query 14

### Anomalous Defensive Mechanism Modification

UEBA Essentials Hunting Query 15

### Anomalous Failed Logon

UEBA Essentials Hunting Query 16

### Anomalous Login to Devices

UEBA Essentials Hunting Query 17

### Anomalous Geo Location Logon

UEBA Essentials Hunting Query 18

### Anomalous Password Reset

UEBA Essentials Hunting Query 19

### Anomalous RDP Activity

UEBA Essentials Hunting Query 20

### Anomalous Resource Access

UEBA Essentials Hunting Query 21

### Anomalous Role Assignment

UEBA Essentials Hunting Query 22

### Anomalous Sign-in Activity

UEBA Essentials Hunting Query 23

## Watchlists

## Playbooks

## Parsers

# URLhaus

The URLhaus solution for Microsoft Sentinel allows enriching incidents with additional information about file hashes, Hostname and URL using feeds and lists from URLhaus.

**Data Connectors:** 0**, Workbooks:** 0**, Analytic Rules:** 0**, Hunting Queries:** 0**, Watchlists:** 0**, Playbooks:** 3, Parsers: 0

## Data Connectors

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

### URLhaus-CheckHashAndEnrichIncident

Once a new Microsoft Sentinel incident is created, this playbook gets triggered and performs the following actions:

1. [Gets Information](https://urlhaus-api.abuse.ch/#payloadinfo) from URLhaus by hashes, provided in the alert custom entities.

2. Enriches the incident with the obtained info.

### URLhaus-CheckHostAndEnrichIncident

Once a new Microsoft Sentinel incident is created, this playbook gets triggered and performs the following actions:

1. [Gets Information](https://urlhaus-api.abuse.ch/#payloadinfo) from URLhaus by hashes, provided in the alert custom entities.

2. Enriches the incident with the obtained info.

### URLhaus-CheckURLAndEnrichIncident

Once a new Microsoft Sentinel incident is created, this playbook gets triggered and performs the following actions:

1. [Gets Information](https://urlhaus-api.abuse.ch/#payloadinfo) from URLhaus by hashes, provided in the alert custom entities.

2. Enriches the incident with the obtained info.

## Parsers

# vArmour Application Controller for Microsoft Sentinel

Connect into Microsoft's vast portfolio of security offerings with vArmour's Application Relationship Management approach visualizing relationships from the application outward to proactively and effectively mitigate business risk.

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

## Data Connectors

### vArmour Application Controller

vArmour reduces operational risk and increases cyber resiliency by visualizing and controlling application relationships across the enterprise. This vArmour connector enables streaming of Application Controller Violation Alerts into Microsoft Sentinel, so you can take advantage of search & correlation, alerting, & threat intelligence enrichment for each log.

## Workbooks

### vArmour Application Controller

Sets the time name for analysis

**Required Data Types**

CommonSecurityLog

vArmourAC

## Analytic Rules

### vArmour AppController - SMB Realm Traversal

Detects when SMB traffic crosses Production and Non-Production Realms. Possible network share discovery or lateral tool transfer across realms

**Required Data Connectors**

vArmourAC

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Vectra AI Stream for Microsoft Sentinel

Vectra AI enables organizations to detect threats by uncovering attacker behaviors within your environment across Network, SaaS and Cloud. The network metadata collected at scale throughout the environment by Vectra can be ingested by Microsoft Sentinel.

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 0**, Hunting Queries:** 10**, Watchlists:** 0**, Playbooks:** 0, Parsers: 1

## Data Connectors

### AI Vectra Stream

The AI Vectra Stream connector allows to send Network Metadata collected by Vectra Sensors accross the Network and Cloud to Microsoft Sentinel

## Workbooks

### AIVectraStreamWorkbook

**Required Data Types**

## Analytic Rules

## Hunting Queries

### Vectra AI - Potential Exfiltration over DNS

Vectra AI Stream Hunting Query 1

### Vectra AI - Malicious Tools File Copy

Vectra AI Stream Hunting Query 2

### Vectra AI - Potential LLMNR/NBT-NS Poisoning and SMB Relay

Vectra AI Stream Hunting Query 3

### Vectra AI - Possible PoshC2 Tunnel

Vectra AI Stream Hunting Query 4

### Vectra AI - Potential DCSync Attack

Vectra AI Stream Hunting Query 5

### Vectra AI - Possible Kali Linux Detected

Vectra AI Stream Hunting Query 6

### Vectra AI - Beaconing Behaviors

Vectra AI Stream Hunting Query 7

### Vectra AI - Suspicious Long DNS Queries

Vectra AI Stream Hunting Query 8

### Vectra AI - Suspicious number of sub-domains

Vectra AI Stream Hunting Query 9

### Vectra AI - Suspicious Unsecured Credentials Group Policy Preferences

Vectra AI Stream Hunting Query 10

## Watchlists

## Playbooks

## Parsers

### Vectra Data Parser

Category: Samples

Function Alias: VectraStream\_function

# Vectra Detect for Microsoft Sentinel

Vectra® is the leader in Security AI-driven cyber threat detection and response for hybrid cloud. Organizations worldwide rely on Vectra to stay ahead of modern cyber-attacks.

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

## Data Connectors

### Vectra AI Detect

The AI Vectra Detect connector allows users to connect Vectra Detect logs with Microsoft Sentinel, to view dashboards, create custom alerts, and improve investigation. This gives users more insight into their organization's network and improves their security operation capabilities.

## Workbooks

### Vectra AI Detect

Start investigating network attacks surfaced by Vectra Detect directly from Sentinel. View critical hosts, accounts, campaigns and detections. Also monitor Vectra system health and audit logs.

**Required Data Types**

CommonSecurityLog

AIVectraDetect

## Analytic Rules

### Vectra AI Detect - Suspected Compromised Account

Create an incident when an Account is suspected to be compromised.

The higher the severity level is, the more immediate attention it requires as Vectra AI engine is more confident that this is a real threat.

Level of severity are: Low, Medium, High, Critical). Recommended configuration is to trigger an alert for at least High and Critical.

**Required Data Connectors**

AIVectraDetect

### Vectra AI Detect - Detections with High Severity

Create an incident for high severity malicious behavior detected by Vectra AI (Threat score superior to 7.0).

The Severity is a mapping with the Threat score assigned to a detection. It ranges between 0 and 10.

The severity\_threshold variable can be adjusted as desired.

**Required Data Connectors**

AIVectraDetect

### Vectra AI Detect - Suspected Compromised Host

Create an incident when a Host is suspected to be compromised.

The higher the severity level is, the more immediate attention it requires as Vectra AI engine is more confident that this is a real threat.

Level of severity are: Low, Medium, High, Critical). Recommended configuration is to trigger an alert for at least High and Critical.

**Required Data Connectors**

AIVectraDetect

### Vectra AI Detect - New Campaign Detected

Identifies when a new Campaign has been detected. This occurs when multiple Detections accross different Hosts are suspected to be part of the same Attack Campaign.

**Required Data Connectors**

AIVectraDetect

### Vectra AI Detect - Suspicious Behaviors

Create an incident for each new malicious behavior detected by Vectra Detect.

By default, it looks through all tactics. This can be modified to create incident only for a subset of tactics.

**Required Data Connectors**

AIVectraDetect

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# VirusTotal

Enriched information can help drive focused investigations in Security Operations.

**Data Connectors:** 0**, Workbooks:** 0**, Analytic Rules:** 0**, Hunting Queries:** 0**, Watchlists:** 0**, Playbooks:** 9, Parsers: 0

## Data Connectors

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

### URL Enrichment - Virus Total domain report - Alert Triggered

This playbook will take each URL entity and query VirusTotal for Domain info (https://developers.virustotal.com/v3.0/reference#domain-info).

### URL Enrichment - Virus Total domain report - Incident Triggered

This playbook will take each URL entity and query VirusTotal for Domain Report (https://developers.virustotal.com/v3.0/reference#domain-info). It will write the results to Log Analytics and add a comment to the incident.

### FileHash Enrichment - Virus Total report - Alert Triggered

This playbook will take each File Hash entity and query VirusTotal for file report (https://developers.virustotal.com/v3.0/reference#file-info).

### FileHash Enrichment - Virus Total report - Incident Triggered

This playbook will take each File Hash entity and query VirusTotal for file report (https://developers.virustotal.com/v3.0/reference#file-info).

### IP Enrichment - Virus Total report - Alert Triggered

This playbook will take each IP entity and query VirusTotal for IP Address Report (https://developers.virustotal.com/v3.0/reference#ip-info). It will write the results to Log Analytics and add a comment to the incident.

### IP Enrichment - Virus Total report - Incident Triggered

This playbook will take each IP entity and query VirusTotal for IP Address Report (https://developers.virustotal.com/v3.0/reference#ip-info). It will write the results to Log Analytics and add a comment to the incident.

### URL Enrichment - Virus Total report - Alert Triggered

This playbook will take each URL entity and query VirusTotal for info (https://developers.virustotal.com/v3.0/reference#url-info).

### URL Enrichment - Virus Total report - Incident Triggered

This playbook will take each URL entity and query VirusTotal for info (https://developers.virustotal.com/v3.0/reference#url-info).

### IP Enrichment - Virus Total Report - Entity Trigger

This playbook will query VirusTotal Report for the selected IP Address (https://developers.virustotal.com/v3.0/reference#ip-info). The report will be added as a comment to the incident

## Parsers

# VMware Carbon Black Cloud

The VMware Carbon Black Cloud solution for Microsoft Sentinel allows ingesting Carbon Black Audit, Notification and Event logs into Microsoft Sentinel.

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

## Data Connectors

### VMware Carbon Black Cloud (using Azure Function)

The [VMware Carbon Black Cloud](https://www.vmware.com/products/carbon-black-cloud.html) connector provides the capability to ingest Carbon Black data into Microsoft Sentinel. The connector provides visibility into Audit, Notification and Event logs in Microsoft Sentinel to view dashboards, create custom alerts, and to improve monitoring and investigation capabilities.

## Workbooks

### VMware Carbon Black Cloud

Sets the time name for analysis

**Required Data Types**

CarbonBlackEvents\_CL

CarbonBlackAuditLogs\_CL

CarbonBlackNotifications\_CL

VMwareCarbonBlack

## Analytic Rules

### Critical Threat Detected

This creates an incident in the event a critical threat was identified on a Carbon Black managed endpoint.

**Required Data Connectors**

VMwareCarbonBlack

### Known Malware Detected

This creates an incident when a known Malware is detected on a endpoint managed by a Carbon Black.

**Required Data Connectors**

VMwareCarbonBlack

## Hunting Queries

## Watchlists

## Playbooks

### Endpoint take action from Teams - Carbon Black

This playbook sends an adaptive card to the SOC Teams channel, lets the analyst decide on action: Quarantine the device or Update the policy. It posts a comment on the incident with the information collected from the Carbon Black and summary of the actions taken, and closes the incident if required.When a new Sentinel incident is created,this playbook gets triggered and performs below actions:

1. Fetches the devices information from CarbonBlack

2. Sends an adaptive card to the SOC Teams channel, let the analyst decide on action: Quarantine the device or Update the policy based on SOC action

![card example](https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/Solutions/CarbonBlack/Playbooks/CarbonBlack-TakeDeviceActionFromTeams/images/adaptiveCard.png?raw=true)

3. Add a comment to the incident with the information collected from the carbon black, summary of the actions taken and close the incident ![Comment example](https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/Solutions/CarbonBlack/Playbooks/CarbonBlack-TakeDeviceActionFromTeams/images/Incident\_Comment.png?raw=true)

### Isolate endpoint - Carbon Black

This playbook will quarantine the host in Carbon Black.When a new Sentinel incident is created,this playbook gets triggered and performs below actions:

1. Fetches the devices information from CarbonBlack

2. Quarantine the device

3. Enrich the incident with device information by fetching from CarbonBlack

![CarbonBlack-Enrich Incident With devices information](https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/Solutions/CarbonBlack/Playbooks/CarbonBlack-QuarantineDevice/images/Incident\_Comment.png?raw=true)

![CarbonBlack-Enrich Incident With devices information](https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/Solutions/CarbonBlack/Playbooks/CarbonBlack-QuarantineDevice/images/designerOverviewLight1.png?raw=true)

![CarbonBlack-Enrich Incident With devices information](https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/Solutions/CarbonBlack/Playbooks/CarbonBlack-QuarantineDevice/images/designerOverviewLight2.png?raw=true)

### Endpoint enrichment - Carbon Black

This playbook will collect device information from Carbon Black and post a report on the incident.When a new Sentinel incident is created,this playbook gets triggered and performs below actions

1. Fetches the devices information from CarbonBlack

2. Enrich the incident with device information by adding a comment to the incident

![Comment example](https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/Solutions/CarbonBlack/Playbooks/CarbonBlack-DeviceEnrichment/images/Incident\_Comment.PNG?raw=true)

![CarbonBlack-Enrich Incident With devices information](https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/Solutions/CarbonBlack/Playbooks/CarbonBlack-DeviceEnrichment/images/designerOverviewLight.png?raw=true)

## Parsers

# VMware ESXi

The VMware ESXi solution for Microsoft Sentinel enables you to ingest VMWare ESXi logs into Microsoft Sentinel.

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 11**, Hunting Queries:** 10**, Watchlists:** 0**, Playbooks:** 0, Parsers: 1

## Data Connectors

### VMware ESXi

The [VMware ESXi](https://www.vmware.com/products/esxi-and-esx.html) connector allows you to easily connect your VMWare ESXi logs with Microsoft Sentinel This gives you more insight into your organization's ESXi servers and improves your security operation capabilities.

## Workbooks

### VMware ESXi

Sets the time name for analysis

**Required Data Types**

## Analytic Rules

### VMware ESXi - Dormant VM started

Detects when dormant VM was started.

**Required Data Connectors**

VMwareESXi

### VMware ESXi - Low patch disk space

This rule is triggered when low patch disk store space is detected.

**Required Data Connectors**

VMwareESXi

### VMware ESXi - Low temp directory space

This rule is triggered when temp directory space is detected.

**Required Data Connectors**

VMwareESXi

### VMware ESXi - Multiple new VMs started

Detects when multiple new VMs were started.

**Required Data Connectors**

VMwareESXi

### VMware ESXi - Multiple VMs stopped

Detects when multiple VMs ware stopped by user.

**Required Data Connectors**

VMwareESXi

### VMware ESXi - New VM started

Detects when new VM was started.

**Required Data Connectors**

VMwareESXi

### VMware ESXi - Root impersonation

Detects when root impersonation occurs.

**Required Data Connectors**

VMwareESXi

### VMware ESXi - Root login

Detects when root user login from uncommon IP address.

**Required Data Connectors**

VMwareESXi

### VMware ESXi - Shared or stolen root account

Detects when shared or stolen root account.

**Required Data Connectors**

VMwareESXi

### VMware ESXi - Unexpected disk image

Detects unexpected disk image for VM.

**Required Data Connectors**

VMwareESXi

### VMware ESXi - VM stopped

Detects when VM was stopped.

**Required Data Connectors**

VMwareESXi

## Hunting Queries

### VMware ESXi - List of dormant users.

VMWareESXi Hunting Query 1

### VMware ESXi - Download errors

VMWareESXi Hunting Query 2

### VMware ESXi - NFC download activities

VMWareESXi Hunting Query 3

### VMware ESXi - Root logins failures

VMWareESXi Hunting Query 4

### VMware ESXi - Root logins

VMWareESXi Hunting Query 5

### VMware ESXi - List of unused VMs

VMWareESXi Hunting Query 6

### VMware ESXi - VM high resource load

VMWareESXi Hunting Query 7

### VMware ESXi - List of powered off VMs

VMWareESXi Hunting Query 8

### VMware ESXi - List of powered on VMs

VMWareESXi Hunting Query 9

### VMware ESXi - List of virtual disks (images)

VMWareESXi Hunting Query 10

## Watchlists

## Playbooks

## Parsers

### VMware ESXi Data Parser

Category: Samples

Function Alias: VMwareESXi

# VMware vCenter

The VMware vCenter Server solution allows you ingest logs from your vCenter platform using Syslog into Microsoft Sentinel.

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

## Data Connectors

### VMware vCenter

The [vCenter](https://www.vmware.com/in/products/vcenter-server.html) connector allows you to easily connect your vCenter server logs with Microsoft Sentinel. This gives you more insight into your organization's data centers and improves your security operation capabilities.

## Workbooks

### vCenter

**Required Data Types**

## Analytic Rules

### vCenter - Root impersonation

Detects when root impersonation occurs.

**Required Data Connectors**

vCenter

### VMware vCenter - Root login

Detects when root user login from uncommon IP address.

**Required Data Connectors**

vCenter

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### vCenter

Category: Samples

Function Alias: vCenter

# Watchlists Utilities Solution

The Watchlist Utilities solution for Microsoft Sentinel contains Playbooks that can help automate watchlist usage and integration with incident's management. These include use cases for adding entities (Hosts, IP, URL, User, etc.) to Microsoft Sentinel Wat

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

## Data Connectors

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

### Add Host To Watchlist - Alert Trigger

This playbook will add a host entity from the alert to a new or existing watchlist.

### Add Host To Watchlist - Incident Trigger

This playbook will add a Host entity to a new or existing watchlist.\*\*Logical flow to use this playbook\*\* 1. The analyst finished investigating an incident and one of its findings is a suspicious Host entity. 2. The analyst wants to enter this entity into a watchlist (can be from block list type or allowed list). 3. This playbook will run as a manual trigger from the full incident blade or the investigation graph blade, or automatically, and will add host to the selected watchlist.

### Add IP To Watchlist - Alert Trigger

This playbook will add a IP entity from the alert to a new or existing watchlist.

### Add IP To Watchlist - Incident Trigger

This playbook will add a IP entity to a new or existing watchlist.\*\*Logical flow to use this playbook\*\* 1. The analyst finished investigating an incident and one of its findings is a suspicious IP entity. 2. The analyst wants to enter this entity into a watchlist (can be from block list type or allowed list). 3. This playbook will run as a manual trigger from the full incident blade or the investigation graph blade, or automatically, and will add host to the selected watchlist.

### Add URL To Watchlist - Alert Trigger

This playbook will add a URL entity from the alert to a new or existing watchlist.

### Add URL To Watchlist - Incident Trigger

This playbook will add a URL entity to a new or existing watchlist.

### Add User To Watchlist - Alert Trigger

This playbook will add a user entity from the alert to a new or existing watchlist.

### Add User To Watchlist - Incident Trigger

This playbook will add a User entity to a new or existing watchlist.\*\*Logical flow to use this playbook\*\* 1. The analyst finished investigating an incident and one of its findings is a suspicious user entity. 2. The analyst wants to enter this entity into a watchlist (can be from block list type or allowed list). 3. This playbook will run as a manual trigger from the full incident blade or the investigation graph blade, or automatically, and will add host to the selected watchlist.

### Watchlist - Change Incident Severity and Title if User VIP - Alert Trigger

This playbook leverages Microsoft Sentinel Watchlists in order to adapt the incidents severity which include User entity and check it against VIP user list.

### Watchlist - Change Incident Severity and Title if User VIP - Incident Trigger

This playbook leverages Microsoft Sentinel Watchlists in order to adapt the incidents severity which include User entity and check it against VIP user list\*\*Logical flow to use this playbook\*\* For each User account included in the incident or alert (entities of type User): 1. Check if User is included in the watchlist. 2. If user is in the watchlist: a. Change the incident severity to Critical b. Modify the incident title that include the User name and the text- \*\*VIP User!!!\*\*

### Watchlists - Inform Subscription Owner

This playbook leverages Microsoft Sentinel Watchlists in order to get the relevant subscription owner contact details, and inform about an ASC alert that occured in that subscription. It uses Microsoft Teams and Office 365 Outlook as ways to inform the sub owner.Note: This playbook utilizes two features currently in Preview. \* Microsoft Sentinel Watchlists \* Microsoft Sentinel Incident Trigger <img src='https://github.com/Azure/Azure-Sentinel/blob/master/Solutions/Watchlists%20Utilities/Playbooks/Watchlist-InformSubowner-IncidentTrigger/images/designerView.png?raw=true'/>

### Watchlist - close incidents with safe IPs

This playbook leverages Microsoft Sentinel Watchlists in order to close incidents which include IP addresses considered safe.For each Ip address included in the alert (entities of type IP): 1. Check if IP is included in watchlist. - If IP is in the watchlist, consider the IP safe, \*\*Add it to Safe IPs array.\*\* - If IP is not in the watchlist, meaning that we are not sure it is safe, \*\*Add it to not Safe IPs array.\*\* 2. Add a comment to the incident the list of safe and not safe IPs found. 3. If the not safe list is empty (length == 0), close the incident as Benign Positive. \*\* Configurations \*\* - Configure the step 'Run query and list results with the identifiers of the Sentinel workspace where the watchlist is stored. - Configure the identity used in the 'Run query and list results' step with the Log Analytics Reader RBAC role on the Microsoft Sentinel resource group. - Configure the Managed Identity of the Logic App with the Microsoft Sentinel Responder RBAC role on the Microsoft Sentinel resource group. - The watchlist used in this example has at list one column named \*\*ipaddress\*\* which stores the safe address. See the csv file attached in this folder as an example. <img src='https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/Solutions/Watchlists%20Utilities/Playbooks/Watchlist-CloseIncidentKnownIPs/images/designerLight1.png'/> <img src='https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/Solutions/Watchlists%20Utilities/Playbooks/Watchlist-CloseIncidentKnownIPs/images/designerLight2.png'/> <img src='https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/Solutions/Watchlists%20Utilities/Playbooks/Watchlist-CloseIncidentKnownIPs/images/commentLight.png'/>

## Parsers

# Windows Firewall

The Windows Firewall solution for Microsoft Sentinel allows you to ingest Windows Firewall Events into Microsoft Sentinel using the Log Analytics agent for Windows

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

## Data Connectors

### Windows Firewall

Windows Firewall is a Microsoft Windows application that filters information coming to your system from the Internet and blocking potentially harmful programs. The software blocks most programs from communicating through the firewall. Users simply add a program to the list of allowed programs to allow it to communicate through the firewall. When using a public network, Windows Firewall can also secure the system by blocking all unsolicited attempts to connect to your computer.

## Workbooks

### Windows Firewall

Gain insights into Windows Firewall logs in combination with security and Azure signin logs

**Required Data Types**

WindowsFirewall

SecurityEvent

SigninLogs

SecurityEvents

WindowsFirewall

WindowsSecurityEvents

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Windows Forwarded Events

The Windows Forwarded Events solution allows you to ingest all Windows Event Forwarding (WEF) logs from the Windows Servers connected to your Microsoft Sentinel workspace using Azure Monitor Agent (AMA).

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

## Data Connectors

### Windows Forwarded Events

You can stream all Windows Event Forwarding (WEF) logs from the Windows Servers connected to your Microsoft Sentinel workspace using Azure Monitor Agent (AMA).

This connection enables you to view dashboards, create custom alerts, and improve investigation.

This gives you more insight into your organization’s network and improves your security operation capabilities. For more information, see the [Microsoft Sentinel documentation](https://go.microsoft.com/fwlink/p/?linkid=2219963&wt.mc\_id=sentinel\_dataconnectordocs\_content\_cnl\_csasci).

## Workbooks

## Analytic Rules

### Chia\_Crypto\_Mining IOC - June 2021

Identifies a match across IOC's related to Chia cryptocurrency farming/plotting activity

**Required Data Connectors**

WindowsForwardedEvents

### SOURGUM Actor IOC - July 2021

Identifies a match across IOC's related to an actor tracked by Microsoft as SOURGUM

**Required Data Connectors**

WindowsForwardedEvents

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Windows Security Events

The Windows Security Events solution for Microsoft Sentinel allows you to ingest Security events from your Windows machines using the Windows Agent into Microsoft Sentinel.

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

## Data Connectors

### Security Events via Legacy Agent

You can stream all security events from the Windows machines connected to your Microsoft Sentinel workspace using the Windows agent. This connection enables you to view dashboards, create custom alerts, and improve investigation. This gives you more insight into your organization’s network and improves your security operation capabilities. For more information, see the [Microsoft Sentinel documentation](https://go.microsoft.com/fwlink/p/?linkid=2220093&wt.mc\_id=sentinel\_dataconnectordocs\_content\_cnl\_csasci).

### Windows Security Events via AMA

You can stream all security events from the Windows machines connected to your Microsoft Sentinel workspace using the Windows agent. This connection enables you to view dashboards, create custom alerts, and improve investigation. This gives you more insight into your organization’s network and improves your security operation capabilities. For more information, see the [Microsoft Sentinel documentation](https://go.microsoft.com/fwlink/p/?linkid=2220225&wt.mc\_id=sentinel\_dataconnectordocs\_content\_cnl\_csasci).

## Workbooks

### Event Analyzer

The Event Analyzer workbook allows to explore, audit and speed up analysis of Windows Event Logs, including all event details and attributes, such as security, application, system, setup, directory service, DNS and others.

**Required Data Types**

SecurityEvent

SecurityEvents

WindowsSecurityEvents

### Identity & Access

Gain insights into Identity and access operations by collecting and analyzing security logs, using the audit and sign-in logs to gather insights into use of Microsoft products.

You can view anomalies and trends across login events from all users and machines. This workbook also identifies suspicious entities from login and access events.

**Required Data Types**

SecurityEvent

SecurityEvents

WindowsSecurityEvents

## Analytic Rules

### ADFS Database Named Pipe Connection

This detection uses Sysmon telemetry to detect suspicious local connections via a named pipe to the AD FS configuration database (Windows Internal Database).

In order to use this query you need to be collecting Sysmon EventIdD 18 (Pipe Connected).

If you do not have Sysmon data in your workspace this query will raise an error stating:

Failed to resolve scalar expression named "[@Name]"

**Required Data Connectors**

SecurityEvents

WindowsSecurityEvents

### AD FS Remote Auth Sync Connection

This detection uses Security events from the "AD FS Auditing" provider to detect suspicious authentication events on an AD FS server. The results then get

correlated with events from the Windows Filtering Platform (WFP) to detect suspicious incoming network traffic on port 80 on the AD FS server.

This could be a sign of a threat actor trying to use replication services on the AD FS server to get its configuration settings and extract

sensitive information such as AD FS certificates.

In order to use this query you need to enable AD FS auditing on the AD FS Server.

References:

https://docs.microsoft.com/windows-server/identity/ad-fs/troubleshooting/ad-fs-tshoot-logging

https://twitter.com/OTR\_Community/status/1387038995016732672

**Required Data Connectors**

SecurityEvents

WindowsSecurityEvents

### AD FS Remote HTTP Network Connection

This detection uses Sysmon events (NetworkConnect events) to detect incoming network traffic on port 80 on AD FS servers. This could be a sign of a threat actor

trying to use replication services on the AD FS server to get its configuration settings and extract sensitive information such as AD FS certificates.

In order to use this query you need to enable Sysmon telemetry on the AD FS Server.

Reference: https://twitter.com/OTR\_Community/status/1387038995016732672

**Required Data Connectors**

SecurityEvents

WindowsSecurityEvents

### Excessive Windows logon failures

User has over 50 Windows logon failures today and at least 33% of the count of logon failures over the previous 7 days.

**Required Data Connectors**

SecurityEvents

WindowsSecurityEvents

### Exchange OAB Virtual Directory Attribute Containing Potential Webshell

This query uses Windows Event ID 5136 in order to detect potential webshell deployment by exploitation of CVE-2021-27065.

This query looks for changes to the InternalHostName or ExternalHostName properties of Exchange OAB Virtual Directory objects in AD Directory Services

where the new objects contain potential webshell objects. Ref: https://aka.ms/ExchangeVulns

**Required Data Connectors**

SecurityEvents

WindowsSecurityEvents

### Gain Code Execution on ADFS Server via SMB + Remote Service or Scheduled Task

This query detects instances where an attacker has gained the ability to execute code on an ADFS Server through SMB and Remote Service or Scheduled Task.

**Required Data Connectors**

SecurityEvents

WindowsSecurityEvents

### AAD Local Device Join Information and Transport Key Registry Keys Access

This detection uses Windows security events to detect suspicious access attempts by the same process

to registry keys that provide information about an AAD joined or registered devices and Transport keys (tkpub / tkpriv).

This information can be used to export the Device Certificate (dkpub / dkpriv) and Transport key (tkpub/tkpriv).

These set of keys can be used to impersonate existing Azure AD joined devices.

This detection requires an access control entry (ACE) on the system access control list (SACL) of the following securable objects:

HKLM:\SYSTEM\CurrentControlSet\Control\CloudDomainJoin (AAD joined devices)

HKCU:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\WorkplaceJoin (AAD registered devices)

HKLM:\SYSTEM\CurrentControlSet\Control\Cryptography\Ngc\KeyTransportKey (Transport Key)

Make sure you set the SACL to propagate to its sub-keys. You can find more information in here https://github.com/OTRF/Set-AuditRule/blob/master/rules/registry/aad\_connect\_health\_service\_agent.yml

Reference: https://o365blog.com/post/deviceidentity/

**Required Data Connectors**

SecurityEvents

WindowsSecurityEvents

### SecurityEvent - Multiple authentication failures followed by a success

Identifies accounts who have failed to logon to the domain multiple times in a row, followed by a successful authentication

within a short time frame. Multiple failed attempts followed by a success can be an indication of a brute force attempt or

possible mis-configuration of a service account within an environment.

The lookback is set to 6h and the authentication window and threshold are set to 1h and 5, meaning we need to see a minimum

of 5 failures followed by a success for an account within 1 hour to surface an alert.

**Required Data Connectors**

SecurityEvents

WindowsSecurityEvents

### New EXE deployed via Default Domain or Default Domain Controller Policies

This detection highlights executables deployed to hosts via either the Default Domain or Default Domain Controller Policies. These policies apply to all hosts or Domain Controllers and best practice is that these policies should not be used for deployment of files.

A threat actor may use these policies to deploy files or scripts to all hosts in a domain.

**Required Data Connectors**

SecurityEvents

WindowsSecurityEvents

### Non Domain Controller Active Directory Replication

This query detects potential attempts by non-computer accounts (non domain controllers) to retrieve/synchronize an active directory object leveraging directory replication services (DRS).

A Domain Controller (computer account) would usually be performing these actions in a domain environment. Another detection rule can be created to cover domain controllers accounts doing at rare times.

A domain user with privileged permissions to use directory replication services is rare. Ref: https://threathunterplaybook.com/notebooks/windows/06\_credential\_access/WIN-180815210510.html

**Required Data Connectors**

SecurityEvents

WindowsSecurityEvents

### NRT Base64 encoded Windows process command-lines

Identifies instances of a base64 encoded PE file header seen in the process command line parameter.

**Required Data Connectors**

SecurityEvents

WindowsSecurityEvents

### NRT Process executed from binary hidden in Base64 encoded file

Encoding malicious software is a technique used to obfuscate files from detection.

The first CommandLine component is looking for Python decoding base64.

The second CommandLine component is looking for Bash/sh command line base64 decoding.

The third one is looking for Ruby decoding base64.

**Required Data Connectors**

SecurityEvents

WindowsSecurityEvents

### NRT Security Event log cleared

Checks for event id 1102 which indicates the security event log was cleared.

It uses Event Source Name "Microsoft-Windows-Eventlog" to avoid generating false positives from other sources, like AD FS servers for instance.

**Required Data Connectors**

SecurityEvents

WindowsSecurityEvents

### AD user enabled and password not set within 48 hours

Identifies when an account is enabled with a default password and the password is not set by the user within 48 hours.

Effectively, there is an event 4722 indicating an account was enabled and within 48 hours, no event 4723 occurs which

indicates there was no attempt by the user to set the password. This will show any attempts (success or fail) that occur

after 48 hours, which can indicate too long of a time period in setting the password to something that only the user knows.

It is recommended that this time period is adjusted per your internal company policy.

**Required Data Connectors**

SecurityEvents

WindowsSecurityEvents

### Potential Fodhelper UAC Bypass

This detection looks for the steps required to conduct a UAC bypass using Fodhelper.exe. By default this detection looks for the setting of the required registry keys and the invoking of the process within 1 hour - this can be tweaked as required.

**Required Data Connectors**

SecurityEvents

WindowsSecurityEvents

### Potential re-named sdelete usage

This detection looks for command line parameters associated with the use of Sysinternals sdelete (https://docs.microsoft.com/sysinternals/downloads/sdelete) to delete multiple files on a host's C drive.

A threat actor may re-name the tool to avoid detection and then use it for destructive attacks on a host.

**Required Data Connectors**

SecurityEvents

WindowsSecurityEvents

### Scheduled Task Hide

This query detects attempts by malware to hide the scheduled task by deleting the SD (Security Descriptor) value. Removal of SD value results in the scheduled task disappearing from schtasks /query and Task Scheduler.

The query requires auditing to be turned on for HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree registry hive as well as audit policy for registry auditing to be turned on.

Reference: https://www.microsoft.com/security/blog/2022/04/12/tarrask-malware-uses-scheduled-tasks-for-defense-evasion/

Reference: https://4sysops.com/archives/audit-changes-in-the-windows-registry/

**Required Data Connectors**

SecurityEvents

WindowsSecurityEvents

### Sdelete deployed via GPO and run recursively

This query looks for the Sdelete process being run recursively after being deployed to a host via GPO. Attackers could use this technique to deploy Sdelete to multiple host and delete data on them.

**Required Data Connectors**

SecurityEvents

WindowsSecurityEvents

### Starting or Stopping HealthService to Avoid Detection

This query detects events where an actor is stopping or starting HealthService to disable telemetry collection/detection from the agent.

The query requires a SACL to audit for access request to the service.

**Required Data Connectors**

SecurityEvents

WindowsSecurityEvents

### Process execution frequency anomaly

Identifies anomalous spike in frequency of executions of sensitive processes which are often leveraged as attack vectors.

The query leverages KQL built-in anomaly detection algorithms to find large deviations from baseline patterns.

Sudden increases in execution frequency of sensitive processes should be further investigated for malicious activity.

Tune the values from 1.5 to 3 in series\_decompose\_anomalies for further outliers or based on custom threshold values for score.

**Required Data Connectors**

SecurityEvents

WindowsSecurityEvents

## Hunting Queries

### Commands executed by WMI on new hosts - potential Impacket

Windows Security Events Hunting Query 1

### Crash dump disabled on host

Windows Security Events Hunting Query 2

### Cscript script daily summary breakdown

Windows Security Events Hunting Query 3

### VIP account more than 6 failed logons in 10

Windows Security Events Hunting Query 4

### Decoy User Account Authentication Attempt

Windows Security Events Hunting Query 5

### Discord download invoked from cmd line

Windows Security Events Hunting Query 6

### Enumeration of users and groups

Windows Security Events Hunting Query 7

### Exchange PowerShell Snapin Added

Windows Security Events Hunting Query 8

### Summary of failed user logons by reason of failure

Windows Security Events Hunting Query 9

### Group added to Built in Domain Local or Global Group

Windows Security Events Hunting Query 10

### Host Exporting Mailbox and Removing Export

Windows Security Events Hunting Query 11

### Hosts with new logons

Windows Security Events Hunting Query 12

### Invoke-PowerShellTcpOneLine Usage.

Windows Security Events Hunting Query 13

### Least Common Parent And Child Process Pairs

Windows Security Events Hunting Query 14

### Least Common Processes by Command Line

Windows Security Events Hunting Query 15

### Least Common Processes Including Folder Depth

Windows Security Events Hunting Query 16

### Masquerading files

Windows Security Events Hunting Query 17

### Potential Exploitation of MS-RPRN printer bug

Windows Security Events Hunting Query 18

### Multiple explicit credential usage - 4648 events

Windows Security Events Hunting Query 19

### New Child Process of W3WP.exe

Windows Security Events Hunting Query 20

### New processes observed in last 24 hours

Windows Security Events Hunting Query 21

### Nishang Reverse TCP Shell in Base64

Windows Security Events Hunting Query 22

### Summary of users created using uncommon/undocumented commandline switches

Windows Security Events Hunting Query 23

### Powercat Download

Windows Security Events Hunting Query 24

### PowerShell downloads

Windows Security Events Hunting Query 25

### New PowerShell scripts encoded on the commandline

Windows Security Events Hunting Query 26

### Entropy for Processes for a given Host

Windows Security Events Hunting Query 27

### Rare processes run by Service accounts

Windows Security Events Hunting Query 28

### Rare Process Path

Windows Security Events Hunting Query 29

### Hosts running a rare process with commandline

Windows Security Events Hunting Query 30

### Hosts running a rare process

Windows Security Events Hunting Query 31

### Service installation from user writable directory

Windows Security Events Hunting Query 32

### Suspected LSASS Dump

Windows Security Events Hunting Query 33

### Suspicious enumeration using Adfind tool

Windows Security Events Hunting Query 34

### Suspicious Windows Login outside normal hours

Windows Security Events Hunting Query 35

### Uncommon processes - bottom 5%

Windows Security Events Hunting Query 36

### Summary of user logons by logon type

Windows Security Events Hunting Query 37

### User Account added to Built in Domain Local or Global Group

Windows Security Events Hunting Query 38

### Long lookback User Account Created and Deleted within 10mins

Windows Security Events Hunting Query 39

### User account added or removed from a security group by an unauthorized user

Windows Security Events Hunting Query 40

### User created by unauthorized user

Windows Security Events Hunting Query 41

### VIP account more than 6 failed logons in 10

Windows Security Events Hunting Query 42

### Windows System Time changed on hosts

Windows Security Events Hunting Query 43

## Watchlists

## Playbooks

## Parsers

# Windows Server DNS

The Windows Server DNS solution for Microsoft Sentinel allows you to ingest DNS analytic and audit logs into Microsoft Sentinel. The DNS logs are collected only from Windows agents.

**Data Connectors:** 2**, Workbooks:** 1**, Analytic Rules:** 5**, Hunting Queries:** 9**, Watchlists:** 0**, Playbooks:** 0, Parsers: 0

## Data Connectors

### DNS

The DNS log connector allows you to easily connect your DNS analytic and audit logs with Microsoft Sentinel, and other related data, to improve investigation.

\*\*When you enable DNS log collection you can:\*\*

- Identify clients that try to resolve malicious domain names.

- Identify stale resource records.

- Identify frequently queried domain names and talkative DNS clients.

- View request load on DNS servers.

- View dynamic DNS registration failures.

For more information, see the [Microsoft Sentinel documentation](https://go.microsoft.com/fwlink/p/?linkid=2220127&wt.mc\_id=sentinel\_dataconnectordocs\_content\_cnl\_csasci).

### Windows DNS Events via AMA (Preview)

The Windows DNS log connector allows you to easily filter and stream all analytics logs from your Windows DNS servers to your Microsoft Sentinel workspace using the Azure Monitoring agent (AMA). Having this data in Microsoft Sentinel helps you identify issues and security threats such as:

- Trying to resolve malicious domain names.

- Stale resource records.

- Frequently queried domain names and talkative DNS clients.

- Attacks performed on DNS server.

You can get the following insights into your Windows DNS servers from Microsoft Sentinel:

- All logs centralized in a single place.

- Request load on DNS servers.

- Dynamic DNS registration failures.

Windows DNS events are supported by Advanced SIEM Information Model (ASIM) and stream data into the ASimDnsActivityLogs table. [Learn more](https://docs.microsoft.com/azure/sentinel/normalization).

For more information, see the [Microsoft Sentinel documentation](https://go.microsoft.com/fwlink/p/?linkid=2225993&wt.mc\_id=sentinel\_dataconnectordocs\_content\_cnl\_csasci).

## Workbooks

### DNS

Gain extensive insight into your organization's DNS by analyzing, collecting and correlating all DNS events.

This workbook exposes a variety of information about suspicious queries, malicious IP addresses and domain operations.

**Required Data Types**

DnsInventory

DnsEvents

DNS

## Analytic Rules

### Potential DGA detected

Identifies clients with a high NXDomain count which could be indicative of a DGA (cycling through possible C2 domains

where most C2s are not live). Alert is generated when a new IP address is seen (based on not being seen associated with

NXDomain records in prior 10-day baseline period).

**Required Data Connectors**

DNS

### Rare client observed with high reverse DNS lookup count

Identifies clients with a high reverse DNS counts which could be carrying out reconnaissance or discovery activity.

Alert is generated if the IP performing such reverse DNS lookups was not seen doing so in the preceding 7-day period.

**Required Data Connectors**

DNS

### DNS events related to mining pools

Identifies IP addresses that may be performing DNS lookups associated with common currency mining pools.

**Required Data Connectors**

DNS

### DNS events related to ToR proxies

Identifies IP addresses performing DNS lookups associated with common ToR proxies.

**Required Data Connectors**

DNS

### NRT DNS events related to mining pools

Identifies IP addresses that may be performing DNS lookups associated with common currency mining pools.

**Required Data Connectors**

DNS

## Hunting Queries

### DNS lookups for commonly abused TLDs

Windows Server DNS Hunting Query 1

### DNS - domain anomalous lookup increase

Windows Server DNS Hunting Query 2

### DNS Full Name anomalous lookup increase

Windows Server DNS Hunting Query 3

### Potential DGA detected

Windows Server DNS Hunting Query 4

### High reverse DNS count by host

Windows Server DNS Hunting Query 5

### Abnormally long DNS URI queries

Windows Server DNS Hunting Query 6

### DNS Domains linked to WannaCry ransomware campaign

Windows Server DNS Hunting Query 7

### Solorigate DNS Pattern

Windows Server DNS Hunting Query 8

### Solorigate Encoded Domain in URL

Windows Server DNS Hunting Query 9

## Watchlists

## Playbooks

## Parsers

# WireX Network Forensics Platform for Microsoft Sentinel

WireX Systems threat detection and response provides easy to use forensics context, delivering months of in-depth visibility to efficiently reveal the scope and impact of security incidents.

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

## Data Connectors

### WireX Network Forensics Platform

The WireX Systems data connector allows security professional to integrate with Azure Sentinel to allow you to further enrich your forensics investigations; to not only encompass the contextual content offered by WireX but to analyze data from other sources, and to create custom dashboards to give the most complete picture during a forensic investigation and to create custom workflows.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# WithSecure™ Elements via Connector for Microsoft Sentinel

WithSecure™ Elements EPP/EDR, an Endpoint Protection and Response (EPR) solution, provides complete Endpoint Security. This integration allows to correlate a rich set of security events (EDR incident, malware, firewall, tampering…) with other sources.

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

## Data Connectors

### WithSecure Elements via Connector

WithSecure Elements is a unified cloud-based cyber security platform.

By connecting WithSecure Elements via Connector to Microsoft Sentinel, security events can be received in Common Event Format (CEF) over syslog.

It requires deploying "Elements Connector" either on-prem or in cloud.

The Common Event Format (CEF) provides natively search & correlation, alerting and threat intelligence enrichment for each data log.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Workplace from Facebook

Ingest common Workplace events into Microsoft Sentinel through Webhooks

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

## Data Connectors

### Workplace from Facebook (using Azure Function)

The [Workplace](https://www.workplace.com/) data connector provides the capability to ingest common Workplace events into Azure Sentinel through Webhooks. Webhooks enable custom integration apps to subscribe to events in Workplace and receive updates in real time. When a change occurs in Workplace, an HTTPS POST request with event information is sent to a callback data connector URL. Refer to [Webhooks documentation](https://developers.facebook.com/docs/workplace/reference/webhooks) for more information. The connector provides ability to get events which helps to examine potential security risks, analyze your team's use of collaboration, diagnose configuration problems and more.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### Workplace\_Facebook

Category: Samples

Function Alias: Workplace\_Facebook

# Zero Networks Segment for Microsoft Sentinel

This solution contains data connectors, parser, workbook, playbooks, analytic rules and hunting queries for Zero Networks Segment audit logs in Microsoft Sentinel

**Data Connectors:** 2**, Workbooks:** 1**, Analytic Rules:** 3**, Hunting Queries:** 4**, Watchlists:** 0**, Playbooks:** 3, Parsers: 1

## Data Connectors

### Zero Networks Segment Audit

The [Zero Networks Segment](https://zeronetworks.com/) Audit data connector provides the capability to ingest Zero Networks Audit events into Microsoft Sentinel through the REST API. This data connector uses Microsoft Sentinel native polling capability.

### Zero Networks Segment Audit (Function) (using Azure Function)

The [Zero Networks Segment](https://zeronetworks.com/product/) Audit data connector provides the capability to ingest Audit events into Microsoft Sentinel through the REST API. Refer to API guide for more information. The connector provides ability to get events which helps to examine potential security risks, analyze your team's use of collaboration, diagnose configuration problems and more.

## Workbooks

### Zero NetWork

None.

**Required Data Types**

ZNAccessOrchestratorAudit\_CL

ZNAccessOrchestratorAuditNativePoller\_CL

ZeroNetworksAccessOrchestratorAuditFunction

ZeroNetworksAccessOrchestratorAuditNativePoller

Analytic Rules

### Zero Networks Segement - Machine Removed from protection

Detects when a machine is removed from protection.

**Required Data Connectors**

ZeroNetworksSegmentAuditFunction

ZeroNetworksSegmentAuditNativePoller

### Zero Networks Segment - New API Token created

Detects when a api token has been created.

**Required Data Connectors**

ZeroNetworksSegmentAuditFunction

ZeroNetworksSegmentAuditNativePoller

### Zero Networks Segment - Rare JIT Rule Creation

Identifies when a JIT Rule connection is new or rare by a given account today based on comparison with the previous 14 days.

JIT Rule creations are indicated by the Activity Type Id 20

**Required Data Connectors**

ZeroNetworksSegmentAuditFunction

ZeroNetworksSegmentAuditNativePoller

## Hunting Queries

### Zero Networks Segment - Excessive access by user

ZeroNetworks Hunting Query 1

### Zero Networks Segment - Excessive access to a built-in group by user

ZeroNetworks Hunting Query 2

### Zero Networks Segment - Inbound Block Rules Deleted

ZeroNetworks Hunting Query 3

### Zero Networks Segment - Outbound Block Rules Deleted

ZeroNetworks Hunting Query 4

## Watchlists

## Playbooks

### Add Asset to Protection - Zero Networks Segment

This playbook takes a host from a Microsoft Sentinel incident and adds it to protection. The playbook is configured to add the machine to protection(learning). If you want to have it go straight to protection, remove the protectAt property in the action.1. For the hosts in the incident, each host is added to protection (learning). 2. A comment is added to Microsoft Sentinel incident.

### Add Block Outbound Rule - Zero Networks Acccess Orchestrator

This playbook allows blocking an IP outbound from protected assets in Zero Networks Segment.1. For the IPs, we add them to a new outbound block rule in Segment. 2. A comment is added to Microsoft Sentinel incident.

### Enrich Incident - Zero Networks Acccess Orchestrator

This playbook will take each Host entity and get its Asset status from Zero Network Segment. The playbook will then write a comment to the Microsoft Sentinel incident with a table of assets and protection statuses.1. For the hosts, we get their asset satus from the REST API. 2. A comment is added to Microsoft Sentinel incident.

## Parsers

### ZNSegmentAudit

Category: Samples

Function Alias: ZNSegmentAudit

# Zero Trust (TIC 3.0) Solution

The Zero Trust (TIC 3.0) Workbook provides a mechanism for viewing log queries aligned to Zero Trust and Trusted Internet Connections models across Microsoft portfolio including Microsoft security offerings, Office 365, Teams and many more.

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

## Data Connectors

## Workbooks

### ZeroTrust(TIC3.0)

**Required Data Types**

## Analytic Rules

### ZeroTrust(TIC3.0) Control Assessment Posture Change

Zero Trust(TIC3.0) Control Assessments have Deviated from Configured Threshold Baselines

**Required Data Connectors**

(none listed)

## Hunting Queries

## Watchlists

## Playbooks

### Notify-GovernanceComplianceTeam

This Security Orchestration, Automation, & Response (SOAR) capability is designed for configuration with the solution's analytics rules. When analytics rules trigger this automation notifies the governance compliance team of respective details via Teams chat and exchange email. This automation reduces requirements to manually monitor the workbook or analytics rules while increasing response times.

### Create-AzureDevOpsTask

This playbook will create the Azure DevOps task filled with the Microsoft Sentinel incident details.

### Create Jira Issue

This playbook will open a Jira Issue when a new incident is opened in Microsoft Sentinel.

## Parsers

# Zimperium MTD for Sentinel

Zimperium Mobile Threat Defense connector gives you the ability to connect the Zimperium threat log with Microsoft Sentinel to view dashboards, create custom alerts, and improve investigation.

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

## Data Connectors

### Zimperium Mobile Threat Defense

Zimperium Mobile Threat Defense connector gives you the ability to connect the Zimperium threat log with Azure Sentinel to view dashboards, create custom alerts, and improve investigation. This gives you more insight into your organization's mobile threat landscape and enhances your security operation capabilities.

## Workbooks

### Zimperium Mobile Threat Defense (MTD)

This workbook provides insights on Zimperium Mobile Threat Defense (MTD) threats and mitigations.

**Required Data Types**

ZimperiumThreatLog\_CL

ZimperiumMitigationLog\_CL

ZimperiumMtdAlerts

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# ZINC Open Source Threat Protection

Microsoft security research teams have detected a wide range of social engineering campaigns using weaponized legitimate open-source software by an actor tracked as ZINC Open Source Threat Protection.

**Data Connectors:** 0**, Workbooks:** 0**, Analytic Rules:** 3**, Hunting Queries:** 0**, Watchlists:** 0**, Playbooks:** 0, Parsers: 0

## Data Connectors

## Workbooks

## Analytic Rules

### AV detections related to Zinc actors

This query looks for Microsoft Defender AV detections related to Zinc threat actor. In Microsoft Sentinel the SecurityAlerts table includes only the Device Name of the affected device,

this query joins the DeviceInfo table to clearly connect other information such as Device group, ip, etc.

This would allow the Microsoft Sentinel analyst to have more context related to the alert, if available.

Reference: https://www.microsoft.com/security/blog/2022/09/29/zinc-weaponizing-open-source-software/

**Required Data Connectors**

MicrosoftThreatProtection

### Zinc Actor IOCs files - October 2022

Identifies a match across filename and commandline IOC's related to an actor tracked by Microsoft as Zinc.

Reference: https://www.microsoft.com/security/blog/2022/09/29/zinc-weaponizing-open-source-software/

**Required Data Connectors**

MicrosoftThreatProtection

SecurityEvents

WindowsSecurityEvents

### Zinc Actor IOCs domains hashes IPs and useragent - October 2022

Identifies a match across domainname, IP, hash and useragent IOCs related to an actor tracked by Microsoft as Zinc.

Reference: https://www.microsoft.com/security/blog/2022/09/29/zinc-weaponizing-open-source-software/

**Required Data Connectors**

DNS

AzureMonitor(VMInsights)

F5

CiscoASA

PaloAltoNetworks

Fortinet

CheckPoint

CEF

MicrosoftThreatProtection

SecurityEvents

Office365

AzureFirewall

WindowsFirewall

WindowsSecurityEvents

WindowsForwardedEvents

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

# Zoom Reports

The Zoom Reports solution enables you to ingest Zoom Reports events into Microsoft Sentinel through the Zoom Report REST API.

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

## Data Connectors

### Zoom Reports (using Azure Function)

The [Zoom](https://zoom.us/) Reports data connector provides the capability to ingest [Zoom Reports](https://marketplace.zoom.us/docs/api-reference/zoom-api/reports/) events into Microsoft Sentinel through the REST API. Refer to [API documentation](https://marketplace.zoom.us/docs/api-reference/introduction) for more information. The connector provides ability to get events which helps to examine potential security risks, analyze your team's use of collaboration, diagnose configuration problems and more.

## Workbooks

## Analytic Rules

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### Zoom

Category: Samples

Function Alias: Zoom

# Zscaler Internet Access for Microsoft Sentinel

This solution package simplifies customer's deployment of their Zscaler Internet Access (ZIA) logs for ingestion into a customer's Microsoft Sentinel workspace.

**Data Connectors:** 1**, Workbooks:** 4**, Analytic Rules:** 2**, Hunting Queries:** 0**, Watchlists:** 0**, Playbooks:** 0, Parsers: 2

## Data Connectors

### Zscaler

The Zscaler data connector allows you to easily connect your Zscaler Internet Access (ZIA) logs with Microsoft Sentinel, to view dashboards, create custom alerts, and improve investigation. Using Zscaler on Microsoft Sentinel will provide you more insights into your organization’s Internet usage, and will enhance its security operation capabilities.​

## Workbooks

### Zscaler Firewall

Gain insights into your ZIA cloud firewall logs by connecting to Microsoft Sentinel.

The Zscaler firewall overview workbook provides an overview and ability to drill down into all cloud firewall activity in your Zscaler instance including non-web related networking events, security events, firewall rules, and bandwidth consumption

**Required Data Types**

### Zscaler Office365 Apps

Gain insights into Office 365 use on your network.

The Zscaler Office 365 overview workbook shows you the Microsoft apps running on your network and their individual bandwidth consumption. It also helps identify phishing attempts in which attackers disguised themselves as Microsoft services.

**Required Data Types**

### Zscaler Threats

Gain insights into threats blocked by Zscaler Internet access on your network.

The Zscaler threat overview workbook shows your entire threat landscape including blocked malware, IPS/AV rules, and blocked cloud apps. Threats are displayed by threat categories, filetypes, inbound vs outbound threats, usernames, user location, and more.

**Required Data Types**

### Zscaler Web Overview

Gain insights into your ZIA web logs by connecting to Microsoft Sentinel.

The Zscaler web overview workbook provides a bird's eye view and ability to drill down into all the security and networking events related to web transactions, types of devices, and bandwidth consumption.

**Required Data Types**

## Analytic Rules

### Discord CDN Risky File Download

Identifies callouts to Discord CDN addresses for risky file extensions. This detection will trigger when a callout for a risky file

is made to a discord server that has only been seen once in your environment. Unique discord servers are identified using the server ID

that is included in the request URL (DiscordServerId in query). Discord CDN has been used in multiple campaigns to download additional payloads

**Required Data Connectors**

Zscaler

### Request for single resource on domain

This will look for connections to a domain where only a single file is requested, this is unusual as most modern web applications require additional recources. This type of activity is often assocaited with malware beaconing or tracking URL's delivered in emails. Developed for Zscaler but applicable to any outbound web logging.

**Required Data Connectors**

Zscaler

## Hunting Queries

## Watchlists

## Playbooks

## Parsers

### ZScalerFW\_Parser

Category: Samples

Function Alias: ZScalerFW\_Parser

### ZScalerWeb\_Parser

Category: Samples

Function Alias: ZScalerWeb\_Parser

# Zscaler Private Access

The Zscaler Private Access (ZPA) data connector provides the capability to ingest Zscaler Private Access events into Microsoft Sentinel.

**Data Connectors:** 1**, Workbooks:** 1**, Analytic Rules:** 10**, Hunting Queries:** 10**, Watchlists:** 0**, Playbooks:** 0, Parsers: 1

## Data Connectors

### Zscaler Private Access

The [Zscaler Private Access (ZPA)](https://help.zscaler.com/zpa/what-zscaler-private-access) data connector provides the capability to ingest [Zscaler Private Access events](https://help.zscaler.com/zpa/log-streaming-service) into Microsoft Sentinel. Refer to [Zscaler Private Access documentation](https://help.zscaler.com/zpa) for more information.

## Workbooks

### Zscaler Private Access (ZPA)

Select the time range for this Overview.

**Required Data Types**

ZPA\_CL

ZscalerPrivateAccess

## Analytic Rules

### Zscaler - Shared ZPA session

Detects shared ZPA session.

**Required Data Connectors**

ZscalerPrivateAccess

### Zscaler - Unexpected event count of rejects by policy

Detects unexpected event count of rejects by policy.

**Required Data Connectors**

ZscalerPrivateAccess

### Zscaler - Forbidden countries

Detects suspicious ZPA connections from forbidden countries.

**Required Data Connectors**

ZscalerPrivateAccess

### Zscaler - Unexpected update operation

Detects unexpected version of update operation.

**Required Data Connectors**

ZscalerPrivateAccess

### Zscaler - Connections by dormant user

Detects ZPA connections by dormant user.

**Required Data Connectors**

ZscalerPrivateAccess

### Zscaler - ZPA connections by new user

Detects ZPA connections by new user.

**Required Data Connectors**

ZscalerPrivateAccess

### Zscaler - ZPA connections from new country

Detects ZPA connections from new country.

**Required Data Connectors**

ZscalerPrivateAccess

### Zscaler - ZPA connections from new IP

Detects ZPA connections from new IP.

**Required Data Connectors**

ZscalerPrivateAccess

### Zscaler - ZPA connections outside operational hours

Detects ZAP connections outside operational hours.

**Required Data Connectors**

ZscalerPrivateAccess

### Zscaler - Unexpected ZPA session duration

Detects Unexpected ZPA session duration.

**Required Data Connectors**

ZscalerPrivateAccess

## Hunting Queries

### Zscaler - Abnormal total bytes size

Zscaler Private Access (ZPA) Hunting Query 1

### Zscaler - Applications using by accounts

Zscaler Private Access (ZPA) Hunting Query 2

### Zscaler - Connection close reasons

Zscaler Private Access (ZPA) Hunting Query 3

### Zscaler - Destination ports by IP

Zscaler Private Access (ZPA) Hunting Query 4

### Zscaler - Users by source location countries

Zscaler Private Access (ZPA) Hunting Query 5

### Zscaler - Top connectors

Zscaler Private Access (ZPA) Hunting Query 6

### Zscaler - Top source IP

Zscaler Private Access (ZPA) Hunting Query 7

### Zscaler - Rare urlhostname requests

Zscaler Private Access (ZPA) Hunting Query 8

### Zscaler - Users access groups

Zscaler Private Access (ZPA) Hunting Query 9

### Zscaler - Server error by user

Zscaler Private Access (ZPA) Hunting Query 10

## Watchlists

## Playbooks

## Parsers

### Zscaler Private Access Data Parser

Category: Samples

Function Alias: ZPAEvent