# SONICWALL®

# Microsoft Sentinel with SonicWall Firewall Integration Guide

This document describes how SonicWall firewall integrates with Microsoft Sentinel. Combining these two tools can significantly enhance your security operations.

Understanding the Microsoft Sentinel and SonicWall Firewall:

- **Microsoft Sentinel** is a scalable, cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution. Microsoft Sentinel solutions provide a consolidated way to acquire Microsoft Sentinel content like data connectors, workbooks, analytics, and automations in user's workspace with a single deployment step.
- SonicWall next-generation firewalls (NGFW) provide the security, control, and visibility you need to maintain an effective cybersecurity posture. With solutions designed for networks of all sizes, SonicWall's award-winning hardware and advanced technology are built into each firewall to give you the edge on evolving threats.

#### Topics:

- Functionality
- Configuration
- Microsoft Sentinel Content Type
- SonicWall Support

## Functionality

The integration of SonicWall next-gen Firewalls with Microsoft Sentinel provides the capability to ingest SonicWall access logs (in syslog format) into Microsoft Sentinel. These integration capabilities enable our partners and customers to forward the firewall logs to Microsoft Sentinel, parse the logs and create custom workflows, and automate the responses.

Data Sources for Microsoft Sentinel in SonicWall firewall integration with Azure Sentinel:

- Microsoft Sentinel comes with several connectors for Microsoft solutions, including Microsoft Threat Protection, Microsoft 365 sources (such as Office 365, Azure AD, and Azure ATP), and more.
- Microsoft Sentinel uses standard syslog as the data source (Common Event Format or CEF) for non-Microsoft solutions like SonicWall.

• To ingest SonicAlert access logs into Azure Sentinel, we will set up a syslog forwarder on a Linux machine (which can be a VM on Azure or a physical machine on-premises).

# Configuration

Follow the below steps to configure Microsoft Sentinel with SonicWall firewall:

- 1. Deploying a Microsoft Sentinel Workspace
- 2. Installing the SonicWall Solution for Microsoft Sentinel
- 3. Installing the Operations Management Suite (OMS) or Log Analytics Agent
- 4. Configuring a Syslog Server on SonicWall Device
- 5. Validating the Data that Reaches Workspace

### Deploying a Microsoft Sentinel Workspace

#### To deploy a Microsoft Sentinel workspace:

- 1. Create a new resource using **deploy a custom template** that builds the resources needed for Microsoft Sentinel.
- 2. Select **QuickStart** mode template and create or select resource group. Let deployment to be completed.
- 3. Do one of the following:
  - Navigate to the resource group.
  - Click the Log Analytics workspace resource.
- Navigate to the Microsoft Sentinel service on Azure Home page.
   If Microsoft Sentinel service is not presented on the home page, click More services.

= Microsoft Azure	$\mathcal P$ Search resources, services, and do
All services	
All	sentinel X Service providers : All Release Status : All
Favorites	Microsoft Sentinel
Recents	Resource type: microsoft.securityinsightsarg/sentinel
Recommended	Give feedback
Categories	R* Help improve this page
AI + machine learning	
Analytics	

5. Click the Sentinel instance within the resource group you created.

### Installing the SonicWall Solution for Microsoft Sentinel

#### To install the SonicWall solution for Microsoft Sentinel:

- 1. Click the Sentinel instance within the resource group you created.
- 2. Install the SonicWall solution from the Content hub:
  - a. Navigate to **Content management > Content hub**.
  - b. Search for SonicWall.
  - c. Select the SonicWall Network Security Solution and click Install.

Dashboard > Microsoft Sentinel						
Selected workspace: 'swaroop-sentine!'	Content hub					×
P Search «	🖒 Refresh 🛓 Install/Update 🗎 Delete 🕂 S	IEM Migration 🛛 🔗 Guides & Feedb	ack			
General	- 247 - 272					
Overview	Solutions Standalone contents	Installed Updates				
🧬 Logs						2
👄 News & guides	♀ sonicwall ×				SonicWall Network Security	
🔎 Search	Status : All Content type : All Support : All	Provider : All Category : All	Content sources : All	88 🗮	SonicWall SonicWall 3.1.0	
Threat management					Provider Support Version	
Incidents	Content title	Status	Content source Provi	ider Support	a birds-eye view across their network alleviating the stress of increasingly sophisticated attacks, increasing volumes of	f 1
Morkbooks	SonicWall Network Security		Solution Sonk	cWall SonicWall	alerts, and long resolution timeframes.	
Hunting						
Notebooks					Content type	
Entity behavior					Analytics rule Data connector Hunting query	- 1
3 Threat intelligence					I Workbook	
MITRE ATT&CK (Preview)					Catagoogi (D	
Content management					Security - Network	
Content hub					Pricing ①	
<ul> <li>Repositories (Preview)</li> </ul>	4			)	Free	
<ul> <li>Community</li> </ul>	< Previous Page 1 V of 1 Next >	Showing 1 to 1 of 1 results.			Contraction of the second seco	

3. Configure the Common Event Format (CEF) via AMA data connector's data collection rule to set the event filter types (Syslog facilities) to collect.

Home > Microsoft	Sentinel > Microso	oft Sentinel   Data connectors	>
Common E	vent Forma	at (CEF) via AMA	
Common	Event Format (CE	F) via AMA	Prerequisites
Connected Status	X Microsoft Provider	4 Days Ago Last Log Received	To integrate with Common Event Format (CEF) via AMA make sure you have:
Description Common Event Form Syslog messages, use	at (CEF) is an industr	y standard format on top of rendors to allow event	To collect data from non-Azure VMs, they must have Azure Arc installed and enabled. Learn more
interoperability amou logs to Microsoft Ser correlation, alerting,	ng different platforms ntinel, you can take ac and threat intelligenc	s. By connecting your CEF dvantage of search & ce enrichment for each log.	Configuration Enable data collection rule
Last data received 4/3/2024, 4:46:43 PM			CEF Events logs are collected only from Linux agents.
Related content	63.4		O Refresh
Workbooks	(47) Queries	<ul> <li>O</li> <li>Analytics rules templates</li> </ul>	Rule name Event filter type
Data received		Go to log analytics	SysLog_Collection_Rule log_local0 : LOG_DEBUG, log_local4 : LOG_DEB
105К-			+Create data collection rule
70K- 35K-			Run the following command to install and apply the CEF collector: sudo wget -O Forwarder_AMA_installer.py https://raw.githubusercontent.c

- 4. Edit the data collection rule or create one if necessary. On the **Collect** tab of the rule's configuration, configure the following:
  - LOG\_LOCAL\* (0-7) to LOG\_DEBUG
  - LOG\_SYSLOG to LOG\_DEBUG
  - LOG\_USER to LOG\_DEBUG

# Installing the Operations Management Suite (OMS) or Log Analytics Agent

The Operations Management Suite (OMS)/Log Analytics Agent provides a Syslog relay.

(i) **NOTE:** Make sure that this agent is installed on a host within the network and configure SonicOS to send ArcSight-formatted Syslog data to the agent. The Agent establishes a secure connection with Azure, so the log data is not sent to the cloud in plaintext.

(i) **NOTE:** Before installing one, review the requirements for the agent (Supported operating systems). Some versions of Linux have additional requirements with regard to Python that you should be aware of.

#### To install the Operations Management Suite (OMS) or Log Analytics Agent:

- 1. On the Microsoft Sentinel page, navigate to Data Connectors under Configuration.
- 2. Search for **SonicWall** and Choose **[Deprecated] SonicWall Firewall via Legacy Agent** and follow the instructions to set up the forwarder agent on your machine.
  - (i) **NOTE:** You can also run scripts to download the installer and execute it. They also include the workspace ID and primary key that the agent needs to connect to the workspace.
- 3. Note down the IP address of the machine.

(i) | NOTE: This IP address is needed for SonicWall configuration.

(i) **IMPORTANT:** Log analytics agent will be retired on August 31, 2024, so make sure you migrate to Azure Monitor Agent (AMA). For more information, refer to migration instructions.

Here are some other reference articles if you want to learn more about the Arc Agent and Azure Monitor Agent:

- Install the Arc Agent/Azure Connected Machine Agent
  - Connected Machine agent prerequisites Azure Arc
  - Overview of the Azure Connected Machine agent Azure Arc
- Install the Azure Monitor Agent extension
  - Azure Monitor Agent overview Azure Monitor
  - Manage Azure Monitor Agent Azure Monitor
- Install the Azure Monitor Agent (AMA) forwarder.
  - Tutorial: Forward Syslog data to Microsoft Sentinel and Azure Monitor by using Azure Monitor Agent

- Configure a Data Collection Rule (DCR)
  - Tools for migrating to Azure Monitor Agent from legacy agents Azure Monitor
  - Collect Syslog events with Azure Monitor Agent Azure Monitor
  - Tutorial: Forward Syslog data to Microsoft Sentinel and Azure Monitor by using Azure Monitor Agent

### Configuring a Syslog Server on SonicWall Device

#### To configure a syslog server:

- 1. Configure a syslog server on your SonicWall device using syslog format as ArcSight (CEF).
- 2. Specify the IP address or Name of your Linux VM as the syslog server, and Syslog Facility should be **Local use 4**.

∩ | NOTE:

- The Syslog data is sent to the OMS Agent on UDP/514.
- For more information, refer to Knowledge Base Article.

### Validating the Data that Reaches Workspace

Once configured, you'll receive SonicOS-generated CEF messages in the Sentinel Workspace.

Validate that the OMS Agent is receiving CEF messages and can connect to Azure. If the validation initially fails, try again. The validation checks the connection to the workspace as well as a stream of CEF from a source. The firewall needs to be actively generating Syslog CEF messages for the validation to pass.

#### Log Analytics Agent



#### (i) NOTE:

- Troubleshoot your CEF or Syslog data connector according to <a href="https://learn.microsoft.com/en-us/azure/sentinel/troubleshooting-cef-syslog?tabs=cef">https://learn.microsoft.com/en-us/azure/sentinel/troubleshooting-cef-syslog?tabs=cef</a>.
- sudo wget -O cef\_troubleshoot.py, https://raw.githubusercontent.com/Azure-Sentinel/master/DataConnectors/CEF/cef\_troubleshoot.py (python cef\_troubleshoot.py [WorkspaceID]).

#### **Azure Monitor Agent**

jalmedjalme-ubuntu-wni-f wdd wget - O Sentinel_MAL troublenhoot.py https://raw.githubusercontent.com/Auur/Auure-Sentinel/mater/DataConnectors/Sym Do/Sentinel_MAL troublenhoot.pytkadug pythubusercontent.com/Auure/Auure-Sentinel/Mater/DataConnectors/SymJog/Sentinel_AXA_troublenhoot.py Reolving rew.githubusercontent.com (raw.githubusercontent.com).ibs.ibs.ibs.ibs.ibs.ibs.ibs.ibs.ibs.ib.ib.ib.ib. Connecting to raw.githubusercontent.com (raw.githubusercontent.com).ibs.ibs.ibs.ibs.ibs.ibs.ibs.ib.ib.ib.ib.ib. Tif request met, mawiling regorder Jou O GK Length 19903 (49%) (rew./plain)
Sentinel_AMA_troubleshoot.py 100%[KB/s in 0.009s
2024-04-04 13:28:47 (5.39 MB/s) - 'Sentinel_ANG_troubleshoot.py' saved [49903/49903]
The scenario chosen is: CIF
formation on more the unlidering series for the and assessed
pratring to fun the variable of non-script for the carbonariad prase validate you are sending messages to the spent machine
Starting validation tests for AMA
verify and agent service is running> Success
Detected AMA running version- 1.29.6
Detected ARC installed on the machine: arcmagent version 1,39,02628.1411
verify_oms_agent_not_running> Success
Starting validation tests for data collection rules
verify_DCR_exists> Success
verify_DCR_content_has_stream> Success
verify_dcr_has_valid_content> Success
check_multi_homing> Success
Starting validation tests for the Syslog daemon
verify_Syslog_daemon_listening> Success
verify_Syslog_daemon_forwarding_configuration> Success
Starting validation tests for the operating system
verify_selinux_state> Success
verify_iptables_policy_permissive> Success
verity_iptables_rules_permissive_514> Success
Verify_lptables_rules_permissive_25300> Success Verify_free_disk_space> Success
Starting validation tests for conturing increments
Attempting to capture events using topdump. This could take up to 10 seconds.
listen to incoming events> Success
Found CEF in stream. Please verify CEF events arrived at your workspace
All tests passed successfully
This script generated an output file located here - /tmp/troubleshooter_output_file.log
Please review it if you would like to get more information on failed tests.
If you would like to open a support case please rup this script with the 'collect' feature flam in order to collect additional system data for trou
bishooting, bython Sentinel MA troubleshoot.pv (STRIAN OFTION) collect' result isg'in order to collect solitional system data for from

#### To validate data on Microsoft Sentinel workspace:

- 1. On the Microsoft Sentinel workspace, navigate to the **General > Logs** link.
- 2. Set a short time range that covers a period where data should have been ingested. It can take several minutes to begin seeing data in Log Analytics. Wait for more time if you do not see data right away.
- 3. Enter a basic query to confirm data is arriving at Sentinel and click **Run**.

Home > Microsoft Sentinel > Microsoft Ser	ritral		
<ul> <li>Microsoft Sentinel Selected workspace "sertinel-test"</li> </ul>	Logs		>
₽ Search <	New Guery 1* × +	💙 Feedback 🗱 Queries	Θ <b>Ω</b> ~
General	🖗 sentimel-test 🔹 💌 🛤 🕄 🚺 🔂 sent 🖉 🕼 😵 🖉 Starte 🗸 😰 Starte 🗸 😰 Starte V. 🚽 New start Autor V. 🛫 Export V. 🔊 Rents V. 🛫 Annual quary		
Overview (Preview)	Tables Queries Functions K Tommendation (17) ng		
a top			
<ul> <li>Nevi &amp; public</li> </ul>	Ja Sarch I		
P Search	(V Hew) = Group by Soution V		
Threat management	I" Colleges all		
Incidents	Favoritas		*
Mońbooks	Yes can add fereities by cloking on Penalts Chart      Add Dockmark		ρ.
Hunting	Inveformented [JTC] 14 Destarlinedar Devisativesian Devisativesian Devisativesian Activity Logicourty	Additional Interview	
<ul> <li>Notebooks</li> </ul>	Microsoft Section     P3/2022,12/MS3/827 PM Soncifiel NSA.3798 P3.5111-44251 171 IPset Dead Rev Detection 3	got+7%_actor+%k*	

#### To get AMA Heartbeat Logs:

Use **Heartbeat** query with a short time range (last 30 minutes):

- Heartbeat
- | distinct Computer, Category, ComputerIP

▶ Run Time range : Last 30 minutes	🔚 Save 🗸 🖻 Sł
1 Heartbeat 2   distinct Computer, Category, Compu	ıterIP
Results Chart 🕅 Add bookmark	
Computer Category	Com
jaime-ubuntu-vm Azure Monitor Age	ent 184.9

(i) **NOTE:** This only applies to AMA, not the OMS/Log Analytics Agent.

# **Microsoft Sentinel Content Type**

The SonicWall Data connector includes a Workbook containing a variety of queries for various security services as well as other traffic and security insights.

To navigate to Microsoft Sentinel content types:

- 1. Navigate to the **Content management > Content hub** link.
- 2. Click the installed **SonicWall Network Security** Solution to view the content types:
  - Workbook
  - Analytics Rules
  - Hunting Query

Dashboard > Micro	osoft Sentinel > Micros	soft Sentinel   Content hu	ub >					
SonicWall N	Network Secu	irity						
🕐 Refresh 🔋 🛙	Delete 🛃 Reinstall							
C 6 Installed content i	items Config	4 unation needed						
SonicWall	Network Security		< ٩	Search				
SonicWall	IN SonicWall	3.1.0		Content name		Create	Content type	Version
Provider capability to ingest Sor	Support nicWall access logson sys	Version log format) into		Recommended] SonicWall Firewall via AMA		1 items	DataConnec	1.0.0
Microsoft Sentinel. 50 orchestrate their organ	C administrators who nee nizations' response to ma	ed to direct and lior security threats	Î	Deprecated) SonicWall Firewall via Legacy Agent	٠	1 items	DataConnec	1.0.0
based on analyzing the	e logs in real-time. Users Reviation the stress of in-	require a birds-eye view		👌 SonicWall - Capture ATP Malicious File Detection			AnalyticsRule	1.0.0
attacks, increasing volu	umes of alerts, and long i	resolution timeframes.	C	SonicWall - Allowed SSH, Telnet, and RDP Connections			AnalyticsRule	1.0.0
			_ C	Outbound SSH/SCP Connections			HuntingQuery	1.0.0
Content type ①		Ø 1	C	] 🥂 SonicWall Workbook			Workbook	1.0.0
Analytics rule	Data connector	Hunting query						
1 Workbock								
Security - Network								
Pricing ①								
(1) Free			*					
Manage Ac	tions 🗸 View detail	ls	4	Previous Page 1 v of 1 Next > Showing 1 to 6 of 6 result	В.			

### Workbook

**SonicWall Workbook** contains the collection of queries to provide visibility into the events reported by the SonicWall firewalls.

Dashboard > Microsoft Sentinel > Microsoft Sentinel   Content hub > SonicWall Network Security > Workbooks >
SonicWall Workbook 🛷 X
in and the second s
O G Subornitesh: Off
SonicWall Workbook for Microsoft Sentinel
Welcome! We've included a collection of queries to provide visibility into the events reported by your Sonicilial freewals.
Use the available filters to update the data on the dashboard. Note that not all filters apply to every query £81 the queries as needed to suit your needs.
Time Range Last 24 hours V O Source Devocr.All V O Source IP.All V O Destination IP.All V O Activity.All V O
V Receil Secrets
- Incomentation
V Attivity Benindown
V Content Fibring
V Denied By Country
✓ Security Services
V Todio and Ensein
V Devied IPs and Ports

You can also select the Auto refresh time for the queries.

🕐 😳 🕄 Auto refresh: Off	
Auto refresh	
Workbook content will refresh automatically on this interval. If you manually refresh content, it will restart the refresh interval.	
Refresh interval:  Off	de
5 minutes     10 minutes	24
O 15 minutes	
One hour	
2 hours	
One day	
Apply Cancel	ł

### Analytics Rules

Topics:

- SonicWall Capture ATP Malicious File Detection
- SonicWall Allowed SSH, Telnet, and RDP Connections

### SonicWall - Capture ATP Malicious File Detection

**SonicWall- Capture ATP Malicious File Detection** identifies malicious file verdicts from the SonicWall Capture ATP service. This analytic rule leverages the SonicWall Firewall ASIM Network Session parser (ASimNetworkSessionSonicWallFirewall).

#### To set rules logic:

1. Click the Analytics rule to create the rule and set the rules logic.

Debboard > Microsoft Sentinel > Microsoft Sentinel [Content hub > Sonicitval Network Security >  Analytics Rules	×
+ duran v. C. belen. P. Analytic methods v. C. Fosto. S. Costo. B. Costo. H. Incost. H. Fosto. F. Souther & Sector.	
More content at Autors by severity	LEARN MORE
Active rules Content hub High (3 Medium (3 Low (3 Line (3 Dimensional (3)	About analytics rules (C
Active rules Rule templates Acousties	SonicWall - Capture ATP Malicious File Detection
P Indefinitive address deal deallocation X V Add There	Medium Content hub Scheduled Severity Content Source Rule Type
Severity Name Rule type Data sources Bactics Bedvilques Source name Medium Sonicital - Capture AIP Malicious C. Scheduled Common Funn +10 & Execution 11204 Sonicital Female	MITE ATTACK
	Arr server Werk Noticide=(Transf) = 1011 ( entered (protect)Provide= totopet(("pietoway Artification process or Altitionalitionation on ("pieto") (produc entered (protect)Provide= ("pietowa") (produc entered (pietoway) (pietoway) An paray nervy 1 pietoway
There are boot and and and	Note:     No have 1 used this template yet flow can use it to make explore name.     Support only the sector will be the interview of the name.     Create rule
Deebbarred & Missen & Continuel & Missen & Continuel Constant back & Continuel Matures	In Consultant St. Annalastica Distant St.
Dashboard 7 Microsoft Sentiner 7 Microsoft Sentiner Content hub 7 Sonicwaii Networ	k security / Analytics Rules /
Analytics rule wizard - Create a new Scheduled rule	
SonicWall - Capture ATP Malicious File Detection	
Constal. Catalalacia Incident estilant Automated estances. Devices	
General Set rule logic incident settings Automated response Review +	+ create
Create an analytics rule that will run on your data to detect threats.	
Analytics rule details	
Name *	
SonicMall - Canture ATD Malicious Eile Detection	
Somervan - Capture Arr Mandous rile Detection	
Description	
This rule identifies malicious file verdicts from the SonicWall Capture ATP service. This and rule leverages the SonicWall Firewall ASIM Network Session parser (ASImNetworkSessionSonicWallFirewall).	alytic
Severity	
Medium	$\sim$
Tactics and techniques (2)	~
inclusion and consideration	
Status	
Enabled	
Next : Set rule logic >	

2. Navigate to Incident Settings, select the Automated response.

3. Review the settings and click **Save** to schedule the rule.



### SonicWall - Allowed SSH, Telnet, and RDP Connections

**SonicWall - Allowed SSH, Telnet, and RDP Connections** identifies allowed inbound SSH, Telnet, and RDP connections. This analytic rule leverages the SonicWall Firewall ASIM Network Session parser (ASimNetworkSessionSonicWallFirewall).

#### To set rules logic:

1. Click the Analytics rule to create the rule and set the rules logic.

I - Alcowed SSN: Beinet, and RDP Connections   Review + create   Intel an analytics rule that will run on your data to detect threats.   Kulgytics rule details   Servicion   This rule signifies allowed inbound SSN, Tehnet, and RDP connections. This analytic rule teverages the SonicWall Frewall ASIM Network Session parser (ASIm Network Session SonicWall Frewall).   Wedum   I - Alcowed SSN: Tehnet, and RDP connections   Review + Create   Review - SonicWall Frewall ASIM Network Session parser (ASIm NetworkSessionSonicWallFirewall).   Review - Create a new Scheduled rule	lytics rule wizard - Create a	a new Schedule	d rule
error       Set rule logic       incident settings       Automated response       Review - create         intere an analytics rule that will run on your data to detect threats.         Analytics rule details         iteme *         Sonic/Wall Freewall ASIM Network Session purser (ASIM Network Session Sonic/Wall Freewall.         intere image:         Sonic/Wall Freewall ASIM Network Session purser (ASIM Network Session Sonic/Wall Freewall.         intere image:         i	all - Allowed SSH, Telnet, and RDP Connections	a new senedate	araic
	naral Set rule lonic Incident settings	Automated response	Bariow - create
rease an analytics rule that will run on your data to detect threats. Inalytics rule details Liane * SonicWall - Allowed SSH, Teinet, and RDP Connections Hescription This rule identifies allowed inbound SSH, Teinet, and RDP connections. This analytic rule leverages the SonicWall Treenal ASM Network Session parser (ASimNetworkSessionSonicWallTreenal).  everity  Medium Tactics and techniques (24)  and > Microsoft Sentinel > Microsoft Sentinel [Content hub > SonicWall Network Security > A  SonicWall - Allowed SSH, Teinet, and RDP Connections  everity  and > Microsoft Sentinel > Microsoft Sentinel [Content hub > SonicWall Network Security > A  SonicWall - Allowed SSH, Teinet, and RDP Connections  everity  and > Microsoft Sentinel > Microsoft Sentinel [Content hub > SonicWall Network Security > A  SonicWall - Allowed SSH, Teinet, and RDP Connections  everity  in the information of the sentinel > Microsoft Sentinel [Content hub > SonicWall Network Security > A  SonicWall - Allowed SSH, Teinet, and RDP Connections  everity  Microsoft Sentinel > Microsoft Sentinel ] Content hub > SonicWall Network Security > A  SonicWall - Allowed SSH, Teinet, and RDP Connections  everity  Microsoft Sentinel = Microsoft Sentinel ] Content hub > SonicWall Network Security > A  Mathematica analytics rule that will run on your data to detect threats.  Inalytics rule details  Eveription  This rule information SH, Teinet, and RDP Connections  everity  Microsoft Sentinel ASM Network Session parser (ASimNetworkSessionSonicWallTreenal).  wereity  Microsoft Sentinel ASM Network Session parser (ASimNetworkSessionSonicWallTreenal).  SonicWall - Allowed SSH, Teinet, and RDP Connections  Everifyion  Tactics and techniques (24)  Tactics and techniques (24)  Tactics and techniques (24)  Tactics  Fast = Tabled  Fas	eral Sectorelogic Incoencisecongs	Automated response	nenew - create
reste en analytics rule that will run on your data to detect threats.			
tralytics rule details   SonicWall - Allowed SSH, Teinet, and RDP Connections Description  This rule identifies allowed inbound SSH, Teinet, and RDP connections. This analytic rule leverages the SonicWall Tremal ASM Network Session parser (ASImNetworkSessionSonicWallTremal). Workum  Modum  Context Set rule logic 1 Category Context Set Set Set Set Set Set Set Set Set Se	create an analytics rule that will run on your data t	o detect threats.	
same * SonicWall - Allowed SSH, Telnet, and RDP Connections	Analytics rule details		
SonicWall - Allowed SSH, Teinet, and RDP Connections  kescription  This rule identifies allowed inbound SSH, Teinet, and RDP connections. This analytic rule leverages the SonicWall Frewall ASM Network Session parser (ASimNetworkSessionSonicWallFrewall).  weekity  Medum  Control - Analytics and techniques (24)  wether an analytics rule that will run on your data to detect threats.  Analytics rule details  iare * SonicWall Frewall ASM Network SSH, Teinet, and RDP Connections  Netription  This rule identifies allowed inbound SSH, Teinet, and RDP Connections  Netription  This rule identifies allowed inbound SSH, Teinet, and RDP Connections  Netription  This rule identifies allowed inbound SSH, Teinet, and RDP Connections  Netription  This rule identifies allowed inbound SSH, Teinet, and RDP Connections  Netription  This rule identifies allowed inbound SSH, Teinet, and RDP Connections  Netription  This rule identifies allowed inbound SSH, Teinet, and RDP Connections  Netription  This rule identifies allowed inbound SSH, Teinet, and RDP Connections  Netription  This rule identifies allowed inbound SSH, Teinet, and RDP Connections  Netription  This rule identifies allowed inbound SSH, Teinet, and RDP Connections  Netription  This rule identifies allowed inbound SSH, Teinet, and RDP Connections  Netription  This rule identifies allowed inbound SSH, Teinet, and RDP Connections  Netription  This rule identifies allowed inbound SSH, Teinet, and RDP connections  Netription  This rule identifies allowed inbound SSH, Teinet, and RDP connections  Netription  This rule identifies allowed inbound SSH, Teinet, and RDP connections  Netription  This rule identifies allowed inbound SSH, Teinet, and RDP connections  Netription  This rule identifies allowed inbound SSH, Teinet, and RDP connections  Netription  This rule identifies allowed inbound SSH, Teinet, and RDP connections  Netription  This rule identifies allowed inbound SSH, Teinet, and RDP connections  Netription  This rule identifies allowed inbound SSH, Teinet, and RDP con	Name *		
hexcription This rule identifies allowed inbound SSH, Tehnet, and RDP connections. This analytic rule leverages the SonicWall Frewall ASM Network Session parser (ASimNetworkSessionSonicWallFirewall).  weeriny Modum  Notices and techniques (24)  Net 1: Set rule logic =  ard > Microsoft Sentinel > Microsoft Sentinel [ Content hub > SonicWall Network Security > A  by tics rule evizard - Create a new Scheduled rule  Hext: Set rule logic incident settings Automated response Review + create  areal Set rule logic incident settings Automated response Review + create  reate an analytics rule that will run on your data to detect threats.  thalytics rule details  ime * SonicWall Frewall ASM Network SSH, Tehnet, and RDP connections  lescription  This rule identifies allowed inbound SSH, Tehnet, and RDP connections  invikWall Frewall ASM Network SSH, Tehnet, and RDP connections  isonicWall Frewall ASM Network SSH, Tehnet, and RDP connections  isonicWall Frewall ASM Network SSH, Tehnet, and RDP connections  isonicWall Frewall ASM Network SSH, Tehnet, and RDP connections  isonicWall Frewall ASM Network SSH, Tehnet, and RDP connections  isonicWall Frewall ASM Network SSH, Tehnet, and RDP connections  isonicWall Frewall ASM Network SSH, Tehnet, and RDP connections  isonicWall Frewall ASM Network SSH, Tehnet, and RDP connections  isonicWall Frewall ASM Network SSH, Tehnet, and RDP connections  isonicWall Frewall ASM Network SSH, Tehnet, and RDP connections  isonicWall Frewall ASM Network SSH, Tehnet, and RDP connections  isonicWall Frewall ASM Network SSH, Tehnet, and RDP connections  isonicWall Frewall ASM Network SSH, Tehnet, and RDP connections  isonicWall Frewall ASM Network SSH, Tehnet, and RDP connections  isonicWall Frewall ASM Network SSH, Tehnet, and RDP connections  isonicWall Frewall ASM Network SSH, Tehnet, and RDP connections  isonicWall Frewall ASM Network SSH, Tehnet, and RDP connections  isonicWall Frewall ASM Network SSH, Tehnet, and RDP connections  isonicWall Frewall ASM Network SSH, Tehnet, and RDP connectio	SonicWall - Allowed SSH, Telnet, and RDP Conner	ctions	
Herription This rule identifies allowed inbound SSH, Tehlert, and RDP connections. This analytic rule tevenages the SonicWall Frewall ASM Network Session parser (ASimNetworkSessionSonicWallFrewal).  Wethin Workum	here in the second s		
In the network at a data module story, terest, and not recented with the restance of solicities and techniques (24)  and backt 2 Set tube logic >  and > Microsoft Sentinel > Microsoft Sentinel   Content hub > SonicWall Network Security > At backt 2 Set tube logic >  and > Microsoft Sentinel > Microsoft Sentinel   Content hub > SonicWall Network Security > At backt 2 Set tube logic >  and > Microsoft Sentinel > Microsoft Sentinel   Content hub > SonicWall Network Security > At backt 2 Set tube logic >  and > Microsoft Sentinel > Microsoft Sentinel   Content hub > SonicWall Network Security > At backt 2 Set fuel logic incident settings Automated response Review + create  and set rule logic incident settings Automated response Review + create  reate an analytics rule that will run on your data to detect threats.  inalytics rule details  and *  SonicWall - Allowed SSH, Tehnet, and RDP Connections  tescription  This nule identifies allowed inbound SSH, Tehnet, and RDP connections.  werity  Modium  v  Textics and techniques (24)  Contexting Automated response Review + create  and techniques (24)  Contexting Automated response Review + create  and techniques (24)  Contexting Automated response Review + create  and techniques (24)  Contexting Automated response Review + create  and techniques (24)  Contexting Automated response Review + create  and Set rule logic Incident setting Automated response Review + create  and techniques (24)  Contexting Automated response Review + create  and techniques (24)  Contexting Automated response Review + create  and techniques (24)  Contexting Automated response Review + create  and techniques (24)  Contexting Automated response Review + create Automated response Review + create  and techniques (24)  Contexting Automated response Review + create Automated response Review + create Automated response Review + create Automated + contexting Automate	escription This pile identifies allowed inhound SSU Televity	and POO connections. This w	ash tir a la lavaranar tha
	SonicWall Firewall ASIM Network Session parser (	ASimNetworkSessionSonicV	VallFirewall).
everify  Modum  Modu Modu Modu Modu Modu Modu Modu Mod			
Medium	Severity		
Tactics and techniques (24)	Medium		~
Anse  Finabled  Finabled Finabled  Finabled  Finabled  Finabled  Finabled  Finabled  Finabled  Finabled Finabled Finabled Finabled  Finabled  Finabled Finabled	Tactics and techniques (24)		
Institution         Interface	menter aux service destructions		
	latus		
And 1 Set tule logic >  and > Microsoft Sentinel > Microsoft Sentinel   Content hub > SonicWall Network Security > A  yetics rule wizard - Create a new Scheduled rule  t-Alexed SNL Binet, and RDP Connections  and Set rule logic Incident settings Automated response Review + create  areat as analytics rule that will run on your data to detect threats.  knalytics rule details  liame *  SonicWall - Allowed SSH, Telnet, and RDP Connections  lescription  This rule identifies allowed inbound SSH, Telnet, and RDP connections.  we writy  Modium  v  Tactics and techniques (24)  Context C	Enabled		
ard > Microsoft Sentinel > Microsoft Sentinel   Content hub > SonicWall Network Security > All ytics rule wizard - Create a new Scheduled rule         I-Aboved SML Benet, and RDP Connections         ard > et rule logic incident settings Automated response Review + create         reate an analytics rule that will run on your data to detect threats.         Analytics rule details         tame *         SonicWall - Allowed SSH, Teinet, and RDP Connections         This rule identifies allowed inbound SSH, Teinet, and RDP connections.         weritiy         Medium         Tactics and techniques (24)         Totals			
Act: Set rule logic 3         and > Microsoft: Sentinel > Microsoft: Sentinel   Content hub > SonicWall Network Security > A         Intersection:         a-Alowed SSN: Feinet, and RDP Connections         erral       Set rule logic incident settings Automated response Review + create         intersection:         intersection: <td< th=""><th></th><th></th><th></th></td<>			
extract state       Create a new Scheduled rule         i-Alowed SRI: Teinet, and RDP Connections         and       Set rule logic       Incident settings       Automated response       Review + create         reate an analytics rule that will run on your data to detect threats.         nalytics rule details         ame *         SonicWall Filewall AGM Network Session parser (ASimNetworkSessionSonicWallTrewall).         invelty         incidum	lext : Set rule logic >		
I - Allowed SSN: Teinet, and RDP Connections  I - Allowed SSN: Teinet, and RDP Connections  Analytics rule logic Incident settings Automated response Review + create  I - Allowed SSN: Teinet, and RDP Connections  I	Next : Set rule logic >	el   Content hub > SonicW	/all Network Security >
erral       Set rule logic       Incident settings       Automated response       Review + create         instate an analytics rule that will run on your data to detect threats.       Analytics rule details       Incident settings       Incident settings         SonicWall - Allowed SSH, Teinet, and RDP Connections       Incident settings       Incident settings       Incident settings         Description       Instruct information of SSH, Teinet, and RDP connections. This analytic rule leverages the SonicWall Freenal ASM Network Session parser (ASImNetwork/SessionSonicWallFreenal).       Incident settings         ieverity       Incident       Incident settings       Incident settings         Tactics and techniques (24)       Incident settings       Incident settings	Next : Set rule logic >	el   Content hub > SonicW	tall Network Security >
ireate an analytics rule that will run on your data to detect threats. Analytics rule details Little * SonicWall - Allowed SSH, Teinet, and RDP Connections Description This rule identifies allowed inbound SSH, Teinet, and RDP connections. This analytic rule leverages the SonicWall Frewall ASM Network Session parser (ASimNetworkSessionSonicWallFirewall). Wedwim Medium Tactics and techniques (24) Tactics Enabled	Next : Set rule logic > Oard > Microsoft Sentinel > Microsoft Sentinel Nytics rule wizard - Create a st - Aloued SSN: Telmet, and RDP Connections	el   Content hub > SonicW a new Schedule	All Network Security >
Treate an analytics rule that will run on your data to detect threats.  Analytics rule details  Lisme * SonicWall - Allowed SSH, Teinet, and RDP Connections  Description This rule identifies allowed inbound SSH, Teinet, and RDP connections. This analytic rule leverages the SonicWall Freewall ASIM Network Session parser (ASimNetworkSessionSonicWallFreewall).  Liverity  Medium Liverity Litts Description Lit	Next : Set rule logic > and > Microsoft Sentinel > Microsoft Sentinel Vtics rule wizard - Create a 4 - Alowed SML Telnet, and RDP Connections weral Set rule logic Incident settings	a l Content hub > Sonick a new Schedule	fall Network Security > cd rule Review + create
reate an analytics rule that will run on your data to detect threats.  Inalytics rule details  SonicWall - Allowed SSH, Telnet, and RDP Connections  Pescription  This rule identifies allowed inbound SSH, Telnet, and RDP connections. This analytic rule leverages the SonicWall Frewall ASIM Network Session parser (ASimNetworkSessionSonicWallFrewall).  We down  Tactics and techniques (24)  Tatus  Enabled	Next : Set rule logic > oard > Microsoft Sentinel > Microsoft Sentinel lytics rule wizard - Create a at - Alowed SSH. Tetret, and RDP Connections neral Set rule logic Incident settings	I Content hub > SonicW a new Schedule Automated response	All Network Security > ed rule ···· Review + create
Analytics rule details  Iame *  SonicWall - Allowed SSH, Teinet, and RDP Connections  Ins rule identifies allowed inbound SSH, Teinet, and RDP connections. This analytic rule leverages the SonicWall Frewall ASIM Network Session parser (ASimNetworkSessionSonicWallFirewall).  Ieverity  Medium  Tactics and techniques (24)  Tatus  Tabled	Next : Set rule logic > Oard > Microsoft Sentinel > Microsoft Sentinel Oytics rule wizard - Create a st - Alowed SSN: Telmet, and RDP Connections neral Set rule logic Incident settings	I Content hub > SonkW a new Schedule Automated response	All Network Security > ed rule ···· Review + create
iame * SonicWall - Allowed SSH, Teinet, and RDP Connections bescription This rule information and RDP connections. This analytic rule leverages the SonicWall Fiewall ASIM Network Session parser (ASimNetworkSessionSonicWallFirewall).  everify  Medium  Tactics and techniques (24)  Tactics Enabled	Next : Set rule logic > oard > Microsoft Sentinel > Microsoft Sentine Ilytics rule wizard - Create a sl - Alowed SSR: Teinet, and RDP Connections neral Set rule logic Incident settings Create an analysics rule that will run on your data t	I Content hub > SonicW a new Schedule Automated response o detect tiveats.	All Network Security > ed rule Review - create
SonicWall - Allowed SSH, Telnet, and RDP Connections  Assoription  This rule intentifies allowed inbound SSH, Telnet, and RDP connections. This analytic rule levenages the SonicWall Firewall ASIM Network Session parser (ASimNetworkSessionSonicWallFirewall).  evenity  Medium  Tactics and techniques (24)  Tatus  Tatus  Tabled	Next : Set rule logic > Doard > Microsoft Sentinel > Microsoft Sentine alytics rule wizard - Create a rear Alowed SSH Seinet, and RDP Connections eneral Set rule logic Incident settings Create an analytics rule that will run on your data t Analytics rule details	I Content hub > SonicM a new Schedule Automated response o detect threats.	Aill Network Security > cd rule ···· Review + create
Itescription This rule identifies allowed inbound SSH, Teinet, and RDP connections. This analytic rule leverages the SonicWall Trenail ASM Network Session parser (ASimNetworkSessionSonicWallTrenail).	Next : Set rule logic > woard > Microsoft Sentinel > Microsoft Sentine hytics rule wizard - Create a kat - Aloved SSH Senet, and RDP Connections meral Set rule logic Incident settings Create an analytics rule that will run on your data t Analytics rule details Name *	I Content hub > SonicW a new Schedule Automated response o detect threats.	All Network Security > cd rule Review + create
Itescription This rule identifies allowed inbound SSH, Teinet, and RDP connections. This analytic rule leverages the SonicWall Frewall ASIM Network Session parser (ASimNetworkSessionSonicWallFirewal).  evenity Medium Medium V Tactics and techniques (24)  Tactics Enabled	Next : Set rule logic > Ourd > Microsoft Sentinel > Microsoft Sentinel Outprics rule wizard - Create a star - Alowed SSH: Teinet, and RDP Connections neral Set rule logic Incident settings Create an analytics rule that will run on your data t Analytics rule details Name * Sonicitial - Alowed SSH, Teinet, and RDP Connect	I Content hub > SonicW a new Schedule Automated response o detect threats.	All Network Security > ed rule Review + create
This rule identifies allowed inbound SSH, Tehnet, and RDP connections. This analytic rule leverages the SonicWall Frewall ASIM Network Session parser (/ASimNetworkSessionSonicWallFirewal).	Next : Set rule logic > ourd > Microsoft Sentinel > Microsoft Sentinel Slytics rule wizard - Create a lat - Aloued SSH. Teinet, and RDP Connections meral Set rule logic Incident settings Create an analytics rule that will run on your data t Analytics rule details Name * Sonicivial - Aloued SSH. Teinet, and RDP Connect	I Content hub > SonicW a new Schedule Automated response o detect threats.	Aall Network Security > ed rule Review + create
evenity Medium  Tactics and techniques (24)  Tactis Enabled	Next : Set rule logic > Over 1 > Microsoft Sentinel > Microsoft Sentinel > Microsoft Sentinel Over 2 > Microsoft Sentinel > Microsoft Sentine Over 2 > Microsoft Sentinel > Microsoft Sentine Over 2 > Microsoft Sentinel > Microsoft Sentine Over 2 > Microsoft >	I Content hub > SonicW a new Schedule Automated response o detect threats.	All Network Security > ed rule Review + create
ieverity Medium  Iactics and techniques (24)  Iactis Iactis Enabled	Next : Set rule logic > Over 1 Set rule logic > Over 2 Microsoft Sentinel > Microsoft Sentinel Over 2 Microsoft Sentinel > Microsoft Sentine Infutics rule wizard - Create at all - Allowed SSH Teinet, and RDP Connections neral Set rule logic Incident settings Create an analytics rule that will run on your data t Analytics rule details Name * Sonic/Wall - Allowed SSH, Teinet, and RDP Connect Description This rule identifies allowed inbound SSH, Teinet, and	Content hub > SonicW     a new Schedule     Automated response     o detect threats.	All Network Security > cd rule Review - create
eveny Medum Itactics and techniques (24) Itactis Itatis Itabled	Next : Set rule logic > Oard > Microsoft Sentinel > Microsoft Sentinel Olytics rule wizard - Create a of - Alowed SSH. Teinet, and RDP Connections neral Set rule logic Incident settings Create an analytics rule that will run on your data t Analytics rule details Name * SonicWall - Allowed SSH, Teinet, and RDP Connect Description This rule identifies allowed inbound SSH, Teinet, a SonicWall Firewall ASIM Network Session parser	I Content hub > Sonick a new Schedule Automated response o detect tiveats. clons	All Network Security > ed rule Review + create nalytic rule leverages the VallTrewal).
Tactics and techniques (24)	Next : Set rule logic > Oard > Microsoft Sentinel > Microsoft Sentinel Ilytics rule wizard - Create a sl - Alowed SSH. Teinet, and RDP Connections neral Set rule logic Incident settings Create an analytics rule that will run on your data t Analytics rule details Name * Sonic/Wall - Alowed SSH, Teinet, and RDP Connect Description This rule identifies allowed inbound SSH, Teinet, a Sonic/Wall Firewall ASIM Network Session parser (	I Content hub > SonicM a new Schedule Automated response o detect threats. clions	Adl Network Security > cd rule Review + create nalytic rule leverages the ValFirewal).
Tactics and techniques (24)	Next : Set rule logic > Deard > Microsoft Sentinel > Microsoft Sentinel Utics rule wizard - Create a I - Alowed SSH: Telest, and RDP Connection neral Set rule logic Incident settings Create an analytics rule that will run on your data t Analytics rule details Name * SonicWall - Allowed SSH, Telest, and RDP Connect Description This rule identifies allowed inbound SSH, Telest, a SonicWall Firewall ASIM Network Session parser	I Content hub > SonicM a new Schedule Automated response o detect threats. tions	All Network Security > cd rule Review + create nalytic rule leverages the VelFirewall).
tatus Enabled	Next : Set rule logic > Ourd > Microsoft Sentinel > Microsoft Sentinel Outfics rule wizard - Create a state and RDP Connections neral Set rule logic Incident settings Create an analytics rule that will run on your data t Analytics rule details Name * SonicWall - Allowed SSH, Teinet, and RDP Connect Description This rule istenties allowed inbound SSH, Teinet, SonicWall Firewall ASIM Network Session parser Severity Medium	I Content hub > SonicW a new Schedule Automated response o detect threats. tions	Aali Network Security > cd rule Review + create nalytic rule leverages the Valifirewal).
Enabled	Next : Set rule logic > oard > Microsoft Sentinel > Microsoft Sentinel Itytics rule wizard - Create a sti - Alowed SSH. Sente, and RDP Connections neral Set rule logic Incident settings Create an analytics rule that will run on your data t Analytics rule details Name * SonicWall - Allowed SSH, Teinet, and RDP Connect Description This rule identifies allowed inbound SSH, Teinet, a Serveitly Medium Tactics and techniques (24)	I   Content hub > SonicW a new Schedule Automated response o detect threats. ctions	All Network Security > cd rule ···· Review + create natytic rule leverages the Valificrevial).
	Next : Set rule logic >  oard > Microsoft Sentinel > Microsoft Sentinel  slytics rule wizard - Create a  slat - Alowed SSH. Teinet, and RDP Connections  neral Set rule logic Incident settings  Create an analytics rule that will run on your data t  Analytics rule details  Name *  SonicWall - Allowed SSH, Teinet, and RDP Connect  Description  This rule identifies allowed inbound SSH, Teinet, a  SonicWall Firewall ASIM Network Session parser ( Severity Medium  Tactics and techniques (24)	I Content hub > SonicW a new Schedule Automated response o detect threats. ctions	All Network Security > cd rule Review + create nalytic rule leverages the Valfirewall).
	Next : Set rule logic > Over : Set rule logic > Over > Microsoft Sentinel > Microsoft Sentine Nytics rule wizard - Create a over Alowed SSH. Teinet, and RDP Connections neral Set rule logic Incident settings Create an analytics rule that will run on your data t Analytics rule details Name * SonicWall - Allowed SSH, Teinet, and RDP Connect Description This rule identifies allowed inbound SSH, Teinet, a SonicWall Firewall ASIM Network Session parser Serveitly Medium Tactics and techniques (24) Satus Serveitly	I Content hub > Sonick a new Schedule Automated response o detect tiveats.	All Network Security > ed rule Review + create natytic rule leverages the VallTrewal().
	Next : Set rule logic > Sourd > Microsoft Sentinel > Microsoft Sentinel > Microsoft Sentinel > Microsoft Sentinel > Microsoft Sentine Set rule wizard - Create as an All-Alowed SSN. Teinet, and RDP Connections meral Set rule logic Incident settings Create an analytics rule that will run on your data t Analytics rule details Name * SonicWall - Allowed SSH. Teinet, and RDP Connect Description This rule identifies allowed inbound SSH. Teinet, a SonicWall Frewall ASIM Network Session parser ( Severity Medium Tactics and techniques (24) Satus Tabled	I Content hub > Sonick a new Schedule Automated response o detect threats.	All Network Security > ed rule Review + create nalytic rule leverages the VallFirewal()
	Next : Set rule logic > Ourd > Microsoft Sentinel > Microsoft Sentine SSE: Sente, and RDP Connections neral Set rule logic Incident settings Create an analytics rule that will run on your data t Analytics rule details Name * SonicKWall - Allowed SSH, Teinet, and RDP Connect Description This rule identifies allowed inbound SSH, Teinet, and RDP Connect Serverity Medium Tactics and techniques (24) Satus The babled	I Content hub > SonicM a new Schedule Automated response o detect threats.	All Network Security > cd rule Review + create nalytic rule leverages the ValFirewal).
	text : Set rule logic >  text : Set rule logic >  text : Set rule logic >  text : Set rule logic Incident settings  reate an analytics rule that will run on your data t  text issue details  text : Set rule details  text : Set rule logic Incident settings  reate an analytics rule that will run on your data t  text : Set rule logic Incident settings  text : Set ru	I Content hub > SonicM a new Schedule Automated response o detect threats. tions	All Network Security > cd rule Review + create nalytic rule leverages the Valfirewall).

- 2. Navigate to Incident Settings, select the Automated response.
- 3. Review the settings and click **Save** to schedule the rule.

### Hunting Query

**Outbound SSH/SCP Connections** query looks for outbound SSH/SCP connections identified by the expected port number (22) or by the SonicWall Deep Packet Inspection services. This query leverages the SonicWall Firewall ASIM Network Session parser.

#### To run query:

- 1. Run the query in one of following ways:
  - Select the Threat hunting query and click **Run** query.

Dashboard > Microsoft Sentinel > Microsoft Sentinel   Cont	ent hub > SonicWall Ne	twork Security >									
Hunting											×
-											
🖒 Refinsh 💿 Last 24 hours 🗸 🕂 New query 🗅 Ru	n selected queries 🔋 🛙	olote 🌵 Hartacti	ons 🗸 💶 Column	s 🔗 Guides & Fer	dback						
								Manine	For state states	E-months I In-	
P dedb87b9-3caa=6000-ae88-1898eed7 X Content s	ource: All X Y Ad	id filter						1.00	Soricital Frevall	Soricital	
<ul> <li>Query</li> </ul>	Results	Results delta	Results delta p	Content source	Data sources	Tactics	Techniqu	Description			
🔽 👷 Outbound SSH/SCP Connections		-		Content hub		Editation	• -2 O	This query looks for expected port numb	outbound SSH/SCP conne er (22) or by the Sonicilial	ctions identified by th I Deep Packet Inspecti	e on
								services. This query I Session parter.	everages the SonicWall Fir	ewall ASIM Network	
											- 1
								ASSelletvorkSess3	ordions chall? Snewall		- I
								extend Service	ytes > 0 and NetworkS Name = coalesce(incle	Grection "Duth pName, DotAppName	)
								where ( DutPor	titumber - 22 and flat	workProtocol in (	10
								4			D I
								View query results >			- 1
								Tactics			- 1
								Differen	result or aid in the adversar	pues and attributes that ry removing files and	- 1
									information from a target in read more on attack.mitre.	etwork.	- 1
								Technica er			- 1
								T1020 (3	Automated Exfiltration		- 1
								T1048 C3	Erlitration Over Alternative	Profescol	- 1
- C							-				
< Previous Page 1 v of 1 Next > Show	ing 1 to 1 of 1 results.							Run query	View results		

• Scroll right and click on three dots the end and run the query.

(i) **NOTE:** You can also create your own hunting query using this.

Dashboard > Microsoft Sentinel > Microsoft Sentinel   Content hub > Sonic/Wall Network Security >								
Hunting								
🕐 Refesh 💿 Last 34 hours 🗸 🕂 New query 🗅 Run selected queries 🛞 Districe 🛛 Hunt actions 🗸 💷 Columns 🔗 Guides & Feetback								
P dedb0t/b-3caa-8x00-ae08-1090eed7 X Content source : All X Y Add filter								Version 1.0.0
Query	Results	Results delta	Results delta p	Content source	Data sources	Tactics	Techniques	Description
Outbound SSH/SCP Connections	Error ①	Error ③	Error ③	Content hub		Exfiltration	<b>9</b> =2 ③	This query looks for out expected part number (
								D Run e
								Add to favorites
								🖉 Edit 🛛 🕹
								Cone
								Delete
								Create analytics rule
								Add to livestream
								+ Create hunt
								Add to existing hunt

For more information about setup instructions, refer to the SonicWall Firewall-Sentinel Integration KB Article. Here is the data connector instructions Article.

# SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year.

The Support Portal enables you to:

- View Knowledge Base articles and Technical Documentation
- View and participate in the Community Forum discussions
- View Video Tutorials
- Access MySonicWall
- Learn about SonicWall Professional Services
- Review SonicWall Support services and warranty information
- Register at SonicWall University for training and certification

### About This Document

- (i) NOTE: A NOTE icon indicates supporting information.
- () | IMPORTANT: An IMPORTANT icon indicates supporting information.
- (i) | **TIP:** A TIP icon indicates helpful information.
- CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.
- M WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

Microsoft Sentinel Integration Guide Updated - April 2024

Copyright © 2024 SonicWall Inc. All rights reserved.

The information in this document is provided in connection with SonicWall and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit https://www.sonicwall.com/legal.