ARCTIC WOLF

Getting Your Arctic Wolf Managed Risk Scanner Online

PRODUCT DOCUMENTATION

Overview

Executing continuous vulnerability scans is a cornerstone of your organization's cybersecurity program. However, the myriad types of single-scan approaches that only offer a point-in-time view of your network can make understanding your risk profile a daunting task.

The Managed Risk scanner provides a continuous view of your vulnerabilities. Constantly updated with the latest threat information, it automatically detects when devices enter and leave your network. And it provides comprehensive visibility into the risk your organization faces.

The Managed Risk scanner uses similar methods to those bad actors use to identify vulnerabilities and map your attack space. For that reason, issues that occur during a scan are equally exploitable by a bad actor seeking to cause a denial of service condition on your network. If you have a device that experiences problems during a scan, we recommend consulting the vendor for an appropriate patch or workaround.

Arctic Wolf Managed Risk Scanner Setup

Follow these quick and easy steps to get your Arctic Wolf Managed Risk scanner online:

Note: please pay close attention to the areas highlighted in BLUE

1

Login

Login to the Arctic Wolf Managed Risk dashboard: dashboard.rootsoc.com

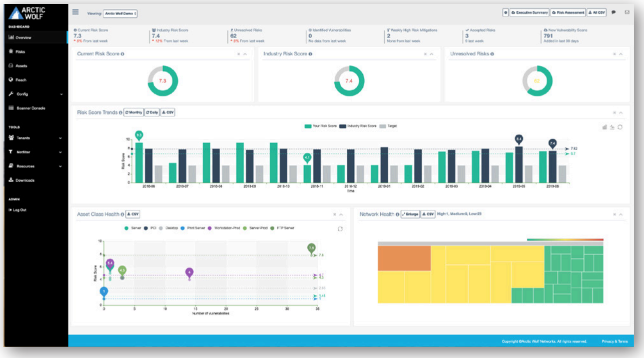
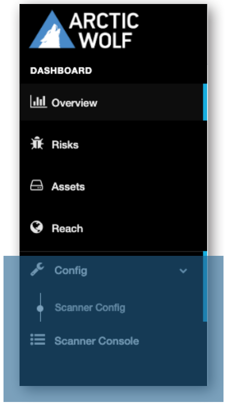


Figure 1: Arctic Wolf Managed Risk Dashboard

2

Managed Risk Scanner Setup

Under the "Config" dropdown, click "Scanner Config"



This is located on the left-hand side of the page and is highlighted in blue

Figure 2: Arctic Wolf Managed Risk Dashboard Left Navigation with Scanner Config drop-down

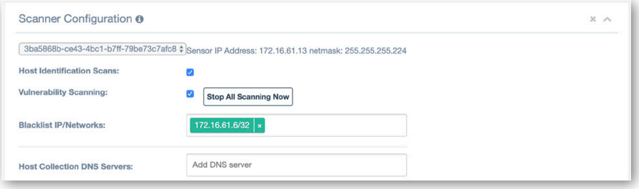
3

Scanner Configuration: Enable blacklisting of the host IP address on the Managed Risk scanner

Next, enable the blacklisting of the host IP address on the Managed Risk scanner. Navigate to the bottom of the page. Be sure to select both:

a. Host Identification Scans

b. Vulnerability Scanning



Scanner Configuration

3ba5868b-ce43-4bc1-b7ff-79be73c7afc8 Sensor IP Address: 172.16.61.13 netmask: 255.255.255.224

Host Identification Scans: ☑

Vulnerability Scanning: ☑ Stop All Scanning Now

Blacklist IP/Networks: 172.16.61.6/32 ×

Host Collection DNS Servers: Add DNS server

Figure 3: Managed Risk Dashboard Scanner Configuration – Blacklisting the host IP address on the Managed Risk scanner

4

Complete the Scanner Configuration Step

Select the “Update Scanner Configuration” button to confirm your changes.

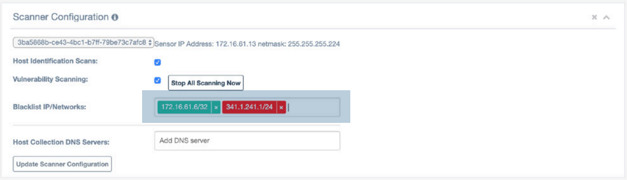
To blacklist IP addresses you don’t want scanned:

a. Login to the Managed Risk dashboard.

b. Under the “Config” dropdown, click “Scanner Config”.

c. Add any IP addresses you do not want to scan in the “Blacklist IP/Networks” text area.

Note: The blacklisted IP address will display as green if it has been inputted correctly and red if there is an error, as shown in Figure 4.



Scanner Configuration

3ba5868b-ce43-4bc1-b7ff-79be73c7afc8 Sensor IP Address: 172.16.61.13 netmask: 255.255.255.224

Host Identification Scans: ☑

Vulnerability Scanning: ☑ Stop All Scanning Now

Blacklist IP/Networks: 🟩 172.16.61.6/32 × 🟥 341.1.241.1/24 ×

Host Collection DNS Servers: Add DNS server

Update Scanner Configuration

Figure 4: Arctic Wolf Managed Risk Dashboard Scanner Configuration – Blacklist IP addresses

To whitelist/schedule IP addresses for scanning:

a. Login to the Managed Risk dashboard.

b. Under the “Config” dropdown, click “Scanner Config”.

c. Find the “Scanner Scanning Schedule” section near the bottom of the page (Fig 5).

d. Fill in the form to set a schedule.

i. In the “Target” field, add the IP address range you would like to schedule using Classless Inter-Domain Routing (CIDR) notation.

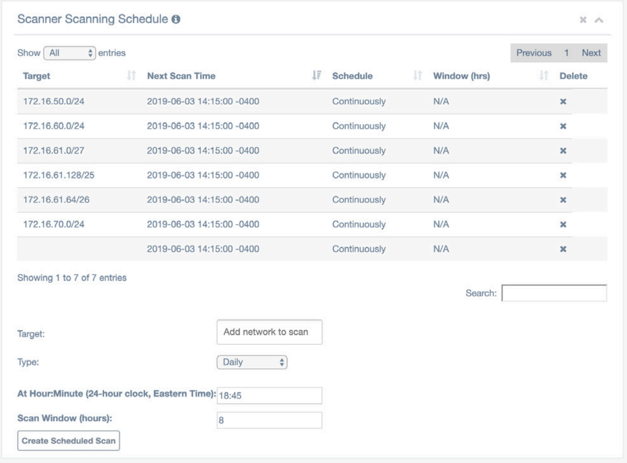
ii. In the “Type” field, select the interval time you would like to scan at (i.e. Daily, Weekly, Monthly).

a. Select the “Continuously” option to *whitelist* an IP address/network.

b. By default, the Managed Risk scanner will scan the current network.

iii. In the “At Hour: Minute” field, provide a time for when the scan will occur at each interval using a 24-hour clock.

e. Select the “Create Scheduled Scan” button to add the scanning schedule.



Scanner Scanning Schedule

Show All entries

Previous 1 Next

Target	Next Scan Time	Schedule	Window (hrs)	Delete
172.16.50.0/24	2019-06-03 14:15:00 -0400	Continuously	N/A	×
172.16.60.0/24	2019-06-03 14:15:00 -0400	Continuously	N/A	×
172.16.61.0/27	2019-06-03 14:15:00 -0400	Continuously	N/A	×
172.16.61.128/25	2019-06-03 14:15:00 -0400	Continuously	N/A	×
172.16.61.64/26	2019-06-03 14:15:00 -0400	Continuously	N/A	×
172.16.70.0/24	2019-06-03 14:15:00 -0400	Continuously	N/A	×
	2019-06-03 14:15:00 -0400	Continuously	N/A	×

Showing 1 to 7 of 7 entries

Search:

Target: Add network to scan

Type: Daily

At Hour:Minute (24-hour clock, Eastern Time): 18:45

Scan Window (hours): 8

Create Scheduled Scan

Figure 5: Arctic Wolf Managed Risk Dashboard—Schedule IP addresses for scanning.

ARCTIC WOLF

SOC2 Type II Certified

AICPA SOC

ISO 27001 CERTIFIED

CYBERGUARD COMPLIANCE