Version

3

PROTECTIVE CLOUD SERVICES USER MANUAL

Corporate Graphics and Communications

guardDog

Step by Step Instructions

Table of Contents

NOTE: Some sections in this manual will only appear for you if you have subscribed to the corresponding module with its accompanying license.

Revision history

Released on October 2022

Updated on October 2023

Terminology

MAC address

A ‘media access control address’ (MAC) address is a hardware identification number that uniquely identifies each device on a network. The MAC address is manufactured into every network card, such as an Ethernet card or Wi-Fi card, and therefore cannot be changed.

IP address

A unique string of characters that identifies each computer using the Internet Protocol to communicate over a network.

Notifications

System alerts that inform the user of events. These can be when an attack is detected, mitigated or a new vulnerability is found.

Units

These are the appliances connected to the network. They can be physical or virtual.

Attacks

Incidents that impact and compromise the devices connected to the network. They are a myriad of attacks that can occur from the outside of the network, to try to get access into it, or from the inside by either infecting a device on the network or performing actions with malicious intent.

Threats

These are vulnerabilities found on devices on the network. They tend to be of a more serious risk and indicate a certain level of danger if left unresolved or not remediated.

Vulnerability

These indicate issues with the devices on the network which pose a risk of being exploited. These can range from very low severity to critical. The more serious these are the more of a threat they pose.

Card

It is the default way of showing information on the user interface.

CVE

This is the "common vulnerability and exposure" identified on devices.

NIST

Is one of the authorities in vulnerability classification. From the main system, when a CVE card is displayed, you can open it to get redirected to the NIST article regarding that vulnerability.

Networks

Networks show the information about devices both inside of the network and outside of it.

- ### Local networks.

  These are the network of devices that is local to where the unit is plugged in. This usually refers to the main network that is reachable by layer2/layer3 connectivity. By default all units of this type share all the devices and network traffic they can see. Some examples of this are the corporate network, campus networks, networks that are connected by direct links, and so on.

- ### Remote networks

  These are very similar to local networks in the way they work. The main difference is that this usually refers to units that are plugged in to remote, private and networks that are not managed by the client. A good example of these would be a home private network from which the employee is working from, a hospitality network where the employee is at, and also a network that is owned and maintained by another company (office buildings, coworking spaces), and so on.

Shared mode

This is the mode selected for unit when it comes to the data they make visible to the customer. By default the local units all share all the data. Remote units, by default, are non-shared, meaning that although the capabilities of the units are exactly the same as local units, they only share limited non-identifiable data to keep the employee's privacy.

Wireless networks

These are specifically non-wired networks detected by the unit. In the system we identify as wireless networks or wireless devices any devices that is transmitting wirelessly. By definition all of those are devices can have a network running such as hotspots, access points, routers and so on. In some cases we will also identify personal devices transmitting wirelessly such as cellphones or other wireless capable devices.

- ### Identified

  These are wireless that have a name being broadcasted or SSID.

- ### Unidentified

  These are wireless that we have not been able to identify or that are not broadcasting its SSID.

Refresh and its rate

The user interface or Protective Cloud Services portal, refreshes automatically every 5 minutes. There is a refresh icon to force the refresh if needed.

GDS ID

This is an identification term provided by the system for each unit to be uniquely identified. This id It cannot be modified by the client. A client can refer to this id when calling support.

Serial number

This is a number automatically generated to identify the unit in order to be registered and assigned to a client. It is composed of 11 alphanumeric characters.

License key

This is a number provided to the client to buy a certain level of access, module, bundle, etc. the license is assigned to each unit to provide the capabilities mentioned earlier.

Classification of attacks

Currently the classification is based on the nature of the attack. From the attacks we work with today we have Dynamic Denial of Service attacks and Man in the Middle.

Detection

To make the system less prone to false positives, we detect attacks when they are detected and validated by the internal system based on the network traffic, patterns and packets identified. The time counter is from where we first see the packet moving on the network until we classify it and validate it.

Mitigation

Our mitigation requires the intervention of a human to make it permanent. We deploy countermeasures to deter and temporarily slow down and even block the attempts made to compromise and impact systems. The time counter reflects the time it took from when we detected the attack and started the countermeasure until we do not see the attack being performed any longer.

Scans

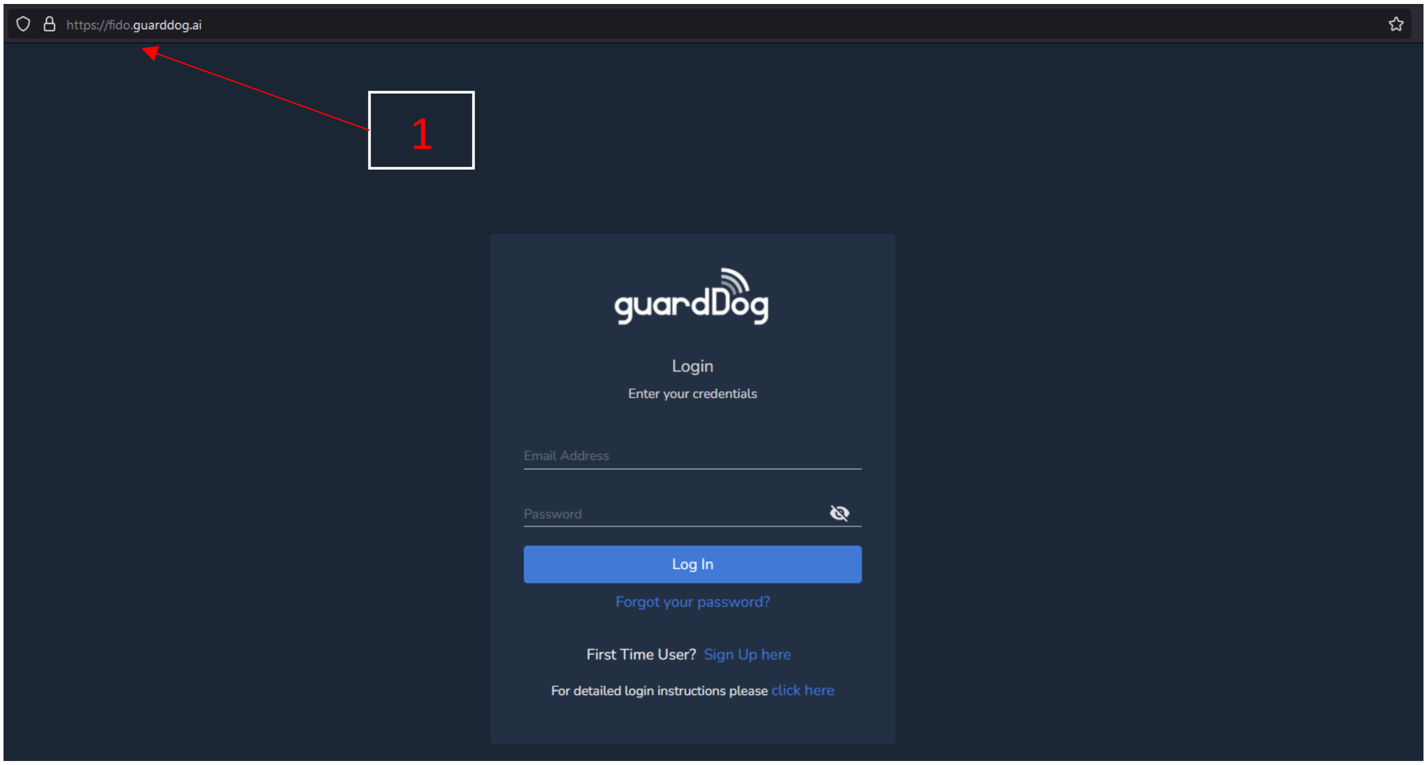
We perform scans multiple times an hour. These scans are classified as wired and wireless depending on the hardware used and where they take place.

- Wired
  Scans that go out on the wire to discover devices and vulnerabilities.
- Wireless
  Scans that are performed wirelessly to watch for attacks and detect wireless devices around the unit.

Login page

Protective Cloud Services portal.

1. Our customer portal is at https://fido.guarddog.ai. Once you go there you will see the screen below. Then enter your credentials.



Login

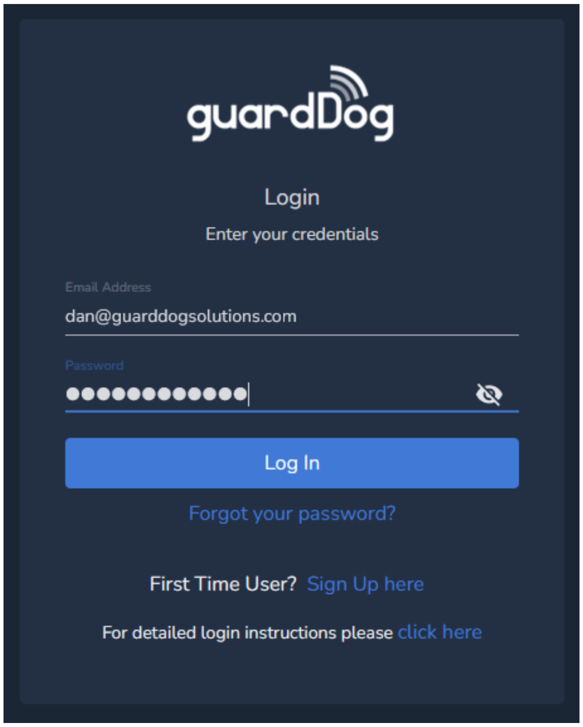
Enter your credentials

Email Address

Password

First Time User? Sign Up here

For detailed login instructions please click here



Login

Enter your credentials

Email Address
dan@guarddogsolutions.com

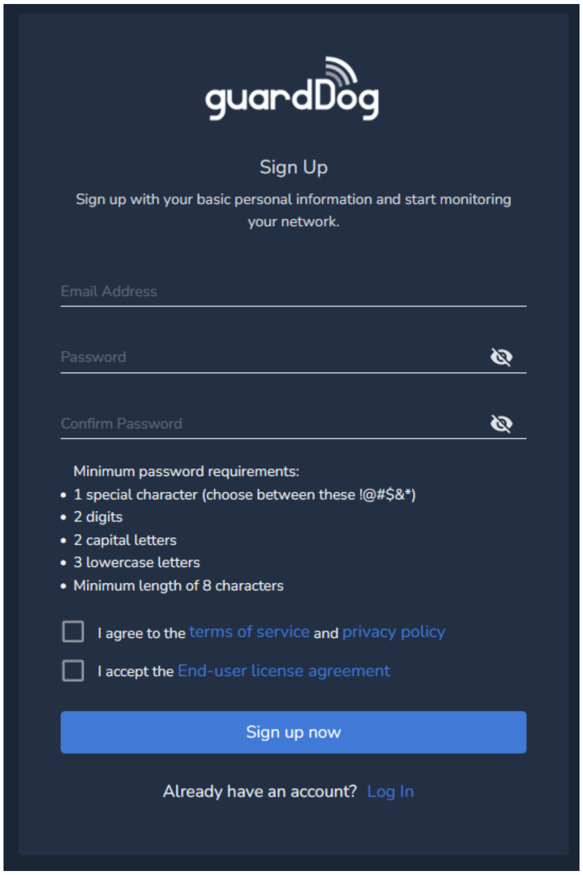
Password
●●●●●●●●●●●●

First Time User? Sign Up here

For detailed login instructions please click here

If it is the first time you are accessing this portal, then you would need to create an account. Click on Sign Up to create the account and then just follow the steps on the screen.

Pay special attention to the requirements for the password. Although we require a password that is at least 8 characters long, it is recommended that you choose a password that is at least 20 characters long.



guardDog

Sign Up

Sign up with your basic personal information and start monitoring your network.

Email Address

Password

Confirm Password

Minimum password requirements:

- 1 special character (choose between these !@#$&*)
- 2 digits
- 2 capital letters
- 3 lowercase letters
- Minimum length of 8 characters

□ I agree to the terms of service and privacy policy

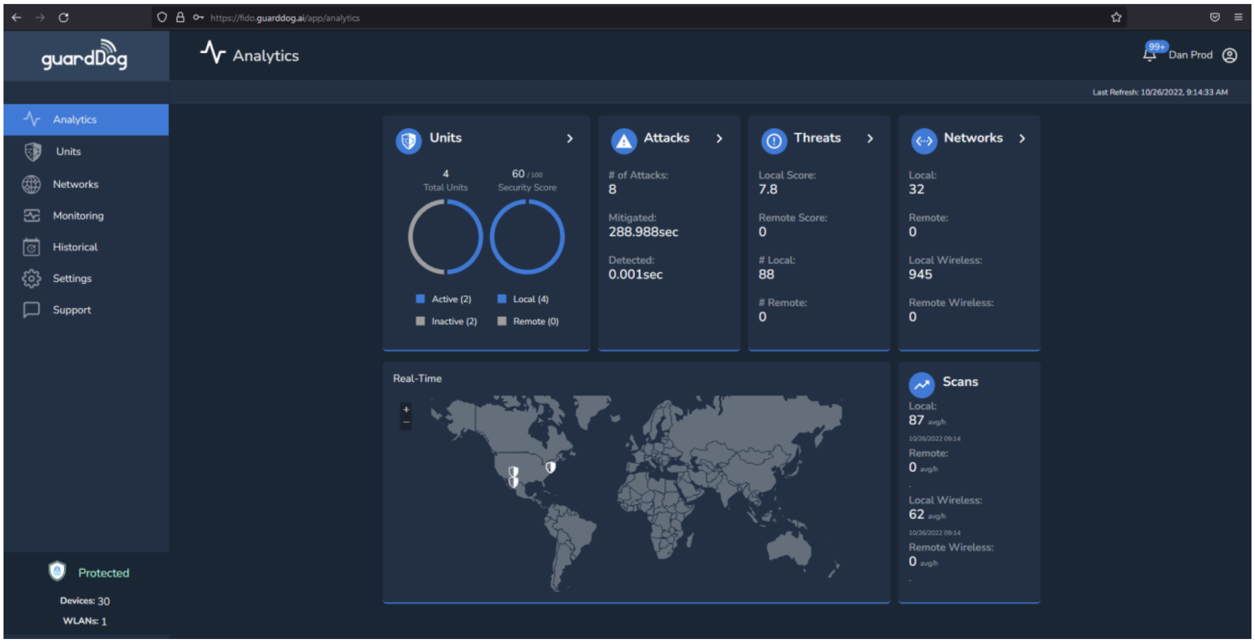
□ I accept the End-user license agreement

Sign up now

Already have an account? Log In

Analytics

This is our current landing page that shows the overall information for the entire system including data from all fido units registered in the system. Depending on the size and resolution of the screen it may fully show the menu on the left hand side of the screen,



Last Refresh: 10/26/2022, 9:14:33 AM

Units: 4 Total Units; 60 / 100 Security Score

Active (2) · Inactive (2) · Local (4) · Remote (0)

Attacks:
# of Attacks: 8
Mitigated: 288.988sec
Detected: 0.001sec

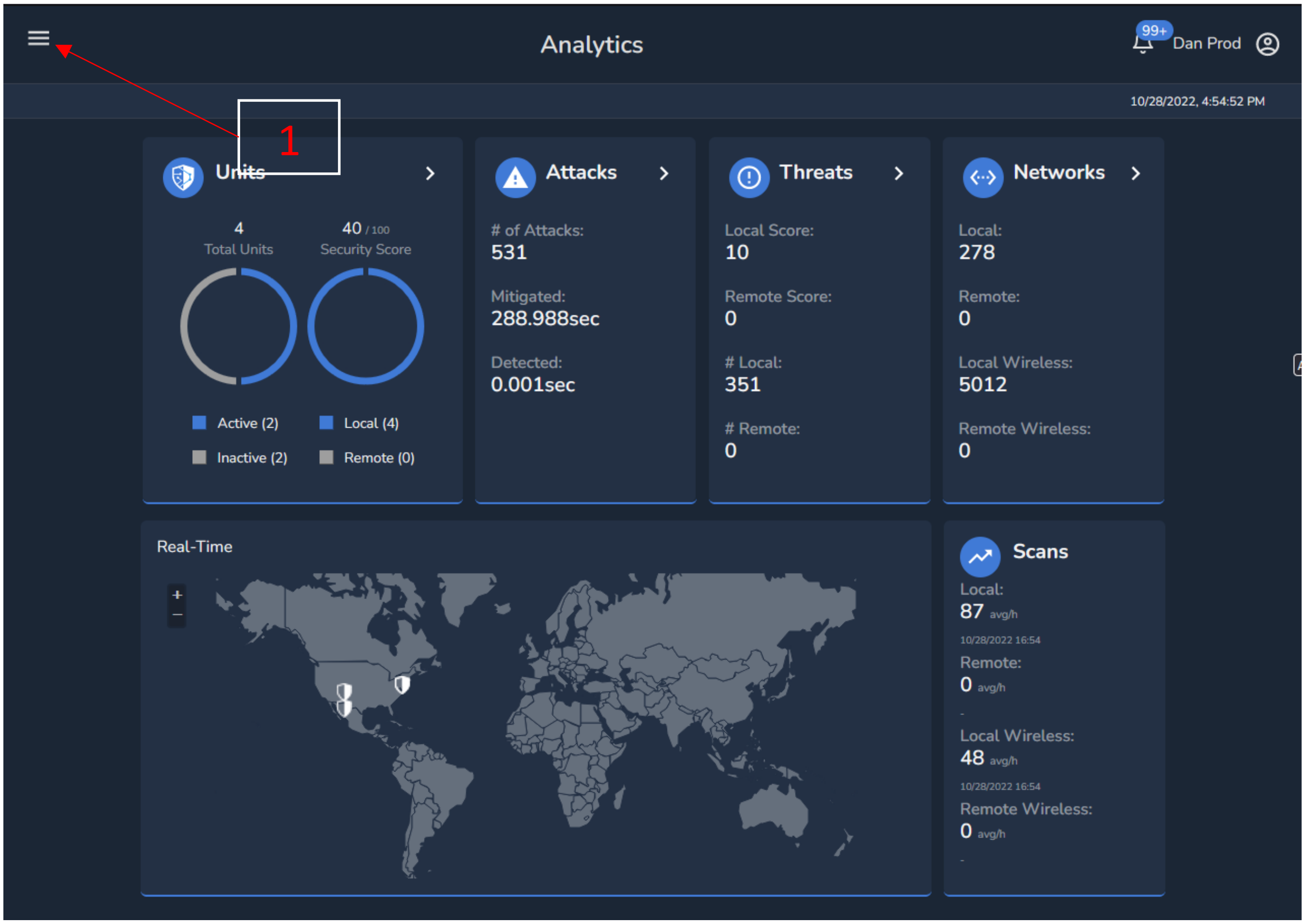
Threats:
Local Score: 7.8
Remote Score: 0
Local: 88
Remote: 0

Networks:
Local: 32
Remote: 0
Local Wireless: 945
Remote Wireless: 0

Scans:
Local: 87 avg/h
10/26/2022 09:14
Remote: 0 avg/h
Local Wireless: 62 avg/h
10/26/2022 09:14
Remote Wireless: 0 avg/h

Protected
Devices: 30
WLANs: 1

or show a reduced menu with the “hamburger menu icon” as shown below. You can display the menu by clicking on it.



10/28/2022, 4:54:52 PM

4 Total Units

40 / 100 Security Score

# of Attacks: 531

Mitigated: 288.988sec

Detected: 0.001sec

Local Score: 10

Remote Score: 0

Local: 351

Remote: 0

Local: 278

Remote: 0

Local Wireless: 5012

Remote Wireless: 0

Local: 87 avg/h

10/28/2022 16:54

Remote: 0 avg/h

-

Local Wireless: 48 avg/h

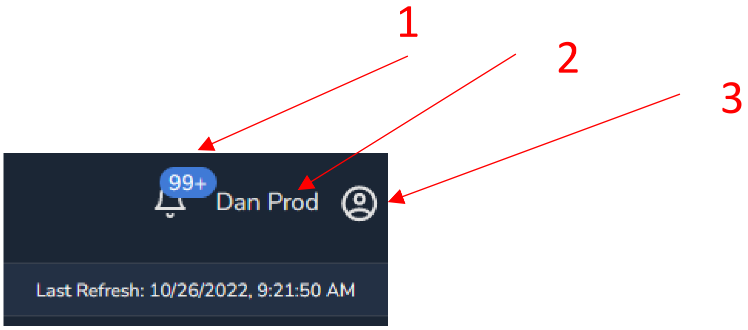
10/28/2022 16:54

Remote Wireless: 0 avg/h

-

Below we have the icons for:

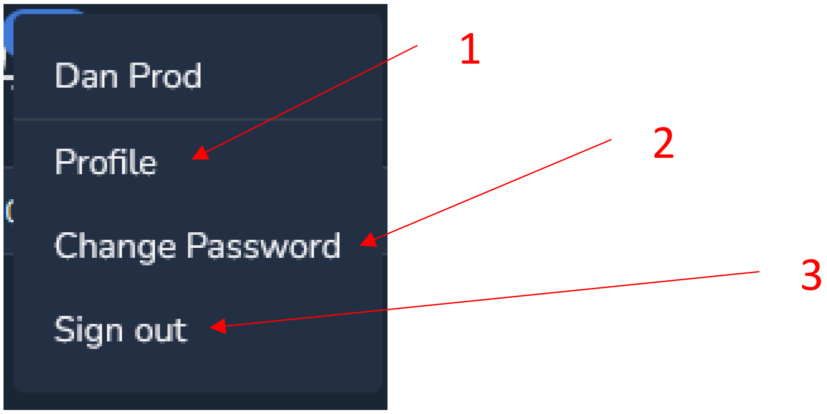
1. notifications
2. the name on the account
3. the avatar for the account



Last Refresh: 10/26/2022, 9:21:50 AM

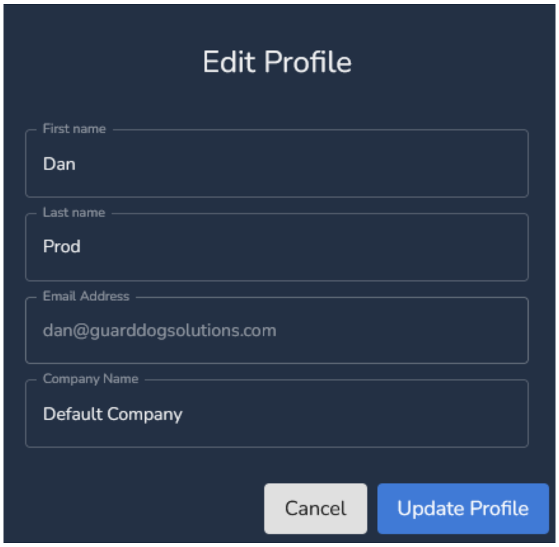
The avatar icon, by clicking on it you will get these options:

1. Profile
2. Change Password
3. Sign out



If you would like to change your password o sign out, then you would need to click on the corresponding option shown.

Clicking on Profile will pop up the customer’s profile with the information you have provided. The recommendation is that you fill this out completely. We take this information to show it in different parts of the portal.



Edit Profile

First name
Dan

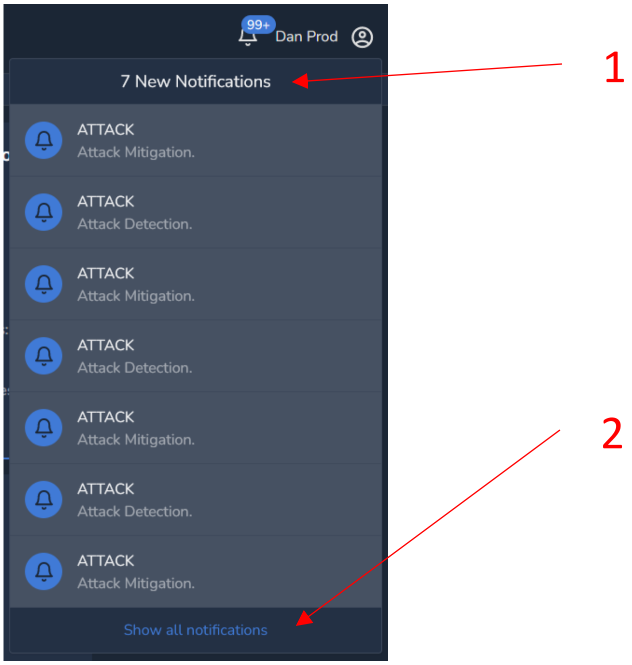
Last name
Prod

Email Address
dan@guarddogsolutions.com

Company Name
Default Company

The notifications icon. Click on it and then you will get the latest 7 notifications. To get to all notifications then you will need to click on “Show all notifications” below.

1. Latest 7 notifications
2. All notifications

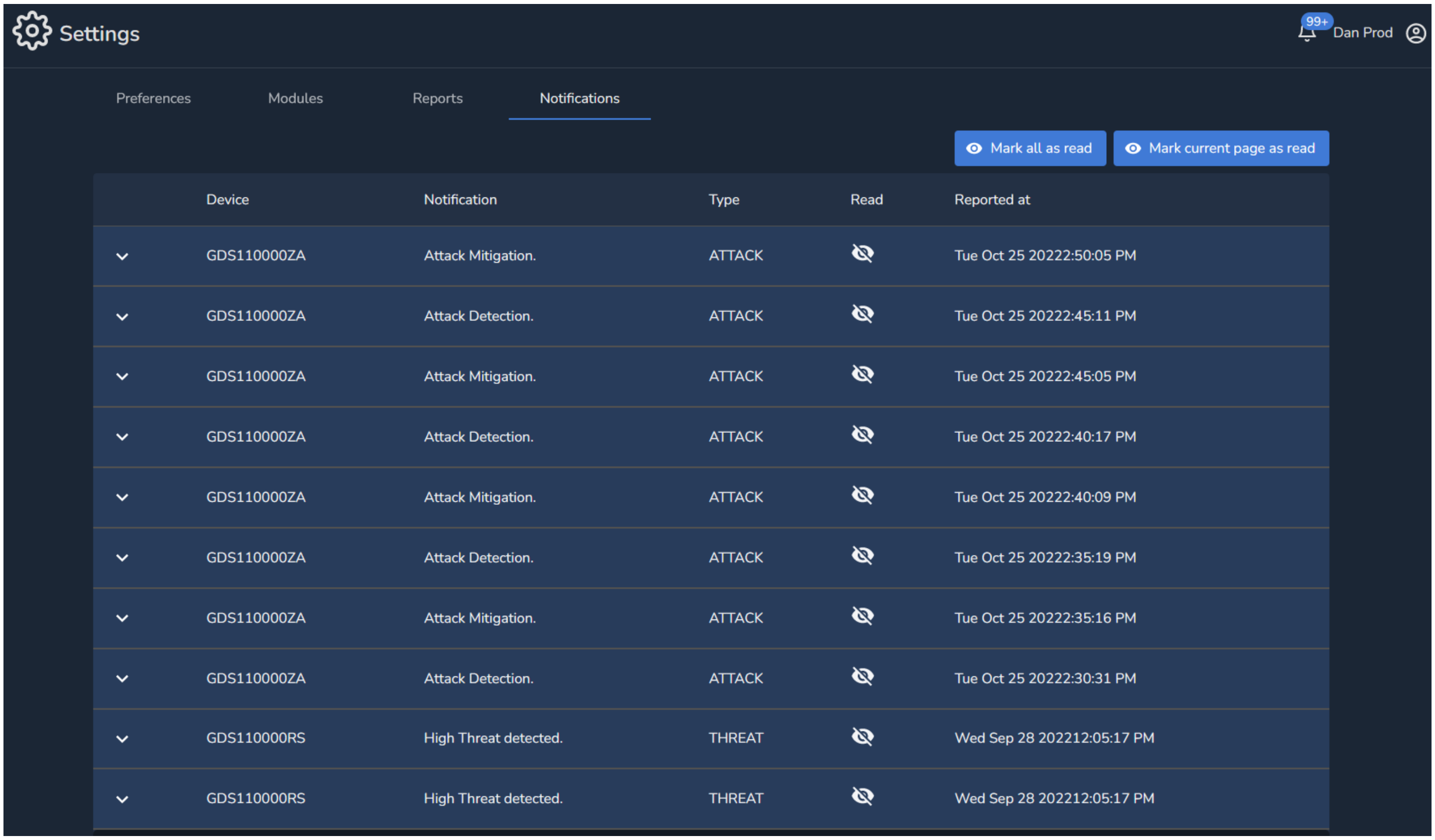


7 New Notifications

- ATTACK
  Attack Mitigation.
- ATTACK
  Attack Detection.
- ATTACK
  Attack Mitigation.
- ATTACK
  Attack Detection.
- ATTACK
  Attack Mitigation.
- ATTACK
  Attack Detection.
- ATTACK
  Attack Mitigation.

Show all notifications

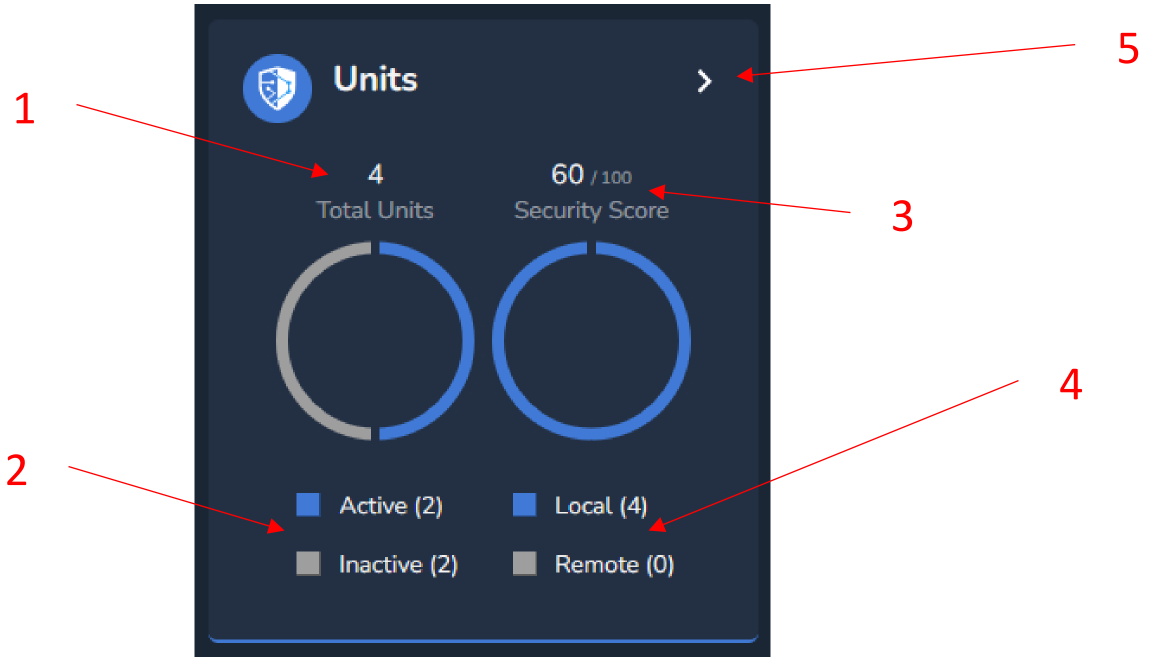
The notifications page. You can get to the page by going to Settings > Notifications. Here is a sample of that page. We will go into more details in the Settings section of this manual.



	Device	Notification	Type	Read	Reported at
⌄	GDS110000ZA	Attack Mitigation.	ATTACK		Tue Oct 25 20222:50:05 PM
⌄	GDS110000ZA	Attack Detection.	ATTACK		Tue Oct 25 20222:45:11 PM
⌄	GDS110000ZA	Attack Mitigation.	ATTACK		Tue Oct 25 20222:45:05 PM
⌄	GDS110000ZA	Attack Detection.	ATTACK		Tue Oct 25 20222:40:17 PM
⌄	GDS110000ZA	Attack Mitigation.	ATTACK		Tue Oct 25 20222:40:09 PM
⌄	GDS110000ZA	Attack Detection.	ATTACK		Tue Oct 25 20222:35:19 PM
⌄	GDS110000ZA	Attack Mitigation.	ATTACK		Tue Oct 25 20222:35:16 PM
⌄	GDS110000ZA	Attack Detection.	ATTACK		Tue Oct 25 20222:30:31 PM
⌄	GDS110000RS	High Threat detected.	THREAT		Wed Sep 28 202212:05:17 PM
⌄	GDS110000RS	High Threat detected.	THREAT		Wed Sep 28 202212:05:17 PM

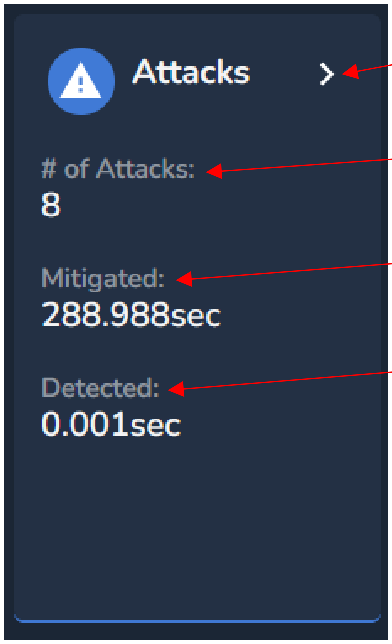
The Units card. The first card we show in the Analytics page is the Units card.

1. This shows the total number of units registered in the system
2. The number of units that are active and those inactive. This refers to the units that are communicating or not with the main system in the Cloud. Once we do not see the unit connected then we will show that unit as inactive.
3. We also show our proprietary simple security score. The Security Score is a graphical representation of the risk and vulnerability of your network and the devices in it. Today the simple score is based on the units you have, the vulnerabilities found and then severity level of those vulnerabilities.
4. There is also the notion of Local and Remote units. Please refer to the Terminology section for more information on this categorization.
5. The tip of the arrow takes you to the Units page when clicked on. See the Units section for more information.



The attacks card. This shows if there have been any attacks so far on your network within the time interval chosen for the module, please refer to the Settings section for more information on this.

1. Arrow to open the attacks page.
2. Total number of attacks
3. The amount of time it took to mitigate all the attacks
4. The amount of time that took to detect the attacks



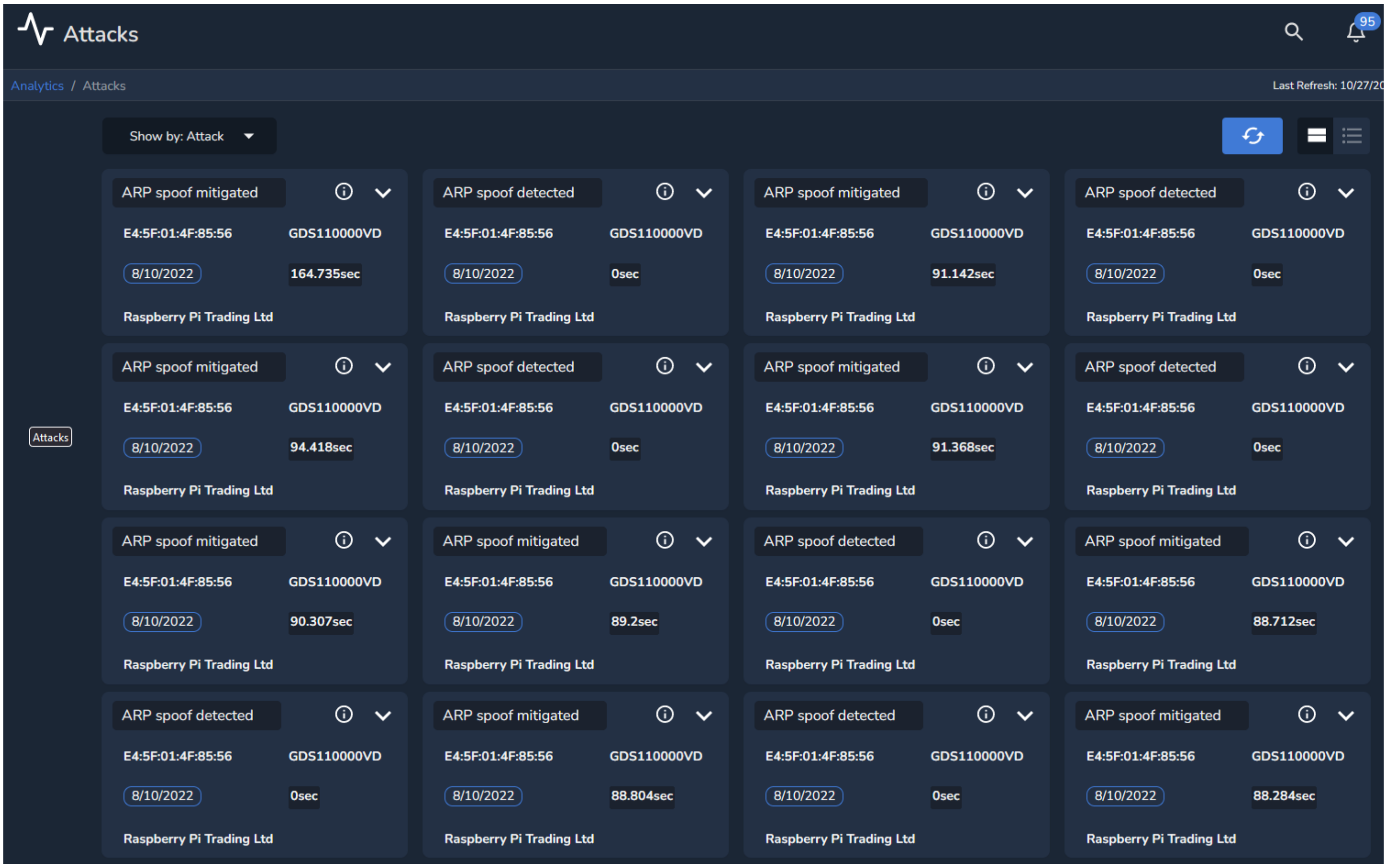
Attacks >

# of Attacks:
8

Mitigated:
288.988sec

Detected:
0.001sec

The attacks page. This page shows all the attacks detected by al units in the system. Here is a sample of it.



Attacks

Analytics / Attacks

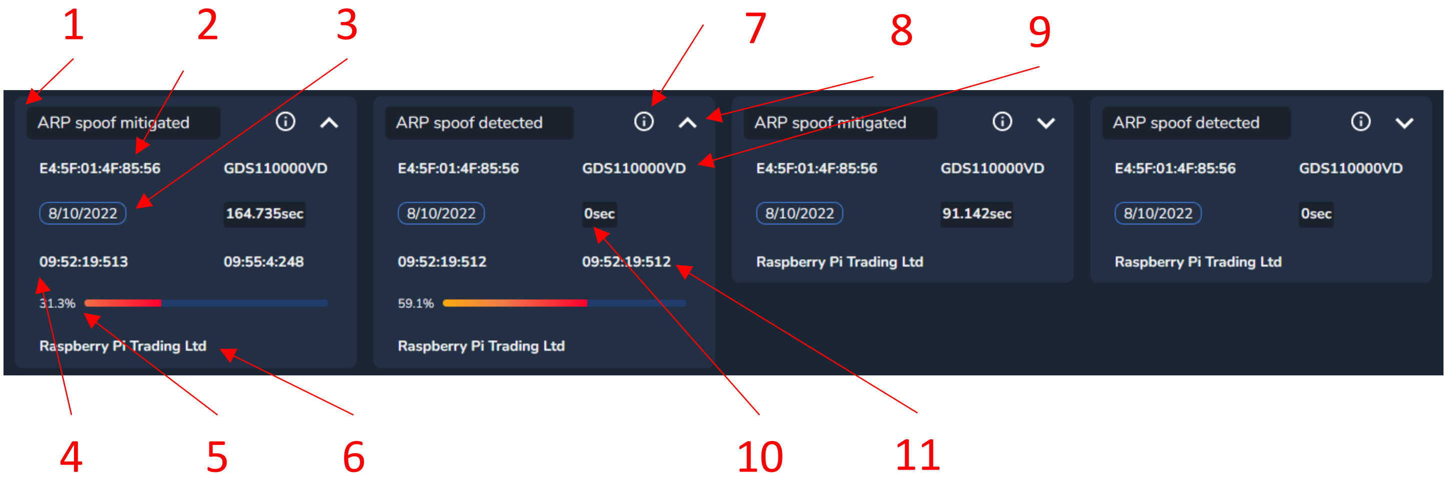
Last Refresh: 10/27/20

Show by: Attack

ARP spoof mitigated E4:5F:01:4F:85:56 GDS110000VD 8/10/2022 164.735sec Raspberry Pi Trading Ltd	ARP spoof detected E4:5F:01:4F:85:56 GDS110000VD 8/10/2022 0sec Raspberry Pi Trading Ltd	ARP spoof mitigated E4:5F:01:4F:85:56 GDS110000VD 8/10/2022 91.142sec Raspberry Pi Trading Ltd	ARP spoof detected E4:5F:01:4F:85:56 GDS110000VD 8/10/2022 0sec Raspberry Pi Trading Ltd
ARP spoof mitigated E4:5F:01:4F:85:56 GDS110000VD 8/10/2022 94.418sec Raspberry Pi Trading Ltd	ARP spoof detected E4:5F:01:4F:85:56 GDS110000VD 8/10/2022 0sec Raspberry Pi Trading Ltd	ARP spoof mitigated E4:5F:01:4F:85:56 GDS110000VD 8/10/2022 91.368sec Raspberry Pi Trading Ltd	ARP spoof detected E4:5F:01:4F:85:56 GDS110000VD 8/10/2022 0sec Raspberry Pi Trading Ltd
ARP spoof mitigated E4:5F:01:4F:85:56 GDS110000VD 8/10/2022 90.307sec Raspberry Pi Trading Ltd	ARP spoof mitigated E4:5F:01:4F:85:56 GDS110000VD 8/10/2022 89.2sec Raspberry Pi Trading Ltd	ARP spoof detected E4:5F:01:4F:85:56 GDS110000VD 8/10/2022 0sec Raspberry Pi Trading Ltd	ARP spoof mitigated E4:5F:01:4F:85:56 GDS110000VD 8/10/2022 88.712sec Raspberry Pi Trading Ltd
ARP spoof detected E4:5F:01:4F:85:56 GDS110000VD 8/10/2022 0sec Raspberry Pi Trading Ltd	ARP spoof mitigated E4:5F:01:4F:85:56 GDS110000VD 8/10/2022 88.804sec Raspberry Pi Trading Ltd	ARP spoof detected E4:5F:01:4F:85:56 GDS110000VD 8/10/2022 0sec Raspberry Pi Trading Ltd	ARP spoof mitigated E4:5F:01:4F:85:56 GDS110000VD 8/10/2022 88.284sec Raspberry Pi Trading Ltd

The attack card. Below we show cards for detection and for mitigation both expanded and collapsed, for more information on this please see Terminology. The card has several elements:

1. Name of the attack detected.
2. MAC address of the attacker.
3. Date of the attack.
4. Time the action started.
5. Percentage of attacks based on overall total.
6. Manufacturer of the attacking device.
7. Information/description icon.
8. Arrow to expand/collapse the card.
9. Unit that performed the action.
10. Total time that took for the action to be performed.
11. Time at which the action performed finished.



ARP spoof mitigated
E4:5F:01:4F:85:56 GDS110000VD
8/10/2022 164.735sec
09:52:19:513 09:55:4:248
31.3%
Raspberry Pi Trading Ltd

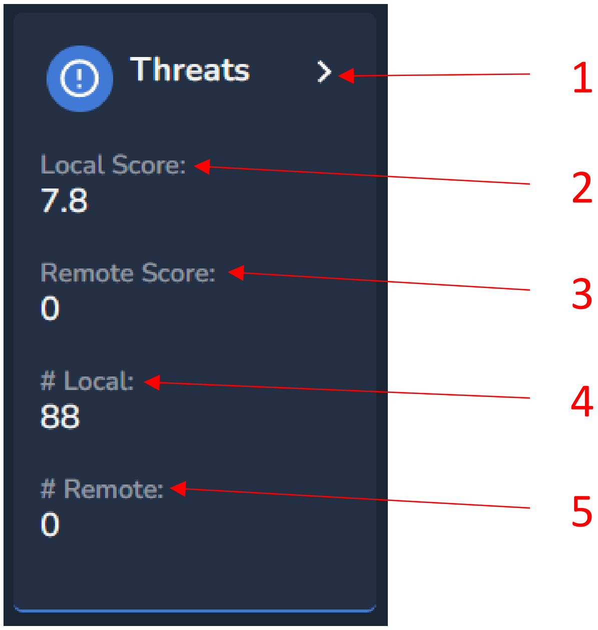
ARP spoof detected
E4:5F:01:4F:85:56 GDS110000VD
8/10/2022 0sec
09:52:19:512 09:52:19:512
59.1%
Raspberry Pi Trading Ltd

ARP spoof mitigated
E4:5F:01:4F:85:56 GDS110000VD
8/10/2022 91.142sec
Raspberry Pi Trading Ltd

ARP spoof detected
E4:5F:01:4F:85:56 GDS110000VD
8/10/2022 0sec
Raspberry Pi Trading Ltd

The threats card. This shows the overall threats information in the system both in local and remote units. Please refer to the Terminology section for more information.

1. Arrow to open the threats page.
2. Local score. The severity level of all local units
3. Remote score. The severity vulnerability level of all remote units.
4. Number of local threats. Total number of threats found by local units.
5. Number of remote threats. Total number of threats found by remote units.



Threats

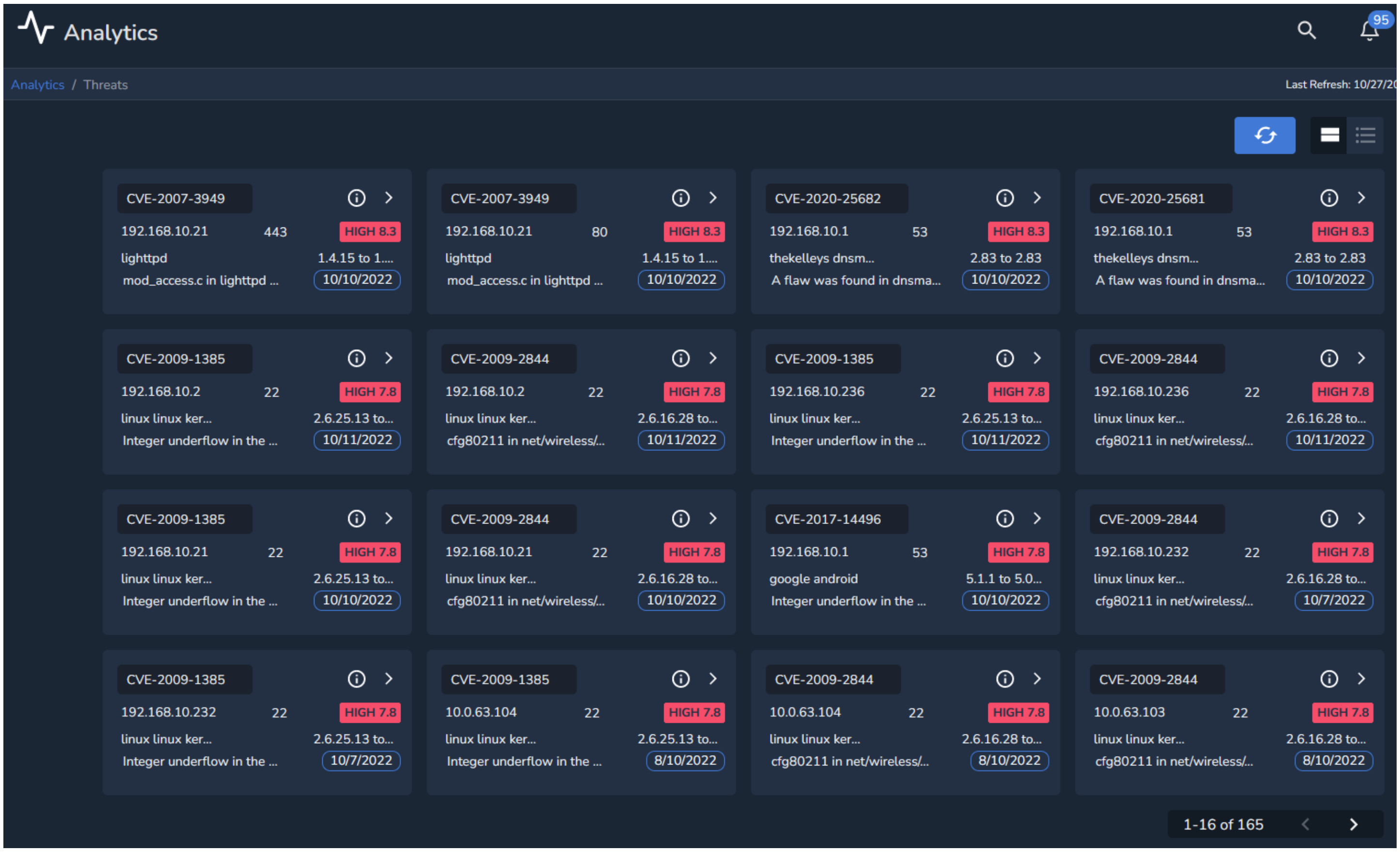
Local Score:
7.8

Remote Score:
0

Local:
88

Remote:
0

The threats page. The page shows all the threats found by all units in the system.



CVE-2007-3949
192.168.10.21 443 HIGH 8.3
lighttpd 1.4.15 to 1....
mod_access.c in lighttpd ... 10/10/2022

CVE-2007-3949
192.168.10.21 80 HIGH 8.3
lighttpd 1.4.15 to 1....
mod_access.c in lighttpd ... 10/10/2022

CVE-2020-25682
192.168.10.1 53 HIGH 8.3
thekelleys dnsm... 2.83 to 2.83
A flaw was found in dnsma... 10/10/2022

CVE-2020-25681
192.168.10.1 53 HIGH 8.3
thekelleys dnsm... 2.83 to 2.83
A flaw was found in dnsma... 10/10/2022

CVE-2009-1385
192.168.10.2 22 HIGH 7.8
linux linux ker... 2.6.25.13 to...
Integer underflow in the ... 10/11/2022

CVE-2009-2844
192.168.10.2 22 HIGH 7.8
linux linux ker... 2.6.16.28 to...
cfg80211 in net/wireless/... 10/11/2022

CVE-2009-1385
192.168.10.236 22 HIGH 7.8
linux linux ker... 2.6.25.13 to...
Integer underflow in the ... 10/11/2022

CVE-2009-2844
192.168.10.236 22 HIGH 7.8
linux linux ker... 2.6.16.28 to...
cfg80211 in net/wireless/... 10/11/2022

CVE-2009-1385
192.168.10.21 22 HIGH 7.8
linux linux ker... 2.6.25.13 to...
Integer underflow in the ... 10/10/2022

CVE-2009-2844
192.168.10.21 22 HIGH 7.8
linux linux ker... 2.6.16.28 to...
cfg80211 in net/wireless/... 10/10/2022

CVE-2017-14496
192.168.10.1 53 HIGH 7.8
google android 5.1.1 to 5.0...
Integer underflow in the ... 10/10/2022

CVE-2009-2844
192.168.10.232 22 HIGH 7.8
linux linux ker... 2.6.16.28 to...
cfg80211 in net/wireless/... 10/7/2022

CVE-2009-1385
192.168.10.232 22 HIGH 7.8
linux linux ker... 2.6.25.13 to...
Integer underflow in the ... 10/7/2022

CVE-2009-1385
10.0.63.104 22 HIGH 7.8
linux linux ker... 2.6.25.13 to...
Integer underflow in the ... 8/10/2022

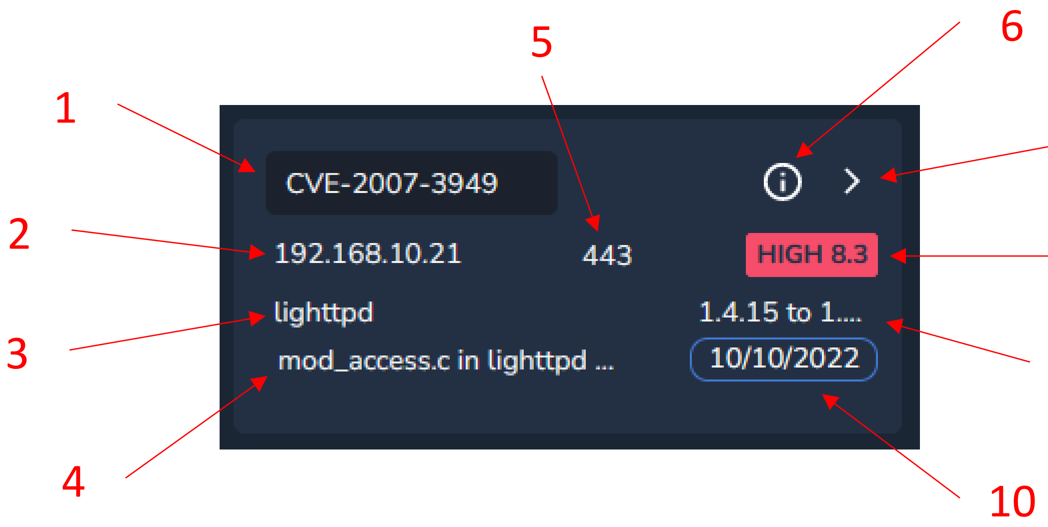
CVE-2009-2844
10.0.63.104 22 HIGH 7.8
linux linux ker... 2.6.16.28 to...
cfg80211 in net/wireless/... 8/10/2022

CVE-2009-2844
10.0.63.103 22 HIGH 7.8
linux linux ker... 2.6.16.28 to...
cfg80211 in net/wireless/... 8/10/2022

The threats card. This card shows the information about a specific threat found on a device connected to the network. The following items are part of the card:

1. CVE of the vulnerability.

2. Device where the vulnerability was found.
3. Software affected.
4. Brief description of the vulnerability.
5. Open port related to it.
6. Information/description icon.
7. Arrow to go to NIST article about the vulnerability.
8. Score of vulnerability.
9. Version impacted.
10. Date discovered.



CVE-2007-3949

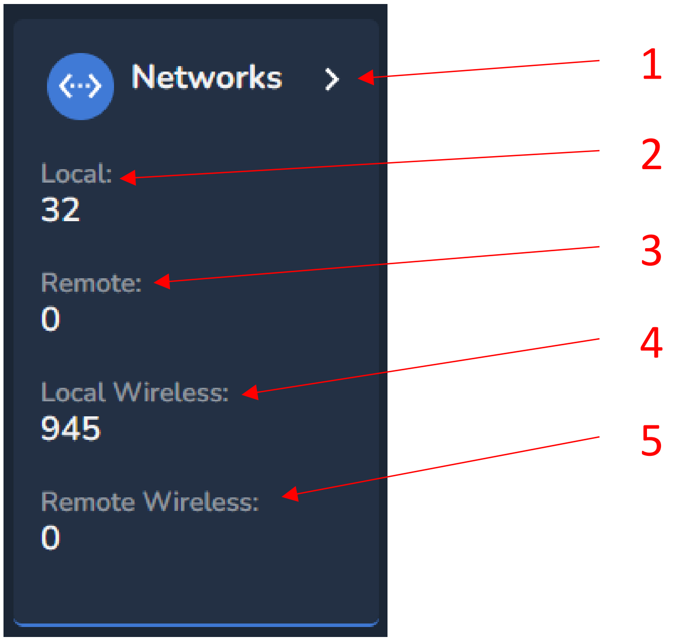
192.168.10.21 443 HIGH 8.3

lighttpd 1.4.15 to 1....

mod_access.c in lighttpd ... 10/10/2022

The networks card. This shows information from the different networks detected by all units, local and remote, registered in the system. Depending on the configuration of the network this will show all devices connected to the network whether they are wired or wireless. Wireless in this card refers to wireless networks found by all the units. For a definition on how local and remote units are classified please refer to the Terminology section.

1. Arrow to open the networks page. The networks page. This takes to same page the Network menu item does. You can get more details by going to the Networks menu option.
2. Local. These shown here are all network devices found by local units.
3. Remote. These represent the total number of connected devices found by remote units.
4. Local wireless. These are the wireless networks, and surrounding wireless devices transmitting, found by local units.
5. Remote wireless. These are the wireless networks, and surrounding wireless devices transmitting, found by remote units.



Networks

Local:
32

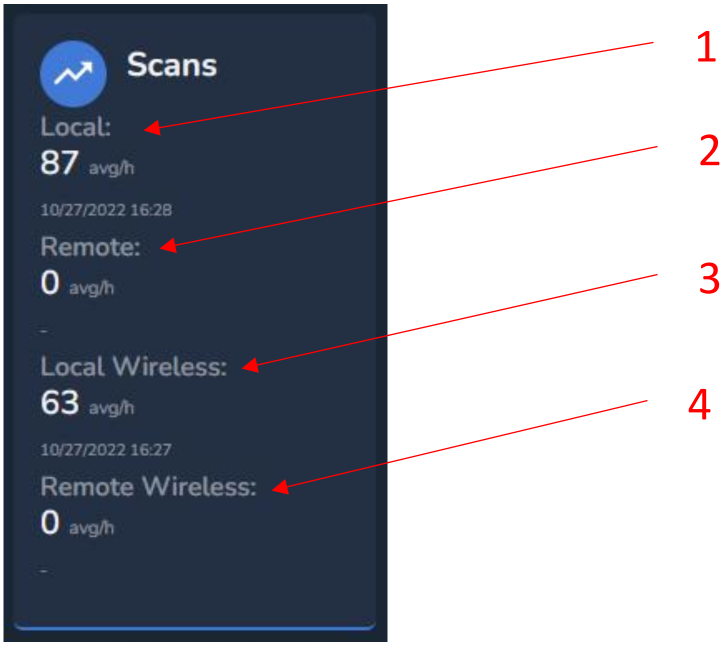
Remote:
0

Local Wireless:
945

Remote Wireless:
0

The scans card. The system is constantly scanning multiple times an hour in both the wire and wireless connections. This is represented by the average number of scans performed in 1 hour based on the last 24 hours. The way to ready this in our example would be that the local units scanned the wired network an average of 87 times per hour, and for the wireless would be that the units scanned the wireless area around them an average of 63 times per hour.

1. Local wired scans.
2. Remote wired scans.
3. Local wireless scans.
4. Remote wireless scans.



Scans

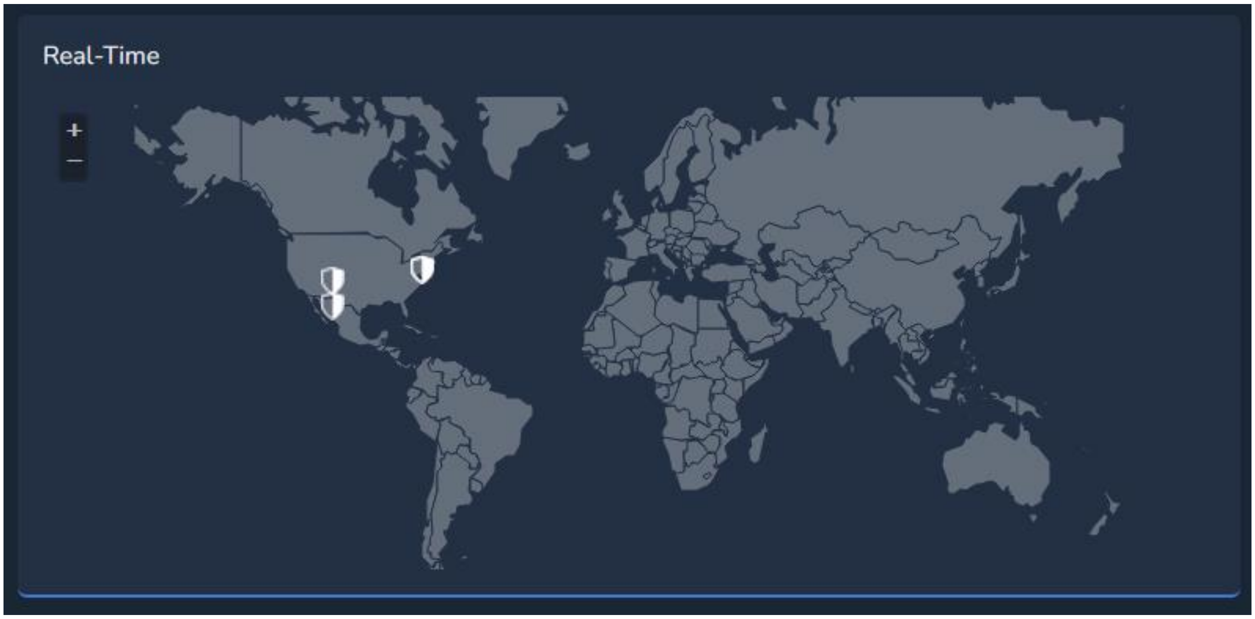
Local:
87 avg/h
10/27/2022 16:28

Remote:
0 avg/h
-

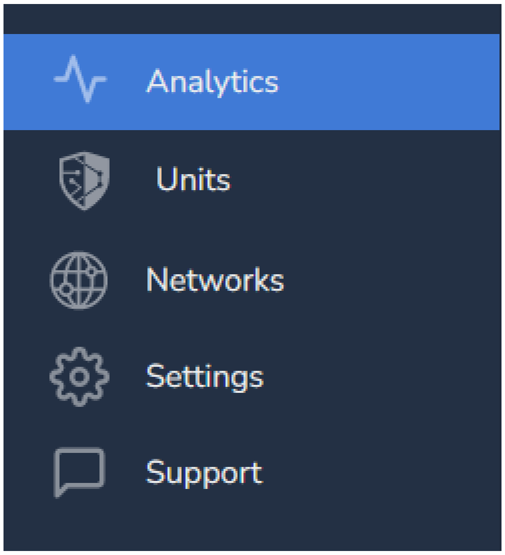
Local Wireless:
63 avg/h
10/27/2022 16:27

Remote Wireless:
0 avg/h
-

The global map. The system is designed with growth and being capable of managing multiple devices throughout the world. In the map we show a shield icon on those locations where a fido unit has been deployed. By clicking on the shield we will show the device GDS id and its location.



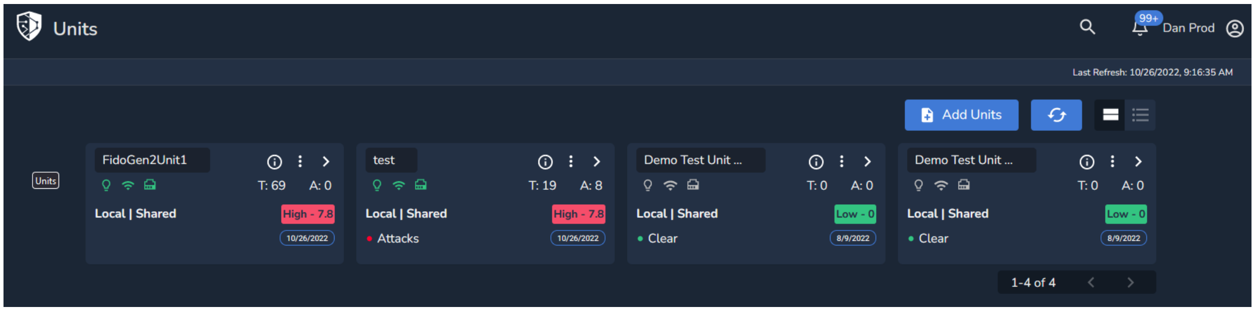
The main menu is located on the left side of the screen. The menu items shown may differ based on the license and modules activated.



Units

This is in reference to those fido units registered in the system. To reiterate we have the notion of local and remote, please see the Terminology section.

This is the main screen for Units. Here all the units registered in the system, both active and inactive, will be shown.



Units

99+ Dan Prod

Last Refresh: 10/26/2022, 9:16:35 AM

Add Units

Units

FidoGen2Unit1
T: 69 A: 0
Local | Shared High - 7.8
10/26/2022

test
T: 19 A: 8
Local | Shared High - 7.8
● Attacks 10/26/2022

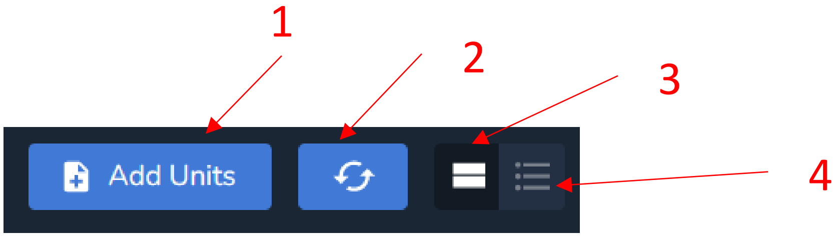
Demo Test Unit ...
T: 0 A: 0
Local | Shared Low - 0
● Clear 8/9/2022

Demo Test Unit ...
T: 0 A: 0
Local | Shared Low - 0
● Clear 8/9/2022

1-4 of 4

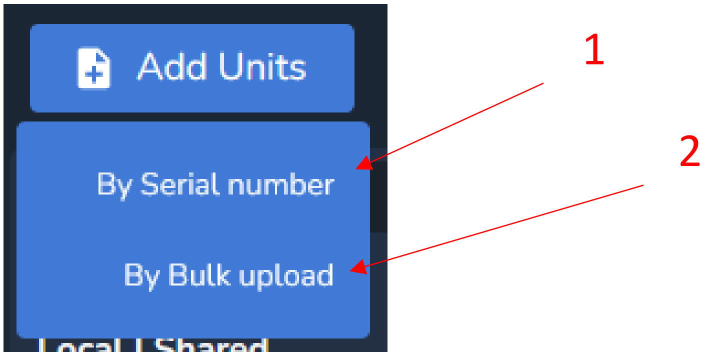
On the top right we have several buttons:

1. Add units
2. Refresh
3. Card view
4. Table view.



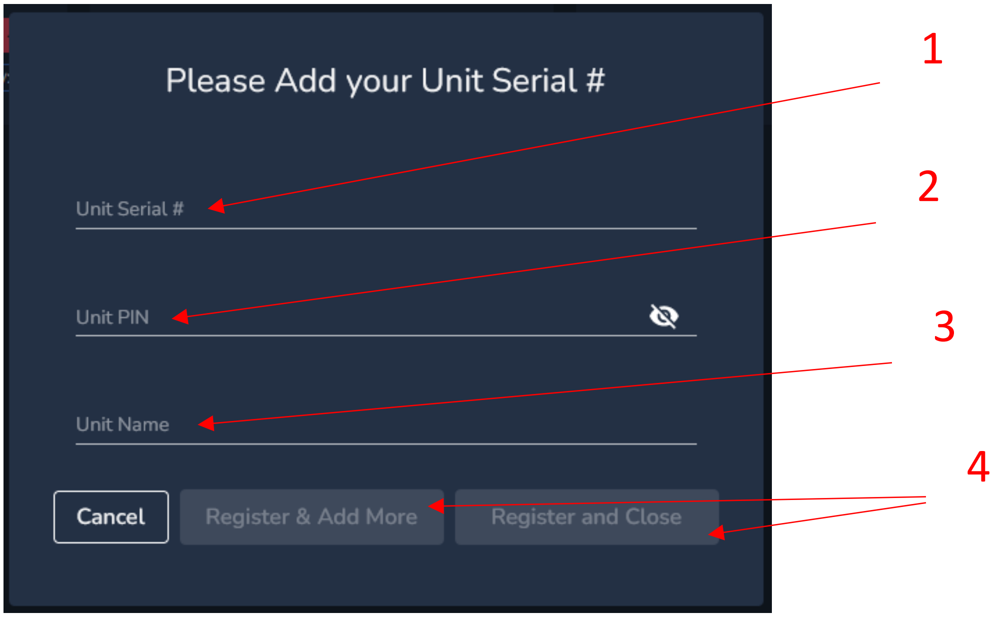
The Add Units button is one of the ways to register units in the system. Once you add the units you will then receive a pop-up with the confirmation on the units being added. By clicking on it we get:

1. Add by serial number. To do this you will need the serial number and pin for the unit. You can find this on the box the unit came in, and on the bottom of the unit itself.
2. Add by bulk upload. This method allows you to add more than one unit at a time.



When adding by serial number you will be prompted to enter:

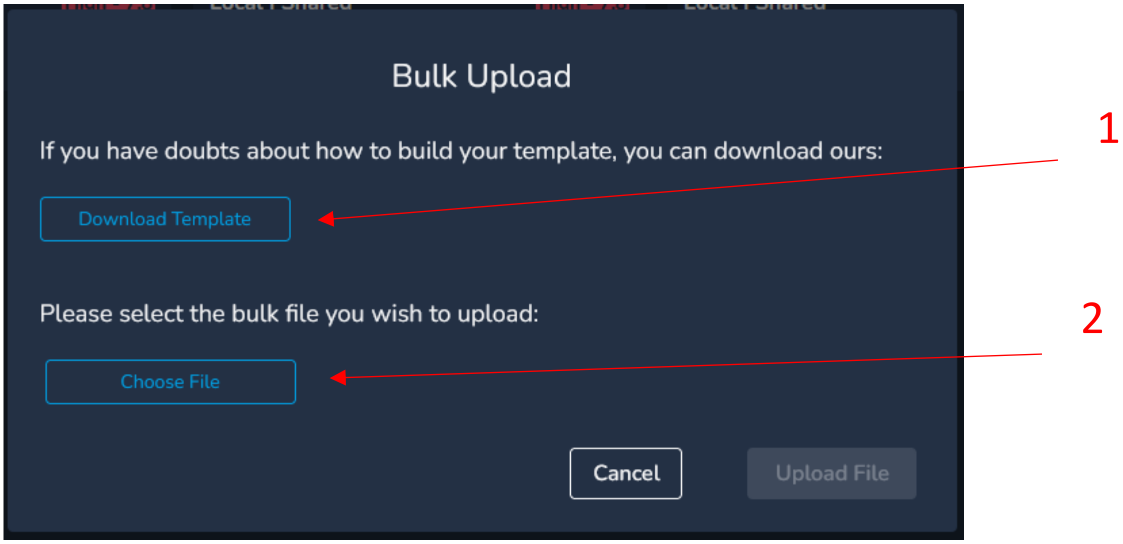
1. Serial number for the unit. You can find this on the label as explained before.
2. PIN number for the unit. You can find this on the label as explained before.
3. A friendly name for the unit. This can be anything you'd like to use to reference the unit being registered (i.e. Lobby unit, 4th floor, Dallas Building 2, HR department, etc)
4. When you have entered all required information then you can choose between registering that one unit and closing the window, or registering that unit and adding another one.



Please Add your Unit Serial #

By clicking on bulk upload, you will then be able to:

1. Download the template to add all fido units in it.
2. Then upload the upload that filled out template to add the fido units.

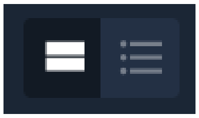


Bulk Upload

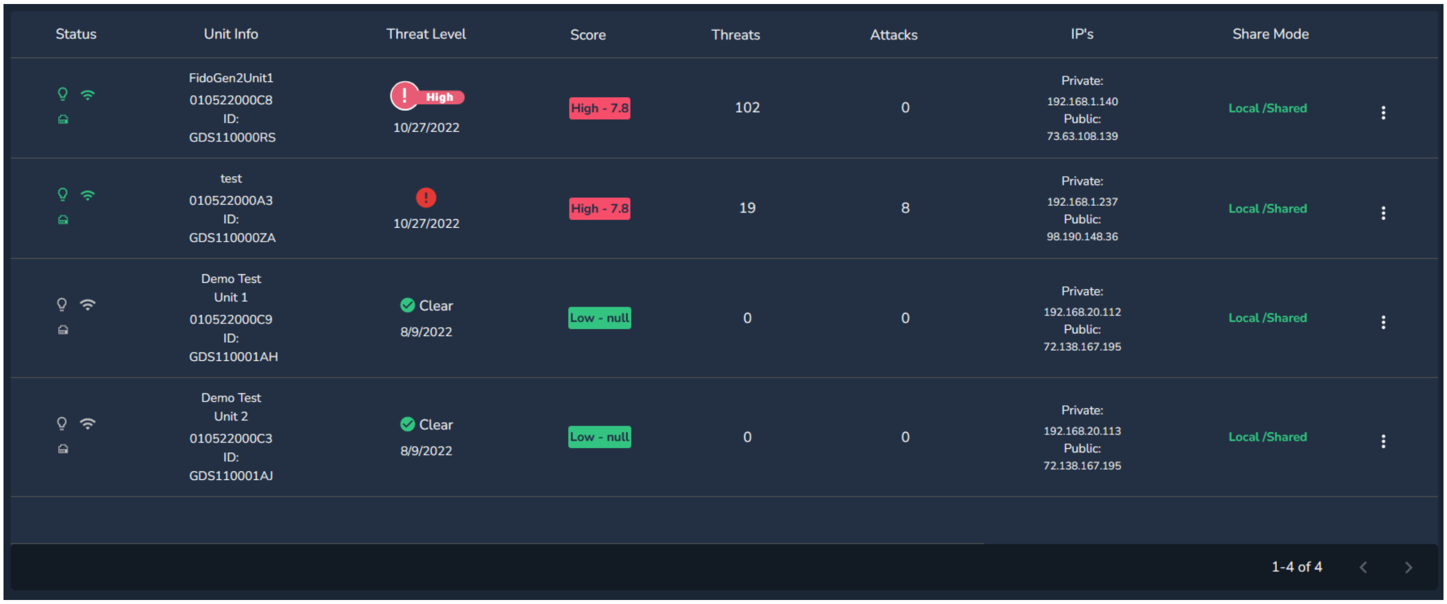
If you have doubts about how to build your template, you can download ours:

Please select the bulk file you wish to upload:

The Card view and Table view buttons allow you to change how the information on the screen is shown. By default the information in the system is shown in



This is an example of how units will show when the table view is selected. The information on this table will be explained next on the unit card.

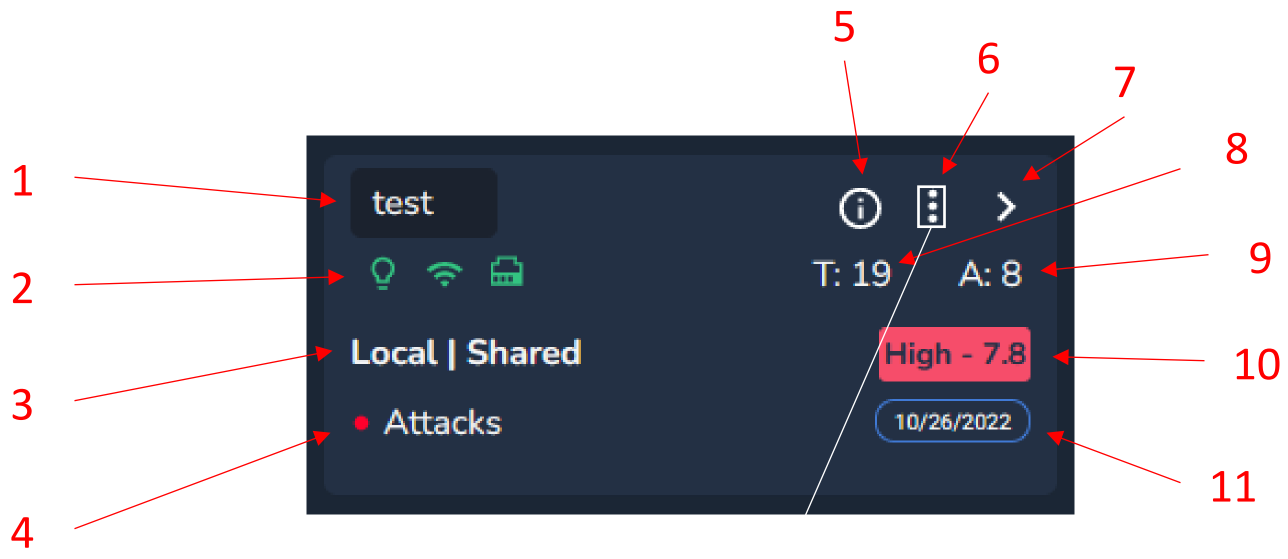


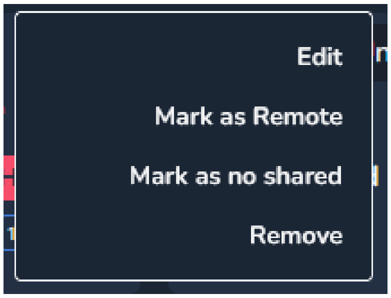
Status	Unit Info	Threat Level	Score	Threats	Attacks	IP's	Share Mode	
💡 📶 🖧	FidoGen2Unit1 010522000C8 ID: GDS110000RS	! High 10/27/2022	High - 7.8	102	0	Private: 192.168.1.140 Public: 73.63.108.139	Local /Shared	⋮
💡 📶 🖧	test 010522000A3 ID: GDS110000ZA	! 10/27/2022	High - 7.8	19	8	Private: 192.168.1.237 Public: 98.190.148.36	Local /Shared	⋮
💡 📶 🖧	Demo Test Unit 1 010522000C9 ID: GDS110001AH	✓ Clear 8/9/2022	Low - null	0	0	Private: 192.168.20.112 Public: 72.138.167.195	Local /Shared	⋮
💡 📶 🖧	Demo Test Unit 2 010522000C3 ID: GDS110001AJ	✓ Clear 8/9/2022	Low - null	0	0	Private: 192.168.20.113 Public: 72.138.167.195	Local /Shared	⋮

The unit card. This is the main card for the unit we have deployed and registered in the system. There are multiple places to look at here:

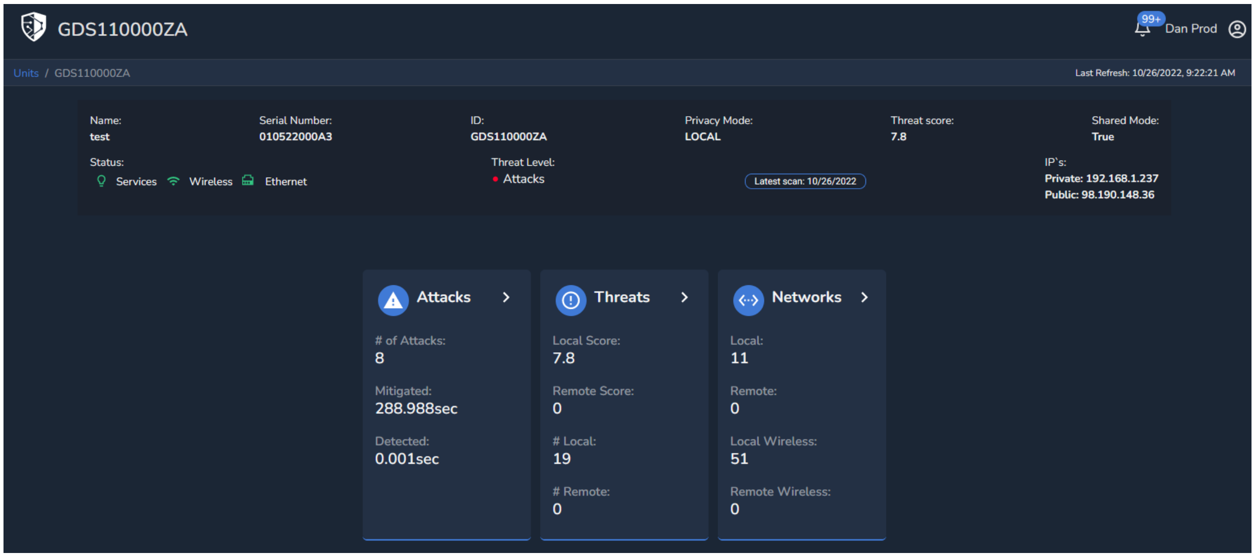
1. Friendly name for the unit. This is the name you chose for the unit when registering it.
2. Status icons. From left to right:
   a. Services up (green) or down (red)
   b. Wireless on
   c. Ethernet on
3. Unit type and Shared mode.
   a. Type (see terminology)
      i. Local
      ii. Remote
   b. Shared mode (see Terminology)
      i. Shared
      ii. Not shared
4. Alert of attacks. This will be displayed when attacks are detected.
5. Information/description icon. By clicking on it you will see a brief description of the card items.
6. Action menu. See the image below for items:
   a. Edit the unit's friendly name

   b. Mark the unit as Local or Remote. This depends on the current mode, so it is dynamic.
   c. Mark as not shared
   d. Remove the unit from the system
7. Open unit. This will display a details page. See Unit Details section.
8. Threat count. Total number of threats found by the unit.
9. Attack count. Total number of attacks detected by the unit.
10. Threat score. Highest level of severity of vulnerabilities found.
11. Last updated. Last time the data was received and refreshed from the unit.





The Unit details page. Below you will see the page where we show all the information related to a specific unit.



GDS110000ZA

99+ Dan Prod

Units / GDS110000ZA

Last Refresh: 10/26/2022, 9:22:21 AM

Name: test

Serial Number: 010522000A3

ID: GDS110000ZA

Privacy Mode: LOCAL

Threat score: 7.8

Shared Mode: True

Status: Services Wireless Ethernet

Threat Level: ● Attacks

Latest scan: 10/26/2022

IP`s:
Private: 192.168.1.237
Public: 98.190.148.36

Attacks

# of Attacks: 8

Mitigated: 288.988sec

Detected: 0.001sec

Threats

Local Score: 7.8

Remote Score: 0

Local: 19

Remote: 0

Networks

Local: 11

Remote: 0

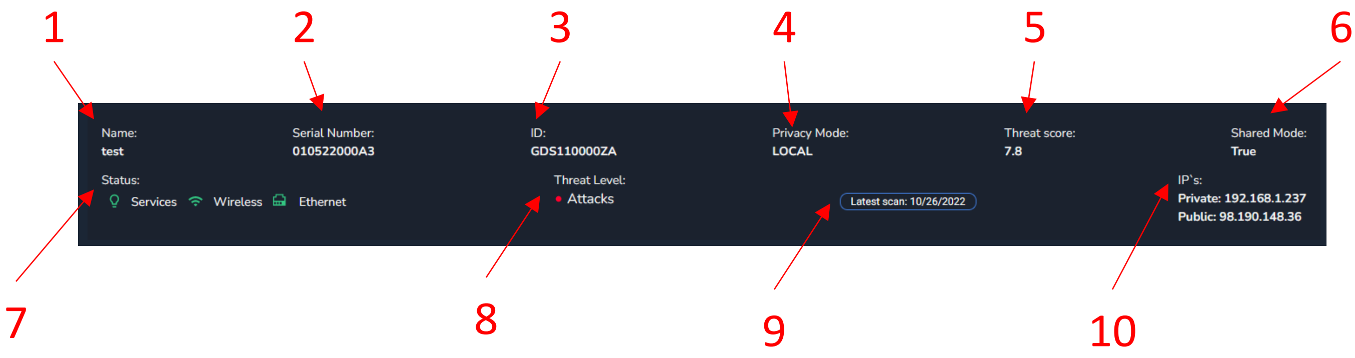
Local Wireless: 51

Remote Wireless: 0

There are multiple items on this page, let’s go through all of them:

1. Friendly name of the unit. This is the name you chose for the unit when registering it.
2. Serial number. This is the serial number that was used to register the unit.
3. GDS ID. This is an identification name provided by the system. This cannot be modified.
4. Privacy mode.
   a. Shared.
   b. Not shared.
5. Threat score.
6. Shared mode.
7. Status icons. From left to right:
   a. Services up (green) or down (red).
   b. Wireless on.
   c. Ethernet on.
8. Threat score. Highest level of severity of vulnerabilities found.
9. Last updated. Last time the data was received and refreshed from the unit.
10. IP addresses.
    a. Private.
    b. Public.
11. Unit attacks card.
    a. Arrow opens attacks page.
    b. Total number of attacks.
    c. The amount of time it took to mitigate all the attacks.
    d. The amount of time that took to detect the attacks.
12. Unit threats card. Based on this unit:
    a. Arrow opens threats page.
    b. Local score. The severity level of all local units.
    c. Remote score. The severity vulnerability level of all remote units.
    d. Number of local threats. Total number of threats found by local units.
    e. Number of remote threats. Total number of threats found by remote units.

13. Unit networks card. Based on this specific unit:
    a. Arrow opens networks page.
    b. Local. These shown here are all network devices found by local units.
    c. Remote. These represent the total number of connected devices found by remote units.
    d. Local wireless. These are the wireless networks, and surrounding wireless devices transmitting, found by local units.
    e. Remote wireless. These are the wireless networks, and surrounding wireless devices transmitting, found by remote units.



Name: test

Serial Number: 010522000A3

ID: GDS110000ZA

Privacy Mode: LOCAL

Threat score: 7.8

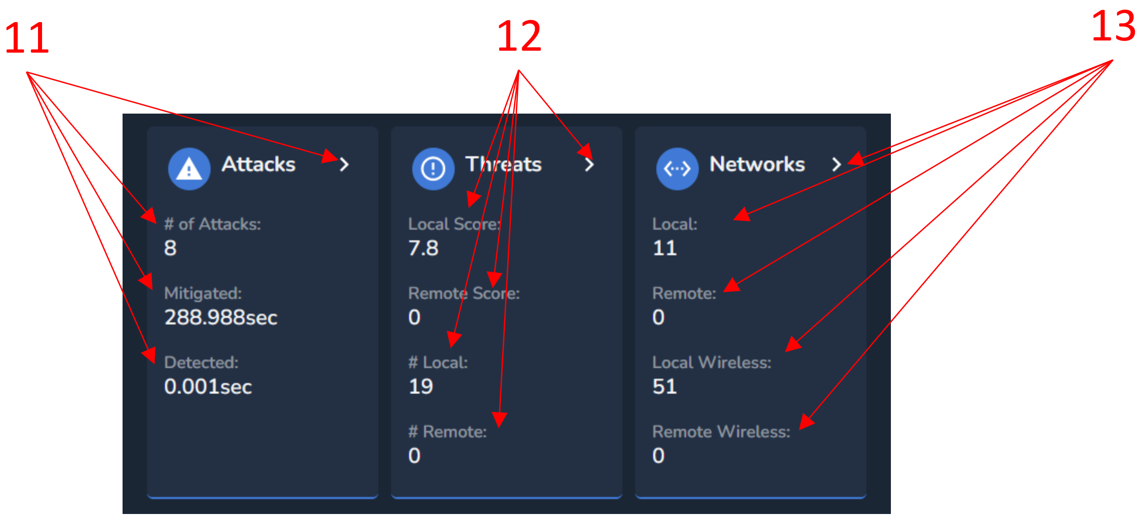
Shared Mode: True

Status: Services Wireless Ethernet

Threat Level: ● Attacks

Latest scan: 10/26/2022

IP`s:
Private: 192.168.1.237
Public: 98.190.148.36



Attacks >

# of Attacks: 8

Mitigated: 288.988sec

Detected: 0.001sec

Threats >

Local Score: 7.8

Remote Score: 0

Local: 19

Remote: 0

Networks >

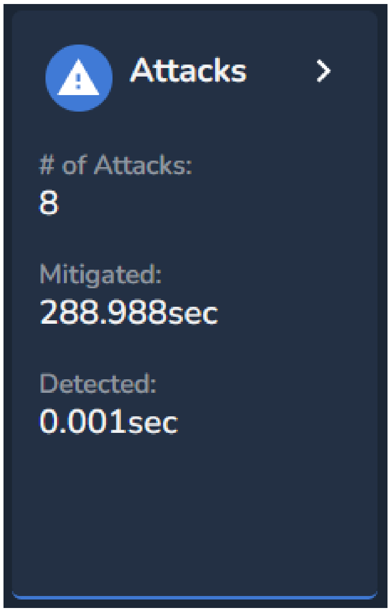
Local: 11

Remote: 0

Local Wireless: 51

Remote Wireless: 0

The unit attacks card. From this card we click the arrow.



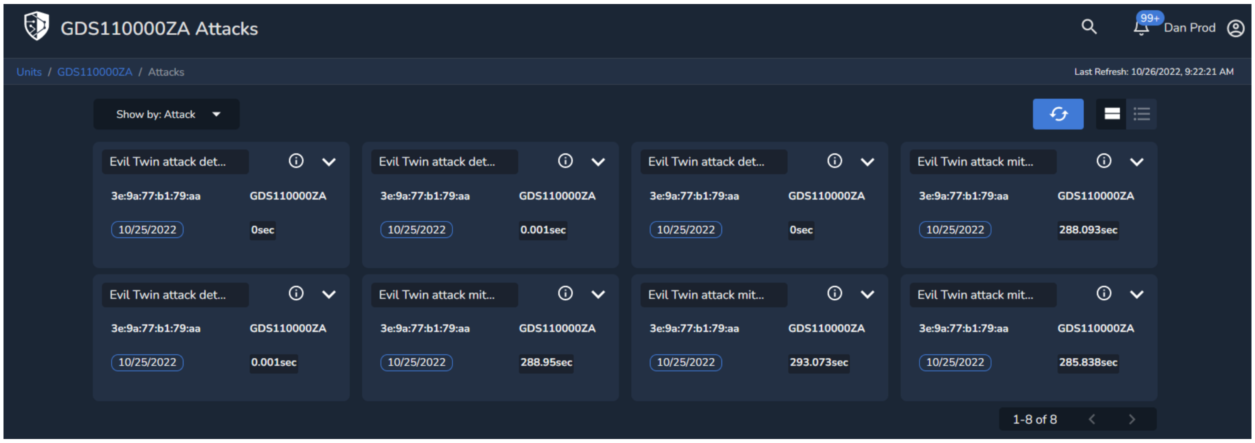
Attacks

# of Attacks:
8

Mitigated:
288.988sec

Detected:
0.001sec

Unit attacks page. And that takes us to this unit attacks page.



GDS110000ZA Attacks

99+ Dan Prod

Units / GDS110000ZA / Attacks

Last Refresh: 10/26/2022, 9:22:21 AM

Show by: Attack

Evil Twin attack det...
3e:9a:77:b1:79:aa GDS110000ZA
10/25/2022 0sec

Evil Twin attack det...
3e:9a:77:b1:79:aa GDS110000ZA
10/25/2022 0.001sec

Evil Twin attack det...
3e:9a:77:b1:79:aa GDS110000ZA
10/25/2022 0sec

Evil Twin attack mit...
3e:9a:77:b1:79:aa GDS110000ZA
10/25/2022 288.093sec

Evil Twin attack det...
3e:9a:77:b1:79:aa GDS110000ZA
10/25/2022 0.001sec

Evil Twin attack mit...
3e:9a:77:b1:79:aa GDS110000ZA
10/25/2022 288.95sec

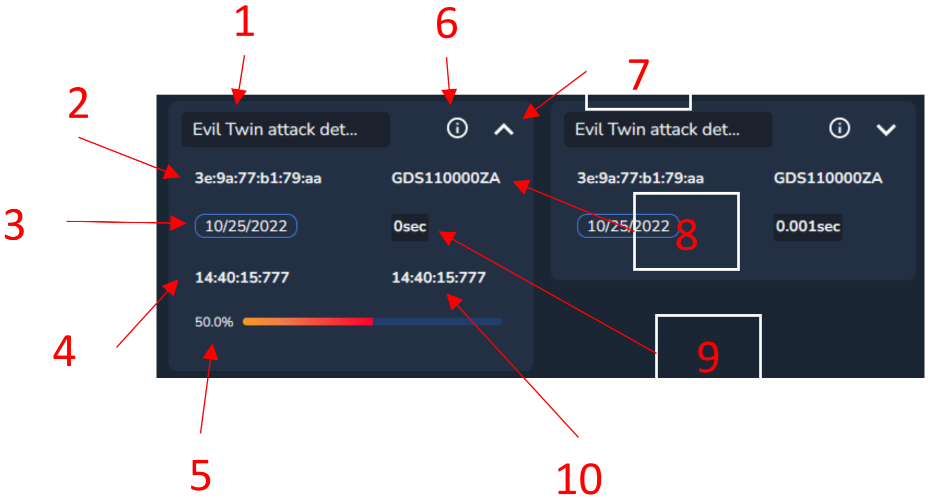
Evil Twin attack mit...
3e:9a:77:b1:79:aa GDS110000ZA
10/25/2022 293.073sec

Evil Twin attack mit...
3e:9a:77:b1:79:aa GDS110000ZA
10/25/2022 285.838sec

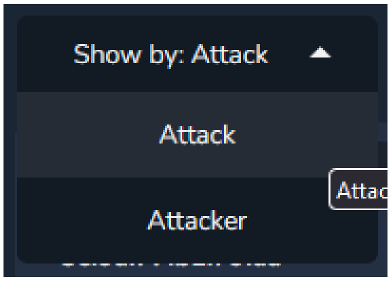
1-8 of 8

Below we show cards expanded and collapsed for an attack. For more information on attack classification please see Terminology. The card has several elements:

1. Name of the attack detected.
2. MAC address of the attacker.
3. Date of the attack.
4. Time the attack started.
5. Percentage of attacks based on overall total.
6. Information/description icon.
7. Arrow to expand/collapse the card.
8. Unit that performed the action.
9. Total time that took for the action to be performed.
10. Time at which the action performed finished.



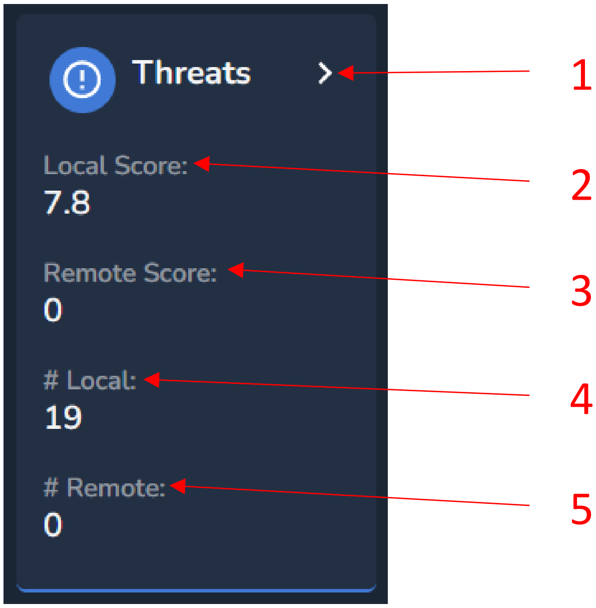
Up top you can select the filter to show attacks by either attack or attacker.



The unit threats card. Going from this card, click on the arrow.

Items shown:

1. Arrow to open the threats page.
2. Local score. The severity level of all local units
3. Remote score. The severity vulnerability level of all remote units.
4. Number of local threats. Total number of threats found by local units.
5. Number of remote threats. Total number of threats found by remote units.



Threats

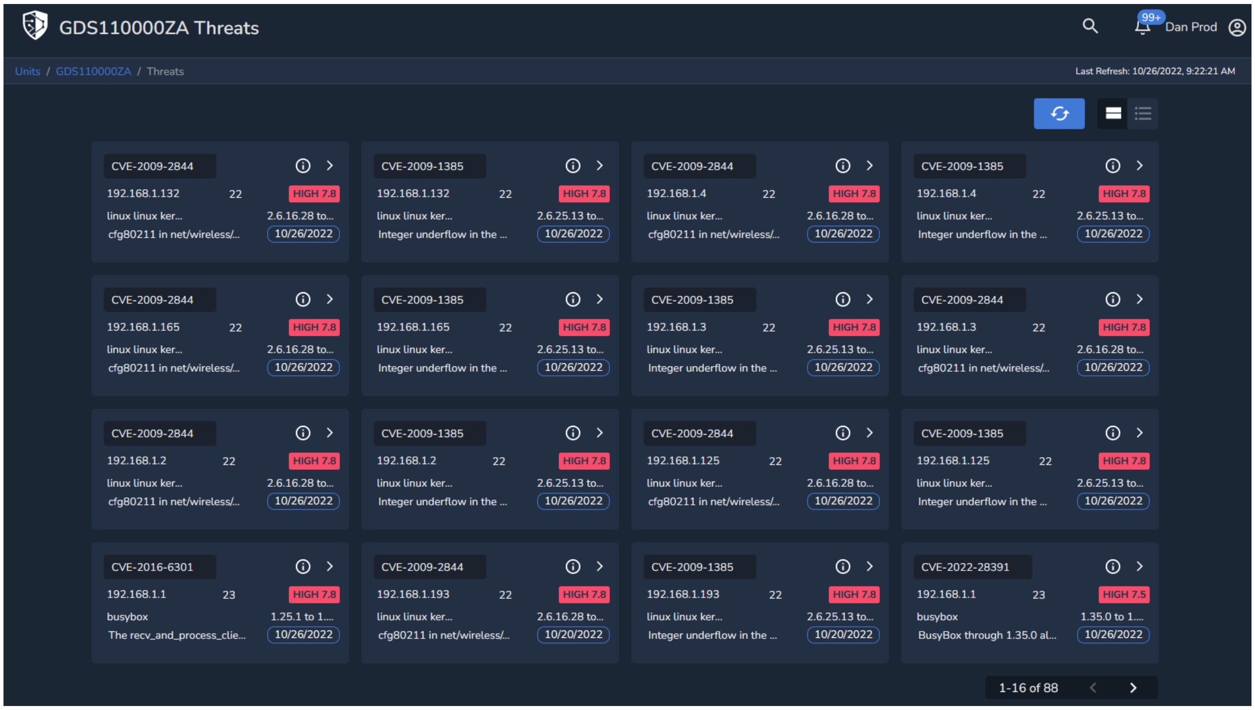
Local Score:
7.8

Remote Score:
0

Local:
19

Remote:
0

The unit threats page. The page below shows all the threats on the networked devices found by the same unit.



GDS110000ZA Threats

Dan Prod

Units / GDS110000ZA / Threats

Last Refresh: 10/26/2022, 9:22:21 AM

CVE-2009-2844
192.168.1.132 22 HIGH 7.8
linux linux ker... 2.6.16.28 to...
cfg80211 in net/wireless/... 10/26/2022

CVE-2009-1385
192.168.1.132 22 HIGH 7.8
linux linux ker... 2.6.25.13 to...
Integer underflow in the ... 10/26/2022

CVE-2009-2844
192.168.1.4 22 HIGH 7.8
linux linux ker... 2.6.16.28 to...
cfg80211 in net/wireless/... 10/26/2022

CVE-2009-1385
192.168.1.4 22 HIGH 7.8
linux linux ker... 2.6.25.13 to...
Integer underflow in the ... 10/26/2022

CVE-2009-2844
192.168.1.165 22 HIGH 7.8
linux linux ker... 2.6.16.28 to...
cfg80211 in net/wireless/... 10/26/2022

CVE-2009-1385
192.168.1.165 22 HIGH 7.8
linux linux ker... 2.6.25.13 to...
Integer underflow in the ... 10/26/2022

CVE-2009-1385
192.168.1.3 22 HIGH 7.8
linux linux ker... 2.6.25.13 to...
Integer underflow in the ... 10/26/2022

CVE-2009-2844
192.168.1.3 22 HIGH 7.8
linux linux ker... 2.6.16.28 to...
cfg80211 in net/wireless/... 10/26/2022

CVE-2009-2844
192.168.1.2 22 HIGH 7.8
linux linux ker... 2.6.16.28 to...
cfg80211 in net/wireless/... 10/26/2022

CVE-2009-1385
192.168.1.2 22 HIGH 7.8
linux linux ker... 2.6.25.13 to...
Integer underflow in the ... 10/26/2022

CVE-2009-2844
192.168.1.125 22 HIGH 7.8
linux linux ker... 2.6.16.28 to...
cfg80211 in net/wireless/... 10/26/2022

CVE-2009-1385
192.168.1.125 22 HIGH 7.8
linux linux ker... 2.6.25.13 to...
Integer underflow in the ... 10/26/2022

CVE-2016-6301
192.168.1.1 23 HIGH 7.8
busybox 1.25.1 to 1....
The recv_and_process_clie... 10/26/2022

CVE-2009-2844
192.168.1.193 22 HIGH 7.8
linux linux ker... 2.6.16.28 to...
cfg80211 in net/wireless/... 10/20/2022

CVE-2009-1385
192.168.1.193 22 HIGH 7.8
linux linux ker... 2.6.25.13 to...
Integer underflow in the ... 10/20/2022

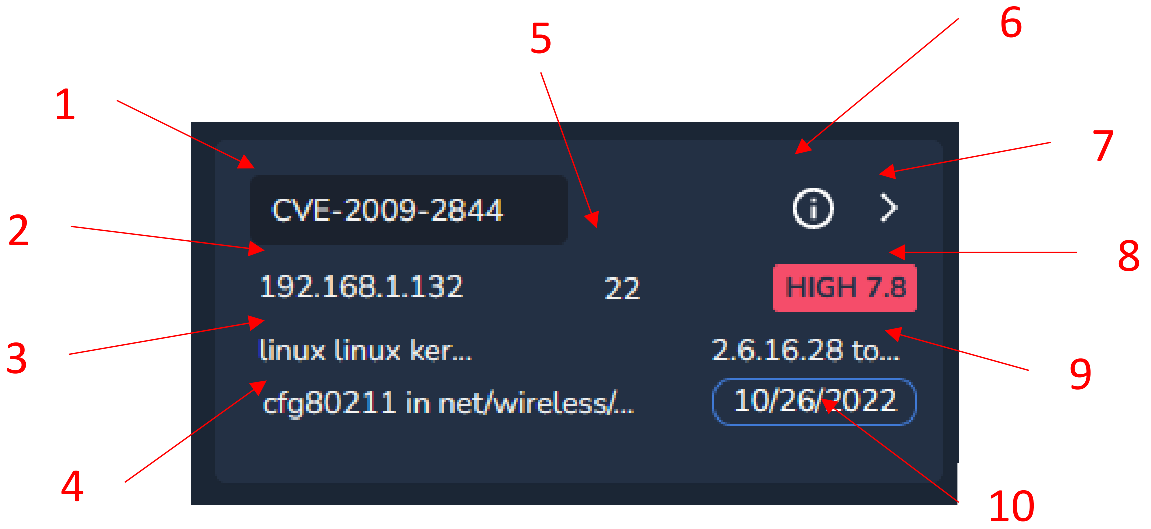
CVE-2022-28391
192.168.1.1 23 HIGH 7.5
busybox 1.35.0 to 1....
BusyBox through 1.35.0 al... 10/26/2022

1-16 of 88

The unit threats card. This card shows the information about a specific threat found on a device connected to the network. The following items are part of the card:

1. CVE of the vulnerability.
2. Device where the vulnerability was found.
3. Software affected.
4. Brief description of the vulnerability.
5. Open port related to it.
6. Information/description icon.

7. Arrow to go to NIST article about the vulnerability.
8. Score of vulnerability.
9. Version impacted.
10. Date discovered.



CVE-2009-2844

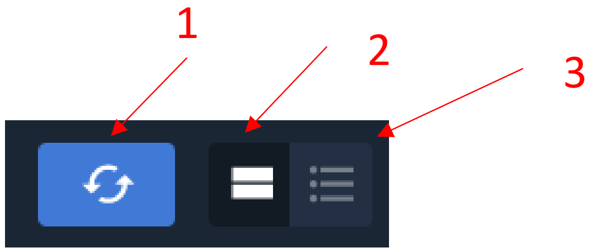
192.168.1.132 22 HIGH 7.8

linux linux ker... 2.6.16.28 to...

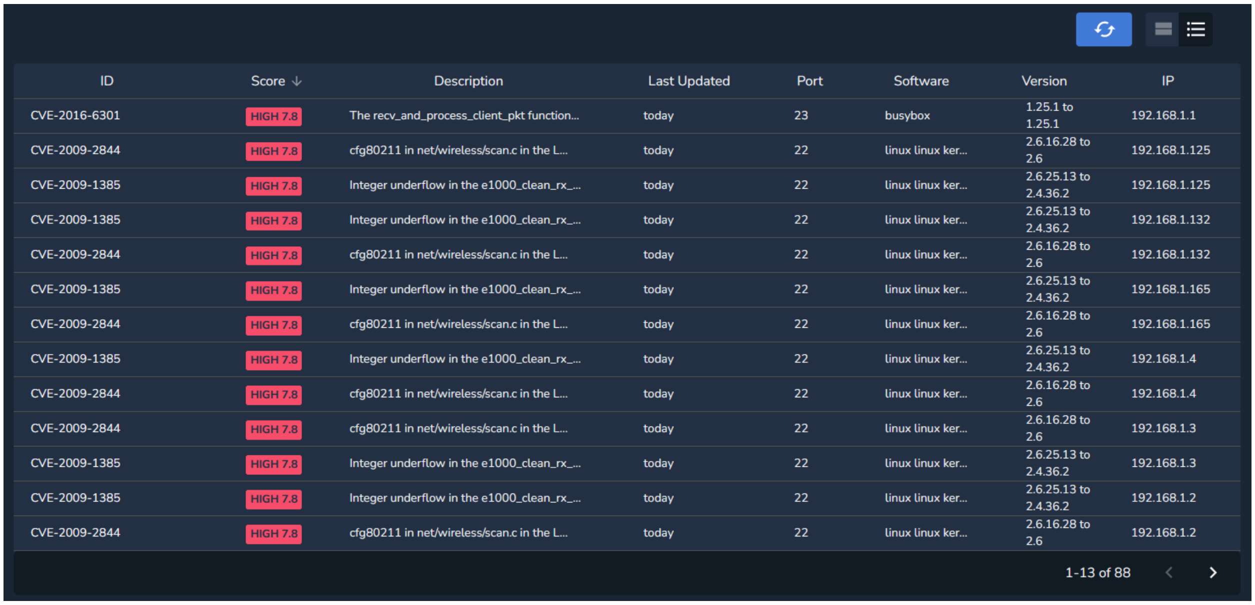
cfg80211 in net/wireless/... 10/26/2022

In most cases when we show cards you can also show the same information in a table view format. Use the icons.

1. Refresh.
2. Card view.
3. Table view.



This is a sample of the unit threats page shown in a table format. As you can see the information is the same as that shown on the threats card.

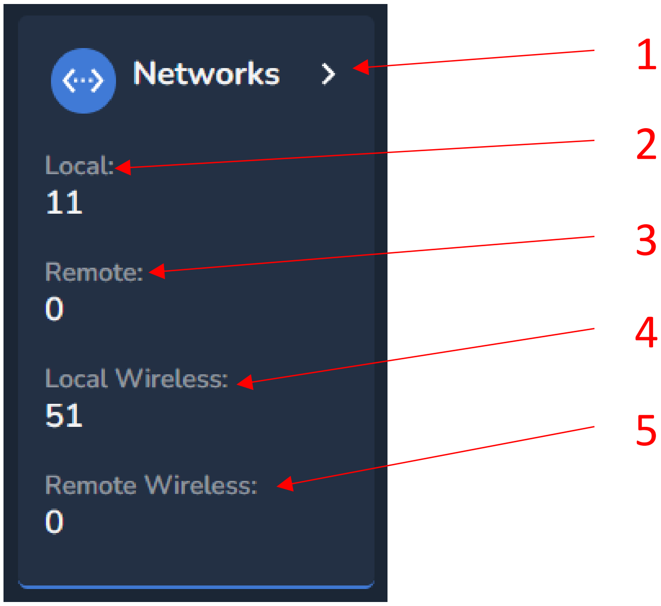


ID	Score ↓	Description	Last Updated	Port	Software	Version	IP
CVE-2016-6301	HIGH 7.8	The recv_and_process_client_pkt function...	today	23	busybox	1.25.1 to 1.25.1	192.168.1.1
CVE-2009-2844	HIGH 7.8	cfg80211 in net/wireless/scan.c in the L...	today	22	linux linux ker...	2.6.16.28 to 2.6	192.168.1.125
CVE-2009-1385	HIGH 7.8	Integer underflow in the e1000_clean_rx_...	today	22	linux linux ker...	2.6.25.13 to 2.4.36.2	192.168.1.125
CVE-2009-1385	HIGH 7.8	Integer underflow in the e1000_clean_rx_...	today	22	linux linux ker...	2.6.25.13 to 2.4.36.2	192.168.1.132
CVE-2009-2844	HIGH 7.8	cfg80211 in net/wireless/scan.c in the L...	today	22	linux linux ker...	2.6.16.28 to 2.6	192.168.1.132
CVE-2009-1385	HIGH 7.8	Integer underflow in the e1000_clean_rx_...	today	22	linux linux ker...	2.6.25.13 to 2.4.36.2	192.168.1.165
CVE-2009-2844	HIGH 7.8	cfg80211 in net/wireless/scan.c in the L...	today	22	linux linux ker...	2.6.16.28 to 2.6	192.168.1.165
CVE-2009-1385	HIGH 7.8	Integer underflow in the e1000_clean_rx_...	today	22	linux linux ker...	2.6.25.13 to 2.4.36.2	192.168.1.4
CVE-2009-2844	HIGH 7.8	cfg80211 in net/wireless/scan.c in the L...	today	22	linux linux ker...	2.6.16.28 to 2.6	192.168.1.4
CVE-2009-2844	HIGH 7.8	cfg80211 in net/wireless/scan.c in the L...	today	22	linux linux ker...	2.6.16.28 to 2.6	192.168.1.3
CVE-2009-1385	HIGH 7.8	Integer underflow in the e1000_clean_rx_...	today	22	linux linux ker...	2.6.25.13 to 2.4.36.2	192.168.1.3
CVE-2009-1385	HIGH 7.8	Integer underflow in the e1000_clean_rx_...	today	22	linux linux ker...	2.6.25.13 to 2.4.36.2	192.168.1.2
CVE-2009-2844	HIGH 7.8	cfg80211 in net/wireless/scan.c in the L...	today	22	linux linux ker...	2.6.16.28 to 2.6	192.168.1.2

The unit networks card. From this card we click on the arrow to show the networks page of the unit.

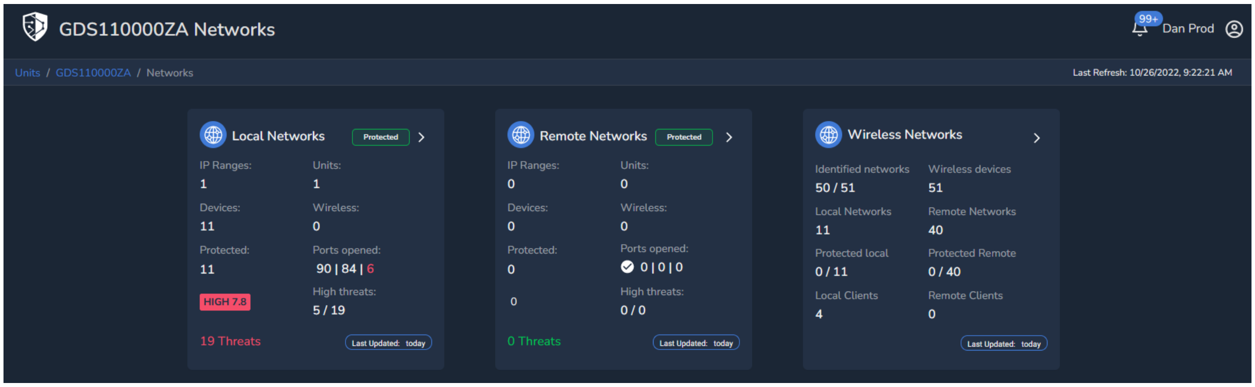
The data we find on this card is as follows:

1. Arrow to open the networks page.
2. Local. These shown here are all network devices found by local units.
3. Remote. These represent the total number of connected devices found by remote units.
4. Local wireless. These are the wireless networks, and surrounding wireless devices transmitting, found by local units.
5. Remote wireless. These are the wireless networks, and surrounding wireless devices transmitting, found by remote units.



The unit networks page. Very much like the global networks page, this shows all information related to the networks found by unit you clicked on. Here we show 3 consolidated cards. For a definition of these please see Terminology.

1. Local Networks.
2. Remote Networks.
3. Wireless Networks.



GDS110000ZA Networks

99+ Dan Prod

Units / GDS110000ZA / Networks

Last Refresh: 10/26/2022, 9:22:21 AM

Local Networks Protected >

IP Ranges: 1
Units: 1
Devices: 11
Wireless: 0
Protected: 11
Ports opened: 90 | 84 | 6
HIGH 7.8
High threats: 5 / 19
19 Threats
Last Updated: today

Remote Networks Protected >

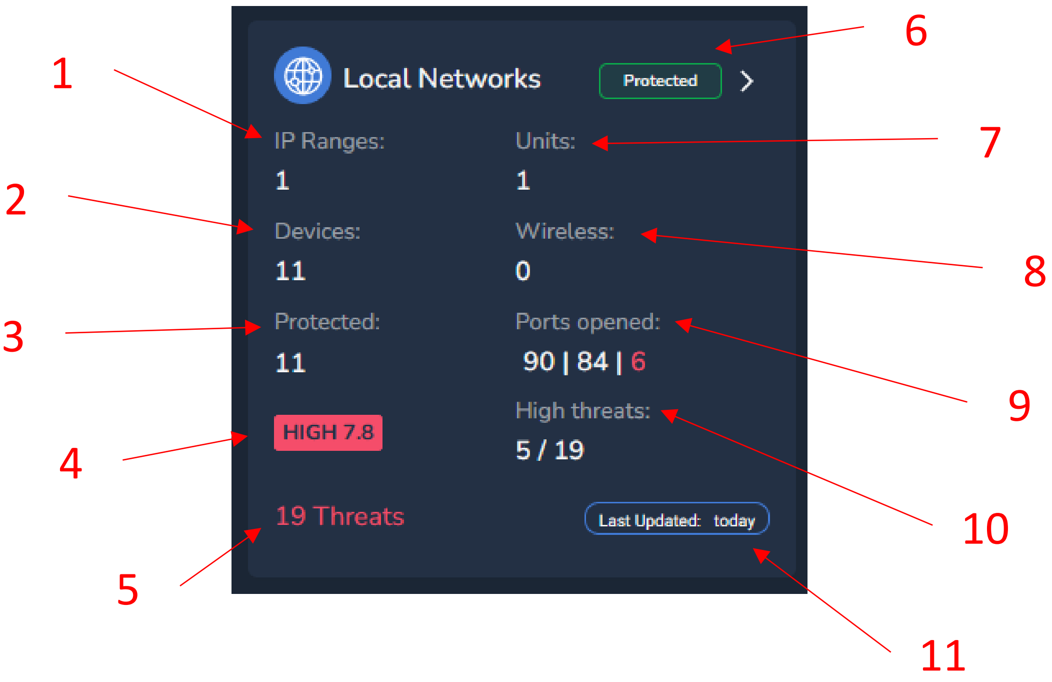
IP Ranges: 0
Units: 0
Devices: 0
Wireless: 0
Protected: 0
Ports opened: ✓ 0 | 0 | 0
0
High threats: 0 / 0
0 Threats
Last Updated: today

Wireless Networks >

Identified networks 50 / 51
Wireless devices 51
Local Networks 11
Remote Networks 40
Protected local 0 / 11
Protected Remote 0 / 40
Local Clients 4
Remote Clients 0
Last Updated: today

The local networks card. Here we have the following items:

1. IP ranges. These are the IP ranges found on the network.
2. Devices. These are the connected devices, both wired and wireless, discovered on the network.
3. Protected devices. These are the total number of protected devices.
4. Severity level. The highest vulnerability severity level found.
5. Threats count. Total number of vulnerabilities found.
6. Protected status. Whether the entire network with all of its devices are protected or not.
7. Units. Fido units found on the network.
8. Wireless. These are the wireless networks (access points or transmitting devices) found around the unit.
9. Ports opened. These show the total number of ports found that are open and those with vulnerabilities related to them. You would read these as 90 total ports open, 84 without vulnerabilities, 6 with vulnerabilities. The last count should show the color of the highest threat found.
10. High threats count. Out of all vulnerabilities found (19), 5 are high.
11. Last updated. Last time we updated this card with the data from the unit.



Local Networks

Protected

IP Ranges: 1

Units: 1

Devices: 11

Wireless: 0

Protected: 11

Ports opened: 90 | 84 | 6

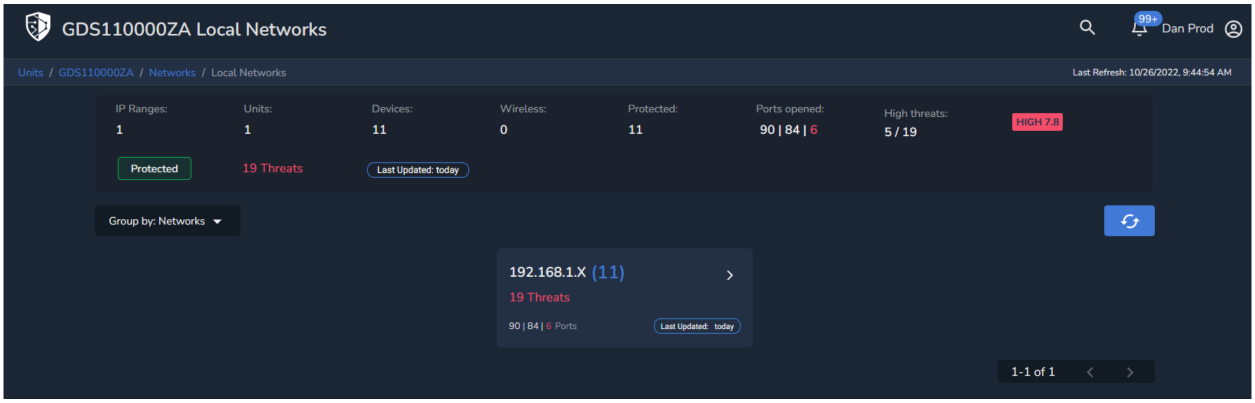
HIGH 7.8

High threats: 5 / 19

19 Threats

Last Updated: today

The unit local networks details page. The information shown across the top of the screen is the same as the one shown on the card we previously went over. Beneath that details section you will see the IP ranges found on the network.



GDS110000ZA Local Networks

Units / GDS110000ZA / Networks / Local Networks

Last Refresh: 10/26/2022, 9:44:54 AM

IP Ranges: 1

Units: 1

Devices: 11

Wireless: 0

Protected: 11

Ports opened: 90 | 84 | 6

High threats: 5 / 19

HIGH 7.8

Protected

19 Threats

Last Updated: today

Group by: Networks

192.168.1.X (11)

19 Threats

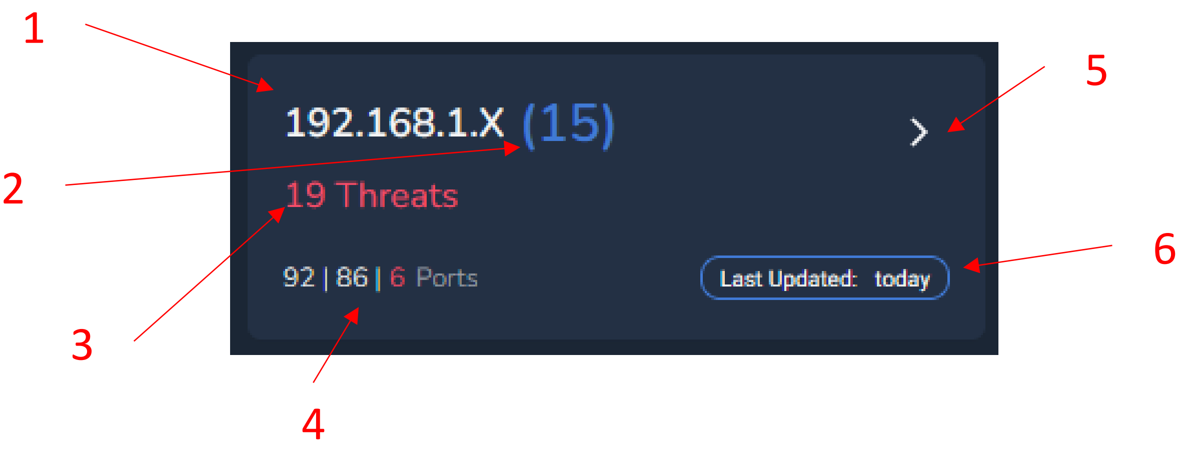
90 | 84 | 6 Ports

Last Updated: today

1-1 of 1

The local networks IP range card. The card shows information we are already familiar with, such as

1. IP range
2. Number of devices
3. Number of threats
4. Ports open and with vulnerabilities
5. Arrow to open the IP range
6. Last updated.



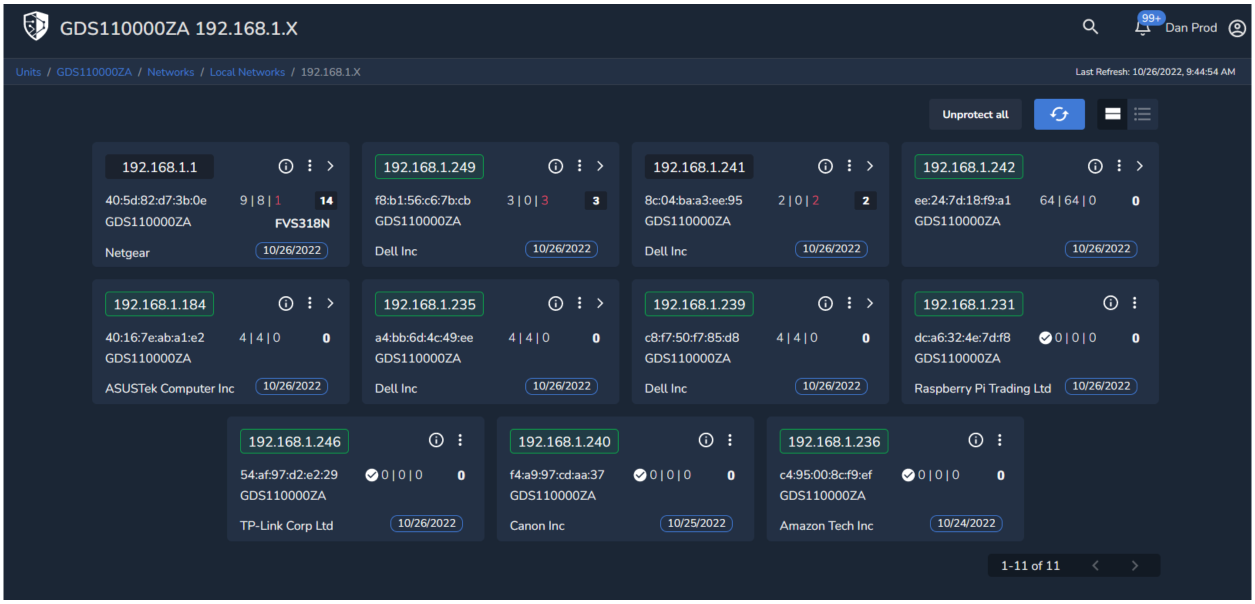
192.168.1.X (15)

19 Threats

92 | 86 | 6 Ports

Last Updated: today

The unit local networks devices page from the selected IP range. By clicking on the arrow on the IP range card we get to this page.


GDS110000ZA 192.168.1.X

Units / GDS110000ZA / Networks / Local Networks / 192.168.1.X

Last Refresh: 10/26/2022, 9:44:54 AM

192.168.1.1
40:5d:82:d7:3b:0e 9 | 8 | 1 14
GDS110000ZA FVS318N
Netgear 10/26/2022

192.168.1.249
f8:b1:56:c6:7b:cb 3 | 0 | 3 3
GDS110000ZA
Dell Inc 10/26/2022

192.168.1.241
8c:04:ba:a3:ee:95 2 | 0 | 2 2
GDS110000ZA
Dell Inc 10/26/2022

192.168.1.242
ee:24:7d:18:f9:a1 64 | 64 | 0 0
GDS110000ZA
10/26/2022

192.168.1.184
40:16:7e:ab:a1:e2 4 | 4 | 0 0
GDS110000ZA
ASUSTek Computer Inc 10/26/2022

192.168.1.235
a4:bb:6d:4c:49:ee 4 | 4 | 0 0
GDS110000ZA
Dell Inc 10/26/2022

192.168.1.239
c8:f7:50:f7:85:d8 4 | 4 | 0 0
GDS110000ZA
Dell Inc 10/26/2022

192.168.1.231
dc:a6:32:4e:7d:f8 ✓ 0 | 0 | 0 0
GDS110000ZA
Raspberry Pi Trading Ltd 10/26/2022

192.168.1.246
54:af:97:d2:e2:29 ✓ 0 | 0 | 0 0
GDS110000ZA
TP-Link Corp Ltd 10/26/2022

192.168.1.240
f4:a9:97:cd:aa:37 ✓ 0 | 0 | 0 0
GDS110000ZA
Canon Inc 10/25/2022

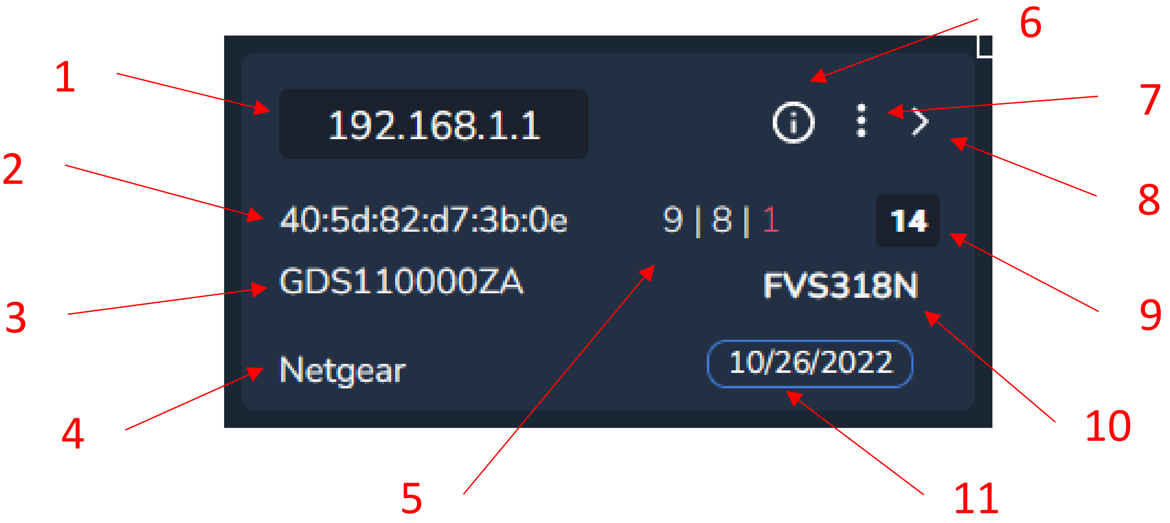
192.168.1.236
c4:95:00:8c:f9:ef ✓ 0 | 0 | 0 0
GDS110000ZA
Amazon Tech Inc 10/24/2022

1-11 of 11

The connected device card. Items for this card:

1. IP of the connected device. To protect this device, click on it. Green means protected.
2. MAC address of the device.
3. Unit that discovered the device.
4. Manufacturer of the device discovered.
5. Port information.
6. Information/description of the card.
7. Actions menu to display options.
8. Arrow to open the device details page.
9. Number of threats.
10. Hostname of the device.

11. Last updated



192.168.1.1

40:5d:82:d7:3b:0e

9 | 8 | 1

14

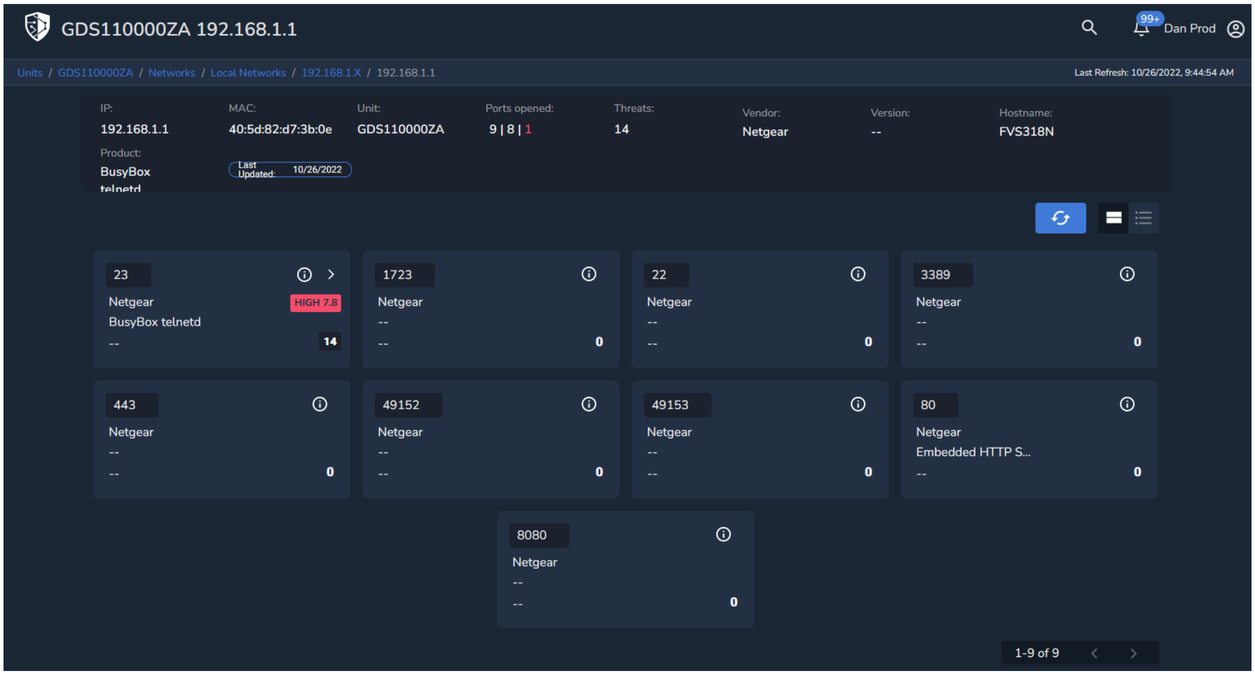
GDS110000ZA

FVS318N

Netgear

10/26/2022

The connected device details page. This next page shows information up at the top that we are already familiar with and then below it, it shows information on the ports identified as opened.



GDS110000ZA 192.168.1.1

Dan Prod

Units / GDS110000ZA / Networks / Local Networks / 192.168.1.X / 192.168.1.1

Last Refresh: 10/26/2022, 9:44:54 AM

IP: 192.168.1.1

MAC: 40:5d:82:d7:3b:0e

Unit: GDS110000ZA

Ports opened: 9 | 8 | 1

Threats: 14

Vendor: Netgear

Version: --

Hostname: FVS318N

Product: BusyBox telnetd

Last Updated: 10/26/2022

23
Netgear
HIGH 7.8
BusyBox telnetd
14
--

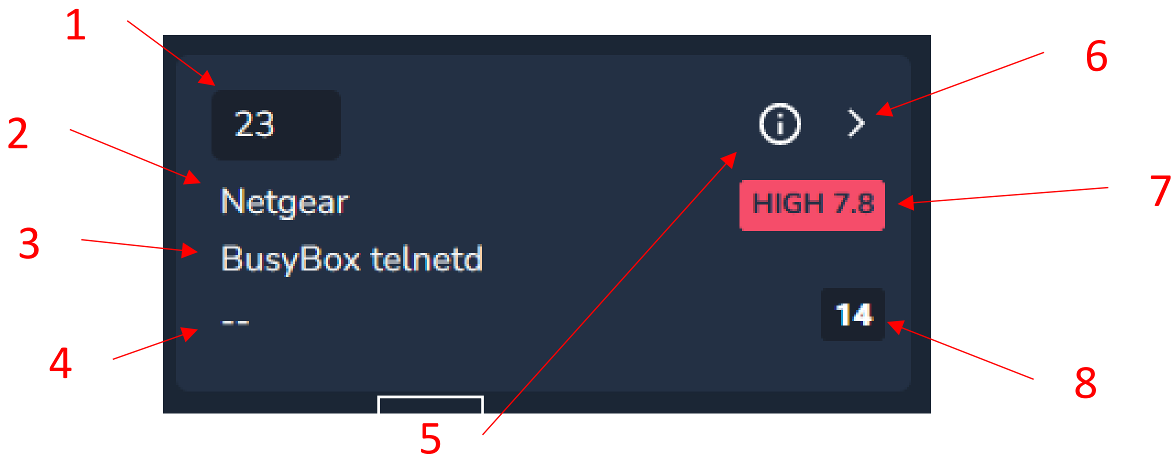
23 Netgear HIGH 7.8 BusyBox telnetd -- 14	1723 Netgear -- -- 0	22 Netgear -- -- 0	3389 Netgear -- -- 0
443 Netgear -- -- 0	49152 Netgear -- -- 0	49153 Netgear -- -- 0	80 Netgear Embedded HTTP S... -- 0
	8080 Netgear -- -- 0		

1-9 of 9

The port card. The following items are part of this card:

1. Port.
2. Manufacturer.
3. Software identified.
4. Version of the software.
5. Information/description of the card.

6. Arrow to open the port card.
7. Vulnerability severity level.
8. Number of threats found.



23

Netgear

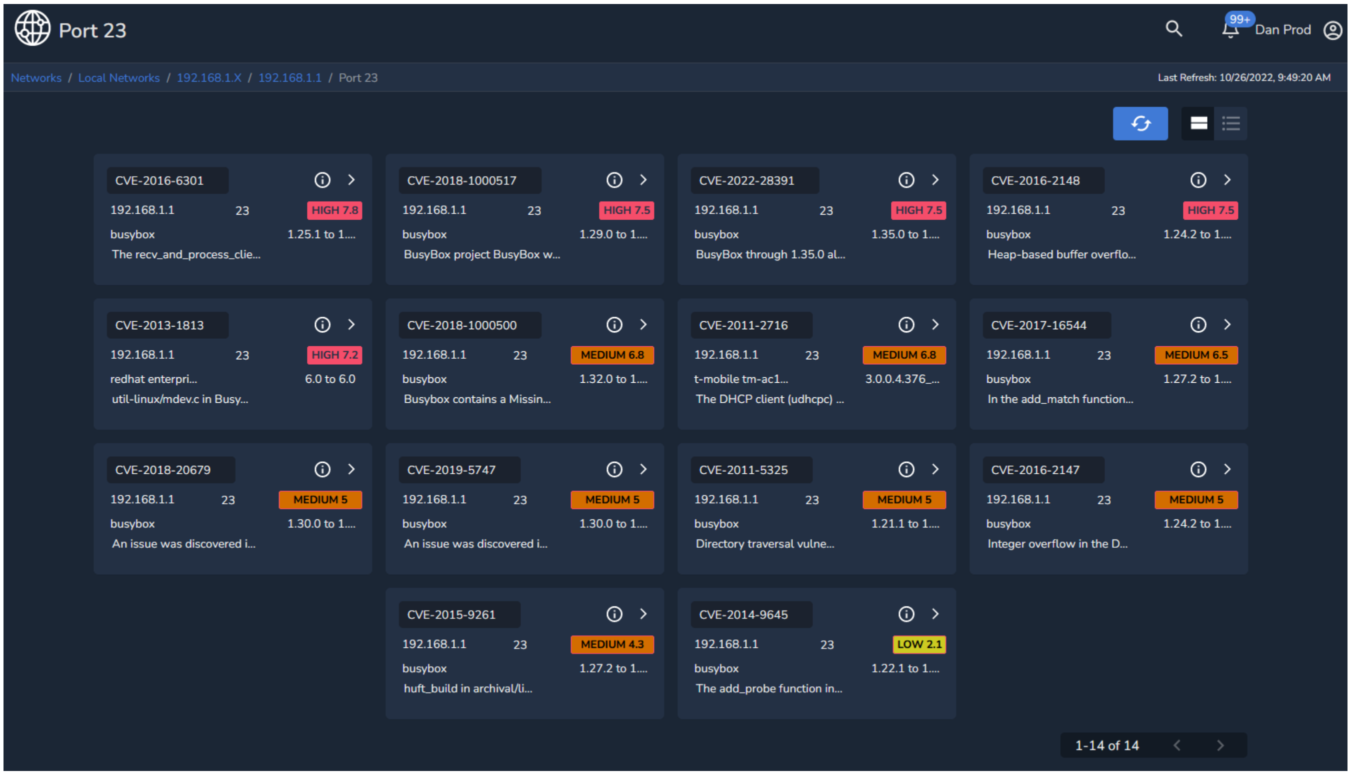
BusyBox telnetd

--

HIGH 7.8

14

The port vulnerabilities page. This page shows all the vulnerabilities found that are related to the open port.



Port 23

Dan Prod

Networks / Local Networks / 192.168.1.X / 192.168.1.1 / Port 23

Last Refresh: 10/26/2022, 9:49:20 AM

CVE-2016-6301
192.168.1.1 23 HIGH 7.8
busybox 1.25.1 to 1....
The recv_and_process_clie...

CVE-2018-1000517
192.168.1.1 23 HIGH 7.5
busybox 1.29.0 to 1....
BusyBox project BusyBox w...

CVE-2022-28391
192.168.1.1 23 HIGH 7.5
busybox 1.35.0 to 1....
BusyBox through 1.35.0 al...

CVE-2016-2148
192.168.1.1 23 HIGH 7.5
busybox 1.24.2 to 1....
Heap-based buffer overflo...

CVE-2013-1813
192.168.1.1 23 HIGH 7.2
redhat enterpri... 6.0 to 6.0
util-linux/mdev.c in Busy...

CVE-2018-1000500
192.168.1.1 23 MEDIUM 6.8
busybox 1.32.0 to 1....
Busybox contains a Missin...

CVE-2011-2716
192.168.1.1 23 MEDIUM 6.8
t-mobile tm-ac1... 3.0.0.4.376_...
The DHCP client (udhcpc) ...

CVE-2017-16544
192.168.1.1 23 MEDIUM 6.5
busybox 1.27.2 to 1....
In the add_match function...

CVE-2018-20679
192.168.1.1 23 MEDIUM 5
busybox 1.30.0 to 1....
An issue was discovered i...

CVE-2019-5747
192.168.1.1 23 MEDIUM 5
busybox 1.30.0 to 1....
An issue was discovered i...

CVE-2011-5325
192.168.1.1 23 MEDIUM 5
busybox 1.21.1 to 1....
Directory traversal vulne...

CVE-2016-2147
192.168.1.1 23 MEDIUM 5
busybox 1.24.2 to 1....
Integer overflow in the D...

CVE-2015-9261
192.168.1.1 23 MEDIUM 4.3
busybox 1.27.2 to 1....
huft_build in archival/li...

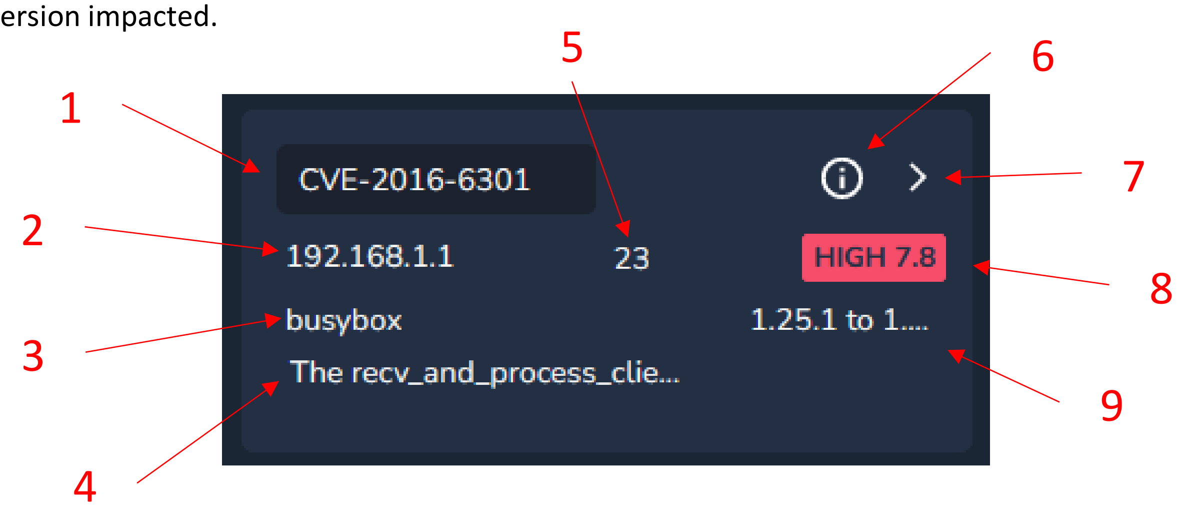
CVE-2014-9645
192.168.1.1 23 LOW 2.1
busybox 1.22.1 to 1....
The add_probe function in...

1-14 of 14

The vulnerability card. This is similar as other vulnerabilities cards we have seen before on this manual. Items are:

1. CVE of the vulnerability.
2. Device where the vulnerability was found.
3. Software affected.

4. Brief description of the vulnerability.
5. Open port related to it.
6. Information/description icon.
7. Arrow to go to NIST article about the vulnerability.
8. Score of vulnerability.
9. Version impacted.



CVE-2016-6301

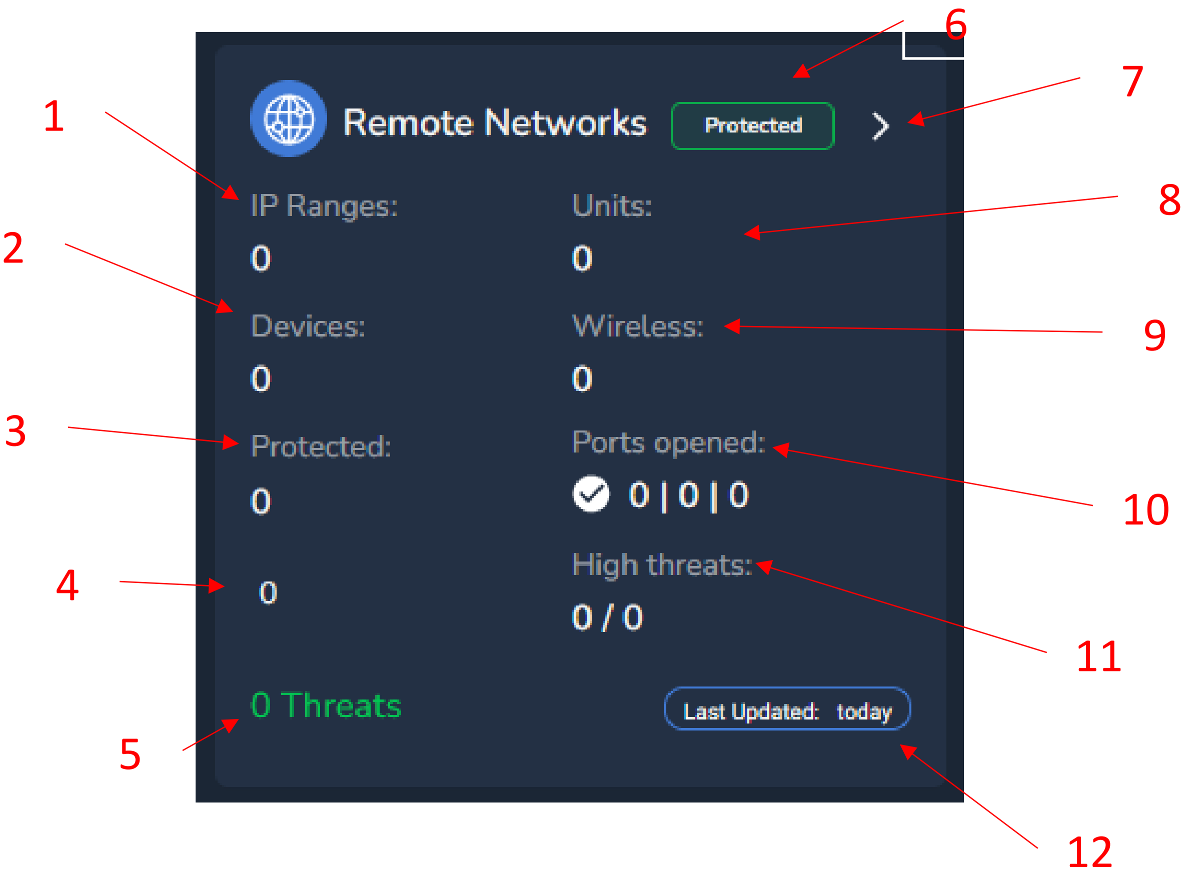
192.168.1.1 23 HIGH 7.8

busybox 1.25.1 to 1....

The recv_and_process_clie...

The unit remote networks card.

1. IP ranges. These are the IP ranges found on the network.
2. Devices. These are the connected devices, both wired and wireless, discovered on the network.
3. Protected devices. These are the total number of protected devices.
4. Severity level. The highest vulnerability severity level found, if any.
5. Threats count. Total number of vulnerabilities found.
6. Protected status. Whether the entire network with all of its devices are protected or not.
7. Arrow to open the remote networks page.
8. Units. Fido units found on the network.
9. Wireless. These are the wireless networks (access points or transmitting devices) found around the unit.
10. Ports opened. These show the total number of ports found that are open and those with vulnerabilities related to them. You would read these as ports open | ports without vulnerabilities | ports with vulnerabilities. The last count should show the color of the highest threat found.
11. High threats count. Out of all vulnerabilities found (19), 5 are high.
12. Last updated. Last time we updated this card with the data from the unit.



Remote Networks
Protected

IP Ranges:
0

Units:
0

Devices:
0

Wireless:
0

Protected:
0

Ports opened:
✓ 0 | 0 | 0

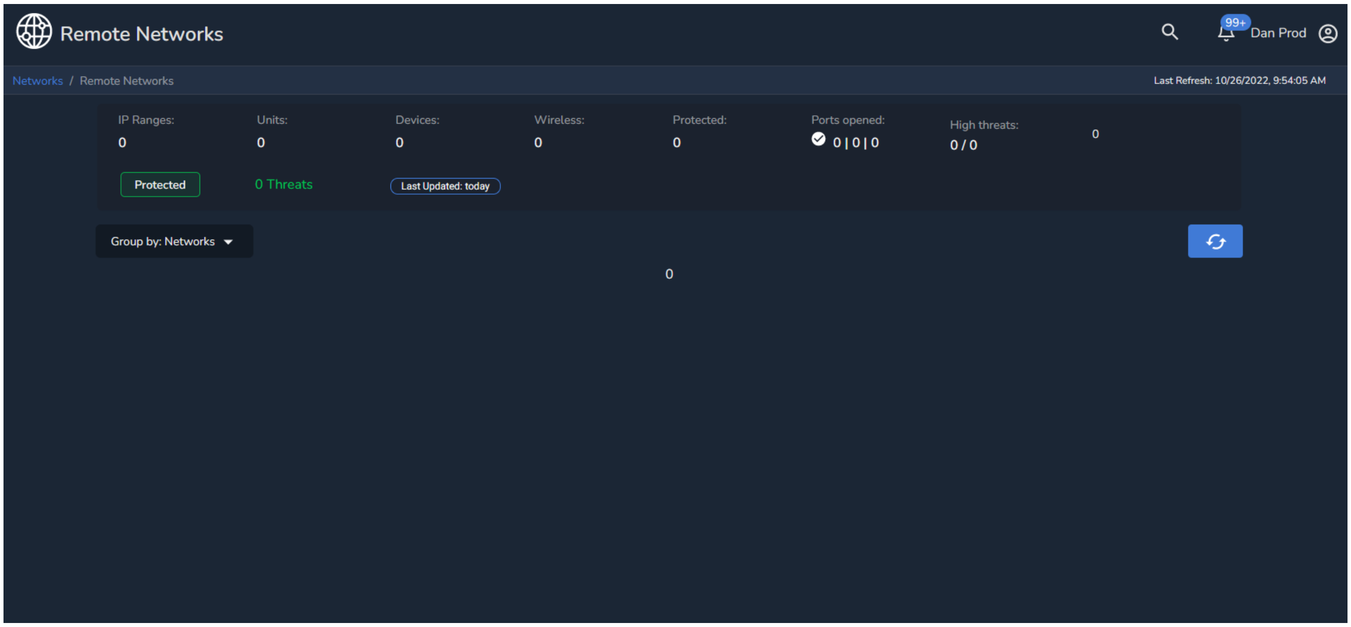
0

High threats:
0 / 0

0 Threats

Last Updated: today

The unit remote networks details page. The top part of the screen shows information from the card we are coming from. The bottom part would show information, just like the local network page, with the IP ranges found on the network where the remote unit is plugged into.



Remote Networks

99+ Dan Prod

Networks / Remote Networks

Last Refresh: 10/26/2022, 9:54:05 AM

IP Ranges:	Units:	Devices:	Wireless:	Protected:	Ports opened:	High threats:	
0	0	0	0	0	✓ 0 | 0 | 0	0 / 0	0

Protected
0 Threats
Last Updated: today

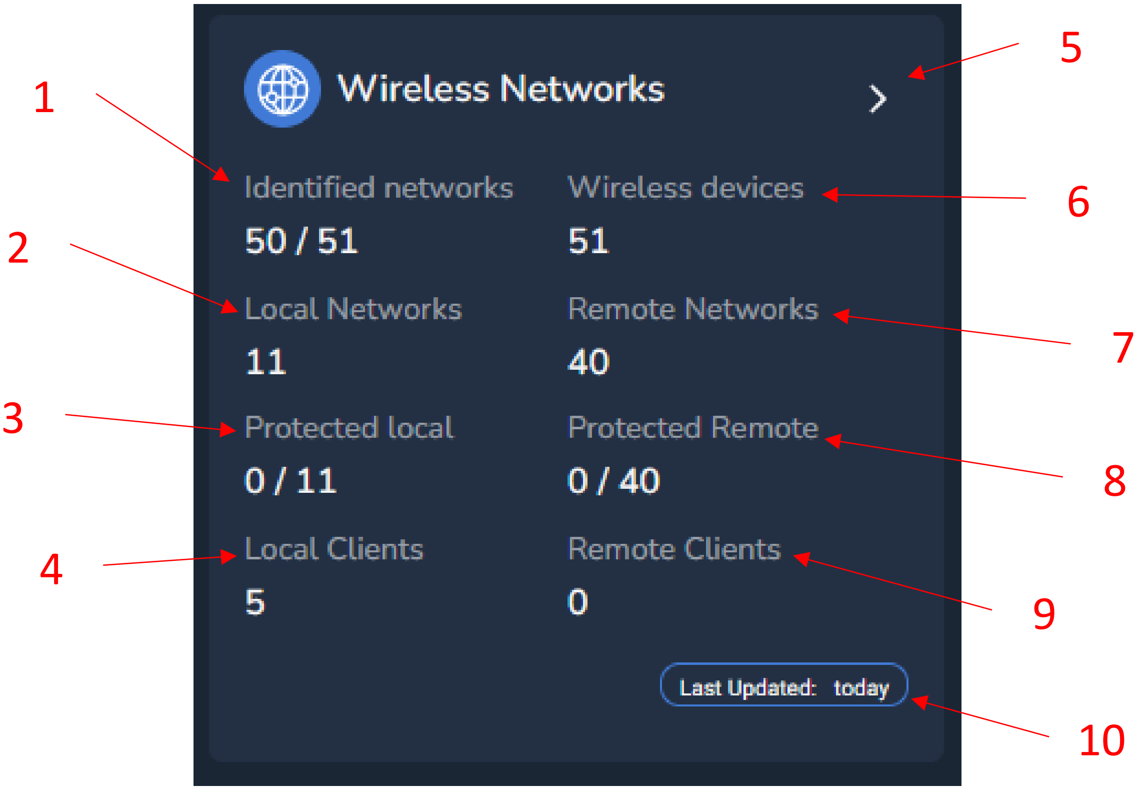
Group by: Networks

0

The unit wireless networks card.

Items on this card:

1. Identified networks. Number of identified networks over total found.
2. Local networks. If the unit is local then it would show wireless networks.
3. Protected local. How many of those wireless are protected.
4. Local clients. How many clients in total are seen in the wireless networks.
5. Arrow to open wireless networks page.
6. Wireless devices. Total number of wireless devices found (access points or transmitting)
7. Remote networks. If the unit is remote then it would show the count here.
8. Protected remote. Protected wireless that are remote.
9. Remote clients . Clients connected to wireless remote.
10. Last updated. Last time data was refreshed.



Wireless Networks

Identified networks
50 / 51

Wireless devices
51

Local Networks
11

Remote Networks
40

Protected local
0 / 11

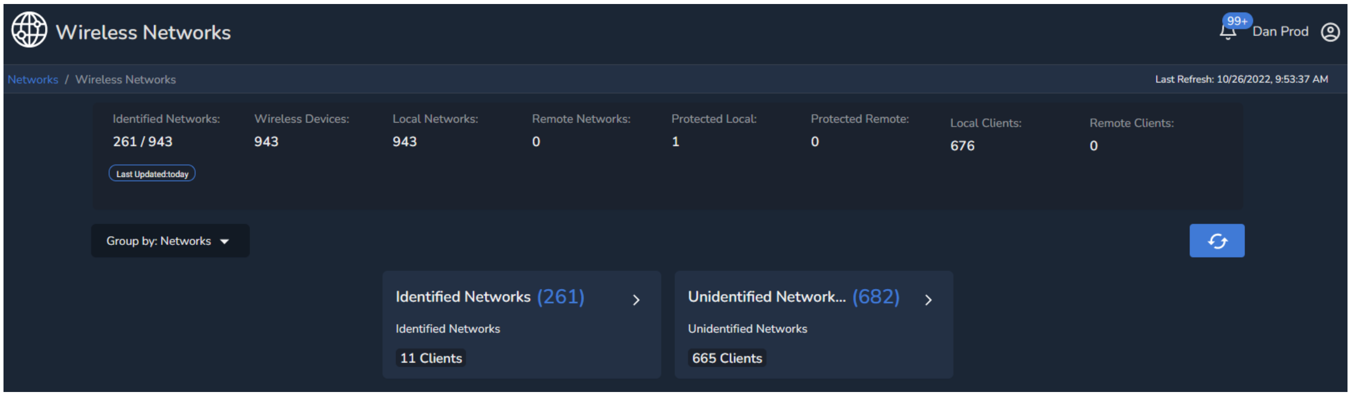
Protected Remote
0 / 40

Local Clients
5

Remote Clients
0

Last Updated: today

The unit wireless networks details page. At the top of the page we show the details on wireless networks as we did on the card you clicked on to get here. Below that section of the page you have wireless we have found that are both identified and unidentified.



Wireless Networks

99+ Dan Prod

Networks / Wireless Networks

Last Refresh: 10/26/2022, 9:53:37 AM

Identified Networks: 261 / 943

Last Updated:today

Wireless Devices: 943

Local Networks: 943

Remote Networks: 0

Protected Local: 1

Protected Remote: 0

Local Clients: 676

Remote Clients: 0

Group by: Networks

Identified Networks (261)

Identified Networks

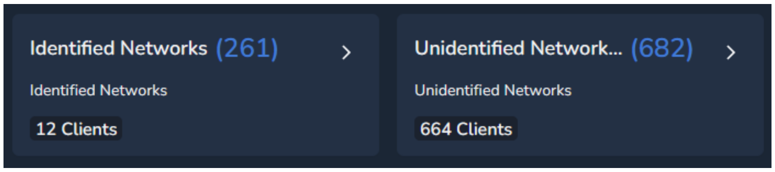
11 Clients

Unidentified Network... (682)

Unidentified Networks

665 Clients

Identified and unidentified wireless networks. In some cases given the nature of wireless networks and the configuration of said networks we may pick up the names, SSID, and some other times those would be hidden and therefore unidentified.



Identified Networks (261)

Identified Networks

12 Clients

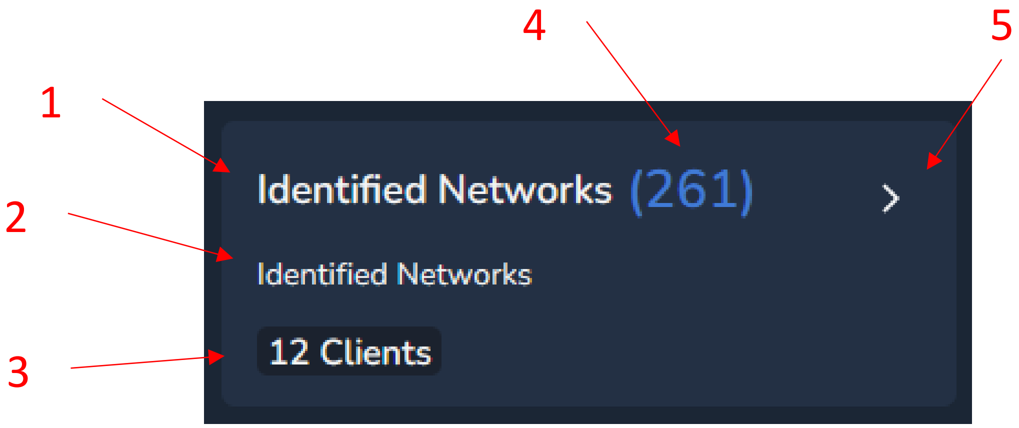
Unidentified Network... (682)

Unidentified Networks

664 Clients

The identified networks card. Items on this card:

1. Identified networks.
2. Subtype, in this case also identified networks.
3. Total number of clients connected to these networks.
4. Total number of those identified networks.
5. Arrow to open the card to see the networks found.

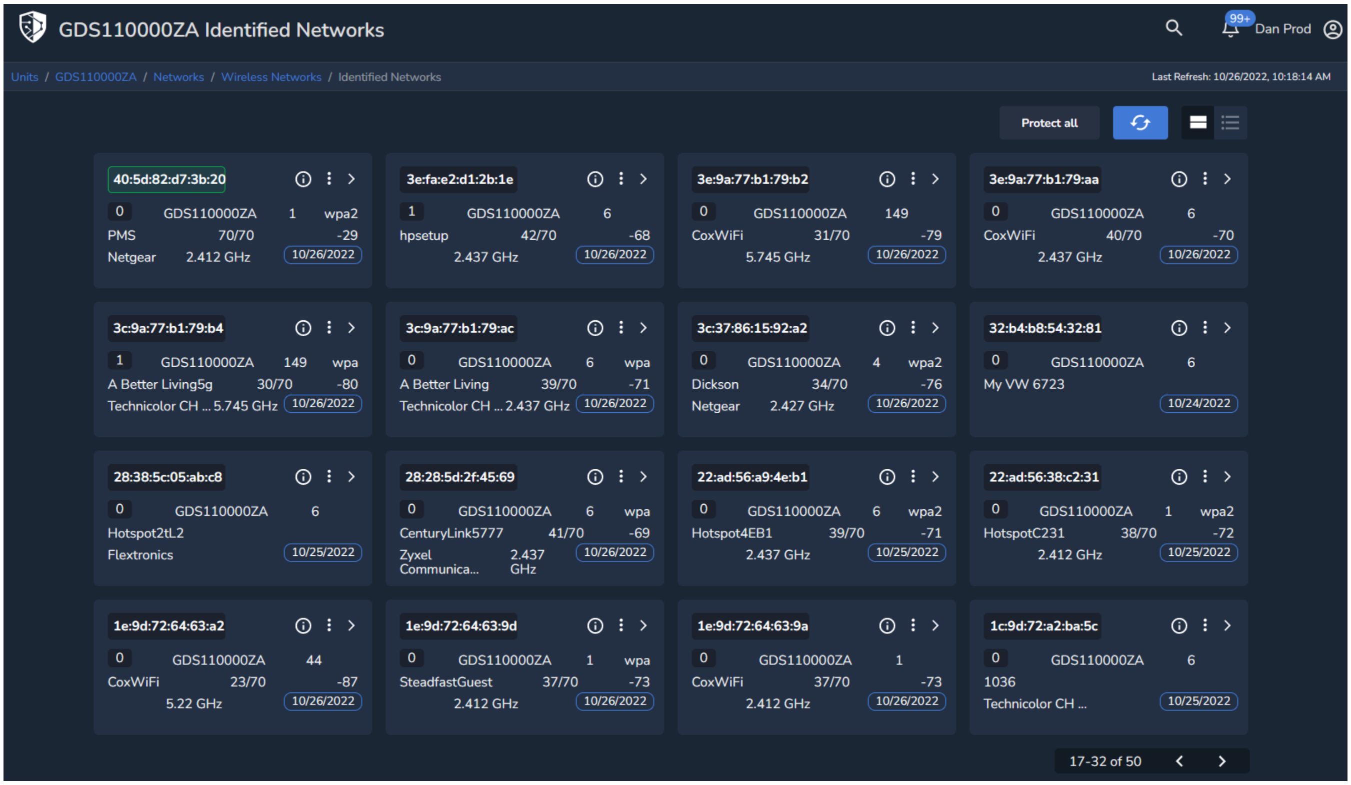


Identified Networks (261)

Identified Networks

12 Clients

The identified networks page. When you click on the arrow it opens this new page with all the networks found.



GDS110000ZA Identified Networks

Units / GDS110000ZA / Networks / Wireless Networks / Identified Networks

Last Refresh: 10/26/2022, 10:18:14 AM

40:5d:82:d7:3b:20
0 GDS110000ZA 1 wpa2
PMS 70/70 -29
Netgear 2.412 GHz 10/26/2022

3e:fa:e2:d1:2b:1e
1 GDS110000ZA 6
hpsetup 42/70 -68
2.437 GHz 10/26/2022

3e:9a:77:b1:79:b2
0 GDS110000ZA 149
CoxWiFi 31/70 -79
5.745 GHz 10/26/2022

3e:9a:77:b1:79:aa
0 GDS110000ZA 6
CoxWiFi 40/70 -70
2.437 GHz 10/26/2022

3c:9a:77:b1:79:b4
1 GDS110000ZA 149 wpa
A Better Living5g 30/70 -80
Technicolor CH ... 5.745 GHz 10/26/2022

3c:9a:77:b1:79:ac
0 GDS110000ZA 6 wpa
A Better Living 39/70 -71
Technicolor CH ... 2.437 GHz 10/26/2022

3c:37:86:15:92:a2
0 GDS110000ZA 4 wpa2
Dickson 34/70 -76
Netgear 2.427 GHz 10/26/2022

32:b4:b8:54:32:81
0 GDS110000ZA 6
My VW 6723
10/24/2022

28:38:5c:05:ab:c8
0 GDS110000ZA 6
Hotspot2tL2
Flextronics 10/25/2022

28:28:5d:2f:45:69
0 GDS110000ZA 6 wpa
CenturyLink5777 41/70 -69
Zyxel Communica... 2.437 GHz 10/26/2022

22:ad:56:a9:4e:b1
0 GDS110000ZA 6 wpa2
Hotspot4EB1 39/70 -71
2.437 GHz 10/25/2022

22:ad:56:38:c2:31
0 GDS110000ZA 1 wpa2
HotspotC231 38/70 -72
2.412 GHz 10/25/2022

1e:9d:72:64:63:a2
0 GDS110000ZA 44
CoxWiFi 23/70 -87
5.22 GHz 10/26/2022

1e:9d:72:64:63:9d
0 GDS110000ZA 1 wpa
SteadfastGuest 37/70 -73
2.412 GHz 10/26/2022

1e:9d:72:64:63:9a
0 GDS110000ZA 1
CoxWiFi 37/70 -73
2.412 GHz 10/26/2022

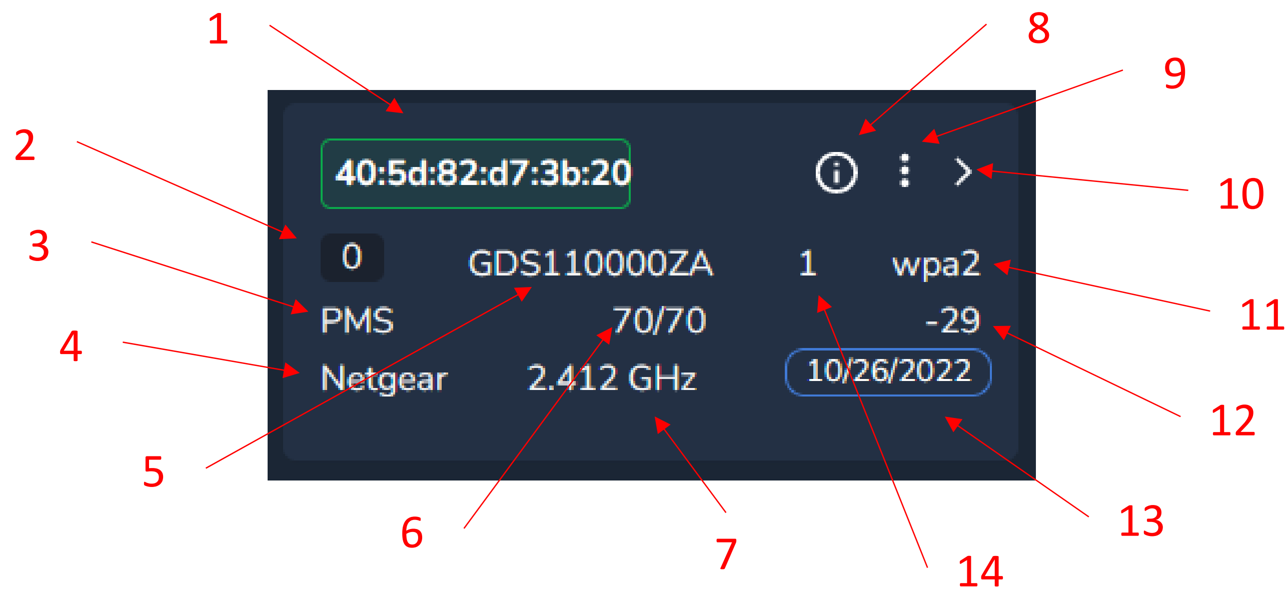
1c:9d:72:a2:ba:5c
0 GDS110000ZA 6
1036
Technicolor CH ... 10/25/2022

17-32 of 50

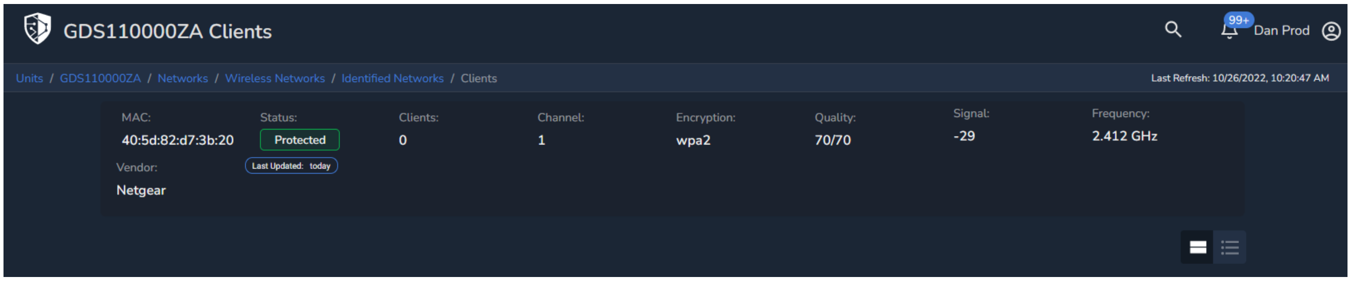
The wireless network card.

Items on the card are as shown:

1. MAC address. To protect this wireless network, click on it. Green means protected.
2. Clients connected to this wireless network.
3. SSID or name of the wireless network.
4. Manufacturer of the device.
5. Unit that found the wireless device.
6. Quality of the signal.
7. Frequency used.
8. Information/description of the card.
9. Actions menu to display options such as to protect the network.
10. Arrow to open the wireless network details page
11. Encryption used.
12. Signal strength.
13. Last updated.
14. Channel of operation.



The wireless network details page. This is the page it opens when we click on the arrow on the card.



GDS110000ZA Clients

99+ Dan Prod

Units / GDS110000ZA / Networks / Wireless Networks / Identified Networks / Clients

Last Refresh: 10/26/2022, 10:20:47 AM

MAC: 40:5d:82:d7:3b:20

Status: Protected

Last Updated: today

Vendor: Netgear

Clients: 0

Channel: 1

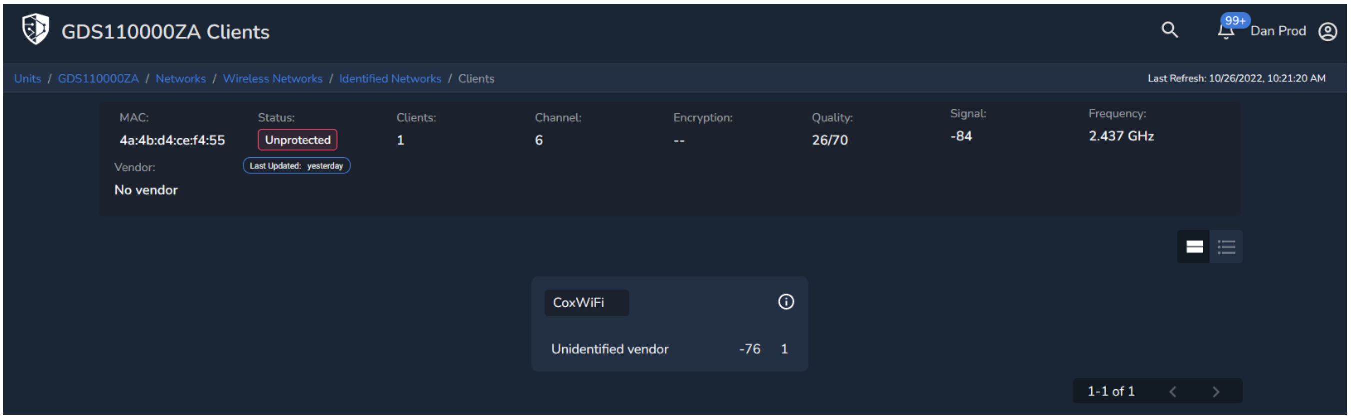
Encryption: wpa2

Quality: 70/70

Signal: -29

Frequency: 2.412 GHz

The wireless network clients page. This shows the information on those clients we identified as connected to the wireless network.



GDS110000ZA Clients

99+ Dan Prod

Units / GDS110000ZA / Networks / Wireless Networks / Identified Networks / Clients

Last Refresh: 10/26/2022, 10:21:20 AM

MAC: 4a:4b:d4:ce:f4:55

Status: Unprotected

Last Updated: yesterday

Vendor: No vendor

Clients: 1

Channel: 6

Encryption: --

Quality: 26/70

Signal: -84

Frequency: 2.437 GHz

CoxWiFi

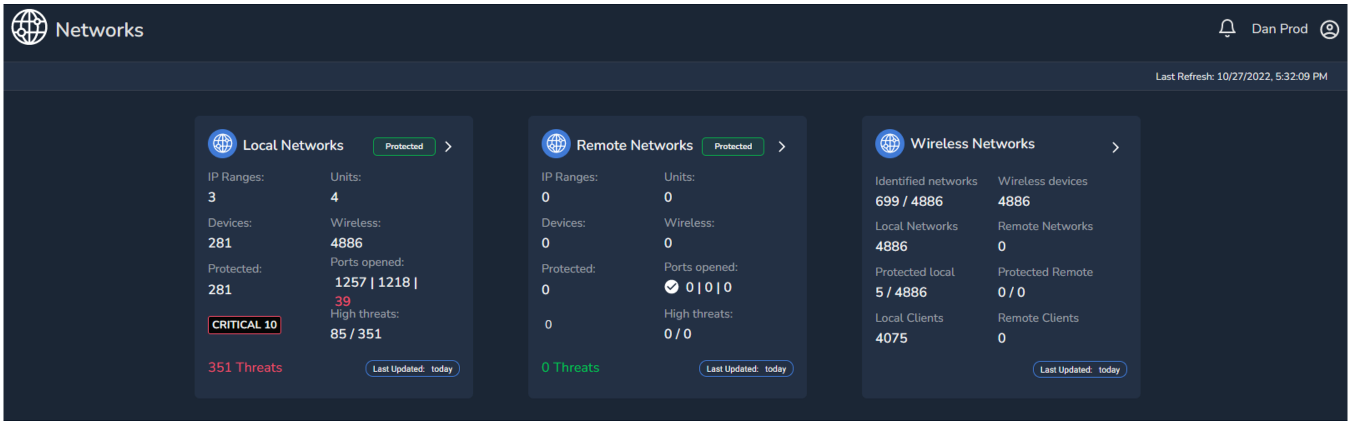
Unidentified vendor -76 1

1-1 of 1

Networks

The networks page. This is very similar to what we just went through but from a global perspective and aggregating data from all the units in the system. Here we show 3 consolidated cards. For a definition of these please see Terminology.

1. Local Networks.
2. Remote Networks.
3. Wireless Networks.



Networks

Dan Prod

Last Refresh: 10/27/2022, 5:32:09 PM

Local Networks Protected

IP Ranges: 3
Units: 4
Devices: 281
Wireless: 4886
Protected: 281
Ports opened: 1257 | 1218 | 39
CRITICAL 10
High threats: 85 / 351
351 Threats
Last Updated: today

Remote Networks Protected

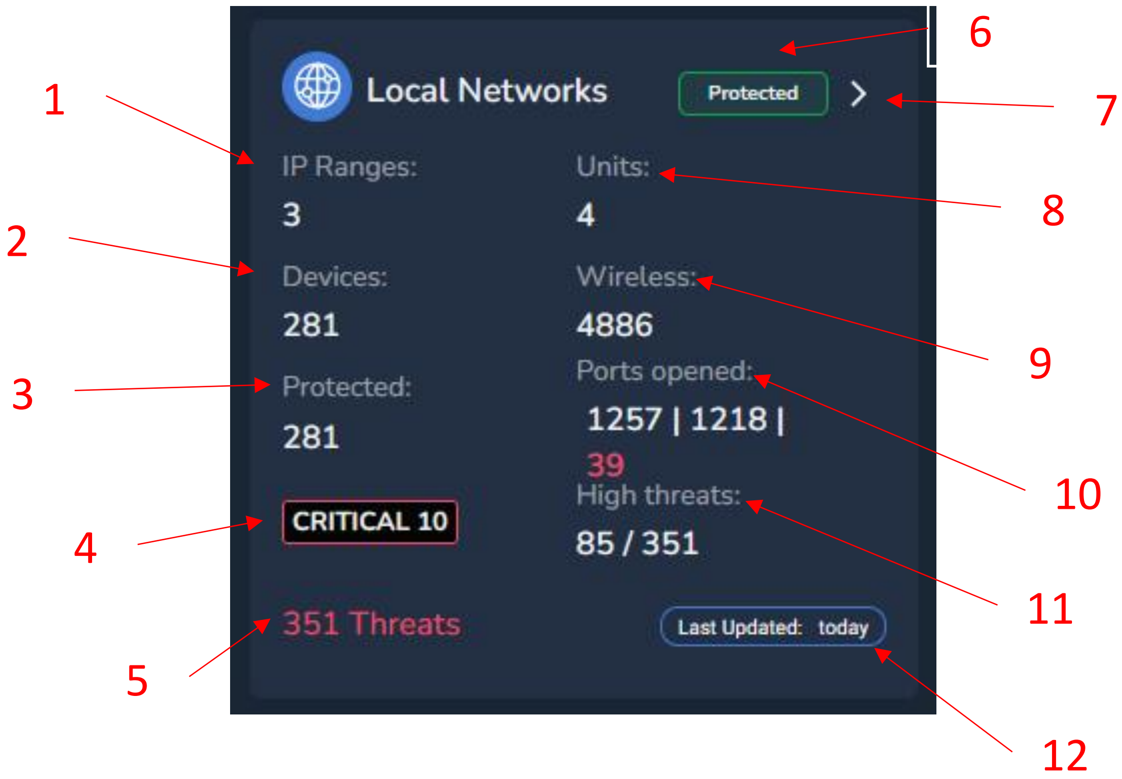
IP Ranges: 0
Units: 0
Devices: 0
Wireless: 0
Protected: 0
Ports opened: ✓ 0 | 0 | 0
0
High threats: 0 / 0
0 Threats
Last Updated: today

Wireless Networks

Identified networks 699 / 4886
Wireless devices 4886
Local Networks 4886
Remote Networks 0
Protected local 5 / 4886
Protected Remote 0 / 0
Local Clients 4075
Remote Clients 0
Last Updated: today

The global local networks card. Here we have the following items:

1. IP ranges. These are the IP ranges found on the network.
2. Devices. These are the connected devices, both wired and wireless, discovered on the network.
3. Protected devices. These are the total number of protected devices.
4. Severity level. The highest vulnerability severity level found.
5. Threats count. Total number of vulnerabilities found.
6. Protected status. Whether the entire network with all of its devices are protected or not.
7. Arrow to open the card.
8. Units. Fido units found on the network.
9. Wireless. These are the wireless networks (access points or transmitting devices) found around the unit.
10. Ports opened. These show the total number of ports found that are open and those with vulnerabilities related to them. You would read these as ports open | ports without vulnerabilities | ports with vulnerabilities. The last count should show the color of the highest threat found.
11. High threats count. Out of all vulnerabilities found (19), 5 are high.
12. Last updated. Last time we updated this card with the data from the unit.



Local Networks

Protected

IP Ranges: 3

Units: 4

Devices: 281

Wireless: 4886

Protected: 281

Ports opened: 1257 | 1218 | 39

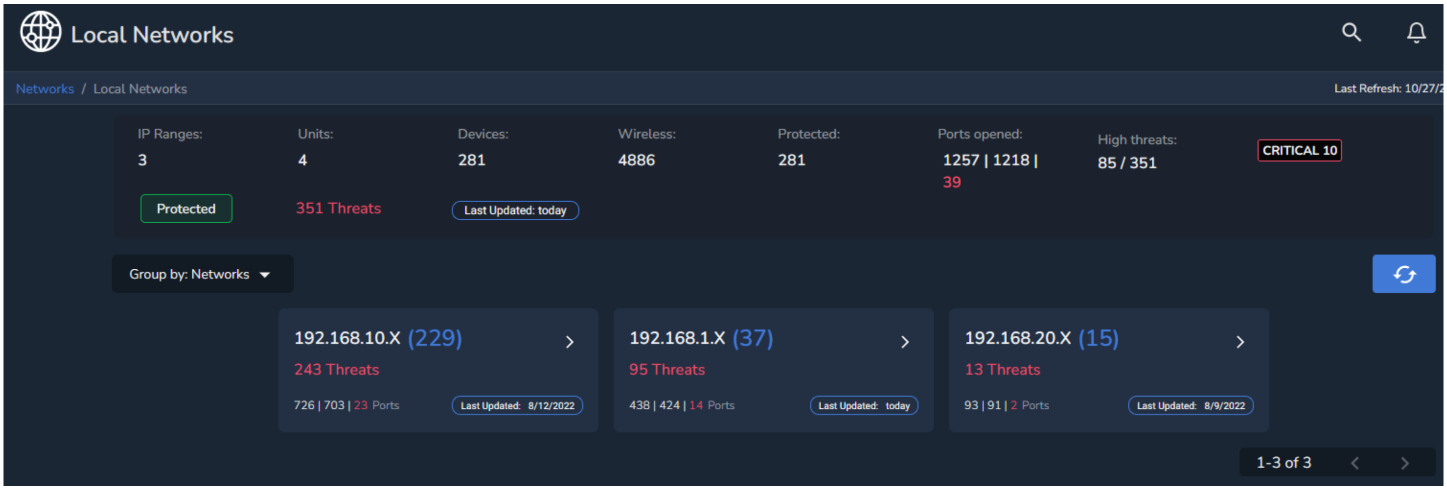
CRITICAL 10

High threats: 85 / 351

351 Threats

Last Updated: today

The local networks page. The information shown across the top of the screen is the same as the one shown on the card we previously went over. Below that details section, you will see the IP ranges found on the network.



Local Networks

Networks / Local Networks

Last Refresh: 10/27/2

IP Ranges: 3

Units: 4

Devices: 281

Wireless: 4886

Protected: 281

Ports opened: 1257 | 1218 | 39

High threats: 85 / 351

CRITICAL 10

Protected

351 Threats

Last Updated: today

Group by: Networks

192.168.10.X (229)
243 Threats
726 | 703 | 23 Ports
Last Updated: 8/12/2022

192.168.1.X (37)
95 Threats
438 | 424 | 14 Ports
Last Updated: today

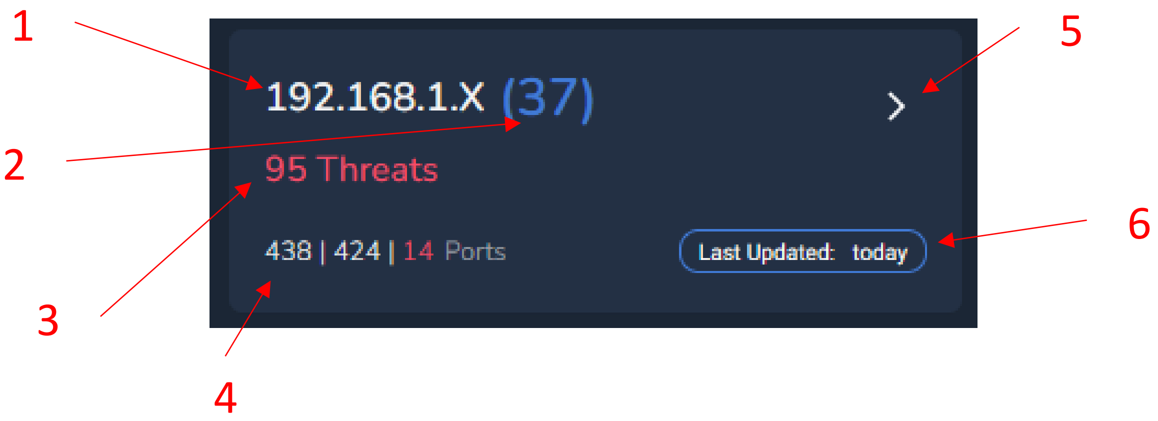
192.168.20.X (15)
13 Threats
93 | 91 | 2 Ports
Last Updated: 8/9/2022

1-3 of 3

The local networks IP range card. The card shows information we are already familiar with, such as

1. IP range
2. Number of devices
3. Number of threats
4. Ports open and with vulnerabilities

5. Arrow to open the IP range
6. Last updated.



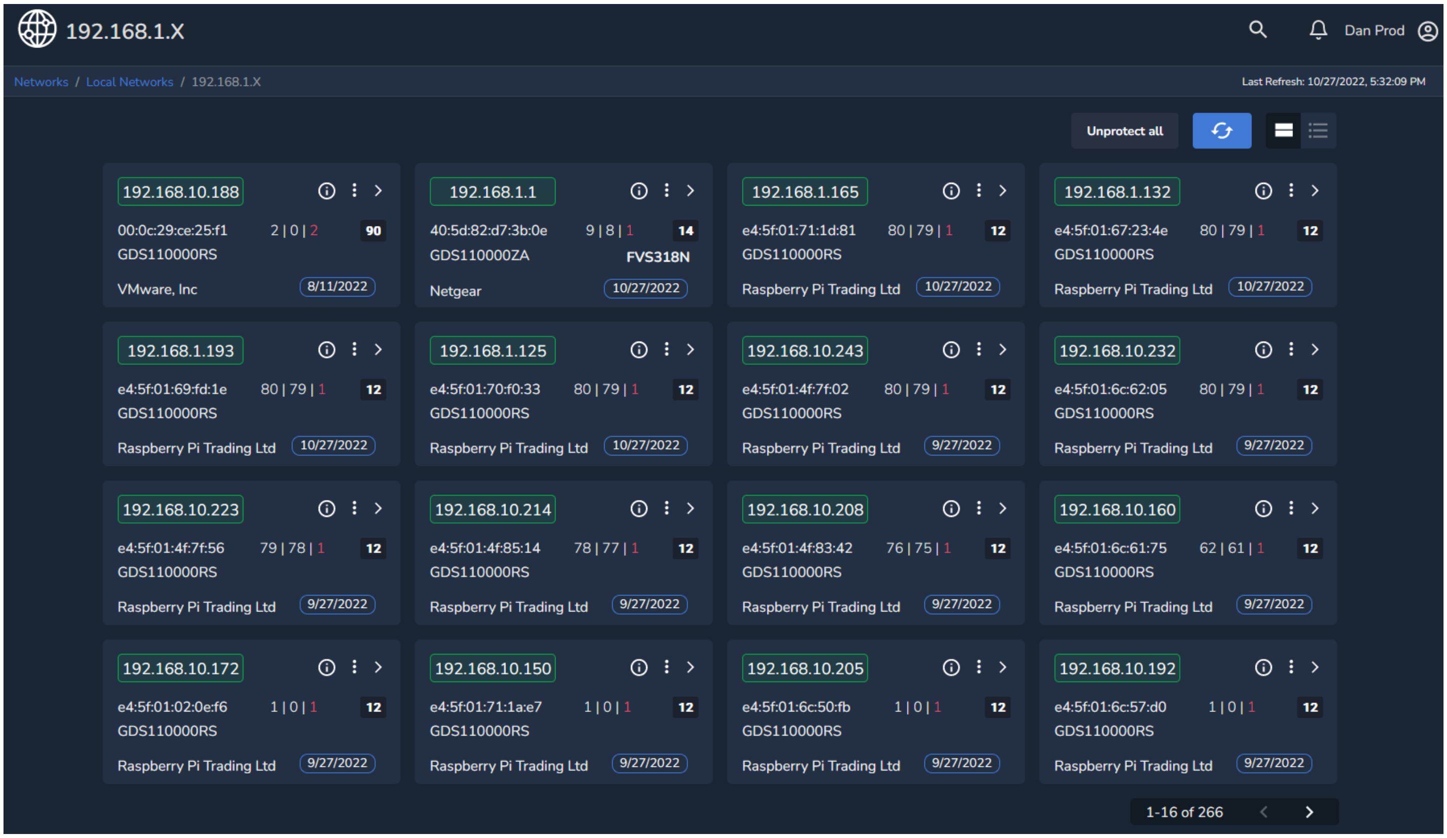
192.168.1.X (37)

95 Threats

438 | 424 | 14 Ports

Last Updated: today

The local networks devices page. By clicking on the arrow on the IP range card we get to this page.



192.168.1.X

Dan Prod

Networks / Local Networks / 192.168.1.X

Last Refresh: 10/27/2022, 5:32:09 PM

192.168.10.188
00:0c:29:ce:25:f1 2 | 0 | 2 90
GDS110000RS
VMware, Inc 8/11/2022

192.168.1.1
40:5d:82:d7:3b:0e 9 | 8 | 1 14
GDS110000ZA FVS318N
Netgear 10/27/2022

192.168.1.165
e4:5f:01:71:1d:81 80 | 79 | 1 12
GDS110000RS
Raspberry Pi Trading Ltd 10/27/2022

192.168.1.132
e4:5f:01:67:23:4e 80 | 79 | 1 12
GDS110000RS
Raspberry Pi Trading Ltd 10/27/2022

192.168.1.193
e4:5f:01:69:fd:1e 80 | 79 | 1 12
GDS110000RS
Raspberry Pi Trading Ltd 10/27/2022

192.168.1.125
e4:5f:01:70:f0:33 80 | 79 | 1 12
GDS110000RS
Raspberry Pi Trading Ltd 10/27/2022

192.168.10.243
e4:5f:01:4f:7f:02 80 | 79 | 1 12
GDS110000RS
Raspberry Pi Trading Ltd 9/27/2022

192.168.10.232
e4:5f:01:6c:62:05 80 | 79 | 1 12
GDS110000RS
Raspberry Pi Trading Ltd 9/27/2022

192.168.10.223
e4:5f:01:4f:7f:56 79 | 78 | 1 12
GDS110000RS
Raspberry Pi Trading Ltd 9/27/2022

192.168.10.214
e4:5f:01:4f:85:14 78 | 77 | 1 12
GDS110000RS
Raspberry Pi Trading Ltd 9/27/2022

192.168.10.208
e4:5f:01:4f:83:42 76 | 75 | 1 12
GDS110000RS
Raspberry Pi Trading Ltd 9/27/2022

192.168.10.160
e4:5f:01:6c:61:75 62 | 61 | 1 12
GDS110000RS
Raspberry Pi Trading Ltd 9/27/2022

192.168.10.172
e4:5f:01:02:0e:f6 1 | 0 | 1 12
GDS110000RS
Raspberry Pi Trading Ltd 9/27/2022

192.168.10.150
e4:5f:01:71:1a:e7 1 | 0 | 1 12
GDS110000RS
Raspberry Pi Trading Ltd 9/27/2022

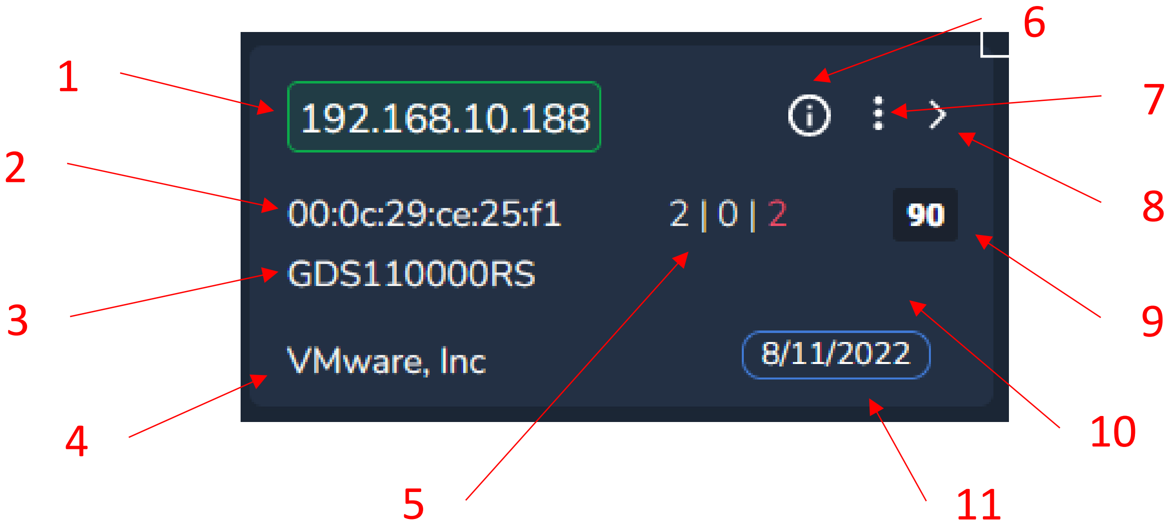
192.168.10.205
e4:5f:01:6c:50:fb 1 | 0 | 1 12
GDS110000RS
Raspberry Pi Trading Ltd 9/27/2022

192.168.10.192
e4:5f:01:6c:57:d0 1 | 0 | 1 12
GDS110000RS
Raspberry Pi Trading Ltd 9/27/2022

1-16 of 266

The connected device card. Items for this card:

1. IP of the connected device. To protect this device, click on it. Green means protected.
2. MAC address of the device.
3. Unit that discovered the device.
4. Manufacturer of the device discovered.
5. Port information.
6. Information/description of the card.
7. Actions menu to display options.
8. Arrow to open the device details page.
9. Number of threats.
10. Hostname of the device would show here.
11. Last updated. Last time we received data for this device.



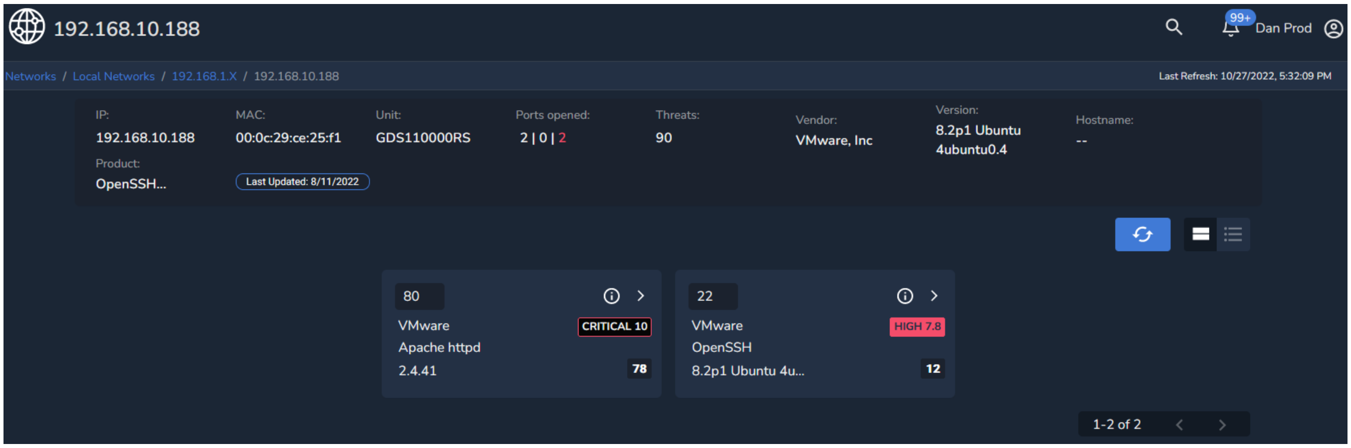
192.168.10.188

00:0c:29:ce:25:f1 2 | 0 | 2 90

GDS110000RS

VMware, Inc 8/11/2022

The connected device details page. This next page shows information up at the top that we are already familiar with and then below it, it shows information on the ports identified as opened.



192.168.10.188

Networks / Local Networks / 192.168.1.X / 192.168.10.188

Last Refresh: 10/27/2022, 5:32:09 PM

IP: 192.168.10.188

MAC: 00:0c:29:ce:25:f1

Unit: GDS110000RS

Ports opened: 2 | 0 | 2

Threats: 90

Vendor: VMware, Inc

Version: 8.2p1 Ubuntu 4ubuntu0.4

Hostname: --

Product: OpenSSH...

Last Updated: 8/11/2022

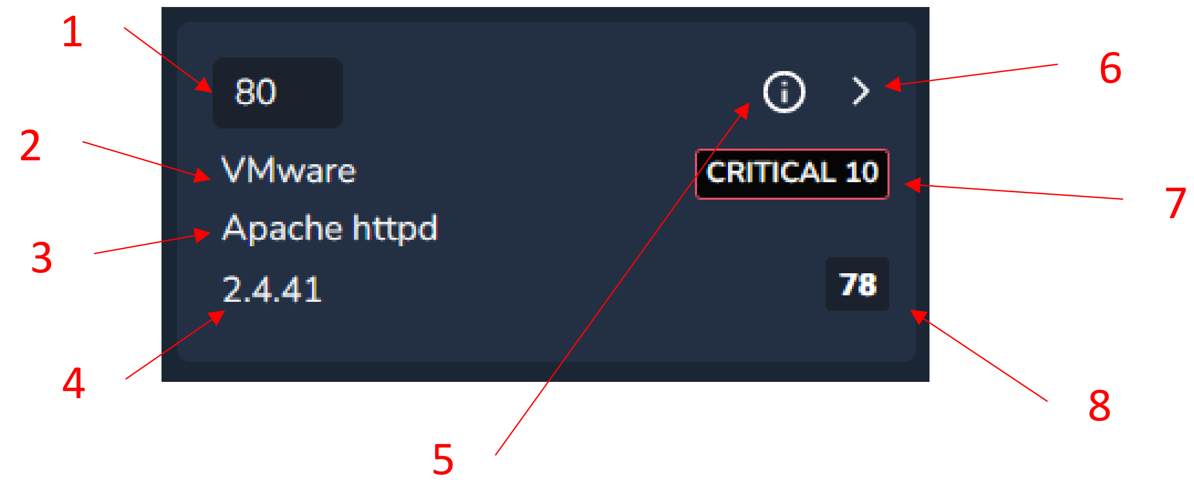
80
VMware
Apache httpd
2.4.41
CRITICAL 10
78

22
VMware
OpenSSH
8.2p1 Ubuntu 4u...
HIGH 7.8
12

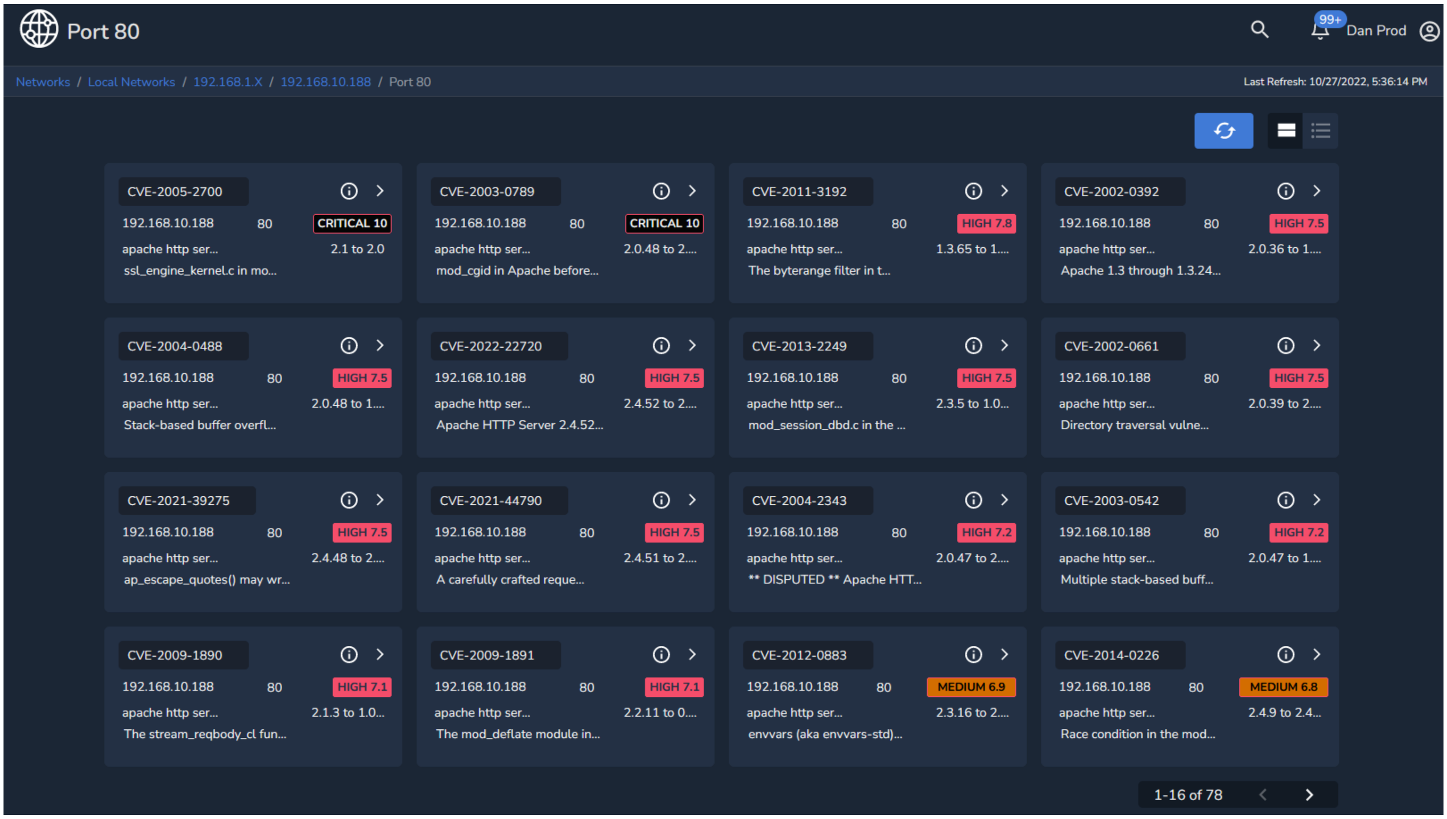
1-2 of 2

The device port card. The following items are part of this card:

1. Port.
2. Manufacturer.
3. Software identified.
4. Version of the software.
5. Information/description of the card.
6. Arrow to open the port card.
7. Vulnerability severity level.
8. Number of threats found.



The device port vulnerabilities page. This page shows all the vulnerabilities found that are related to the open port.



Port 80

99+ Dan Prod

Networks / Local Networks / 192.168.1.X / 192.168.10.188 / Port 80

Last Refresh: 10/27/2022, 5:36:14 PM

CVE-2005-2700
192.168.10.188 80 CRITICAL 10
apache http ser... 2.1 to 2.0
ssl_engine_kernel.c in mo...

CVE-2003-0789
192.168.10.188 80 CRITICAL 10
apache http ser... 2.0.48 to 2....
mod_cgid in Apache before...

CVE-2011-3192
192.168.10.188 80 HIGH 7.8
apache http ser... 1.3.65 to 1....
The byterange filter in t...

CVE-2002-0392
192.168.10.188 80 HIGH 7.5
apache http ser... 2.0.36 to 1....
Apache 1.3 through 1.3.24...

CVE-2004-0488
192.168.10.188 80 HIGH 7.5
apache http ser... 2.0.48 to 1....
Stack-based buffer overfl...

CVE-2022-22720
192.168.10.188 80 HIGH 7.5
apache http ser... 2.4.52 to 2....
Apache HTTP Server 2.4.52...

CVE-2013-2249
192.168.10.188 80 HIGH 7.5
apache http ser... 2.3.5 to 1.0...
mod_session_dbd.c in the ...

CVE-2002-0661
192.168.10.188 80 HIGH 7.5
apache http ser... 2.0.39 to 2....
Directory traversal vulne...

CVE-2021-39275
192.168.10.188 80 HIGH 7.5
apache http ser... 2.4.48 to 2....
ap_escape_quotes() may wr...

CVE-2021-44790
192.168.10.188 80 HIGH 7.5
apache http ser... 2.4.51 to 2....
A carefully crafted reque...

CVE-2004-2343
192.168.10.188 80 HIGH 7.2
apache http ser... 2.0.47 to 2....
** DISPUTED ** Apache HTT...

CVE-2003-0542
192.168.10.188 80 HIGH 7.2
apache http ser... 2.0.47 to 1....
Multiple stack-based buff...

CVE-2009-1890
192.168.10.188 80 HIGH 7.1
apache http ser... 2.1.3 to 1.0...
The stream_reqbody_cl fun...

CVE-2009-1891
192.168.10.188 80 HIGH 7.1
apache http ser... 2.2.11 to 0....
The mod_deflate module in...

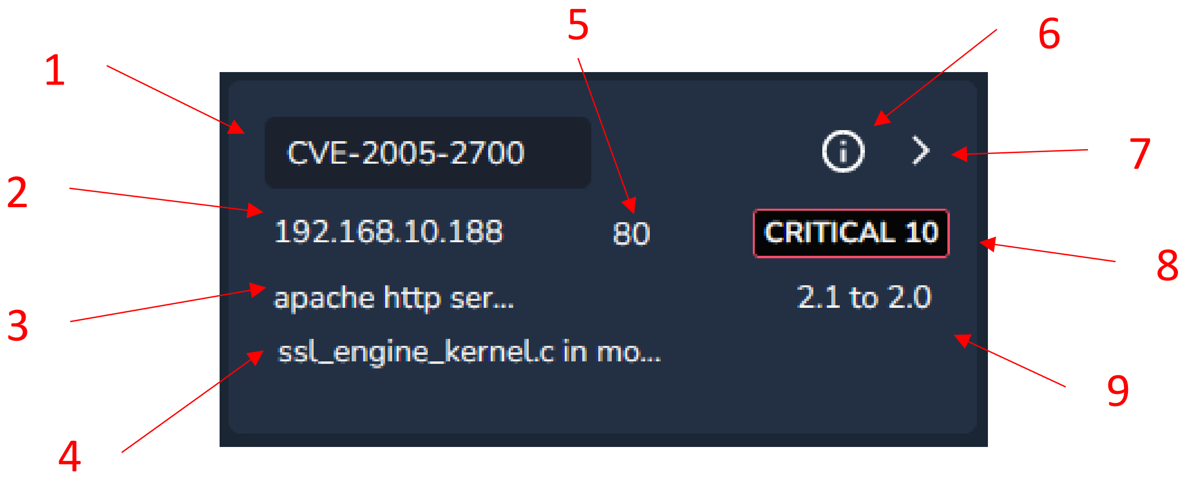
CVE-2012-0883
192.168.10.188 80 MEDIUM 6.9
apache http ser... 2.3.16 to 2....
envvars (aka envvars-std)...

CVE-2014-0226
192.168.10.188 80 MEDIUM 6.8
apache http ser... 2.4.9 to 2.4...
Race condition in the mod...

1-16 of 78

The port vulnerability card. This is similar as other vulnerabilities cards we have seen before on this manual. Items are:

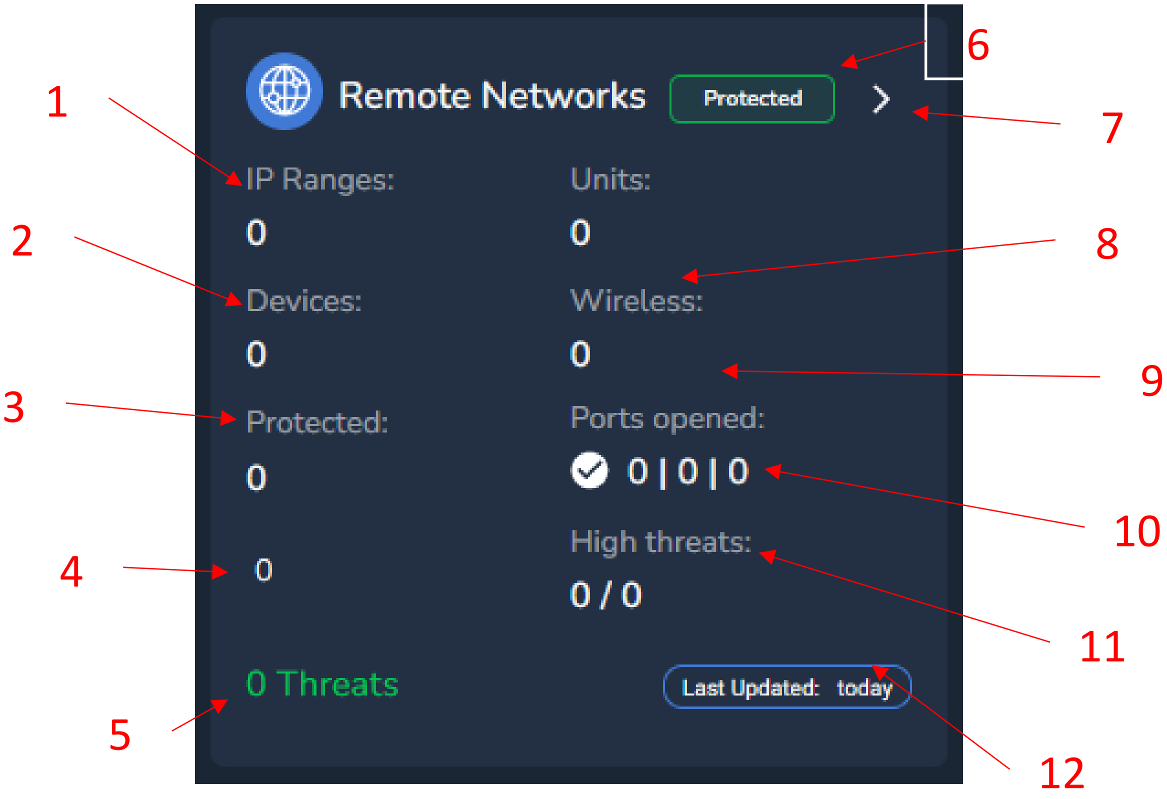
1. CVE of the vulnerability.
2. Device where the vulnerability was found.
3. Software affected.
4. Brief description of the vulnerability.
5. Open port related to it.
6. Information/description icon.
7. Arrow to go to NIST article about the vulnerability.
8. Score of vulnerability.
9. Version impacted.



CVE-2005-2700
192.168.10.188 80 CRITICAL 10
apache http ser... 2.1 to 2.0
ssl_engine_kernel.c in mo...

The global remote networks card. Items for this card are similar from what we have seen before:

1. IP ranges. These are the IP ranges found on the network.
2. Devices. These are the connected devices, both wired and wireless, discovered on the network.
3. Protected devices. These are the total number of protected devices.
4. Severity level. The highest vulnerability severity level found, if any.
5. Threats count. Total number of vulnerabilities found.
6. Protected status. Whether the entire network with all of its devices are protected or not.
7. Arrow to open the remote networks page.
8. Units. Fido units found on the network.
9. Wireless. These are the wireless networks (access points or transmitting devices) found around the unit.
10. Ports opened. These show the total number of ports found that are open and those with vulnerabilities related to them. You would read these as ports open | ports without vulnerabilities | ports with vulnerabilities. The last count should show the color of the highest threat found.
11. High threats count. Out of all vulnerabilities found (19), 5 are high.
12. Last updated. Last time we updated this card with the data from the unit.


Remote Networks

Protected

IP Ranges:
0

Units:
0

Devices:
0

Wireless:
0

Protected:
0

Ports opened:
✓ 0 | 0 | 0

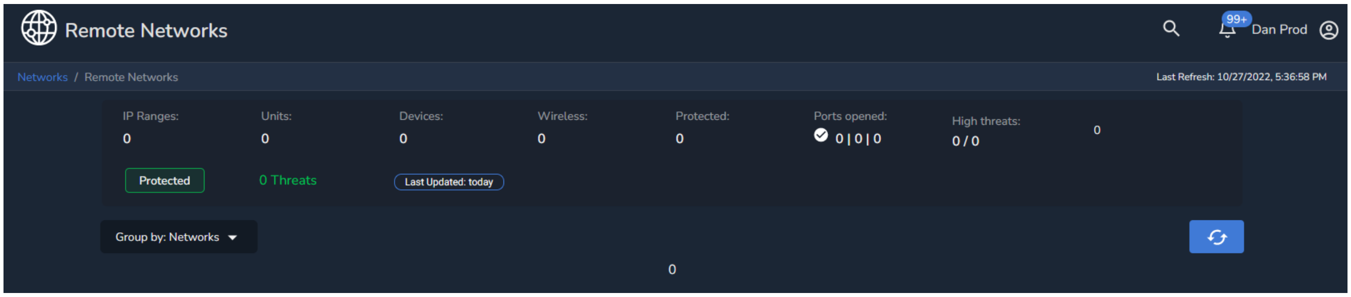
0

High threats:
0 / 0

0 Threats

Last Updated: today

The remote networks details page. When you have units that are marked as remote then the data will be shown on this page below. This is very similar to the local networks page.



Last Refresh: 10/27/2022, 5:36:58 PM

IP Ranges: 0

Units: 0

Devices: 0

Wireless: 0

Protected: 0

Ports opened: 0 | 0 | 0

High threats: 0 / 0

0

0 Threats

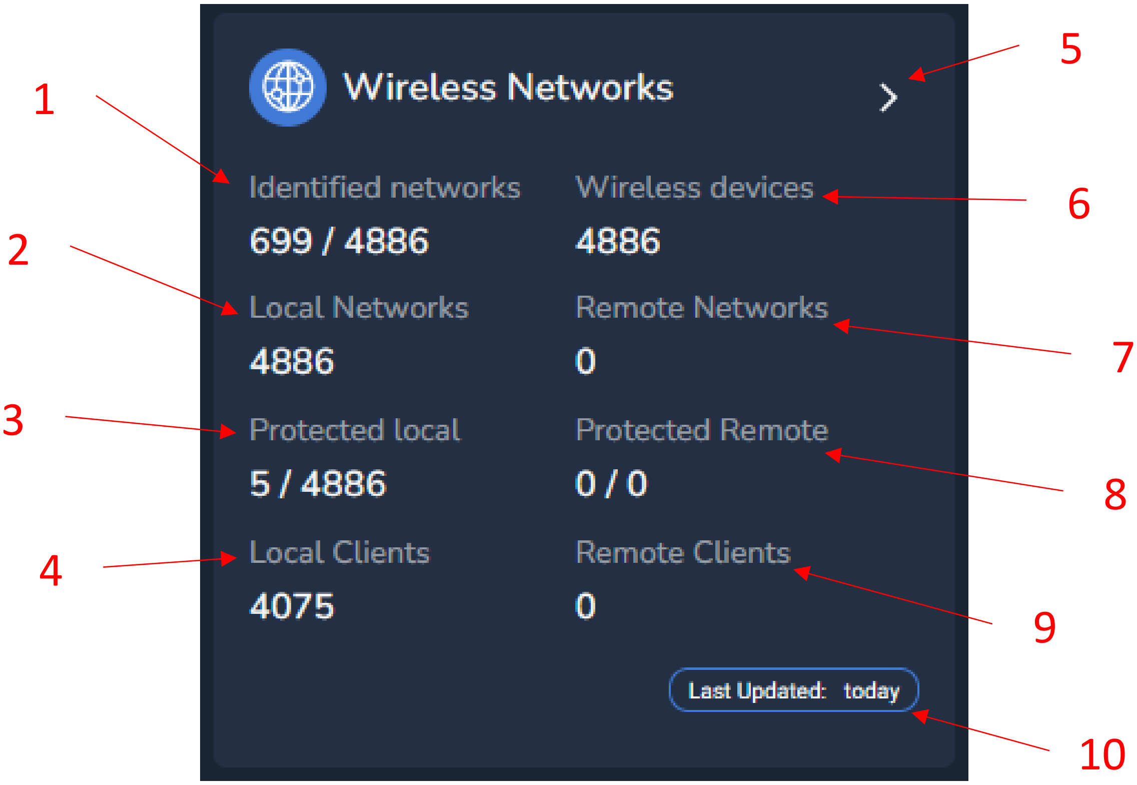
Last Updated: today

Group by: Networks

0

The global wireless networks card. Items on this card:

1. Identified networks. Number of identified networks over total found.
2. Local networks. If the unit is local then it would show wireless networks.
3. Protected local. How many of those wireless are protected.
4. Local clients. How many clients in total are seen in the wireless networks.
5. Arrow to open wireless networks page.
6. Wireless devices. Total number of wireless devices found (access points or transmitting)
7. Remote networks. If the unit is remote then it would show the count here.
8. Protected remote. Protected wireless that are remote.
9. Remote clients . Clients connected to wireless remote.
10. Last updated. Last time data was refreshed.



Wireless Networks

Identified networks
699 / 4886

Wireless devices
4886

Local Networks
4886

Remote Networks
0

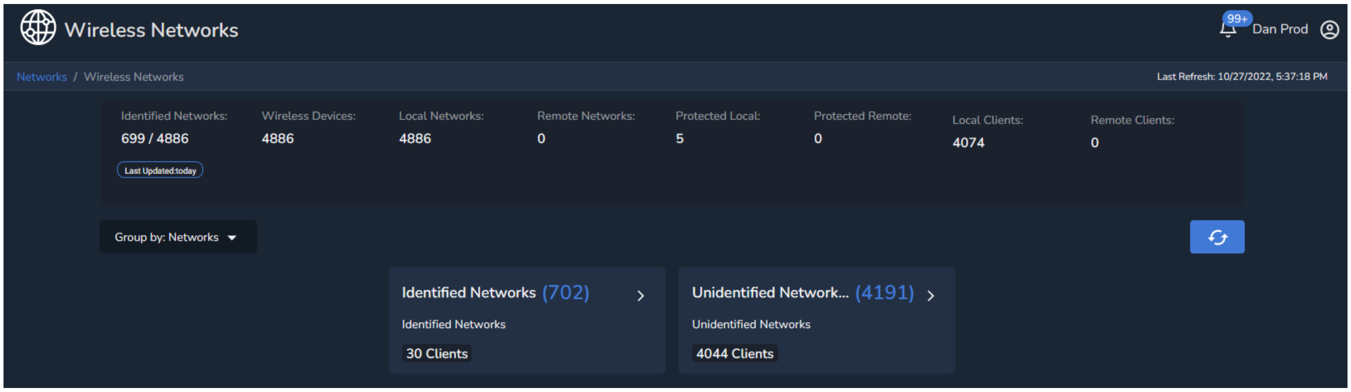
Protected local
5 / 4886

Protected Remote
0 / 0

Local Clients
4075

Remote Clients
0

The wireless networks details page. At the top of the page we show the details on wireless networks as we did on the card you clicked on to get here. Below that section of the page you have wireless we have found that are both identified and unidentified.



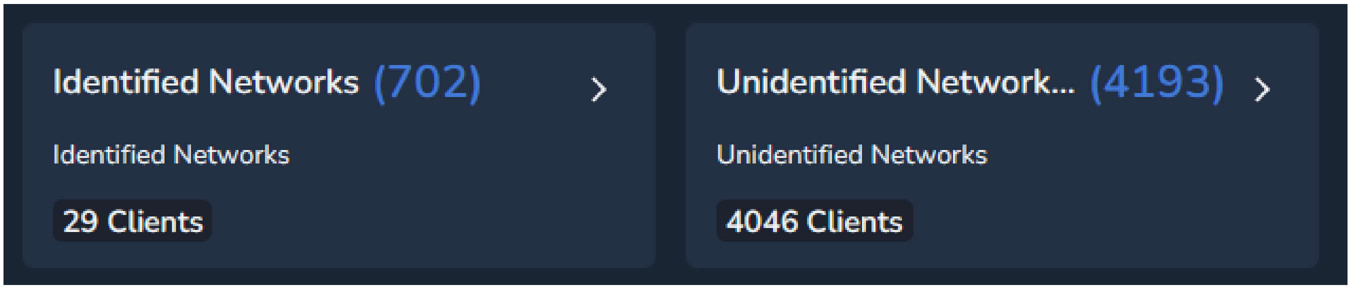
Last Refresh: 10/27/2022, 5:37:18 PM

Identified Networks:	Wireless Devices:	Local Networks:	Remote Networks:	Protected Local:	Protected Remote:	Local Clients:	Remote Clients:
699 / 4886	4886	4886	0	5	0	4074	0

Identified Networks (702)
Identified Networks
30 Clients

Unidentified Network... (4191)
Unidentified Networks
4044 Clients

Identified and unidentified wireless networks. In some cases given the nature of wireless networks and the configuration of said networks we may pick up the names, SSID, and some other times those would be hidden and therefore unidentified.



Identified Networks (702)

Identified Networks

29 Clients

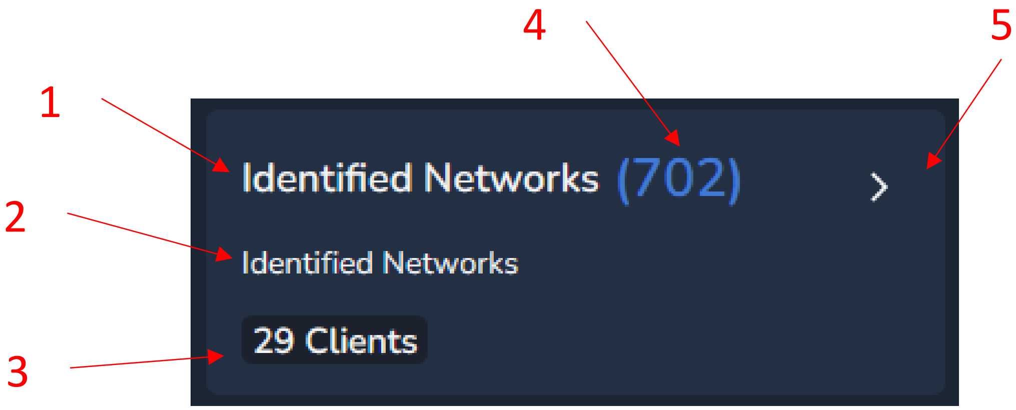
Unidentified Network... (4193)

Unidentified Networks

4046 Clients

The identified networks card. Items on this card:

1. Identified networks.
2. Subtype, in this case also identified networks.
3. Total number of clients connected to these networks.
4. Total number of those identified networks.
5. Arrow to open the card to see the networks found.

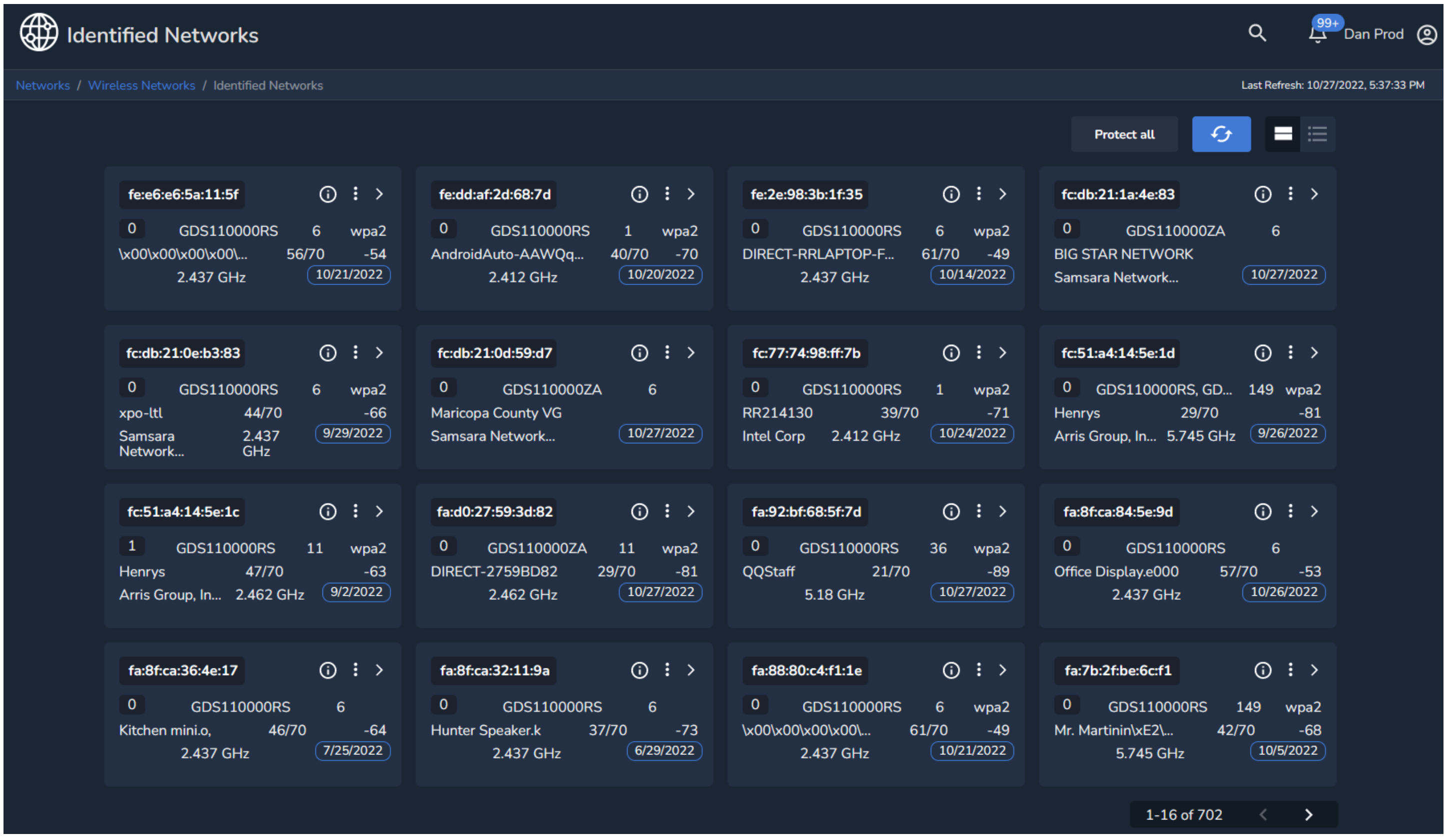


Identified Networks (702)

Identified Networks

29 Clients

The identified networks page. When you click on the arrow it opens this new page with all the networks found.



Networks / Wireless Networks / Identified Networks

Last Refresh: 10/27/2022, 5:37:33 PM

fe:e6:e6:5a:11:5f
0 GDS110000RS 6 wpa2
\x00\x00\x00\x00\... 56/70 -54
2.437 GHz 10/21/2022

fe:dd:af:2d:68:7d
0 GDS110000RS 1 wpa2
AndroidAuto-AAWQq... 40/70 -70
2.412 GHz 10/20/2022

fe:2e:98:3b:1f:35
0 GDS110000RS 6 wpa2
DIRECT-RRLAPTOP-F... 61/70 -49
2.437 GHz 10/14/2022

fc:db:21:1a:4e:83
0 GDS110000ZA 6
BIG STAR NETWORK
Samsara Network... 10/27/2022

fc:db:21:0e:b3:83
0 GDS110000RS 6 wpa2
xpo-ltl 44/70 -66
Samsara Network... 2.437 GHz 9/29/2022

fc:db:21:0d:59:d7
0 GDS110000ZA 6
Maricopa County VG
Samsara Network... 10/27/2022

fc:77:74:98:ff:7b
0 GDS110000RS 1 wpa2
RR214130 39/70 -71
Intel Corp 2.412 GHz 10/24/2022

fc:51:a4:14:5e:1d
0 GDS110000RS, GD... 149 wpa2
Henrys 29/70 -81
Arris Group, In... 5.745 GHz 9/26/2022

fc:51:a4:14:5e:1c
1 GDS110000RS 11 wpa2
Henrys 47/70 -63
Arris Group, In... 2.462 GHz 9/2/2022

fa:d0:27:59:3d:82
0 GDS110000ZA 11 wpa2
DIRECT-2759BD82 29/70 -81
2.462 GHz 10/27/2022

fa:92:bf:68:5f:7d
0 GDS110000RS 36 wpa2
QQStaff 21/70 -89
5.18 GHz 10/27/2022

fa:8f:ca:84:5e:9d
0 GDS110000RS 6
Office Display.e000 57/70 -53
2.437 GHz 10/26/2022

fa:8f:ca:36:4e:17
0 GDS110000RS 6
Kitchen mini.o, 46/70 -64
2.437 GHz 7/25/2022

fa:8f:ca:32:11:9a
0 GDS110000RS 6
Hunter Speaker.k 37/70 -73
2.437 GHz 6/29/2022

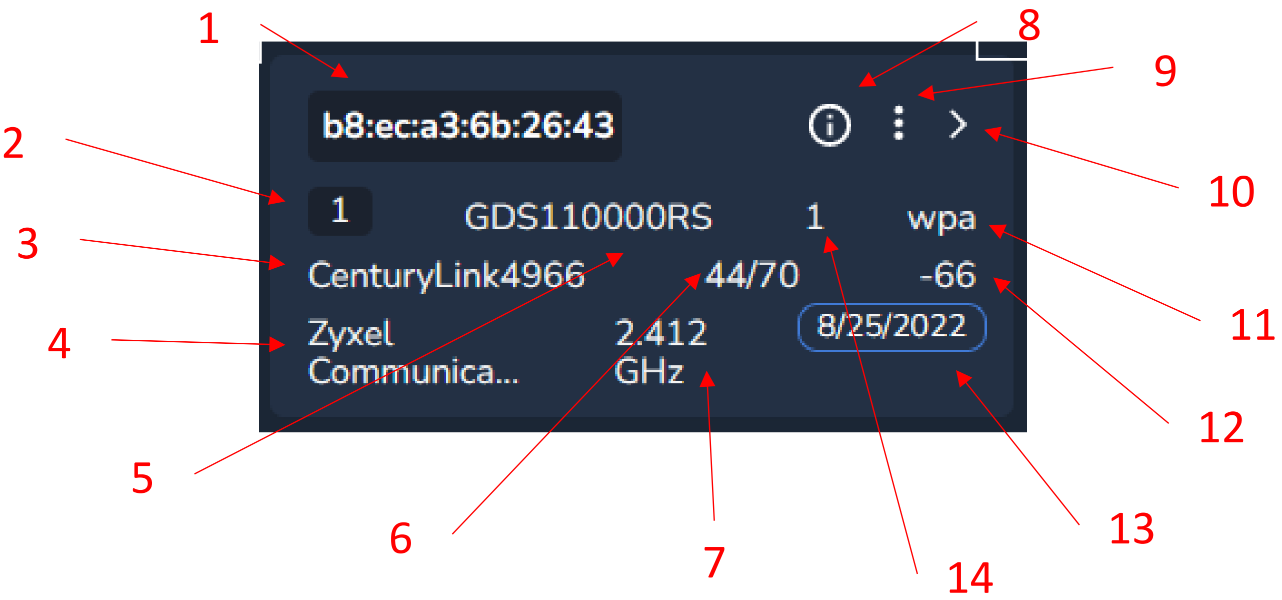
fa:88:80:c4:f1:1e
0 GDS110000RS 6 wpa2
\x00\x00\x00\x00\... 61/70 -49
2.437 GHz 10/21/2022

fa:7b:2f:be:6c:f1
0 GDS110000RS 149 wpa2
Mr. Martinin\xE2\... 42/70 -68
5.745 GHz 10/5/2022

1-16 of 702

The wireless network card. Items on the card are as shown:

1. MAC address. To protect this wireless network, click on it. Green means protected.
2. Clients connected to this wireless network.
3. SSID or name of the wireless network.
4. Manufacturer of the device.
5. Unit that found the wireless device.
6. Quality of the signal.
7. Frequency used.
8. Information/description of the card.
9. Actions menu to display options such as to protect the network.
10. Arrow to open the wireless network details page
11. Encryption used.
12. Signal strength.
13. Last updated.
14. Channel of operation.



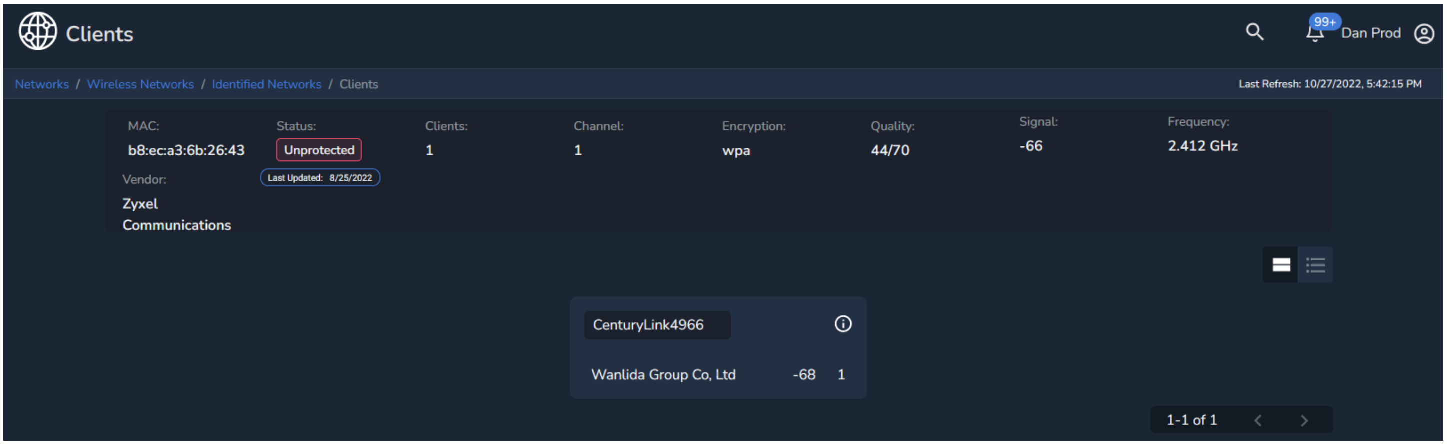
b8:ec:a3:6b:26:43

1 GDS110000RS 1 wpa

CenturyLink4966 44/70 -66

Zyxel Communica... 2.412 GHz 8/25/2022

The wireless network details page.



Clients

Dan Prod

Networks / Wireless Networks / Identified Networks / Clients

Last Refresh: 10/27/2022, 5:42:15 PM

MAC:	Status:	Clients:	Channel:	Encryption:	Quality:	Signal:	Frequency:
b8:ec:a3:6b:26:43	Unprotected	1	1	wpa	44/70	-66	2.412 GHz

Vendor: Zyxel Communications

Last Updated: 8/25/2022

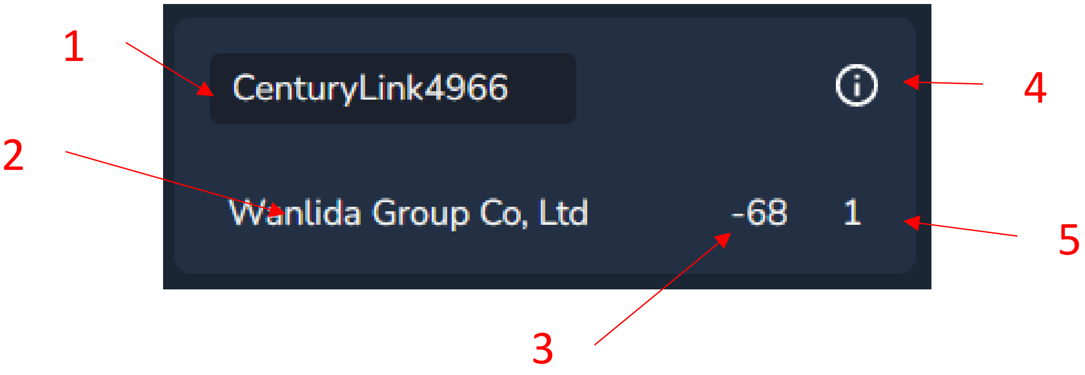
CenturyLink4966

Wanlida Group Co, Ltd -68 1

1-1 of 1

The wireless network clients card. This card shows the information on the client connected to the wireless network we opened previously. Items on this card:

1. Wireless network name (SSID).
2. Manufacturer of the client hardware device.
3. Information/description of the card.
4. Strength of the signal.
5. Number of packets captured.

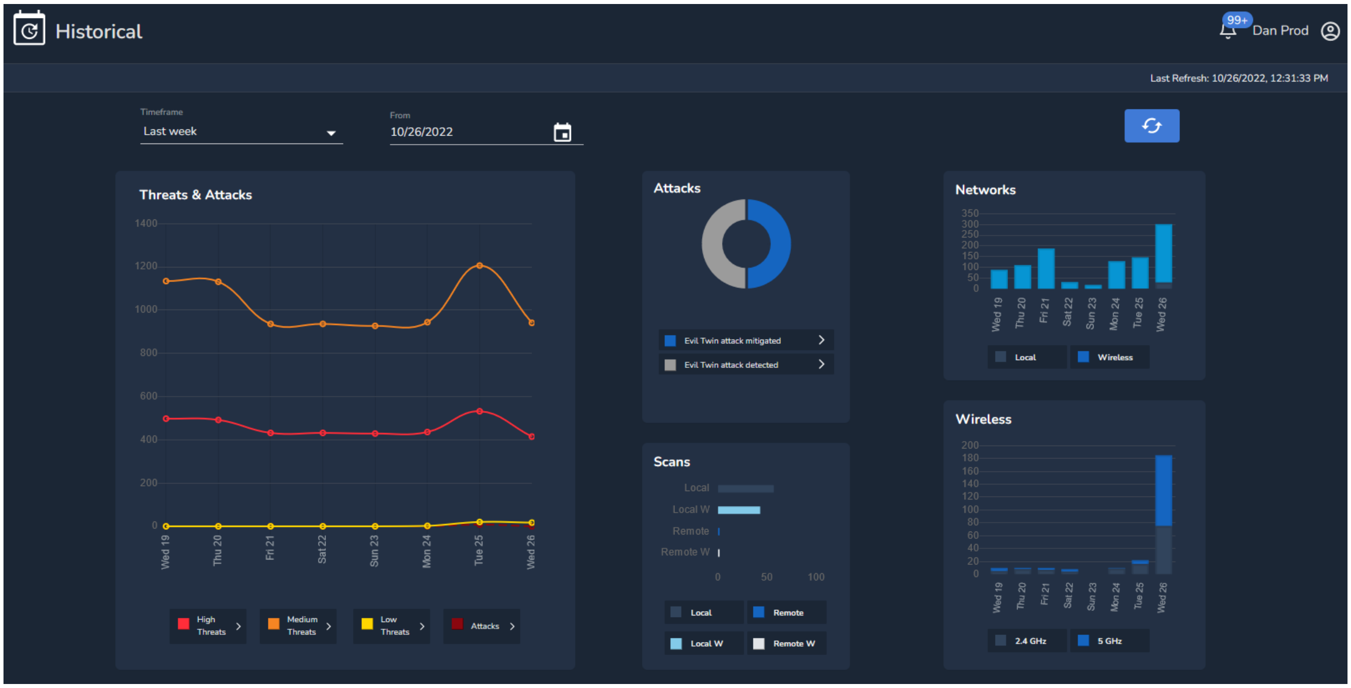


CenturyLink4966

Wanlida Group Co, Ltd -68 1

Historical

The global historical page.



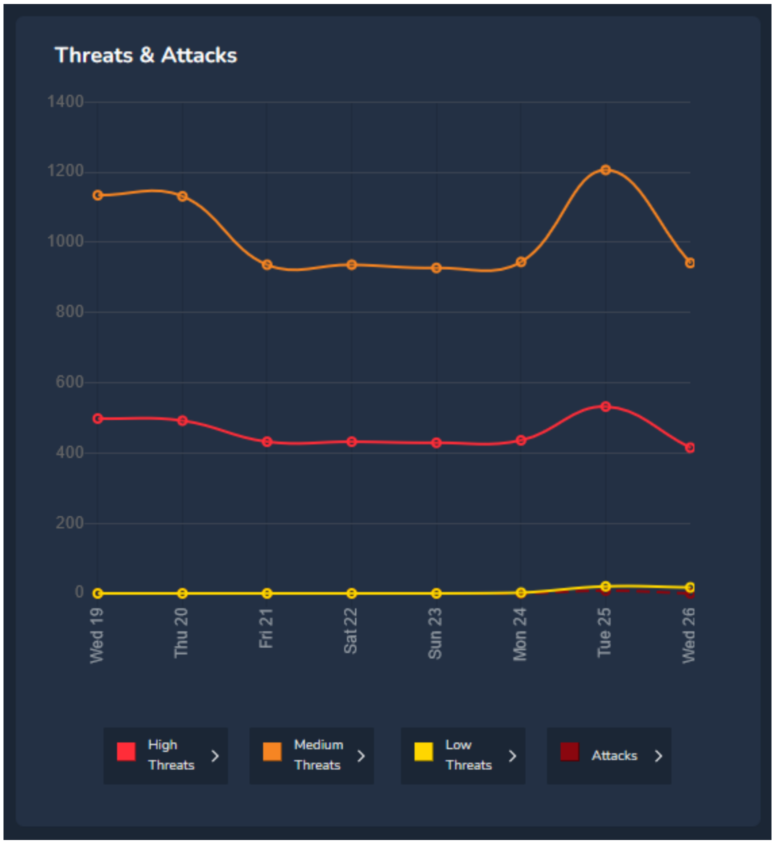
Historical

Last Refresh: 10/26/2022, 12:31:33 PM

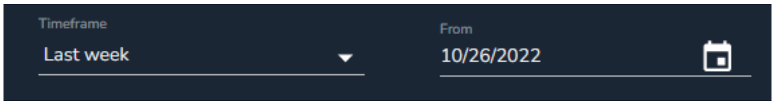
Timeframe: Last week

From: 10/26/2022

The historical threats and attacks graphic card.

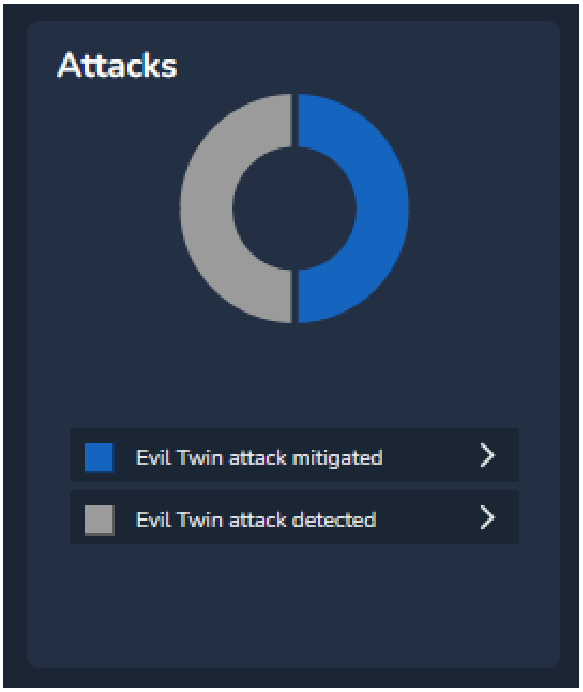


The timeframe selector.

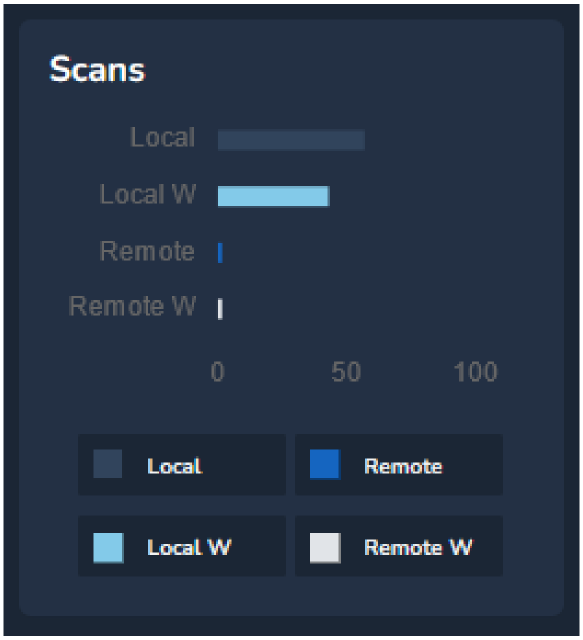

Timeframe
Last week

From
10/26/2022

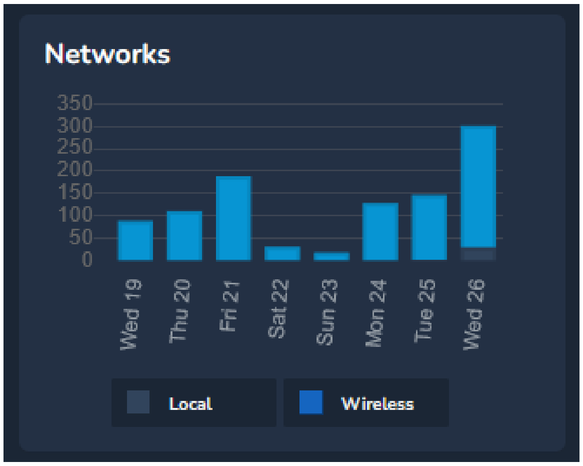
The historical attacks card.



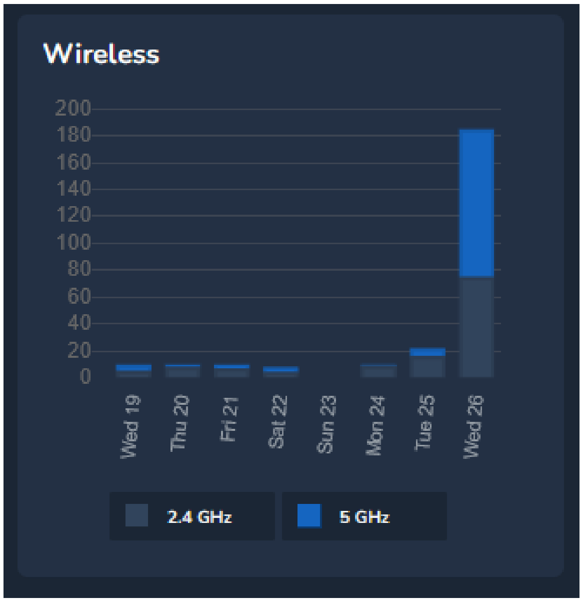
The historical scans card.



The historical networks card.



The historical wireless card.

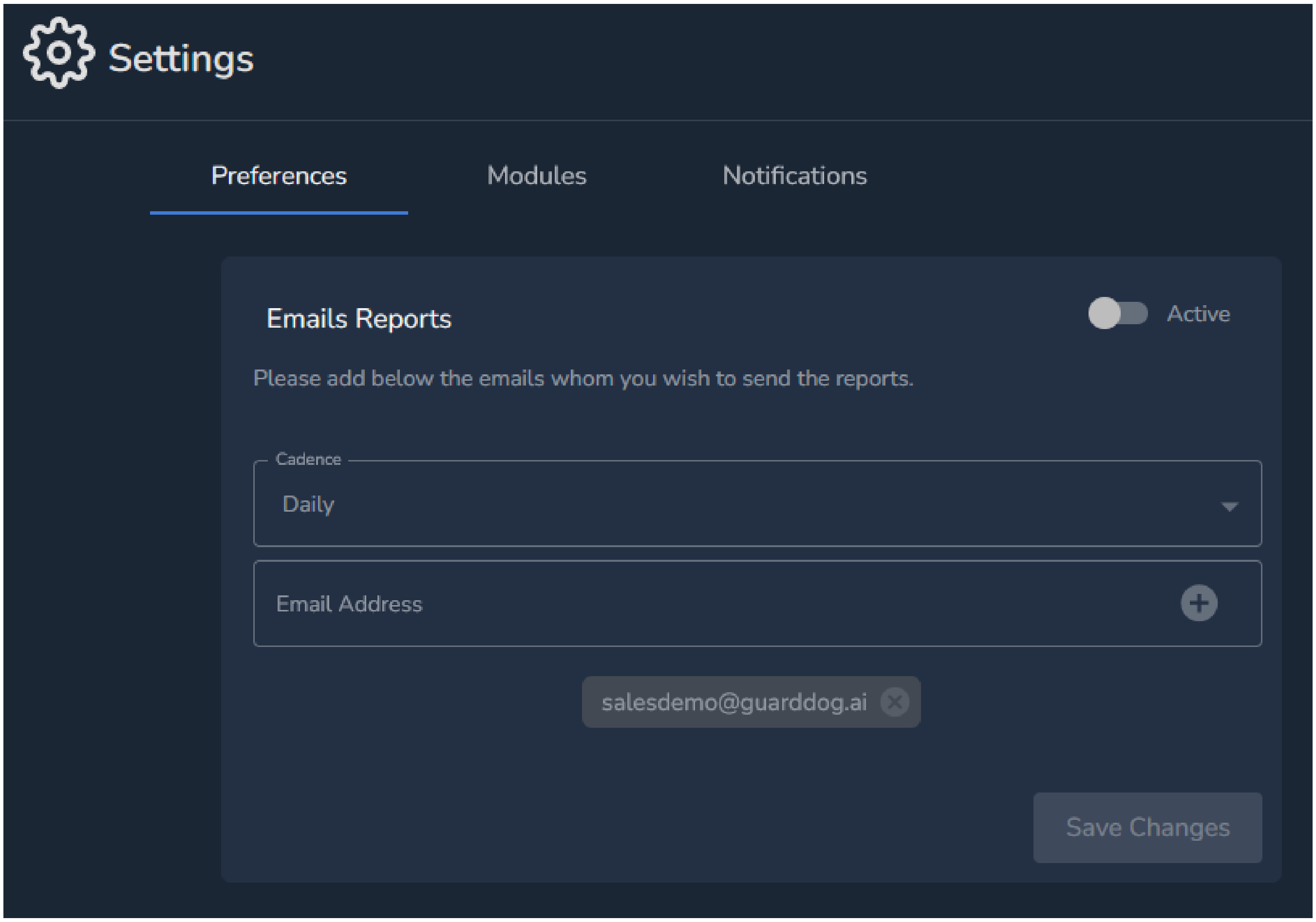


Settings

The settings page. This is the page where we have multiple sections in regards to how the system and the portal is configured for the client.

Preferences

At this moment this is where we have the ability to configure an email report with a specific cadence.



Emails Reports

Active

Please add below the emails whom you wish to send the reports.

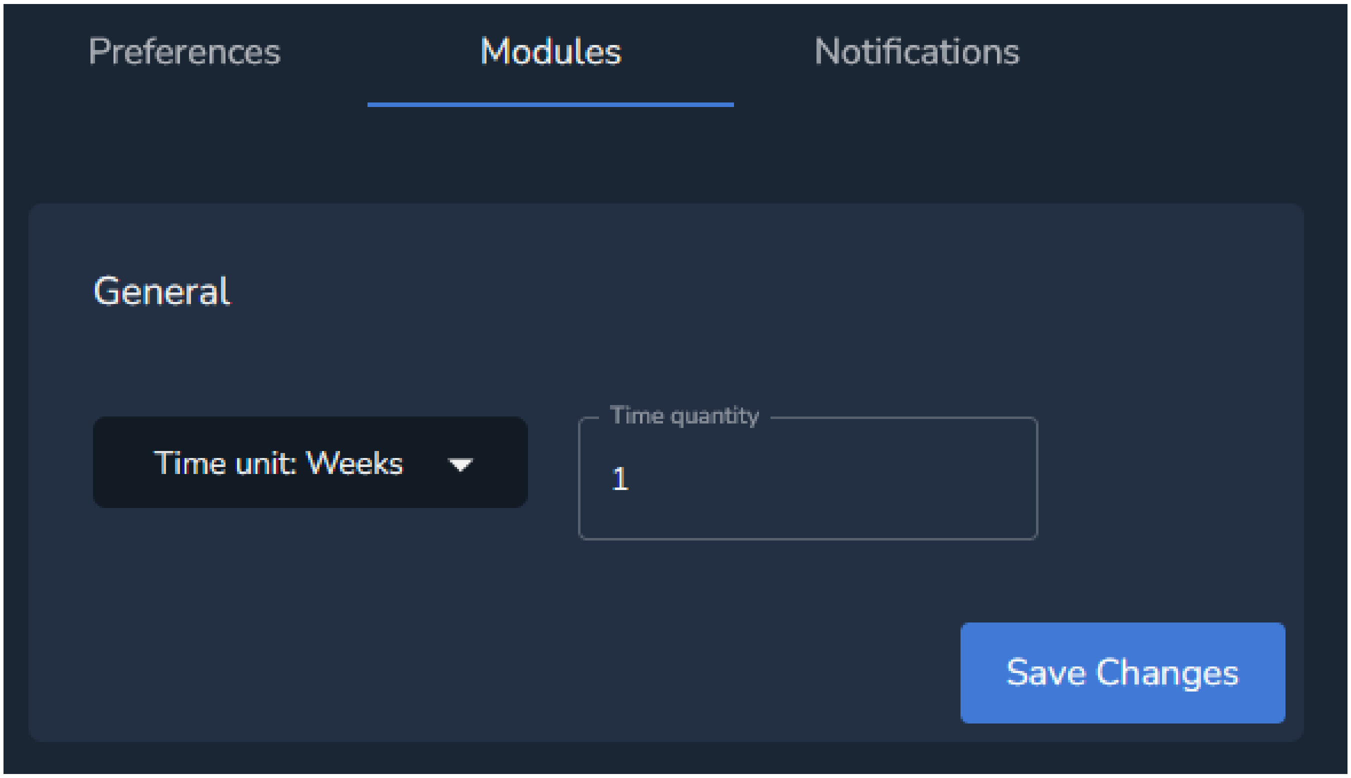
Cadence: Daily

Email Address

salesdemo@guarddog.ai

Modules

This contains configuration settings for modules. In the image below you have the option to select the time interval for the information shown in the portal. By default the modules are configured to show the data from the last week but there are many other possible combinations between the quantity and the timeframe. Don't forget to click on save changes.

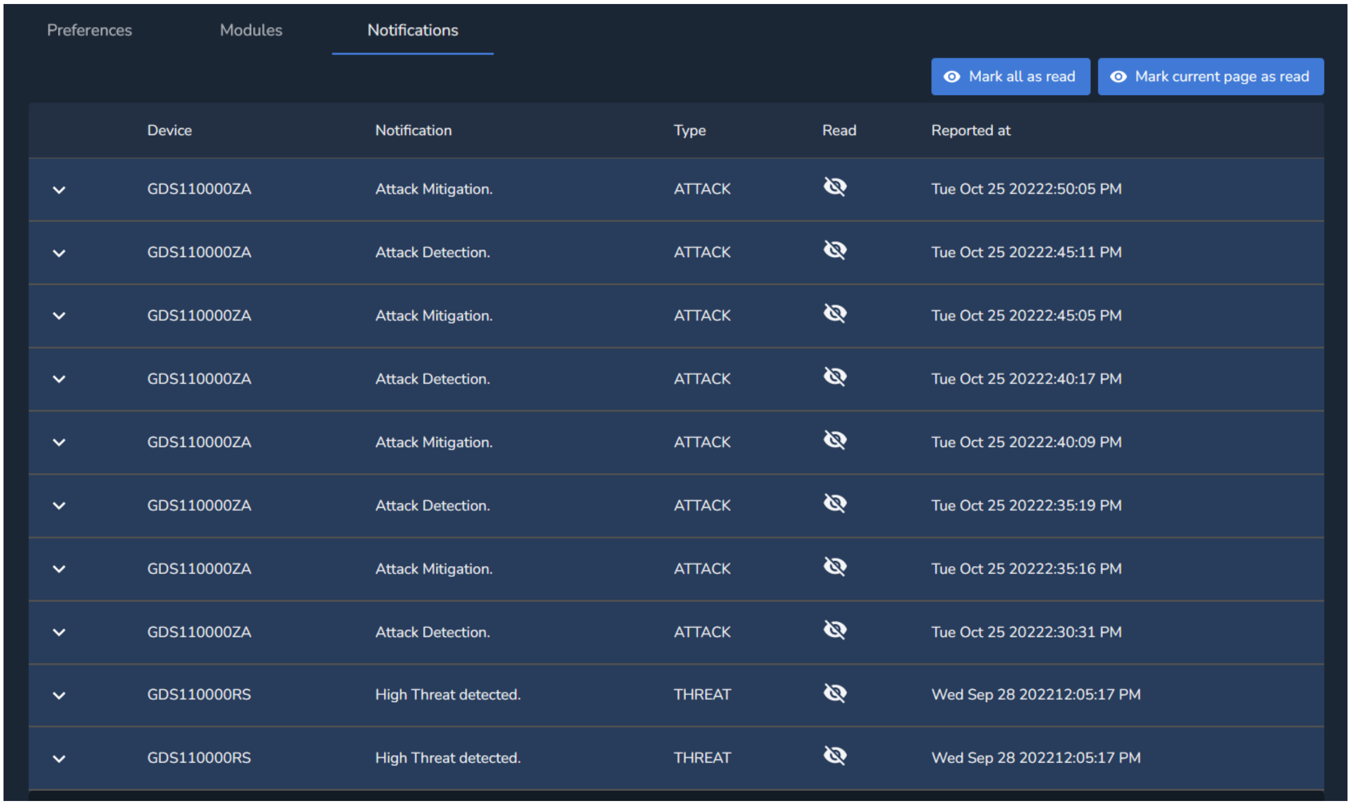


General

Time unit: Weeks

Time quantity
1

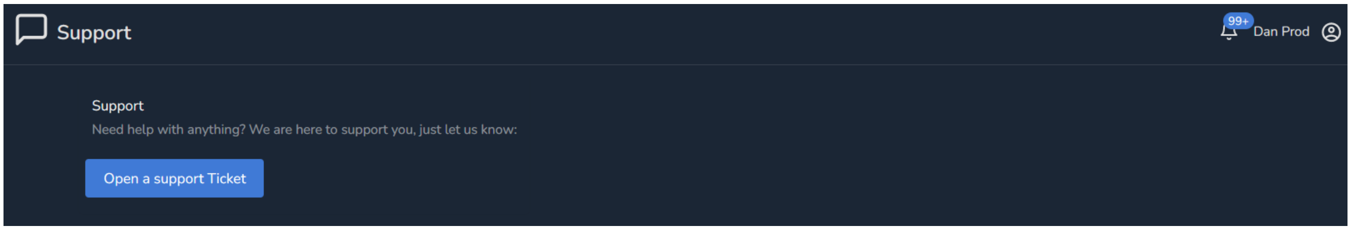
Notifications



	Device	Notification	Type	Read	Reported at
⌄	GDS110000ZA	Attack Mitigation.	ATTACK	⊘	Tue Oct 25 20222:50:05 PM
⌄	GDS110000ZA	Attack Detection.	ATTACK	⊘	Tue Oct 25 20222:45:11 PM
⌄	GDS110000ZA	Attack Mitigation.	ATTACK	⊘	Tue Oct 25 20222:45:05 PM
⌄	GDS110000ZA	Attack Detection.	ATTACK	⊘	Tue Oct 25 20222:40:17 PM
⌄	GDS110000ZA	Attack Mitigation.	ATTACK	⊘	Tue Oct 25 20222:40:09 PM
⌄	GDS110000ZA	Attack Detection.	ATTACK	⊘	Tue Oct 25 20222:35:19 PM
⌄	GDS110000ZA	Attack Mitigation.	ATTACK	⊘	Tue Oct 25 20222:35:16 PM
⌄	GDS110000ZA	Attack Detection.	ATTACK	⊘	Tue Oct 25 20222:30:31 PM
⌄	GDS110000RS	High Threat detected.	THREAT	⊘	Wed Sep 28 202212:05:17 PM
⌄	GDS110000RS	High Threat detected.	THREAT	⊘	Wed Sep 28 202212:05:17 PM

Support

The support page. This is the page where you can create a ticket that will reach support directly. To do that please click on the “Open a support ticket” button on the screen.



Support

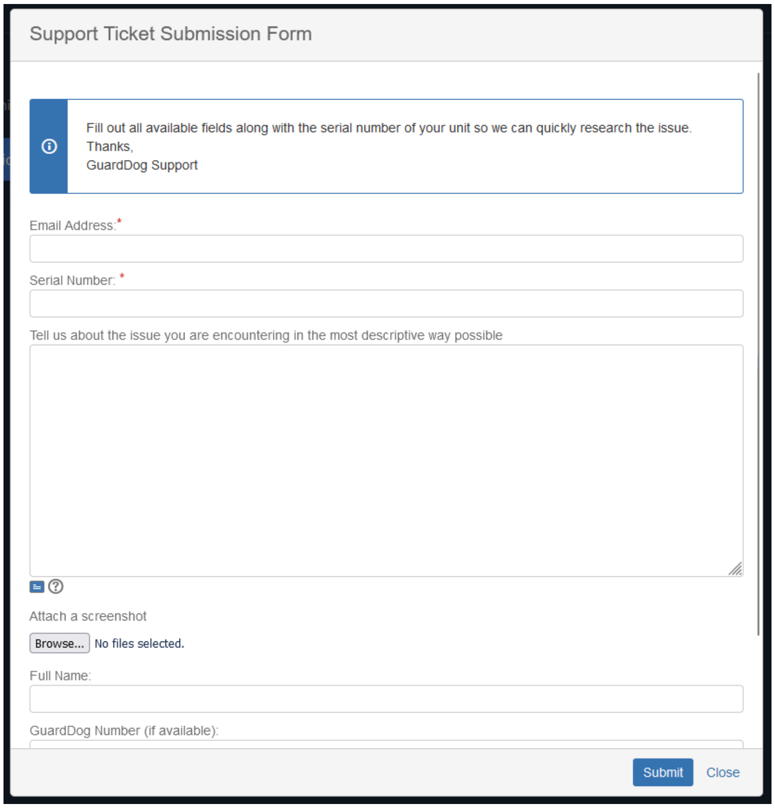
99+ Dan Prod

Support

Need help with anything? We are here to support you, just let us know:

Open a support Ticket

The support form. This form will open. Please fill out all fields and make sure to add as much information as possible about the incident this ticket is in reference to.



Support Ticket Submission Form

Fill out all available fields along with the serial number of your unit so we can quickly research the issue.
Thanks,
GuardDog Support

Email Address:*

Serial Number: *

Tell us about the issue you are encountering in the most descriptive way possible

Attach a screenshot

Browse... No files selected.

Full Name:

GuardDog Number (if available):

Submit Close

How do I…

… create an account?

Go to https://fido.guarddog.ai and click on Sign Up as shown at the beginning of this manual.

… choose a secure password?

When you are creating an account you will see on the screen the requirements for a secure password. Even when our minimum required is 8 characters we recommend at least 20 to make it real secure.

… log in to the portal?

Go to https://fido.guarddog.ai and enter the credentials for the account that has been previously created in the system.

… register my fido unit?

Login to https://fido.guarddog.ai and then go to Units > Add Units and select if you would like to add it by serial number or in bulk. Refer to this manual for steps on how to do it. You also have the option to use the QR code on the label that comes with the unit to register the unit on the system.

… find the serial number for it?

There are multiple places you will find this label. There are a few labels on the box that came with the unit and also on the bottom of the unit. The serial number and PIN are required to register the unit.

… protect my local network devices?

By default all devices that are visible, connected and discovered on the network where the units are plugged into are protected. You have the option to manually protect/unprotect these devices should you need to.

… make sure all devices are protected when the Protected Status on the local network says Unprotected?

In some cases when you manually change the protected status of the network devices and then change the time interval in Settings > Modules, you may see that not the entire network is protected. Change it back to the way you had it before and make sure you mark as protected the devices you want to protect. Once you do that you should be able to go back to the other time interval and see all protected.

… protect a wireless network?

This is an important step. By default, we do not protect any wireless networks unless you tell the system to do it. One way to do this is by going to Networks > Wireless Networks > Identified networks > Select the network to protect and click on the mac address of it. Done.

… change the time interval used to show data?

To do this go to Settings > Modules and then choose the desired time interval.

… show a table view on a screen?

There are many pages that are some using our default way of formatting the data on the screen by using cards. In pages like Units, attacks, threats, local networks, wireless networks and some other ones, you can click on the table icon on the top right corner of the main area on the screen and you can choose between card view or table view.

Steps

The steps described below are to launch attacks and detect them when a Fido unit is plugged into the network. In order to check that the same attacks can be executed successfully run through the same steps (9 onwards) without the Fido unit plugged in.

1. Get a Fido unit
2. Register for an account at https://fido.guarddog.ai
3. Login with your credentials.
4. Make sure you have internet access.
5. Make sure the port you plug the unit into has access to the internet and that it is configured to see all network traffic. This usually is accomplished by enabling port mirroring but it is not the only option.
6. Plug unit in to make sure the latest updates are downloaded. Allow for enough time for this to be completed (although it is usually done within minutes depending on the speed of the network, how busy it is and factoring in any congestion, giving it about 1h to 2h should be sufficient.)
7. Register the Fido unit in portal using the serial and pin provided with the Fido unit
   a. The unit can be registered and added to the account even before plugging in the unit
8. Once the unit is operational the 3 status icons in the Units card will show green
9. Make sure the unit is functional and data is being shown from the network that is plugged into
10. Go to the Networks page, then to Wireless and then to Identified wireless
11. Find your wireless network there and click on Protect.
12. Make sure to fill out all information on your Profile.
13. Enjoy your new Fido unit.