Phen-ai/CheckMate Training Guide

Powered by CCG

Training Guide

CCG

2024.09.12

Submitted by: **Canfield CyberDefense Group**
4110 Aspen Hill Rd. #300, Rockville, Maryland, 20853
Phone: 240-390-3978 | Fax: 301-570-6993
Email: info@cancgroup.com
https://www.phen-ai.com

Canfield CyberDefense Group is
Certified as a Woman Owned Small Business (WOSB), EDWOSB, SBA 8(a),
GSA IT 70 Schedule, Maryland registered MBE-DBE, VA-SWaM
ISO9001:2015
TS Facility Clearance

Security Category: Moderate

Release History

RELEASE	SOFTWARE VERSION	DATE	AUTHORS	DESCRIPTION
Initial Draft	1.7.0	02.01.2023	KT	Initial Content
Update	2	08.01.2023	KT	Content Update
Update	3.1	08.20.2023	KT	Content Update
Update	3.2	08.31.2023	KT	Reformed Layout
Update	9.24.1	07.27.2024	DF	Document Overhaul
Update	9.24.1	08.31.2024	DF	Content Update
Update	9.24.1	09.12.2024	RL	Formatting & Content Update

Table of Contents

1) Overview

This is a training document, where the user will get to know how to use the CanSecure platform. That this training document will only provide a brief description about the features, and NOT an in-depth description of every feature. In order to understand a feature in-depth, please read the user guide, which talks about each feature and their purpose in detail.

2) What to expect?

Users can expect to learn the basics of CanSecure, NeTERS, and Smart Log Analyzer for day-to-day monitoring with Phen-AI. This document will also include the references of the chapters from the user guide, and page number from user guide as necessary. This training module will NOT give in-depth information about features of CheckMate and/or Phen-AI. This training document will NOT provide information about trouble-shooting or any technical support. This document is only meant to give brief training to prepare users to use the product as a reviewer and not an administrator. To learn in-depth configurations and procedures, users are encouraged to refer to the user guide, and for troubleshooting please refer to administrator guide.

3) How to access CanSecure?

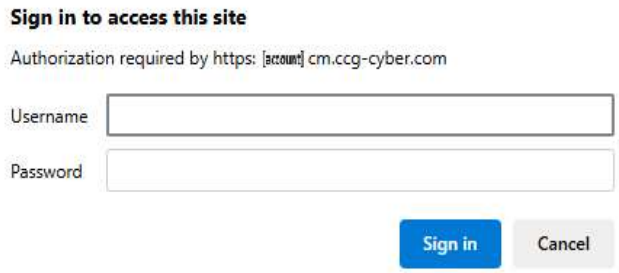
CanSecure is a web based interface that can be accessed through any internet connection. There are currently no local application or mobile applications for this product.

To access the CanSecure, your company will be given an account, from which, the employer has the control over how much access they want to give their employees. Each employee gets their unique username, from which they can access canSecure, and their username determines their limits to the network's security access.

This url is formatted the following way, https://[account].cm.ccg-cyber.com/ with [account] being the unique identifier for the company.

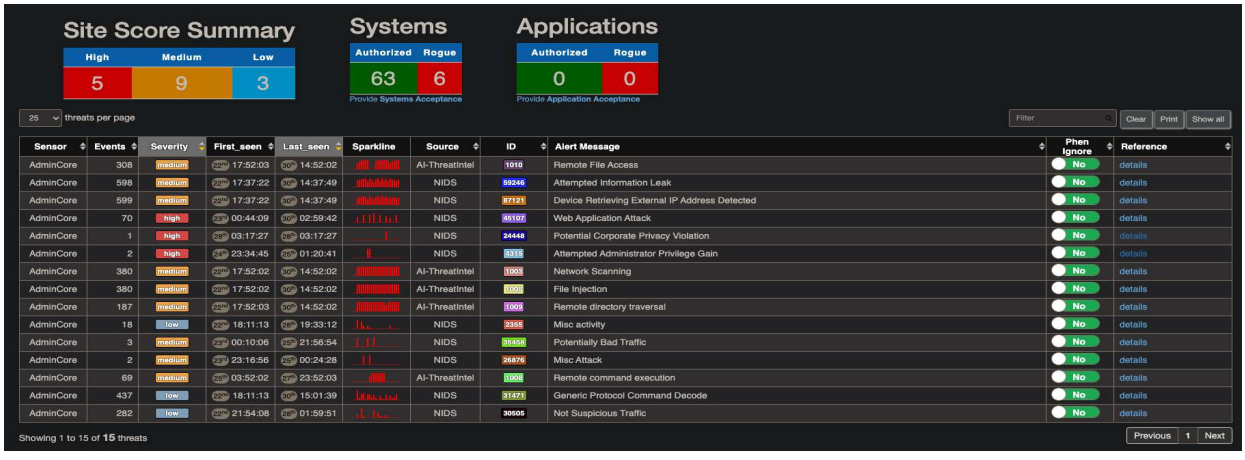
4. Chapter 1: CanSecure

4.1 Create profile and login



Once the URL given by the employer is entered, it will lead you to this popup window. Enter the username and password given to the employee to login. Note that every employee will have their own unique username and password, and password can be changed at any time.

Once logged in, the first things to observe will be the Site Score Summary, Systems, and Applications status. You can manage Application authorizations by clicking on the Applications, and Systems will let you manage Authorizations for Systems.



The main page will display a summary of the network activity. The main indexes to look out for here are first_seen, last_seen, Alert message and the devices that are ignored by Phen-AI, these devices will be indicated on the second from right index, where the user has all the control over the configuration of Phen-AI.

4.2 Password Change

4.2.1 Why change password?

The first thing to do once you receive your password from your employer, would be to change it for security purposes, treat it as a temporary password. Every company gets an admin account and all the other accounts (employee accounts) are child accounts. The employer has control over all distributed permissions of the child accounts. This password reset is not forced on a user so it must be done manually after logging in. When an administrator resets a users password it is recommended that they change it as Phen-AI will log all changes made and users do not want actions taken on their behalf.

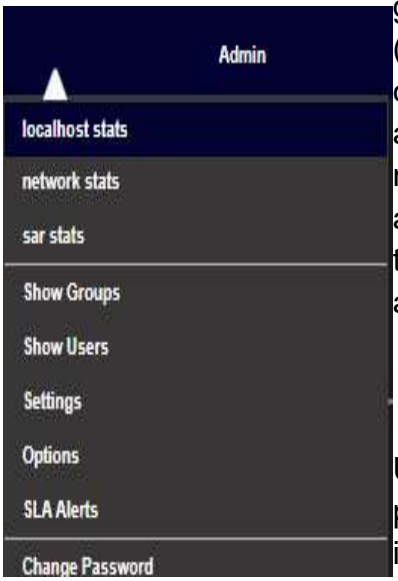
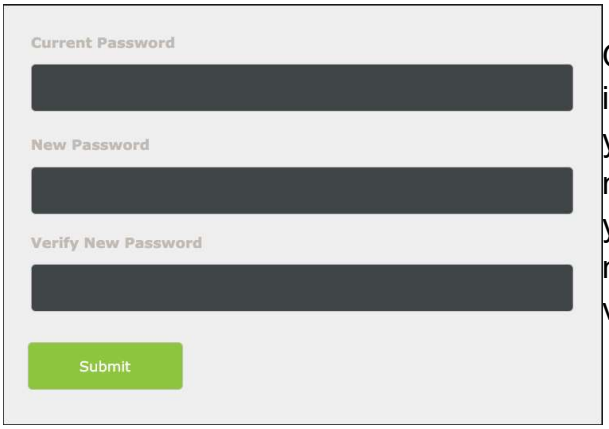


Figure 4.2.2 Change Password

4.2.2 How to change password?

Under the admin tab, there is an option that says change password, which will allow you to change your password. It is important to remember that this admin tab is **NOT** the same as the admin account of the company/corporation.

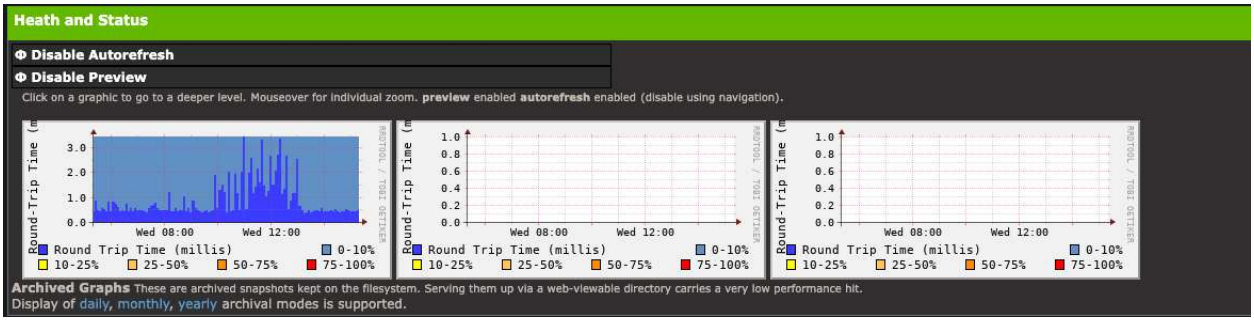
Note: This admin tab will appear in every account regardless of whether the account is an admin account or an Employee/child account. Please note that any changes made in employee accounts will **NOT** affect the admin account, but the admin account has the control over the permissions that the employee accounts get. Admin account has its own privileges which allows the admin account to override the permissions that employees have granted.



Once you click the change password option it will lead you to the following page where you can change your password. First you need to enter the password given to you by your employer and then you can create a new password in the next text field, and then verify your new password and click submit.

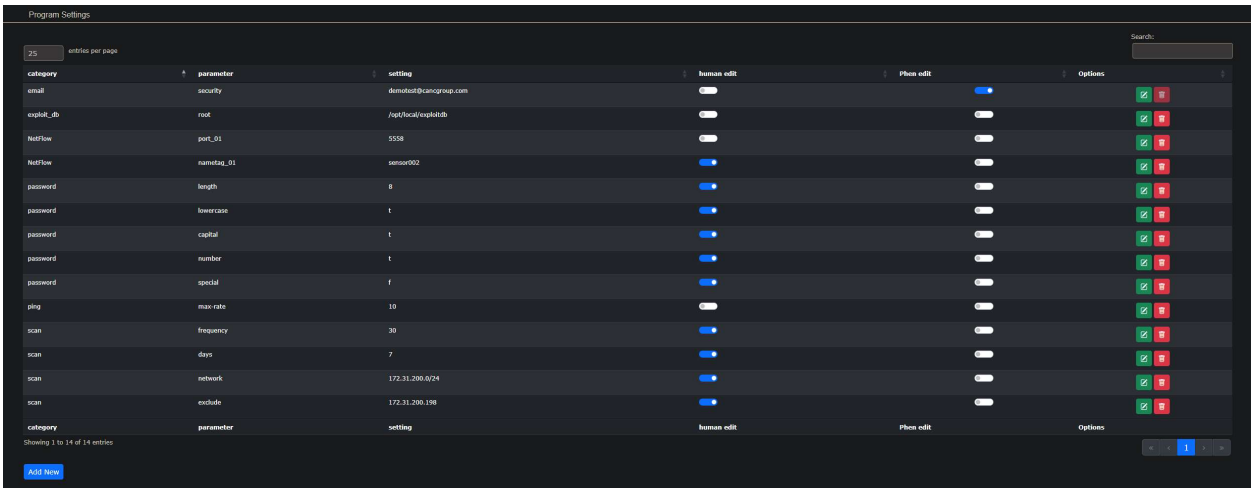
4.3 Health and Status

Under the Admin tab you will find the network stats which gives the health and status of the sensor(s).



It shows the sensor network condition daily, monthly and yearly. This will allow you to do trending on what the sensor is capturing.

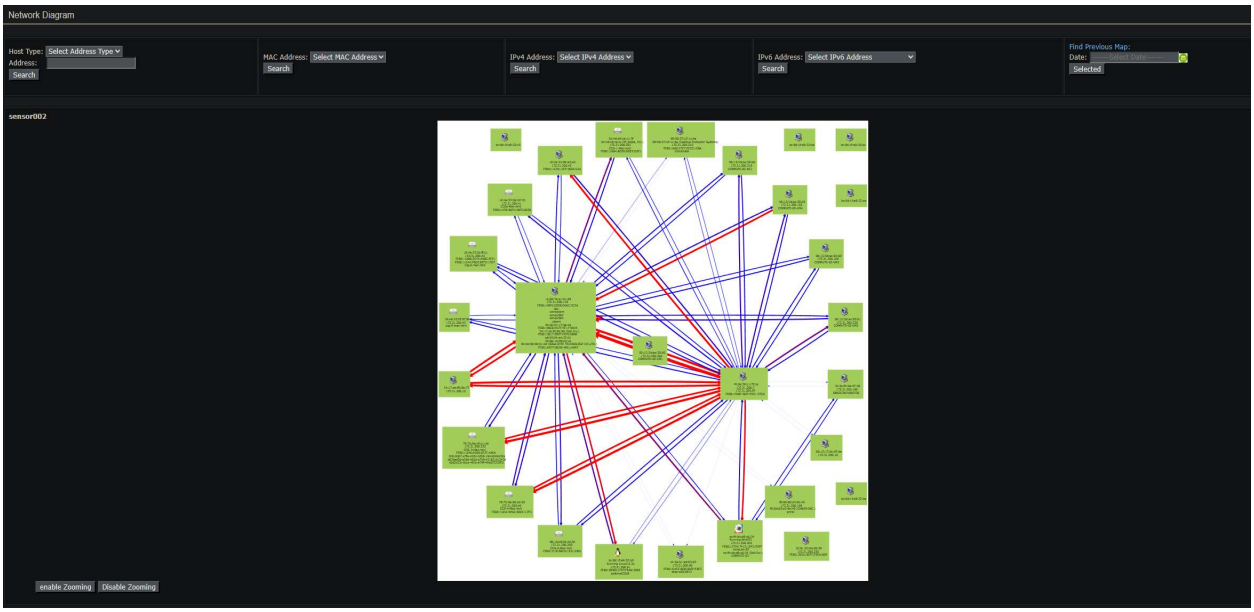
4.4 Settings



Click the admin tab and select settings, it lets you configure the permissions for Phen-AI. You can also create new settings by clicking “Add New”, and can provide Phen-AI with new instruction sets.

5. Chapter 2: NeTERS

5.1 Network Graph/Activities



This is a map of your entire network. You can visualize what Phen-AI has discovered and should be a representation of every connected device. Phen-AI will give the IP address, MAC address, and the hostname if it can resolve. Phen-AI will attempt to get the operating system type to give the image for windows/mac/cisco/linux or whatever the driving operating system might be.

5.2 HIDS (Host-Based Intrusion Detection System)

This page shows the list of processes interacting with your system to detect suspicious activity or unusual behaviors/patterns associated with humans or software. Each tab breaks down security domains of interest to keep the network secure.

6. Chapter 3: SmartLog Analyzer

6.1 Syslog

Syslog, system logging protocol, gives a visual demonstration of the network activity. Below is the vocabulary and their meaning:

Severity = Errors, warnings, notice, etc

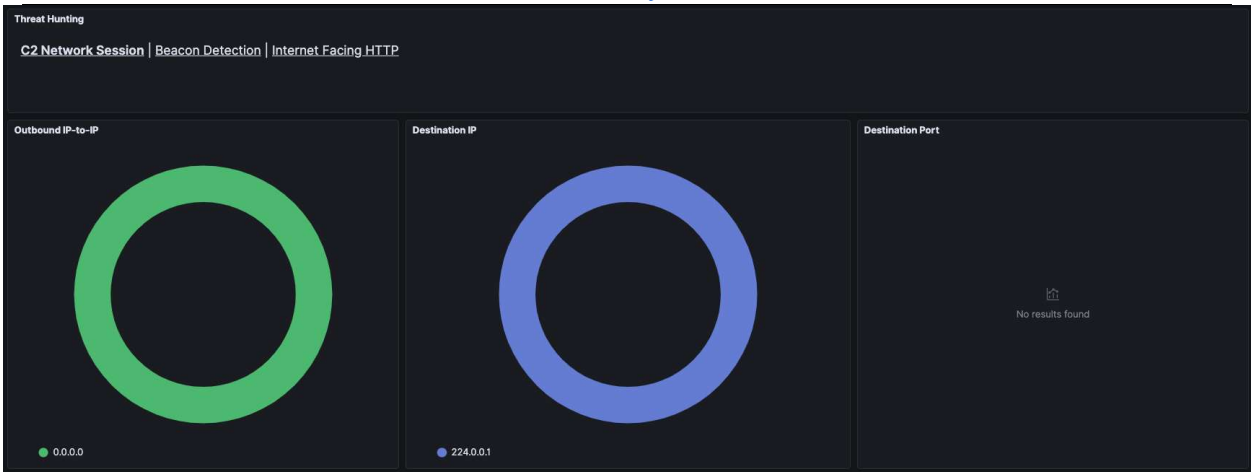
Nodes = devices

Processes = Software and services that run on the Nodes (devices)

Facilities = The programs that run in the background.

Phen-AI queries the log data every 10 seconds to keep information as up to date without causing congestion.

6.2 Threat Hunting



This page provides information about all the threats that Phen-AI sees. The sections are broken down to networking, beacons for port statistics, and HTTP traffic.

This provides information about Command and control networks, Beacon Detection, and the threats from the Internet facing HTTP. more information in depth can be found in the user guide, which talks about what each part and symbols symbolizes and what each graph represents. This too gets updated every 10 seconds with new data by Phen-AI.

7. Chapter 4: Customer dashboards

There are 4 customer dashboards that come preinstalled:

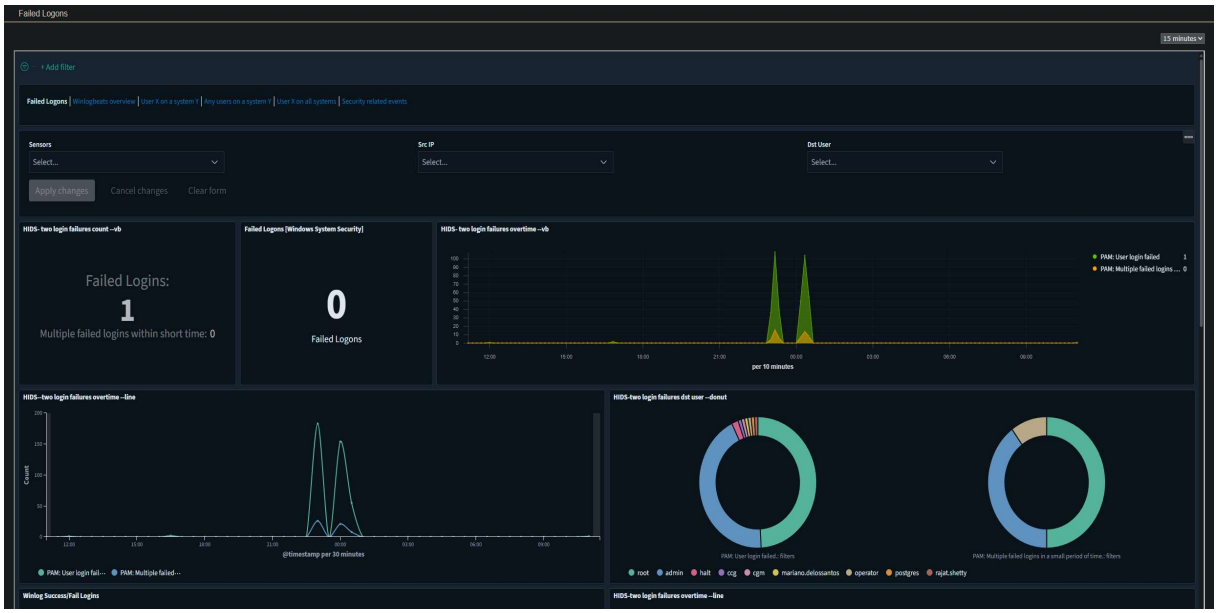
Failed Logins = Details on login information

PenTest scanner = results from the scans

Compliance dashboards = a list of industry compliances and the customer site score

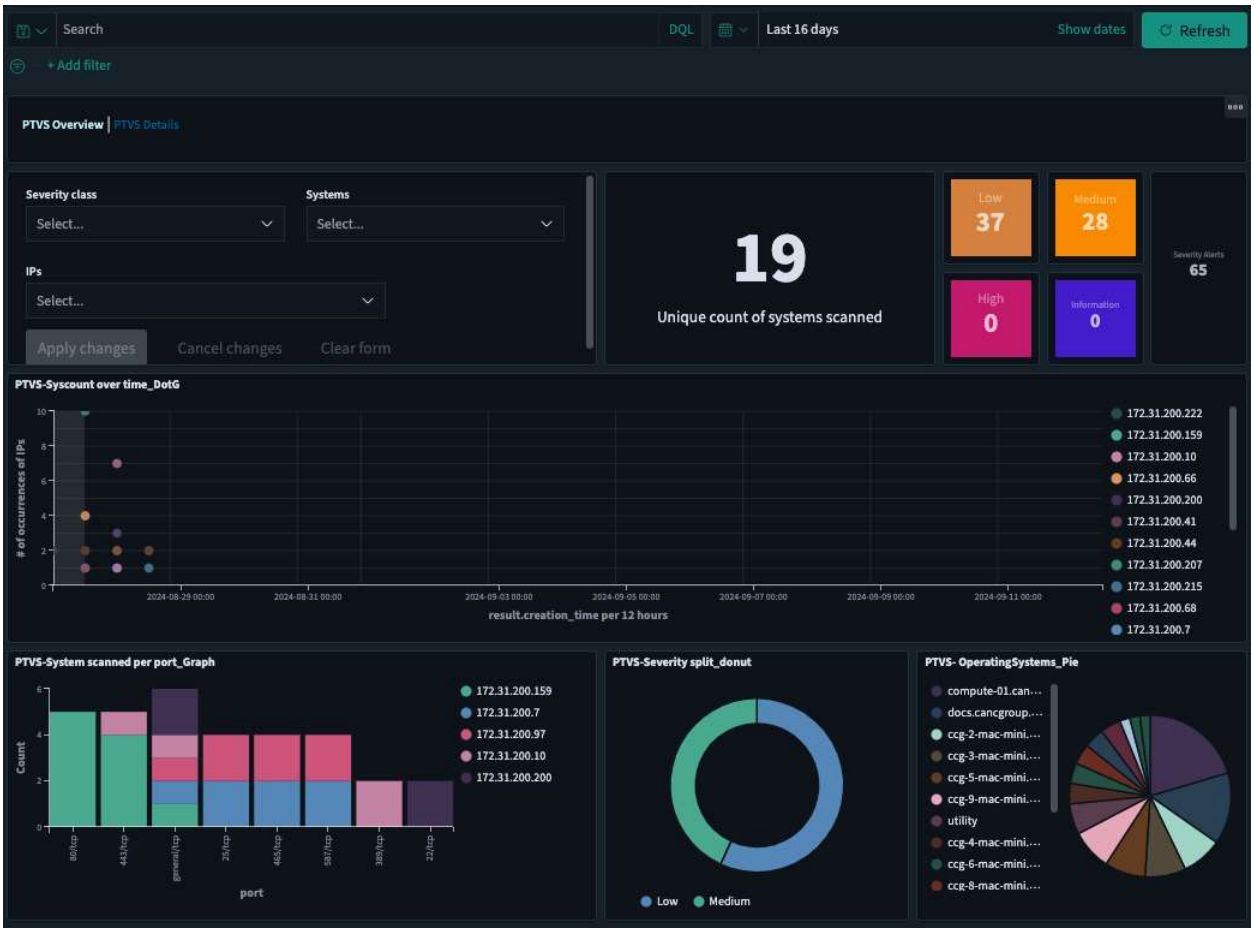
CVEs dashboard = a list of vulnerabilities that were detected and their fixes

7.1 Failed logins



On this dashboard you are able to see the successful and unsuccessful logins. It shows which device the login attempts were made and how many failures occurred in particular time-frames.

7.2 PenTest scanner



There are two tabs in the PenTest scanner dashboard giving a brief description of the scan results. On the overview tab you are able to see which IP addresses were scanned and which ports were found open.

The details tab shows information on the ports being used, severity of vulnerability on each system, frequency, and the associated IP for each one.

7.3 Compliance Dashboard

This dashboard gives tabs on the current industry regulations and how your network scores. Within each tab there are a set of rules that devices are scanned against to make sure the network stays within complaince.

7.4 CVEs Dashboard

The CVE dashboard shows devices with known vulnerabilities and the published fixes. Checkmate pulls data from multiple sources to make sure the operating systems and applications of devices on the network are secure by constantly checking for exploits and fixes.

Page intentionally left blank