CCG

Sensor Installation Guide

CCG

10.17.2024

support@cancgroup.com
4110 Aspen Hill Rd, Suite 300
Rockville, MD 20853
240.390.3978
https://www.phen-ai.com

Table of Contents

Canfield CyberDefense Group ©2024

support@cancgroup.com
4110 Aspen Hill Rd, Suite 300
Rockville, MD 20853
240.390.3978
https://www.phen-ai.com

Introduction

Your first step in getting the most from CCG's Cyber Protection will be to connect the CCG sensor into your company's network.

Using CCG's Cyber Protection with the sensor will allow your company to be protected. In choosing CheckMate, your company will be provided protections that identify and alert incoming and existing Cyber Threats to your company. Detection and protection technology covers (1) Network Traffic Monitoring, (2) an Intrusion Detection System (IDS), and (3) Insider Threats and Behavior analytics. You will get the coverage provided by CCG's patented Cyber Security Software: CheckMate and Phen®.

The focus of this document is to guide you through connecting the sensor. From that point, CCG's patented AI, Phen® will administer and manage your sensor to provide information to the AdminCore with the least impact on your network.

The Network Installation

The sensor plugs into a switch or router depending on the layout of the network. It must be connected into a device that can do port mirroring or spanning in order to investigate the traffic of the network. This will provide the capabilities of discovering insider threats, creating behavioural analytics, and meeting compliance coverage.

Sensor Installation

Plugging in the Sensor

Fig. 0.0.1: full front sensor image

Canfield CyberDefense Group ©2024

Fig. 0.0.2: close-up/actual sensor image

Note: *The purpose of the port labeled as "DATA" is to feed the data to the sensors from the network, in other words, DATA is inbound, and the port labelled as "MGMT", short for management, which is outbound, is to feed the data to adminCore from the sensor for further process (read outbound section).*

Plug in the Power and RJ-45 Cable wire into the Sensor.

1. Network **Data** SPAN/TAP port
    1. Plug the White dongle labeled "DATA" into the 3rd USB port from the top. The USB port is also labeled "DATA" (view image **Fig. 0.0.2**)
    2. Get the RJ-45/CAT5 network cable.
    3. Plug the one into the "DATA" labeled dongle on the Sensor.
    4. Plug the other end of the cable into your SPAN ported switch or gear.
2. Network **MGMT** port.
    1. Plug the RJ-45 cable from the "MGMT" port (above as Ethernet).

Canfield CyberDefense Group ©2024

support@cancgroup.com
4110 Aspen Hill Rd, Suite 300
Rockville, MD 20853
240.390.3978
https://www.phen-ai.com

2. Plug the other end into a switch.
3. The interface should be configured vi DHCP (from the pre-install guide).

3. Power
    1. The one end is plugged into the wall as normal.
    2. The other end of the cable is plugged into the "AC power" port on the bottom of the Sensor.
4. Video / Keyboard (optional, not recommended)
    1. Plug an HDMI cable into the "HDMI" labeled port on the side.
    2. Plug in a USB keyboard into the 4th USB port, below the "DATA" port.

Network Port Configurations

Port connections to and from the sensor. These connection are to and from one of the AdminCore systems only.

Inbound to the Sensor

Inbound port 22 allows Phen.AI® to connect and manage the sensor. This allows Phen.AI® to adjust application, performance, investigations, and depth.

• 22/tcp ← *AdminCore's IP* (Phen.AI's® interactions)

Outbound from the Sensor

The outbound connections are for data transfer of data, syslog and HIDS specific data. Also this allows for the regular updating of signatures for various software products.

- 22/tcp → *AdminCore's IP* (Phen.AI's® interactions)
- 514/udp, tcp → *AdminCore's IP* (Syslog Data)
- 1514/tcp → *AdminCore's IP* (HIDS Data)
- 5045/tcp → *AdminCore's IP* (IDS Data)
- 555x/udp, tcp → *AdminCore's IP* (Flow *Data)*
- 8140/tcp → *AdminCore's IP* (Phen.AI's® application / system configuration) **Enterprise Only**

Canfield CyberDefense Group ©2024