# Version Description Documentation

**Software Version: 9.24.1.6**

**November 2024**

Canfield CyberDefense Group ©2024

# Release History

| RELEASE | SOFTWARE VERSION | DATE | AUTHORS | DESCRIPTION | APPROVED BY |
|---|---|---|---|---|---|
| Final | 9.24.1.6 | November 21st, 2024 | RS | Final | RC |
| | | | | | |

# Table of Contents

# CHAPTER 1: DOCUMENT OVERVIEW

## 1.1 Introduction

This manual will provide an understanding of the software being delivered. Providing versions and verification sizes with checksums of each component.

## 1.2 Acronyms and Abbreviations

List of Acronyms and abbreviations with expansions used in this manual.

**Table 1-3: Acronyms and Abbreviations**

| ACRONYM | EXPANSION |
|---------|-----------|
| ATO | Authorization To Operate |

# CHAPTER 2: PRODUCT DESCRIPTION

## 2.1 Introduction

Canfield CyberDefense Group's (CCG) CheckMate software solution satisfies the ATO and will provide a complete solution with an automated deployment process that is required to meet the customer's analytic goals. CCG understands the mission is to provide a non-programmatic, non-scripted analytic platform that is not limited to a single optimized result.  The CheckMate automation capabilities will engage in sophisticated analytic tasks that will simplify a personal analyst's level of effort resulting in reduced cost and saving time.

The CheckMate system is installed and configured centrally located at the customer site.  The system is an analytic cloud environment that scales to customer needs.  All data is stored, processed, and displayed privately at the customer site. CheckMate allows for simultaneous processing and analysis by Phen-AI and analysts. The highest security and protection for the data are provided within CheckMate ensuring quality *Confidentiality, Integrity, and Availability* (CIA) and security protections.

## 2.2 Product Overview

**Table 2-3: File Verification**

| SOFTWARE NAME | SHA256 SUM | SIZE |
|---|---|---|
| pupmod-ccg-u-sensor | 95640b31ec3477aa8a9bda4169626a1d995094c3cf3eb7c34cd153452fc32deb | 67628 bytes |
| pupmod-ccg-u-ccg | 2ba22a7134f3ac34be4155d665b6ac13e1136cebf95bb4eda3864f37cbd4c57b | 1138676 bytes |
| pupmod-ccg-u-cansecure | 8a89fd11f6787b4ed06dbc79f930f1b18993a0e1008b8f2b0f01044a508b5d0c | 88352 bytes |
| **updates-9_24_1_6.zip** | **5878077347fc440b9ff0133da6654fdf455ce4c48c20951c92a37619dce9889f** | **1210895 bytes** |

# CHAPTER 3: PRODUCT PROVIDER CONTACT

## 3.1 Contact Information

**Table 3-2: Contact Information**

| WHO | ADDRESS |
| --- | --- |
| Rosy Canfield<br>President | rosy.canfield@cancgroup.com<br>410.707.2783 |
| Ray Canfield<br>VP, Technology Director | ray.canfield@cancgroup.com<br>240.390.3978, ext. 103 |
| Support | support@cancgroup.com<br>240.390.3978, ext. 101 |

# CHAPTER 4: VERSIONING SCHEMAS

## 4.1 Versioning Schema

**Table 4-2: Versioning Schema**

| NUMBER | DESCRIPTION |
|---|---|
| **Major** | Build number (9 currently) |
| **Minor** | Current Year (2024) |
| **Release** | An incremental number based on the month of the distribution.<br><br>• 1 == January<br><br>• 4 == April<br><br>• 7 == July<br><br>• 10 == October |
| **Patch** | Starts with 0 for a give Major/Minor release and is incremental for any required patches delivered during that release. |

# CHAPTER 5: DEPENDENCIES

## 5.1 Introduction

Here is a list of various software needed to install the Checkmate software.

**Table 5-2: Dependency Versioning**

| PRODUCT | VERSION |
|---|---|
| **Puppet** | 7.9.3-1 |
| **Oracle Linux** | 8.10 |

# CHAPTER 6: NEW COMPONENT LIST

## 6.1 New Components/Requirements

| Name | Vendor | Version |
|---|---|---|
| Oracle Enterprise Linux (OLE) | Oracle Corporation | 8.1 |
| OpenSearch | Amazon Web Services | 2.x |
| SIMP | Sicura | 7.9 |
| Wazuh | Wazuh | 4.0.1 |
| Suricata | OSIF | 6.0.x |
| Winlogbeat | Elastic | 8.x |
| VMWare (Player) | VMWare | 16 |
| Filebeat | Elastic | 7.x |
| zeek | Vern Paxson | 6.x |
| PostgreSQL | PostgreSQL GDG | 10 |

# CHAPTER 7: CORRECTIONS/FIXES

## 7.1 External Corrections (tickets)

None.

## 7.2 Product Corrections (tickets)

**Table 7-4: Product Tickets**

| ID | PROJECT | PRIORITY | SEVERITY | DATE SUBMITTED | DATE UPDATED | SUMMARY |
|----|---------|----------|----------|----------------|--------------|---------|
| 717 | ccg-pupmod | High | Major | 11/19/2024 | 11/21/2024 | Missing pupmod bits fixed |

## 7.3 Possible Problems and Known Errors

None

Canfield CyberDefense Group ©2024

# APPENDIX A: MANUAL INTRODUCTION

## A. 1 (U) Writing Conventions

(U) Appendix Table A- explains the writing conventions used in this manual.

**Appendix Table A-2: Writing Conventions**

| USAGE | STYLE | EXAMPLES / DESCRIPTIONS |
|---|---|---|
| All output | Courier New, 10 point | • The following message appears: `Do you want to monitor the shutdown from the console port?` |
| All Linux commands and users | Courier New, 11 point | • Use the `date` command to set or view the date and time for the system.<br>• Log on to the server as `root`. |
| All input | **Bold** | • Type **anonymous** in the User field.<br>• At the prompt, type **cd .. ; ls −lh** to move up one directory and display the contents in detail. |
| All menus, tabs, options, buttons, icons, and hardware switches | **Bold** | • Click the **System** icon and select **Options** from the menu. |
| All files, directories, and scripts | *Italicized* | • The */data* partition is denoted by */dev/md0*.<br>• View the */etc/raidtab* configuration file. |
| Names of all windows, screens, toolbars, and fields | Initial Capital Letters | • The System Maintenance window displays the Repair Options toolbar after the information is processed. |
| All abbreviations, acronyms, and system names | CAPITALIZED | • NT and UNIX-based workstations can remotely access the GLOBAL Viewer Service. |

| USAGE | STYLE | EXAMPLES / DESCRIPTIONS |
|---|---|---|
| All output | `Courier New, 10 point` | • The following message appears: `Do you want to monitor the shutdown from the console port?` |
| All keyboard keys | <In angle brackets> | • When complete, press <Enter>.<br>• To log off, press <Ctrl> + <Alt> + <Delete>.<br><br>    **NOTE:** Keys separated by a plus symbol are to be pressed simultaneously. Keys separated by a comma are to be pressed consecutively. Example: To check formatting, press <Ctrl> + <A>, <F9>. |
| Variable information | *<In Angle Brackets, Italicized, and with Initial Capital Letters>* | • The terminal displays: `Good morning,` *`<Name>`*`, today is` *`<Date>`*`.`<br>• At prompt, type the ***<User Name>***. |
| All referenced external documents | *Italicized and with Initial Capital Letters* | • Refer to the *System Hardware Manual* for information on running systems diagnostics. |
| Notes, cautions, and warnings | **NOTE:**, **CAUTION:**, and **WARNING:** are bold and in all capital letters | • Notes provide additional information.<br>• Cautions alert to potential damage to equipment, problems with the application, or issues with the system.<br>• Warnings alert to potential physical injury to personnel. |

**NOTE**: (U) More than one convention style can apply to a particular usage.

(U) Example: Type **`cd home/power`**.

The command **`cd home/power`** is in Courier New 11 point because it is a command and written in bold because it is input.

(U) Example: Verify the image by typing **`verify flash <File Name>`**.

The command **`verify flash <File Name>`** is in Courier New 11 point because it is a command and written in bold because it is input. **`<File Name>`** is also in brackets, italicized, and written with initial caps because it is a variable.