

Operator Guide



CCG

08.31.2024

Submitted by: **Canfield CyberDefense Group**
4110 Aspen Hill Rd Rockville, Maryland, 20853 #300
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

Release History

RELEASE	SOFTWARE VERSION	DATE	AUTHORS	DESCRIPTION
Initial Draft	1.7.0	07.01.2015	RwC	Initial Content
Update	8.30	07.23.2022	RwC	Content update
Update	8.4.0	09.14.2022	AJM	Content update
Update	8.5.0	10.01.2022	KT	Content update
Update	8.5.1	08.01.2023	KT	Images update
Update	8.5.2	08.11.2023	KT	Content added
Update	8.5.3	08.17.2023	KT	Content added
Update	8.6.0	09.21.2023	RB	Content added
Update	9.24.1	07.27.2024	DF	Document redone
Update	9.24.1	08.31.2024	DF	Content updated

Table of Contents

CheckMate.....	5
OVERVIEW.....	6
SITE SCORE SUMMARY.....	7
CHAPTER 1 OPERATION.....	11
1.1 INTRODUCTION.....	11
1.2 SYSTEM PURPOSE AND CAPABILITIES.....	11
1.3 CANSECURE PROCESS.....	11
1.3.1 Device Detection.....	12
1.3.2 Device Enumeration.....	12
1.3.3 Configuration of the PenTesting scanning software.....	12
1.3.4 Execution of the Pen-testing Software.....	12
1.3.5 Exploitation.....	12
1.3.6 Configuration.....	15
1.3.6.1 Network Scope.....	15
1.3.6.2 Scan Frequency.....	15
1.3.6.3 Observer.....	16
1.3.6.4 Starting a system.....	16
1.4 REPORTS.....	17
1.4.1 Reading of the Reports.....	19
1.5 NOTES.....	20
1.5.1 Creating notes.....	20
1.5.2 Managing Notes.....	20
1.6 OVERRIDES AND FALSE POSITIVES.....	20
1.6.1 What is a false positive?.....	20
1.6.2 Creating an Override.....	21
1.6.3 Automatic False Positives.....	21
CHAPTER 2 PROCESSING DETAILS.....	33
2.1.1.1 Filter Syntax.....	33
2.1.1.2 Unidirectional and/or Bidirectional.....	35
2.1.1.3 Saving Filters.....	35
2.1.1.4 Options.....	36
List Flows.....	36
CHAPTER 3 PROFILES.....	39
3.1 PROFILE TYPES.....	39
3.2 PROFILE CHANNELS.....	40
3.3 CREATING PROFILES.....	41
3.4 MANAGING PROFILES.....	42
3.5 CONVERTING PROFILES.....	42
CHAPTER 4 DETAIL GRAPHS.....	44
4.1.1.1 Example 1.....	44
CHAPTER 5 TOP PORT THREATS.....	45
5.1 HOW DATA IS COLLECTED.....	45

5.2 WHAT AND WHERE.....	45
CHAPTER 6 ALERTS.....	49
CHAPTER 7 SMART LOG ANALYZER.....	50
CONN.LOG.....	56
HTTP.LOG.....	58
DHCP.LOG.....	58
SMTP.LOG.....	58
SSL.LOG.....	58
SSH.LOG.....	58
Temporal Score Metrics.....	67
FAQ.....	71

CheckMate

OVERVIEW

CheckMate stands as CCG's premier cyber-defense security solution. This comprehensive system functions as an all-inclusive powerhouse, encompassing every essential element to effectively address 18 of the 20 SANS Critical Controls. At its core, CheckMate leverages the revolutionary Cyber Security artificial intelligence technology, "Phen.AI," firmly establishing its position as a provider of best in class technology.

By harnessing the advanced capabilities of Phen.AI, CheckMate employs an innovative Advanced Persistent Defense (APD) architecture. This strategic foundation ensures a proactive security approach, empowering organizations to actively anticipate evolving threats. A standout feature of CheckMate is its robust API, facilitating comprehensive scans of applications, devices, logs, and traffic, thereby providing real-time protection against the latest and most critical IT vulnerabilities. This all-encompassing solution not only guarantees cyber resilience but also does so with efficiency and cost-effectiveness, firmly establishing CheckMate as an indispensable asset in the cybersecurity landscape.

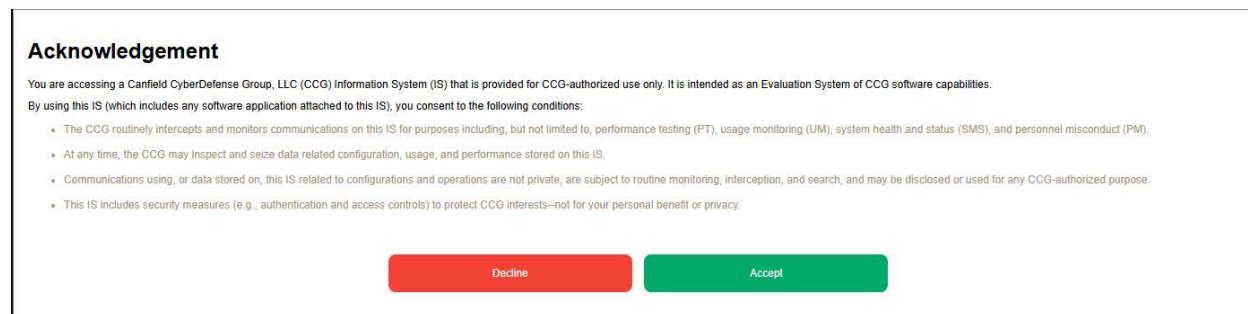


Figure: CheckMate User Login

The usage acceptance page when first logging into the CheckMate system.

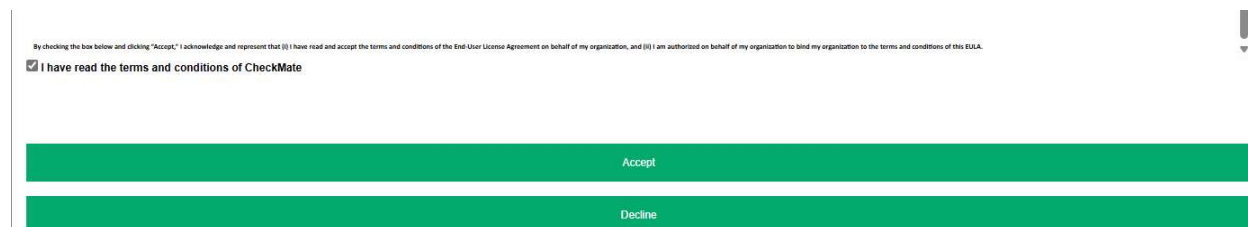


Figure: Terms and conditions

You must put a check to accept the terms and conditions in order for the accept button to appear. This is the last step before being able to access the CheckMate dashboard.

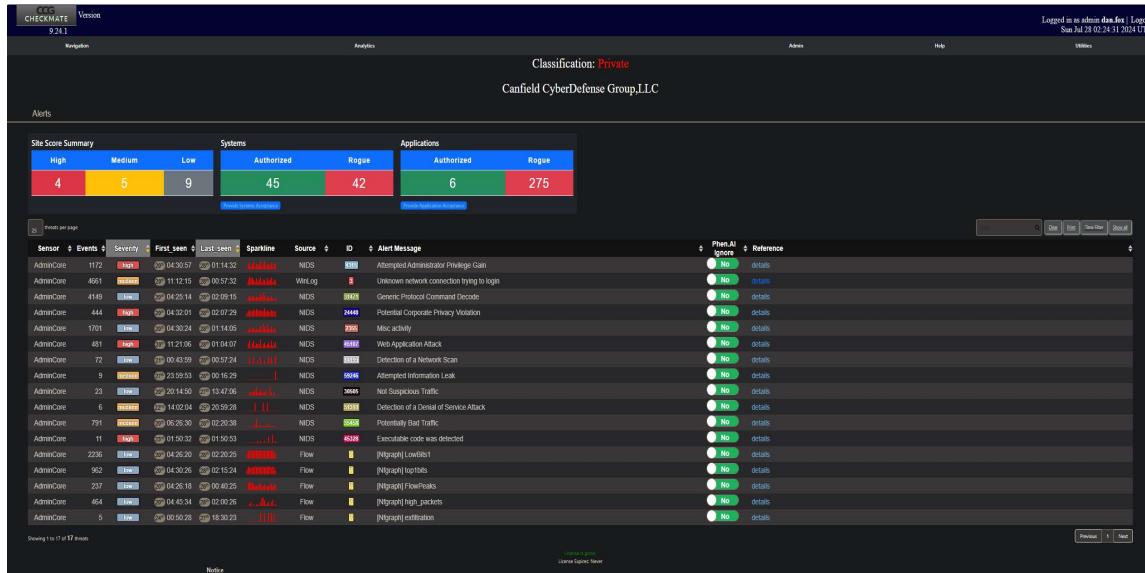
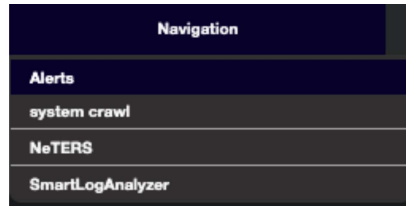


Figure: CheckMate Home Page

Above is the image of what users will see the first thing when they open CheckMate. This is Alert's page. To get to the alerts page from anywhere in the CheckMate, just hover-over to **Navigation > Alerts**



The Alert page is a summary of all the important things a user needs to know, using the table and special colors to indicate the severity of the alert, as well as CheckMate's ability to give it a score, helps user to decide which alert needs to be addressed first. Alert page creates a very easily readable and user friendly interface for user(s).

	This is the version of your CheckMate
	Displays the classification
	Shows who is logged in + time date and day + a button for logging out

SITE SCORE SUMMARY






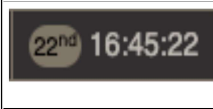






	Total number of high severity alerts.
--	--

<div style="background-color: #0056b3; color: white; padding: 2px; text-align: center; font-weight: bold;">Medium</div> <div style="background-color: #c4803d; color: white; padding: 10px; text-align: center; font-size: 24px; font-weight: bold;">0</div>	Total number of medium severity alerts.
<div style="background-color: #0070c0; color: white; padding: 2px; text-align: center; font-weight: bold;">Low</div> <div style="background-color: #666666; color: white; padding: 10px; text-align: center; font-size: 24px; font-weight: bold;">9</div>	Total number of low severity alerts.

SYSTEM

<div style="background-color: #0056b3; color: white; padding: 2px; text-align: center; font-weight: bold;">Authorized</div> <div style="background-color: #006400; color: white; padding: 10px; text-align: center; font-size: 24px; font-weight: bold;">0</div>	Total number of authorized devices on your network.
<div style="background-color: #0056b3; color: white; padding: 2px; text-align: center; font-weight: bold;">Rogue</div> <div style="background-color: #cc0000; color: white; padding: 10px; text-align: center; font-size: 24px; font-weight: bold;">0</div>	Total number of Unauthorized devices on your network.

APPLICATIONS

	<p>Indicates the total number of authorized applications running on network systems</p>
	<p>Indicates the total number of unauthorized applications running on network systems</p>
	<p>Represents the admin sensor</p>
	<p>Represents the number of events, in this row there were 35 events</p>
	<p>Indicates the severity is high.</p>
	<p>This indicates the time and 22nd is the date which means on 22nd at 16 hours – 45 minutes and 22 seconds – this could be either last seen or first seen, the label should be on the top row of the table</p>
	<p>Sparkline graph indicates how many times this error has appeared</p>
	<p>This is the source, whatever that is happening is coming from HIDS and you may want to go check HIDS logs(if you haven't given phen.ai the permission to take action). The HIDS logs will show the actual error</p>
	<p>This is an ID number, every Alert is given an ID number which should help you locate the error by its ID, every Alert will have its own and individual ID number.</p>
	<p>This is just an error message. This provides more information about the error.</p>
	<p>This toggle switch instructs Phen to ignore a particular event. When set to no, Phen will continue to monitor and increase the count of the detected event. When set to yes, Phen will no longer display the event but still monitor its occurrence.</p>
	<p>Details will take you to the source and will provide you with the logs and visualization of that alert.</p>

CanSecure

CHAPTER 1 OPERATION

1.1 INTRODUCTION

This chapter provides an overview of CanSecure, including purpose and capabilities, process and data flow, and prerequisites. It will also briefly cover a few of the product offerings.

1.2 SYSTEM PURPOSE AND CAPABILITIES

CanSecure utilizes various computer, internet, and web standards to verify and help IT staff secure devices. Many aspects of NIST standards include Security Content Automation Protocol (SCAP), Open Vulnerability and Assessment Language (OVAL), Common Vulnerabilities and Exposures (CVE), Common Platform Enumeration (CPE), CVSS. Also in use is MITRE ATT&CK, Open Web Application Security Project (OWASP), Continuous Asset Evaluation, Situational Awareness, and Scoring (CAESARS), as well as, NIST-800-37. CanSecure embraces Payment Card Industry Data Security Standard (PCI-DSS) v3.0, and Health Insurance Portability and Accountability (HIPAA) standards where applicable.

Hardware devices include Keyboard Video Mouse (KVM) switches, power management, Dell with RAC, Hewlett Packard (HP) with ILO, and generic computers running Linux or Windows, Virtual systems (VMware or Oracle VirtualBox), International Business Machines (IBM) Blade Centers, routers, switches, Wireless Access Points and Routers. OS software includes Microsoft Windows, MacOS X, Unix/Linux (RedHat & Debian), Cisco iOS, and Cisco NX-OS.

CanSecure gathers software vulnerabilities testing. It scans the various system devices, stores the collected data, compares the collected data to known vulnerability signatures, and then reports the state of those devices. In the final phase, Phen provides in-depth penetration testing of network devices. It will try exploiting the device with various security technologies.

CanSecure validation methods include:

- External Port examination.
- Internal application and patch status.
- Web vulnerabilities. Both known and fuzzing technologies.
- Database injection.
- Cross site scripting (XSS).

1.3 CANSECURE PROCESS

Phen manages various components of software through the following processes:

- Device Detection
- Device Enumeration
- Configuration of the Pentesting Scanning Software
- Execution of the Pentesting
- Exploitation.

1.3.1 DEVICE DETECTION

This is the process of looking at the network with passive and active components and tracking the addresses of active devices. Phen starts with active discovery and creates a passive digital network view to instantly detect new and changed systems and applications within the network.

1.3.2 DEVICE ENUMERATION

This is an Asset Inventory and Management (ITAM) process which revolves around creating a detailed, up-to-date inventory of all IT assets, which is leveraged to drive any IT-related decisions. Once the various devices have been identified, the next step includes the enumeration of hardware and software in use for each active device. Versions and types are detected and stored.

1.3.3 CONFIGURATION OF THE PENTESTING SCANNING SOFTWARE

In this phase, CanSecure uses the information acquired about each active device to add, update, or validate the configuration of all the software components required to perform vulnerability scans and pen-testing software. To manage them, Phen employs enumeration information as well as knowledge of the numerous scanning software components.

1.3.4 EXECUTION OF THE PEN-TESTING SOFTWARE

Initiate the various scanning software to provide the most full picture of the security posture of any given device. This process identifies vulnerabilities and tests reliable methods for detecting security threats in software.

1.3.5 EXPLOITATION

Upon getting the collection of possible device vulnerabilities, the CanSecure solution takes the next step to validate the various issues. The penetration at this point goes far enough to verify that the vulnerability exists. CanSecure will attempt to evaluate the security of an IT infrastructure by safely trying to exploit vulnerabilities including compromised servers, endpoints, web applications, wireless networks, network devices, mobile devices and other potential points of exposure.

QoD

QoD	QoD Type	Description
100%	exploit	The detection happened via an exploit and therefore is fully verified.
99%	remote_vul	Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerability.
98%	remote_app	Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.
97%	package	Authenticated package-based checks for Linux(oid) systems.

97%	registry	Authenticated registry-based checks for Windows systems.
95%	remote_active	Remote active checks (code execution, traversal attack, sql injection etc.) where the response shows the likely presence of the vulnerable application or of the vulnerability. "Likely" means that only rare circumstances are possible where the detection would be wrong.
80%	remote_banner	Remote banner check of applications that offer patch level in version. Many proprietary products do so.
80%	executable_version	Authenticated executable version checks for Linux(oid) or Windows systems where applications offer patch level in version.
75%		This value was assigned to any pre-QoD results during system migration. However, some NVTs eventually might own this value for some reason.
70%	remote_analysis	Remote checks that do some analysis but which are not always fully reliable.
50%	remote_probe	Remote checks where intermediate systems such as firewalls might pretend correct detection so that it is actually not clear whether the application itself answered. This can happen for example for non-TLS connections.
30%	remote_banner_unreliable	Remote banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to back port patches.
30%	executable_version_unreliable	Authenticated executable version checks for Linux(oid) systems where applications don't offer patch level in version identification.
1%	general_note	General note on potential vulnerability without finding any present application.

PEN TEST / SCANNER

Phen, the Cyber SME (subject matter expert) continually reviews the systems and scanning processes to improve performance and accuracy. This is the most efficient way to drive the scanning engine. While CanSecure will manage the entire scan process and everything else mentioned in this chapter, there are times and circumstances when a system security administrator may want to step in and resolve issues that might have been discovered.

This chapter explains how to set up and perform vulnerability scans and penetration testing on your systems. It begins with the basic steps and later sections cover detailed scan configurations and result analysis.

After the system scan is started, the progress can be monitored through the web GUI. The device being scanned will show results of each test along with details of each test performed.

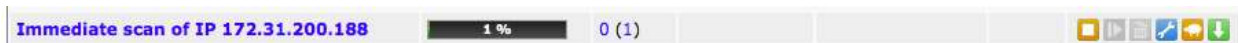



Fig. 6.2: After the start, the progress is displayed.

The colors and the fill level of the status bar give the current status of the scan. As soon as the scan is completed, the column 'Severity' notifies the criticality of the vulnerabilities found. The prior column 'Solution Type'  shows the type of solution available.













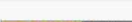



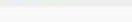

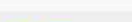

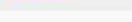

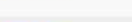








libpng vulnerability	 7.5 (High)	75%	172.31.200.17 (lazlohol-Gazelle-Professional.redrum.org.home)	general/libpng	
SMTP too long line	 7.5 (High)	75%	172.31.200.17 (lazlohol-Gazelle-Professional.redrum.org.home)	25/tcp (IANA: smtp)	
User Mountable NFS shares	 7.5 (High)	75%	172.31.200.17 (lazlohol-Gazelle-Professional.redrum.org.home)	2049/udp (IANA: nfs)	
SMTP antivirus scanner DoS	 7.2 (High)	75%	172.31.200.17 (lazlohol-Gazelle-Professional.redrum.org.home)	25/tcp (IANA: smtp)	
Mozilla Firefox Multiple Vulnerabilities Apr-09 (Linux)	 6.8 (Medium)	75%	172.31.200.17 (lazlohol-Gazelle-Professional.redrum.org.home)	general/tcp	
Adobe Flash Player Multiple Security Bypass Vulnerabilities - 01 Feb14 (Linux)	 6.4 (Medium)	75%	172.31.200.17 (lazlohol-Gazelle-Professional.redrum.org.home)	general/tcp	
Firefox URL Spoofing And Phising Vulnerability (Linux)	 5.8 (Medium)	75%	172.31.200.17 (lazlohol-Gazelle-Professional.redrum.org.home)	general/tcp	
Mozilla Firefox SOCKS5 Proxy Server DoS Vulnerability Aug-09 (Linux)	 5.0 (Medium)	75%	172.31.200.17 (lazlohol-Gazelle-Professional.redrum.org.home)	general/tcp	
libpng pngwutil.c NULL pointer Vulnerability	 5.0 (Medium)	75%	172.31.200.17 (lazlohol-Gazelle-Professional.redrum.org.home)	general/tcp	
Mozilla Firefox 'window.print()' Denial Of Service Vulnerability (Linux)	 5.0 (Medium)	75%	172.31.200.17 (lazlohol-Gazelle-Professional.redrum.org.home)	general/tcp	
Check if Mailserver answer to VRFY and EXPN requests	 5.0 (Medium)	99%	172.31.200.17 (lazlohol-Gazelle-Professional.redrum.org.home)	25/tcp (IANA: smtp)	
Oracle VM VirtualBox Unspecified Vulnerability-03 Aug2014 (Linux)	 4.4 (Medium)	75%	172.31.200.17 (lazlohol-Gazelle-Professional.redrum.org.home)	general/tcp	


Fig. 6.3: The results are already available before the scan is completed.

The system can be managed via the actions in the right column:

-  Starting a currently not running system.
-  Stopping a currently running system. All discovered results will be written to the database.
-  Resuming a stopped system.
-  Moving a system to the trash.
-  Editing a system.
-  Cloning of a system.
-  Exporting a system as xml object. The object can be imported again to another CanSecure appliance.

Even before the scan is completed the results can be viewed (see figure 6.3) by clicking on the progress bar. The results being displayed are not complete yet. Progress can continue to be monitored at the top right via the progress bar. This page does **not** reload automatically.

In order to obtain different representations of the results, you can move the mouse over the title bar. It opens a pull-down menu where you can choose different representation formats





The report can be exported in various different formats as well. The export formats are selected in the title bar as well. Afterwards the report can be downloaded by clicking the  button. Reports and report formats are discussed in more detail in section *Reports*.

1.3.6 CONFIGURATION

The configuration of the scan parameters are all handled by Phen.

1.3.6.1 NETWORK SCOPE

The first step is to define the network(s) that Phen is responsible for. Click the “Admin” tab and select “settings” to define the settings in checkmate.

category	parameter	setting	human edit	Phen edit	Options
email	security	demotest@canigroup.com	<input type="checkbox"/>	<input checked="" type="checkbox"/>	 
exploit_db	root	/opt/local/exploitdb	<input type="checkbox"/>	<input type="checkbox"/>	 

1.3.6.2 SCAN FREQUENCY

Next is the configuration of the frequency to scan each system. CanSecure has been designed to allow Phen to drive the scanner to perform daily scans. If no entry is made then Phen will schedule systems every 24 hours from its installation.

scan	frequency	30	<input checked="" type="checkbox"/>	<input type="checkbox"/>	 

Phen will investigate the network(s) and identify all devices in the network it has been given access to. After identifying all of the devices and their configurations, Phen uses this and other knowledge about the environment to monitor all of the devices.

If applications run on unusual ports, they should be monitored and tested with CanSecure. The default port lists should be verified under *Configuration* submenu *Port Lists*, NOTE: this default list can't be modified. If necessary, create your own list that includes your ports if they are custom.

- **Alive Test** Should the scan check if a target (Targets) is reachable. Options are:
 - ICMP Ping
 - TCP Service Ping
 - ARP Ping
 - ICMP & TCP Service Ping
 - ICMP & ARP Ping
 - TCP Service & ARP Ping
 - ICMP, TCP Service & ARP Ping

Devices must be configured to allow ICMP traffic or you can get misleading results. In some environments routers and firewall systems respond to a TCP Service Ping with a TCP-RST even though the host is actually not alive. This is another area the IA will identify and resolve problems by running the scanner.

- **SSH Credential** Selection of a user that can log into the target system of a scan if it is a Linux or UNIX system. This allows for an *Authorized Scan* (see section *Authenticated Scan*).
- **SMB Credential** Selection of a user that can log into the target system of a scan if it is a Microsoft Windows system. This allows for an *Authorized Scan* (see section *Authenticated Scan*).
- **ESXi Credential** Selection of a user that can log into the target system of a scan if it is a VMWare ESXi system. This allows for an *Authorized Scan* (see section *Authenticated Scan*).

1.3.6.3 **OBSERVER**








Once Phen creates the system and it is saved it will be displayed in the system overview.

After logging in the user can see those systems and can access the respective reports.

1.3.6.4 **STARTING A SYSTEM**

Phen has already selected the schedule for each device. Once a system is saved it will be displayed next.

The system can be managed via the action icons in the title bar:

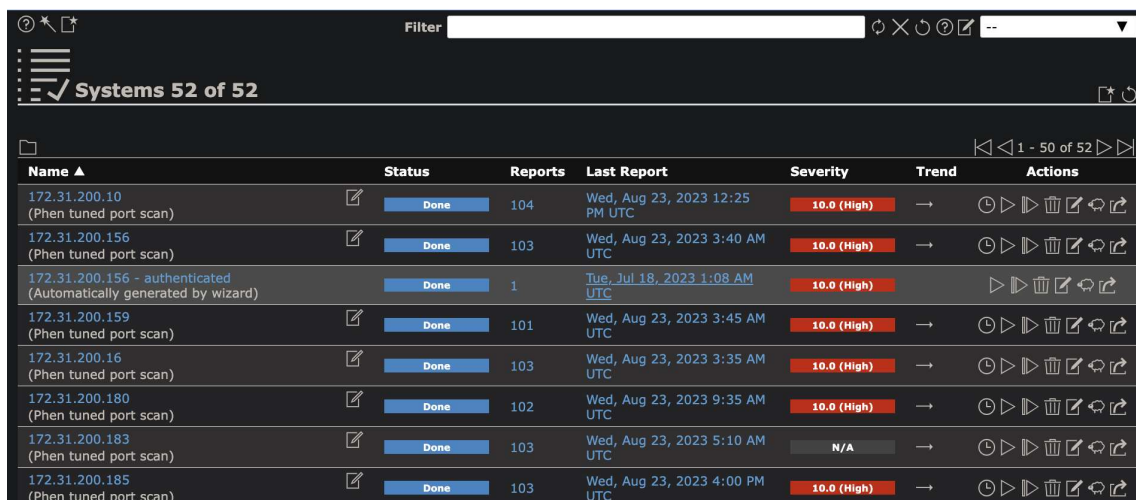
-  Starting of a currently not running system.
-  Stopping of a currently running system. All discovered results will be written to the database.
-  Resuming a stopped system.
-  Moving of a system to the trashcan.
-  Editing of a system.
-  Cloning of a system.
-  Exporting of a system as xml object. The object can be imported again on another CanSecure appliance.

Alternatively starting a system can be performed via the overview page that can be accessed by selecting *Scan Management* and then *systems* (see figure *The control of the system is performed in the right column of the overview.*).

The status bar shows information about the status of a scan. The following colors and states are possible:

- The system has not been run since it was created.
- The system is currently running and is partially completed. The information is based on the number of NVTs executed on the selected hosts. For this reason the information does not necessarily correlate with the time spent.
- The system was just started. CanSecure is preparing the scan.

- The system was deleted. The actual deletion process can take some time as reports need to be deleted as well.
- The system was stopped recently. However, the scan engine has not reacted respectively yet.
- The last scan was stopped by the user prematurely. The latest report is possibly not yet complete. Other reasons for this status could be the reboot of CanSecure or a power outage. After restarting the scanner the system will be resumed automatically.



Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
172.31.200.10 (Phen tuned port scan)	Done	104	Wed, Aug 23, 2023 12:25 PM UTC	10.0 (High)	→	⏸️ ⏪ ⏩ 🗑️ 📄 🔄
172.31.200.156 (Phen tuned port scan)	Done	103	Wed, Aug 23, 2023 3:40 AM UTC	10.0 (High)	→	⏸️ ⏪ ⏩ 🗑️ 📄 🔄
172.31.200.156 - authenticated (Automatically generated by wizard)	Done	1	Tue, Jul 18, 2023 1:08 AM UTC	10.0 (High)	→	⏸️ ⏪ ⏩ 🗑️ 📄 🔄
172.31.200.159 (Phen tuned port scan)	Done	101	Wed, Aug 23, 2023 3:45 AM UTC	10.0 (High)	→	⏸️ ⏪ ⏩ 🗑️ 📄 🔄
172.31.200.16 (Phen tuned port scan)	Done	103	Wed, Aug 23, 2023 3:35 AM UTC	10.0 (High)	→	⏸️ ⏪ ⏩ 🗑️ 📄 🔄
172.31.200.180 (Phen tuned port scan)	Done	102	Wed, Aug 23, 2023 9:35 AM UTC	10.0 (High)	→	⏸️ ⏪ ⏩ 🗑️ 📄 🔄
172.31.200.183 (Phen tuned port scan)	Done	103	Wed, Aug 23, 2023 5:10 AM UTC	N/A	→	⏸️ ⏪ ⏩ 🗑️ 📄 🔄
172.31.200.185 (Phen tuned port scan)	Done	103	Wed, Aug 23, 2023 4:00 PM UTC	10.0 (High)	→	⏸️ ⏪ ⏩ 🗑️ 📄 🔄

Fig6.18: The control of the system is performed in the right column of the overview

- An error has occurred. The latest report is possibly not yet complete or is missing completely.
- The system has been completed successfully.
- The system is a container system.

1.4 REPORTS

The results of a scan are summarized in a report. Reports can be viewed with a browser and downloaded from the appliance in different formats. Once a scan has been started the report of the results found so far, can be viewed. Once a scan is complete its status changed to Done. From now on no additional results will get added. For more information on reports please refer to the Reports chapter as well.

The report summary gives a quick overview over the current state. It shows if a scan is complete and how many vulnerabilities have already been found. From the summary a report can be downloaded directly in many different formats. The following formats are supported (see also section *Report Plugins*)

- **ARF: Asset Reporting Format v1.0.0** This format creates a report that represents the NIST Asset Reporting Format.
- **CPE – Common Enumeration CSV Table** This report selects allCPE tables and creates a single comma separated file.
- **CSV hosts** This report creates a comma separated file containing the systems discovered.
- **CSV Results** This report creates a comma separated file with the results of a scan.
- **PDF – Security Report (recommended)** This is the complete Security report with all vulnerabilities.
- **GXR PDF – Executive Report (recommended)** This is a shortened report for management.
- **HTML** This report is in HTML format.
- **ITG – IT-Grundschutz catalog** This report is guided by the BSI IT-Grundschutz catalog.
- **LaTeX** This report is offered as LaTeX source text.
- **NBE** This is the old OpenVAS/Nessus report format.

Since a report often contains a lot of findings, the complete report as well as only filtered results can be viewed and downloaded. In the default setting only the High and Medium risks are being displayed. This can be changed very easily. In the Filtered Results section shows the filtered results. As long as the scan is still running can cause rearrangements here.

To interpret the results please note the following information:

- False Positives

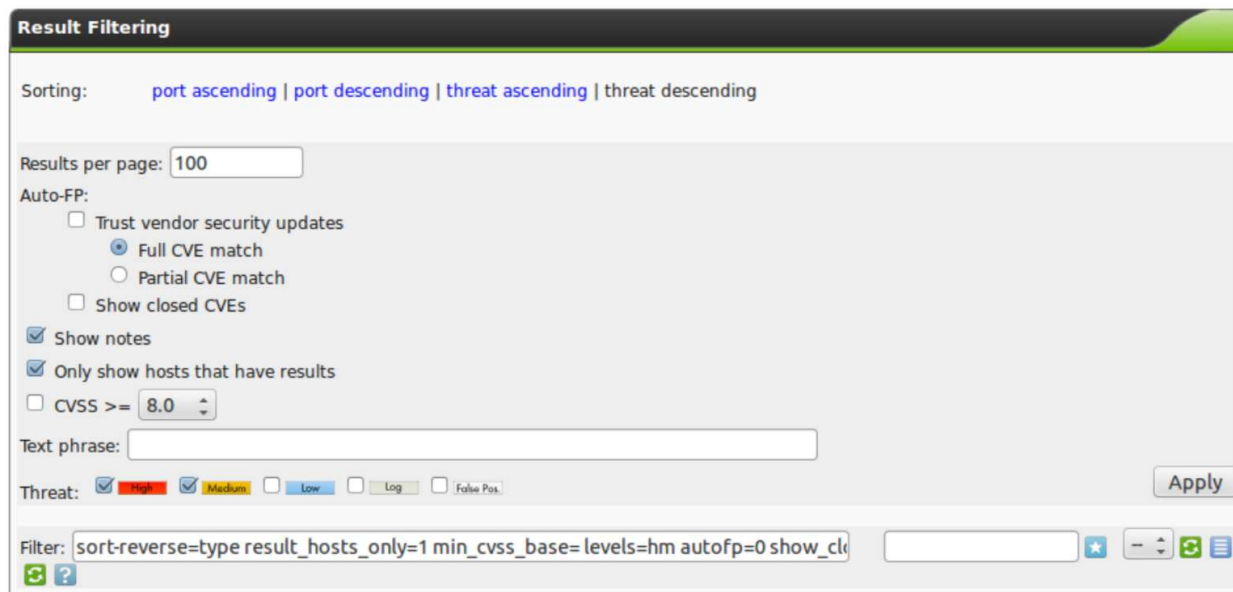


Fig. 6.22: Report Filtering.

A false positive is a finding that describes a problem that does not exist in reality. Vulnerability scanners often find evidence that point at a vulnerability. However, a final judgment cannot be made. There are two options available:

- Reporting of a potentially nonexistent vulnerability (False Positive).
- Ignoring reporting of a potentially existing vulnerability (False Negative).

Since a user can identify, manage and as such deal with false positives compared to false negatives, CanSecure Vulnerability scanner and pentest reports all potentially existing vulnerabilities. It is the user's responsibility to categorize them.

This problem is very common with Enterprise Linux distributions. If, for example, a SSH service in version 4.4 is installed and the software reports this version during a connection attempt, a vulnerability scanner, that knows of a vulnerability in this version, will report this as such. The vendor potentially already addressed the vulnerability and released version 4.4-p1 that is already installed. This version still reports to the outside version 4.4 so that the vulnerability scanner cannot differentiate. If the user knows of this circumstance an Override can be configured (see section *Overrides and False Positives*). The AutoFP function (see section *Automatic False Positives*) can assist here as well.

- Multiple findings can have the same cause. If an especially old software package is installed, often multiple vulnerabilities exist. Each of these vulnerabilities is tested by an individual plugin and causes an alert. The installation of a current package will then remove a lot of vulnerabilities at once.
- Important are findings of the levels High High and Medium Medium. Address these findings in order of priority. Before addressing medium level findings, high level findings should get

addressed. Only in exceptional cases, when it is known that the high alerts need to be less considered (because the service cannot be reached through the firewall) should this approach be deviated from.

- Low **Low** and Log **Log** are mostly interesting for detailed understanding. This is why these findings are filtered out by default. These findings can hold very interesting information however and considering them will increase the security of your network and systems. For their understanding often a deeper knowledge of the applications is required. Typical for an alert at the log level is that a service uses a banner with its name and version number. This could be useful for an attacker during an attack if this version has a known vulnerability.
- To simplify the remediation of vulnerabilities every alert offers a solution for problems directly. In most cases it will be referred to the latest vendor software package. In some cases a configuration change will be mentioned.
- References explain the vulnerabilities further. Even though the alerts contain a lot of information external references are always listed. These refer to web sites on which the vulnerability was already discussed. Additional background information is available such as who discovered the vulnerability, what effects it could have and how the vulnerability can be remediated.

1.4.1 READING OF THE REPORTS





The report contains a list of all of the vulnerabilities detected by CanSecure (see figure *List of discovered vulnerabilities*)



Vulnerability	Severity	QoD	Host	Location	Actions
ProFTPD Server SQL Injection Vulnerability	7.5 (High)	75%	192.168.155.200	21/tcp	[Icons]
phpMyAdmin Configuration File PHP Code Injection Vulnerability	7.5 (High)	75%	192.168.155.200	80/tcp	[Icons]
PHP-CGI-based setups vulnerability when parsing query string parameters from php files.	7.5 (High)	75%	192.168.155.200	80/tcp	[Icons]
phpinfo() output accessible	7.5 (High)	75%	192.168.155.200	80/tcp	[Icons]
PHP Remote Code Execution and Denial of Service Vulnerabilities Dec13	7.5 (High)	75%	192.168.155.200	80/tcp	[Icons]
PHP Multiple Buffer Overflow Vulnerabilities - Jan15	7.5 (High)	75%	192.168.155.200	80/tcp	[Icons]
PHP Multiple Double Free Vulnerabilities - Jan15	7.5 (High)	75%	192.168.155.200	80/tcp	[Icons]

Fig. 6.23: List of discovered vulnerabilities

To support the administrator with the analysis of the results the severity of a vulnerability (CVSS, see also section CVSS) is displayed directly as a bar.

To point the administrator to a simple solution the column Solution-Type  displays the existence of a solution. The column will display if a vendor patch  exists or a workaround  is available. It will also be displayed if no solution for a vulnerability exists . If the column of the respective vulnerability still appears empty then the respective NVT has not been updated yet.

The column Quality of Detection (QoD) provides information in regards to the reliability of the successful detection of a vulnerability. This assessment is implemented into all existing NVTs step by step (see section *Network Vulnerability Tests*). This column allows to be filtered as well. By default only NVTs with a QoD of 70% are displayed. Vulnerabilities with a lower reliability of detection are not displayed in the report. The possibility of false positives is thereby lower.

In the respective vulnerability view, additional, more detailed information is available.

1.5 NOTES

Notes allow adding comments to a Network Vulnerability Test (NVT). They will also be displayed in the reports. A Note can be added to a specific result, a specific system, a risk level, port or host and as such will only appear in specific reports. A Note can be generalized just as well so that it will be displayed in all reports.

1.5.1 CREATING NOTES

To create a new note select the finding in the report you want to add a note to and click *New Note* . Alternatively you can create a note without relation to a finding. However, CanSecure cannot suggest any meaningful values for the different fields in the following dialogue.

A new window opens in which exactly those criteria of the selected vulnerability are preset.

Individual values can be selected and deselected to generalize or the note even further or make it more specific. Additionally the note can be activated for a specific period of time. This allows adding of information to a note that a security update is uploaded in the next seven days. For the next seven days the note will be displayed in the report that the vulnerability is being worked on.

1.5.2 MANAGING NOTES

The created notes can be displayed under *Scan Management* and *Notes*. Here completely new notes can be added as well. Among others it is being displayed if created notes are currently active. Additionally notes can be edited. To search for a specific note a search filter can be used respectively. This will make it easier to find a specific note when especially a great deal of notes is available. The search filter can be opened respectively and text entered appropriately or it can be entered directly into the filter window at the top. These filters can, of course, be saved for later use as well.

1.6 OVERRIDES AND FALSE POSITIVES

The results of a report can not only be supplemented through meaningful or helpful data but the severity of the results can be modified. This is called Override by CanSecure. These overrides are especially useful to manage results that are discovered as a false positive and that have been given a critical severity but should be given a different severity (i.e. False Positive) in the future. The same is true for results that only have been given the severity Log but should be assigned a higher severity locally. These can be managed with an override as well. The use of overrides makes also sense to manage acceptable risks. The risk of a vulnerability can be ranked new and as such the risks that, in your opinion, are not critical can be re-evaluated in the results.

1.6.1 WHAT IS A FALSE POSITIVE?

A false positive is a result that describes a problem that does not exist in reality. Often vulnerability scanners find proof that point to a security issue. A final prediction is not possible, however. Two options are now available:

- Reporting of a potentially non-existent vulnerability (False Positive).
- Omission of the reporting of the potentially existing vulnerability (False Negative).

Since a user is able to recognize, manage and handle these as it is not the case with false negatives, CanSecure vulnerability scanner reports all potentially existing vulnerabilities. It is the responsibility of the user to organize them.

Note: Consider the new concept of Quality of Detection (see sections *Reading of the Reports* and

Network Vulnerability Tests).

This problem is especially typical with Enterprise Linux distributions. If, for example, a SSH service in version 4.4 is installed and the software reports this version during a connection attempt, a vulnerability scanner, that knows of a vulnerability in this version, will report this as such. The vendor potentially already addressed the vulnerability and released version 4.4-p1 that is already installed. This version still reports to the outside version 4.4 so that the vulnerability scanner cannot differentiate. If the scan administrator knows of this circumstance an override can ensure that these results are no longer being displayed.

1.6.2 CREATING AN OVERRIDE

Overrides like notes can be created in different ways. The simplest way to get to this option is through the respective scan result in a report. At the top right of each finding the *Add Override* icon can be found.

Overrides have the same function as notes, however, they add the possibility to adjust the severity:

- High
- Medium
- Low
- Log
- False Positive

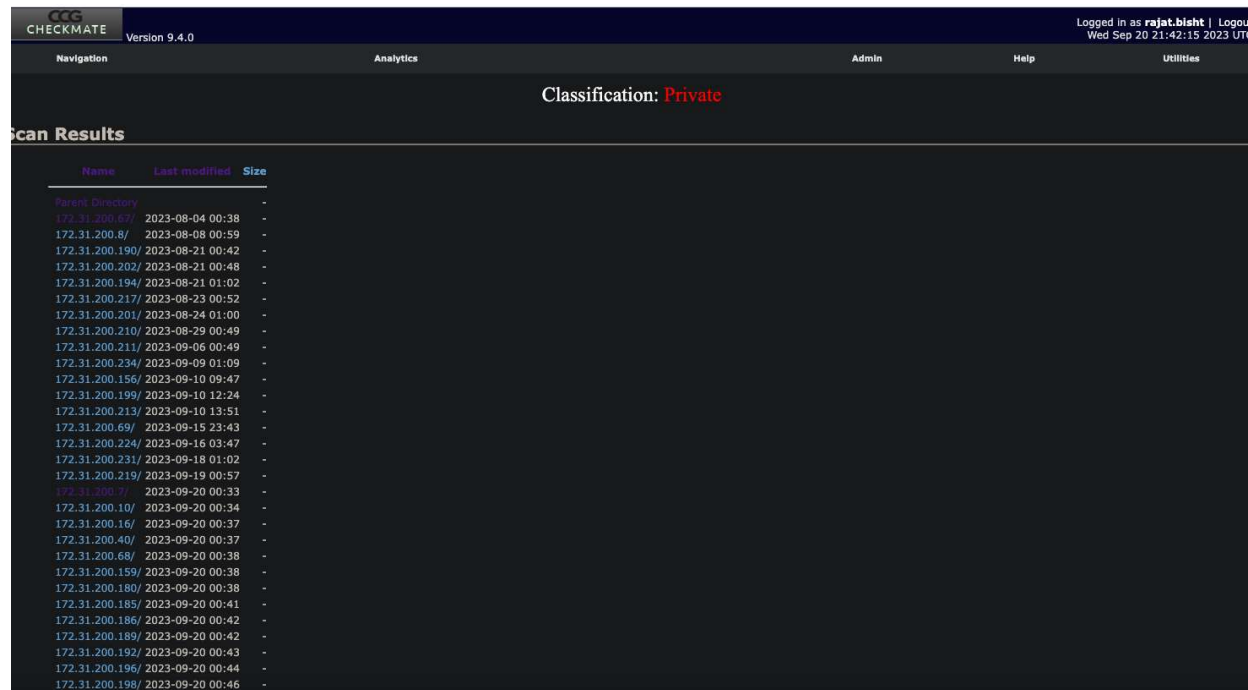
Vulnerabilities with the level False Positive are not being displayed in the reports. But special reports for findings of this level can be created. As with overrides they can have a time limitation.

1.6.3 AUTOMATIC FALSE POSITIVES

CanSecure is able to detect false positives automatically and can assign an override automatically. However the target system must be analyzed internally and externally with an authenticated scan. An authenticated scan can identify vulnerabilities in locally installed software. As such vulnerabilities can be identified that can be exploited by local users or are available to an attacker if he already gained local access as an unprivileged user for example. In many cases an attack occurs in different phases and an attacker exploits multiple vulnerabilities to increase his privileges.

SYSTEM CRAWL

System Crawl located inside Navigation tabs scans your network, including subsystems, revealing port details, IP addresses, running services, and network connections.



CCG
CHECKMATE Version 9.4.0 Logged in as **rajat.bisht** | Logout
Wed Sep 20 21:42:15 2023 UTC

Navigation Analytics Admin Help Utilities

Classification: **Private**

Scan Results

Name	Last modified	Size
Parent Directory		-
172.31.200.67/	2023-08-04 00:38	-
172.31.200.8/	2023-08-08 00:59	-
172.31.200.190/	2023-08-21 00:42	-
172.31.200.202/	2023-08-21 00:48	-
172.31.200.194/	2023-08-21 01:02	-
172.31.200.217/	2023-08-23 00:52	-
172.31.200.201/	2023-08-24 01:00	-
172.31.200.210/	2023-08-29 00:49	-
172.31.200.211/	2023-09-06 00:49	-
172.31.200.234/	2023-09-09 01:09	-
172.31.200.156/	2023-09-10 09:47	-
172.31.200.199/	2023-09-10 12:24	-
172.31.200.213/	2023-09-10 13:51	-
172.31.200.69/	2023-09-15 23:43	-
172.31.200.224/	2023-09-16 03:47	-
172.31.200.231/	2023-09-18 01:02	-
172.31.200.219/	2023-09-19 00:57	-
172.31.200.7/	2023-09-20 00:33	-
172.31.200.10/	2023-09-20 00:34	-
172.31.200.16/	2023-09-20 00:37	-
172.31.200.40/	2023-09-20 00:37	-
172.31.200.68/	2023-09-20 00:38	-
172.31.200.159/	2023-09-20 00:38	-
172.31.200.180/	2023-09-20 00:38	-
172.31.200.185/	2023-09-20 00:41	-
172.31.200.186/	2023-09-20 00:42	-
172.31.200.189/	2023-09-20 00:42	-
172.31.200.192/	2023-09-20 00:43	-
172.31.200.196/	2023-09-20 00:44	-
172.31.200.198/	2023-09-20 00:46	-

NeTERS

INTRODUCTION

This chapter provides a detailed How-to-Use guide for NeTERS, including its purpose and communication with other network devices.

PURPOSE OF THE SYSTEM

NeTERS provides network monitoring. For users to analyze communications between devices on the same network, NeTERS provides a detailed user-friendly GUI (Graphical User Interface). The NeTERS system can tag, collect, trace, inspect, and identify media documents, file documents, web code, and applications in transit as well as their paths. In addition, NeTERS will create real-time network maps. NeTERS can also detect viruses and track them down to their source.

COMMUNICATIONS BETWEEN DEVICES

NeTERS uses the sensors that are on the network to trace the communication of any activities happening on the network. More sensors on a network will provide more areas to look over on a network.

HOW TO USE NETERS?

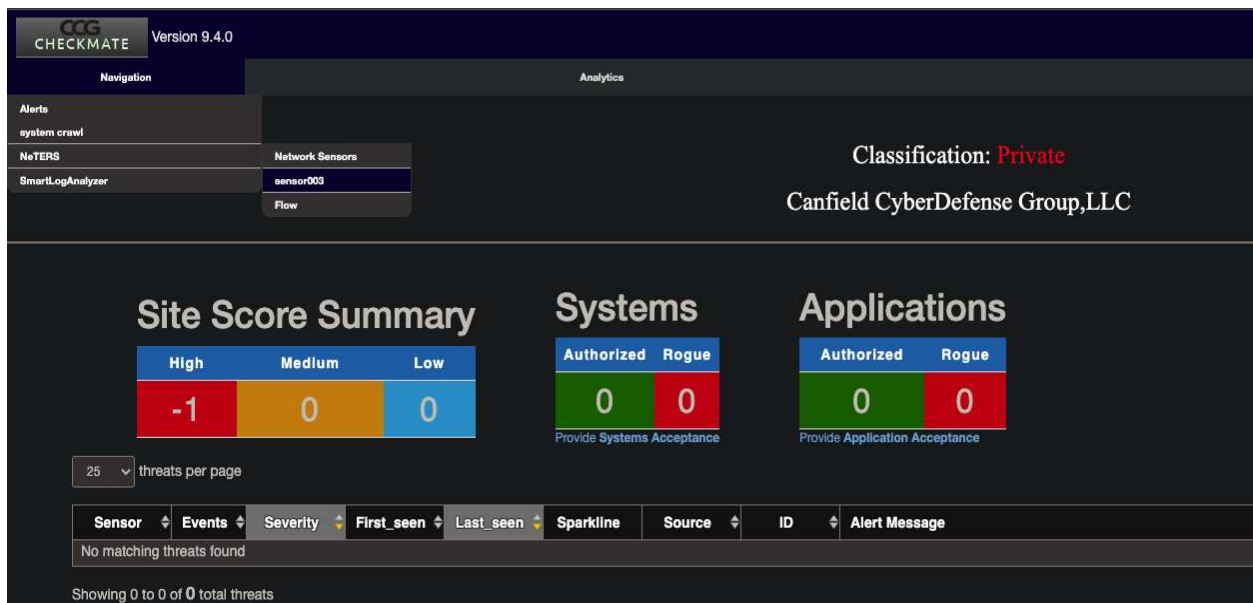


Figure 1: Home page

There are two methods for accessing NeTERS from CanSecure. To begin, hover over the navigation tab in the upper left-hand corner, which will display a drop-down menu similar to the one shown in the image above. This drop down menu should have two options, the first of which is NeTERS home, which will open a new page. (See **Figure 1: Home page.**)

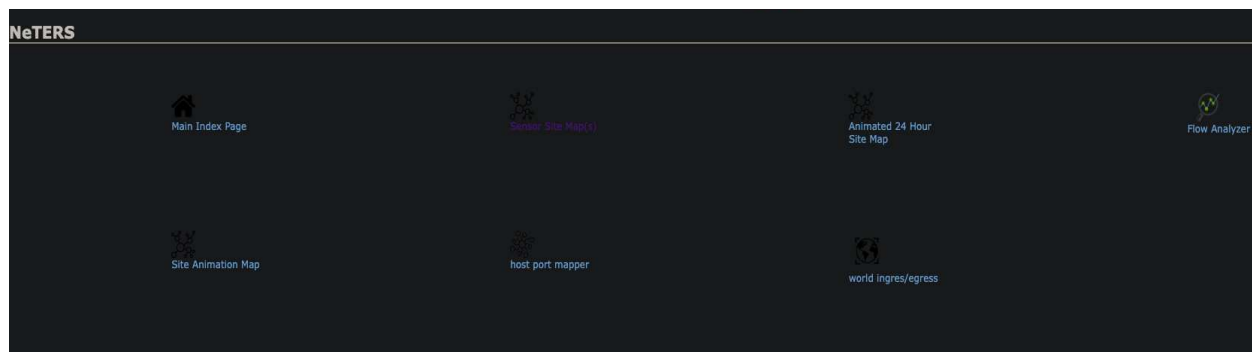


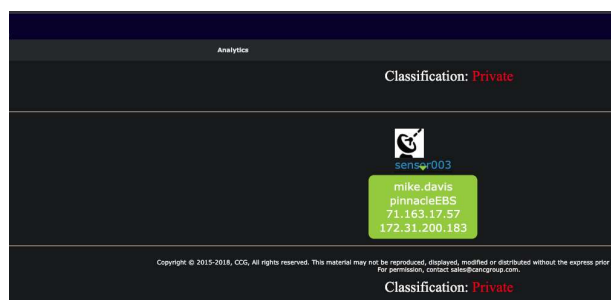
Figure 2: Main NeTERS page



Figure 3.1: Sensor list page

By clicking “Sensor site-maps”, NeTERS will display the list of sensors placed on a network. See **Figure 3.1: Sensor list page**.

Second way to enter NeTERS is by clicking Network Sensors from the drop down menu (see **Figure 1: Home page**) it shell take you to the same page as the first method did. (see **Figure 3.2.: Main NeTERS page – selection of a sensor**)



When users hover over one of the network sensors, a green box appears beneath the sensor icon and the icon expands. The green box contains three items of information: (1) the sensor's name, (2) the sensor's IP address, and (3) the Network's IP address NeTERS then takes you to the Network Diagram of that network sensor by clicking on the sensor icon.

Figure 3.2.: Main NeTERS page – selection of a sensor

Note: NeTERS uses the sensors that have been placed on a network, the more sensors there are the better view and information NeTTER provides.

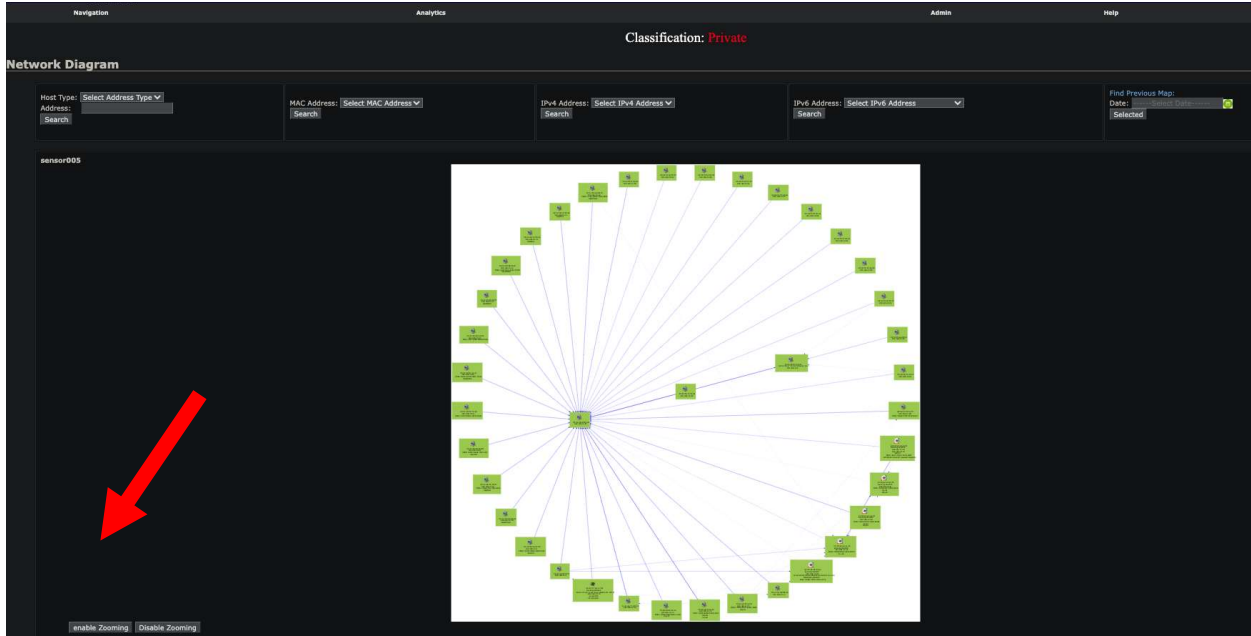
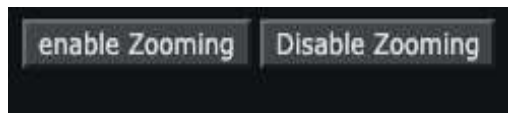


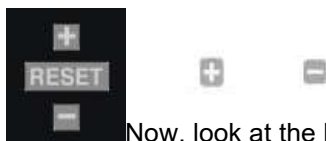
Figure 4.1.0: Sensor insight

Above is an actual image (**Figure 4.1.0: Sensor insight**) of how the sensor data is displayed. On the diagram, notice how there are green boxes inside the network and small white boxes surrounding it. In addition, there are red and blue lines. Nodes are those green and white boxes. Each node is a network-connected device, and the green nodes are Network-pinned nodes. White nodes, on the other hand, are not pinged by the network: this is why white nodes are also referred to as "destinations," because devices on the network only send data in, and the white node does not respond, whereas green nodes can exchange messages. The darker the blue line, the more signal interactions are taking place between each device.



Notice on the bottom left corner, where the red arrow is pointed, there are two buttons, one enables zoom and other one disables the zoom.

Figure 4.1.1: Zoom buttons



Now, look at the bottom right corner, there are three buttons. A network diagram can be zoomed in, zoomed out, and using and reset the network diagram's size reset to its default setting.

NETWORK DIAGRAM FILTER (NDF)

NeTERS has the capability of filtering out devices that are currently connected or have been connected in the past. The NeTERS filters will help you sort between devices, since NeTERS also provides data on each device. There are 3 types of filters, 1) Host Address Search (HAS), 2) Host Device Search (HDS), and 3) Time Based – Network Activity Search (TB-NAS). The **Figure 4.1.3 A: NeTERS Filter** illustrates the appearance of the NeTERS filter.

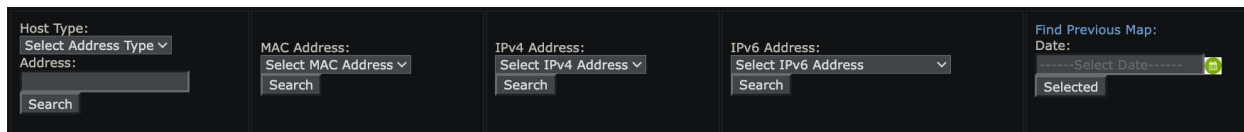


Figure 4.1.3 A: NeTERS Filter

HOST ADDRESS SEARCH (HAS):

If you notice, on the very left corner, the network diagram filter gives an option that lets you enter the host type and Address. This search box is called Host Address Search (HAS) By left clicking on the host type, a dropdown menu shows up. This dropdown menu lets users select from three host types – Mac Address, IPV4, and IPV6. (visit the following hyperlinks to learn more about – [MAC address](#), [IPV4](#) and [IPV6](#))

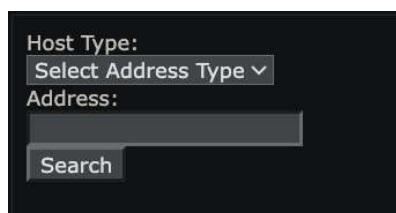


Figure 4.1.3 B: NeTERS Filter - HAS

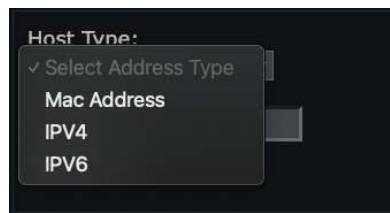


Figure 4.1.3 C: NeTERS Filter – HAS list

Select which host type is the address that you are searching for, then in the address box, write down the address.

HOST DEVICE SEARCH (HDS):

Human brain can only remember so much, therefore users aren't expected to know every host's addresses. Therefore, the next three filters in the NDF (Network Diagram Filter) will allow users to search for the devices, which are or have been on the network, by their host addresses.

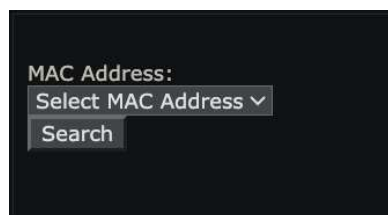


Figure 4.1.3 D: MAC Address List

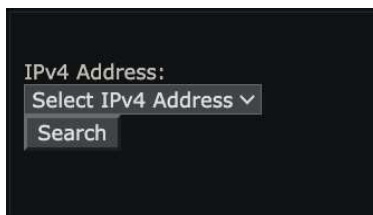


Figure 4.1.3 E: IPv4 Address List

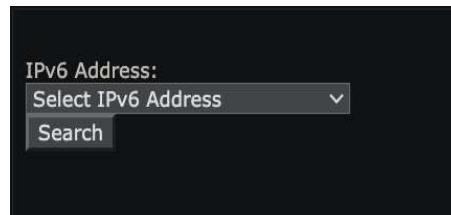


Figure 4.1.3 F: IPv6 Address List

As shown in above screen captures (images **Figure 4.1.3 D**, **Figure 4.1.3 E** and **Figure 4.1.3 F**) these drop down menus are called Host Device Search (HDS). HDS allow users to select any MAC, IPV4 or IPV6 addresses on the network. (**Note:** these host addresses are the ones that are ALREADY on your network, unlike VPN, these dropdown menus do not provide new or temporary host addresses!).

Every host address has its own profile on NeTERS. Therefore, every search made using HAS or HDS filter will open up the profile page of the searched host address. These profiles are called Host profile (HP) or Host Address Profile (HAP). you will see HP and HAP being used interchangeably. (See page ## for an in-depth understanding of how to navigate through these host profiles (HP) to get the information you require.)

TIME BASED – NETWORK ACTIVITY SEARCH (TB-NAS):

Last but not least, TB-NDS. This filter is unique compared to the other filters. NeTERS keeps the data of network activity from hour-to-hour, day-to-day, month-to-month and year-to-year. Meaning, users can check the history of the network activity from any time. See **Figure 4.1.3 G: Map Search**



Figure 4.1.3 G: Map Search

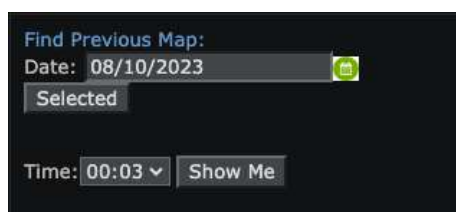


Figure 4.1.3 H: Map Time

Selection

TB-NAS is very straightforward, the user will select a date, then TB-NAS will prompt the user to enter time. The hours in NeTERS are military time based, which means the time can be any hour of the day from 1 through 24 (Notice, there is no slot to enter AM or PM). Once a user clicks the “show me” button, NeTERS will not lead the user to any host profiles; however, it will change the Network Diagram. After using the TB-NAS filter, the user will exit from the real-time network diagram to the network diagram from whatever date and time selected by the user.

HOW TO NAVIGATE HOST ADDRESS PROFILE (HAP)?

Let’s assume, you used the HAS filter to search for some IPV4 address. Once you click search, you will be taken to the HAP (Host Address Profile). See **Figure 4.2.0: HAP Insight** to see how an HAP looks like.

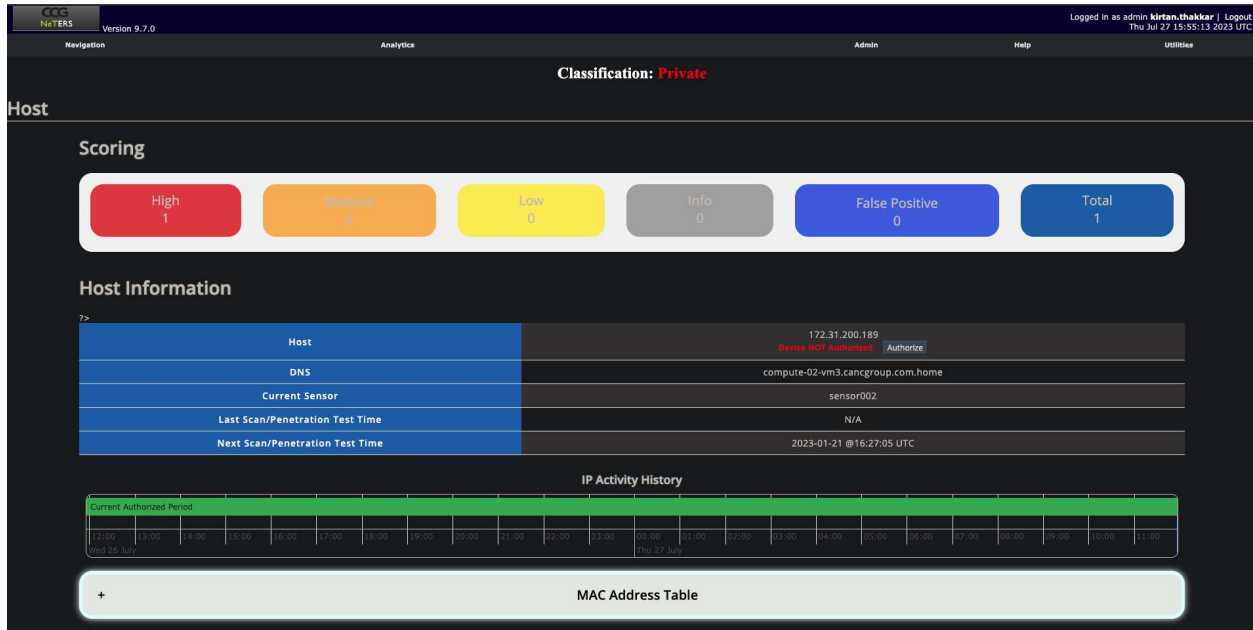


Figure 5.1.0: HAP Insight

Just to recap, NeTERS can see every activity going on in the network, which includes files in transit, tracing them and devices on the network, and HAP is the place that lets you see the files in transit and helps you trace them. NeTERS traces files by the host addresses. Therefore, by entering an HAP, you can see every file that has ever entered or transferred through this host address.

SCORING:

PhenAi runs a vulnerability check every day, and it rates the vulnerability on a scale of low to high. And depending on how many vulnerabilities Phen has detected, and what ratings it gives, will determine the numbers shown in the scoring (red box, orange box and yellow box). Phen also collects information on the vulnerability that it detects and if Phen finds any, it will indicate it in the gray box in scoring. Phen is very good at its job and it is not easy to fool him, therefore if there is any “false positive” vulnerability, Phen will also indicate that in the blue box. Lastly, the green box, it’s just the total amount of vulnerabilities in the network.

HOST INFORMATION:

Host information is a table of information, which provides information such as, host address, DNS, current sensor, Last scan time and next scan time. It also allows users to authorize or unauthorize the host address of that HAP.

IP ACTIVITY HISTORY:



Figure 5.2.1: IP Activity History

This timeline is meant to show the data of when the IP was authorized, and the times when the network was active.



Figure 5.2.2 A: IP Activity History

Above image shows that the IP was authorized from Monday October 24th 2020 through Thursday October 27th 2020. Now if the user zooms in to the timeline, it will show the exact time as when exactly the IP was authorized and when exactly the IP was unauthorized. See image above.

The IP was authorized at 12:56 on Monday August 7th 2023.



Figure 5.2.2 B: IP Activity History

As shown in the image above, the IP was unauthorized at 12:56 on Monday August 7th 2023.

MAC ADDRESS TABLE:

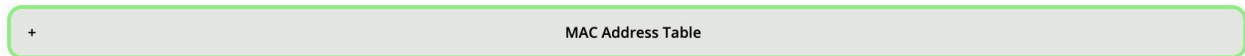


Figure 5.2.3: MAC Address Table

Mac address Table provides information about device-to-device communications. See image below (**Figure 5.2.4: MAC Address Table**).

MAC Address Table		
Last MAC address	First Seen	Last Seen
A8:BB:50:AE:DE:31	2021-06-22 19:37:29	2021-07-03 16:29:12
B4:AE:28:DE:A9:6F	2021-07-30 05:38:20	2021-07-30 06:08:24
34:17:eb:f0:89:33	2023-06-29 01:40:53	2023-06-29 04:10:09

Figure 5.2.4: MAC Address Table

The MAC Address Table has three columns. Last Mac Address, First Seen, and Last Seen. Last Mac Address provides a list of different MAC Addresses that were connected to the current MAC Address. This list is set to a new-to-old order, which means the very new ones are going to be ordered. First Seen gives information about when was the first time the associated ID was seen. And Last Seen gives information about when these MAC Addresses were last associated.

Inbound Data

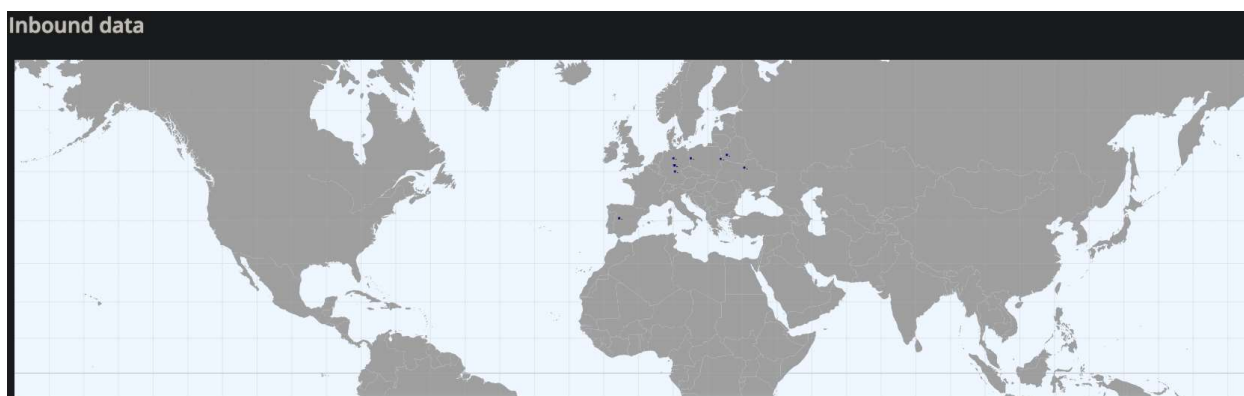


Figure 5.2.5: Inbound data

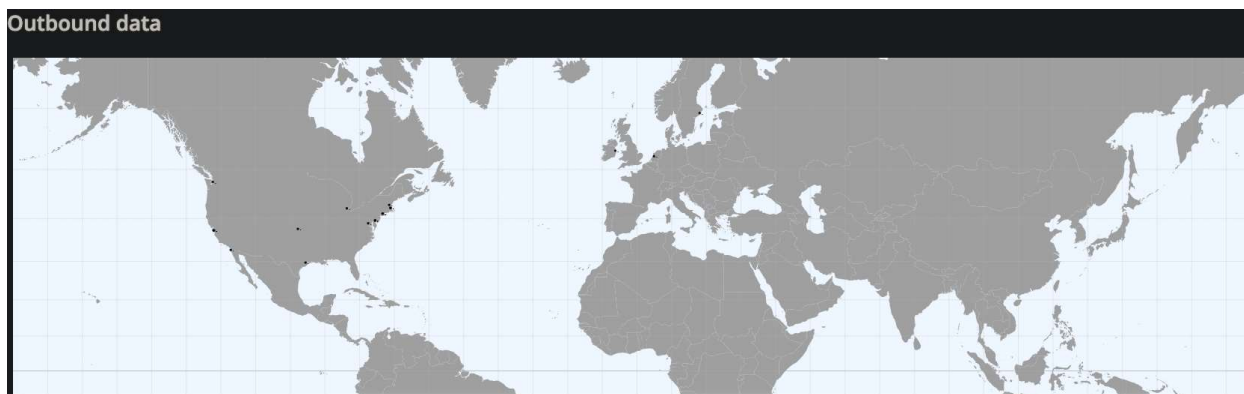


Figure 5.2.6: Outbound data

With NeTERS, users can locate a public server that is connected to their own server from anywhere in the world. The feature allows users to check the source and destination of data packages. The inbound map indicates where the signals originate, and the outbound map indicates where they go. Despite looking similar, each map has a slightly different meaning.

Server Software Table and Client Software Table are used to feed data into the geolocations.

Server/Client Software Table (S/C – ST)

+ Server Software Table				
TCP Protocol	Client Service	Port	First Seen	Last Seen
6	[unknown:@https]	443	2023-06-05 02:24:10	2023-06-05 02:24:12
6	[ssl:TLS 1.0 Client Hello]	443	2023-06-17 22:14:17	2023-06-23 19:16:38
6	[http:Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)]	443	2023-05-26 00:33:40	2023-06-23 17:14:31
6	[http:Wget/1.19.5 (linux (gnu))]	80	2023-06-18 12:40:07	2023-06-18 19:14:53
6	[http:Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/113.0]	80	2023-04-13 18:56:00	2023-04-14 01:58:10
6	[http:RokuOS/12.0.0.4184, Ignition X/14.1.2022120820 (roku, Roku)]	80	2023-06-23 16:27:50	2023-06-23 18:03:17
6	[http:Debian APT-HTTP/1.3 (2.4.8) non (interactive)]	80	2023-04-12 22:15:32	2023-06-27 16:42:23
6	[http:Microsoft (CryptoAPI/10.0)]	443	2023-06-12 23:38:32	2023-06-19 13:00:28

Figure 5.2.6: S/C-ST – 1

+ Client Software Table				
TCP Protocol	Client Service	Port	First Seen	Last Seen
17	[domain:DNS SQR No Error]	53	2023-06-17 12:43:12	2023-06-17 12:43:13
6	[sql:MySQL 6.0.12-1.fc39.src.rpm HTTP/1.1]	42560	2023-05-16 03:20:22	2023-05-24 01:42:43

Figure 5.2.7: S/C-ST – 2

The ST (Inbound) and ST (Outbound) images show the information related to what is being sent and received on each server port. There are columns for Client Services in both tables that show what is happening on those ports as well as what TCP protocol is being used. First Seen and Last Seen simply show when the Client service started on those ports and when the Client Service ends. The only difference is that in S-ST (Inbound) the Client Service is sent out from those ports, and vice versa on C-ST (Outbound).

However, the Client Services sometimes will show up on the ports where it is not supposed to be, and that is where the next part comes into play.

Inbound Ports Table Search (IPTS)

Inbound Ports Table		
Search for Port number...		
port	description	status
53	[Domain Name System](/wiki/Domain_Name_System) (DNS)	Official
123	[Network Time Protocol](/wiki/Network_Time_Protocol) (NTP), used for time synchronization	Official
34567	EDI service[196]	Official
35357	OpenStack ID Service	Official
36963	Unreal Software multiplayer games, such as Counter Strike 2D (2D clone of [Counter Strike])	Unofficial
37601	Epipole File Transfer Protocol [197]	Official
37659	Axence nVision[_citation needed](/wiki/Wikipedia:Citation_needed)_]	Unofficial
37777	[Digital Video Recorder] hardware[_citation needed](/wiki/Wikipedia:Citation_needed)_]	Unofficial

Figure 5.2.8 A: IPTS

Figure 5.2.8 B: IPT – Search bar

IPTS is basically just a port search table where the search bar takes an input of the port number. Once the port number is entered, NeTERS uses IANA’s database to display the information regarding what services the port is supposed to be used for.

Figure A: TCP & UDP protocol – legend

Legend of TCP and UDP protocol table cells for port numbers	
Cell	Description
Yes	Described protocol <i>is</i> assigned by IANA for this port, and <i>is</i> : standardized, specified, or widely used for such.
Unofficial	Described protocol <i>is not</i> assigned by IANA for this port, but <i>is</i> : standardized, specified, or widely used for such.
Assigned	Described protocol <i>is</i> assigned by IANA for this port, ^[2] but <i>is not</i> : standardized, specified, or widely used for such.
No	Described protocol <i>is not</i> : assigned by IANA for this port, standardized, specified, or widely used for such.
Reserved	Port is reserved by IANA, ^[2] generally to prevent collision having its previous use removed. ^{[3][4]} The port number may be available for assignment upon request to IANA. ^[3]

CHAPTER 2 PROCESSING DETAILS

You can process and filter the Flow data according your needs, by navigating to Navigations – NetTERS – Flow.

Flow Processing [List last 500 sessions](#) | [Top 10 Src IPs](#) | [Top 10 Dst IPs](#) | [Top 10 Src Port](#) | [Top 10 Dst Port](#) | [Top 10 Proto](#)

Source:	Filter:	Options:
<input type="checkbox"/> sensor003 <input type="checkbox"/> sensor002 <input type="checkbox"/> fw-external <input type="checkbox"/> fw-internal <input type="checkbox"/> All Sources	<div style="border: 1px solid #ccc; height: 100px; width: 100%;"></div> <p>and <none></p>	<input type="radio"/> List Flows <input checked="" type="radio"/> Stat TopN Top: 10 Stat: Any IP Address order by: flows Limit: <input type="checkbox"/> Packets > 0 - Output: <input type="checkbox"/> / IPv6 long

Figure 10 Processing display

- Select the Flow sources to process. You may select multiple sources.
- Enter a Flow filter.
- Select any options for the analysis.
- Click 'process'.

A default filter is supplied when a specific protocol is selected in the main graph. You may add any further filter expressions as needed.

By just clicking **process**, a top 10 statistics of the any IP address ordered by flows is calculated.

However, you may change this at any time.

The sources, the filter as well as all options from the processing form are compiled into the appropriate NeTERS command. For convenience a short description of the filter syntax and options follows.

2.1.1.1 FILTER SYNTAX

The filter syntax is similar to the well-known pcap library used by tcpdump. The filter can span several lines. Anything after a '#' is treated as a comment and ignored to the end of the line. There is virtually no limit in length of the filter expression. All keywords are case independent, unless otherwise noted. For a complete filter syntax see the **NeTERS(1)** man page.

Any filter consists of one or more expressions **expr**. Any number of **expr** can be linked together:

Filter = **expr**, **expr and expr**, **expr or expr**, **not expr**, (**expr**), **not** (**expr**)

expr can be one of the following filter primitives: Any
any Used as dummy filter. Use '**not any**' to block all flows.

Protocol version: **inet** or **ipv4** for IPv4 and **inet6** or **ipv6** for Ipv6

PROTOCOL: **proto** <protocol> where **protocol** can be any known protocol such as **TCP**, **UDP**, **ICMP**, **GRE**, **AH** etc. or **proto num** where num is the protocol number.

IP address

[SourceDestination] **IP** <ipaddr> or

[SourceDestination] **HOST** <ipaddr> with <ipaddr> as any valid IPv4 or IPv6 address. SourceDestination may be omitted.

[SourceDestination] **IP IN** [<iplist>]

[SourceDestination] **HOST IN** [<iplist>
iplist space separated list of individual <ipaddr>
[SourceDestination]

Defines the IP address to be selected and can be **SRC DST** or any combination of **SRC and/or DST**.
Omitting SourceDestination is equivalent to **SRC or DST**.

[inout]
Defines the interface to be selected and can be **IN** or **OUT**.

Network

[SourceDestination] **NET a.b.c.d m.n.r.s** for IPv6 network netmask pair
[SourceDestination] **NET net/num** with net as a valid IPv4 or IPv6 network and num as mask bits.
The number of mask bits must match the appropriate address family IPv4 or IPv6.
Networks may be abbreviated such as 172.16/16 if they are unambiguous.

Port

[SourceDestination] **PORT [comp] num** with num as a valid port number. If comp is omitted, '=' is assumed.
[SourceDestination] **PORT IN** [<portlist>
Portlist space separated list of individual port numbers

Interface

[inout] **IF num** with num as an interface number.

Flags

flags tcpflags
With tcpflags as a combination of:

- A ACK.
- S SYN.
- F FIN.
- R Reset.
- P Push.
- U Urgent.
- X All flags on.

The ordering of the flags is not relevant. Flags not mentioned are treated as don't care. In order to get those flows with only the SYN flag set, use the syntax '**flags S and not flags AFRPU**'.

TOS

tos value: Type of service: Value 0..255.

Packets

packets [comp] num: Limit the packet count in the Flow record.

Bytes

bytes [comp] num: Limit the byte count in the Flow record.

Packets per second: Calculated value.

pps [comp] num [scale] to specify the pps of the flow: **Duration:** Calculated value
duration [comp] num to specify the duration in milliseconds of the flow.

Bits per second: Calculated value.

bps [comp] num [scale] to specify the bps of the flow: **Bytes per packet:** Calculated value.
bpp [comp] num [scale] to specify the bpp of the flow.

AS

[SourceDestination] **AS num** with num as a valid AS number.
[scale] scaling factor. Maybe (Kilo) k, (Mega) m, (giga) g, (Terna) t. Factor is 1024.
[comp]

The following comparators are supported:

=, ==, >, <, EQ, LT, GT. If comp is omitted, '=' is assumed.

Examples:

tcp and (src ip 172.16.17.18 or dst ip 172.16.17.19)

tcp and (net 172.16/16 and src port > 1024 and dst port 80) and bytes > 2048

2.1.1.2 UNIDIRECTIONAL AND/OR BIDIRECTIONAL

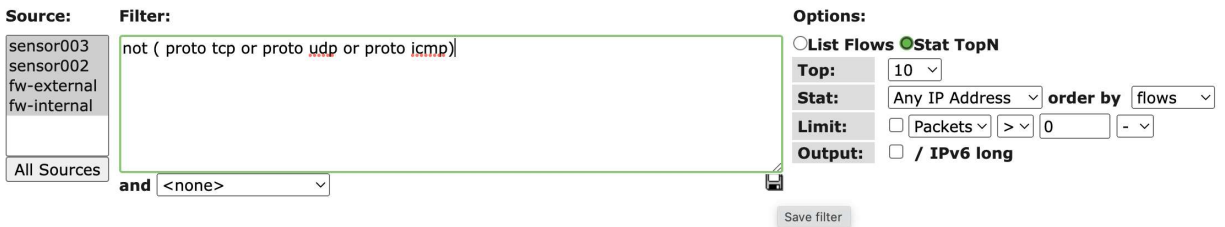
- Unidirectional shows flows from host A to B and then host B to host A
- Bidirectional shows flows between Host A and B combined
- Can be used with any of the other filters (src port, src host plus many more)
- List of filters can be found in the section above.

You need to select either a Single Time-slot or Time Window

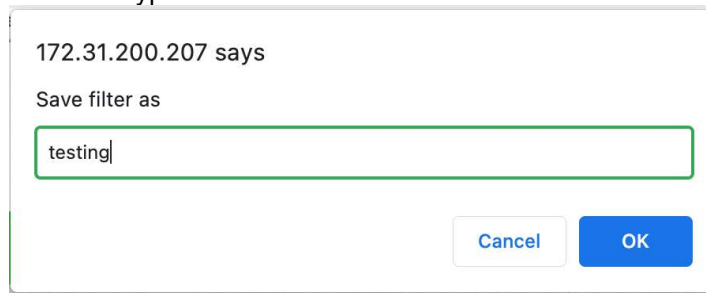
2.1.1.3 SAVING FILTERS

An often-used filter can be saved and used at any time later while processing flows. To create such a custom filter, enter the filter in the text box and click on the diskette symbol to save your filter. After successfully saved, the filter is available in the select box. The resulting filter is always the filter in the text box and the saved filter, therefore logically linked 'and'. A saved filter may be deleted or edited at any time by selecting the filter and clicking on the appropriate icon – either edit, or delete.

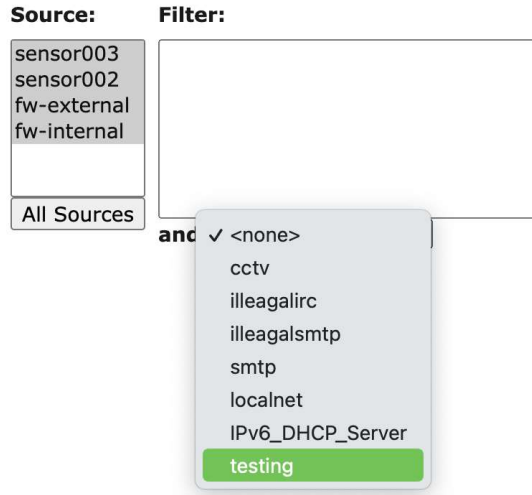
Type in the filter and hit the save icon on the bottom right of the text field.



type in the name of the filter and hit “ok”



See the filter in the “and” drop down selection box.



2.1.1.4 OPTIONS

When processing Flow data, there are two general options, listing flows and creating a flow statistics. You can switch between the two options by clicking on the appropriate button. Depending on what you have selected, the panel automatically adapts to all available options.

List Flows

Limit to

List only the first N flows of the selected time slot

Equivalent to NeTERS option: -c N

Option to aggregate the flows.

Aggregate

By clicking on the checkboxes, you can select how you want to have your flows aggregated. You may also aggregate entire subnets when selecting srcIPv4/<subnet bits>

By default the flows are not aggregated.

Equivalent to NeTERS option: -a -A <aggregate options>

Sort

When listing flows from different channels/sources you may sort them according the start time of the flows. Otherwise the flows are listed in sequence of the selected channels.

Equivalent to NeTERS option: -m

Output

Select one of the available formats to list the flows. The predefined formats '**line**', '**long**' and '**extended**' are always available and correspond the output formats of NeTERS likewise. However, you may specify any time additional output formats by selecting '**custom**'. Enter your own format now in the text input which appears.

Example:

Clear Form process

Options:

List Flows Stat TopN

Limit to: 20 Flows

bi-directional

proto

Aggregate

srcPort srcIPv4/ 24

dstPort dstIPv6/ 24

Sort:

start time of flows

custom ... / IPv6 long

Output: Enter custom output format:

%sap %sas -> %dap %das

Figure 11 Custom Format

By clicking on the diskette symbol, you save your new format, which appears now in the selection menu, ready to use.

For better readability IPv6 addresses are shortened, such as that the middle nibbles are cut and replaced by dots '...'. Most often this is good enough to recognize a wanted IPv6 address you are looking for. If you need the full IPv6 address, check the option '**IPv6 long**'

Top

Equivalent to NeTERS option: -o <format>

Stat

Limit the statistics to the first top N

Aggregate

Equivalent to NeTERS option: -n <N>

Select the statistics you want from the menu and the order option

Limit

Equivalent to NeTERS option: -s <stat>/<order>

This option is only available for the flow record statistics and is equivalent to the aggregate option in **List flows**. See the description above.

Output

Equivalent to NeTERS option: -S

Limit the output only to those statistic lines whose packets or bytes match the specified limit.

Equivalent to NeTERS option: -L <limits>

This option is identical to the Output option in '**List flows**'. See the description above.

Flow Processing [List last 500 sessions](#) | [Top 10 Src IPs](#) | [Top 10 Dst IPs](#) | [Top 10 Src Port](#) | [Top 10 Dst Port](#) | [Top 10 Proto](#)

Clear Form process

Source: sensor003
sensor002
fw-external
fw-internal
All Sources

Filter: proto tcp

and <none>

Options:

List Flows Stat TopN

Top: 10

Stat: Flow Records **order by** flows

bi-directional

proto

Aggregate

srcPort srcIP

dstPort dstIP

Limit: Packets > 0 -

Output: line / IPv6 long

Flows Info

DATE FLOW SEEN	DURATION	PROTO	PROTO ID	FLOWS(%)	PACKETS(%)	BYTES(%)	PPS	BPS	BPP
2022-09-14 06:54:48.642	318.667	TCP	172.31.200.201:39472	->	18.233.222.53:80	13	863	2	
2022-09-14 08:03:14.657	5.002	TCP	172.31.200.183:60064	->	172.31.200.207:1514	12	804	2	
2022-09-14 08:00:01.106	60.856	TCP	172.31.200.183:59722	->	172.31.200.207:5514	40	6644	2	
2022-09-14 08:03:07.654	7.002	TCP	172.31.200.207:1514	->	172.31.200.183:60062	10	536	2	
2022-09-14 07:57:57.291	302.583	TCP	172.31.200.183:53154	->	172.31.200.207:5045	176	80942	2	
2022-09-14 08:03:07.653	0.000	TCP	172.31.200.207:1514	->	172.31.200.183:60056	2	80	2	
2022-09-14 08:03:25.662	7.003	TCP	172.31.200.207:1514	->	172.31.200.183:60068	10	536	2	
2022-09-14 08:03:32.665	0.001	TCP	172.31.200.207:1514	->	172.31.200.183:60070	8	432	2	
2022-09-14 08:00:01.107	60.856	TCP	172.31.200.207:5514	->	172.31.200.183:59722	40	2080	2	
2022-09-14 08:03:07.652	0.000	TCP	172.31.200.183:60056	->	172.31.200.207:1514	2	104	2	

Figure 12 Processing Details Results

Note: Depending on the size of your network, Flow processing may consume a lot of time and resources, when you select a large time window and multiple resources.

CHAPTER 3

PROFILES

A profile is a specific view on the Flow data. A profile is defined by its **name**, **type** and one or more **profile filters**, which are any valid filters accepted by NeTERS. The profile 'live', 'ports', and 'ports' profiles are always available and is used to store your incoming Flow data without filtering. You can switch back and forth to any profile using the pull down menu in the upper right corner of the web page.

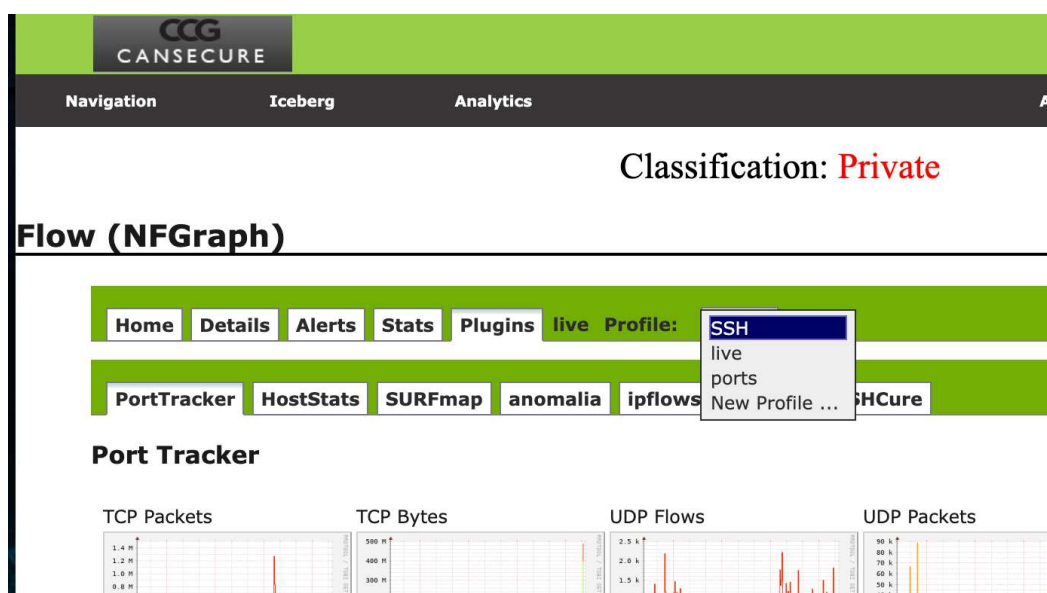


Figure 13 Profile Selection

3.1 PROFILE TYPES

A profile can be either of type **History** or **Continuous**. A history profile starts and ends back in the past and remains static. It neither grows nor expires. A continuous profile may start in the past and is continually updated while new Flow data becomes available. It grows dynamically and may have its own expire values set. Old data expires after a given amount of time or when a certain profile size is reached. Additionally a profile can be created as a **Shadow** profile, which means no Flow data is collected, and therefore saves disk space. A shadow profile accesses the data of profile 'live' when data processing is done with the proper profile filters applied first.

Continuous	History
<ul style="list-style-type: none"> ● Contains Flow data ● Has dedicated expire values 	<ul style="list-style-type: none"> ● Contains Flow data ● Starts and ends at defined time

Continuous / Shadow	History / Shadow
<ul style="list-style-type: none"> ● Contains no Flow data ● Inherits expire values from profile 'live' 	<ul style="list-style-type: none"> ● Contains no Flow data ● Starts and ends at defined time

3.2 PROFILE CHANNELS

A profile contains one or more profile channels. A profile channel is defined by its channel filter, color, sign and order in which the channel is displayed in the graph. A channel is based on one or more Flow sources from the 'live' profile. The number of channels is independent of the number of Flow sources.

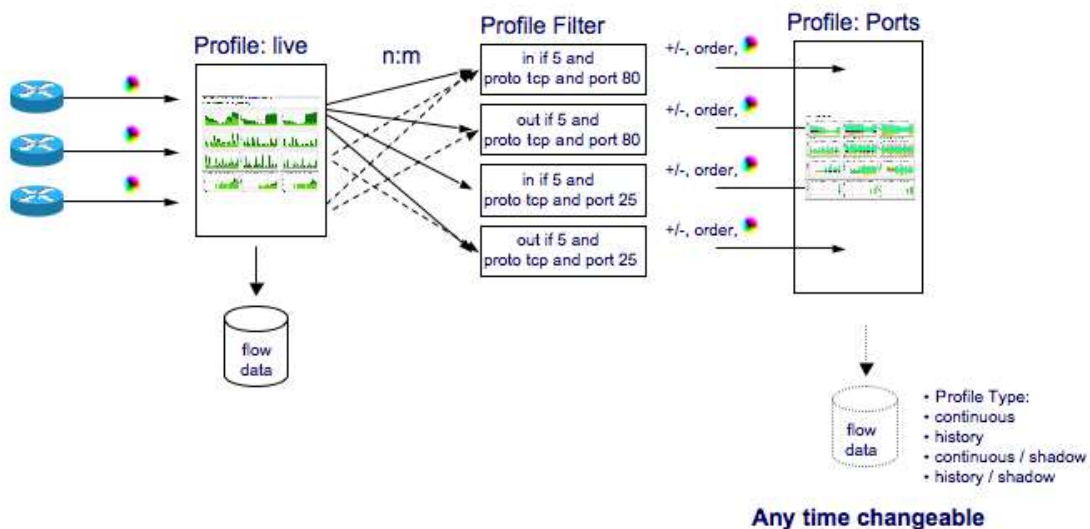


Figure 14 Profile Channels

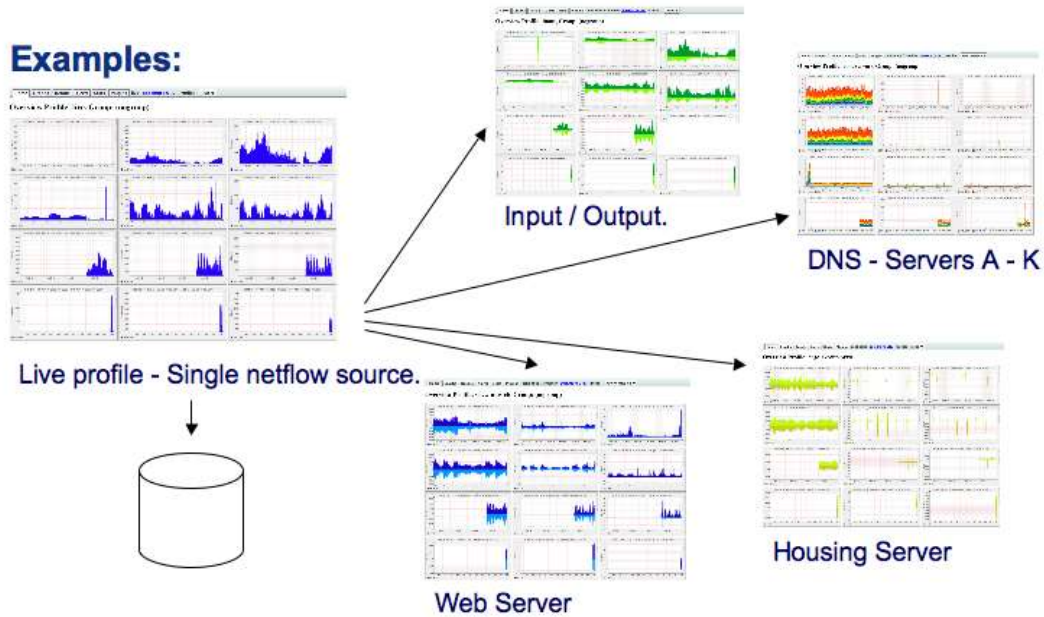


Figure 15 Profile Examples

- Can create graphs based on specific information
 - ASNs,
 - Host/Destination IPs/Ports
 - In/Out interfaces
 - Among others

3.3 CREATING PROFILES

Select the "New profile..." entry in the profile pull down menu. Complete the 'New Profile' form to start building the profile. By moving the mouse over the '?' icon, a help text appears to guide you through the process of creating the profile.

Profile: live	
Group:	(nogroup)
Description:	
Type:	live
Start:	2023-08-01-19:55
End:	2023-08-23-20:55
Last Update:	2023-08-23-20:55
Size:	93.5 MB
Max. Size:	unlimited
Expire:	never
Status:	OK
▼ Channel List:	
▼ sensor002	
Colour:	#786d64 Sign: + Order: 1
Filter:	any
Sources:	sensor002

Profiles may be grouped together for easier selection in the profile menu. Select either an existing profile group, or create a new group according to your needs. There is no difference to other profiles other than grouping the profiles in the profile menu.

The profile type '**Continuous**' or '**History**' is automatically detected according the '**Start**' and '**End**' values you enter. As profiles are created from Flow data from profile 'live', the start and end of the profile must fall in the time range of the profile 'live'.

- If you leave the '**Start**' and '**End**' inputs empty, a continuous profile is created and starts from the time the profile is created.
- If you enter a '**Start**' time but no '**End**' time, a continuous profile is created. Data from the past up to to time, the profile is created is profiled and updated immediately when the profile is created.
- If you enter a '**Start**' and '**End**' time a history profile is automatically created.

EXPIRE / MAX SIZE

A continuous profile may expire due to the age of the data or the profile size used on disk. Expiring starts whenever one of the two limits is reached. Expiring ends at the configured value **\$low_water** (in %). By setting any of these values to 0, the limit does not apply.

PROFILE

For compatibility, a profile with 1:1 channels may be created, which means, that for every Flow source in the live profile a corresponding channel in the profile will be automatically created. The selected sources and the filter in the profile create dialogue are taken for this 1:1 profile. This is the easiest type of a profile.

INDIVIDUAL CHANNELS

For new style profiles select this option. In the 'new profile' dialogue entries for Flow sources as well as for the common filter disappears, as these parameters are now individual for each channel and entered in the channel dialogue.

CREATING CHANNELS


After the profile has been successfully created, one or more channels can be added now by clicking on the '+' icon at the right hand side of the '**Channel List**'.

The parameters color, sign and order are used to display the channel correctly in the graph. The filters as well as the Flow sources are needed to correctly profile the channel. The procedure of adding a channel to a new profile can be repeated as often as required to complete the profile. When all channels are added the new profile must be committed to activate the new profile. This is done by clicking on the checkmark on the right hand side of the '**Status**' line.

Once the profile is committed, the build process starts if required. Depending on how long back in the past the profile starts, this can take a considerable amount of time. You can follow the build process by looking at the progress bar, showing you the percentage of completion. This progress bar is updated automatically every 5 seconds. Note: There are no graphs available in the profile as long as the profile is not completely built.

Please note: For the '**live**' profile, channels have to be configured.

3.4 MANAGING PROFILES

Profiles can be modified by selecting the '**Stat**' tab of the profile and click on any of the available edit icons  of the desired parameter. By clicking on the edit icon of a channel, you may modify the requested channel. All changes will affect the profile immediately. You may also add or delete channels in a continuous profile. However, please note, that adding a new channel to an already existing profile will not rebuild any data for this channel for data in the past. Deleting a channel or the entire profile may be done by clicking on the trash icon.

3.5 CONVERTING PROFILES

Profile may be converted into another type as desired. However, not all conversions are possible. The figure below shows and explains the possible conversions.

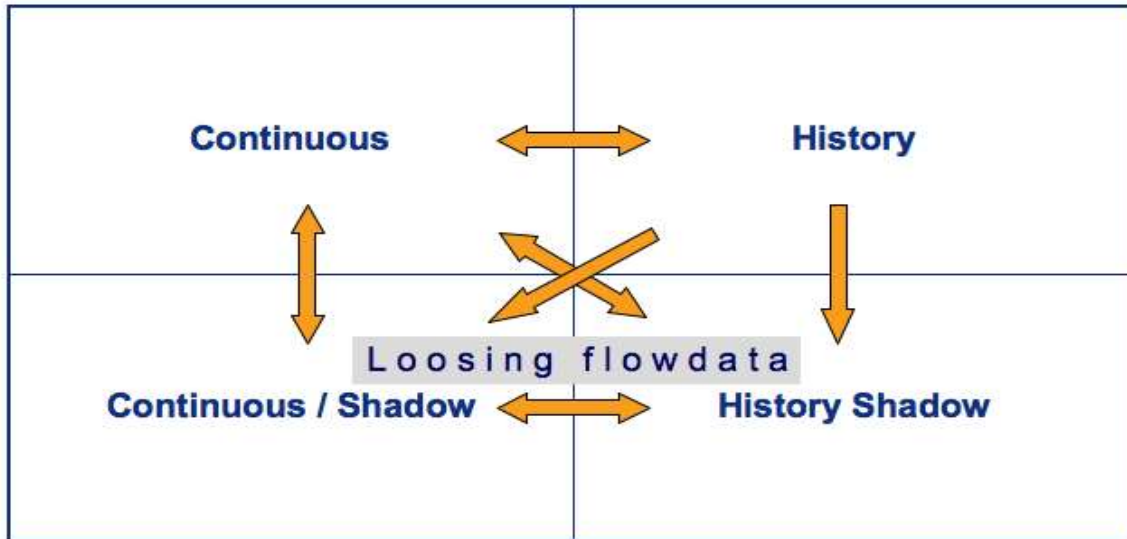


Figure 16 Profile conversion

By switching a profile type between continuous and history you may temporary stop collecting data for a profile or continuing to collect data from a stopped profile. Note, that you will loose all Flow data, when a profile is converted to a shadow profile. When switching back, the data recording resumes at the time of switching.

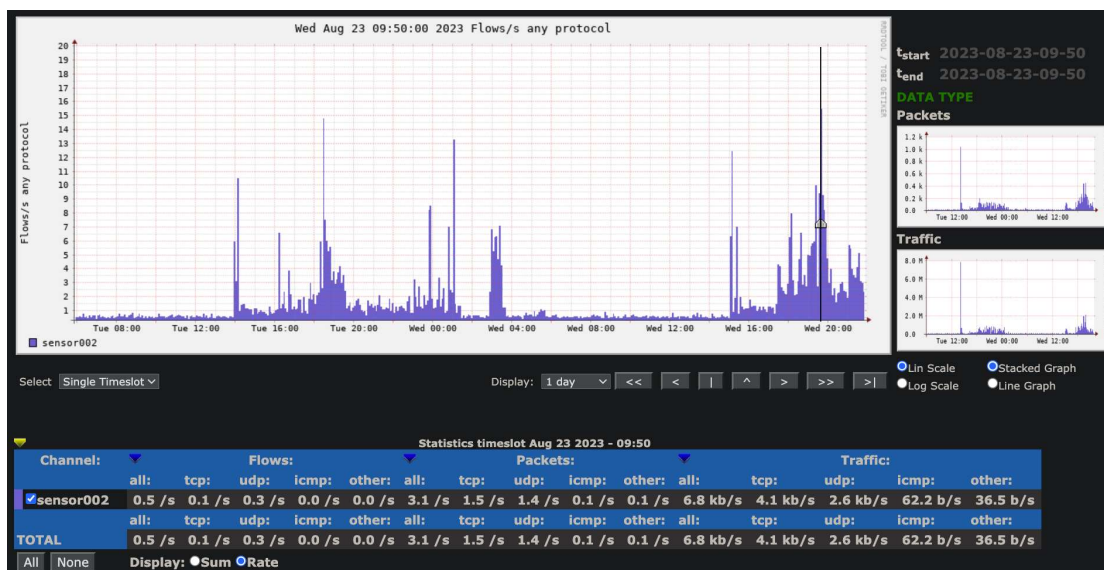
CHAPTER 4

DETAIL GRAPHS

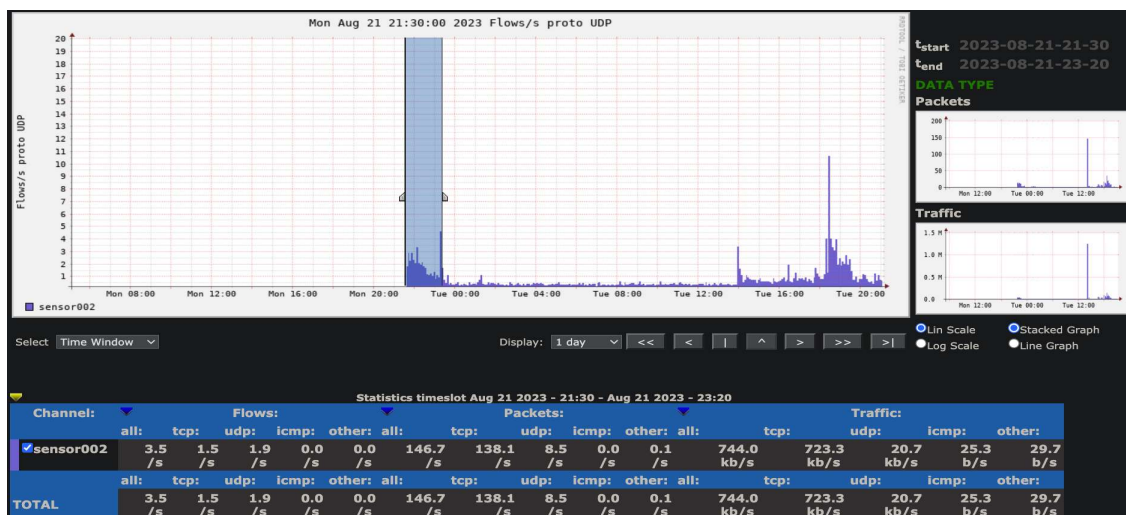
Once up and running you should be able to see the GUI. A quick example of troubleshooting using the tool:

4.1.1.1 EXAMPLE 1

* Looking at the “home” tab, the bits/s graph shows a spike in traffic at about midnight:



Wanting to investigate this in more detail, we can change the “Single Time slot” to “Time Window” and highlight that spike using the graph:



CHAPTER 5

TOP PORT THREATS

5.1 How data is collected

This is how the data was collected. The summary and choices in developing the interface configuration are a result of analyzing 5,000 attacks a day over a 6 month period concluding in April 2019.

5.2 What and Where

The top 4 ports used in the attacks, were present in 65% of the attacks.

- ssh (tcp port 22)
- http (tcp port 80)
- https (tcp port 443)

Those were closely followed by

- ftp (tcp ports 20 and 21).
- rdp (tcp and udp on port 3389)

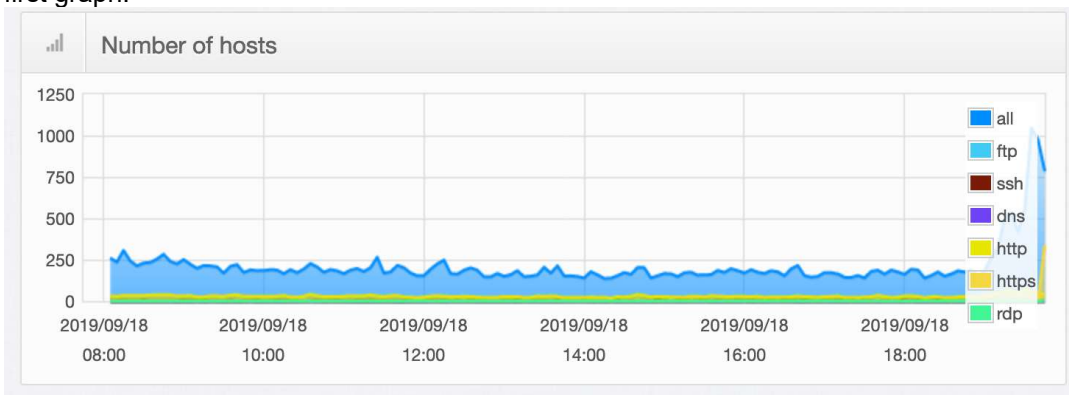
And due to prevalence by state actors in the past

- dns (udp port 53)

This is all being presented in the **NeTERS** FLOW data “plugin” called “hoststats”. That **NeTERS** GUI will point at the following URL:

https://<CheckMate_IP>/NeTERS/nfgraph/index.php?sub_tab=1

To start you will see the following two images. Data is sorted by various traffic types, listed on the right. These are the most common attack types (as reported above), along with “all” data. Each port traffic is defined by a unique color, and similar colors are used for similar port traffic types. The first graph presents the number of Flow records over time and broken out by port traffic type. **Flow** is defined as “*all packets with the same source/destination IP address, source/destination ports, protocol interface and class of service.*” The second graph, in a similar fashion, presents the number of active hosts over time and, again, is broken out by port traffic type. The colors scheme here match the port traffic types of the first graph.



The next important page here is the “Details” on the left. Select that to gain insight into the various port traffic.



Home / Details Profile: all

< 21.8.2023 17:05 202308211705 > Type filter

Timeslot Filter

Results Number of results 20

IP address	In			Out			In						Out						In		Out		Action	
	flows	packets	bytes	flows	packets	bytes	SYN	ACK	FIN	RST	PSH	URG	SYN	ACK	FIN	RST	PSH	URG	unique IPs	sources	unique IPs	sources		
4.27.3.151	1	1	105	1	1	225	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	Action
8.254.14.2	4	4	368	4	4	662	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	Action

The “Details” page provides the following layout.

One of the first helpful selections would be made by selecting our “Profile” on the right. This is our port traffic type. With the images showing an example of selecting the “ssh” port traffic.

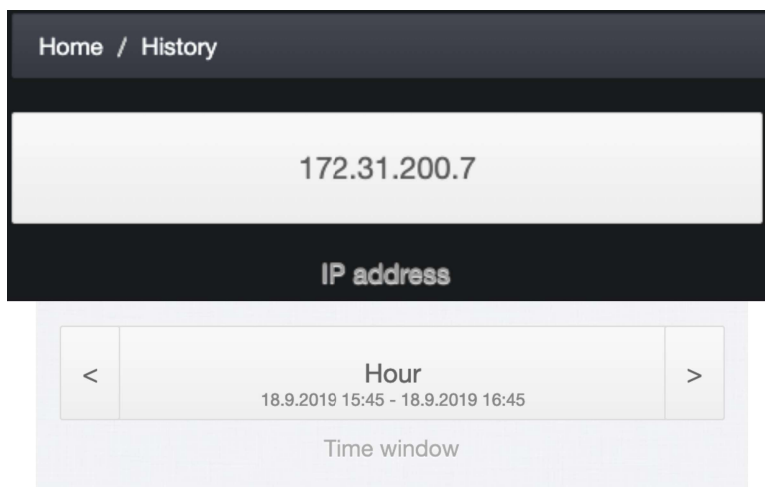


Once filtering on the “ssh” port traffic, we get a more defined table of information presented here. This provides us the ability to sort on source and/or destination systems that are part of the “ssh” application communication. This can be sorted in direction of “In” (destination) or “Out” (source) of the communication. For each of these this can be sorted by “packets”, “bytes” or “flows” depending on what your desire to see. On the right we also see the green box ■ under the “source” column, providing us an understanding of what CheckMate sensor observed this communication. And with knowledge of the sensor location, will provide some useful understanding of concern.

Results																				Number of results			
IP address	In			Out			In						Out						In		Out		
	flows	packets	bytes	flows	packets	bytes	SYN	ACK	FIN	RST	PSH	URG	SYN	ACK	FIN	RST	PSH	URG	unique IPB	sources	unique IPB	sources	
4.27.3.151	1	1	105	1	1	225	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	Action
8.254.14.2	4	4	368	4	4	662	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	Action
13.71.55.58	1	13	1735	1	11	4751	1	1	1	1	0	1	1	1	0	1	0	1	1	1	1	1	Action
13.107.42.1	1	1	88	1	1	92	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	Action
13.107.42.2	2	2	210	2	2	276	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	Action
17.253.200.1	2	2	166	2	2	342	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	Action

By selecting the “IP address” in the table, detailed information about that specific hosts interactions are presented in table form. This allows for both in and out bound communications for the selected host and the give port traffic type.

Also the “History” from the menu on the left may be selected and then you can identify your host of interest by typing that in the “IP Address” field.



Home / History

172.31.200.7

IP address

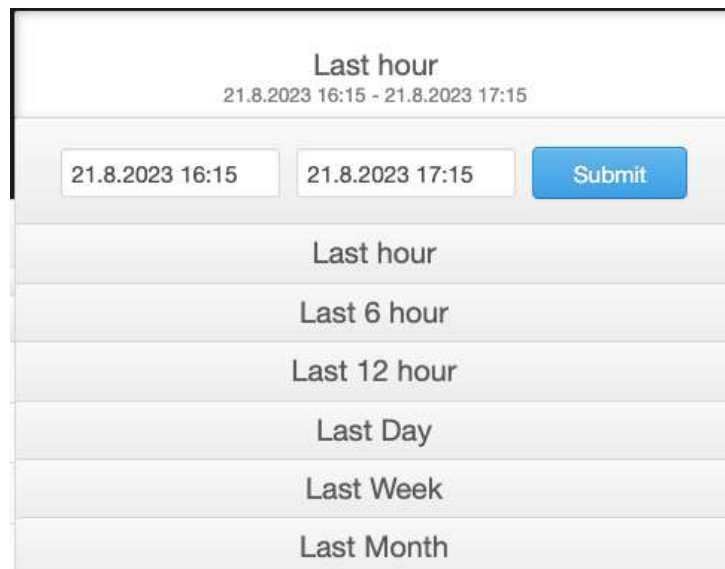
< Hour >

18.9.2019 15:45 - 18.9.2019 16:45

Time window

In ether case, the time window of communications concerning this host may be adjusted in the “Time window” selection.

The drop down provides a simple selection or a more complex method by selecting start/stop times. The complex method allows pint point selection on the time window of known concerns.



Last hour

21.8.2023 16:15 - 21.8.2023 17:15

21.8.2023 16:15 21.8.2023 17:15 Submit

Last hour

Last 6 hour

Last 12 hour

Last Day

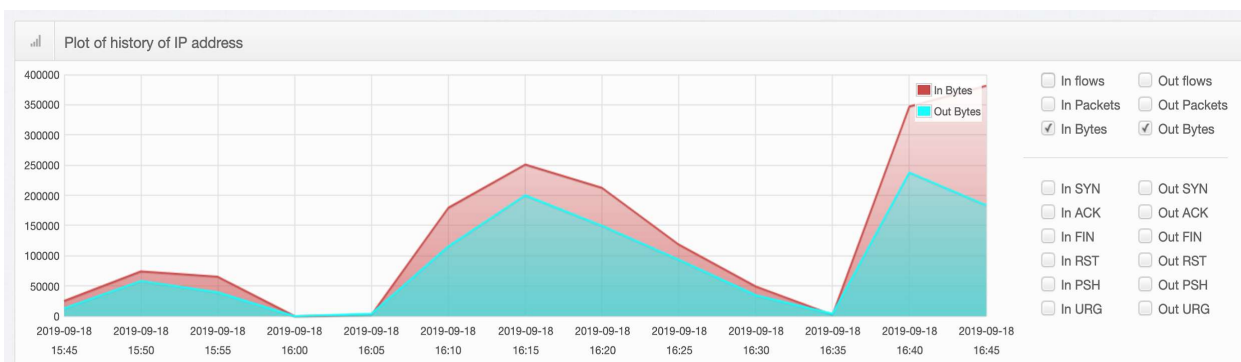
Last Week

Last Month

The details provided in the table and graphs at the bottom provide detailed understanding of this system and what it's doing and when for the selected port traffic type. The table will allow (just as the "Details" above), selection for "In" (IPs traffic to this system by remote IP) and "Out" (IP traffic to other systems from this IP). Sorting is also by "packets", "bytes" or "flows". Also shown are the sensors that have observed the communications between the two systems.

History of IP address																						
Timeslot	In			Out			In						Out						In		Out	
	flows	packets	bytes	flows	packets	bytes	SYN	ACK	FIN	RST	PSH	URG	SYN	ACK	FIN	RST	PSH	URG	unique IPS	sources	unique IPS	sources
2023-08-21 16:15	49	522	369975	49	544	81528	30	30	30	0	30	0	30	30	30	12	30	0	3	3	3	3
2023-08-21 16:20	72	673	466635	72	695	105870	37	37	37	0	37	0	37	37	37	16	37	0	4	4	4	4
2023-08-21 16:25	62	892	587640	62	892	229342	36	36	36	0	36	0	36	36	35	17	36	0	4	4	4	4

IP types (available in the table) are also visible by graph at the bottom. This has been used to help track and understand this system in DoS and other nefarious hacking efforts.



CHAPTER 6 ALERTS

Alerts allow you to execute specific actions based on specific conditions. A filter applied to the 'live' profile, conditions, triggers and alert actions defines an alert.

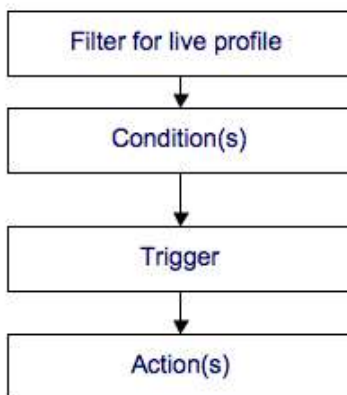


Figure 1 Alert Flow

High			Medium			Low			Authorized		Rogue		Authorized		Rogue					
53			9			3			9		67		1		0					
									Provide Systems Acceptance				Provide Application Acceptance							
25 threats per page																	Filter	Clear	Print	Show all
Sensor	Events	Severity	First_seen	Last_seen	Sparkline	Source	ID	Alert Message	Phen Ignore	Reference										
AdminCore	760	high	20:00:01	20:17:45:01		ML-HostThreat	713	Beaconing to remote IP: 98.137.11.164 Detected	No	details										
AdminCore	190	high	20:20:52:04	20:17:52:14		AI-ThreatIntel	1001	Malware Indicators	No	details										
AdminCore	155	high	21:06:48	20:08:57:53		NIDS	4319	Attempted Administrator Privilege Gain	No	details										
AdminCore	112	high	21:06:48	20:03:41:04		NIDS	45107	Web Application Attack	No	details										
AdminCore	8	high	21:20:14	19:21:20:06		PenTest	i	"172.31.200.7 scan finished with severity 10.0"	No	details										
AdminCore	8	high	21:10:12	19:21:10:08		PenTest	i	"172.31.200.207 scan finished with severity 10.0"	No	details										
AdminCore	8	high	21:10:12	19:21:10:08		PenTest	i	"172.31.200.216 scan finished with severity 10.0"	No	details										
AdminCore	6	high	21:00:14	19:21:00:10		PenTest	i	"172.31.200.189 scan finished with severity 10.0"	No	details										
AdminCore	8	high	21:30:08	19:21:30:15		PenTest	i	"172.31.200.40 scan finished with severity 10.0"	No	details										
AdminCore	8	high	00:50:08	20:00:50:10		PenTest	i	"172.31.200.97 scan finished with severity 10.0"	No	details										
AdminCore	4	high	00:40:05	20:00:40:14		PenTest	i	"172.31.200.186 scan finished with severity 10.0"	No	details										
AdminCore	8	high	01:50:10	20:01:50:12		PenTest	i	"172.31.200.196 scan finished with severity 10.0"	No	details										
AdminCore	7	high	01:30:09	20:01:30:12		PenTest	i	"172.31.200.212 scan finished with severity 10.0"	No	details										
AdminCore	27	high	03:10:00	20:08:56:50		NIDS	24448	Potential Corporate Privacy Violation	No	details										
AdminCore	1	high	03:18:18	19:03:18:18		NIDS	45328	Executable code was detected	No	details										
AdminCore	8	high	02:50:07	20:02:50:11		PenTest	i	"172.31.200.230 scan finished with severity 10.0"	No	details										
AdminCore	8	high	03:35:12	20:03:35:13		PenTest	i	"172.31.200.16 scan finished with severity 10.0"	No	details										
AdminCore	8	high	04:00:09	20:04:00:14		PenTest	i	"172.31.200.215 scan finished with severity 10.0"	No	details										
AdminCore	8	high	03:45:12	20:03:45:12		PenTest	i	"172.31.200.159 scan finished with severity 10.0"	No	details										
AdminCore	8	high	03:55:14	20:03:55:06		PenTest	i	"172.31.200.200 scan finished with severity 10.0"	No	details										
AdminCore	8	high	03:45:12	20:03:45:12		PenTest	i	"172.31.200.203 scan finished with severity 10.0"	No	details										
AdminCore	8	high	05:15:08	20:05:15:06		PenTest	i	"172.31.200.225 scan finished with severity 10.0"	No	details										

CHAPTER 7

SMART LOG ANALYZER

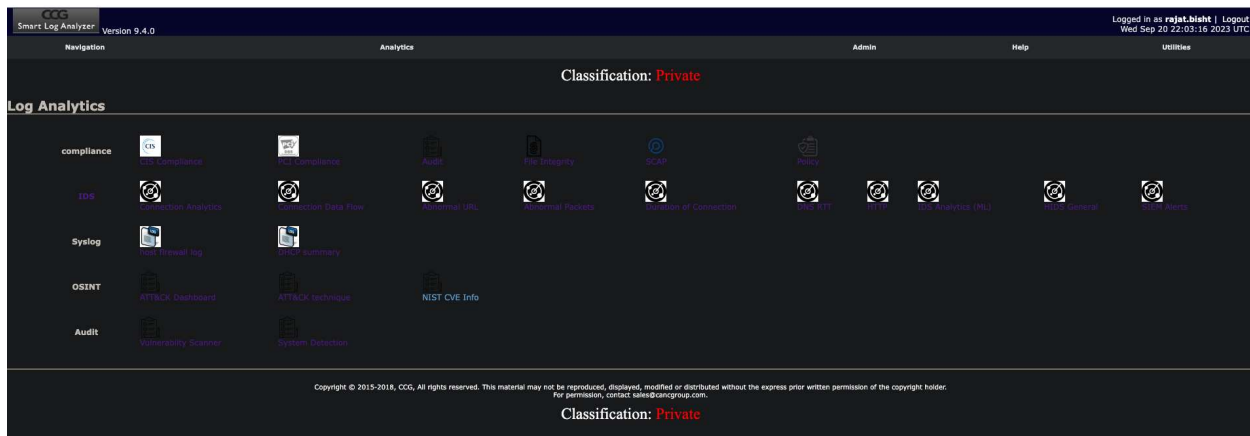
Smart Log Analyzer

Log Analytics, your comprehensive tool for monitoring and analyzing various log data within your organization's network infrastructure. This user manual will guide you through the various analytics modules and features available to help you gain valuable insights and enhance the security and compliance of your network.

The dashboard represents a summary of all notable event activity over the last 24 hours. A notable event is the result of a security-oriented correlation search that scans the indexed logs until a match is found. When a notable event is created, it represents a potential issue or threat requiring a review and, depending upon the outcome of the review, an investigation.

Steps

- Click on Navigation and smart log analyzer.

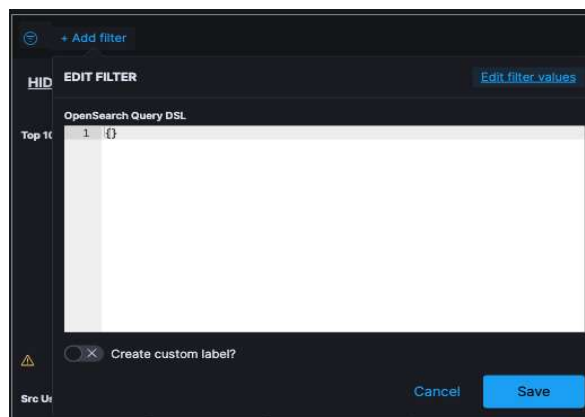
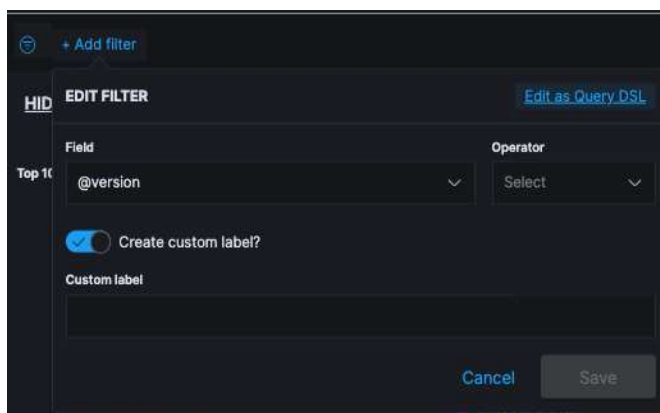


To view the log Analytics navigate to the **main index** and click **Navigation** and scroll down select **CCG dashboard**. You will observe the various analytics modules and features available to help you gain valuable insights and enhance the security and compliance of your network.

Compliance Analytics

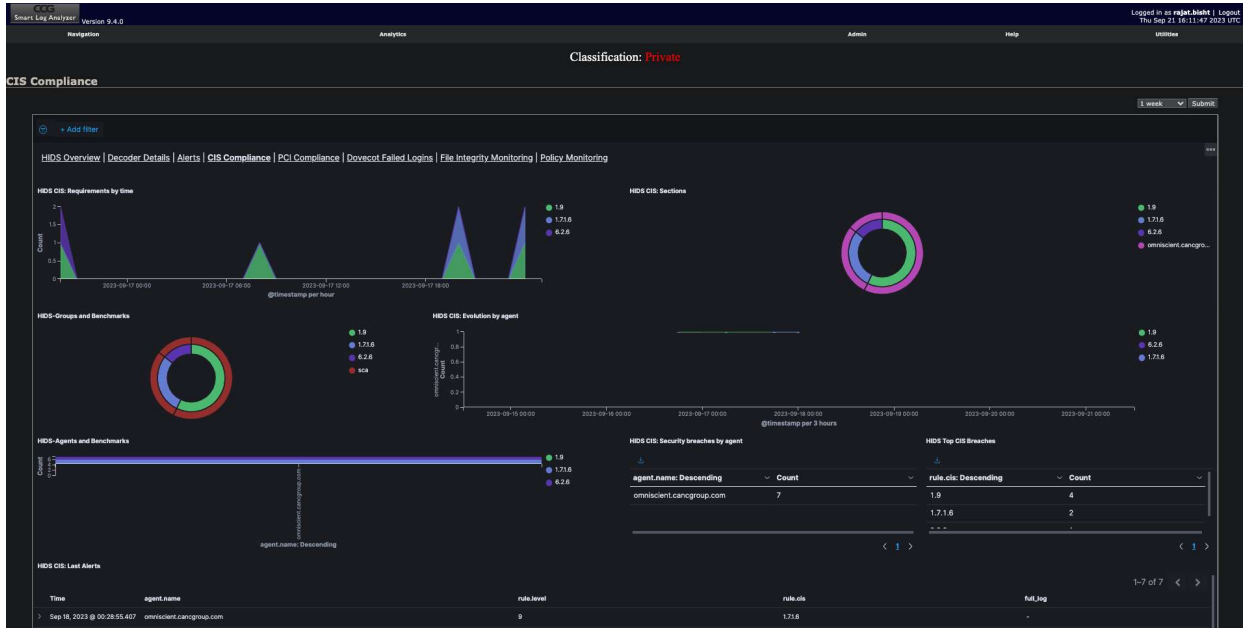
Compliance encompasses a comprehensive dashboard panel featuring a set of critical components for maintaining security and regulatory compliance within your network. Within this dashboard, you'll find various panels, including the HIDS Overview, Decoder Details, Alerts, CIS Compliance, PCI Compliance, Dovecot Failed Logins, File Integrity Monitoring, and Policy Monitoring. Each of these panels plays a vital role in monitoring, assessing, and ensuring the integrity and security of your network infrastructure. Whether it's tracking intrusion attempts, decoding network data, monitoring compliance with industry standards, or identifying security policy violations, the CIS Compliance dashboard provides a holistic view to help you effectively manage your network's security and compliance requirements.

Compliance dashboard offers advanced filtering capabilities, allowing you to refine your analysis based on specific criteria. You can filter data according to indexes, data types, and custom fields, enabling you to focus on the most relevant information for your compliance and security assessments. Additionally, the dashboard supports open search DSL queries, empowering you to perform customized and precise searches tailored to your unique requirements. These powerful filtering and query options provide you with the flexibility needed to effectively investigate and address compliance and security concerns within your network.



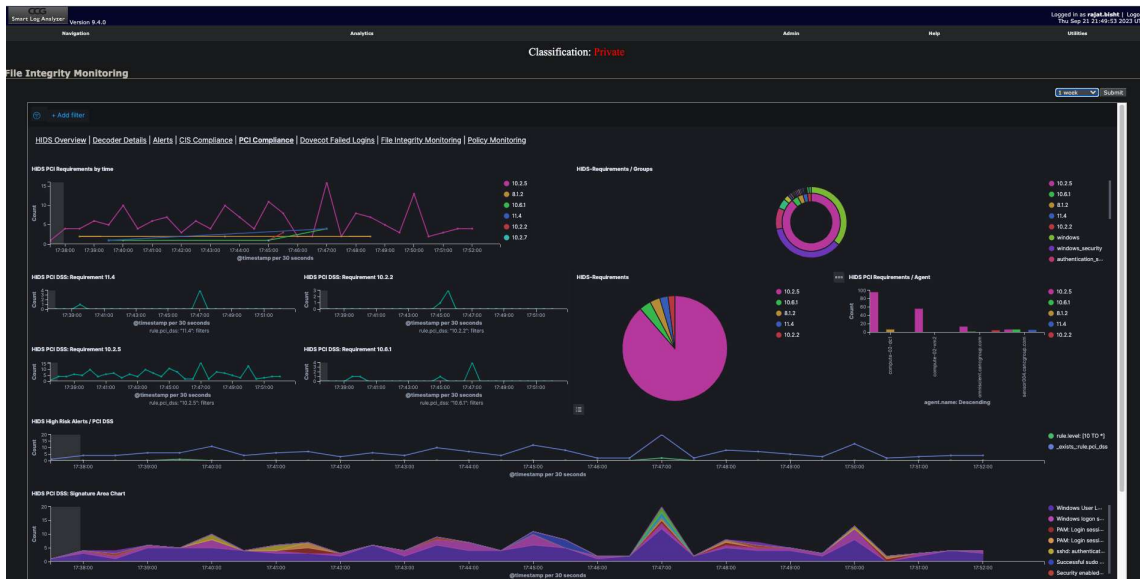
1. CIS Compliance

Monitor and assess your network's compliance with the Center for Internet Security (CIS) benchmarks and recommendations. It gives a graphical representation of HIDS CIS: Requirements by time, Sections, Groups and Benchmarks, Evolution by agent, agents and benchmarks, security breaches by agent, breaches, last alerts.



2. PCI Compliance

Analyze logs to ensure compliance with Payment Card Industry Data Security Standard (PCI DSS) requirements. It gives a graphical representation of HIDS PCI: Requirements by time, Groups, Risk alerts, Signature area chart, Checksum changed, Table integrity checksum changed, Last alerts, Requirements by agent.



3. Audit Analytics

3.1 File Integrity

Track changes in files and directories for security and compliance purposes. The dashboard displays HIDS FIM Alerts over time, Top agents, top agents added, top agents deleted and changed, top files with Root/Admin access, top file changed at the same time.



3.2 SCAP

Utilize the Security Content Automation Protocol (SCAP) for standardized security assessment and monitoring.

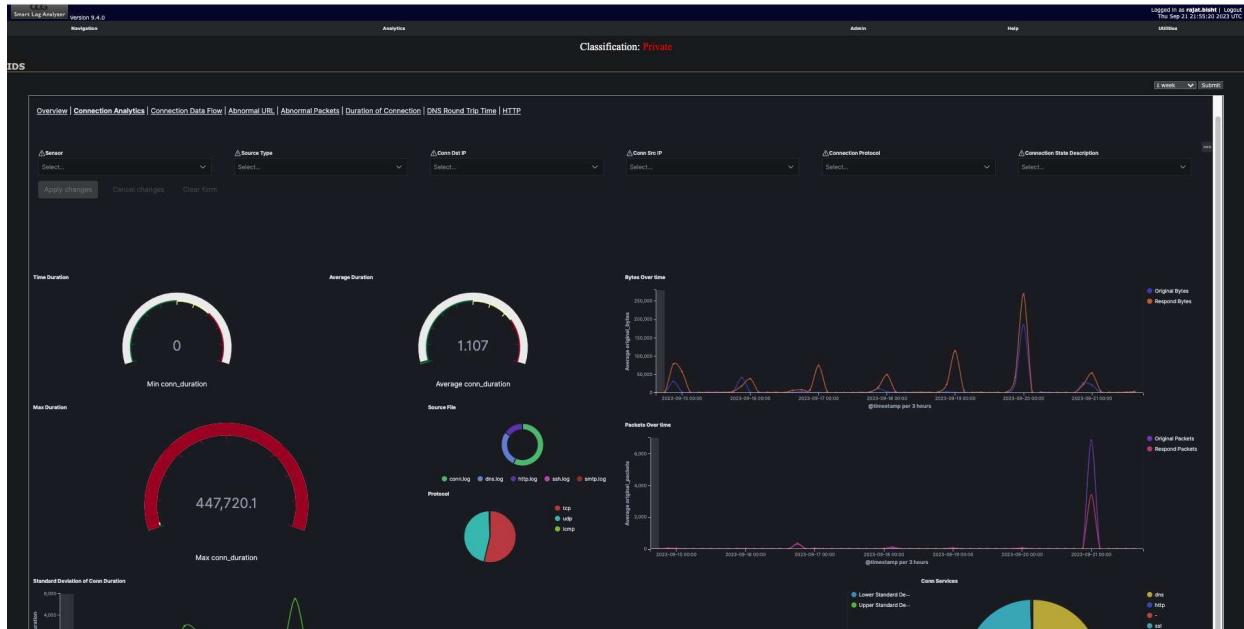
3.3 Policy

Audit logs against predefined security policies to ensure compliance.

4. IDS Analytics

IDA (Intrusion Detection and Analysis) comprises a dynamic Dashboard panel, offering a comprehensive array of features critical for effective intrusion detection and network analysis. Within this dashboard, you will find a range of essential panels, including Connection Analytics, Connection Data Flow, Abnormal URL Detection, Abnormal Packets Analysis, Duration of Connection, DNS Round Trip Time Monitoring, and HTTP Traffic Analysis. These panels collectively provide you with the tools and insights needed to detect and respond to network intrusion, assess connection behavior, identify anomalies, and analyze network performance, helping you maintain the security and integrity of your network infrastructure effectively.

IDS (Intrusion Detection System) module offers users powerful data filtering capabilities. With these features, users can fine tune their analysis by filtering data based on several key criteria, including the sensor used, source type, destination IP address (conn dst ip), source IP address (conn src ip), connection protocol, and connection state description.



4.1 Connection Analytics

Analyze network connections for security threats and anomalies.

4.2 Connection Data Flow

Visualize the flow of data between network endpoints.

4.3 Abnormal URL Detection

Identify and investigate abnormal URLs accessed within your network.

4.4 Abnormal Packets

Detect unusual network packets that may indicate a security breach.

4.5 Duration of Connection

Monitor the duration of network connections for suspicious activity.

4.6 DNS RTT

Analyze DNS Round-Trip Time for performance and security insights.

4.7 HTTP Analysis

Investigate HTTP traffic for potential threats and vulnerabilities.

4.8 IDS Analytics (Machine Learning)

Leverage machine learning for advanced intrusion detection.

5.9 HIDS General

Analyze Host-based Intrusion Detection System (HIDS) logs for security incidents.

5.10 SIEM Alerts

Receive Security Information and Event Management (SIEM) alerts for proactive threat detection.

6. Syslog Analytics

6.1 Host Firewall Log

Monitor host firewall logs for network security analysis.

6.2 DHCP Summary

Analyze Dynamic Host Configuration Protocol (DHCP) logs for network activity insights.

7. Threat Intelligence OSINT (Open Source Intelligence)

Leverage open-source intelligence for threat analysis and identification.

7.1 ATT&CK Dashboard

Access the MITRE ATT&CK framework dashboard to understand adversary tactics and techniques.

7.2 ATT&CK Technique Analysis

Analyze specific ATT&CK techniques to enhance threat detection and response.

7.3 NIST CVE Info

Access National Institute of Standards and Technology (NIST) Common Vulnerabilities and Exposures (CVE) information for vulnerability management.

8. Audit

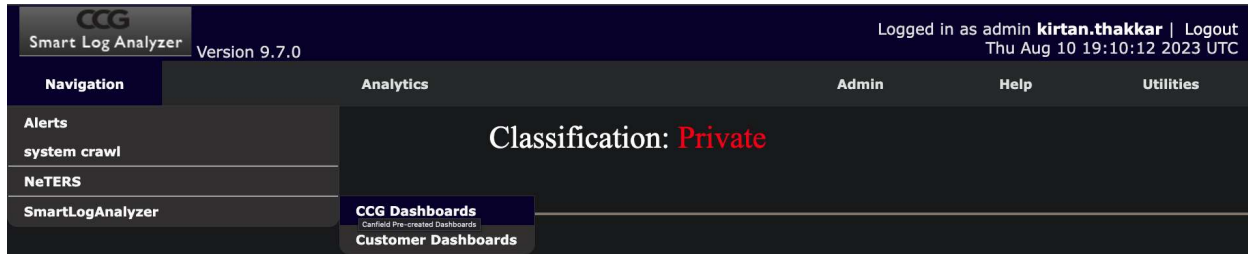
8.1 Vulnerability Scanner

Utilize the vulnerability scanner to identify and prioritize network vulnerabilities.

8.2 System Detection

System Detection feature to identify and analyze system configurations and characteristics for enhanced network security.

Customer Dashboard



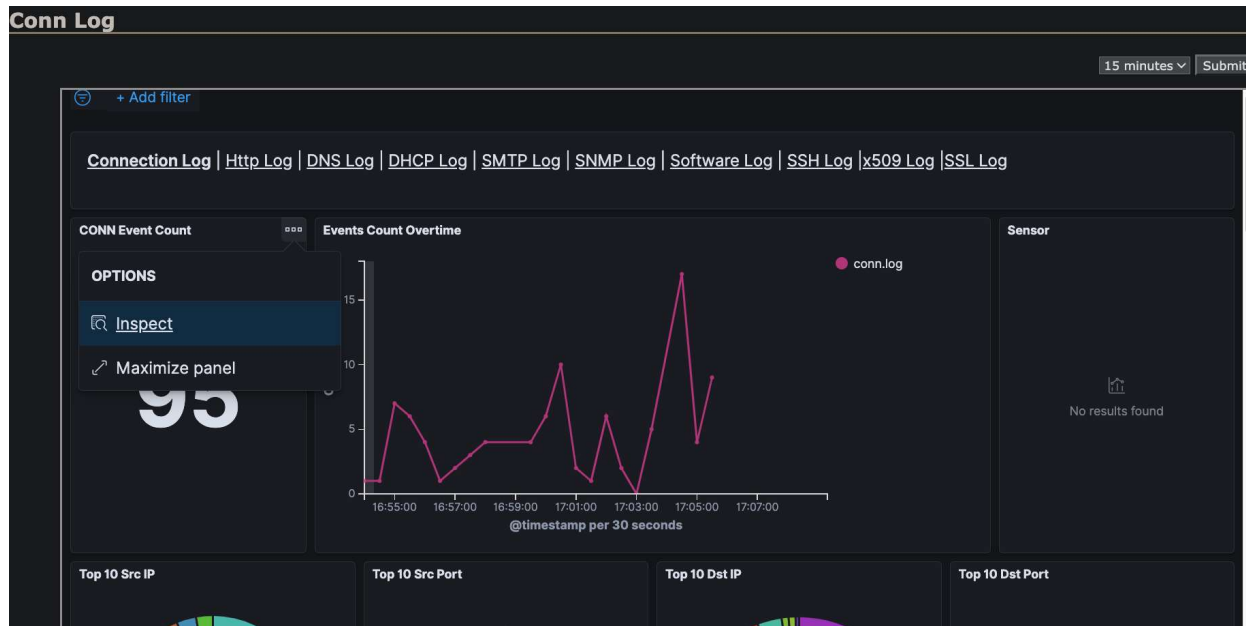
This section describes the Log Correlation Engine (LCE), which is a software module that aggregates, normalizes, correlates, and analyzes the event log data that is collected by the various equipment within an infrastructure.

Smart Log Analyzer; a component within CheckMate creates a variety of logs when run in its default configuration. This data can be intimidating for a first-time user. In this section, take a brief look at the sorts of logs SLA creates. We will look at logs created in the traditional format, as well as logs in JSON format.

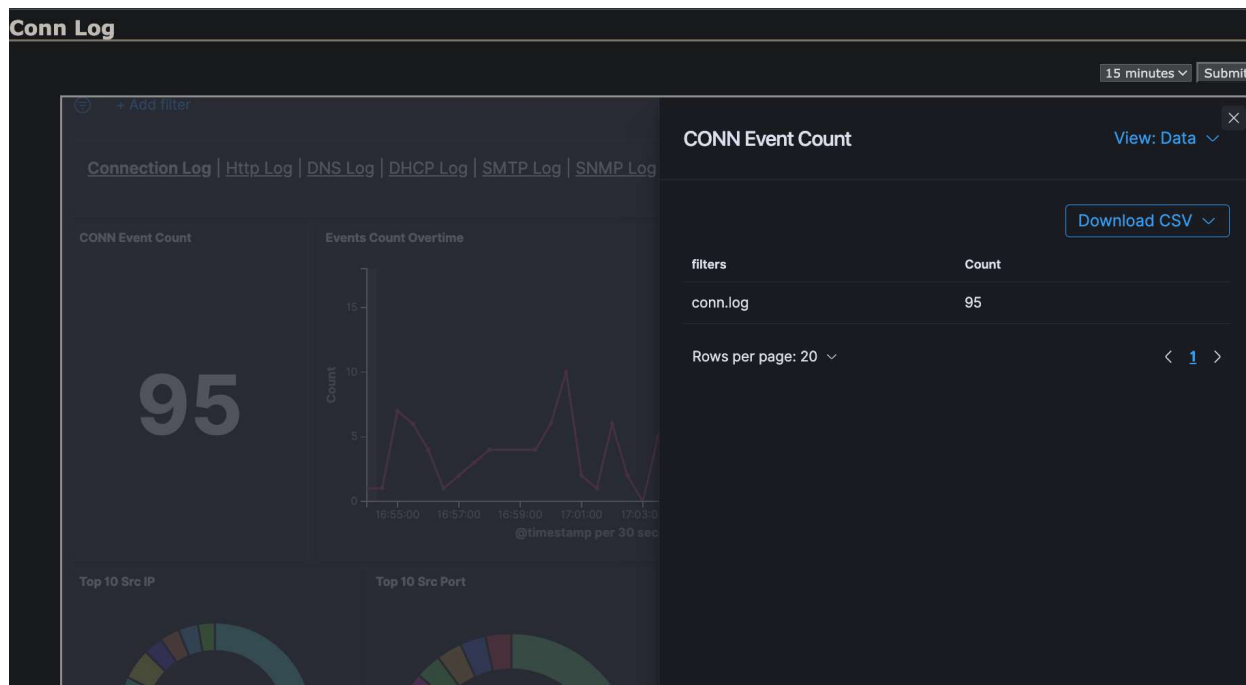
It encompasses a wide range of log types such as HTTP_Log, filtered logs, Software Logs, Connection Logs (Conn Log), DHCP Logs, SMTP Logs, SNMP Logs, SSH Logs, DNS Round Trip Time (DNS RTT) metrics, event processing logs, records of failed login attempts (Failed Logins), x509 certificate-related logs (x509 Log), SSL-related logs (SSL Log), and reporting logs (Report) for comprehensive security and compliance assessment, Apache logs, NIST 800-53 compliance logs, and Host-based Intrusion Detection System (HIDS) reports, offering specialized insights and reporting to address specific security and compliance requirements. This diverse array of logs and functionalities empowers users to effectively monitor, analyze, and secure their network infrastructure while ensuring compliance with industry standards and regulations.

CONN.LOG

The connection log, or **conn.log**, is one of the most important logs SLA creates. It may seem like the idea of a “connection” is most closely associated with stateful protocols like Transmission Control Protocol (TCP), unlike stateless protocols like User Datagram Protocol (UDP). SLA’s **conn.log**, however, tracks both sorts of protocols. This section of the manual will explain key elements of the **conn.log**. **The three dots allow you to customize time range, inspect and maximize panel.**



The **inspect** option allows you to data and request in a Downloadable CSV format.

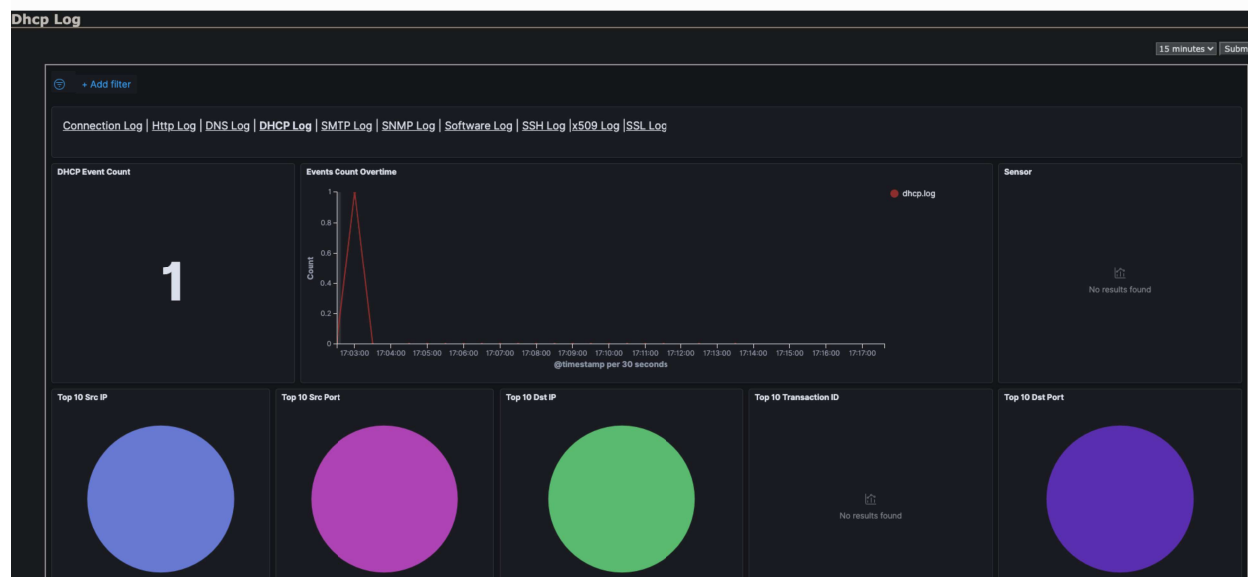


HTTP.LOG

The HyperText Transfer Protocol (HTTP) log, or http.log, is another core data source generated by SLA. With the transition from clear-text HTTP to encrypted HTTPS traffic, the http.log is less active in many environments. In some cases, however, organizations implement technologies or practices to expose HTTPS as HTTP. Whether you're looking at legacy HTTP on the wire, or HTTPS that has been exposed as HTTP, SLA http.log offers utility for examining normal, suspicious, and malicious activity.

DHCP.LOG

Dynamic Host Configuration Protocol is a core protocol found in Internet Protocol (IP) networks. Using the protocol, DHCP servers provide clients with IP addresses and other key information needed to make use of the network. This entry will describe some aspects of SLA's dhcp.log that may be of use to network and security personnel.



SMTP.LOG

In the section discussing the http.log, we noted that most HTTP traffic is now encrypted and transmitted as HTTPS. We face a similar situation with Simple Mail Transfer Protocol (SMTP). For a protocol with “simple” in its name, modern instantiations of SMTP are surprisingly complex.

For the purpose of this manual, it's sufficient to recognize that a mail user agent (MUA) seeking to submit email via SMTP will contact a mail submission agent (MSA). Modern implementations will use ports 587 or 465 TCP, which is encrypted using TLS. Unencrypted implementations will use port 25 TCP.

SSL.LOG

In the section discussing the http.log, we noted that most HTTP traffic is now encrypted and transmitted as HTTPS. SLA does not create a https.log, because Zeek (or other network inspection tools, for that matter) does not natively recognize HTTP when it is encrypted as HTTPS.

HTTPS is most often encrypted using Transport Layer Security (TLS), which presents many variants in live traffic. SLA parses TLS traffic and records its findings in the ssl.log. SSL refers to Secure Sockets Layer, an obsolete predecessor to TLS.

TLS is not restricted to encrypting HTTPS, however. Many other protocols use TLS to encrypt their contents, including Simple Mail Transfer Protocol (SMTP)

SSH.LOG

Secure Shell (SSH) is one of the fundamental protocols of the Internet age. System administrators use SSH to securely access systems, typically running a SSH has always been encrypted, so security analysts have never examined its contents as they may have done with Telnet or other clear text system administration protocols.

x509.log

In the last section we looked at SLA's ssl.log, a source which offered details on TLS connections. In this section we will look at an associated source, SLA's x509.log. The x509.log captures details on certificates exchanged during certain TLS negotiations. We will compare sessions using TLS 1.2 and TLS

Log Report

The log Report shows the system logs(syslogs):The name Syslog is short for System Logging Protocol. This is a messaging standard that is used for sending performance and error data from running software that is either implementing applications or services within operating systems.

UTILITIES

INTRODUCTION:

On the top right hand corner you will see a tab called Utilities, which provides the user with a different calculators to calculate CVSS, and IP. Also, it provides a random password generator so that users can have a highly secured password.

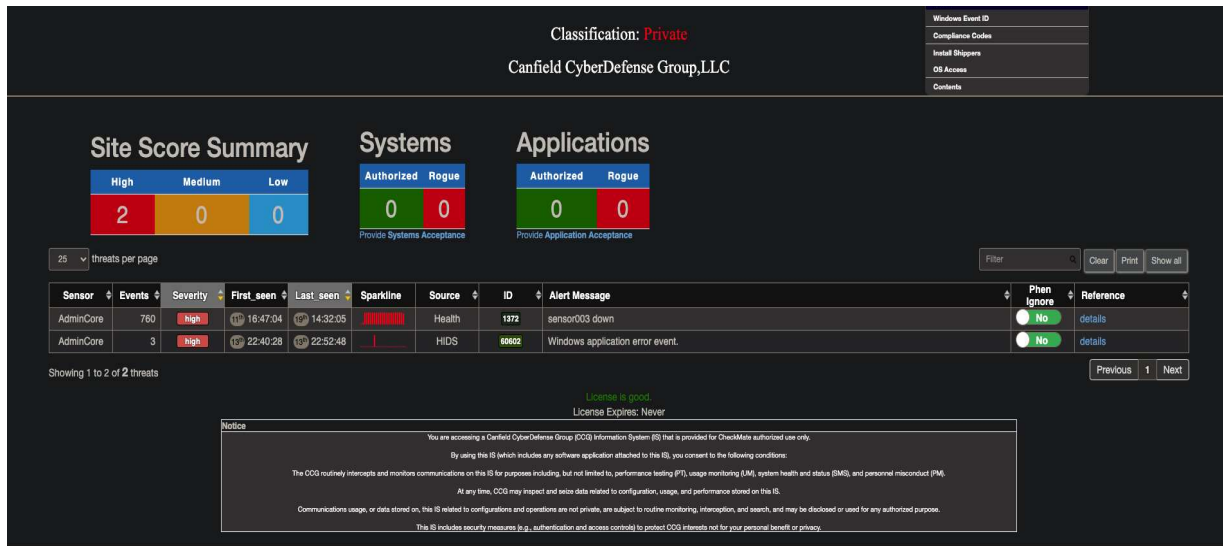


Figure 1.1: Home page

If you hover over the utilities tab, it will prompt a menu. Once the menu is dropped, it will prompt 6 options.

- RPN Calculator
- CVSS v2 Calculator
- CVSS v3 Calculator
- Password Randomizer
- IP Calculator (IPv4)
- Clock

RPN CALCULATOR

RPN Calculator (also known as a Scientific calculator) provides the same features as any hardware scientific calculator. See the image below.

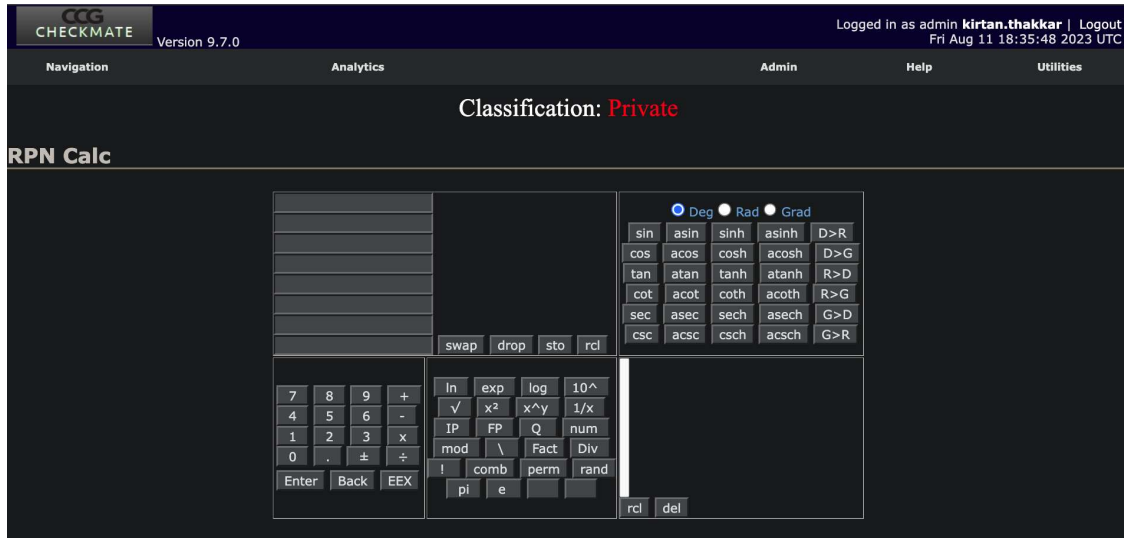


Figure 2: RNP Calc

HOW TO USE IT?



Figure 2.1.1: Field of values



Figure 2.2.1: Math Keyboard



Figure 2.3.1: Numeric/Arithmetic Keyboard

DISPLAY:

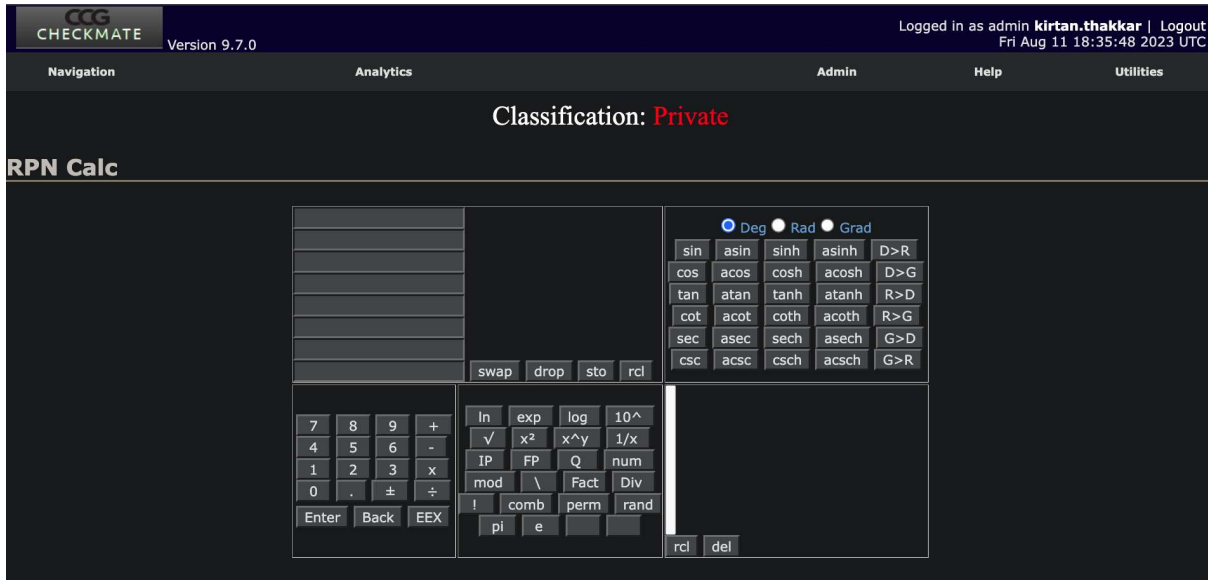
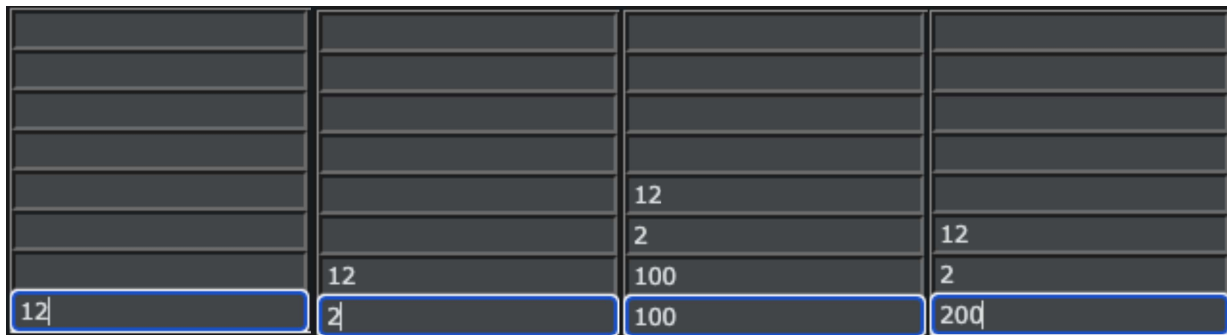


Figure 2.1.1 shows a field where the user would be entering the amount to be calculated.



As you can see in the images above, we entered 12, clicked enter which would send the value a line up. Then 2 was entered and then 100. Once all the digits that need to be calculated, click the arithmetic sign (+,-,/,*) the last amount in the queue will be calculated with the one right above it. So, after entering 100, in this example, addition (+) was clicked; therefore, $100 + 100 = 200$, $200 + 2 = 202$, and $202 + 12 = 214$, so the final answer would be 214.

Figure 2.2.1, shows the keyboard which can be used to enter values and perform calculation; however, it is not compulsory that the users have to use the given graphical keyboard to perform calculation. A physical keyboard can also be used to enter values and perform calculations.

DISPLAY CONTROLLER:



Figure 2.4.1: Controllers

Figure 2.4.1 shows four buttons, swap, drop, so, and rcl. These buttons control 2 panels, see images below:



Figure 2.1.2: Field of values

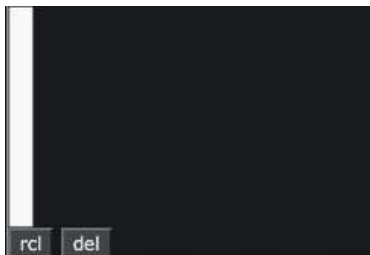


Figure 2.5.2: Field of values

Swap feature:



Figure 2.1.3: Field of values



Figure 2.1.3: Field of values

Swap button swaps the values from the current box with the value in the box right above the blue box. The reason behind the swap button being there is because placement of values matters highly in many arithmetic operations. For instance, subtraction, division, and multiplication.

For instance, if 4 is entered and then 2 and the user subtracts, they get $4 - 2 = 2$; however, if these values are they get -2, and that is the purpose of swap.

DROP FEATURE:

Drop button removes a value from the sack in the display panel.

STO FEATURE:

Sto button is used for the recall panel, Sto stores the value from the display panel to the recall panel.

RCL FEATURE:

Rcl is a short form for recall, which simply pushes the value from the blue box into the stack. See image below.



Figure 2.1.4: Field of values

KEYBOARDS:



Figure 2.3.2: Numeric/Arithmetic Keyboard **Figure 2.6.1:** Math Symbol Keyboard



Figure 2.2.2: Math Keyboard

Above are the graphical keyboards that let the users make various calculations such as Arithmetic and trigonometric operations.

CVSS V2 CALCULATOR (COMMON VULNERABILITY SCORING SYSTEM)

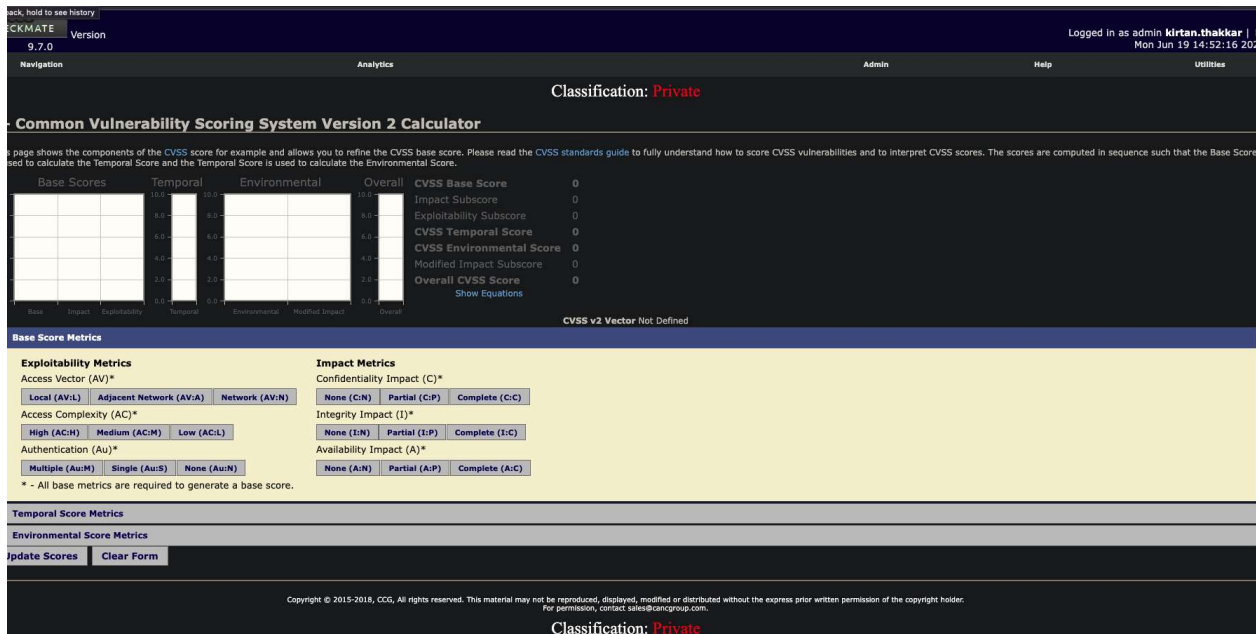


Figure 3.1.1: CVSS – 2 Calculator

Under the utilities tab, CVSS V2 and V3 are listed in the second and third position. CVSS V2 has a section for bar graphs (see image below) and three collapsible forms, called **Base Score Metrics**, **Temporal Score Metrics**, and **Environmental Score Metrics**. Each form has a different effect on the bar graph.

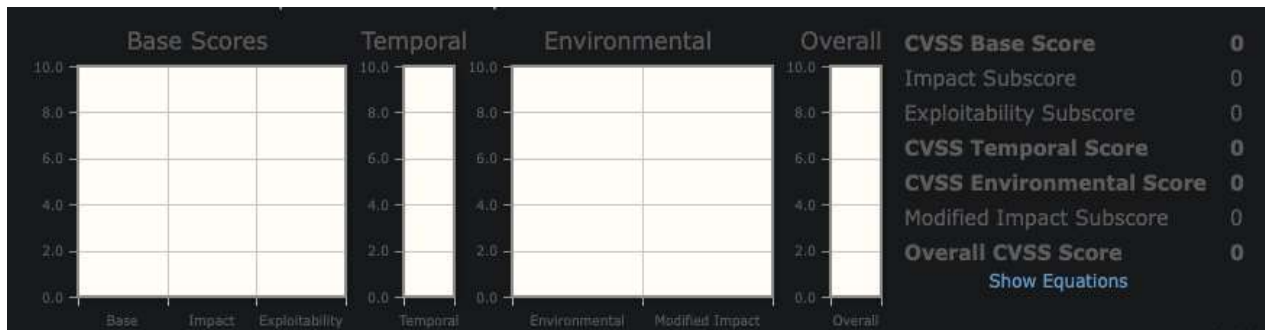


Figure 3.2.1: Graph & Analysis Area

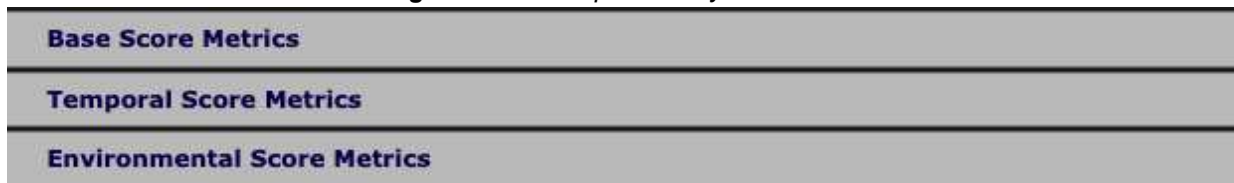


Figure 3.3.1: Metrics

BASE SCORE METRICS:

Base Score Metrics

Exploitability Metrics

Access Vector (AV)*

Local (AV:L) Adjacent Network (AV:A) Network (AV:N)

Access Complexity (AC)*

High (AC:H) Medium (AC:M) Low (AC:L)

Authentication (Au)*

Multiple (Au:M) Single (Au:S) None (Au:N)

Impact Metrics

Confidentiality Impact (C)*

None (C:N) Partial (C:P) Complete (C:C)

Integrity Impact (I)*

None (I:N) Partial (I:P) Complete (I:C)

Availability Impact (A)*

None (A:N) Partial (A:P) Complete (A:C)

* - All base metrics are required to generate a base score.

Figure 3.4.1: Base Score Metrics

Base Score Metrics allows users to create Exploitability Metrics and Impact Metrics, based on which the bar graph is generated. (see the first image on next page)

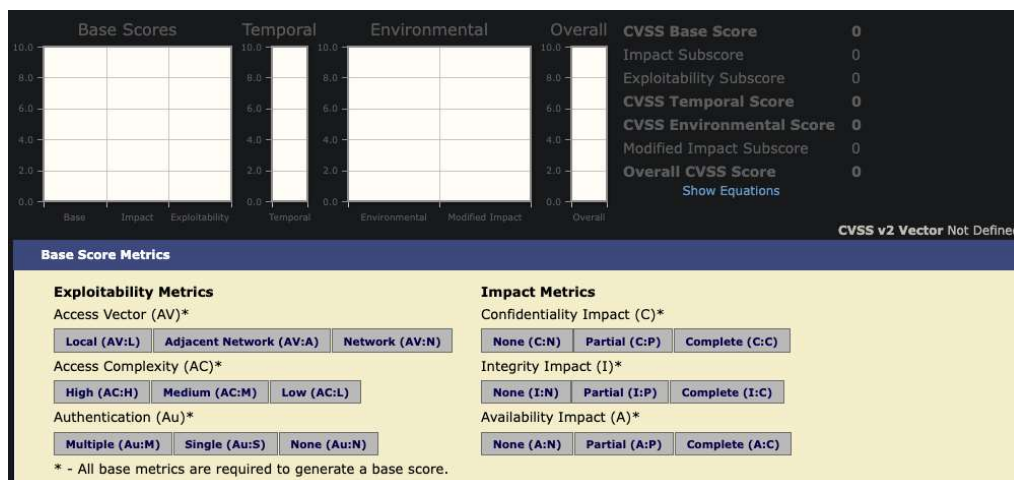


Figure 3.1.2: CVSS – 2 Calculator – graph, Analysis and Base Score Matrices

This graph is based on the input selected in the Base Score Metrics. On the right hand side it displays the result in simple English terms.

NOTE: no matter whether the user uses all the metrics or just one, the base metrics MUST have input in order to see the results. If the base metrics tab does not have input, the other two metrics will not show the results. Base metrics is base for the other two metrics

On the right hand side under the overall CVSS Score (see the following image), there is a link that says “Show Equations”, by clicking that link, it will popup a small dialog box which shows the equation used behind the calculation with all the details regarding the math behind it. (see image below)



DRAFT CVSS v2.10 Equations (last revised 3-20-07)

CVSS Base Score Equation

```

BaseScore = (.6*Impact +.4*Exploitability-1.5)*f(Impact)
Impact = 10.41 * (1 - (1 - ConfImpact) * (1 - IntegImpact) * (1 - AvailImpact))
Exploitability = 20 * AccessComplexity * Authentication * AccessVector
f(Impact) = 0 if Impact=0; 1.176 otherwise
AccessComplexity = case AccessComplexity of
    high: 0.35
    medium: 0.61
    low: 0.71
Authentication = case Authentication of
    Requires no authentication: 0.704
    Requires single instance of authentication: 0.56
    Requires multiple instances of authentication: 0.45
    
```

Close

Figure 3.2.2:
Equation insight

Exploitability Metrics provides inputs for Access Vector (AV), Access Complexity (AC), Authentication (Au); whereas,

Impact Metrics provides inputs for Confidentiality Impact (C), Integrity Impact (I), Availability Impact (A).

Base Score Metrics

<p>Exploitability Metrics</p> <p>Access Vector (AV)*</p> <p>Local (AV:L) Adjacent Network (AV:A) Network (AV:N)</p> <p>Access Complexity (AC)*</p> <p>High (AC:H) Medium (AC:M) Low (AC:L)</p> <p>Authentication (Au)*</p> <p>Multiple (Au:M) Single (Au:S) None (Au:N)</p>	<p>Impact Metrics</p> <p>Confidentiality Impact (C)*</p> <p>None (C:N) Partial (C:P) Complete (C:C)</p> <p>Integrity Impact (I)*</p> <p>None (I:N) Partial (I:P) Complete (I:C)</p> <p>Availability Impact (A)*</p> <p>None (A:N) Partial (A:P) Complete (A:C)</p>
---	--

* - All base metrics are required to generate a base score.

Figure 3.4.2: Base Score Metrics

TEMPORAL SCORE METRICS

Temporal Score Metrics provides input for Exploitability (E), Remediation Level (RL), Report Confidence (RC).

After selecting the inputs, the bar graph in Temporal raises in blue. As mentioned earlier, base metrics must have inputs in order for Temporal Score Metrics to output its results on the bar graph.



Figure 3.2.2: Graph & Analysis Area - Temporal

Base Score Metrics

Exploitability Metrics

Access Vector (AV)*

Access Complexity (AC)*

Authentication (Au)*

* - All base metrics are required to generate a base score.

Impact Metrics

Confidentiality Impact (C)*

Integrity Impact (I)*

Availability Impact (A)*

Temporal Score Metrics

Exploitability (E)

Remediation Level (RL)

Report Confidence (RC)

Figure 3.1.3: CVSS – 2 Calculator – Base & Temporal Score Matrices

Environmental Score Metrics provides **General Modifiers**, and **Impact Sub score Modifiers**. **General Modifiers** provide the input list as follows: Collateral Damage Potential (CDP), Target Distribution (TD); whereas, **Impact Sub-score** provides Confidentiality Requirement (CR), Integrity Requirement (IR), Availability Requirement (AR).

Once the input was entered in the base score matrices and Environmental Score Metrics, two bar graphs in Environmental raise up, one for Environmental and Modified impact.

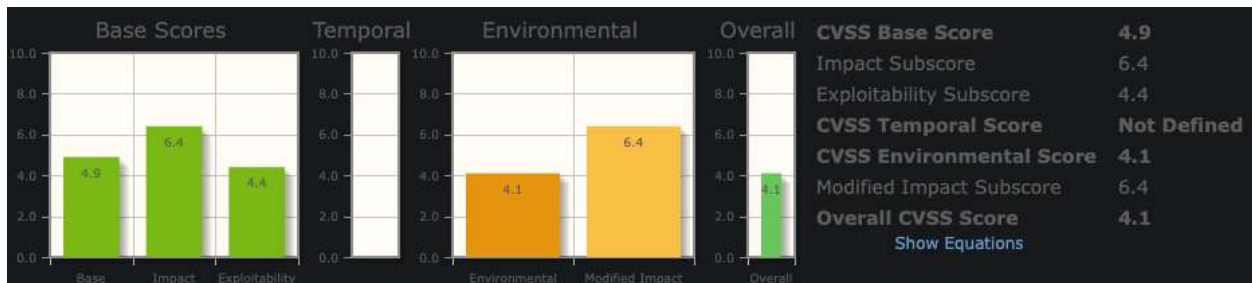


Figure 3.2.3: Graph & Analysis Area – Environmental

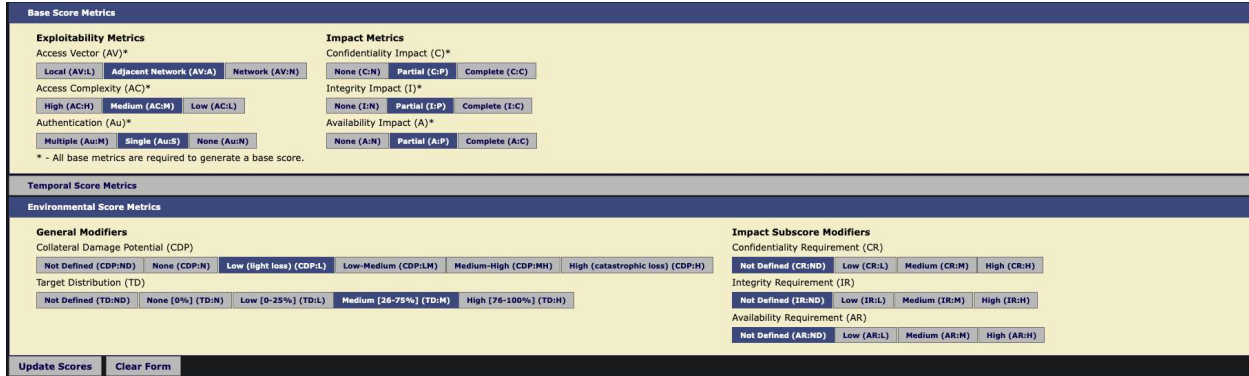


Figure 3.1.4: CVSS – 2 Calculator – Base & Environmental Score Matrices

PASSWORD RANDOMIZER:



Figure 4.1.1: Password Randomizer

This is one of the smallest and simplest features of CheckMate. Password generator creates a password for the user. Password generator has 5 options, which let you select how long and what kind of characters you want in your password, and the password generator will randomly generate a password for you. Users can use this password for literally anything, such as social media, emails, bank account, etc.

The numbers in the small boxes, in the above image, are the place holder or default values that tells the Random Generator about how many characters of each kind to use. For instance, in the above image, the random generator is using 5 lowercase characters, 5 uppercase, 3 numbers characters, 1 special character and 1 password (like space). And the total of these numbers is the total length of the password, so in this case we have: $5+5+3+1+1 = 15$.

Clock

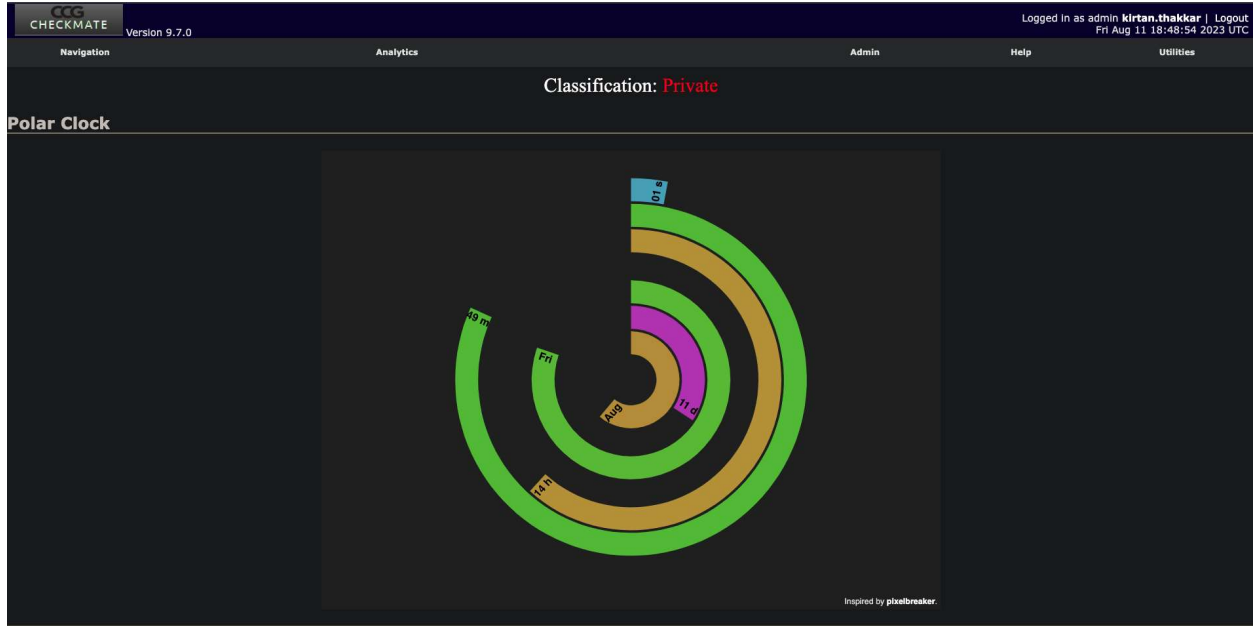
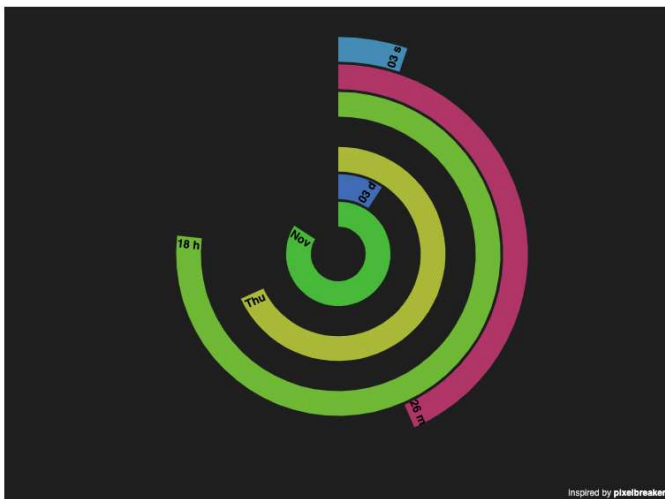


Figure 5.1.1: Clock

Above image is a polar clock. A polar clock is a clock that shows the time data from month through the current second. Below is the list of what each different colored strip represents (from most inner strips through most outer strips).



1. Month
2. n^{th} Day of the month
3. Week days
4. Hours
5. Minute
6. Second

FAQ

- **Why is my checkmate sometimes delayed in displaying the threats?**

It has to do with the timezone, if your desktop is using any time zone other than UTC, will need to calculate the difference in order to get your accurate time.