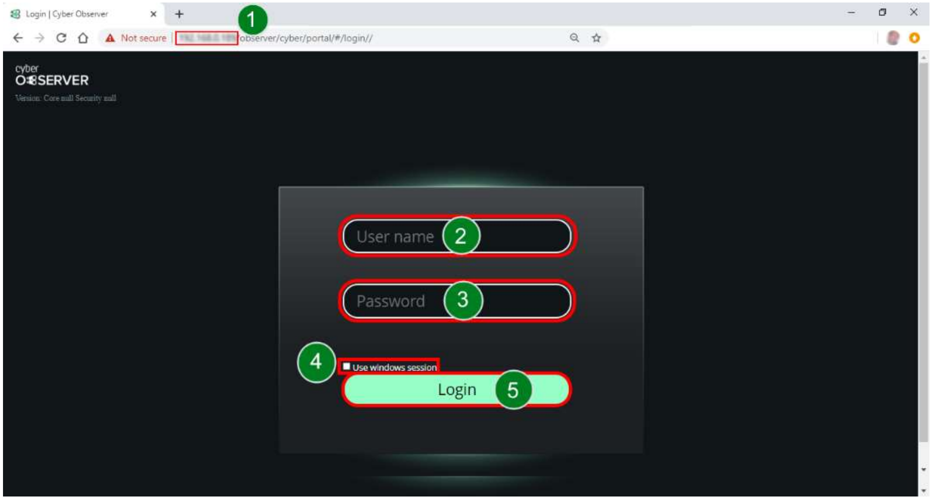
1 Checking Your Cyber Defense Status

Cyber Observer automatically assesses your security ecosystem and evaluates each domain. It then provides a score so that you can quickly identify areas that are properly covered and those that need improvement.

1.1 Log on to the system

The Cyber Observer system runs on a server that processes the events it receives from the cybersecurity and related tools in the organization's network. As a server, it is accessed through own IP address. To log on to Cyber Observer:

1. Open an internet browser and enter the **IP address** of the Cyber Observer server into the URL address line (1).
2. The browser window shows the login dialog to log on to the Cyber Observer server.



3. Enter your **User name** (2) and **Password** (3) into the relevant fields.
4. If you are logging on using the Active Directory account, then tick the **Use windows session** checkbox (4). See description of Single Sign On
5. Click **Login** to enter the Cyber Observer server.

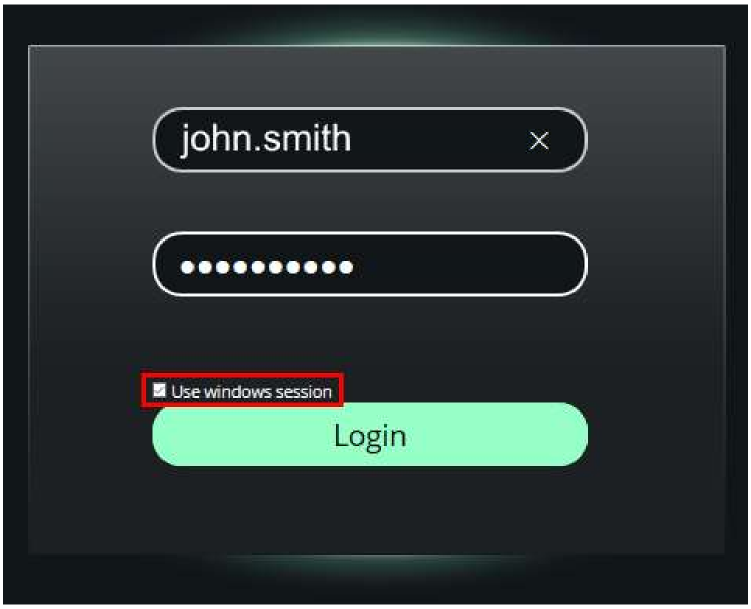
NOTE: cyber observer supports Active Directory and local users authentication. For more information see

1.1.2 Single Sign On

An authorized user can log on to the Cyber Observer server's domain with a Single Sign On.

The login dialog that appears when opening Cyber Observer includes the Use windows session checkbox.

Ticking this checkbox logs on to all the servers in the same domain as Cyber Observer.



1.2 Cyber Observer Status Bar

The status bar indicates the number of tools with which Cyber Observer cannot connect. This status bar appears at the top of every page so that you will always know if there is a connection error that requires your attention.

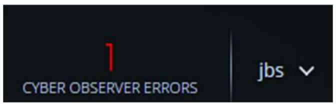
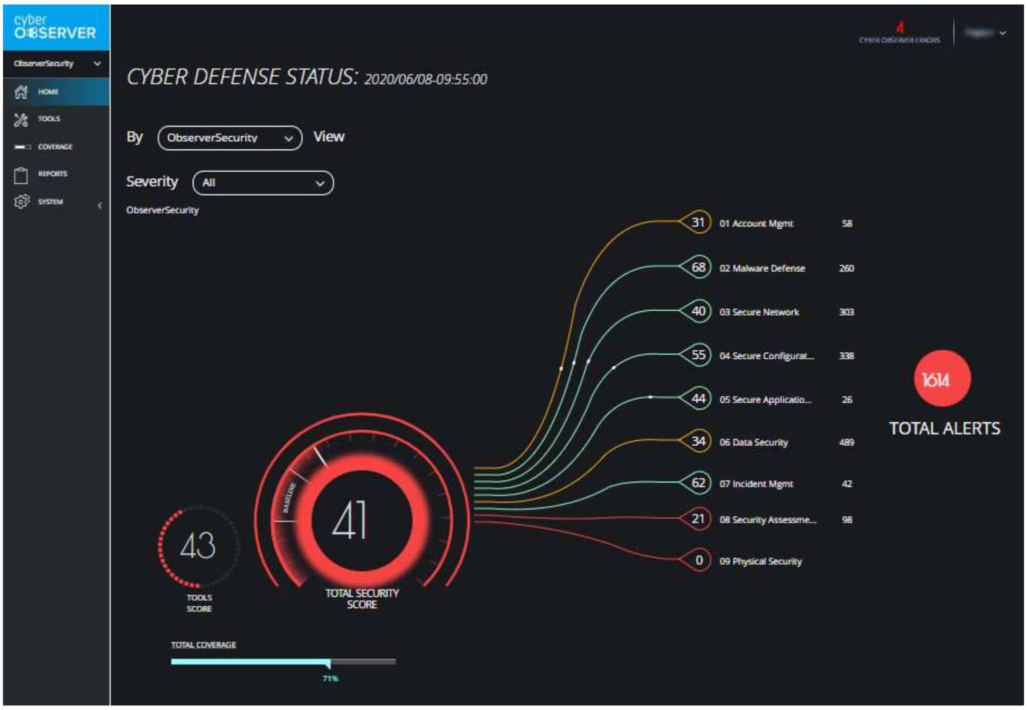


Figure 1 Number of disconnected tools

1.3 Cyber Defense Status

The **HOME** page displays a detailed view of the current status of your organization's cyber defense.



CYBER DEFENSE STATUS: 2020/06/08-09:55:00

By ObserverSecurity View

Severity All

ObserverSecurity

31	01 Account Mgmt	58
68	02 Malware Defense	260
40	03 Secure Network	303
55	04 Secure Configurat...	338
44	05 Secure Applicatio...	26
34	06 Data Security	489
62	07 Incident Mgmt	42
21	08 Security Assessme...	98
0	09 Physical Security	

Figure 2 Cyber Defense Status

Element	Description
1	Filter by View and by Severity
2	The domain's cyber defense score, domain type, and CSC alerts for that domain
3	Total number of alerts for all domains
4	Tools Score
5	Total Score
6	Coverage

The following sections describe each of these in more detail.

1.3.1 Filtering by View

By default, the data displayed in the Cyber Defense Status on the **HOME** page is based on the internal Observer Security View. However, you can filter the data to display the statistics according to various Views.

When you filter by a View:

- All of the statistics on the **HOME** page change to show how much they comply with the selected View
- The View in the menu shows the current View.

Figure 3 Selected View appears at the top of the menu

To filter by a View:

On the **HOME** page, from the **By View** dropdown list, select a View.

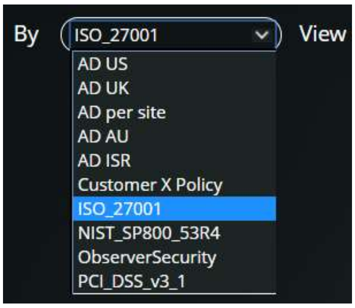


Figure 4 Filtering by a View

> **Note**
>
> The Views displayed in this list depend on user permissions. See section שגיאה! מקור ההפניה לא נמצא. “שגיאה! מקור ההפניה לא נמצא.”.
>
> **Note**
>
> The views that appear in the home screen rotate, changing the view that appears. See שגיאה! מקור ההפניה לא נמצא..

For information about configuring Views, see section שגיאה! מקור ההפניה לא נמצא. “שגיאה! מקור ההפניה לא נמצא.”.

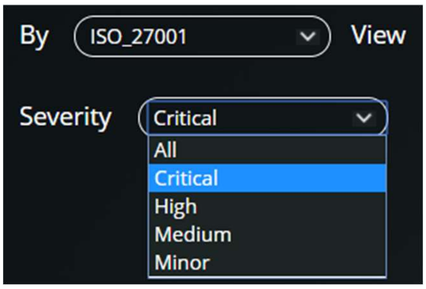
1.3.2 Filtering by Alert Severity

By default, all statistics are displayed on the **HOME** page, regardless of their severity. However, you might only want to see alerts that are categorized as critical, high, medium, or minor.

When you filter the statistics displayed by alert severity, alerts that are at least the selected severity are displayed on the Home page. For example, you can show only **Critical** or **High** alerts in a particular view, enabling you to deal with the most urgent alerts.

To filter by alert severity:

On the **HOME** page, from the Severity dropdown list, select a level of severity.



By ISO_27001 View

Severity Critical

Figure 5 Filtering by severity

1.3.3 Domain Alerts

The **HOME** page displays a list of all of the domains that the defined view is tracking. Each domain is color-coded so that you can instantly see which ones have alerts associated with them.

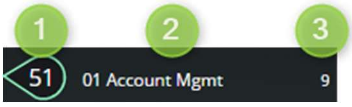
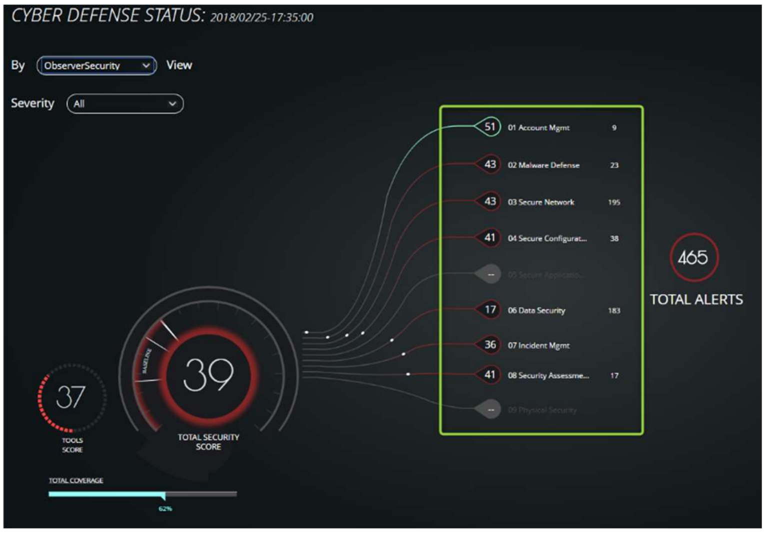


Figure 6 Domains (HOME page)

1. The domain's cyber defense score.
2. The security domain.
3. The number of CSCs associated with that domain that are alerting.



CYBER DEFENSE STATUS: 2018/02/25-17:35:00

By ObserverSecurity View

Severity All

51 01 Account Mgmt 9
43 02 Malware Defense 23
43 03 Secure Network 195
41 04 Secure Configurat... 38
-- 05 Secure Applicatio...
17 06 Data Security 183
36 07 Incident Mgmt
41 08 Security Assessme... 17
-- 09 Physical Security

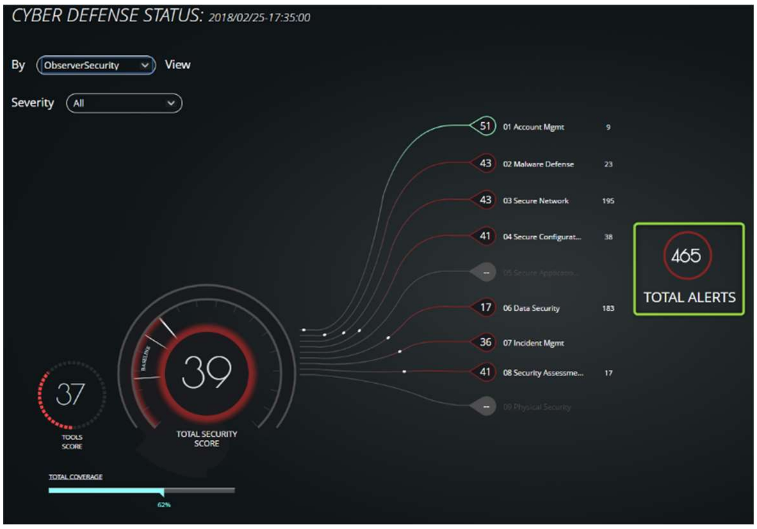
replace picture with more colors (less red)

Figure 7 Domains

For more information about a domain, click its score or the name of the domain (see section שגיאה! מקור ההפניה לא נמצא. “שגיאה! מקור ההפניה לא נמצא.”).

1.3.4 Total Alerts

TOTAL ALERTS is the aggregate of all of the CSC alerts detected for all domains in the current view.



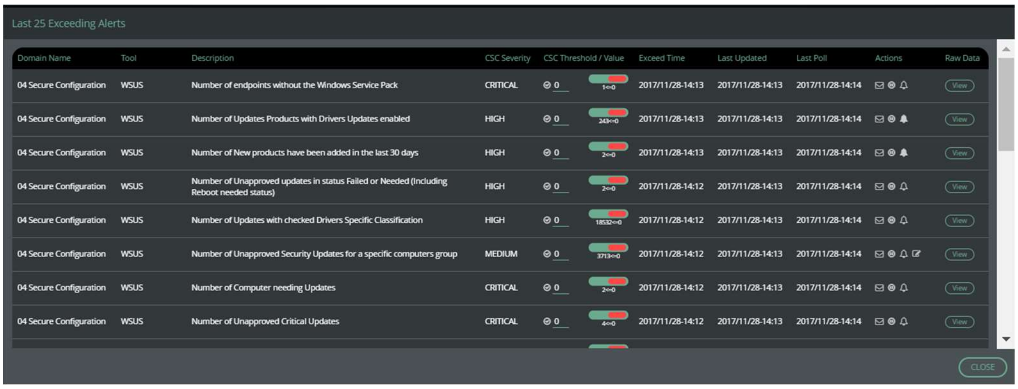
CYBER DEFENSE STATUS: 2018/02/25-17:35:00

By ObserverSecurity View

Severity All

Figure 8 Total number of alerts

To find out more information about the **TOTAL ALERTS**, click it. The last 25 alerts are displayed.



Last 25 Exceeding Alerts

Domain Name	Tool	Description	CSC Severity	CSC Threshold / Value	Exceed Time	Last Updated	Last Poll	Actions	Raw Data
04 Secure Configuration	WSUS	Number of endpoints without the Windows Service Pack	CRITICAL	0 1<=0	2017/11/28-14:13	2017/11/28-14:13	2017/11/28-14:14		View
04 Secure Configuration	WSUS	Number of Updates Products with Drivers Updates enabled	HIGH	0 243<=0	2017/11/28-14:13	2017/11/28-14:13	2017/11/28-14:14		View
04 Secure Configuration	WSUS	Number of New products have been added in the last 30 days	HIGH	0 2<=0	2017/11/28-14:13	2017/11/28-14:13	2017/11/28-14:14		View
04 Secure Configuration	WSUS	Number of Unapproved updates in status Failed or Needed (Including Reboot needed status)	HIGH	0 2<=0	2017/11/28-14:12	2017/11/28-14:13	2017/11/28-14:14		View
04 Secure Configuration	WSUS	Number of Updates with checked Drivers Specific Classification	HIGH	0 18532<=0	2017/11/28-14:12	2017/11/28-14:13	2017/11/28-14:14		View
04 Secure Configuration	WSUS	Number of Unapproved Security Updates for a specific computers group	MEDIUM	0 3713<=0	2017/11/28-14:12	2017/11/28-14:13	2017/11/28-14:14		View
04 Secure Configuration	WSUS	Number of Computer needing Updates	CRITICAL	0 2<=0	2017/11/28-14:12	2017/11/28-14:13	2017/11/28-14:14		View
04 Secure Configuration	WSUS	Number of Unapproved Critical Updates	CRITICAL	0 4<=0	2017/11/28-14:12	2017/11/28-14:13	2017/11/28-14:14		View

Figure 9 List of the last 25 alerts for all domains

- **Domain Name:** The domain where the alert was identified.
- **Tool:** The tool in which the alert was identified.
- **Description**: A description of the CSC.
- **CSC Severity**: The importance of the alert: Critical, High, Medium, or Minor.
- **CSC Threshold/Value**: The CSC value that Cyber Observer platform is expecting from the tool, compared with the value that was gathered. To stop generating alerts for this CSC, set the threshold to the expected value.

Symbol	Definition
🟥	▪ There was no option to retrieve information from the tool ▪ This feature is not being used in the connected tool

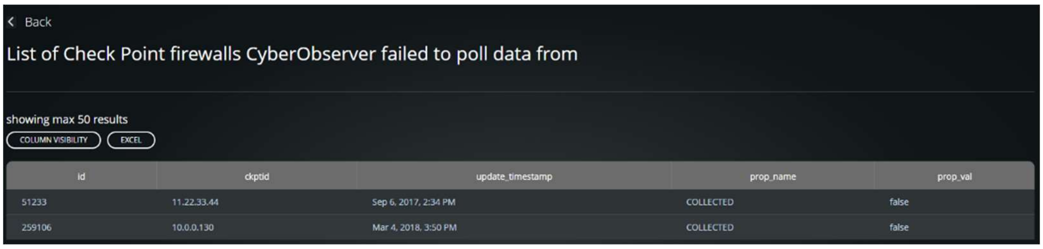
▬	■ The current user does not have permissions to view this information
🟩	No issues detected
🟥	There is a problem that needs to be fixed.
🟨	A yellow background indicates that there is a problem with the data (data integrity) and the information cannot be displayed properly.

- **Exceed Time:** The date and time that the threshold for this CSC was exceeded.
- **Actions**: Actions that you can take for this CSC:

Symbol	Definition
⚙	Change the CSC settings
ℹ	Add free-text comments to the CSC
✉	Manually create a ticket that will be sent by email to your organization's ticketing system
⏸	Pause the CSC; the CSC will not affect the Security Score of the domain that the specific CSC belongs to.
🔔	Send an automatic email to the tool owner if the CSC exceeds a certain threshold
✎	Configure the CSC to include or exclude certain types of data

> **Note**
>
> Not all actions are available for all CSCs.

- **Raw Data:** Click the **View** button in this column to view the raw data associated with this CSC alert.



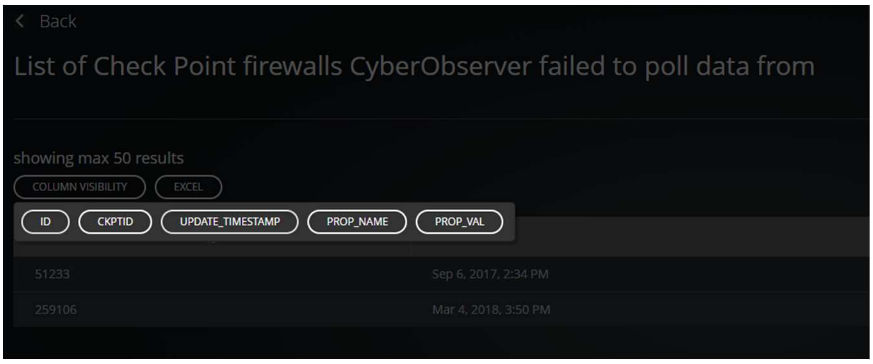
List of Check Point firewalls CyberObserver failed to poll data from

showing max 50 results

id	ckptid	update_timestamp	prop_name	prop_val
51233	11.22.33.44	Sep 6, 2017, 2:34 PM	COLLECTED	false
259106	10.0.0.130	Mar 4, 2018, 3:50 PM	COLLECTED	false

Figure 10 Raw data for a CSC alert

- To set which columns are shown, click **COLUMN VISIBILITY** and click the column names to show or hide them.



< Back

List of Check Point firewalls CyberObserver failed to poll data from

showing max 50 results

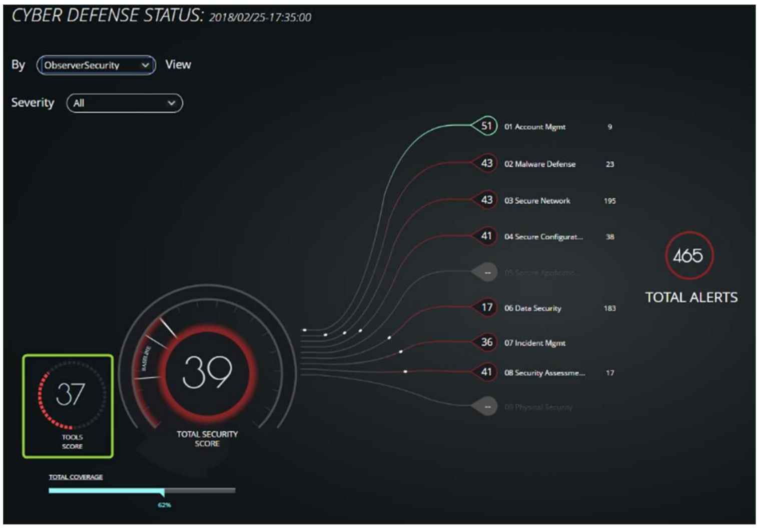
51233	Sep 6, 2017, 2:34 PM
259106	Mar 4, 2018, 3:50 PM

Figure 11 Show or hide raw data columns

- To download the raw data as a CSV file, click **EXCEL**.

1.3.5 Tools Security Score

Cyber Observer assigns a score to each of the cyber defense tools you have installed and are tracking. This score is the average of all individual tool scores.



CYBER DEFENSE STATUS: 2018/02/25-17:35:00

By ObserverSecurity View

Severity All

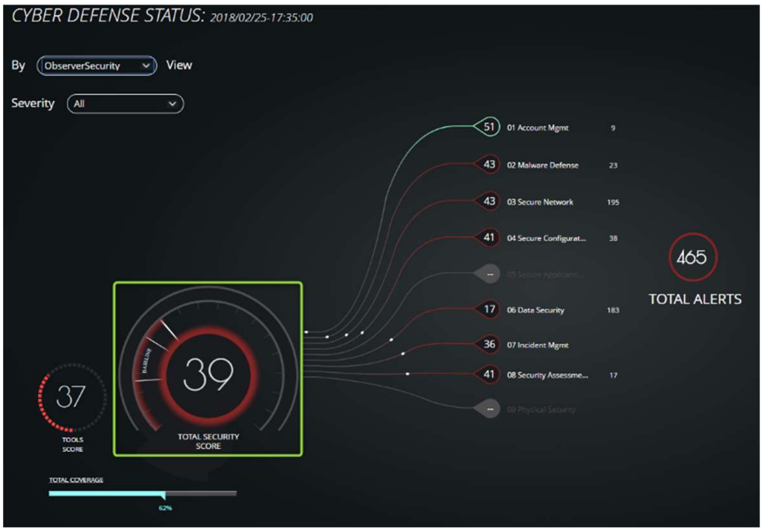
Replace picture

Figure 12 Tools Score

To find out more information about the **TOOLS SCORE**, click it. The **TOOLS SCORE** page opens (see section שגיאה! מקור ההפניה לא נמצא. “שגיאה! מקור ההפניה לא נמצא.”).

1.3.6 Total Security Score

The **TOTAL SECURITY SCORE** is a score out of 100 that the system calculates to rate your organization's cyber defense status. It is based on all of the individual domain scores. The higher the score, the more protected your organization is.



CYBER DEFENSE STATUS: 2018/02/25-17:35:00

By ObserverSecurity View

Severity All

51	01 Account Mgmt	9
43	02 Malware Defense	23
43	03 Secure Network	195
41	04 Secure Configurat...	38
--	05 Secure Applicatio...	
17	06 Data Security	183
36	07 Incident Mgmt	
41	08 Security Assessme...	17
--	09 Physical Security	

Figure 13 Total Score

1.3.6.1 Baseline

It is expected that the scores for each domain will fluctuate within a certain acceptable range, affecting the **TOTAL SECURITY SCORE**. This acceptable range is called the baseline. The baseline is calculated by Cyber Observer as it learns your organization's usage patterns. It is based on the trending CSC alerts in all of the domains.

As soon as Cyber Observer detects a change in daily behavior, it sends an email alert to a predefined list of managers. These managers will verify the reason for the change in behavior as soon as possible.

It is recommended that you check which new CSCs are exceeding their baseline. To do this, click **TOTAL ALERTS**.

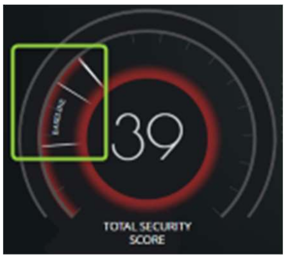
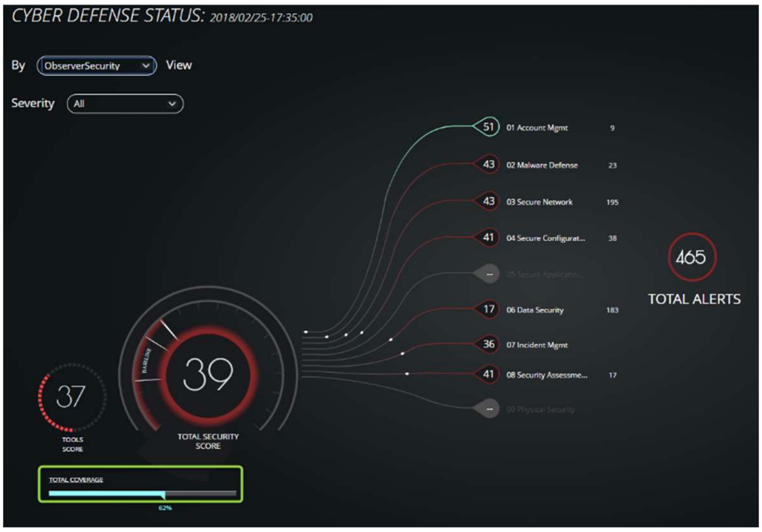


Figure 14 Baseline

1.3.7 Total Coverage

The **TOTAL COVERAGE** score indicates how protected your organization is by the security tools that are connected to the Cyber Observer system, and which tool capabilities the system recommends that you add.

The score is the maximum **TOTAL SECURITY SCORE** you can reach once all of the CSC alerts are properly resolved.



CYBER DEFENSE STATUS: 2018/02/25-17:35:00

By ObserverSecurity View

Severity All

51	01 Account Mgmt	9
43	02 Malware Defense	23
43	03 Secure Network	195
41	04 Secure Configurat...	38
--	05 Secure Applicatio...	
17	06 Data Security	183
36	07 Incident Mgmt	
41	08 Security Assessme...	17
--	09 Physical Security	

Figure 15 Total Coverage

To find out more information about the **TOTAL COVERAGE** score, click it. The Total Coverage page opens (see section שגיאה! מקור ההפניה לא נמצא. “שגיאה! מקור ההפניה לא נמצא.”).