COMODO
Creating Trust Online®

Comodo
cWatch MDR
Software Version 2.23

Administrator Guide
Guide Version 2.23.062520

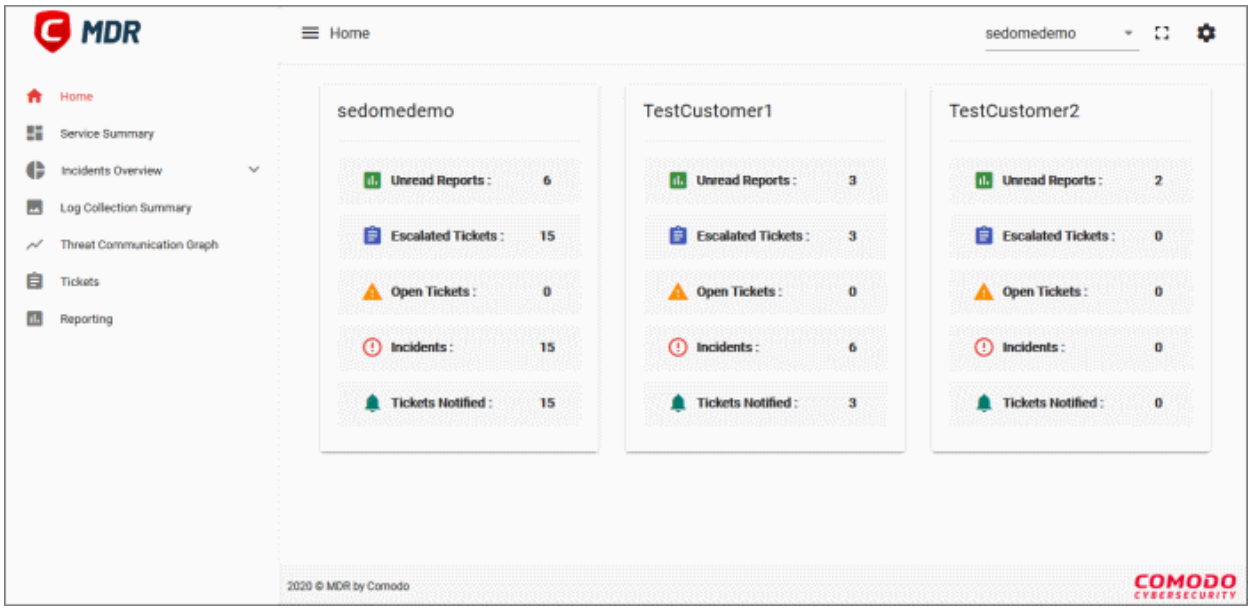
Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

Table of Contents

1 Introduction to Comodo cWatch MDR

cWatch Managed Detection & Response (MDR) shows threats and behavioral anomalies detected on your network and managed endpoints. Featuring 24/7 threat monitoring and comprehensive reports, cWatch MDR provides the network-wide intelligence admins need to remediate existing threats and anticipate future threats.

Leveraging a combination of technologies deployed at the host and network layers, advanced analytics, threat intelligence, and human expertise in incident investigation with Comodo's 24/7 Security Operations Center (SOC) service, MDR is a comprehensive security solution.



Features

- Network Detection & Response
- Endpoint Detection & Response
- Web Detection & Response
- Cloud Detection & Response
- Real-time event monitoring and processing
- Office 365 integration with MDR

Guide Structure

This guide is intended to take you through the configuration and use of cWatch MDR and is broken down into the following main sections.

- **Introduction to Comodo cWatch Network**
  - **Purchase a License**
  - **Log-in to the Administrative Console**
- **The Home Screen**
- **Service Summary**
- **Incidents Overview**
- **Log Collection Summary**
- **Threat Communication Graph**
- **Reports**

1.1 Purchase a License

You can purchase MDR licenses via Comodo One, Comodo Dragon and ITarian portals.

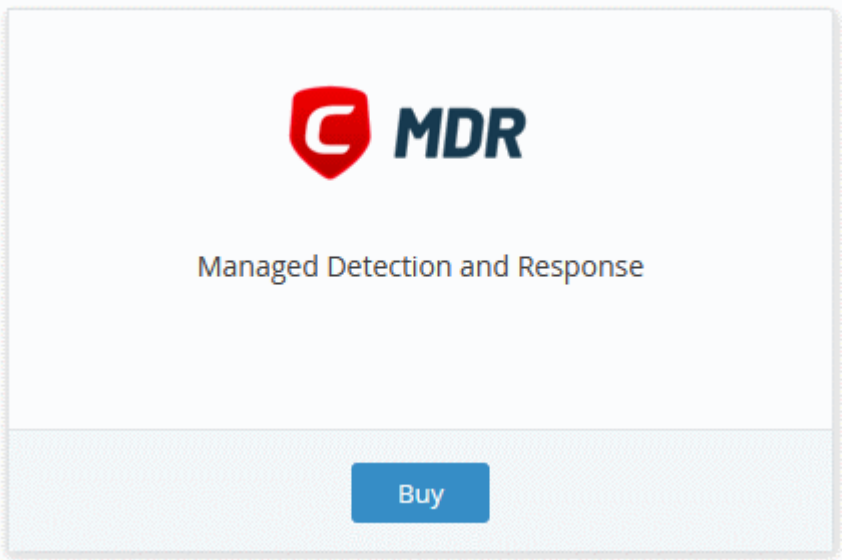
- Open the 'Store' areas of Comodo One, Comodo Dragon and ITarian to subscribe for MDR licenses.
  - **Click here** to know how to sign up for a free C1 account
  - **Click here** for details about how to sign up for a free Comodo Dragon account.
  - **Click here** to know how to sign up for a free ITarian account

There are two variants of the MDR module:

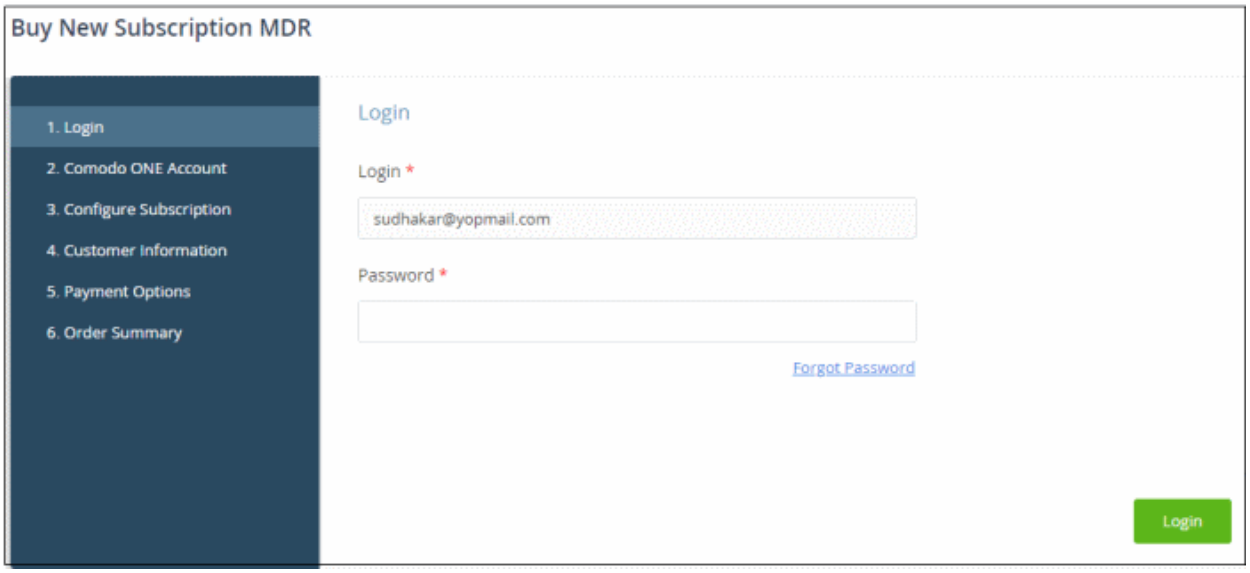
- **MDR Force Protect Endpoint** – MDR receives logs from the Comodo Client Security (CCS) installations on the managed endpoints for processing. Comodo's SOC team will analyze and provide insight about internal threats. Contact your account manager for configuring your endpoints to forward logs to MDR.
- **MDR Force Detect Network** – MDR receives logs from sensors installed on your networks for processing. Comodo's SOC team will analyze and provide insight about threats on your networks. Contact your account manager for provisioning sensors on your networks.

Purchasing is the same for both Comodo One, Comodo Dragon and ITarian. The following tutorial explains how to subscribe via Comodo One.

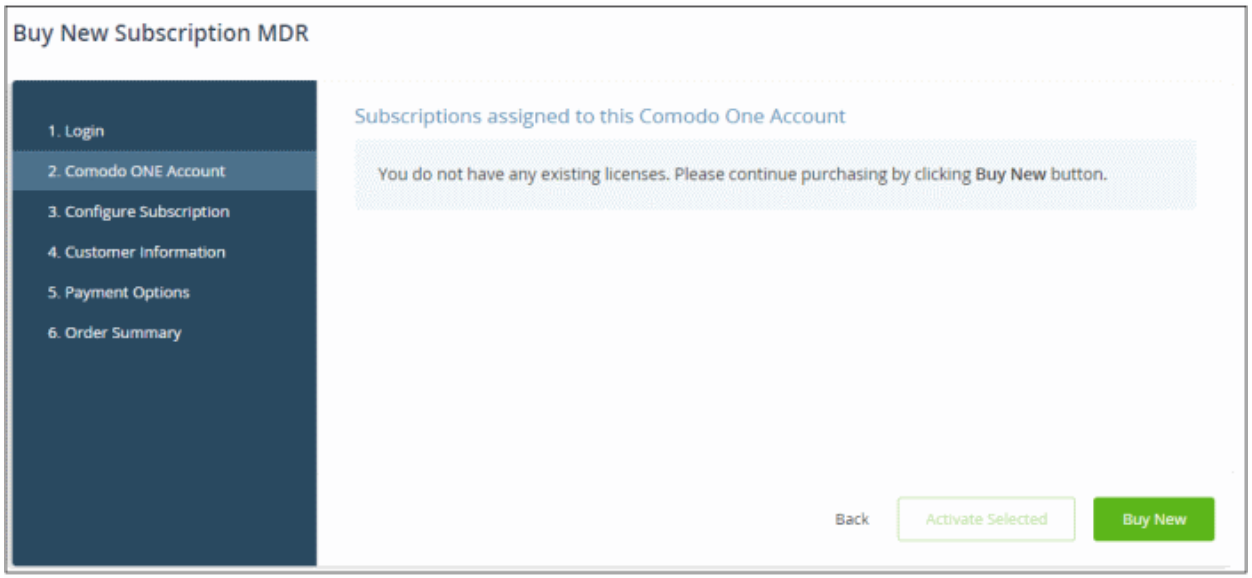
- Login to your **Comodo One** / **Comodo Dragon** / **ITarian** account
- Click 'Store' on the menu bar
- Locate the 'MDR' tile and click 'Buy'



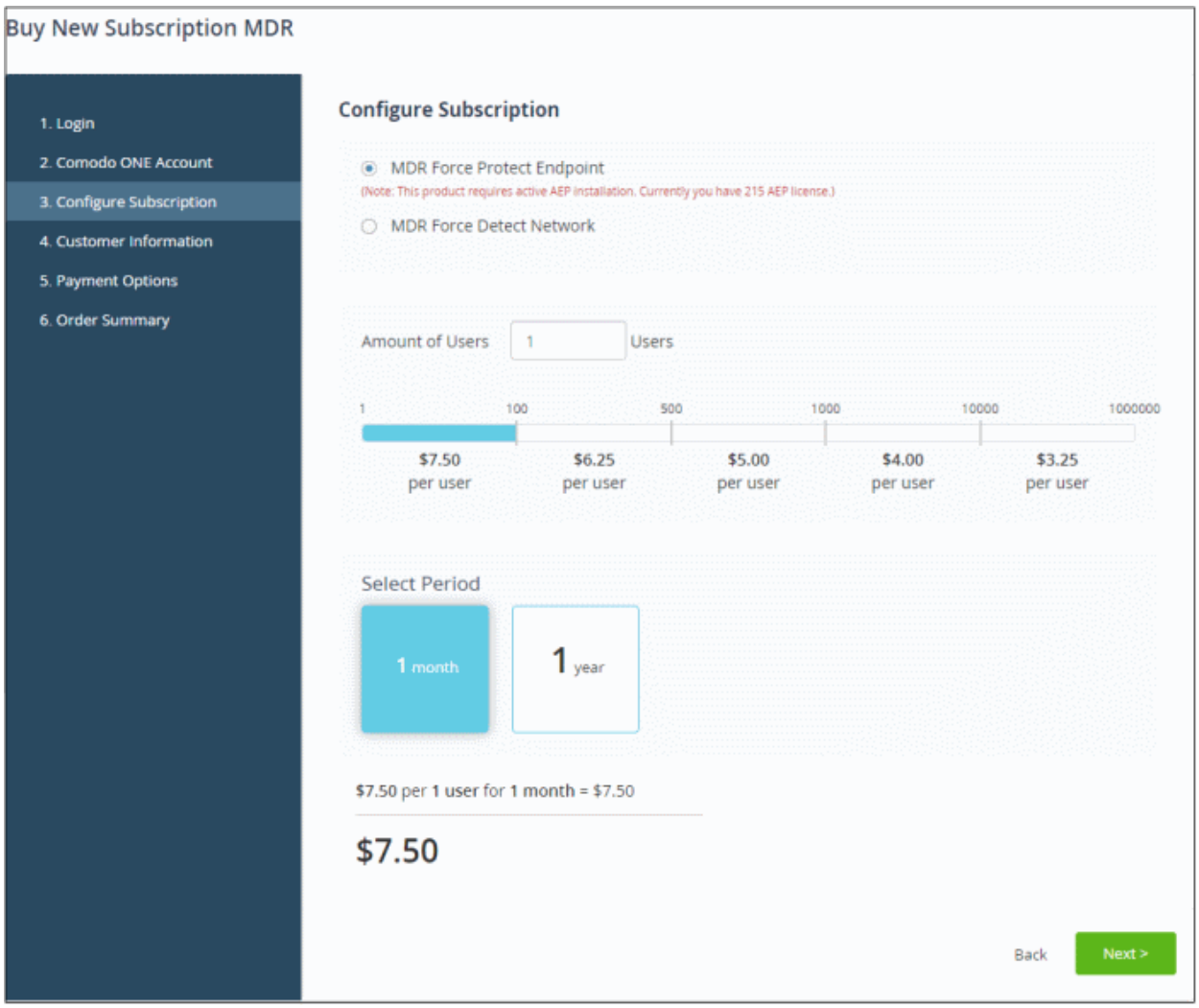
- The product order page opens:



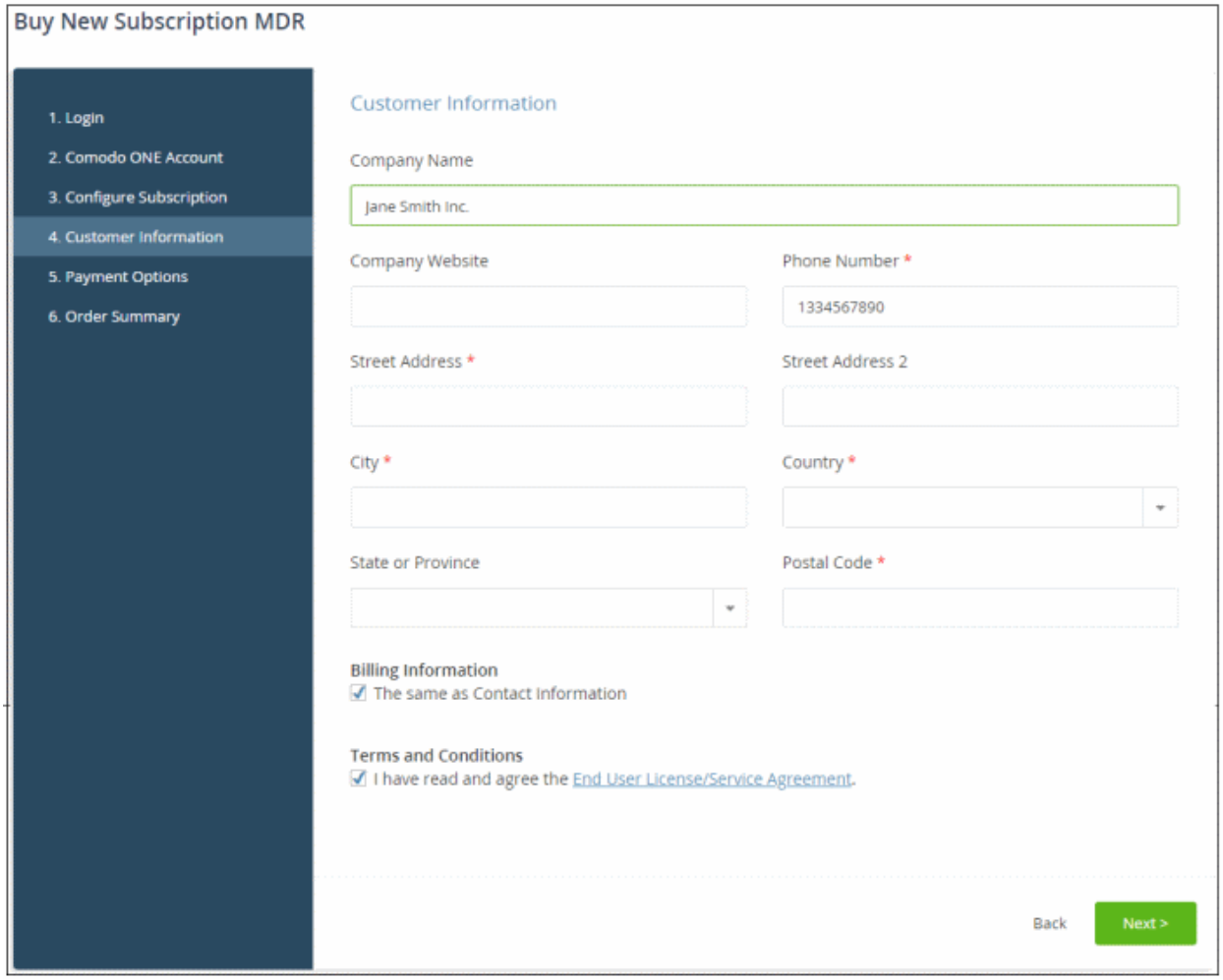
- Your username is pre-populated
- Enter your portal account password then click 'Login'



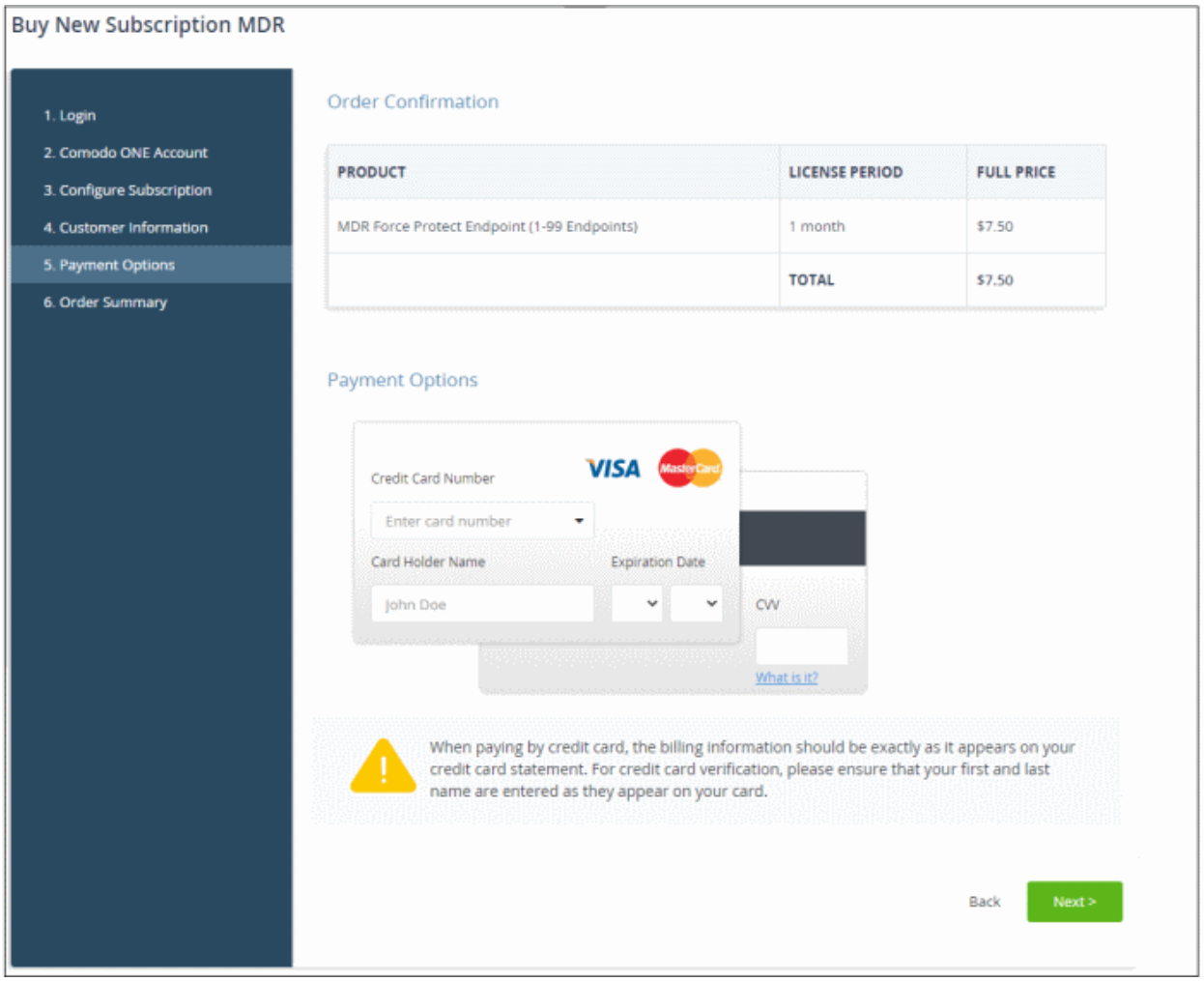
- Click the 'Buy New' button.
- The next step is to configure your subscription package:



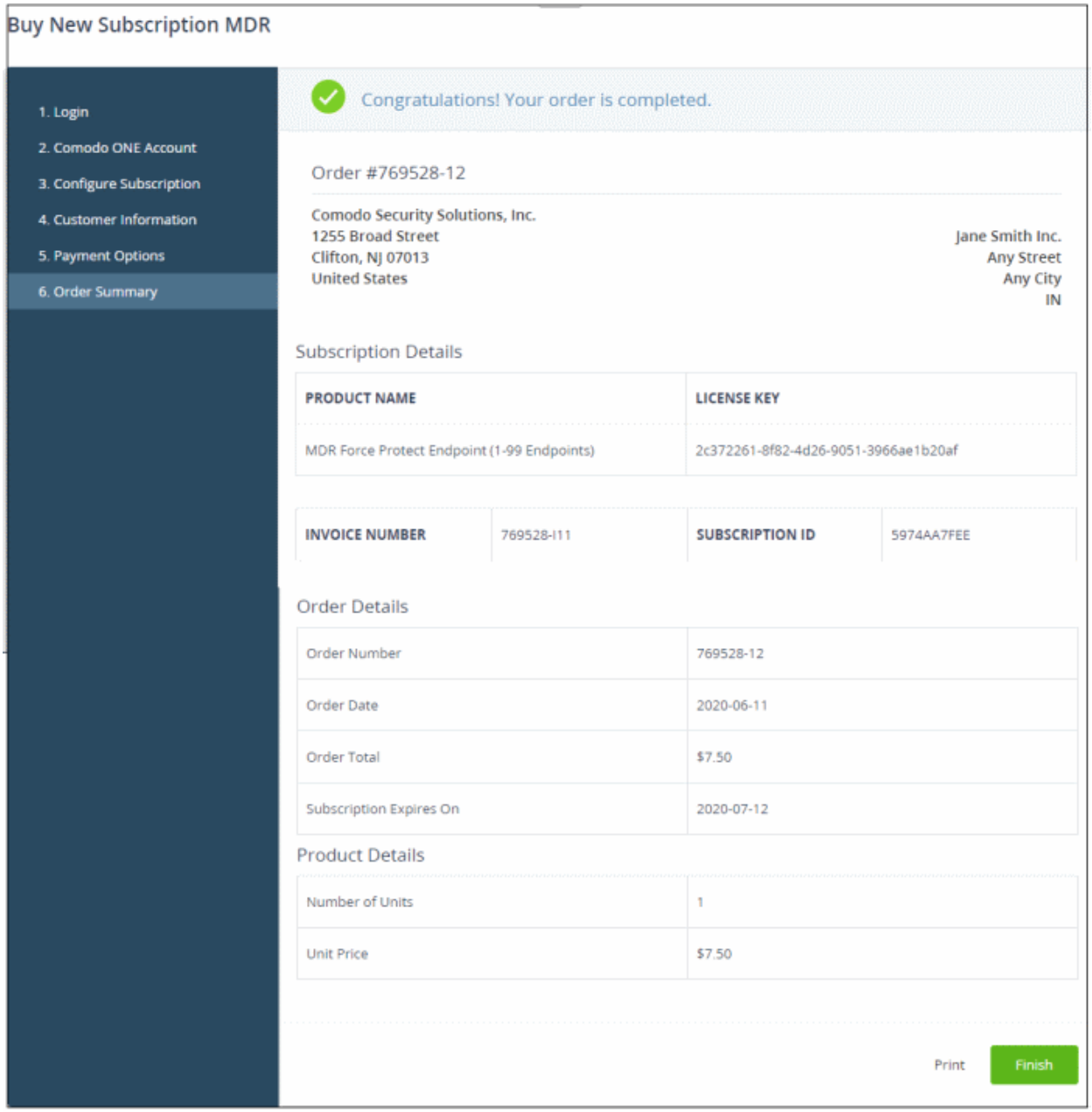
- Select the license type.
  - Note- You can buy additional license types after completing the purchase process. See at the end of this section for **more information**.
- Select the number of user licenses you require.
  - The per-user rate depends on the number of users.
- Select the license period. The minimum license period is one month.
- Click 'Next' to continue to customer information.
- Enter your company name, website and address details:



- Agree to the terms and conditions then click 'Next'



- Review your order and enter your payment details
- Click 'Next'
- Your order is submitted and processed. You will receive an order confirmation mail with your license key.
- The order summary page is shown after your order has been processed:



- Click 'Print' to make a hard-copy of the order summary.
- Click 'Finish' to complete the purchase process.

Purchase additional MDR licenses

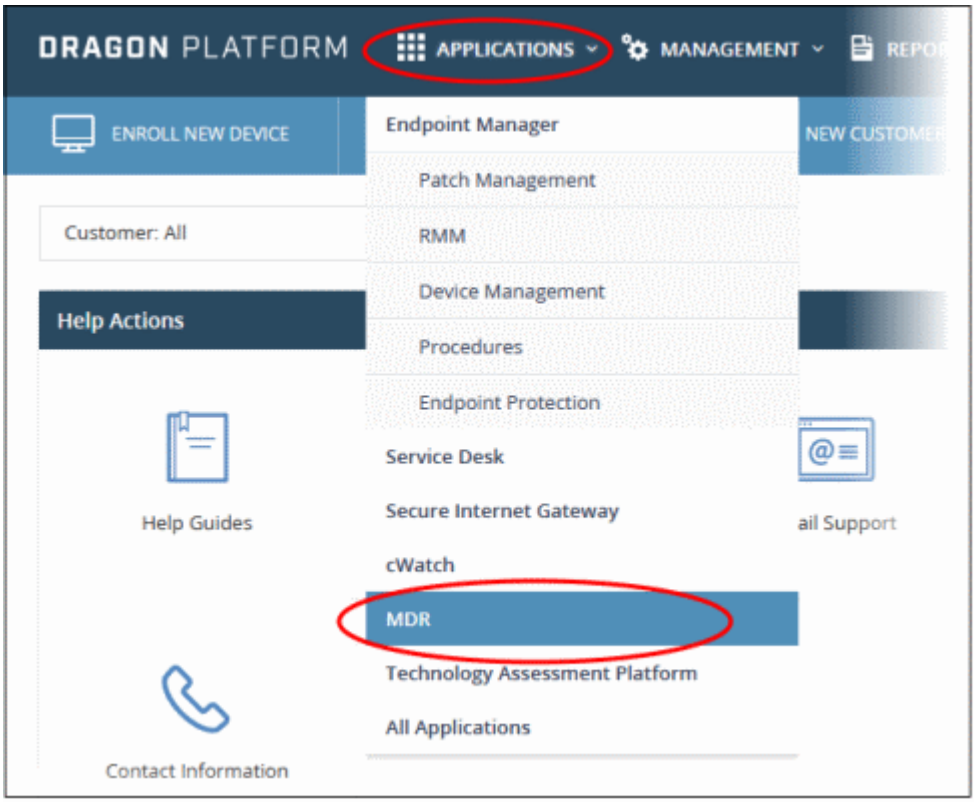
- Click 'Management' > 'Applications' on the portal menu bar
- Click the 'MDR' tile
- Click the 'Subscriptions' tab if not open already
- Click 'Add New Subscription'
- The product purchase page opens.
- Login to your account and complete the purchase process for additional / different license type as explained above.

After you subscribe for MDR, Comodo will continuously review the raw data from your instance and update MDR so it delivers the information most relevant to your needs.

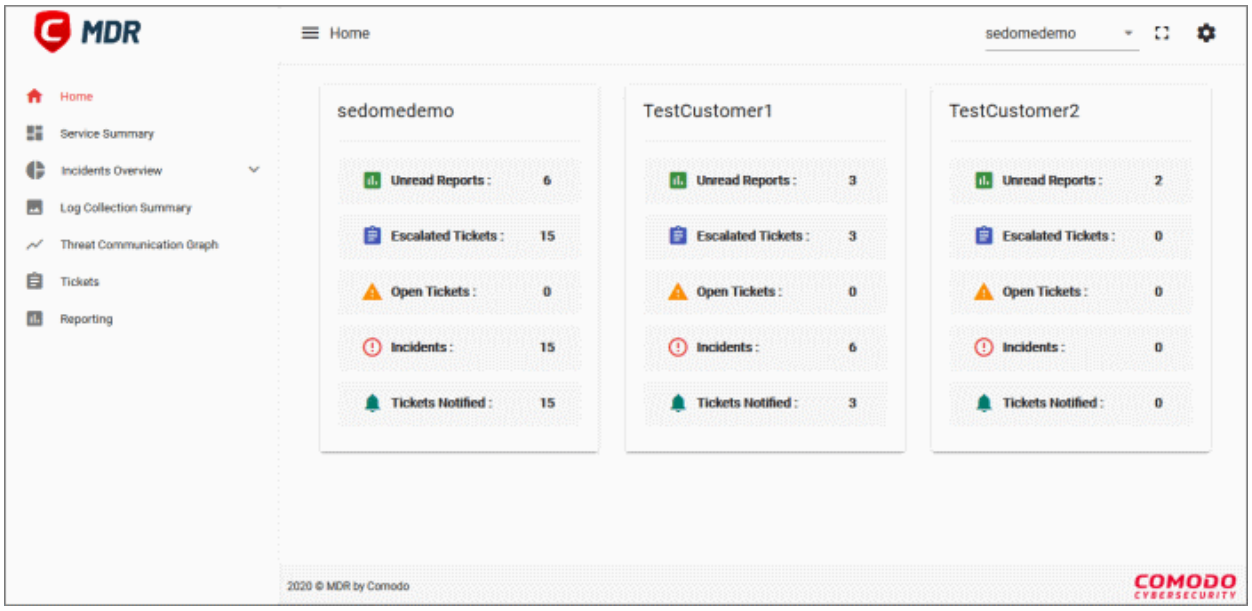
1.2 Log-in to the Admin Console

You can open the cWatch MDR admin interface after logging-in to your Comodo One / Comodo Dragon / ITarian account.

- Login to your **Comodo One** / **Comodo Dragon** / **ITarian** account
- Click 'Applications' then 'MDR'



MDR application opens at the home screen.



Note – MDR will open at the service summary screen if there is only one customer for your account.

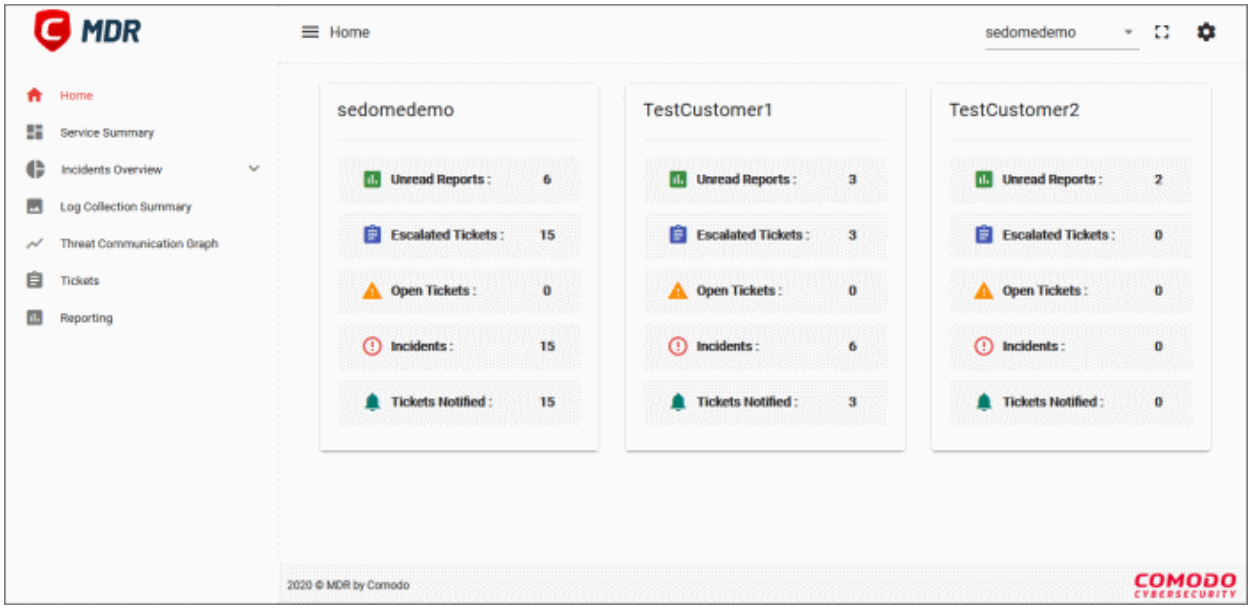
2 The Home Screen

Managed Detection & Response (MDR) is an integrated suite of managed detection-response technologies comprising Network Detection & Response (NDR), Endpoint Detection & Response (EDR), Web Detection & Response (WDR) and Cloud Detection & Response (CDR).

After you subscribe for MDR, Comodo will continuously review the raw data from your instance and update MDR so it delivers the information most relevant to your needs.

The home screen shows at-a-glance summary of customers' statistics on tiles such as incidents, tickets, reports and so on.

- Click 'Home' on the left if not already open.
  - Note- Home screen is shown if there are more than one customer for the account.



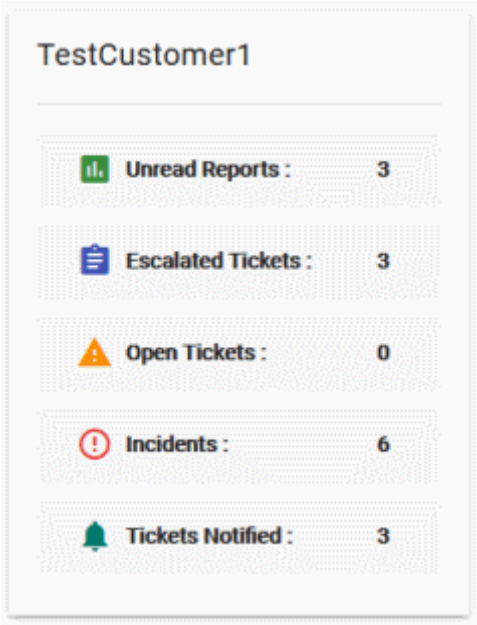
Click this to expand / collapse the left menu

Click the drop-down and select your customer

Click this button to toggle between full screen and normal

Click this button to configure **notification settings**. This area also allows you to configure to collect data from **Office 365 accounts**.

Clicking an item in each tile opens its respective section:



- **Customer name** – Clicking this will open the **service summary** screen.
- **Unread reports**- Opens the **reports** section.
- **Incidents** – Opens the **incidents** screen.
- **Escalated tickets, open tickets and tickets notified** – Opens the **tickets** section.

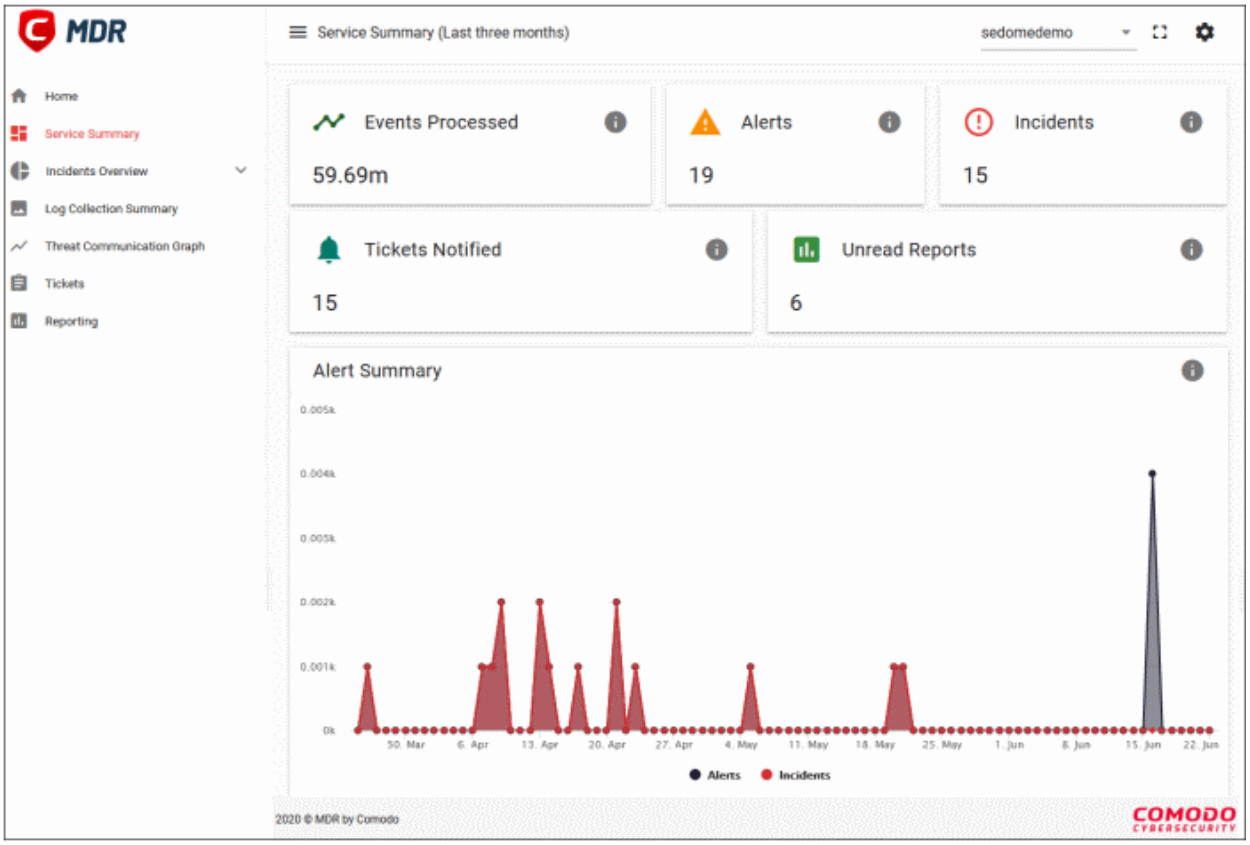
Click the following links to find out more about each interface:

- **The Home Screen**
- **Service Summary**
- **Incidents Overview**
  - **Incidents**
  - **Threat Summary**
- **Log Collection Summary**
- **Threat Communication Graph**
- **Tickets**
- **Reports**
- **Notification Settings**
- **Integrate your Office 365 Account with MDR**

3 Service Summary

The service summary shows the total number of event queries processed, the number of alerts and threats, and more.

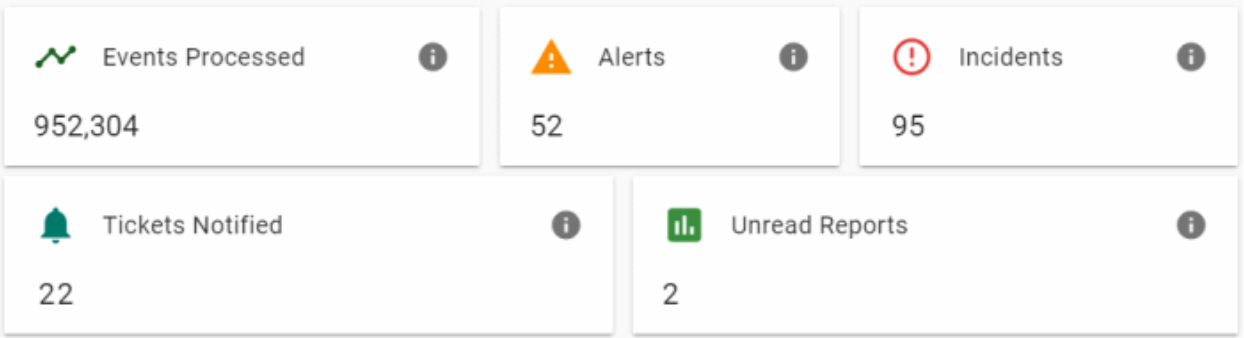
- Select a customer at top-right or click the customer name on the home screen tile.
  - You can also click 'Service Summary' in the left-menu



The tiles along the top show:

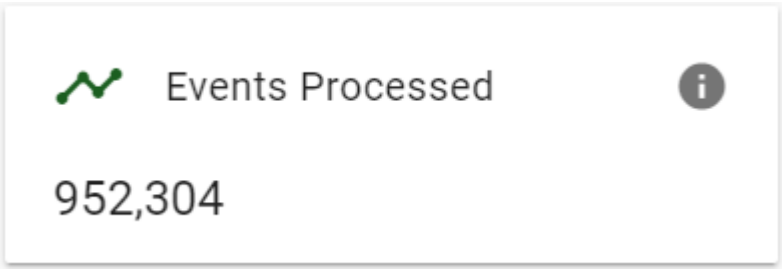
- The number of events processed
- The number of alerts generated
- The number of incidents minus false-positives
- The number of incidents closed by the SOC team with notifications sent to customers.
- The number of unread reports.

Data is provided for the past 90 days.



Events Processed

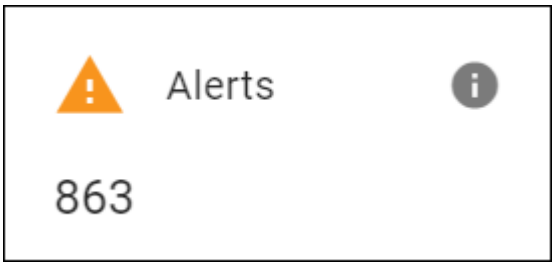
The number of events in the last 90 days.



- Click the tile to open the **log collection summary** screen where you can view the events in detail.

Alerts

The number of events that matched a rule and created an alert.



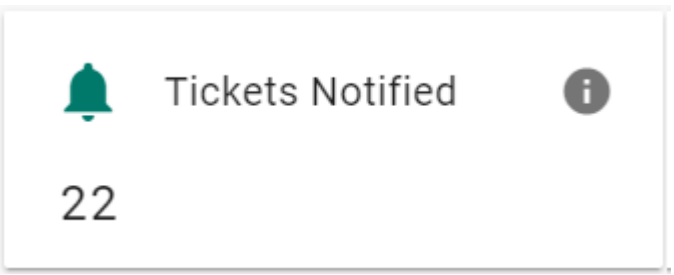
Incidents

The total number of alerts (incidents) minus false-positives for the last 90 days.

- Click the tile to open the **incidents** screen where you can analyze the incidents.

Notifications

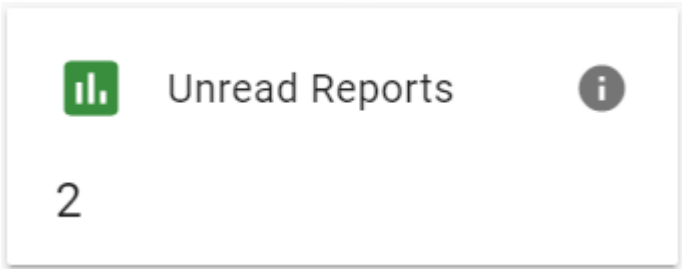
The number of notifications sent to customers after the SOC team closed an incident



- Click the tile to open the **tickets** section

Unread Reports

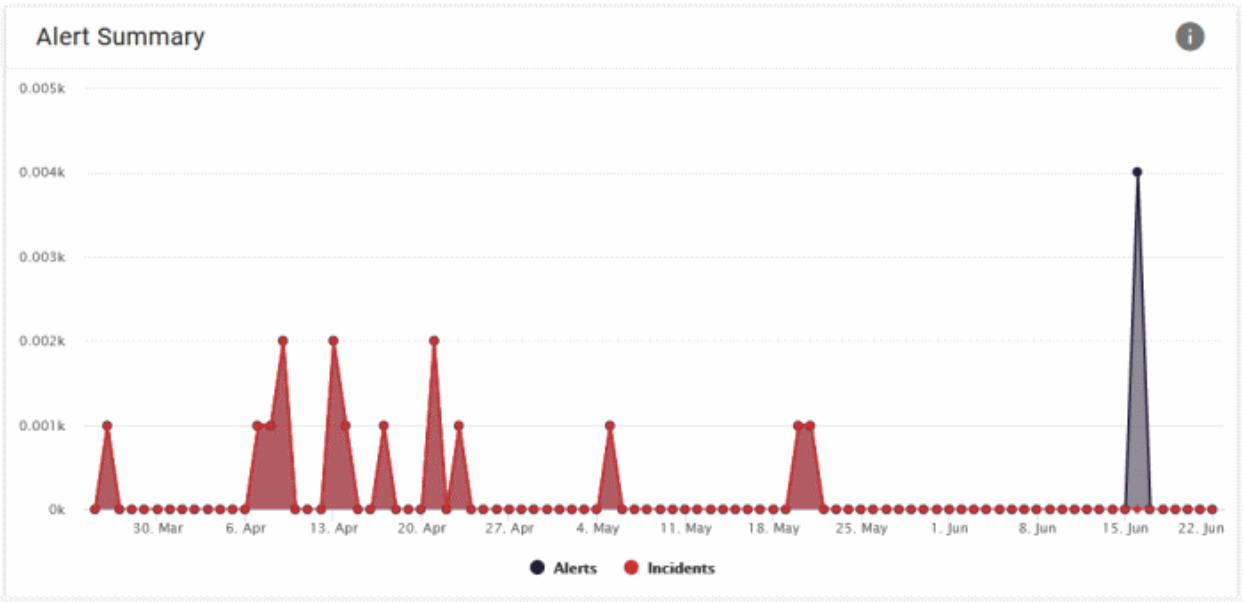
The number of reports that the customer is yet to download and view.



- Click the tile to open the **reports** section

Alert Summary

Shows alerts versus actual incidents (alerts minus false-positives). Data is for the last 3 months.



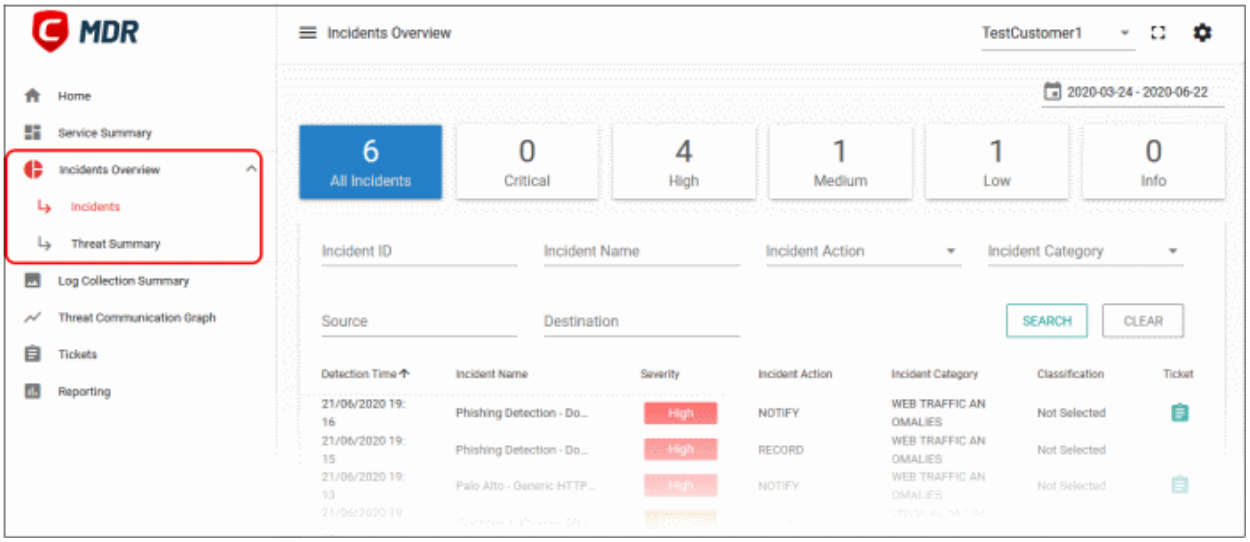
- Click the 'Alerts' or 'Incidents' text at the bottom to remove that particular graph. Click on it again to view.
- Place your mouse over a particular day to view more details for that day.

4 Incidents Overview

An at-a-glance summary of the incidents and threats on your network. The 'incidents' interface lets you view incidents by type, name and more.

The 'threat summary' dashboard shows attack sources, types of attack, attack origin and destination, and more.

- Click 'Incidents Overview' on the left



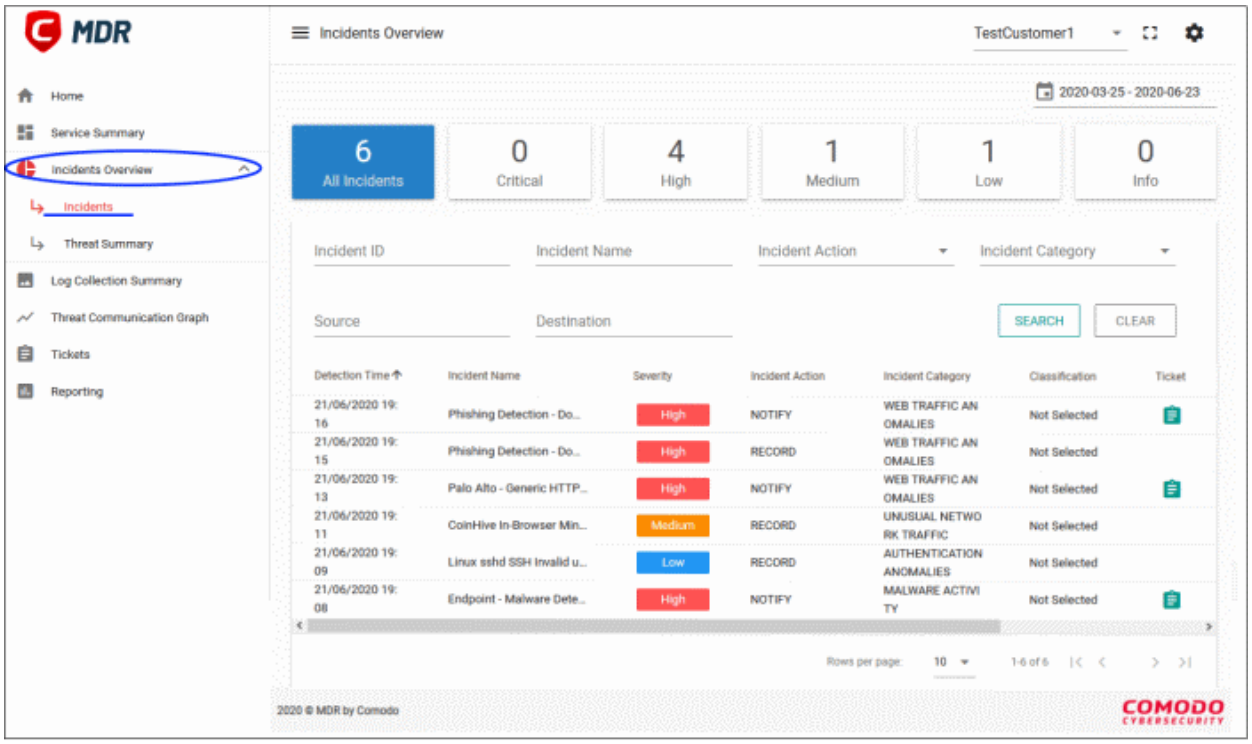
Click the following links for more about each area:

- **Incidents**
- **Threat Summary**

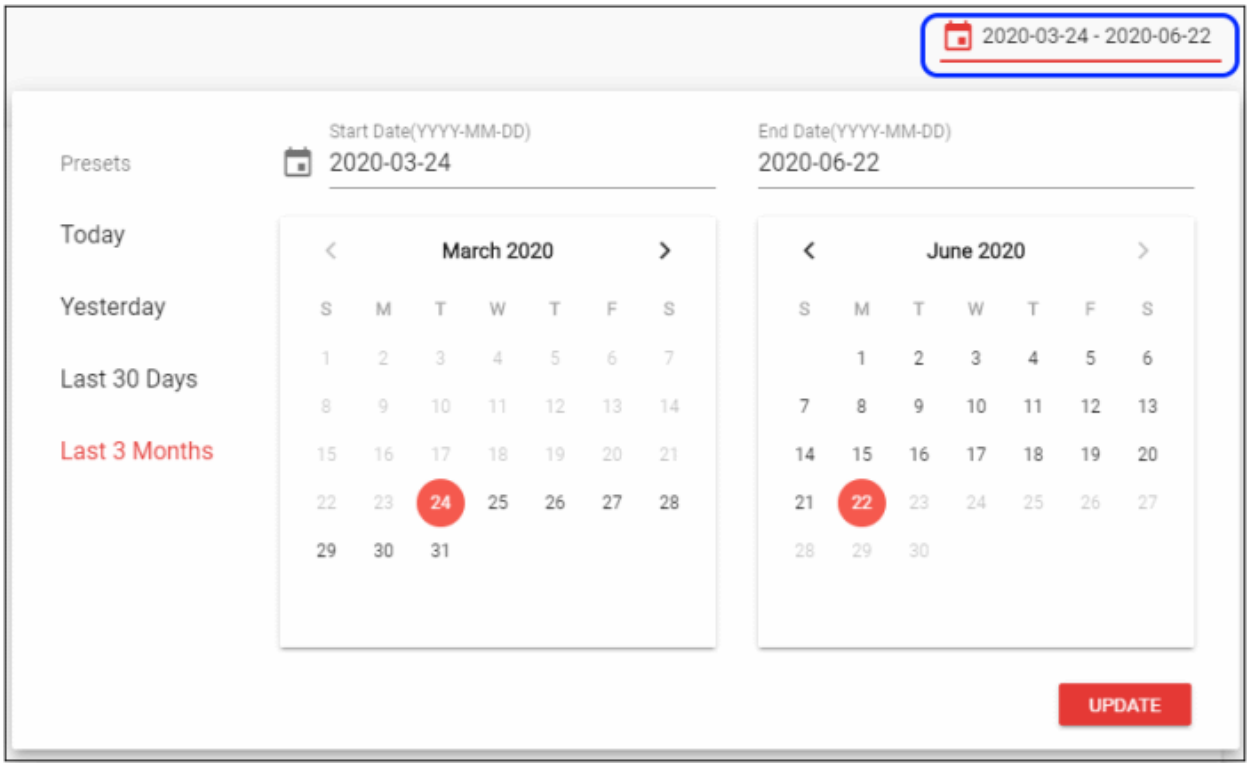
4.1 Incidents

Shows the top incidents on your network by type, and the severity of those incidents. Further details on each incident are shown in the table in the lower pane.

- Click 'Incidents Overview' > 'Incidents' to open the interface
- Select a customer at top-right



- By default, statistics are shown for the past seven days
- To view the data for a different time period, click the date range at the top and choose from the options:



- To view data for a custom period, select from and to dates from the calendars
- Click 'Update'

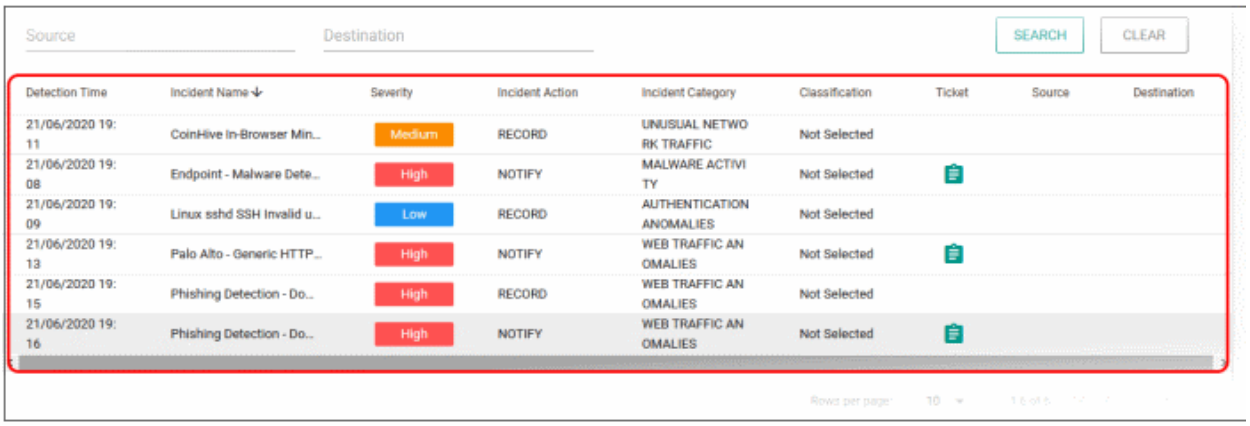
The top pane shows the incidents by their severity.

- Click a tile to view the incidents at the bottom pane

Use the filters to search for particular incidents:

- Enter / select the filter parameter(s) and click 'Search'
- Incidents matching the filter are shown below.
- Click 'Clear' to view all incidents again.

The lower pane shows the incidents for the selected time period:

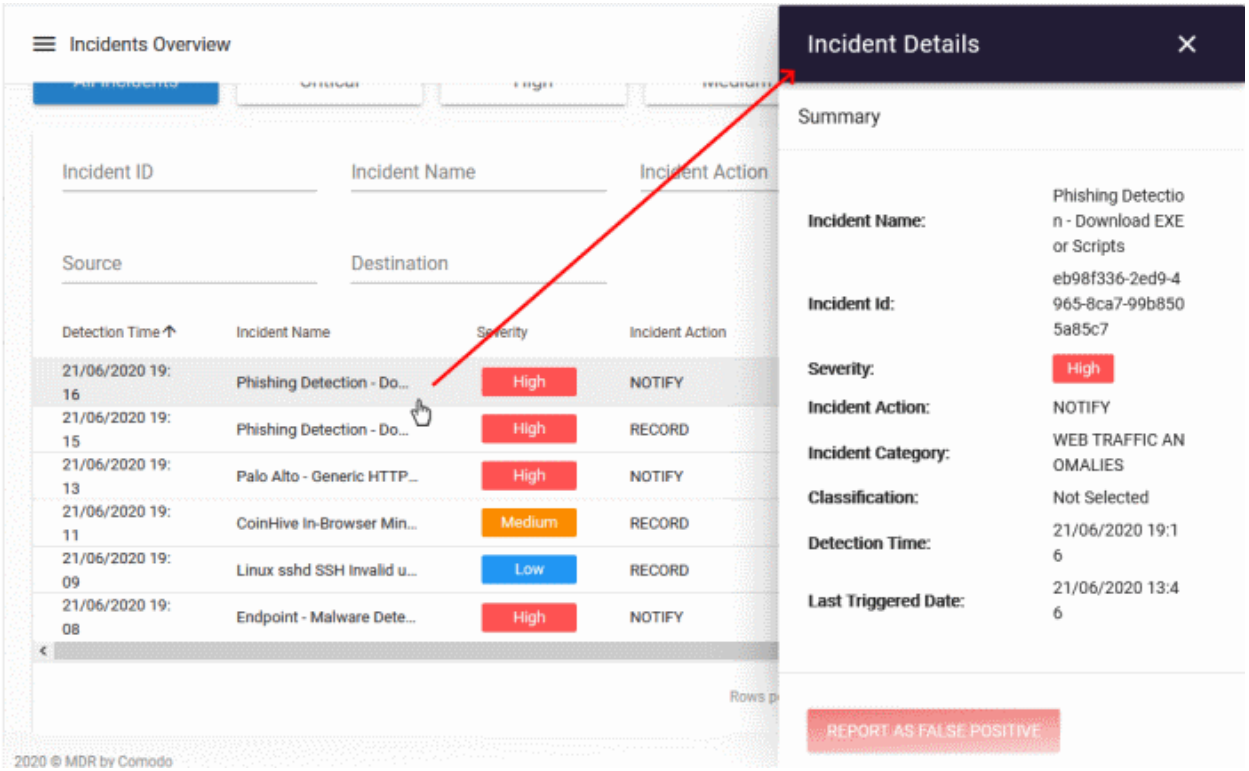


Click a column header to sort the incidents by alphabetical / ascending / descending order.

- **Detection Time** – The date and time the incident was logged.
- **Incident Name** – The rule label that triggered the incident.
- **Severity** – Incident grade whether critical, high, medium, low or information
- **Incident Action** – The response to the incident per the rule
- **Incident Category** – The incident type. For example, 'Malware activity' or 'Unusual network Traffic'
- **Classification** – Indicates to which the group the rule that triggered the incident is added to.
- **Ticket** – Opens the related incident's **tickets** interface.
- **Source** – The origin IP address that the rule detected
- **Destination** – The final network / endpoint IP address

View incident details

- Click anywhere on an incident row to view even more details like incident ID, admin remarks, and more.

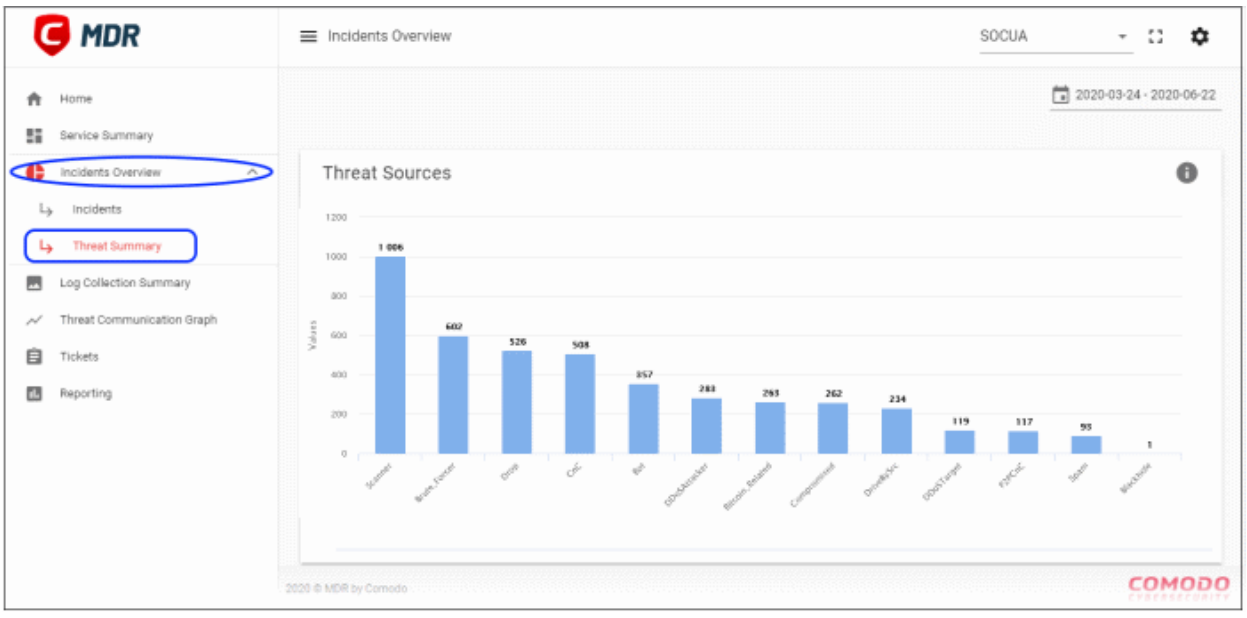


- Click 'Report as False Positive' if you know the incident is not a threat or malicious.

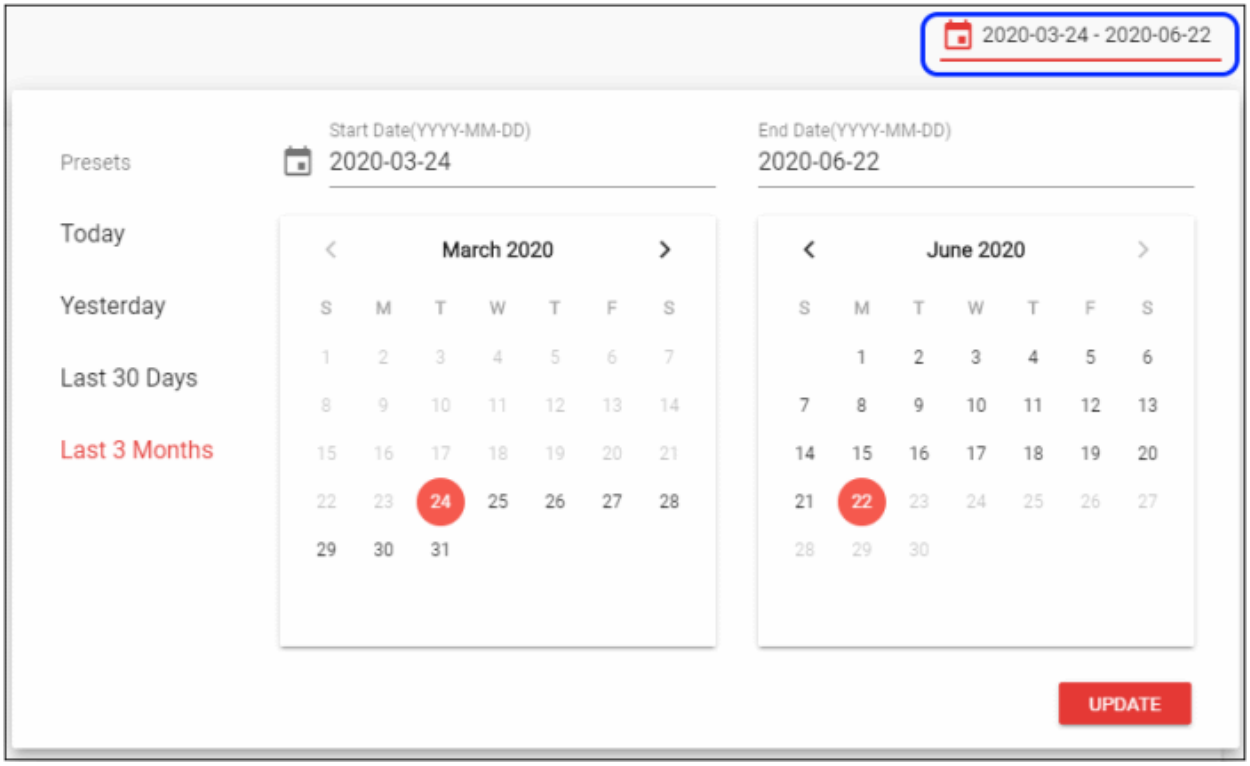
4.2 Threat Summary

The 'Threat Summary' dashboard shows attack sources, types of attack, attack origin and destination, and more.

- Click 'Incidents Overview' > 'Threat Summary' to open the interface
- Select a customer at top-right

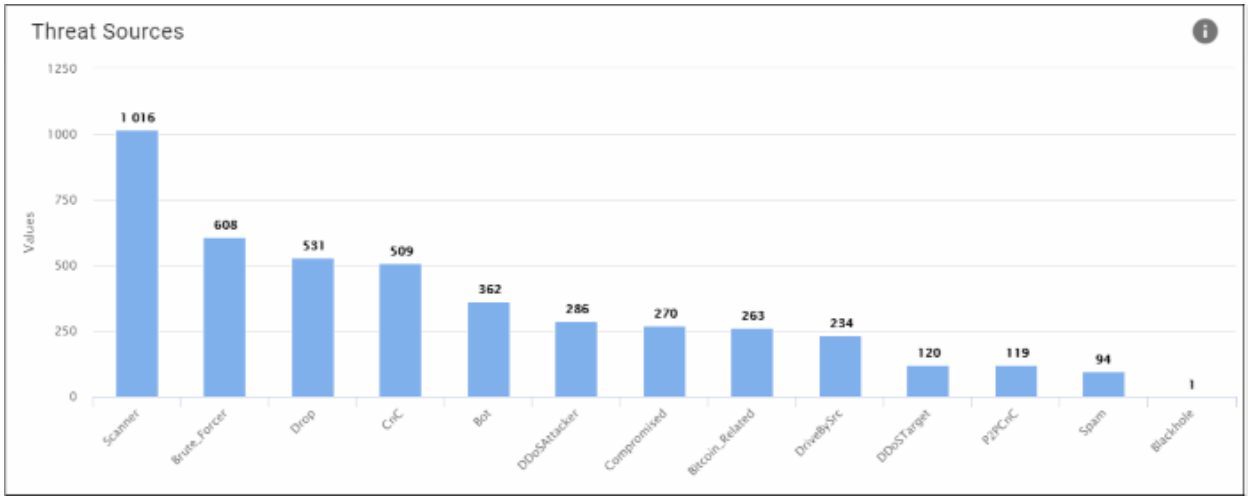


- Statistics are shown for the past seven days by default.
- Click the date range above the chart to change the time-period shown:



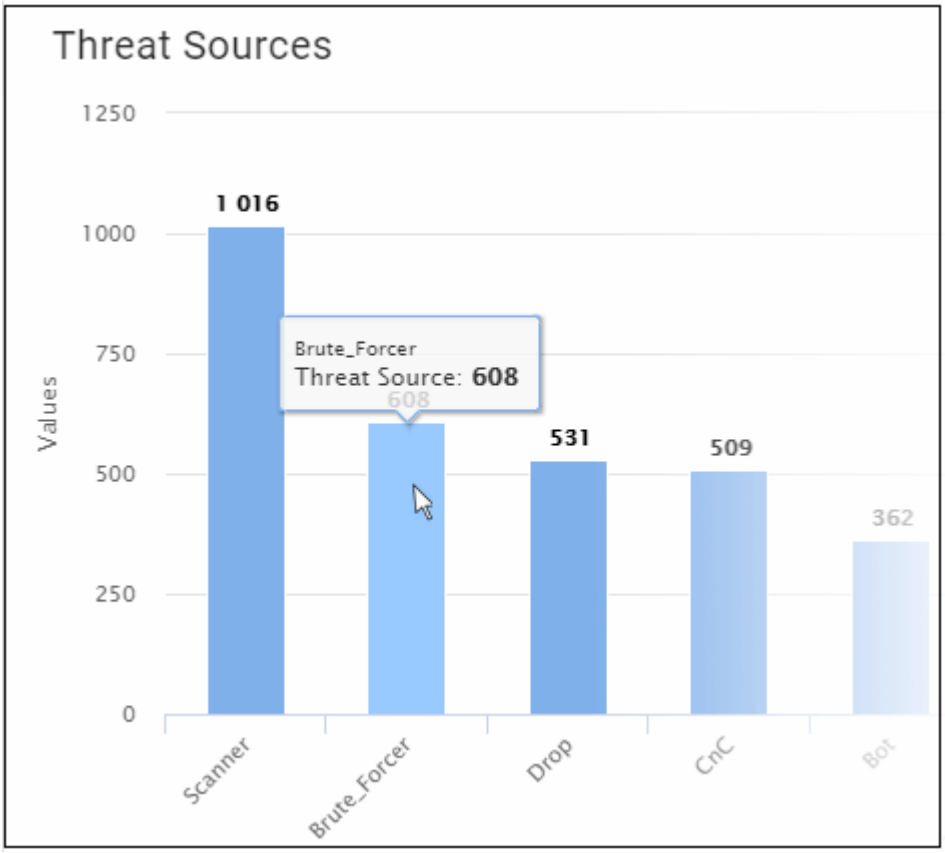
Threat Sources

Shows the types of threats that occurred over the selected time-period, and the number of sources for each:



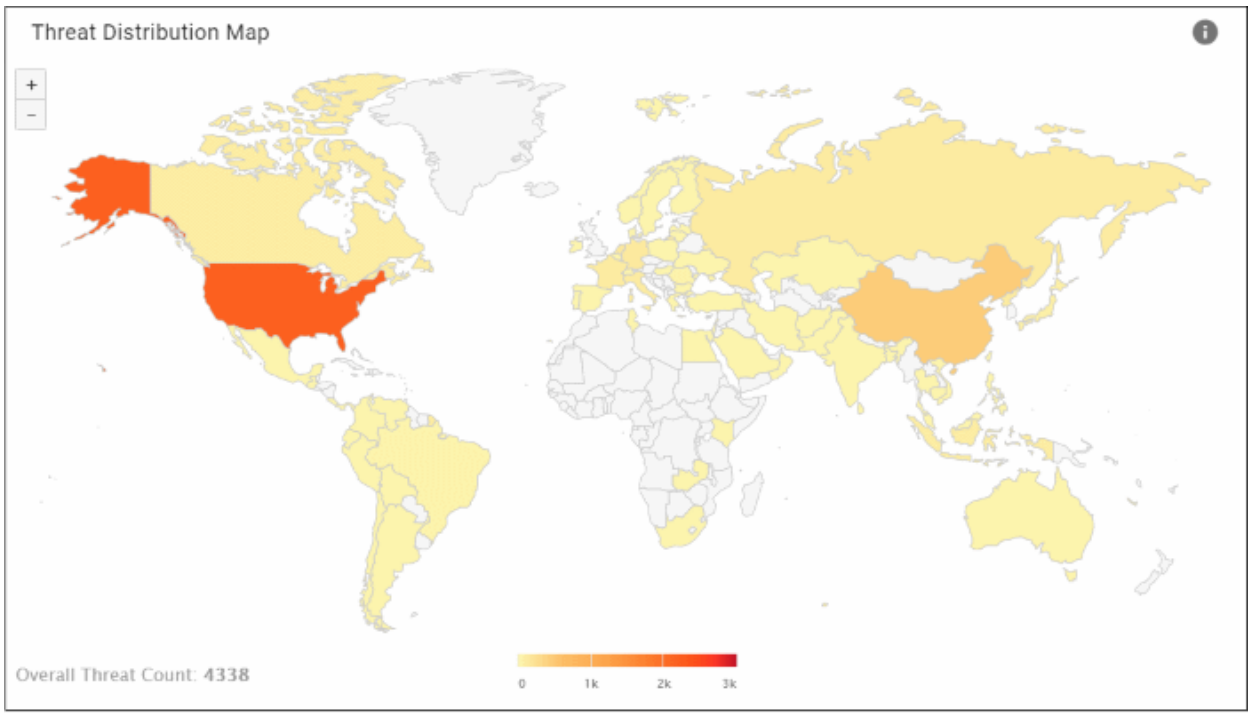
- X-axis – The name of the threat
- Y-axis – Number of sources for each threat category

- Click a bar graph to view its details:

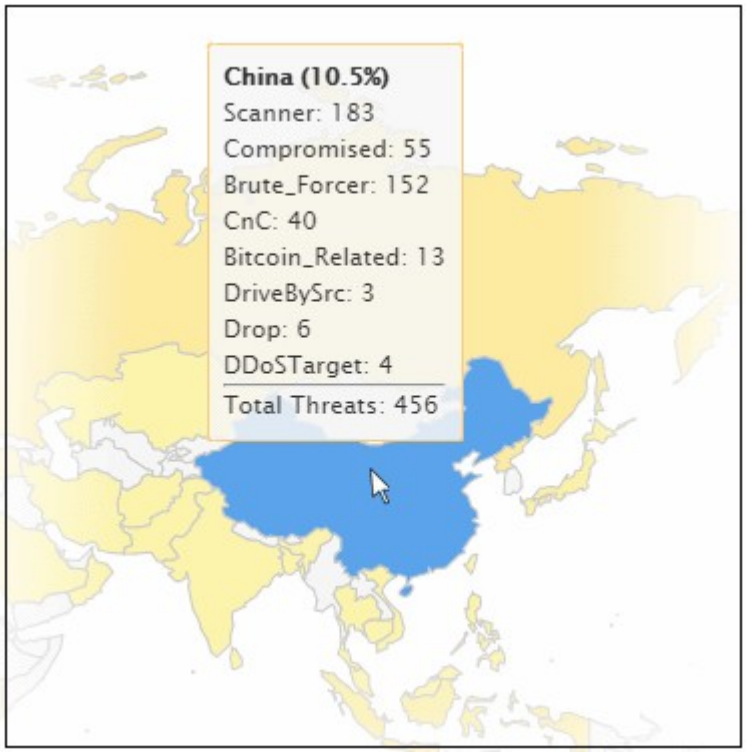


Threat Distribution Map

- A heat map of the threat sources

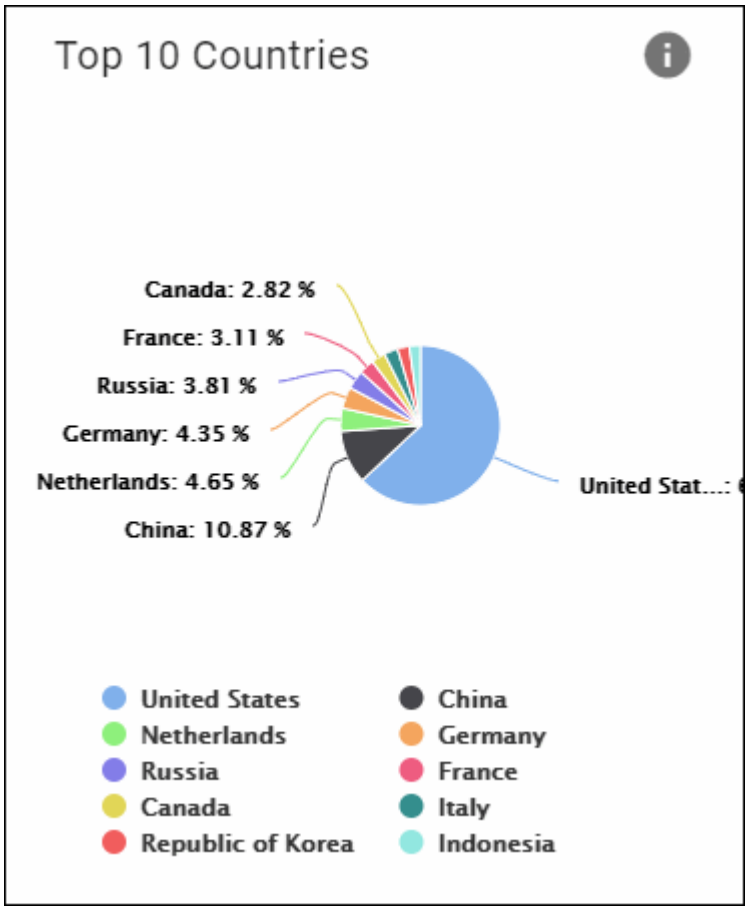


- Click a country to view details of the threat categories from that country:

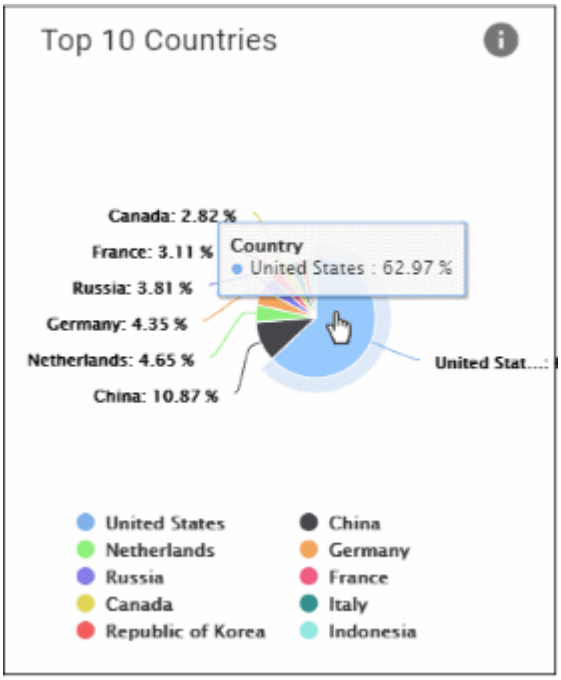


Top 10 Countries

'Top 10 Countries' shows the details of countries from where both incoming and outgoing threats were recorded. The details are shown by percentage.



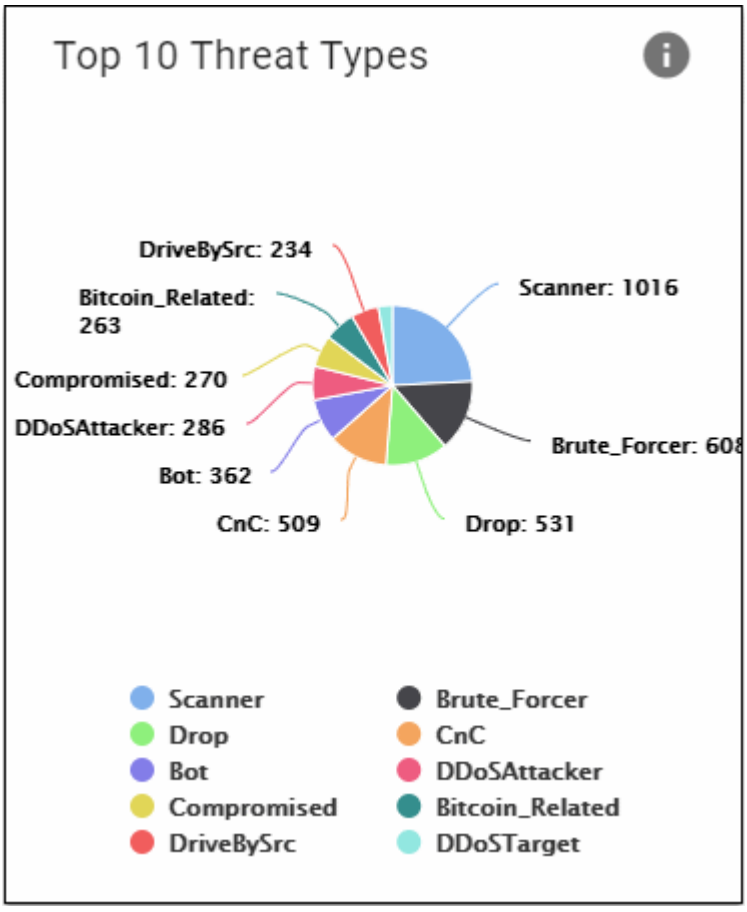
- Placing the mouse cursor over a segment will display further details.



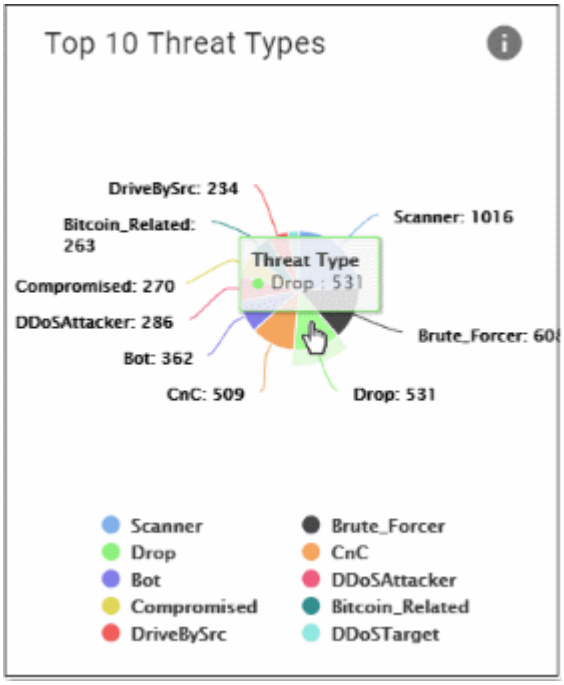
- Click a country legend below to enable/ disable its data. For example, click 'China' and this segment will be removed from the pie chart. Click the legend again to view it.

Top 10 Threat Types

This pie-chart shows the details of top ten-most incoming and outgoing threat types that were recorded.



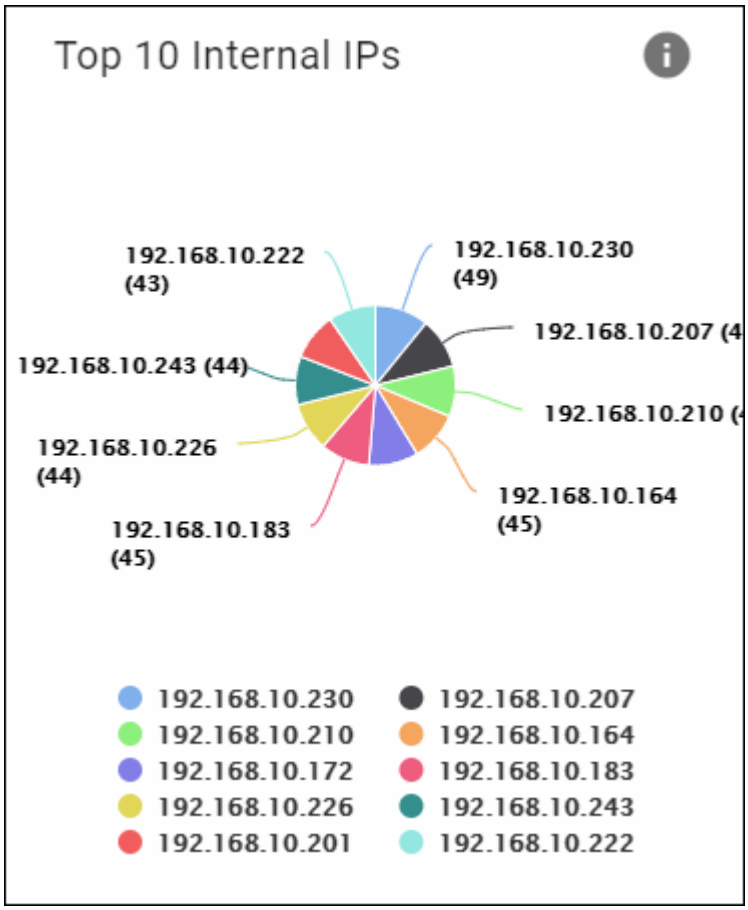
- Placing the mouse cursor over a segment will display further details.



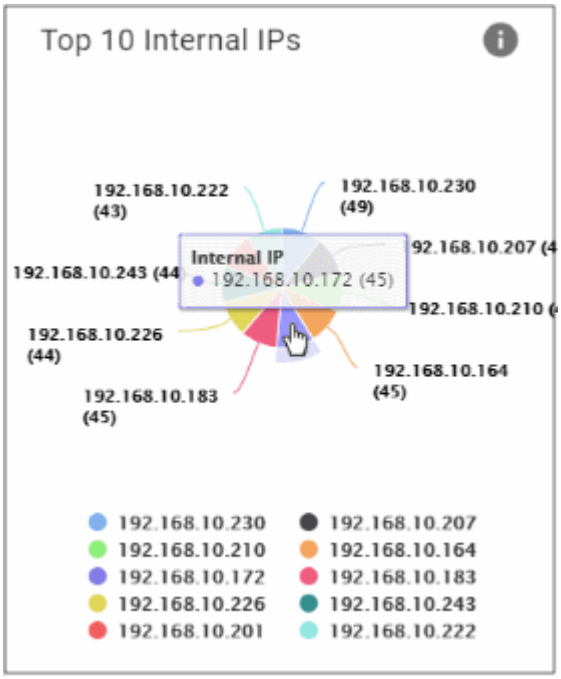
- Click a threat name below to enable/ disable its data. For example, click 'Scanner' and this segment will be removed from the pie chart. Click the legend again to view it.

Top 10 Internal IPs

This pie chart shows the details of endpoints from which the threat types originated. The number beside an IP indicates the threat counts that originated from the endpoint.



- Placing the mouse cursor over a segment will display further details.

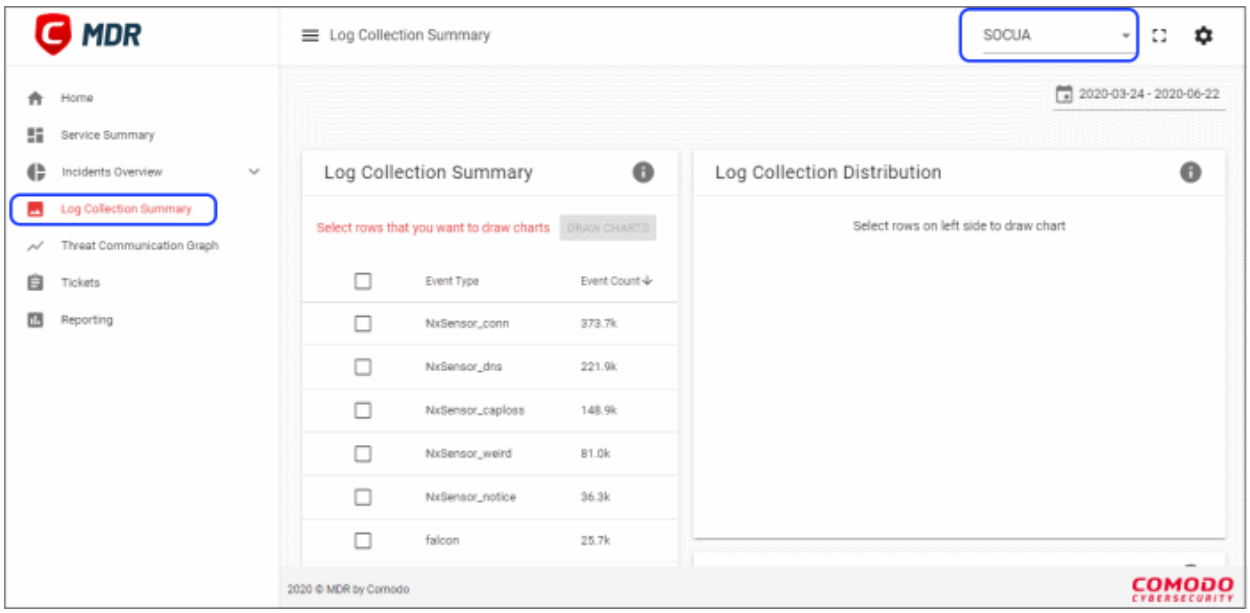


- Click an IP to enable/ disable its data. For example, click '192.168.10.222' and this segment will be removed from the pie chart. Click the IP again to view it.

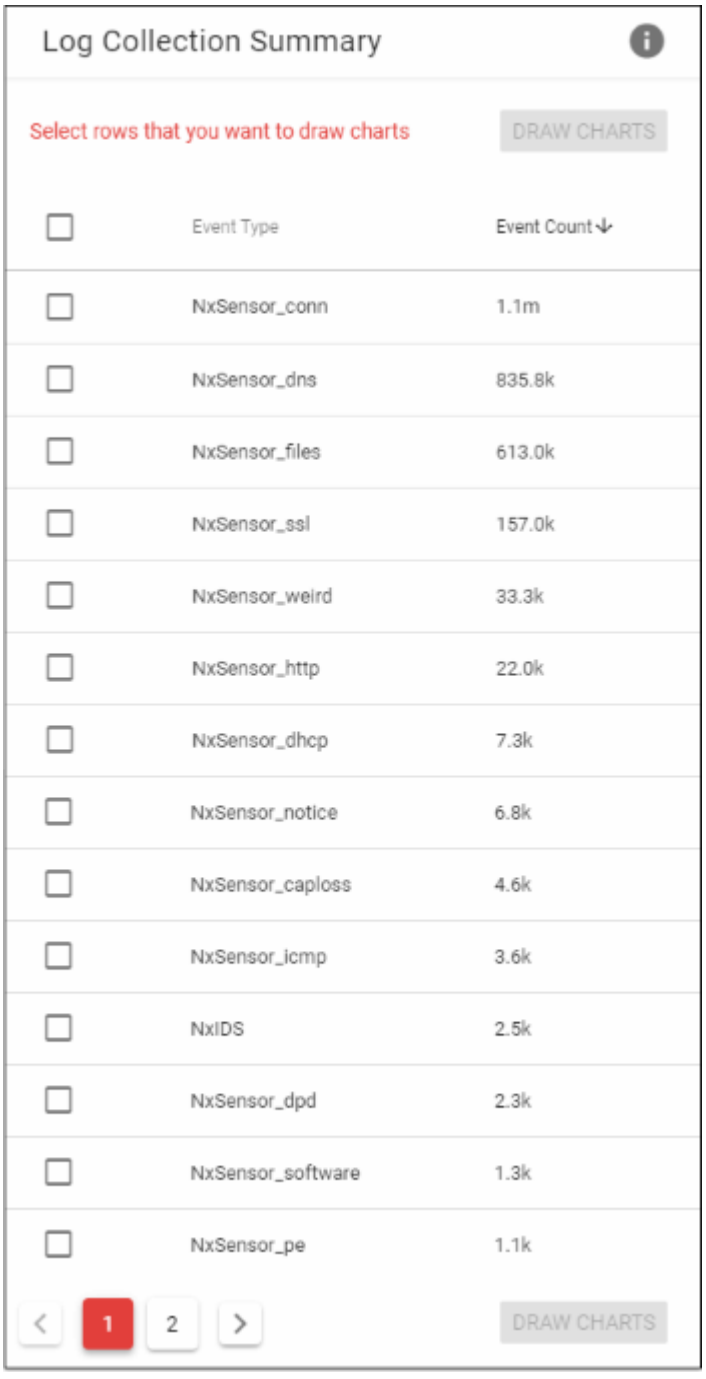
5 Log Collection Summary

The log summary screen is a record of logs from all cWatch MDR sources. For example, logs collected from cWatch MDR sensors placed on your network.

- Click 'Log Collection Summary' on the left and select a customer at top-right:



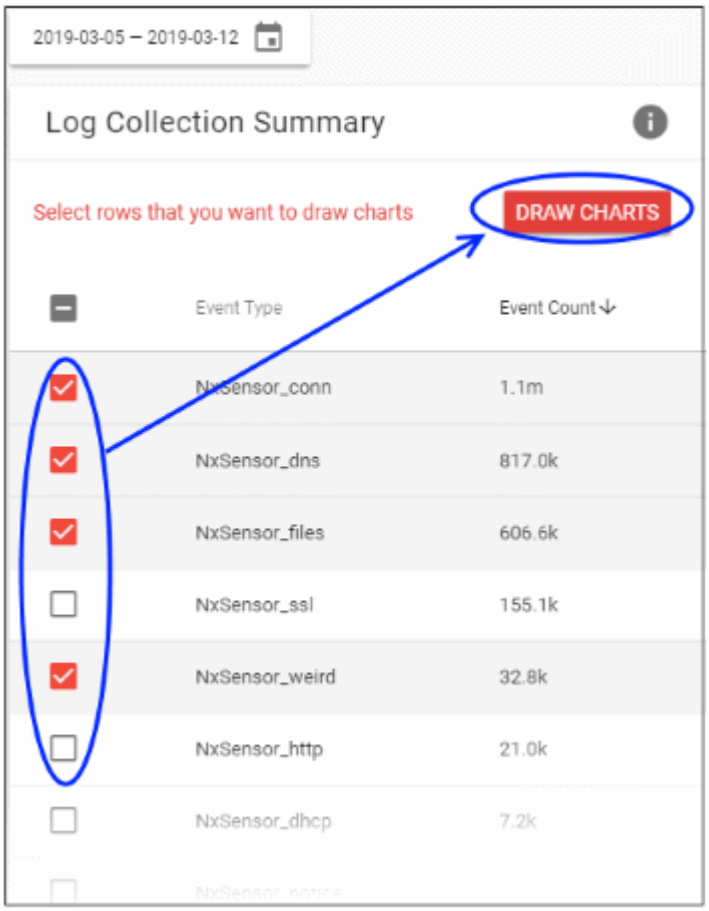
- Results are shown for the past seven days by default. Click the date above the table to view a different time frame.
- The summary panel shows the log source and the total number of logs from that source. You can use these logs to generate graphs for the selected time period:



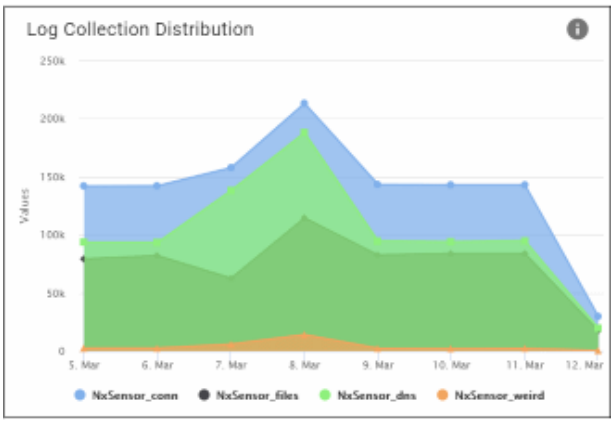
- **Event Type** – Name of the log source. Each source creates logs for different types of event
- **Event Count** – Total number of logs from the source for the selected time-period

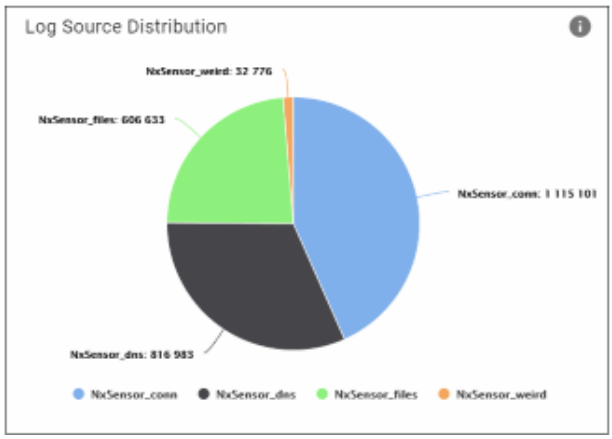
Log Collection Distribution and Log Source Distribution

- Select one or more log sources in the 'Log Collection Summary' table on the left
- Click 'Draw Charts':



The log collection and source distribution charts are shown on the right:

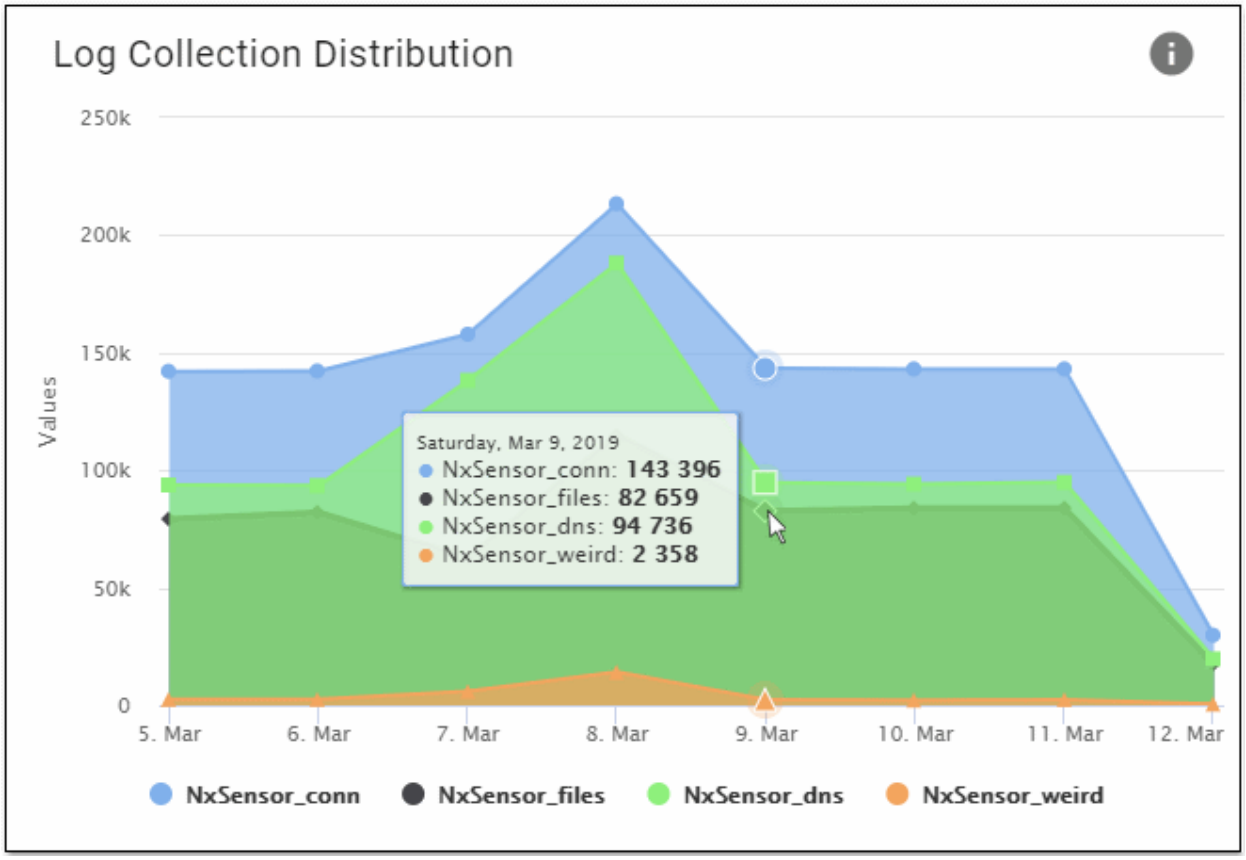


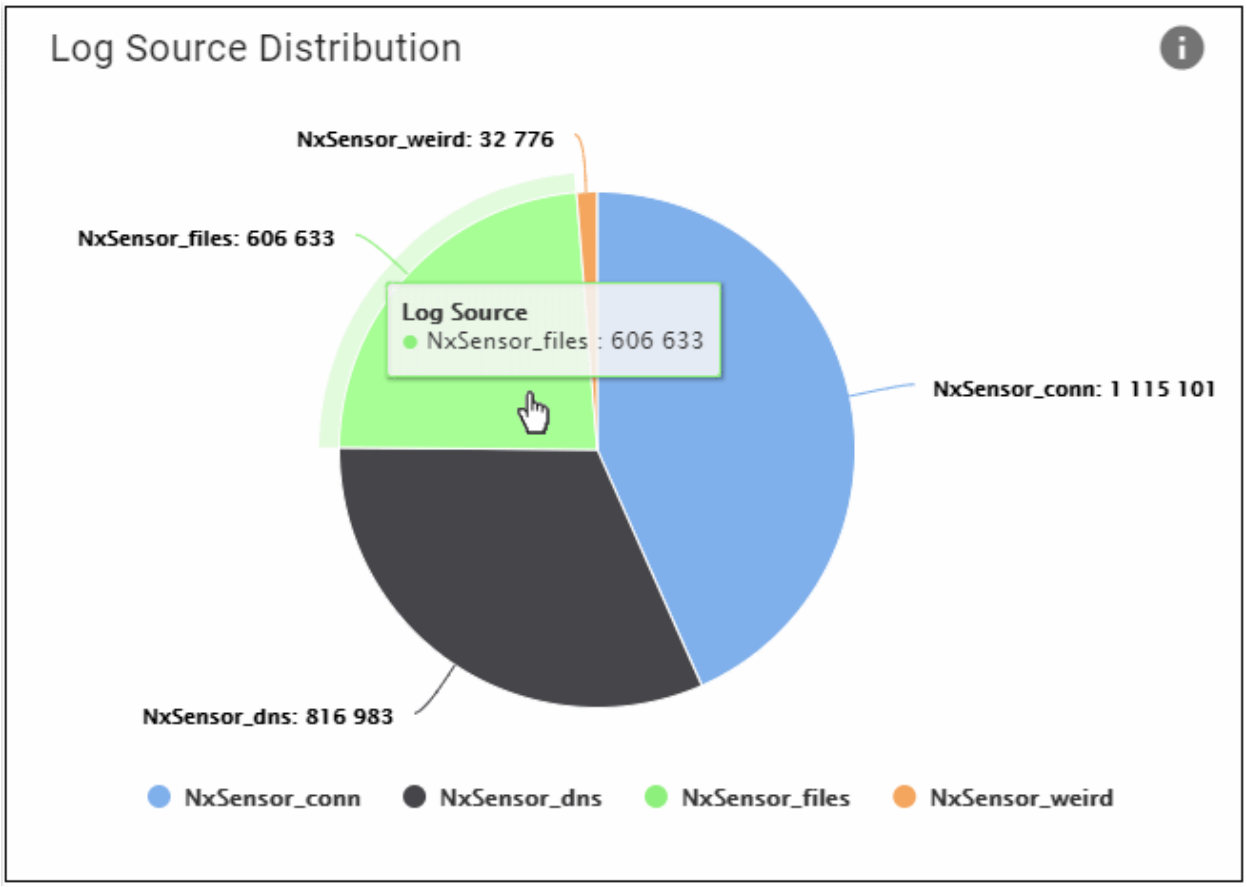


Log Collection Distribution – Line chart. Shows how many logs were generated per-day from your sources, over your selected time period.

Log Source Distribution – Pie Chart. Shows the total logs collected from your selected sources, over your selected time period. Each segment represents the total logs from a particular source.

- Click a source name under the chart to remove its data from the graphic. Click the name again to re-add the data.
- Place your mouse cursor over a pie segment or date to view more details:

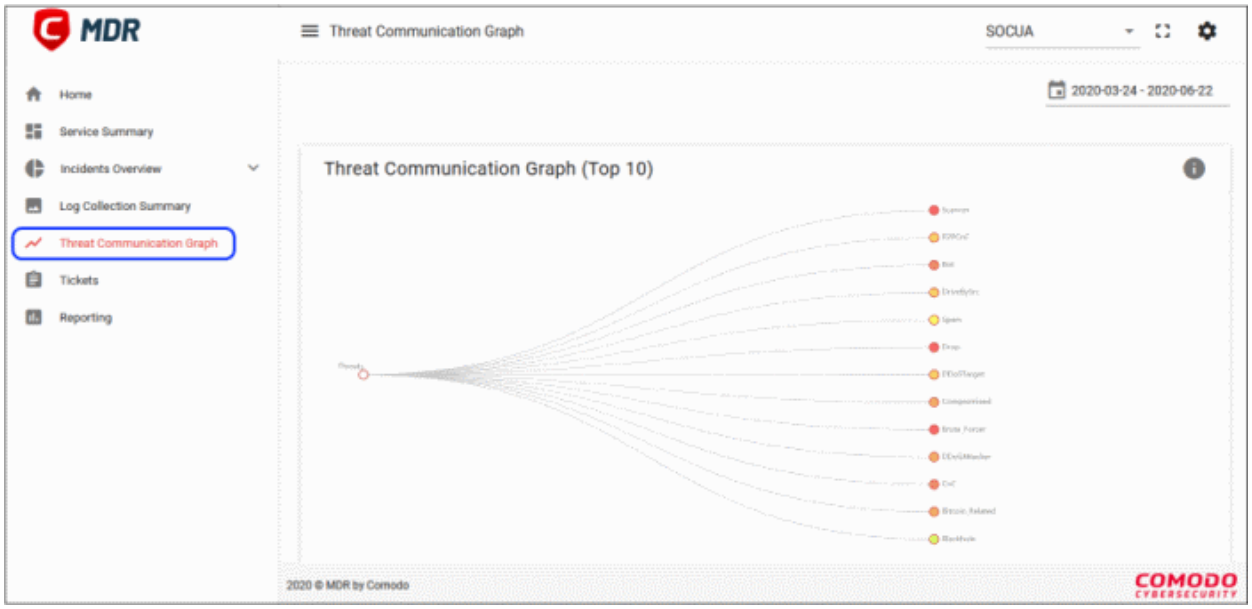

Log Collection Distribution
250k
200k
150k
100k
50k
0
Values
Saturday, Mar 9, 2019
NxSensor_conn: 143 396
NxSensor_files: 82 659
NxSensor_dns: 94 736
NxSensor_weird: 2 358
5. Mar
6. Mar
7. Mar
8. Mar
9. Mar
10. Mar
11. Mar
12. Mar
NxSensor_conn
NxSensor_files
NxSensor_dns
NxSensor_weird


Log Source Distribution
NxSensor_weird: 32 776
NxSensor_files: 606 633
Log Source
NxSensor_files : 606 633
NxSensor_conn: 1 115 101
NxSensor_dns: 816 983
NxSensor_conn
NxSensor_dns
NxSensor_files
NxSensor_weird

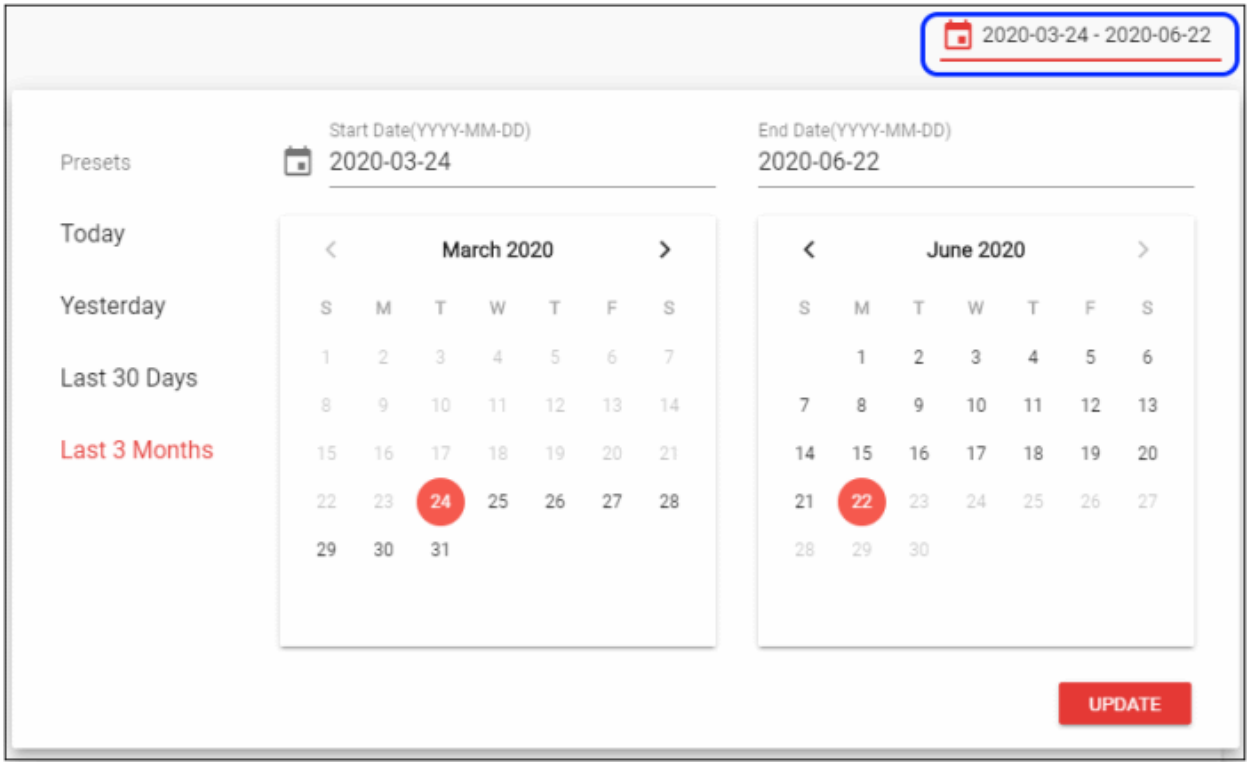
6 Threat Communication Graph

Click 'Threat Communication Graph' on the left and select a customer at top-right

- This graph shows how external IPs attempted to communicate with internal IPs to deliver specific types of threat.
  - Click a threat category on the right to reveal the internal addresses targeted by that type of attack.
  - Next, click an internal address to see the IPs that contacted it to try and deliver the threat.
- The color-tone of the circle indicates the volume of communications. White = low, yellow = medium, red = high.

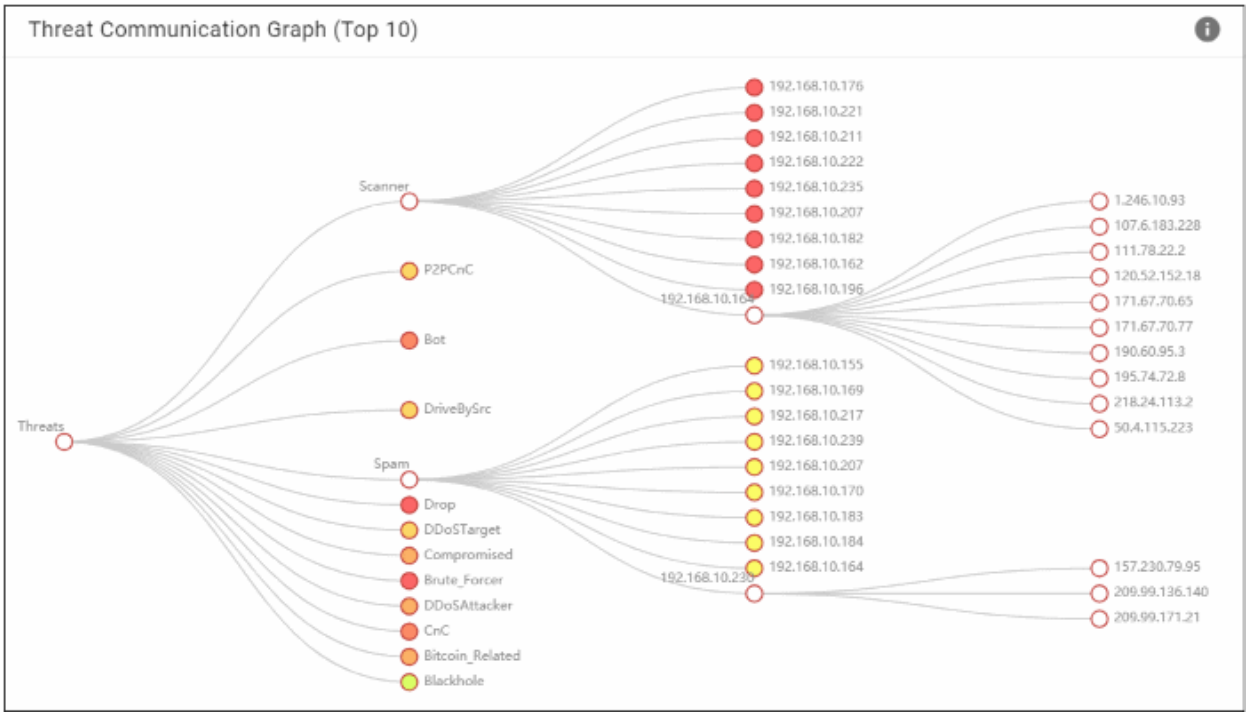


- Statistics are shown for the past seven days by default
- Click the date above the chart if you want to view a different time-frame:



View threats in tree view

- Click a threat to the view the details of affected internal IPs

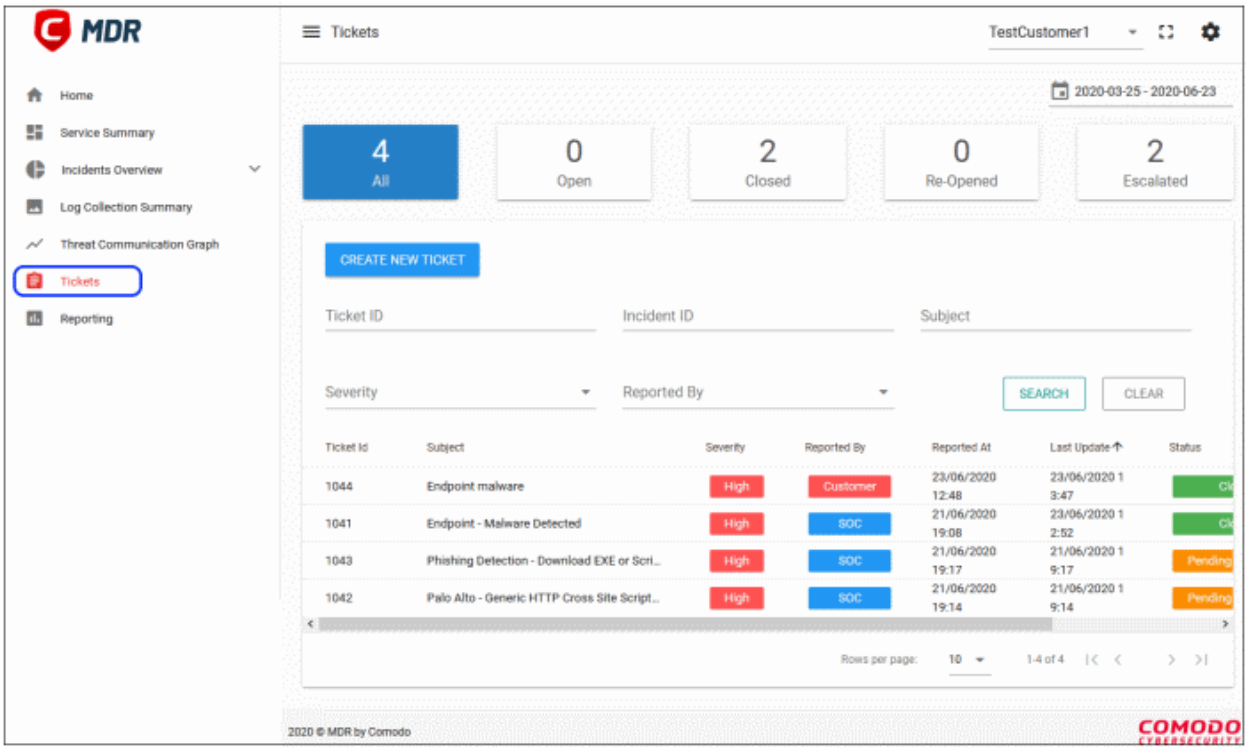


- Click an internal IP to view details of threat from blacklisted IPs
- Node color tones range from white to red depicting the intensity of threat communication
- Click again to collapse the tree view

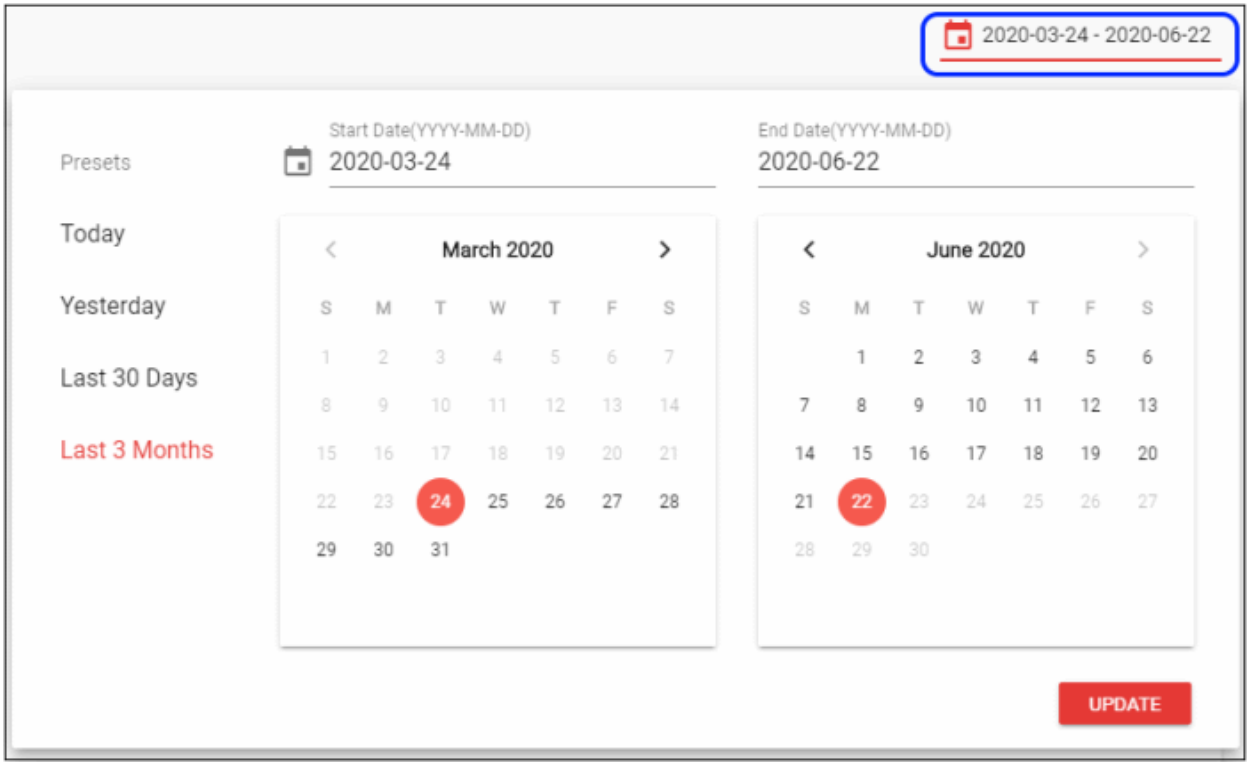
7 Tickets

Click 'Tickets' on the left menu

- Tickets are a two-way communication system via the MDR interface between customer and Comodo's security operations center (SOC) team. For example, if any threats or anomalies are found on your network, SOC team raises a ticket so customer can view and attend to the problem.
- Similarly, customer can create a ticket, for example, request the SOC team to check for particular threats.

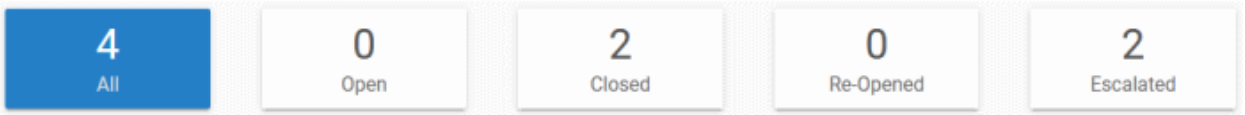


- By default, ticket details are shown for the past seven days
- To view the data for a different time period, click the date range at the top and choose from the options:



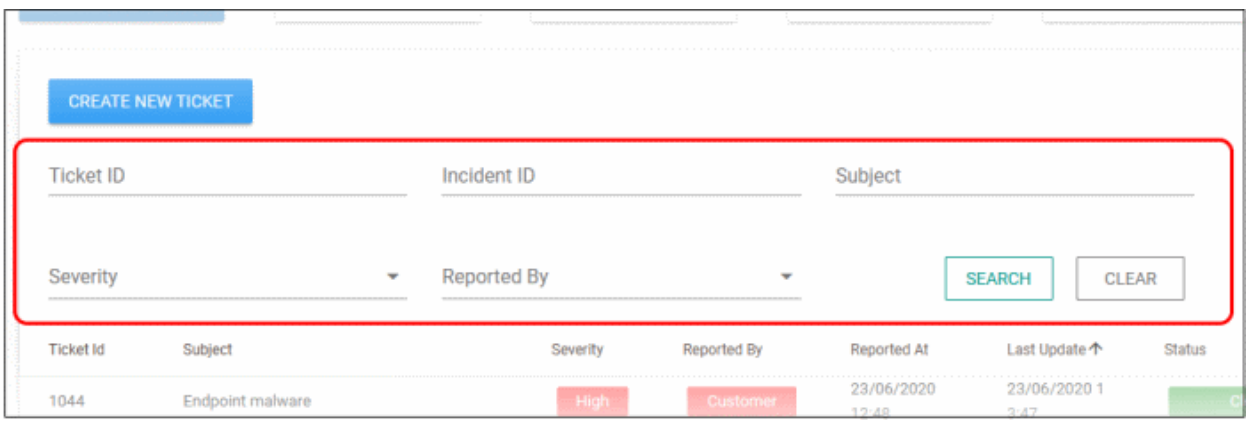
- To view data for a custom period, select from and to dates from the calendars
- Click 'Update'

The top pane shows the tickets by their statuses.



- Click a tile to view the respective type of tickets at the bottom pane
  - Open – Number of tickets whose issues are not yet addressed.
  - Closed – Issues resolved and tickets closed by the customer or the SOC team.
  - Re-opened – Closed tickets that are opened again by the customer or the SOC team.
  - Escalated – Tickets can be escalated by SOC team only. This may be to remind customers to attend to issues immediately.

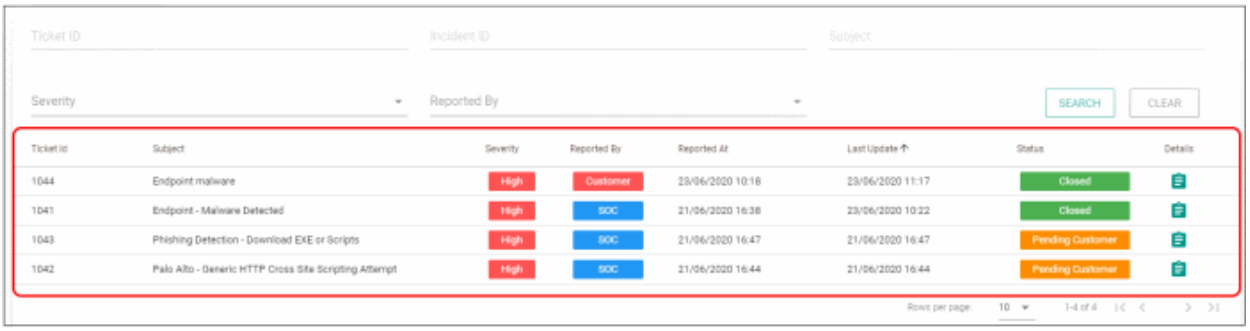
Use the filters to search for particular tickets:



- Enter / select the filter parameter(s) and click 'Search'
- Tickets matching the filter are shown below.

- Click 'Clear' to view all tickets again.

The lower pane shows the tickets for the selected time period:

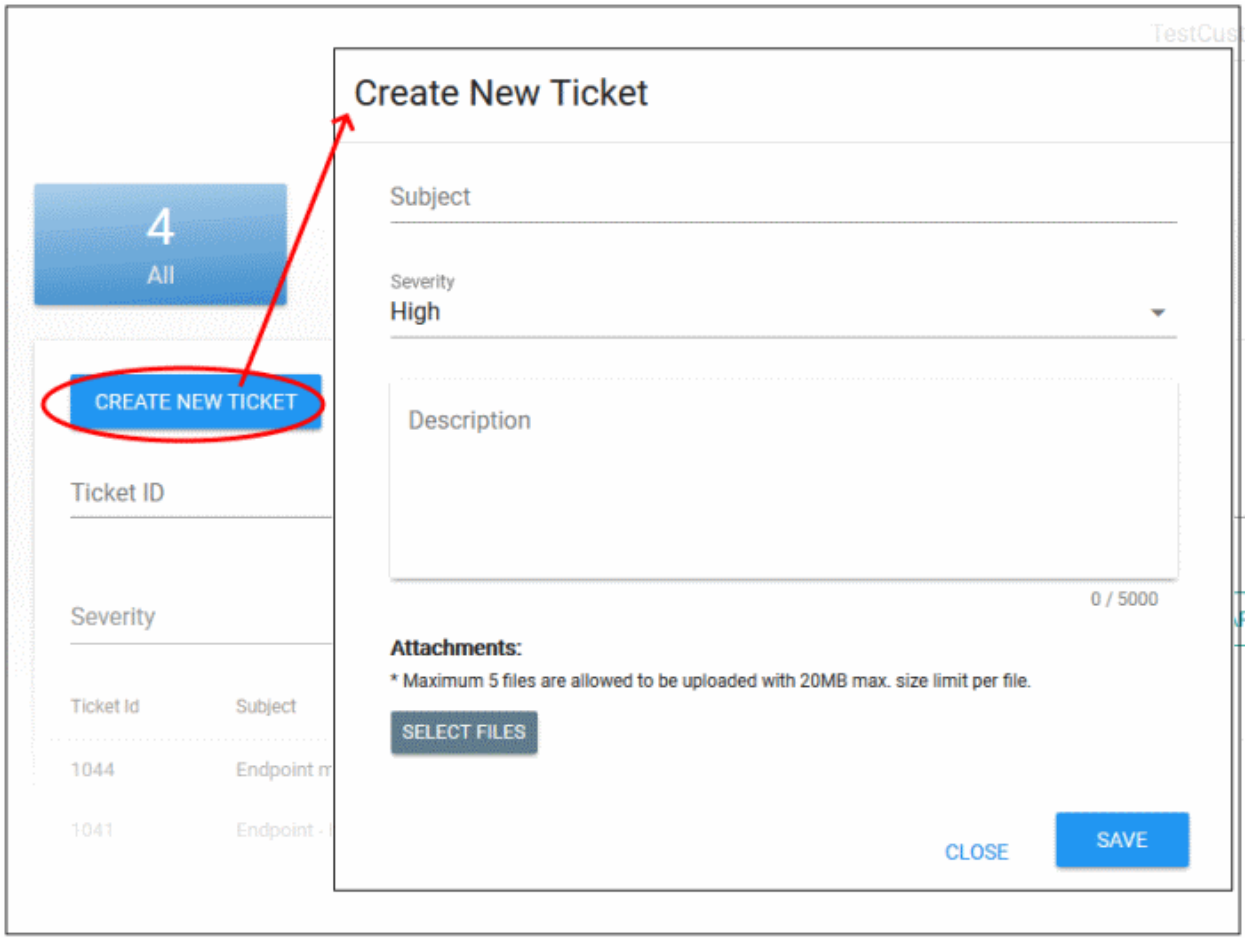


Click a column header to sort the tickets by alphabetical / ascending / descending order.

- **Ticket ID** – Auto generated ticket reference number
- **Subject** – The ticket subject that was entered while creating the ticket
- **Severity** – Ticket urgency grade. Possible values are:
  - All
  - Info
  - Low
  - Medium
  - High
  - Critical
- **Reported by** – Indicates who created the ticket. It can be SOC team or the customer.
- **Reported at** – Date and time of ticket creation.
- **Last update** – Date and time of the latest response to the ticket
- **Status** – Indicates the latest position of the ticket. Possible values are:
  - Closed – This can be done either by the customer or the SOC team
  - Pending Customer – Ticket waiting for response from the customer
  - Pending SOC – Ticket waiting for response from the SOC team
  - Reopened – A closed ticket is opened again by SOC or by the customer
- **Details** – Click this to **view the history of the ticket**.

Create a ticket

- Click 'Create New Ticket'



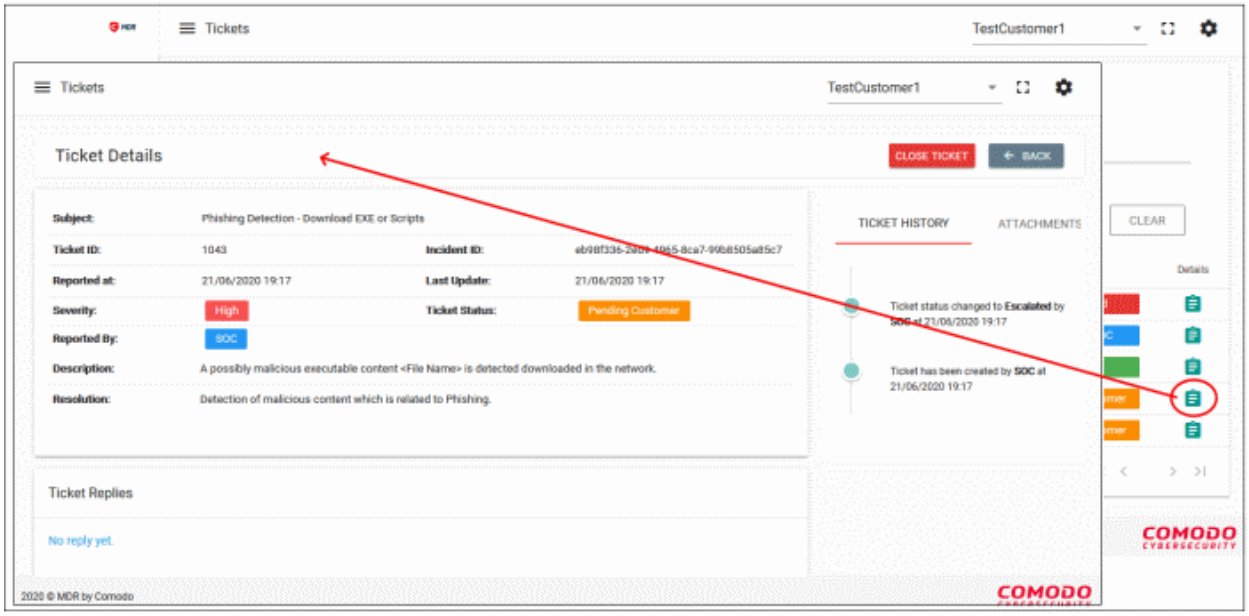
- Subject – Enter an appropriate label for the ticket.
- Description – State your requirements in detail not exceeding 5000 characters.
- Attachments – Upload any reference files if required. Click 'Select Files', navigate to the location and click 'Open'.

- Click 'Save'

The ticket is created and the status shows as 'Pending SOC'. The SOC team will analyze your request and reply to the ticket. You can either close and respond again.

Ticket Details

- Click the ticket icon in the 'Details' column

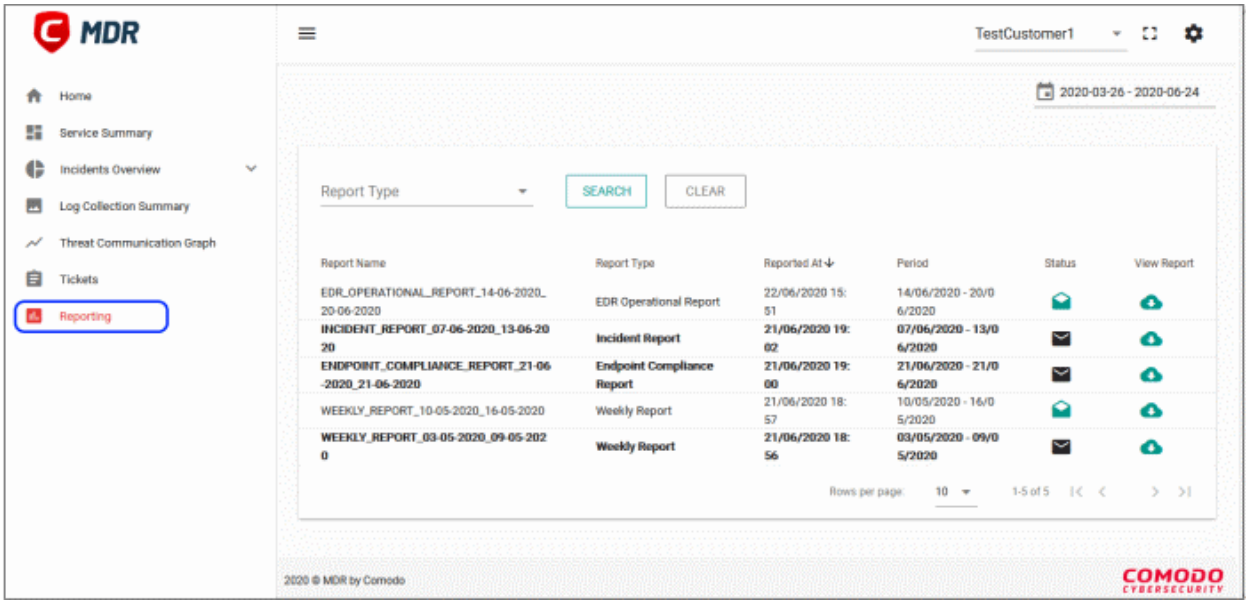


- Ticket Details – The top pane shows the ticket details such as ticket subject, ticket ID and more.
- Ticket Replies – Shows responses from the customer and the SOC team.
- Reply to Ticket – Enter your response and if you want to upload any files, click 'Select Files' in the 'Attachments' section below and complete the upload process.
- Reply – Click this button at the bottom to respond to the SOC team.
- Close Ticket – Click this button at top-right to end the ticket issue.
- Re-open – Shows only for closed tickets. Click this button to open a closed ticket.
- Ticket History – Shows the details of the ticket, such as who created the ticket, replies from the customer and SOC team.
- Attachments – Shows the details of uploaded files.
- Back – Click this to return to the tickets screen.

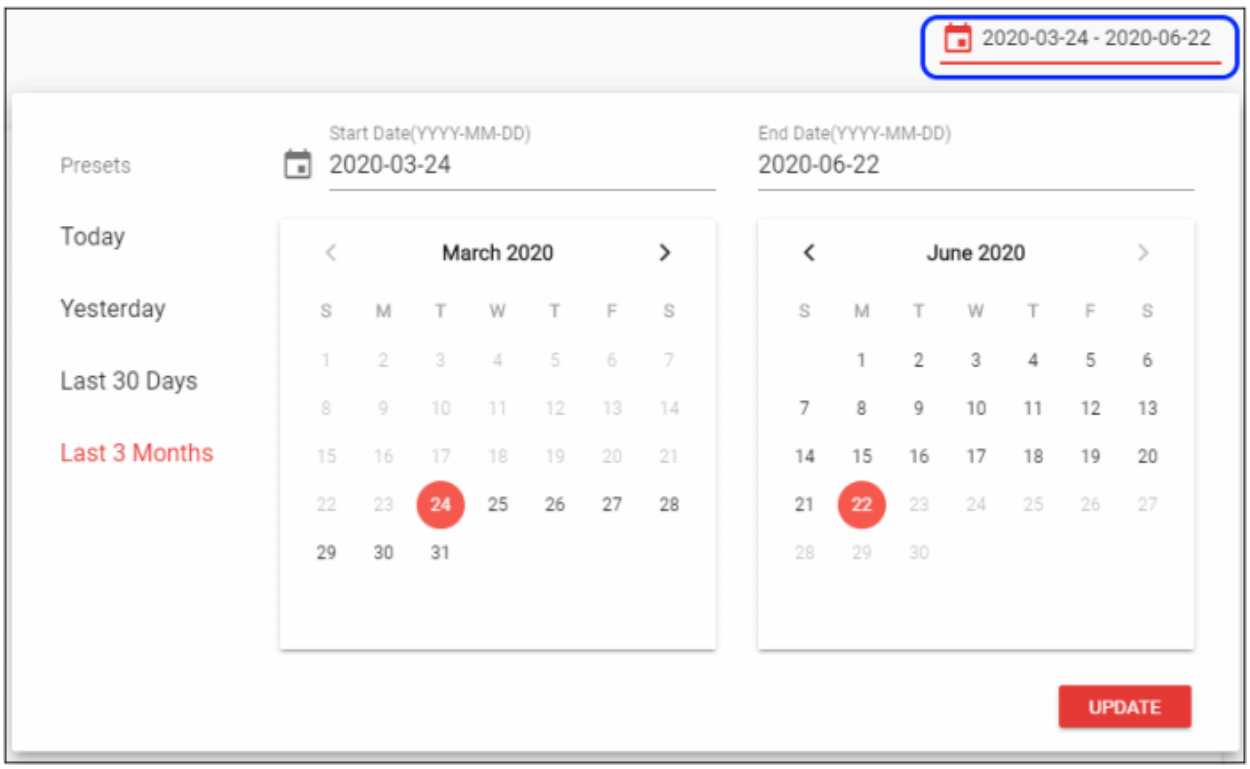
8 Reports

Click 'Reporting' on the left menu

- MDR provides a variety of reports such as endpoint compliance, weekly report and more.

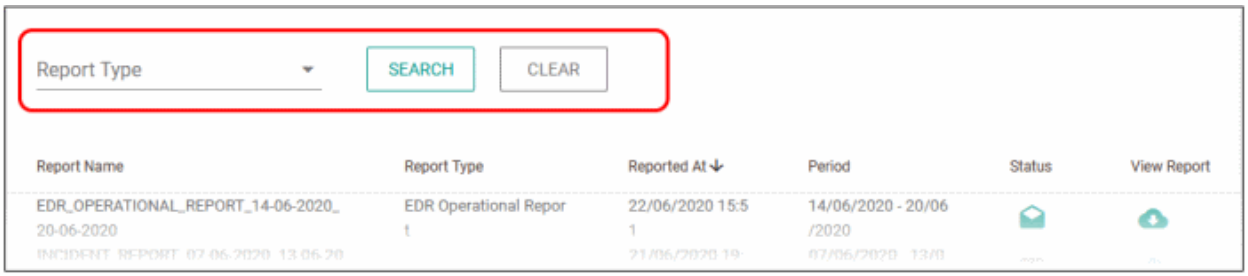


- By default, reports are shown for the past seven days
- To view reports for a different time period, click the date range at the top and choose from the options:



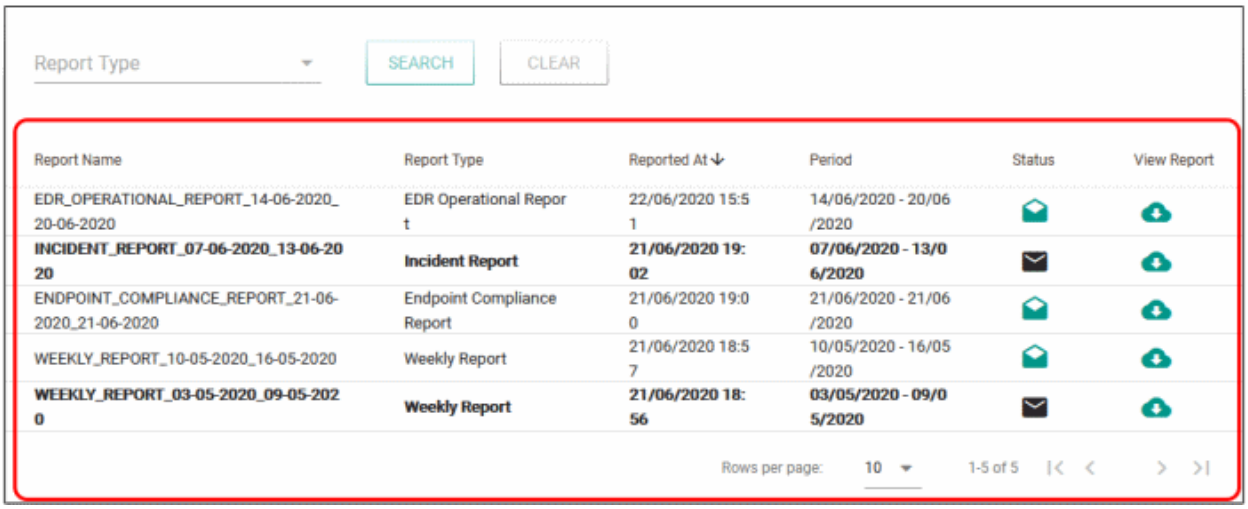
- To view data for a custom period, select from and to dates from the calendars
- Click 'Update'

Use the filters to search for particular reports:



- Select the report type click 'Search'
- Reports matching the filter are shown below.
- Click 'Clear' to view all reports again.

The lower pane shows the reports for the selected time period:

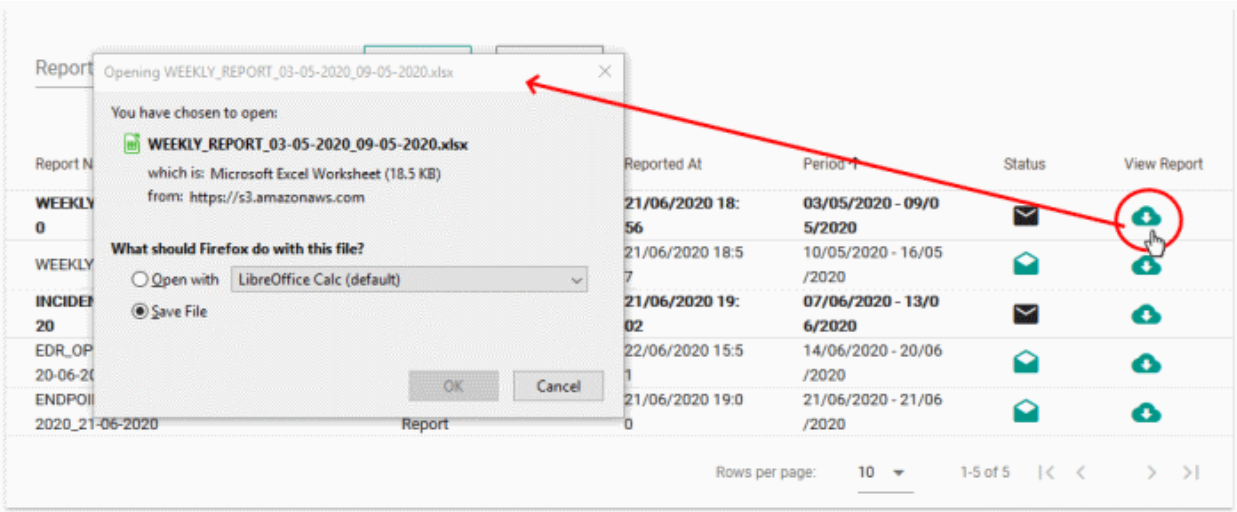


Click a column header to sort the reports by alphabetical / ascending / descending order.

- Report Name – The report label
- Report Type – Report category
- Reported at – Report generated date and time
- Period – Indicates the 'from' and 'to' days for which the report is generated
- Status – Whether the report is downloaded or not. Closed envelope icon indicates the report is not downloaded.
- View Report- Click this to save the report.

Download a report

- Click the arrow in the report row that you want to save:



- Click 'OK' to save the report.

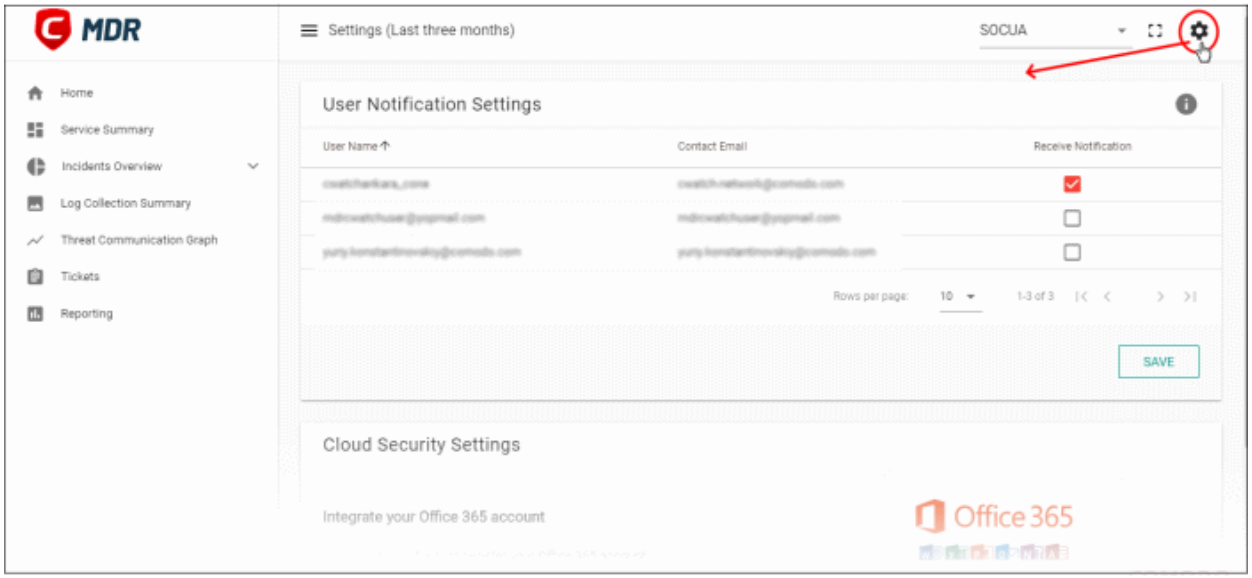
The following report types are generated in MDR.

Report Type	Frequency	Description
Weekly report	Weekly	Report of actionable incidents, unusual network traffic, threat types, log collection summary and more.
EDR operational report	Weekly	The report contains continuous monitoring and response service outputs for advanced threat protection of endpoints.
Dashboard report	On-demand	Total events received from sources such as domain controller, Palo Alto, web proxy, ProffPoint and so on.
Endpoint compliance report	Weekly	Details such as total number of enrolled devices, last reporting status, Comodo anti-virus product version status, new malwares detected in past one week and so on.
Executive report	Monthly	This report includes work summary like investigated and notified incident details and log collection details. Report also contains some analytics on data collected from customer and provides summary about overall security level of the customer.
Threat intelligence report	Monthly	A report of vulnerabilities analyzed by the SOC team on all customer products. It includes the latest threats analyzed as well as the result of SOC checks in the customer networks.
Incident report	Weekly	Contains information about network and system security.

9 Notification Settings

- Configure who should receive alert emails sent by Comodo SOC team. For examples, incident notifications are sent to the selected users.

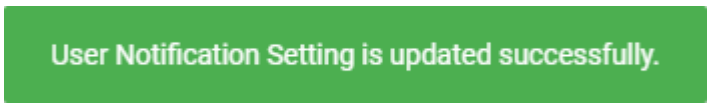
Click the settings icon at top-right to open the screen:



Admins and staff in your portal account (Comodo One, Dragon Platform and ITarian) are shown in the user list.

- **User Name** – User ID of the staff
- **Contact Email** – Email address provided at the time of enrolling the staff. Notification mails are sent to this address.
- **Receive Notification** – Enable / disable for email notification.

Click 'Save' after selecting the users. A confirmation message is shown:



10 Integrate your Office 365 Account with MDR

You can integrate your Office 365 account with MDR so any threats and behavioral anomalies are detected. Once integrated, our SOC team analyzes data logs from your Office 365 account for malware activity and other anomalies.

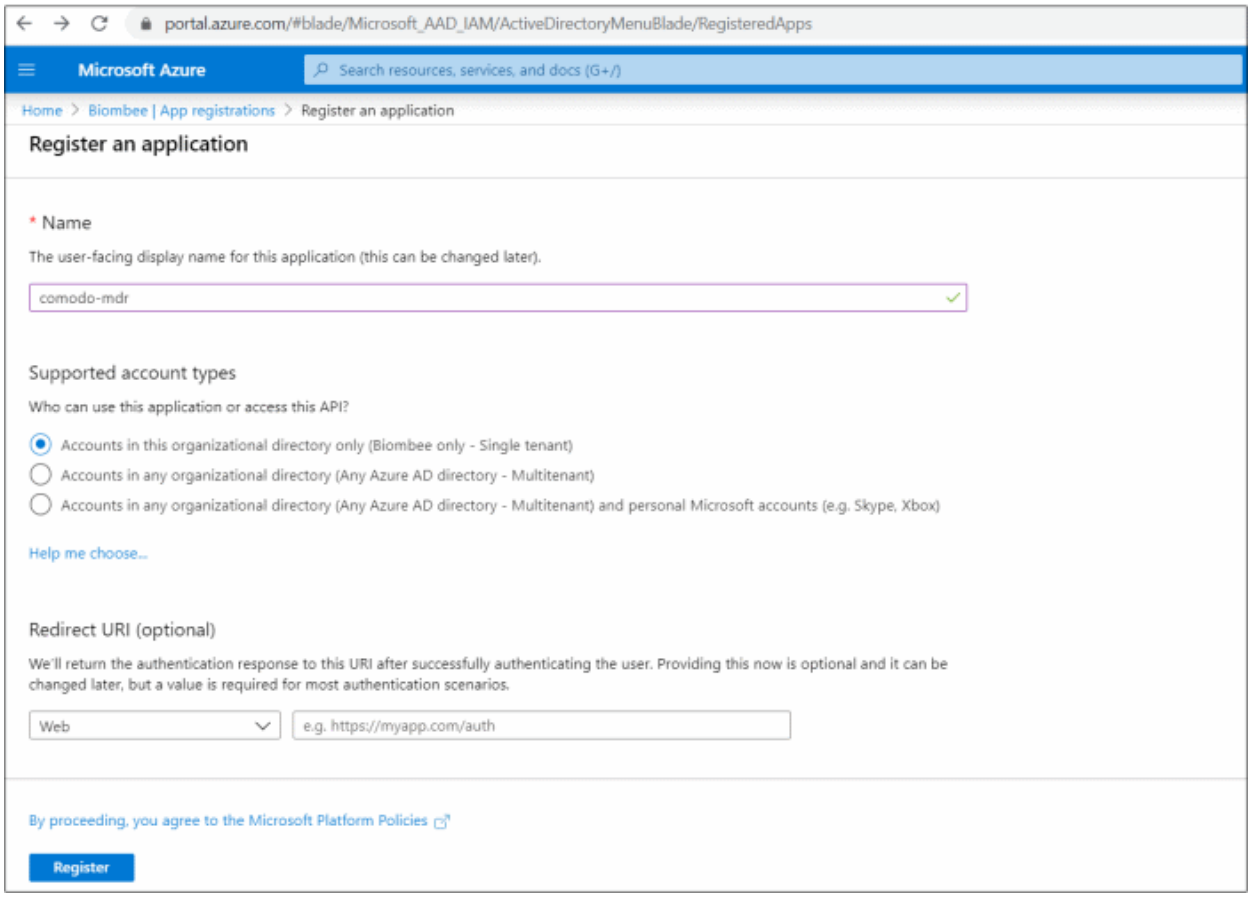
You have to first configure your Azure AD application and MDR so as to collect data.

Configuration Steps

- **Step 1 - Create an API integration application within registry**
- **Step 2 - Create security credentials for registered application**
- **Step 3 - Add permissions for the registered application**
- **Step 4 - Configure MDR with Azure application registration attributes (Tenant Id, Client Id, Secret Key)**

Step 1 - Create an API Integration Application within Registry

- Log into your Azure account (**https://portal.azure.com**).
- Navigate to App registrations and create a new app by clicking '+ New registration'
- Fill application details as shown below:

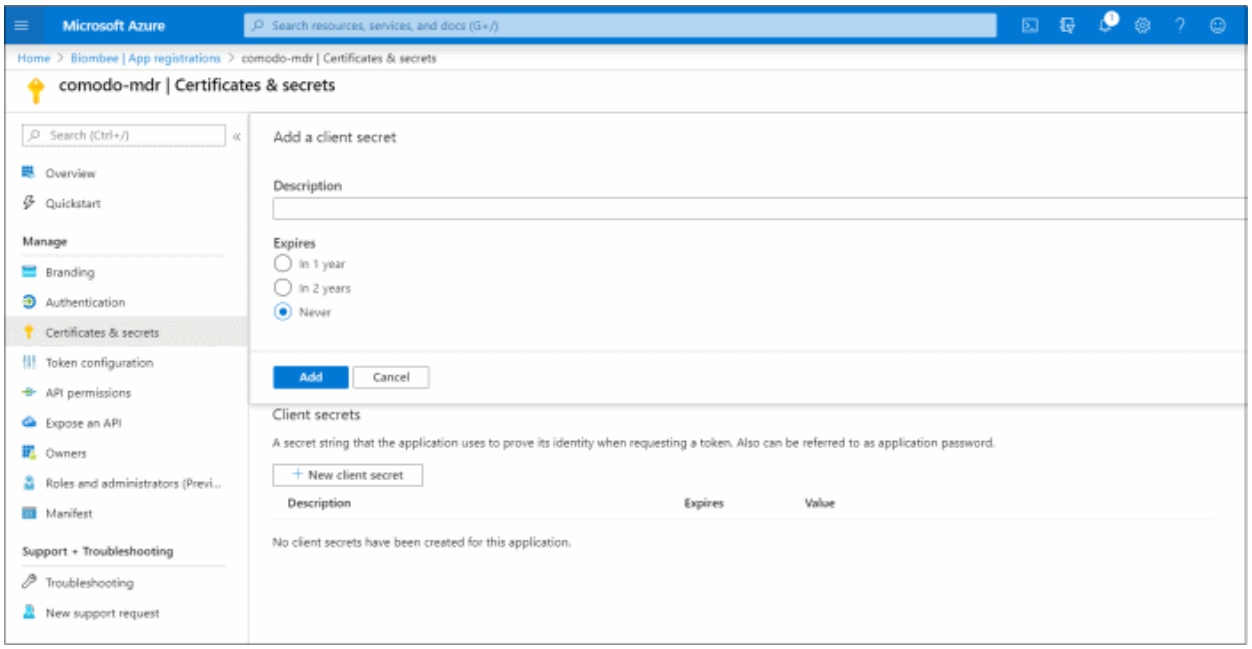


  - **Name:** comodo-mdr (or any other suitable label)
  - **Supported account types:** Choose "Accounts int this organizational directory only"
- Click 'Register'

Note down the Application (client) ID and Directory (tenant) ID.

Step 2 - Create Security Credentials for Registered Application

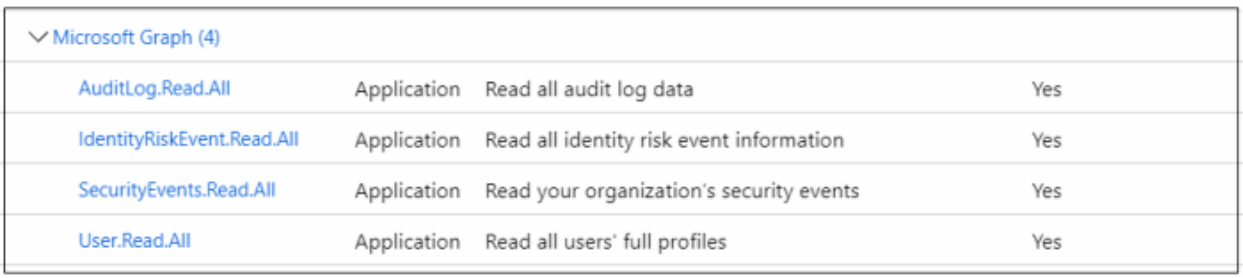
- Click 'Certificates & Secrets' on the left



- Click '+New client secret'
- Create a secret insert description for the key, select expiration of 'Never', then click 'Add' (only then will the key/secret be generated)
- Copy the new client secret value.

Step 3 - Add Permissions for the Registered Application

- Click 'API Permissions' on the left then 'Add a Permission'
- Click 'Microsoft Graph' and select 'Application Permissions'
- Add permissions as shown below:

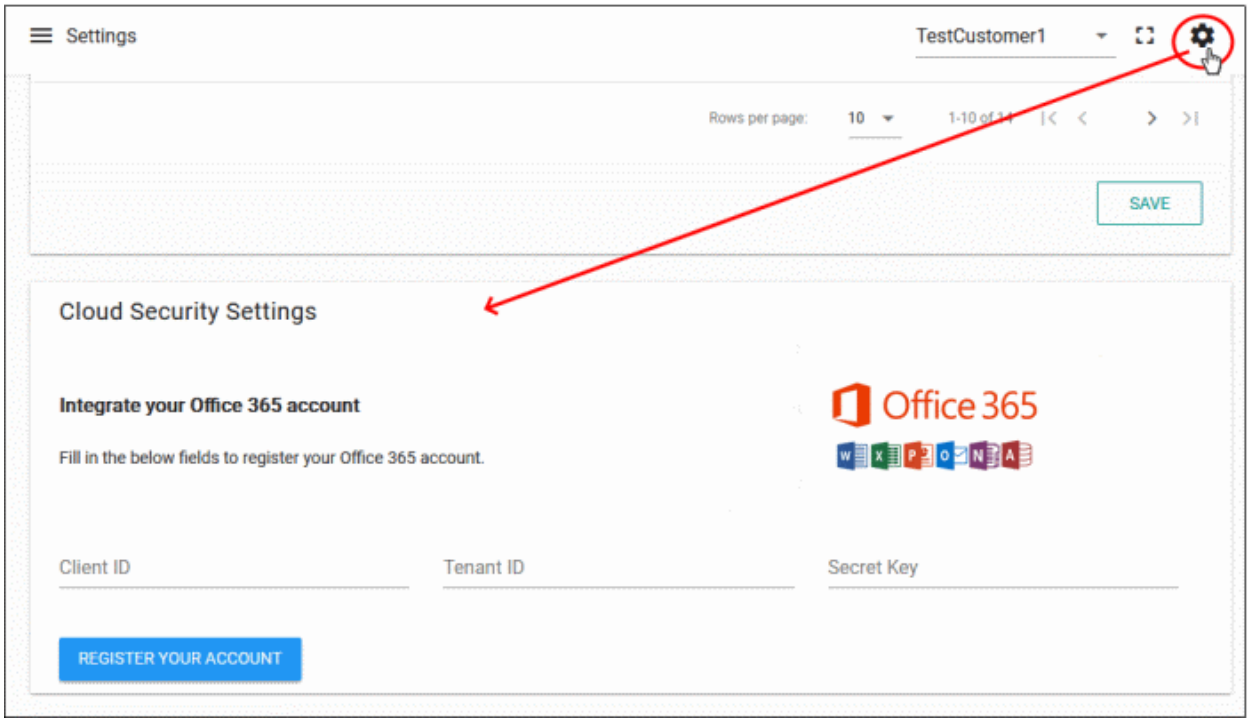


- Click 'Add a permission' again and select 'Office 365 Management API' and toggle 'Application Permissions'.
- Add permissions as shown below:

Office 365 Management APIs (6)			
ActivityFeed.Read	Application	Read activity data for your organization	Yes
ActivityFeed.ReadDlp	Application	Read DLP policy events including detected sensitive data	Yes
ActivityReports.Read	Application	Read activity reports for your organization	Yes
ActivityReports.Read	Application	Read activity reports for your organization	Yes
ThreatIntelligence.Read	Application	Read threat intelligence data for your organization	Yes
ThreatIntelligence.Read	Application	Read threat intelligence data for your organization	Yes

Step 4 - Configure MDR with Azure Application Registration Attributes (Tenant Id, Client Id, Secret Key)

- Log into MDR Customer Portal.
- Click "Settings" at the top left of the screen and scroll down to 'Cloud Security Settings'



- Enter your client ID, tenant ID (generated in **step 1**) and secret key (generated in **step 2**) into the respective fields.
- Click "Register Your Account"

That's it, your Office 365 cloud account is integrated with MDR. Contact your Comodo account manager for support if you have any trouble integrating your cloud account with MDR.

About Comodo Security Solutions

Comodo Security Solutions is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Comodo provides complete, end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats. With over 80 million installations of its threat prevention products, Comodo provides an extensive suite of endpoint, website and network security products for MSPs, enterprises and consumers.

Continual innovation and a commitment to reversing the growth of zero-day malware, ransomware, data-breaches and internet-crime distinguish Comodo Security Solutions as a vital player in today's enterprise and home security markets.

About Comodo Cybersecurity

In a world where preventing all cyberattacks is impossible, Comodo Cybersecurity delivers an innovative cybersecurity platform that renders threats useless, across the LAN, web and cloud. The Comodo Cybersecurity platform enables customers to protect their systems and data against even military-grade threats, including zero-day attacks. Based in Clifton, New Jersey, Comodo Cybersecurity has a 20-year history of protecting the most sensitive data for both businesses and consumers globally. For more information, visit comodo.com or our **blog**. You can also follow us on **Twitter** (@ComodoDesktop) or **LinkedIn**.

1255 Broad Street

Clifton, NJ 07013

United States

Tel : +1.877.712.1309

Tel : +1.888.551.1531

https://www.comodo.com

Email: **EnterpriseSolutions@Comodo.com**