COMODO
Creating Trust Online®

cWatch

Comodo EDR

Software Version 1.7

Quick Start Guide

Guide Version 1.1.042519

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

Comodo EDR - Quick Start

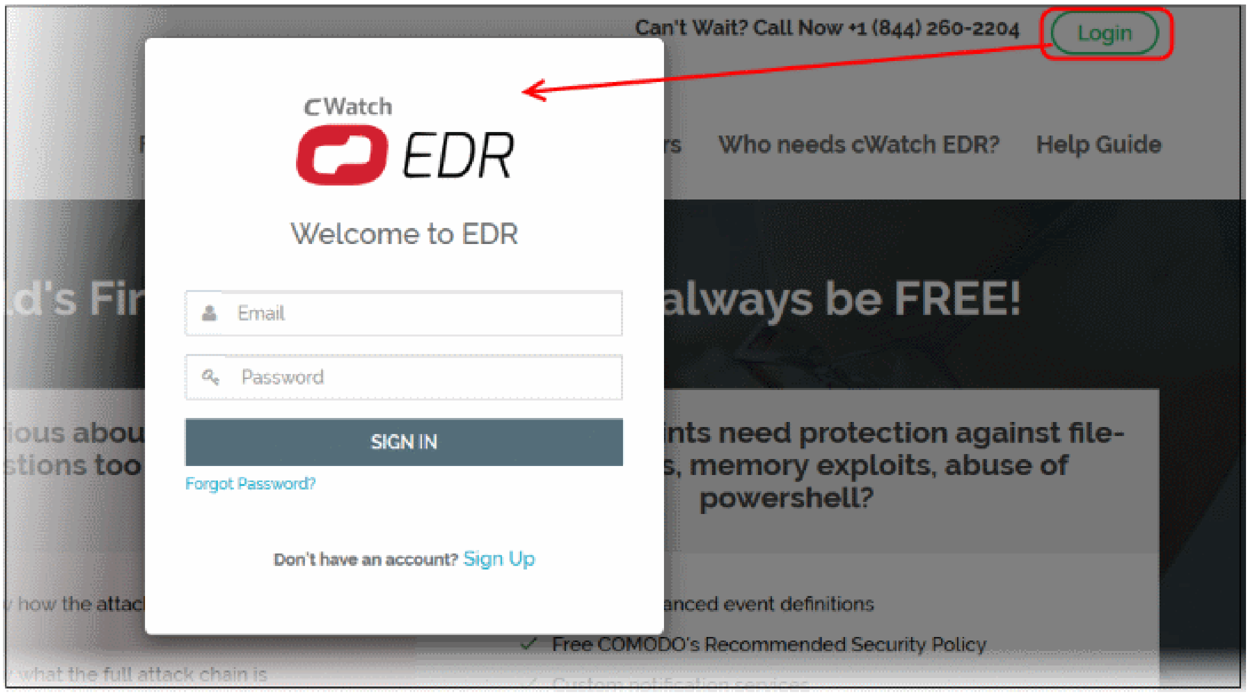
This tutorial explains how to setup Comodo Endpoint Detection and Response (EDR). The guide will take you through the following processes:

Step 1 - Login to EDR

There are two ways to access the EDR interface:

Login at EDR portal

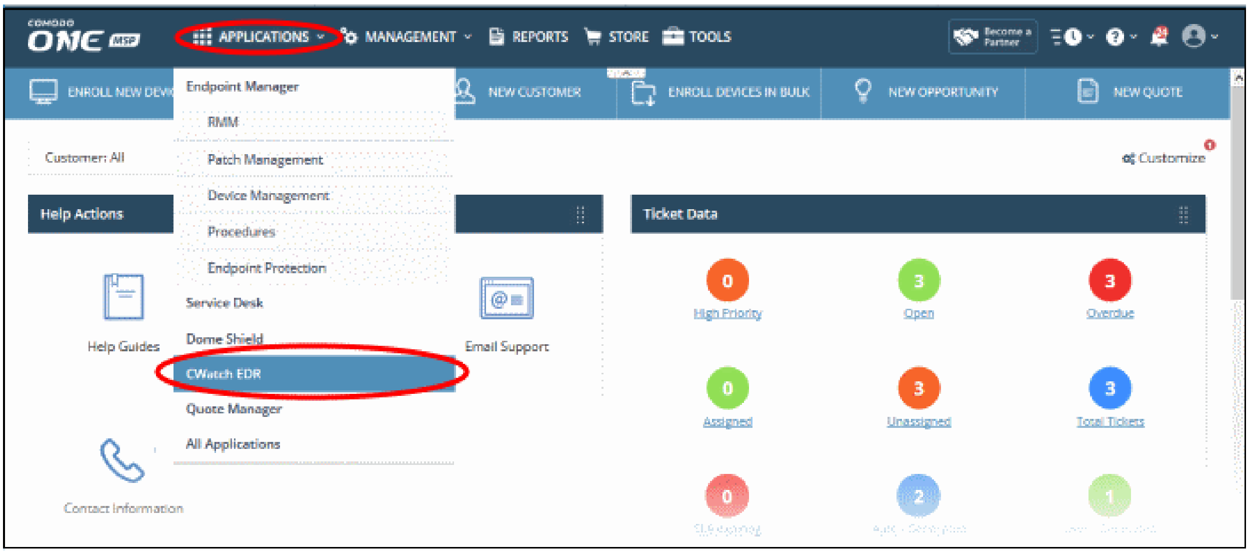
- Go to https://edr.cwatch.comodo.com/login and click 'Login' at top-right:


Can't Wait? Call Now +1 (844) 260-2204
Login
Who needs cWatch EDR?
Help Guide
d's Fir
always be FREE!
ious abou
tions too
nts need protection against file-
s, memory exploits, abuse of
powershell?
how the attac
anced event definitions
✓ Free COMODO's Recommended Security Policy
what the full attack chain is
CWatch
EDR
Welcome to EDR
Email
Password
SIGN IN
Forgot Password?
Don't have an account? Sign Up

- Enter your credentials and click 'Sign in'. Click 'Forgot Password' if you can't remember your password.
- EDR opens at the dashboard after you login.

Comodo One MSP Customers:

- Login to your account at https://one.comodo.com
- Click 'Applications' > 'cWatch EDR' to open the application in new tab:



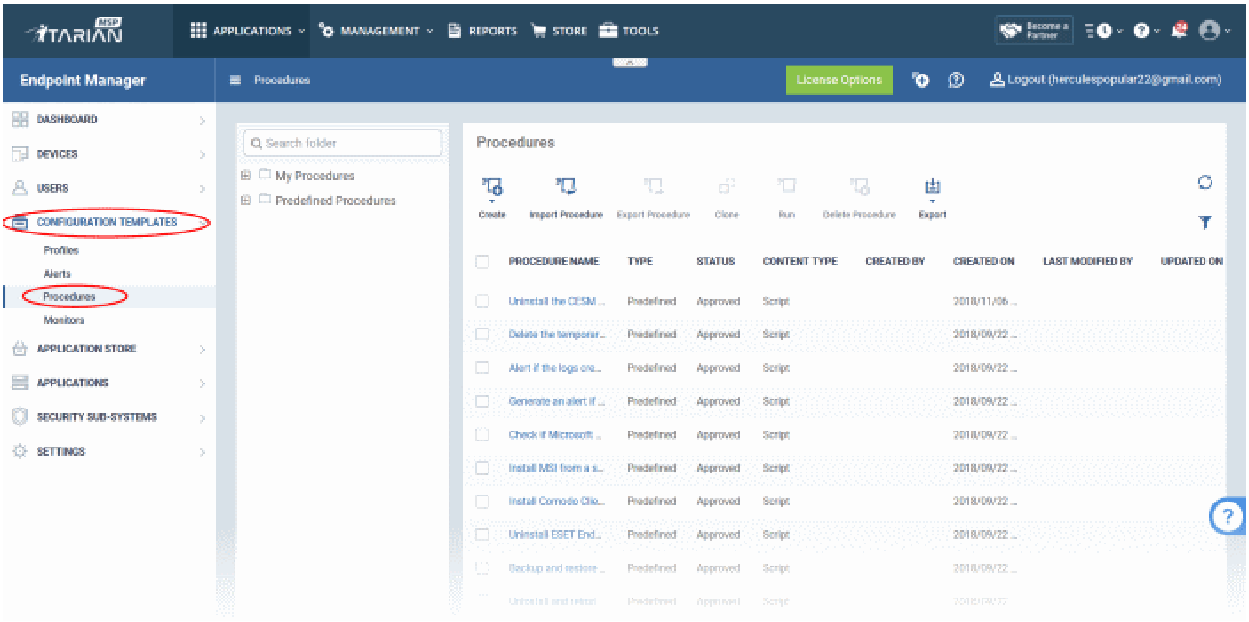
Step 2 - Add Endpoints to EDR

You need to install the EDR agent on all endpoints that you wish to monitor. There are two ways to do this:

1. Individual Endpoints.
   - Click 'Download Agent' at the bottom-left of the EDR interface
   - Install the agent on every target machine
   - Click here to view a tutorial on this process

2. **Group Policy Management (GPO).** See the GPO guide at https://help.comodo.com/topic-444-1-910-11939-Introduction-to-Agent-Deployment-via-GPO.html for help with this.

3. **Script execution via Endpoint Manager.** Use an Endpoint Manager script to deploy the agent. You can download the script from: https://scripts.comodo.com/frontend/web/topic/enroll-comodo-edr-agent



PROCEDURE NAME	TYPE	STATUS	CONTENT TYPE	CREATED BY	CREATED ON	LAST MODIFIED BY	UPDATED ON
Uninstall the CESM ...	Predefined	Approved	Script		2018/11/06 ...		
Delete the temporar...	Predefined	Approved	Script		2018/09/22 ...		
Alert if the logs cre...	Predefined	Approved	Script		2018/09/22 ...		
Generate an alert if ...	Predefined	Approved	Script		2018/09/22 ...		
Check if Microsoft ...	Predefined	Approved	Script		2018/09/22 ...		
Install MSI from a s...	Predefined	Approved	Script		2018/09/22 ...		
Install Comodo Clie...	Predefined	Approved	Script		2018/09/22 ...		
Uninstall ESET End...	Predefined	Approved	Script		2018/09/22 ...		
Backup and restore ...	Predefined	Approved	Script		2018/09/22 ...		
Uninstall and reinst	Predefined	Approved	Script		2018/09/22		

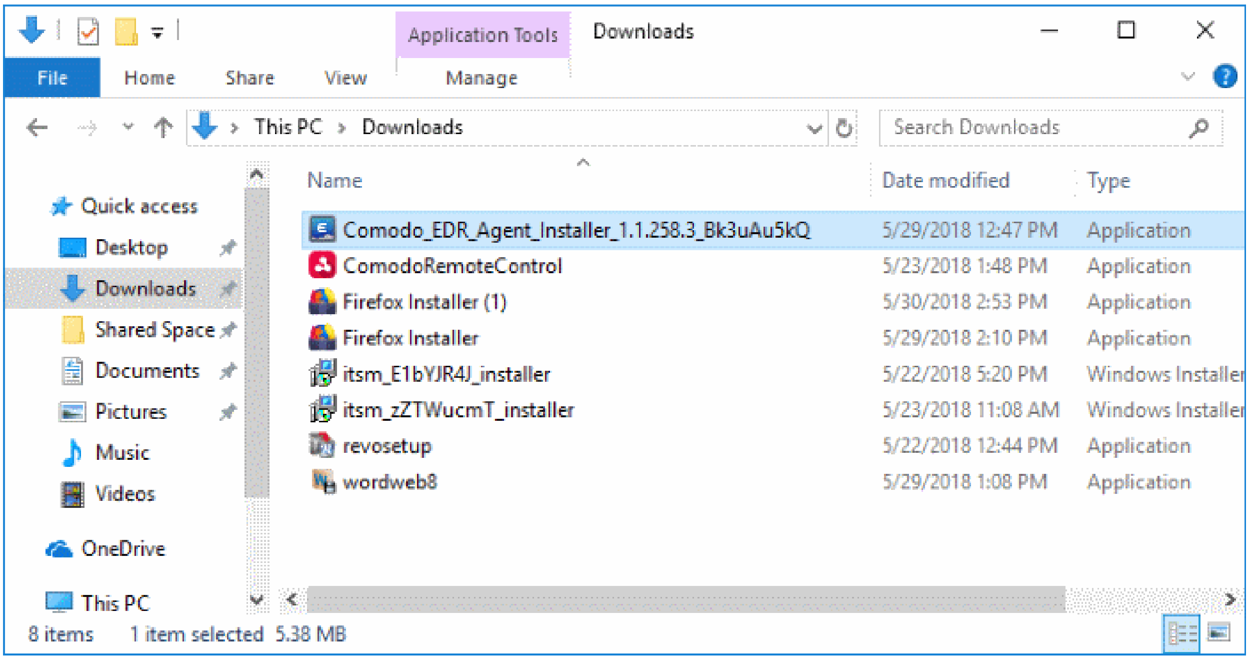
You need to create a custom procedure in Endpoint Manager to run the script:

- Login at https://one.comodo.com
- Click 'Applications' > 'Endpoint Manager'
- Click 'Configuration Templates' > 'Procedures'
- Click 'Create' > 'Create Script Procedure'
- The script you downloaded earlier goes in the 'View Procedure' tab. Please remember you need to modify this script to suit your use case.

See '**Create a custom procedure**' for help to create a custom script.

Add endpoints individually

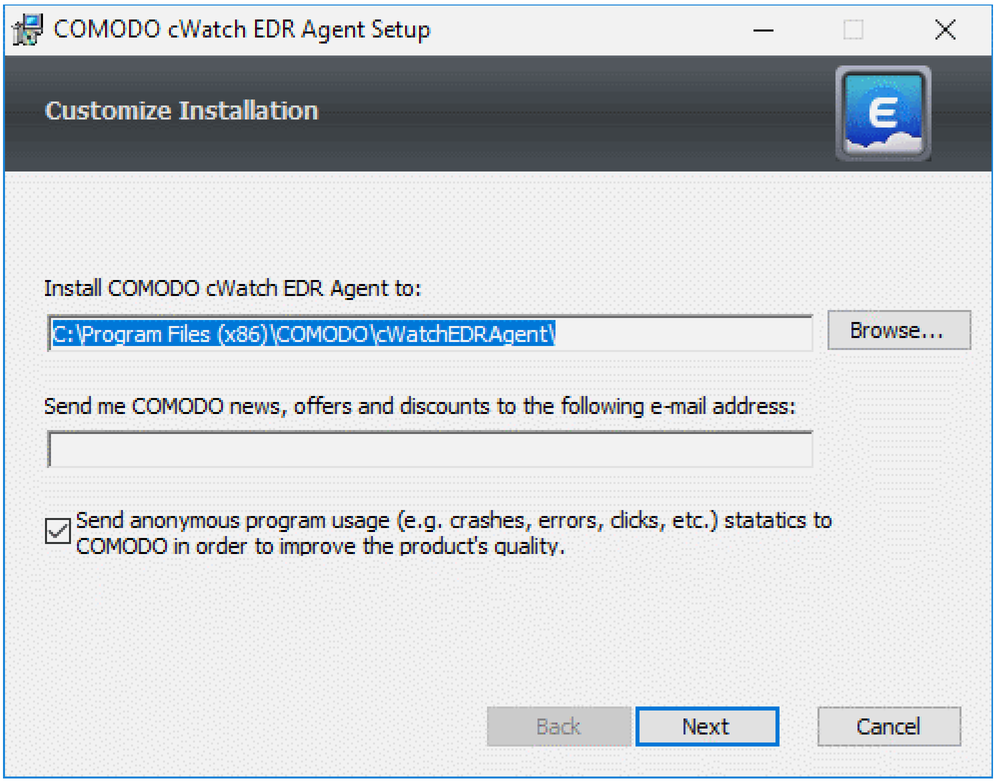
- **Login** to your EDR account from each endpoint and download the agent from there.
- Click 'Download Agent' in the left menu.



Name	Date modified	Type
Comodo_EDR_Agent_Installer_1.1.258.3_Bk3uAu5kQ	5/29/2018 12:47 PM	Application
ComodoRemoteControl	5/23/2018 1:48 PM	Application
Firefox Installer (1)	5/30/2018 2:53 PM	Application
Firefox Installer	5/29/2018 2:10 PM	Application
itsm_E1bYJR4J_installer	5/22/2018 5:20 PM	Windows Installer
itsm_zZTWucmT_installer	5/23/2018 11:08 AM	Windows Installer
revosetup	5/22/2018 12:44 PM	Application
wordweb8	5/29/2018 1:08 PM	Application

8 items 1 item selected 5.38 MB

- Open the setup file to start the installer



COMODO cWatch EDR Agent Setup

Customize Installation

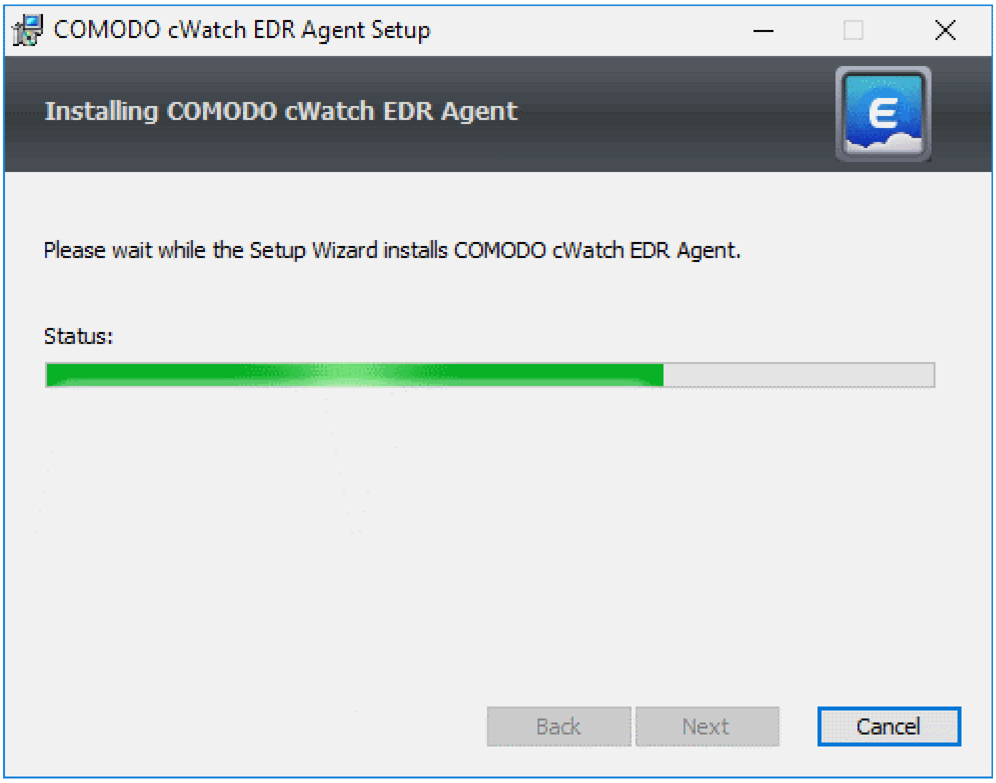
Install COMODO cWatch EDR Agent to:

C:\Program Files (x86)\COMODO\cWatchEDRAgent\

Send me COMODO news, offers and discounts to the following e-mail address:

☑ Send anonymous program usage (e.g. crashes, errors, clicks, etc.) statatics to COMODO in order to improve the product's quality.

- The default installation location is C:\Program Files (x86)\COMODO\cWatchEDRAgent\. Click 'Browse...' to choose a different installation location.
- Click 'Next' to continue the installation



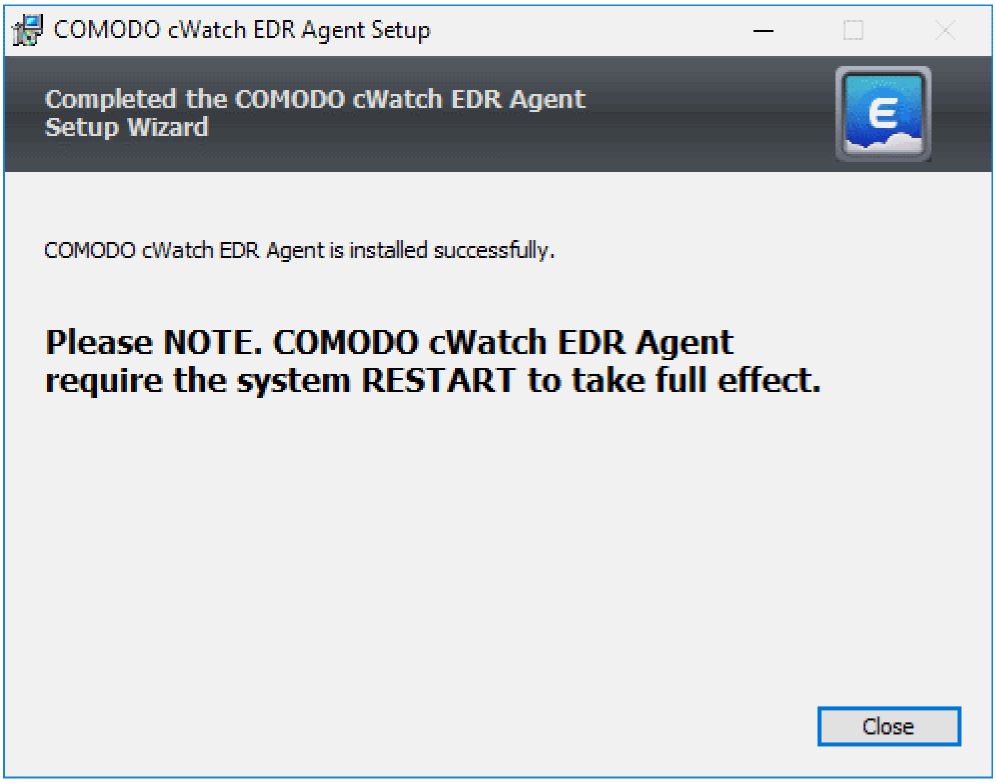
COMODO cWatch EDR Agent Setup

Installing COMODO cWatch EDR Agent

Please wait while the Setup Wizard installs COMODO cWatch EDR Agent.

Status:

You must restart the endpoint to complete the installation:



COMODO cWatch EDR Agent Setup

Completed the COMODO cWatch EDR Agent Setup Wizard

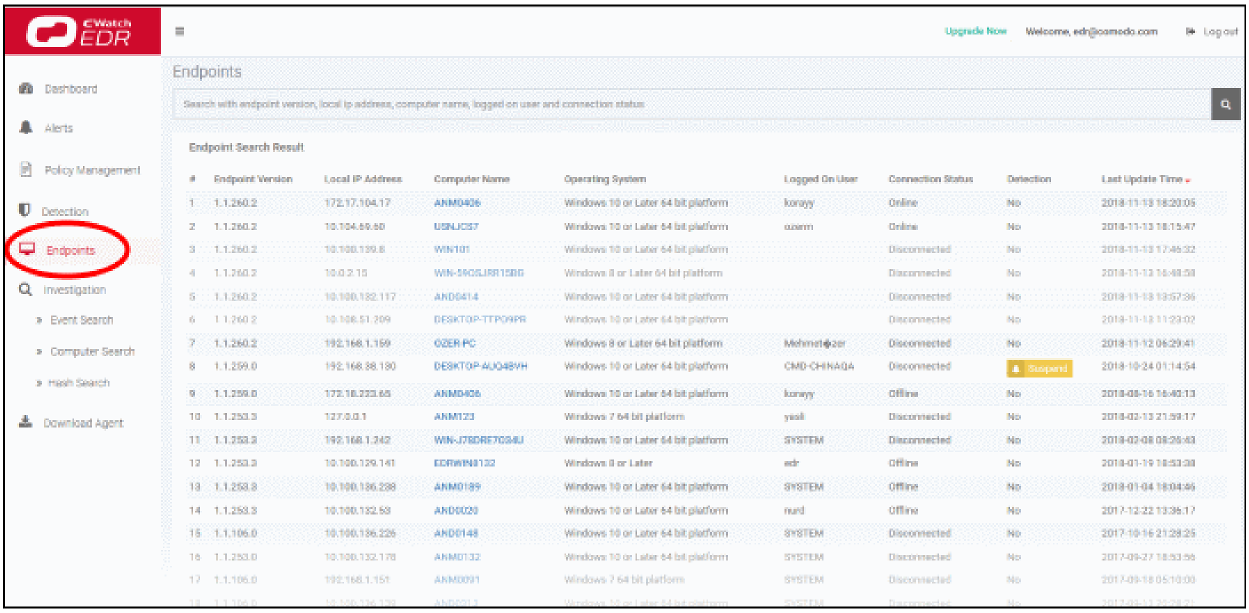
COMODO cWatch EDR Agent is installed successfully.

Please NOTE. COMODO cWatch EDR Agent require the system RESTART to take full effect.

- Click 'Close'
- Restart the endpoint to finalize the installation.

That's it. The endpoint now is enrolled to EDR and can be found in the 'Endpoints' area:

- Login to EDR as described earlier
- Click 'Endpoints' in the left-menu. This area lists all endpoints you have added to EDR:



Endpoints

Search with endpoint version, local ip address, computer name, logged on user and connection status

Endpoint Search Result

#	Endpoint Version	Local IP Address	Computer Name	Operating System	Logged On User	Connection Status	Detection	Last Update Time
1	1.1.260.2	172.17.104.17	ANM0406	Windows 10 or Later 64 bit platform	korayy	Online	No	2018-11-13 18:20:05
2	1.1.260.2	10.104.69.60	USNJC57	Windows 10 or Later 64 bit platform	ozerm	Online	No	2018-11-13 18:15:47
3	1.1.260.2	10.100.139.8	WIN101	Windows 10 or Later 64 bit platform		Disconnected	No	2018-11-13 17:46:32
4	1.1.260.2	10.0.2.15	WIN-59OSLIRR15BG	Windows 8 or Later 64 bit platform		Disconnected	No	2018-11-13 16:48:58
5	1.1.260.2	10.100.132.117	AND0414	Windows 10 or Later 64 bit platform		Disconnected	No	2018-11-13 13:57:36
6	1.1.260.2	10.108.51.209	DESKTOP-TTPO9PR	Windows 10 or Later 64 bit platform		Disconnected	No	2018-11-13 11:23:02
7	1.1.260.2	192.168.1.159	OZER PC	Windows 8 or Later 64 bit platform	Mehmetözer	Disconnected	No	2018-11-12 06:29:41
8	1.1.259.0	192.168.88.130	DESKTOP-AUQ48VH	Windows 10 or Later 64 bit platform	CMD-CHINAQA	Disconnected	Suspend	2018-10-24 01:14:54
9	1.1.259.0	172.18.223.65	ANM0406	Windows 10 or Later 64 bit platform	korayy	Offline	No	2018-08-16 16:40:13
10	1.1.253.3	127.0.0.1	ANM123	Windows 7 64 bit platform	yasli	Disconnected	No	2018-02-13 21:59:17
11	1.1.253.3	192.168.1.242	WIN-J78DRF7C04U	Windows 10 or Later 64 bit platform	SYSTEM	Disconnected	No	2018-02-08 08:26:43
12	1.1.253.3	10.100.129.141	EDRWIN8132	Windows 8 or Later	edr	Offline	No	2018-01-19 18:53:38
13	1.1.253.3	10.100.186.238	ANM0189	Windows 10 or Later 64 bit platform	SYSTEM	Offline	No	2018-01-04 18:04:46
14	1.1.253.3	10.100.132.53	AND0020	Windows 10 or Later 64 bit platform	nurd	Offline	No	2017-12-22 13:36:17
15	1.1.106.0	10.100.136.226	AND0148	Windows 10 or Later 64 bit platform	SYSTEM	Disconnected	No	2017-10-16 21:28:25
16	1.1.253.0	10.100.132.178	ANM0132	Windows 10 or Later 64 bit platform	SYSTEM	Disconnected	No	2017-09-27 18:53:56
17	1.1.106.0	192.168.1.151	ANM0091	Windows 7 64 bit platform	SYSTEM	Disconnected	No	2017-09-18 05:10:00
18	1.1.106.0	10.100.136.139	AND0013	Windows 10 or Later 64 bit platform	SYSTEM	Disconnected	No	2017-09-13 20:28:21

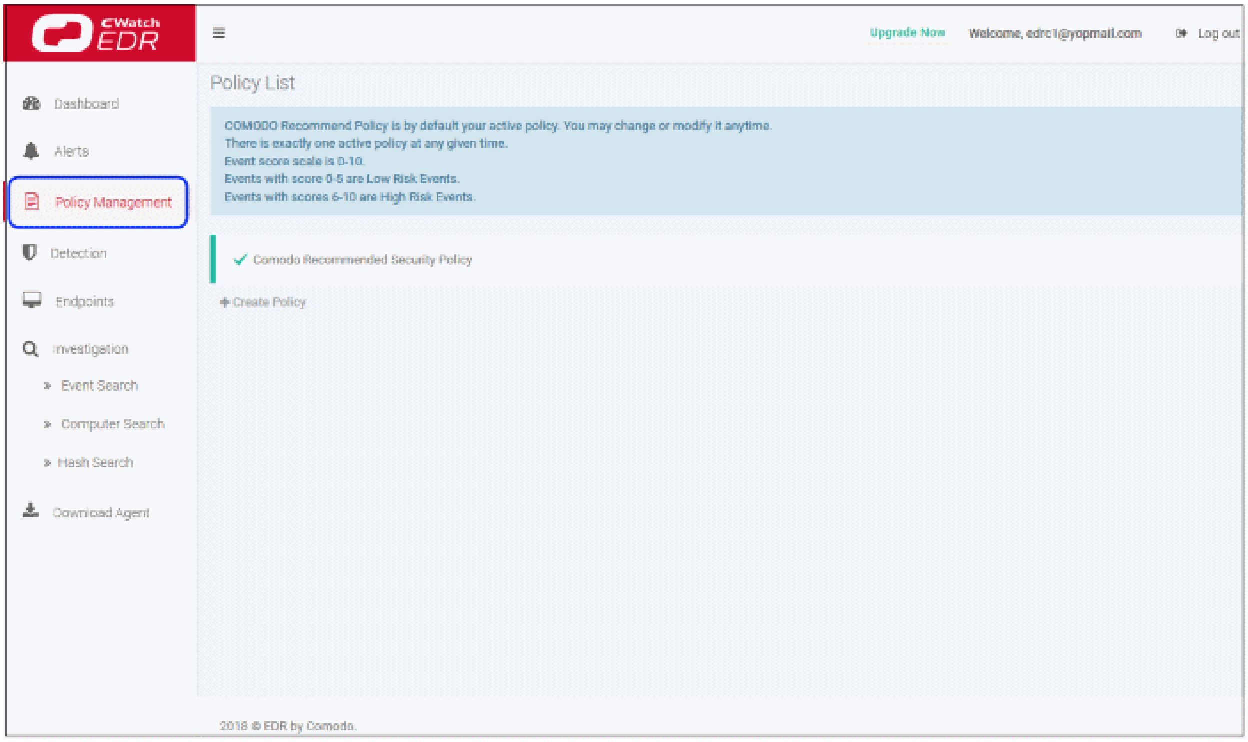
Step 3 - Manage EDR Policies

- An EDR policy determines which events will generate an alert for you.
- There are 7 event categories. You can define specific rules within each category.
- Comodo EDR ships with a default security policy that is applied to all enrolled endpoints.
- You can also create custom policies according to your requirements.
- Only one policy can be active at a time. You cannot delete the active policy.

Note. EDR policies do not determine which events are monitored and logged, they determine which events you *receive alerts* for. cWatch automatically logs all events and submits suspicious files to Valkyrie for analysis, regardless of EDR policy. This means cWatch will always catch zero-day malware, even if you prefer to disable some alerts in a policy.

You can search raw logs in the 'Investigation' screen.

- Click 'Policy Management' on the left to manage EDR security policies:



Policy List

COMODO Recommend Policy is by default your active policy. You may change or modify it anytime.
There is exactly one active policy at any given time.
Event score scale is 0-10.
Events with score 0-5 are Low Risk Events.
Events with scores 6-10 are High Risk Events.

✓ Comodo Recommended Security Policy

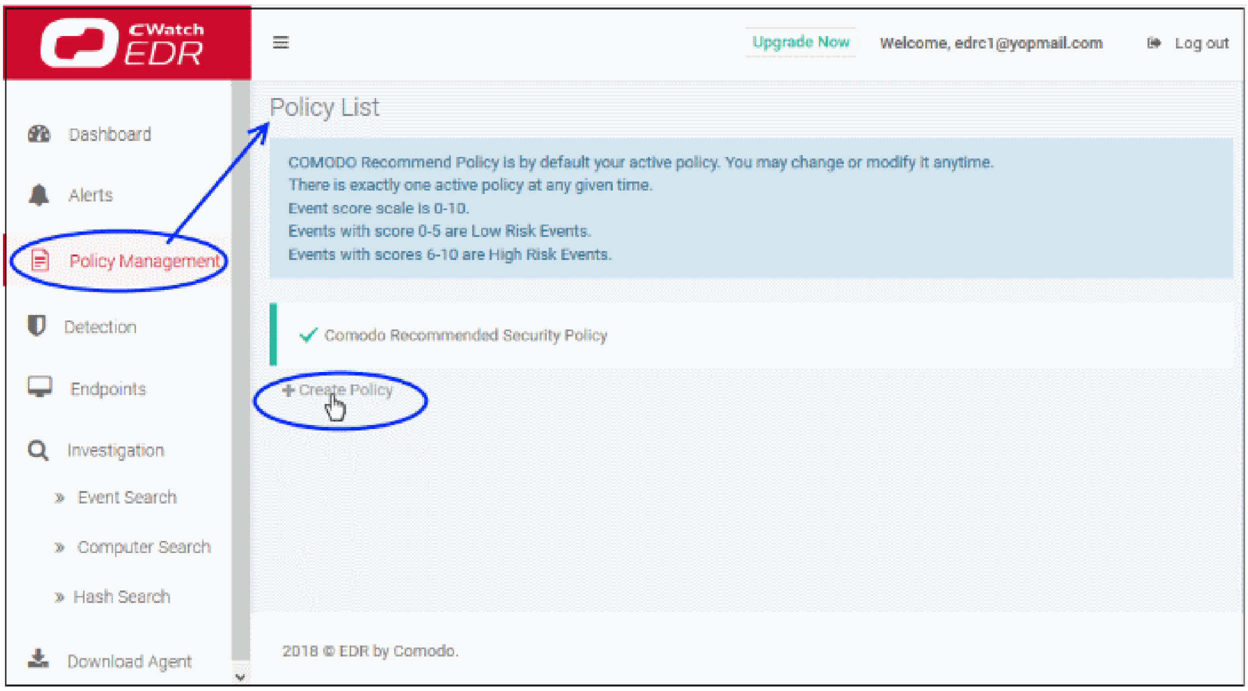
+ Create Policy

2018 © EDR by Comodo.

- The screen shows general information about policies and lists the default 'Comodo Recommended Security Policy'.
- A check-mark beside a policy indicates it is currently active.

Create and Activate a Policy

- Click 'Create Policy':



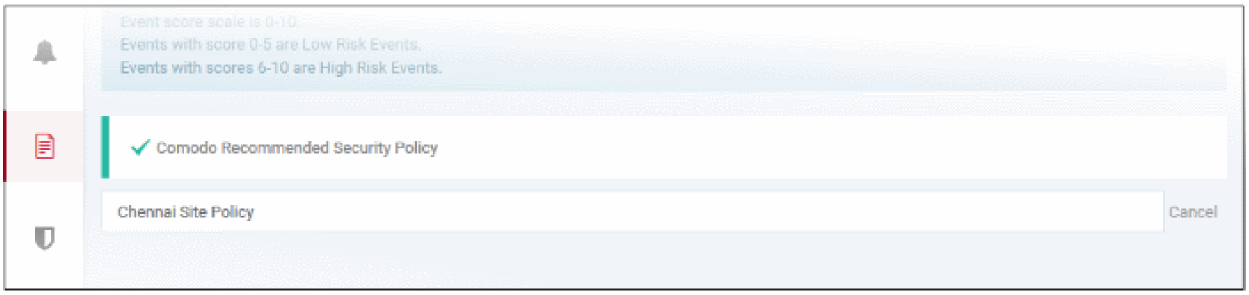
Policy List

COMODO Recommend Policy is by default your active policy. You may change or modify it anytime.
There is exactly one active policy at any given time.
Event score scale is 0-10.
Events with score 0-5 are Low Risk Events.
Events with scores 6-10 are High Risk Events.

✓ Comodo Recommended Security Policy

2018 © EDR by Comodo.

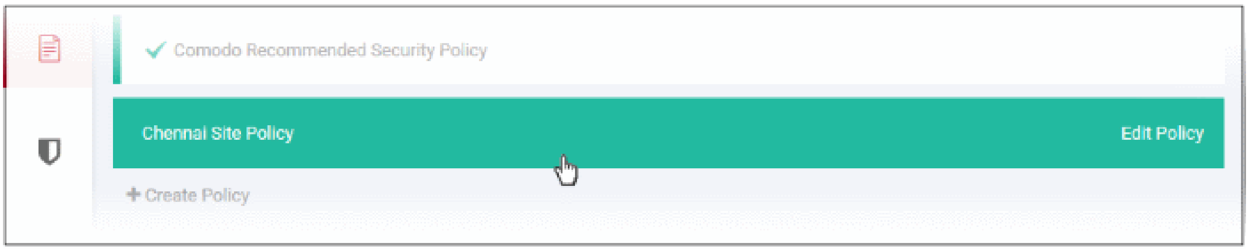
- Create a name for the policy and press enter:


Event score scale is 0-10.
Events with score 0-5 are Low Risk Events.
Events with scores 6-10 are High Risk Events.

✓ Comodo Recommended Security Policy

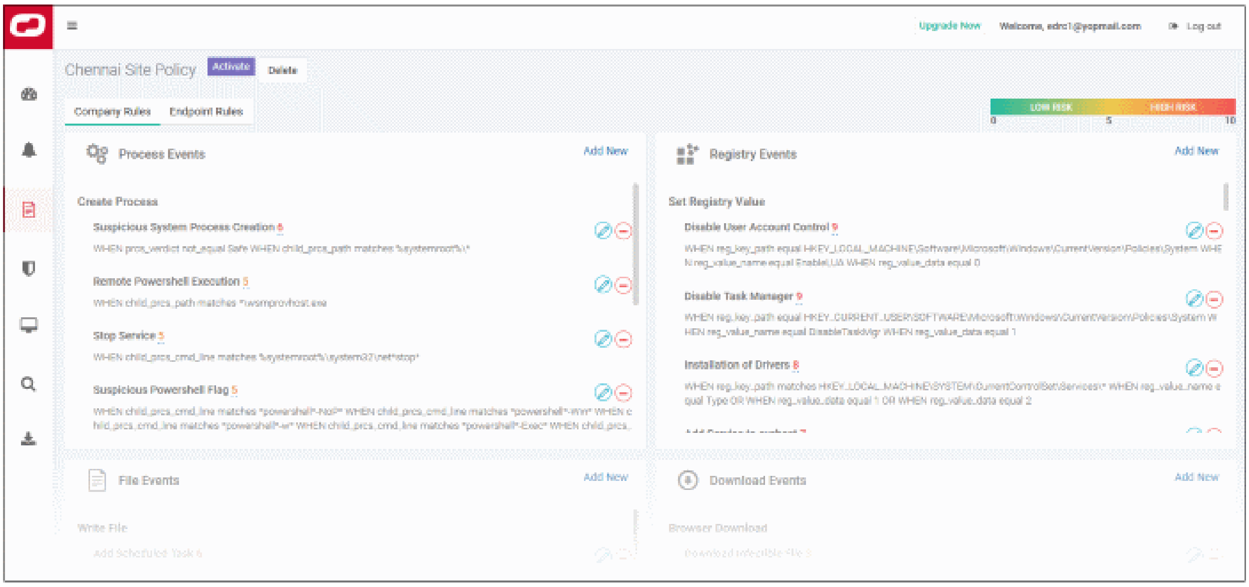
Chennai Site Policy

- Now, click on the policy name to view and edit its current details:


✓ Comodo Recommended Security Policy

Chennai Site Policy

- The new policy is automatically assigned a set of default rules.
- You can add new rules, edit or delete rules as required.



Create Process

Suspicious System Process Creation 6

WHEN prcs_verdict not_equal Safe WHEN child_prcs_path matches %systemroot%*

Remote Powershell Execution 5

WHEN child_prcs_path matches *\wsmprovhost.exe

Stop Service 5

WHEN child_prcs_cmd_line matches %systemroot%\system32\net*stop*

Suspicious Powershell Flag 5

WHEN child_prcs_cmd_line matches *powershell*-NoP* WHEN child_prcs_cmd_line matches *powershell*-Win* WHEN child_prcs_cmd_line matches *powershell*-w* WHEN child_prcs_cmd_line matches *powershell*-Exec* WHEN child_prcs...

Set Registry Value

Disable User Account Control 9

WHEN reg_key_path equal HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System WHEN reg_value_name equal EnableLUA WHEN reg_value_data equal 0

Disable Task Manager 9

WHEN reg_key_path equal HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System WHEN reg_value_name equal DisableTaskMgr WHEN reg_value_data equal 1

Installation of Drivers 8

WHEN reg_key_path matches HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\* WHEN reg_value_name equal Type OR WHEN reg_value_data equal 1 OR WHEN reg_value_data equal 2

Write File

Add Scheduled Task 6

Browser Download

Download Infectible File 3

The policy interface has two tabs - 'Company Rules' and 'Endpoint Rules'.

- **Company Rules** - Create rules by event category. Company rules are applied to all protected endpoints. See '**Company Rules**' for more information.
- **Endpoint Rules** - Create additional conditions for each event category and apply to specific endpoints. See '**Endpoint Rules**' for more details.

Company Rules

There are seven event categories in the company rules section.

Each category has conditions or rules that can be implemented in your policy. You can create new conditions and edit or delete a condition from an category.

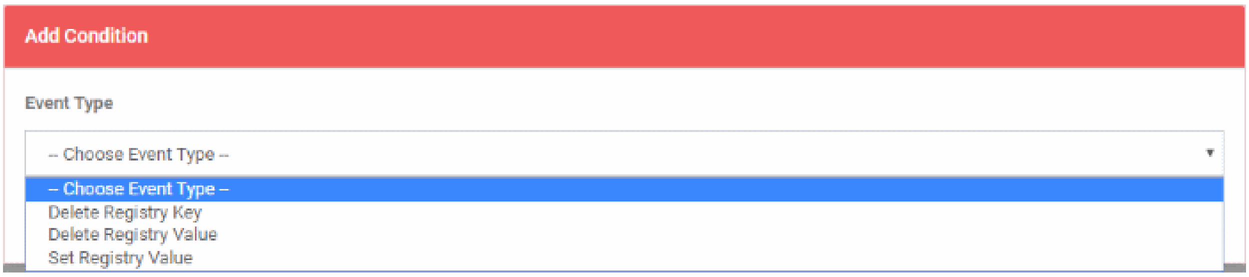
The built-in event categories are:

- **Process Events** - Rules to alert you when processes are invoked by an application
- **Registry Events** - Rules to alert you about changes to the Windows registry on your endpoints.
- **File Events** - Rules to alert you about modifications to system files.
- **Download Events** - Rules to alert you when files are downloaded via browsers, emails, shared folders or external drives.
- **Upload Events** - Rules to alert you when files are transferred to shared folders or external drives.
- **Defense+ Events** - Rules to alert you when processes attempt to access critical operating system functions or launch attacks.
- **Network Events** - Rules to alert you about any service listening to ports and network connections on your endpoints.

To create a new condition

- Click 'Add New' at the top of an event category:

The 'Add Condition' dialog will open:



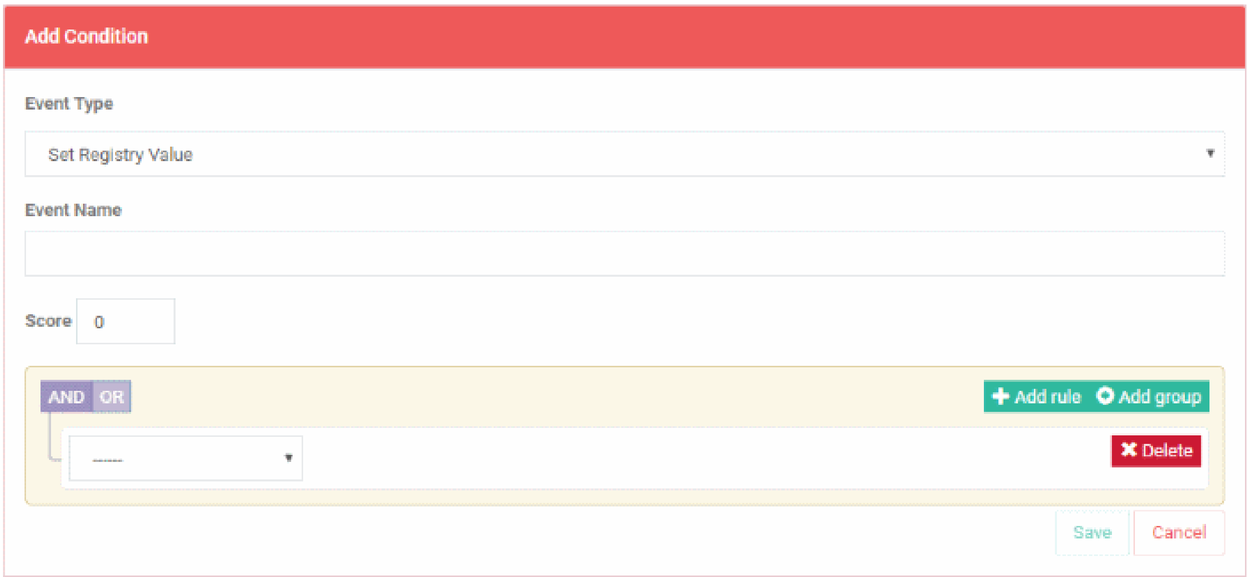
Add Condition

Event Type

-- Choose Event Type --

-- Choose Event Type --
Delete Registry Key
Delete Registry Value
Set Registry Value

- '**Event Type**' - choose the type of incident that you want EDR to detect. The event types available depend on the event category chosen.
- In the example above, the category is 'Registry Events', so the available event types are 'Delete Registry Key', 'Delete Registry Value' and 'Set Registry Value'.
- After choosing a type, you must next construct your condition. You do this by choosing the specific criteria which should be monitored. Again, the criteria vary by event category and event type.
- In the example above we will chose 'Registry Events' > 'Set Registry Value'. The available criteria for 'Set Registry Value' let you specify which key names, values or paths should be monitored.



Add Condition

Event Type

Set Registry Value

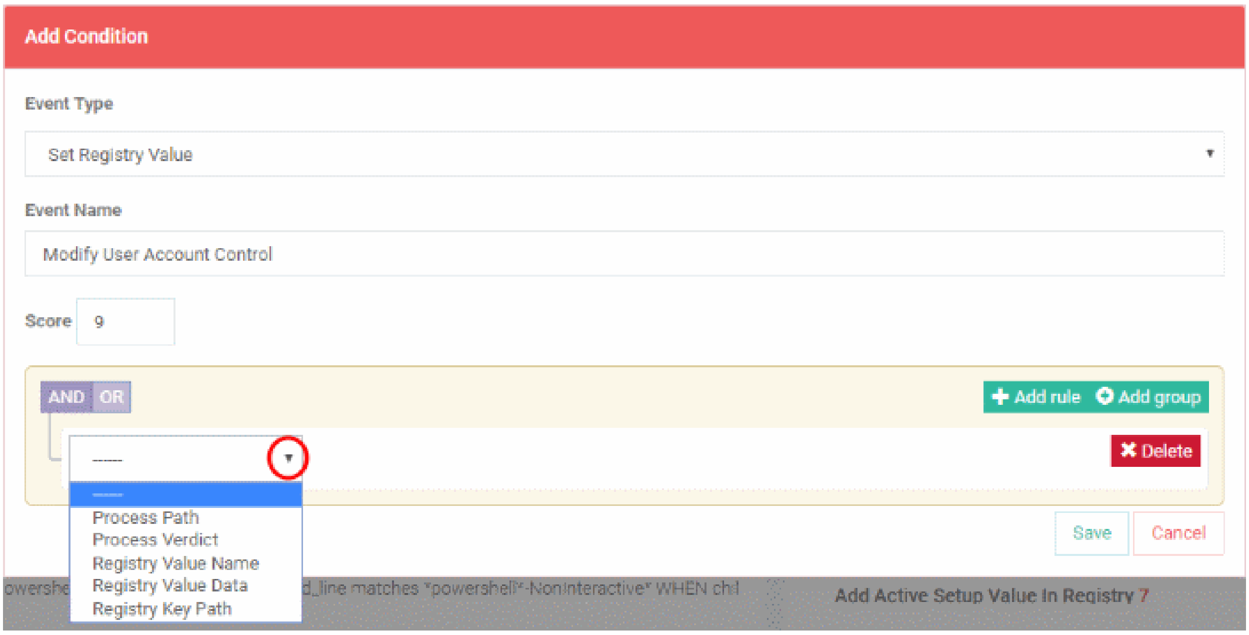
Event Name

Score 0

- Event Name - Create a label for your condition. This label will be shown as 'Alert Name' in the 'Alerts' interface.
- Score - Rate the event according to how seriously you judge the incident. Scores range from 0 to 10.
  - Scores 0 to 5 - Low risk events
  - Scores 6 to 10 - High risk events

The next step is configure the parameters and conditions for the rule.

- Click the arrow below 'AND/OR'



Add Condition

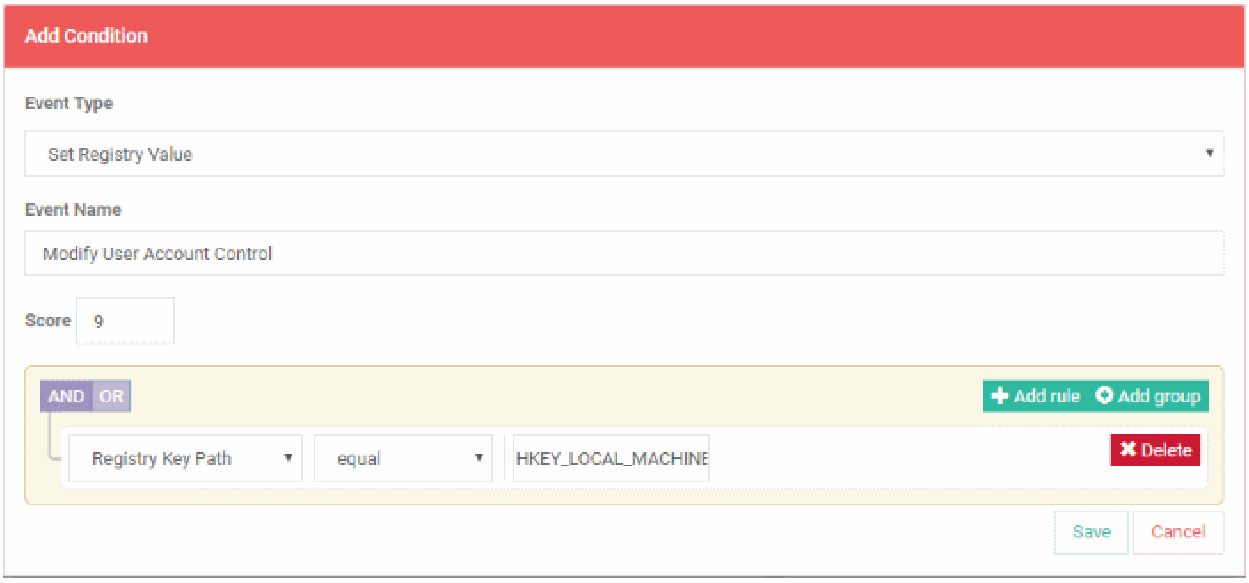
Event Type: Set Registry Value

Event Name: Modify User Account Control

Score: 9

The parameters depend on the selected category and event type.

- Choose the parameter you wish to monitor
- In the second box select the condition. The conditions list varies for different parameters.
- In the third box, enter or select the value. You have to enter the value or select depending on the parameter.



Add Condition

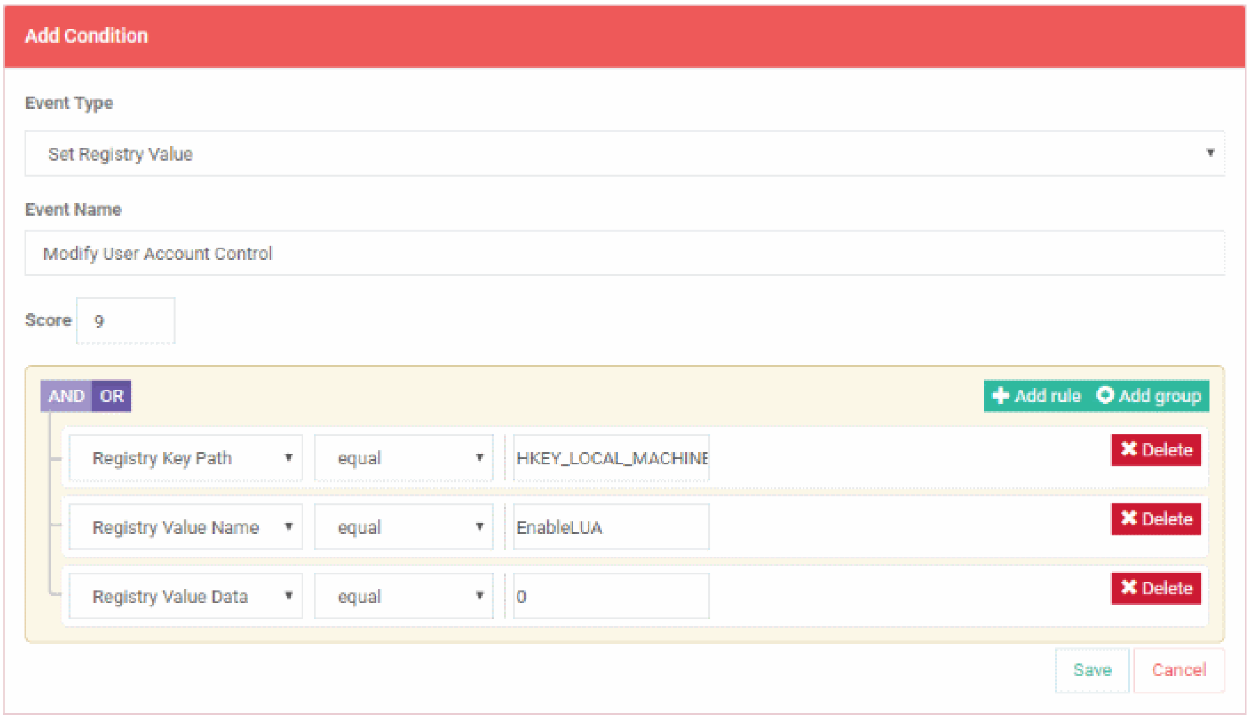
Event Type: Set Registry Value

Event Name: Modify User Account Control

Score: 9

Registry Key Path | equal | HKEY_LOCAL_MACHINE

- Click 'Delete' to remove the rule
- Click 'Save' if the rule satisfies your requirement
- To add multiple rules, click 'Add rule'
- Define parameters and condition as explained above.



Add Condition

Event Type

Set Registry Value

Event Name

Modify User Account Control

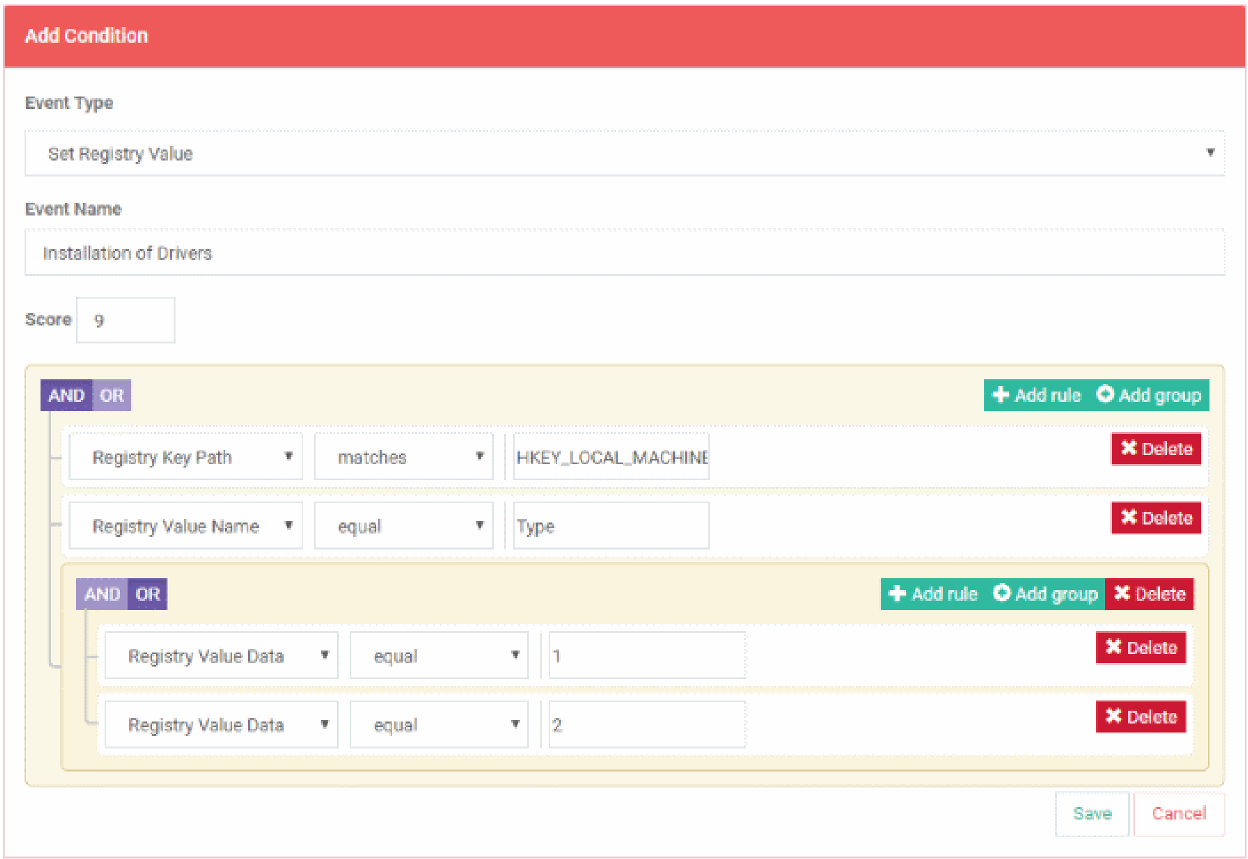
Score 9

Registry Key Path	equal	HKEY_LOCAL_MACHINE
Registry Value Name	equal	EnableLUA
Registry Value Data	equal	0

- Use 'AND' or 'OR' operators for the rule per your requirement

You can add multiple rules and define their relationship with 'AND', 'OR' operators.

- To add a group, click 'Add group'
- Define parameters and conditions as explained above.



Add Condition

Event Type

Set Registry Value

Event Name

Installation of Drivers

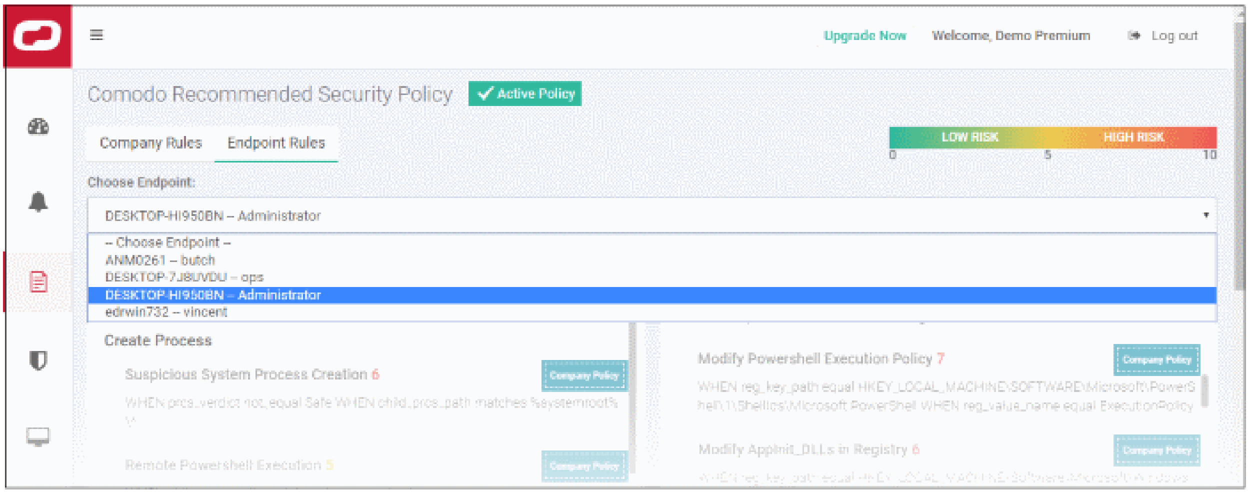
Score 9

Registry Key Path	matches	HKEY_LOCAL_MACHINE
Registry Value Name	equal	Type
Registry Value Data	equal	1
Registry Value Data	equal	2

- Use 'AND' or 'OR' operators for groups (and within a group for rules) per your requirements.
- Click 'Save' when done.
- An alert will be created if the rule condition(s) are met
- To edit a rule, click the pencil icon beside it and update as required. The process is same as explained above.

Endpoint Rules

- Click 'Policy Management' on the left then the 'Endpoint Rules' tab
- Select the endpoint from the drop-down



Choose Endpoint:

DESKTOP-HI950BN – Administrator

-- Choose Endpoint --
ANM0261 – butch
DESKTOP-7J8UVDU – ops
DESKTOP-HI950BN – Administrator
edrwin732 – vincent

Create Process

Suspicious System Process Creation 6

WHEN prcs_verdict not_equal Safe WHEN child_prcs_path matches %systemroot%*

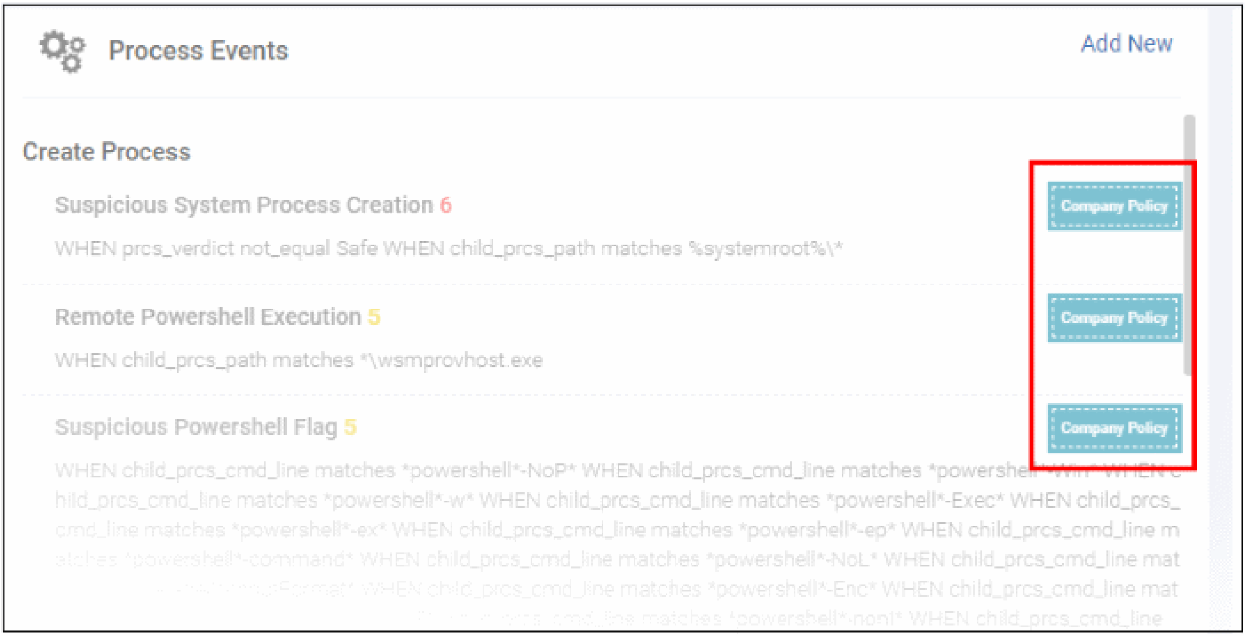
Remote Powershell Execution 5

Modify Powershell Execution Policy 7

WHEN reg_key_path equal HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PowerShell\1\ShellIds\Microsoft.PowerShell WHEN reg_value_name equal ExecutionPolicy

Modify AppInit_DLLs in Registry 6

- All the event rules under 'Company Rules' will be applicable for the endpoint and shown as 'Company Policy', which cannot be edited or removed from here.



Create Process

Suspicious System Process Creation 6

WHEN prcs_verdict not_equal Safe WHEN child_prcs_path matches %systemroot%*

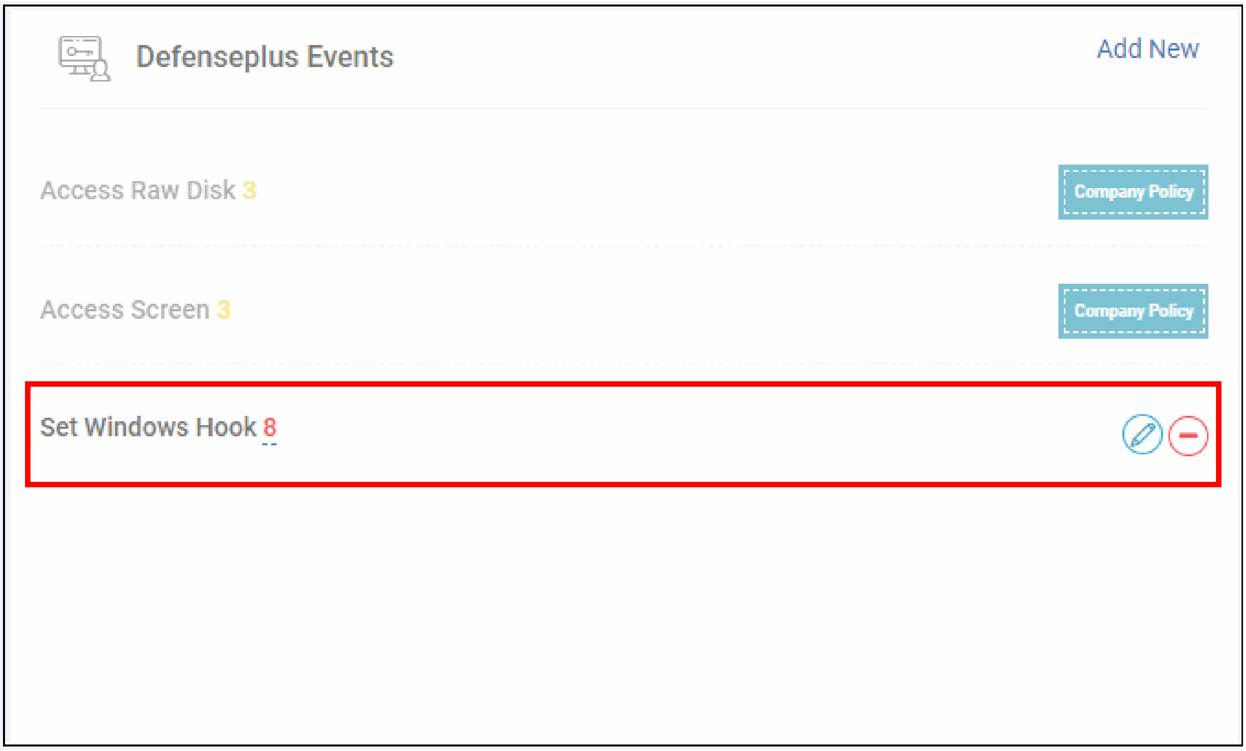
Remote Powershell Execution 5

WHEN child_prcs_path matches *\wsmprovhost.exe

Suspicious Powershell Flag 5

WHEN child_prcs_cmd_line matches *powershell*-NoP* WHEN child_prcs_cmd_line matches *powershell*-Win* WHEN child_prcs_cmd_line matches *powershell*-w* WHEN child_prcs_cmd_line matches *powershell*-Exec* WHEN child_prcs_cmd_line matches *powershell*-ex* WHEN child_prcs_cmd_line matches *powershell*-ep* WHEN child_prcs_cmd_line matches *powershell*-command* WHEN child_prcs_cmd_line matches *powershell*-NoL* WHEN child_prcs_cmd_line mat[illegible] WHEN child_prcs_cmd_line matches *powershell*-Enc* WHEN child_prcs_cmd_line mat[illegible] child_prcs_cmd_line matches *powershell*-nonI* WHEN child_prcs_cmd_line

- Add new rules under event categories that will be applicable for the selected endpoint only
- Click 'Add New' link and follow the same process as explained under 'Company Rules'



Defenseplus Events

Add New

Access Raw Disk 3 | Company Policy

Access Screen 3 | Company Policy

Set Windows Hook 8

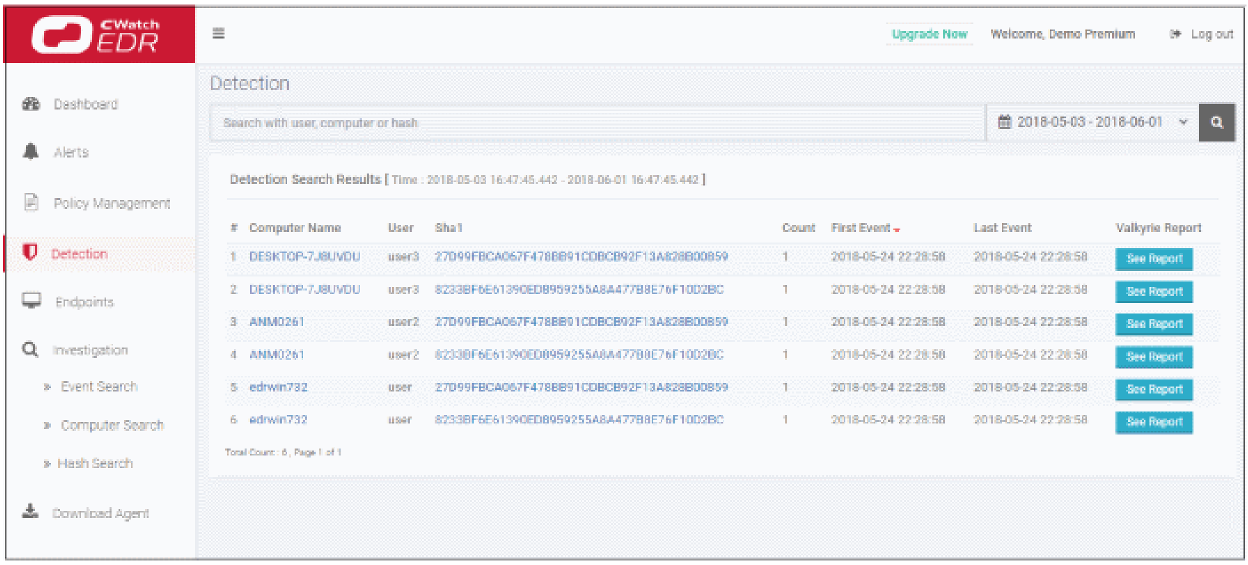
- The added rule can be edited or removed from the event category.
- To edit a rule, click the pencil icon beside it and update as required. The process is same as explained above.

See '**Manage EDR Policies**' for more help with this.

Step 4 - View Events Details on Endpoints

The 'Detection' screen shows detailed information about malicious events on your endpoints.

- Click 'Detection' on the left to open the 'Detection' interface



Detection

Search with user, computer or hash

2018-05-03 - 2018-06-01

Detection Search Results [Time : 2018-05-03 16:47:45.442 - 2018-06-01 16:47:45.442]

#	Computer Name	User	Sha1	Count	First Event	Last Event	Valkyrie Report
1	DESKTOP-7J8UVDU	user3	27D99FBCA067F478BB91CDBCB92F13A828B00859	1	2018-05-24 22:28:58	2018-05-24 22:28:58	See Report
2	DESKTOP-7J8UVDU	user3	8233BF6E61390ED8959255A8A477B8E76F10D2BC	1	2018-05-24 22:28:58	2018-05-24 22:28:58	See Report
3	ANM0261	user2	27D99FBCA067F478BB91CDBCB92F13A828B00859	1	2018-05-24 22:28:58	2018-05-24 22:28:58	See Report
4	ANM0261	user2	8233BF6E61390ED8959255A8A477B8E76F10D2BC	1	2018-05-24 22:28:58	2018-05-24 22:28:58	See Report
5	edrwin732	user	27D99FBCA067F478BB91CDBCB92F13A828B00859	1	2018-05-24 22:28:58	2018-05-24 22:28:58	See Report
6	edrwin732	user	8233BF6E61390ED8959255A8A477B8E76F10D2BC	1	2018-05-24 22:28:58	2018-05-24 22:28:58	See Report

Total Count : 6 , Page 1 of 1

Detection Search Results - Table of Column Descriptions

Column Header	Description

Computer Name	The name of the endpoint. Click the computer name to view its full details. See '**Computer Search**' for details.
User	The user who is logged in to the endpoint.
Sha 1	Hash value of the detected malware. Click the hash value to view its full details. See '**Hash Search**' for details.
Count	Number of times the malicious event was detected on the endpoint.
First Event	Date and time the event was first detected on the endpoint.
Last Event	Date and time the event was most recently detected on the endpoint.
Valkyrie Report	Unknown and suspicious files are analyzed by Comodo's Valkyrie, an advanced file analysis and file verdict system. Click 'See Report' to view the file analysis. See **https://help.comodo.com/topic-397-1-773-9563-Introduction-to-Comodo-Valkyrie.html** for more information about Valkyrie.

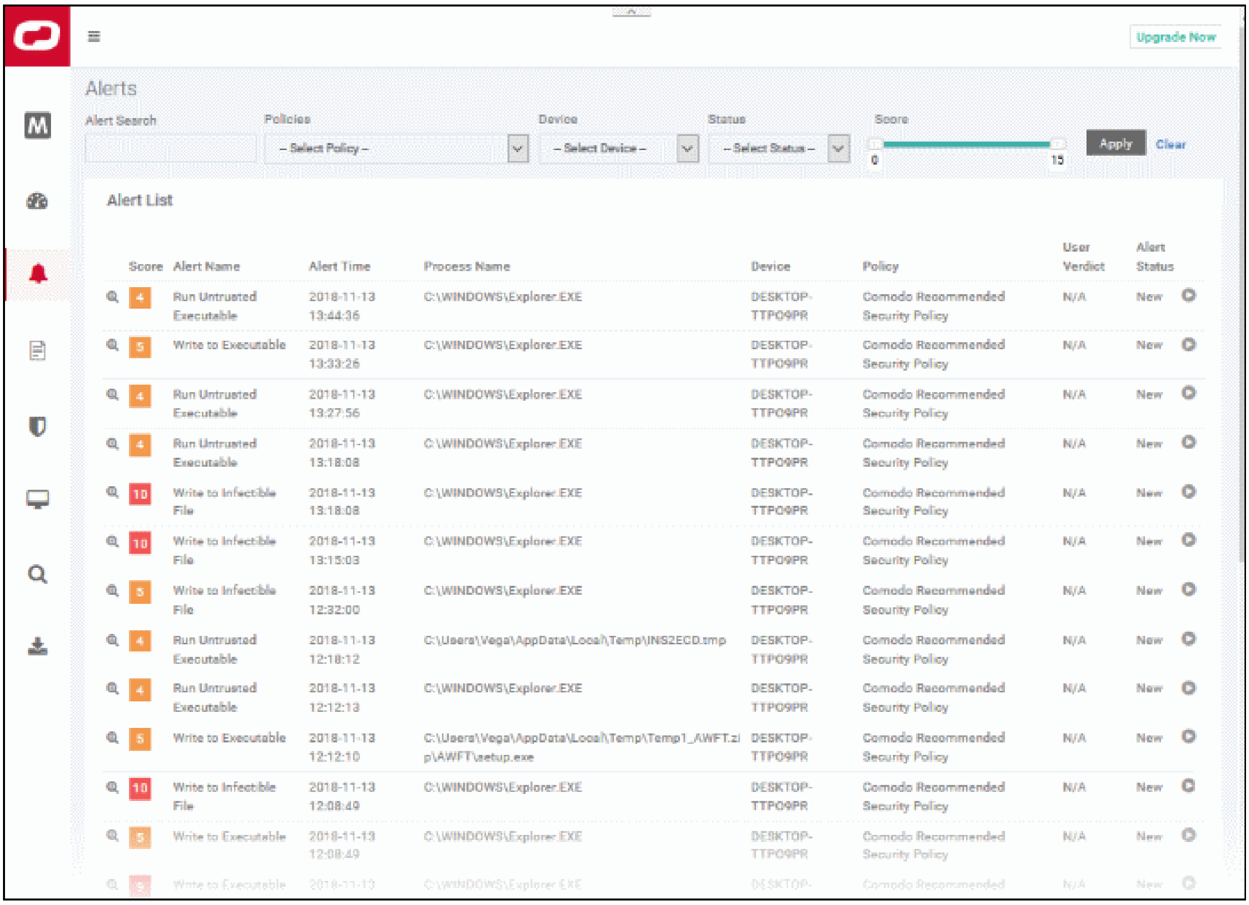
- The 'Search' box above the table lets you filter the list:
  - Type full or partial search terms in the search box and press enter.
  - Matching results will be automatically displayed
  - Clear the search terms and click 'Search' again to reset the list.
- Click any column header to sort items in ascending/descending/alphabetical order.
- Use the time-range drop-down to show event information for a specific date or date range.

See '**Viewing Event Details on Endpoints**' topic if you need more help with this.

Step 5 - View Alerts

Alerts are created when an event on your network matches a rule in your EDR policy. See '**Manage EDR Policies**' if you want to learn about policies and rules.

- Click 'Alerts' on the left to open the interface:



Alerts

Alert Search | Policies: – Select Policy – | Device: – Select Device – | Status: – Select Status – | Score: 0 – 15

Alert List

Score	Alert Name	Alert Time	Process Name	Device	Policy	User Verdict	Alert Status
4	Run Untrusted Executable	2018-11-13 13:44:36	C:\WINDOWS\Explorer.EXE	DESKTOP-TTPO9PR	Comodo Recommended Security Policy	N/A	New
5	Write to Executable	2018-11-13 13:33:26	C:\WINDOWS\Explorer.EXE	DESKTOP-TTPO9PR	Comodo Recommended Security Policy	N/A	New
4	Run Untrusted Executable	2018-11-13 13:27:56	C:\WINDOWS\Explorer.EXE	DESKTOP-TTPO9PR	Comodo Recommended Security Policy	N/A	New
4	Run Untrusted Executable	2018-11-13 13:18:08	C:\WINDOWS\Explorer.EXE	DESKTOP-TTPO9PR	Comodo Recommended Security Policy	N/A	New
10	Write to Infectible File	2018-11-13 13:18:08	C:\WINDOWS\Explorer.EXE	DESKTOP-TTPO9PR	Comodo Recommended Security Policy	N/A	New
10	Write to Infectible File	2018-11-13 13:15:03	C:\WINDOWS\Explorer.EXE	DESKTOP-TTPO9PR	Comodo Recommended Security Policy	N/A	New
5	Write to Infectible File	2018-11-13 12:32:00	C:\WINDOWS\Explorer.EXE	DESKTOP-TTPO9PR	Comodo Recommended Security Policy	N/A	New
4	Run Untrusted Executable	2018-11-13 12:18:12	C:\Users\Vega\AppData\Local\Temp\INS2ECD.tmp	DESKTOP-TTPO9PR	Comodo Recommended Security Policy	N/A	New
4	Run Untrusted Executable	2018-11-13 12:12:13	C:\WINDOWS\Explorer.EXE	DESKTOP-TTPO9PR	Comodo Recommended Security Policy	N/A	New
5	Write to Executable	2018-11-13 12:12:10	C:\Users\Vega\AppData\Local\Temp\Temp1_AWFT.zip\AWFT\setup.exe	DESKTOP-TTPO9PR	Comodo Recommended Security Policy	N/A	New
10	Write to Infectible File	2018-11-13 12:08:49	C:\WINDOWS\Explorer.EXE	DESKTOP-TTPO9PR	Comodo Recommended Security Policy	N/A	New
5	Write to Executable	2018-11-13 12:08:49	C:\WINDOWS\Explorer.EXE	DESKTOP-TTPO9PR	Comodo Recommended Security Policy	N/A	New
[illegible]	Write to Executable	2018-11-13	C:\WINDOWS\Explorer.EXE	DESKTOP-	Comodo Recommended	N/A	New

Alerts - Table of Column Descriptions	
Column Header	**Description**
Score	The rating you specified for the event when creating the rule. You can apply a score between 0 and 10 based on the severity you place on the event. See '**Manage EDR Policies**' for more information.
Alert Name	The label you gave to the condition when creating the rule. Alerts are generated when rule conditions are triggered. See '**Manage EDR Policies**' for more information.
Alert Time	The date and time the warning was created.
Process Name	Path of the application that caused the event.
Device	The name of the endpoint from which the event was logged.
Policy	The name of the security policy that created the alert.
User Verdict	The status assigned to the alert by the admin who dealt with the issue. Options include: • False Positive - Admin does not consider the incident a security threat • True Positive - Admin confirms the incident occurred. The 'Score' attached to the incident should determine the response required. • Add comments. Note - The comments will not appear in the list of user verdicts
Alert Status	Progress of the alert. Statuses include:

	• New - Work has not yet started on the alert • In progress - An admin is attending to the alert • Resolved - An admin has submitted a verdict for the alert

Filter options

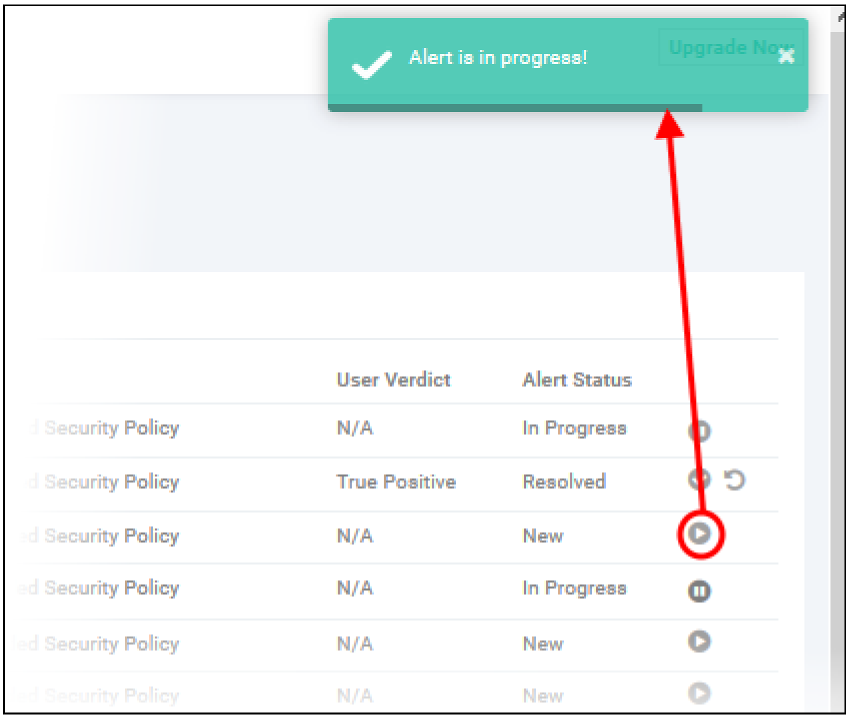
You can search for particular alerts using the following filters:

- Alert Name - Search by alert label.
- Alert Time - Search by when the alert was generated.
- Process Name - Search by process name
- Devices - Select the device on which the event occurred
- Policy - Filter by policy that triggered the alert
- User Verdict - Filter by status awarded to the alert by an admin.
- Alert Status - Filter by any of the 3 progress levels - 'New', 'In progress' or 'Resolved'.

- Enter / select the filter and click 'Apply'
- Click 'Clear' to remove the search filters

You can configure multiple filters to search for a particular alert. For example, you can search for an event by its alert name, policy and the endpoint.

- Click the play icon beside the 'New' alert status to submit the verdict.

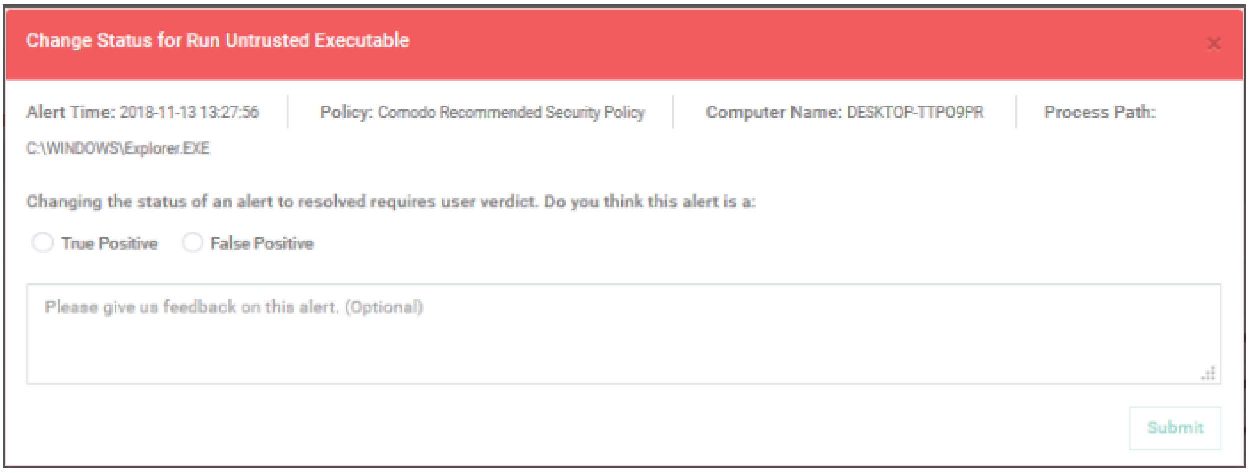


Alert is in progress!

	User Verdict	Alert Status
Security Policy	N/A	In Progress
Security Policy	True Positive	Resolved
Security Policy	N/A	New
Security Policy	N/A	In Progress
Security Policy	N/A	New
Security Policy	N/A	New

The alert status will change to 'In progress'

- Click the progress icon to submit the verdict



Change Status for Run Untrusted Executable

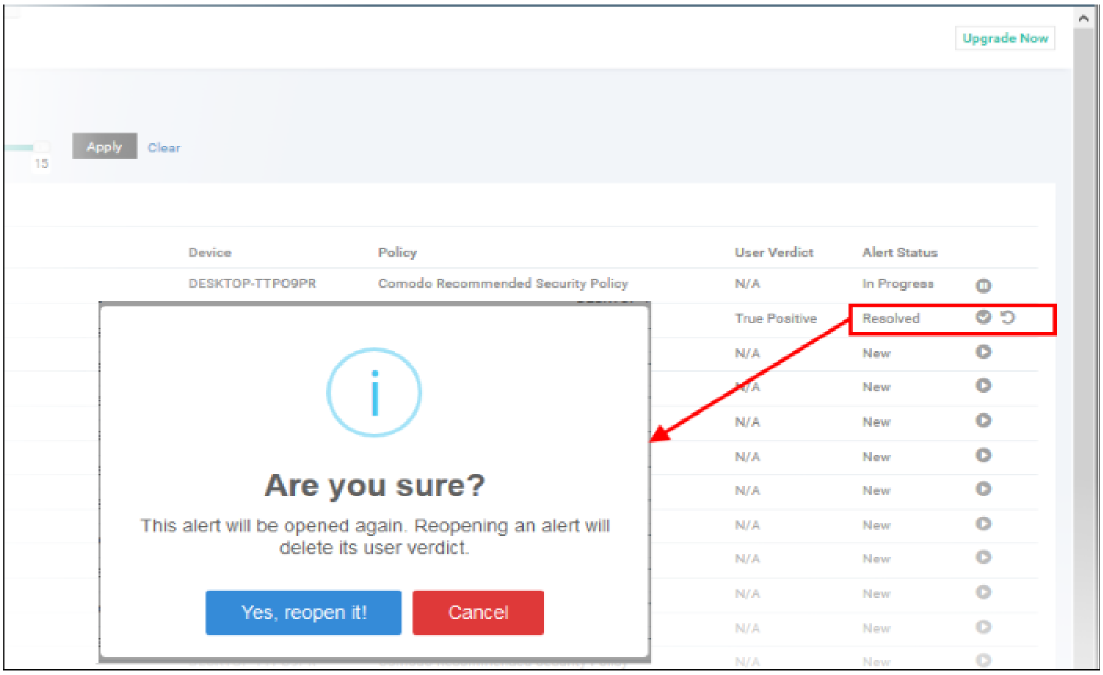
Alert Time: 2018-11-13 13:27:56 | Policy: Comodo Recommended Security Policy | Computer Name: DESKTOP-TTPO9PR | Process Path: C:\WINDOWS\Explorer.EXE

Changing the status of an alert to resolved requires user verdict. Do you think this alert is a:

○ True Positive ○ False Positive

Please give us feedback on this alert. (Optional)

- Click 'Submit' to resolve the alert
- Click the reopen icon if you want to change the verdict.



Device	Policy	User Verdict	Alert Status
DESKTOP-TTPO9PR	Comodo Recommended Security Policy	N/A	In Progress
		True Positive	Resolved
		N/A	New
		N/A	New
		N/A	New
		N/A	New
		N/A	New
		N/A	New
		N/A	New
		N/A	New
		N/A	New
		N/A	New

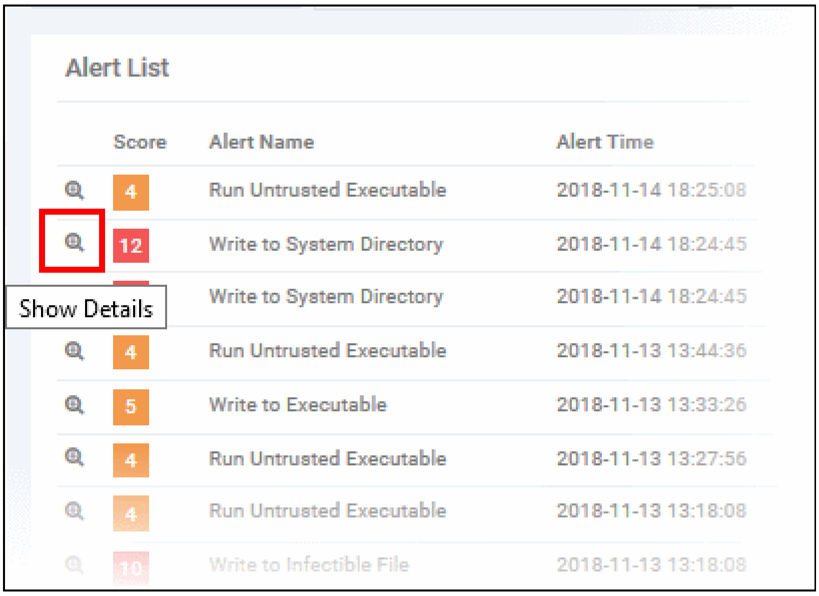
Are you sure?

This alert will be opened again. Reopening an alert will delete its user verdict.

- Click 'Yes, reopen it!' to change the verdict
- Click 'Cancel' to keep the verdict unchanged

View Event Details

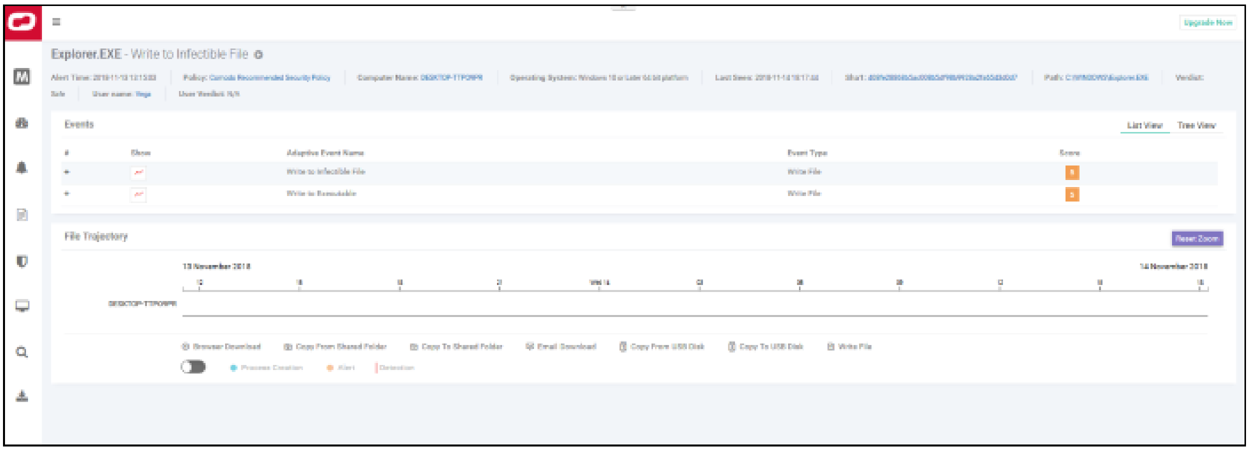
- Click 'Show Details' in the 'Score' column:



Alert List

	Score	Alert Name	Alert Time
	4	Run Untrusted Executable	2018-11-14 18:25:08
	12	Write to System Directory	2018-11-14 18:24:45
Show Details		Write to System Directory	2018-11-14 18:24:45
	4	Run Untrusted Executable	2018-11-13 13:44:36
	5	Write to Executable	2018-11-13 13:33:26
	4	Run Untrusted Executable	2018-11-13 13:27:56
	4	Run Untrusted Executable	2018-11-13 13:18:08
	10	Write to Infectible File	2018-11-13 13:18:08

This open the information screen for that event:



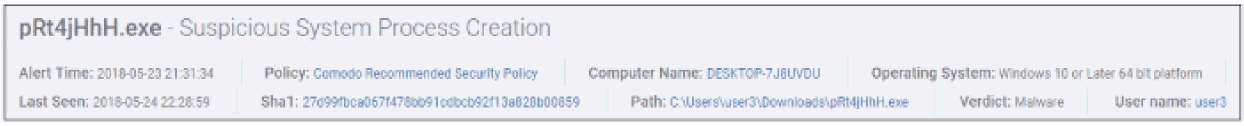
Explorer.EXE - Write to Infectible File

Events

#	Show	Adaptive Event Name	Event Type	Score
+		Write to Infectible File	Write File	[illegible]
+		Write to Executable	Write File	[illegible]

File Trajectory

The top part of the screen shows details such as the alert name and the application that generated the event:



pRt4jHhH.exe - Suspicious System Process Creation

Alert Time: 2018-05-23 21:31:34 | Policy: Comodo Recommended Security Policy | Computer Name: DESKTOP-7J8UVDU | Operating System: Windows 10 or Later 64 bit platform

Last Seen: 2018-05-24 22:28:59 | Sha1: 27d99fbca067f478bb91cdbcb92f13a828b00859 | Path: C:\Users\user3\Downloads\pRt4jHhH.exe | Verdict: Malware | User name: user3

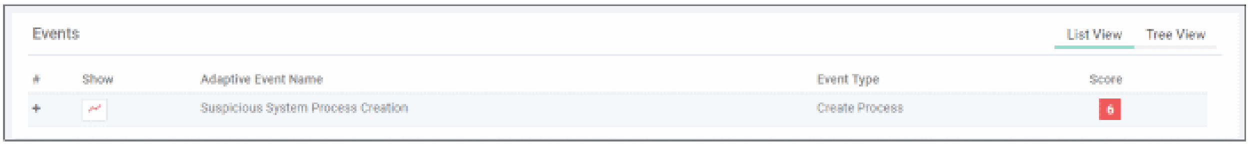
- Alert and application name is shown at the top
- Alert Time - Date and time of the alert
- Policy - Name of the security policy. Click the name of the policy to open the policy management screen. See '**Manage EDR Policies**' for more information.
- Computer Name - Name of the endpoint from which the event was logged. Clicking the endpoint will open the 'Computer Search' screen with the endpoint preselected. See '**Computer Search**' for more details.
- Operating System - Details of the endpoint's OS from which the event was logged.
- Last Seen - The last date and time the endpoint communicated with EDR.
- Sha 1 - The hash value of the file. Clicking the hash value will open the 'Hash Search' screen with the file preselected. See '**Hash Search**' for more information.
- Path - The full process path of the event that was logged. Clicking the process path will open the 'Event

Search' screen with the event query auto-filled in the search field. See '**Event Search**' for more details.

- Verdict - Valkyrie results after the analysis.
- User name - The logged in user name of the endpoint. Clicking the name will open the 'Event Search' screen with the event query auto-filled in the search field. See '**Event Search**' for more details.
- User Verdict - The admin's conclusion on the nature of alert. The options given to declare the results are 'True Positive' and False Positive'.

Events

Details of the event are shown in the main pane:

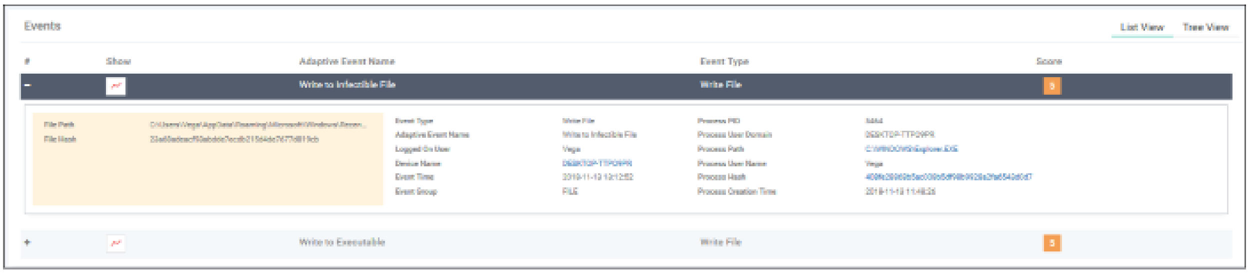


Events

List View | Tree View

#	Show	Adaptive Event Name	Event Type	Score
+	📈	Suspicious System Process Creation	Create Process	6

- **List View**
  - Show - Click 📈 icon to view the event timeline. See '**Process Timeline**' for more details.
  - Adaptive Event Name - Label given to the event when creating the security rule.
  - Event Type - The category of event
  - Score - The event severity. This was specified when the rule was created.
  - Click anywhere in the row to view all event fields for that event type. The number of event fields shown depends on the event type.:



Events

List View | Tree View

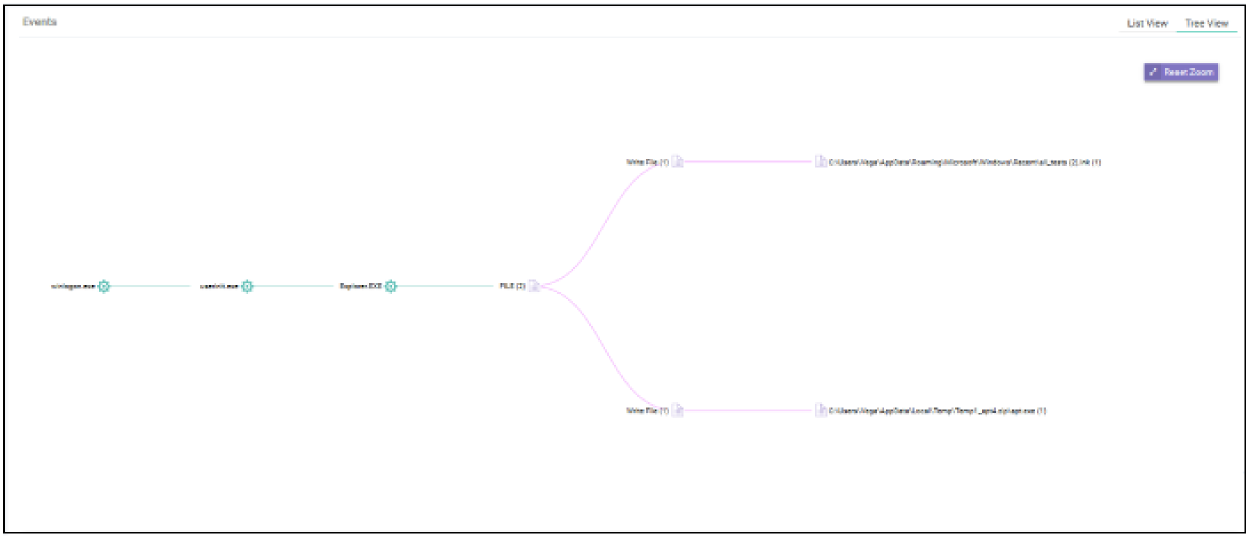
#	Show	Adaptive Event Name	Event Type	Score
−	📈	Write to Infectible File	Write File	5

File Path: C:\Users\Vega\AppData\Roaming\Microsoft\Windows\Recen...
File Hash: 22a69adeacf93abdda7ecdb21564da7677d819cb

Event Type	Write File	Process PID	5444
Adaptive Event Name	Write to Infectible File	Process User Domain	DESKTOP-TTPO9PR
Logged On User	Vega	Process Path	C:\WINDOWS\Explorer.EXE
Device Name	DESKTOP-TTPO9PR	Process User Name	Vega
Event Time	2019-11-13 12:12:52	Process Hash	4098e28969b5ac039b5df98b9928a2fa6542d0d7
Event Group	FILE	Process Creation Time	2019-11-13 11:48:26

#	Show	Adaptive Event Name	Event Type	Score
+	📈	Write to Executable	Write File	5

- **Tree View**
  - Click 'Tree View' link at top-right of 'Events' section


Events
List View
Tree View
Reset Zoom
winlogon.exe
userinit.exe
Explorer.EXE
FILE (2)
Write File (1)
C:\Users\Vega\AppData\Roaming\Microsoft\Windows\Recent\all_tests (2).lnk (1)
Write File (1)
C:\Users\Vega\AppData\Local\Temp\Temp1_apid.zip\apt.exe (1)

The screen shows the full process path of the event. Clicking any process label will open the 'Event Search' screen with the event query auto-filled in the search field. See '**Event Search**' for more details.

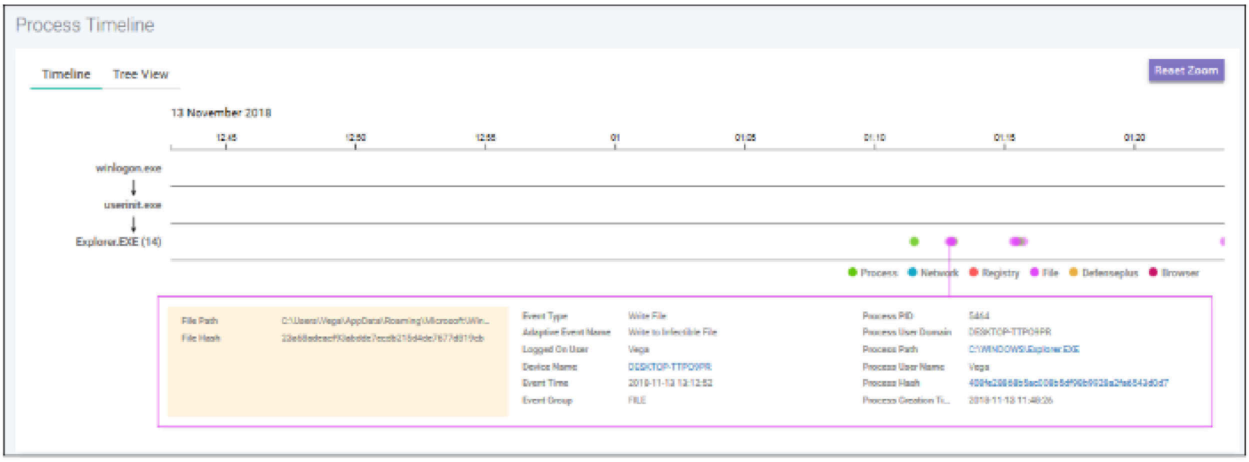
- Zoom in or out using your mouse. Right-click and move the chart left or right. Click 'Reset Zoom' to return to default view.

Process Timeline of the Event

Shows the various activities happening in an event for each file type

Timeline View

- Click the 'Show in Process Timeline' icon of the event



File Path C:\Users\Vega\AppData\Roaming\Microsoft\Win...
File Hash 22e68adcacf93abdde7ccdb215d4de7677d819cb

Event Type Write File
Adaptive Event Name Write to Infectible File
Logged On User Vega
Device Name DESKTOP-TTPO9PR
Event Time 2018-11-13 13:12:52
Event Group FILE

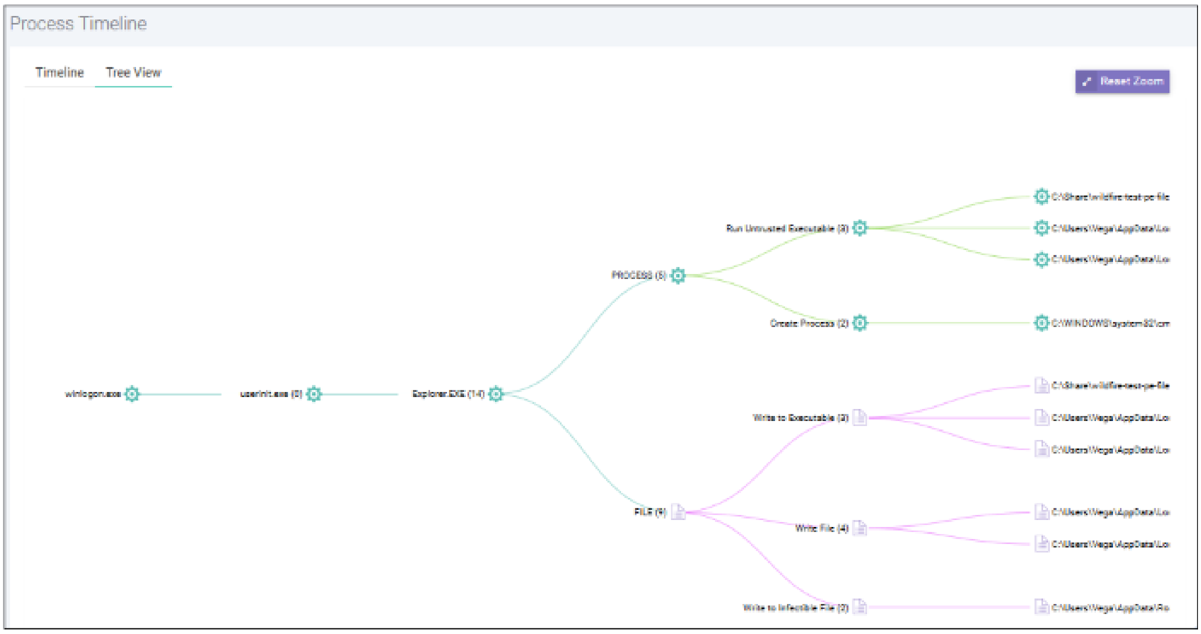
Process PID 5464
Process User Domain DESKTOP-TTPO9PR
Process Path C:\WINDOWS\Explorer.EXE
Process User Name Vega
Process Hash 409fe28868b5ac008b5df90b9928a2fa6543d0d7
Process Creation Ti... 2018-11-13 11:48:26

The 'Process Timeline' screen will open

The screen shows the time at which each event occurred. See '**Process Timeline**' for more details.

Tree View

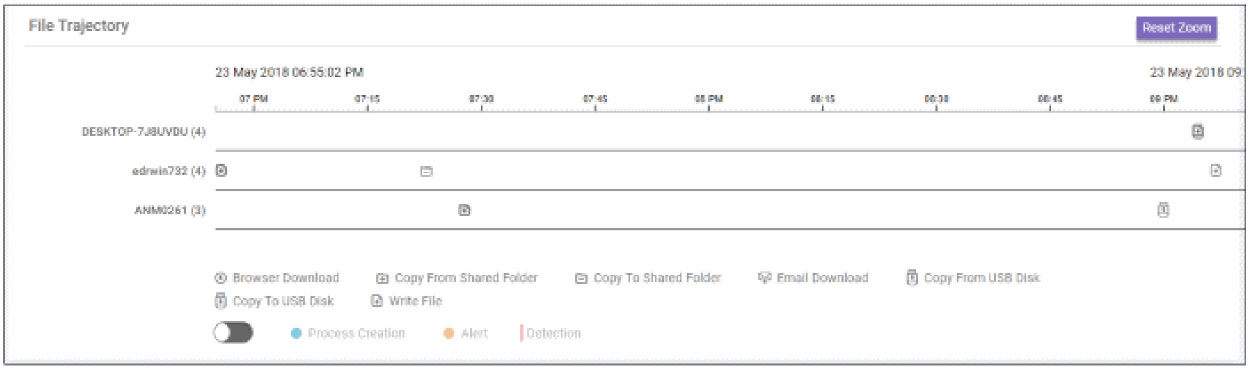
- Click the 'Show in Process Timeline' icon of the event
- Click 'Tree View'



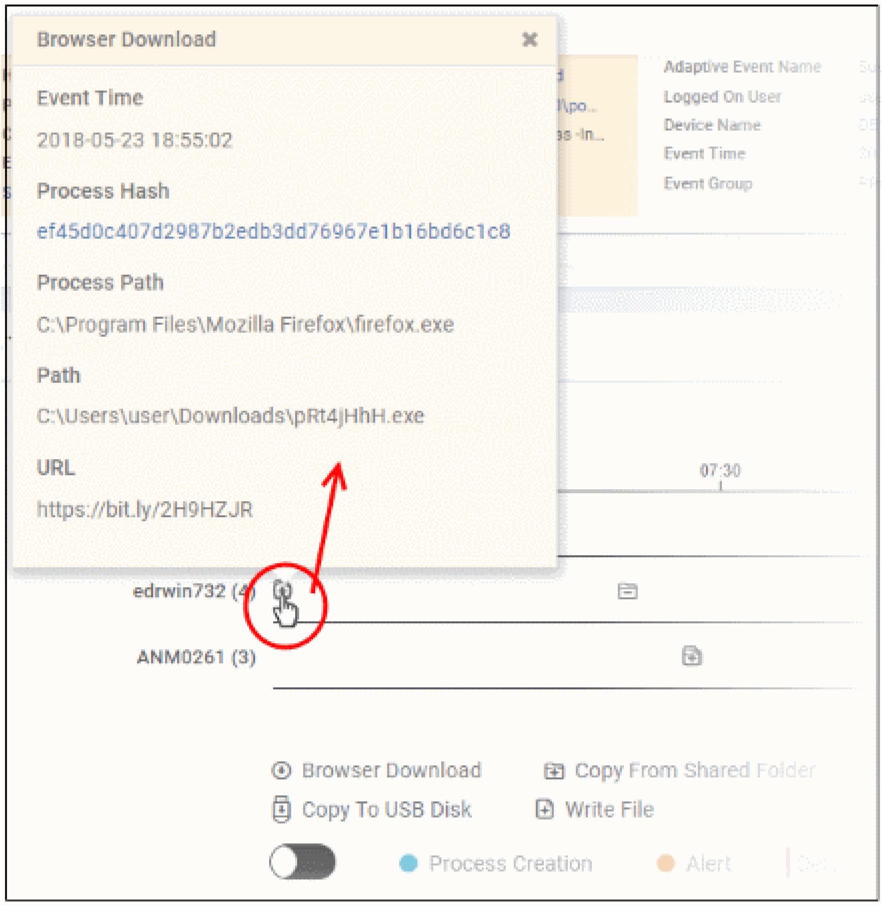
The screen shows the tree view of the event occurrences. See '**Process Timeline**' for more details.

File Trajectory

The bottom section of the screen displays the movement of the file, that is from where it was downloaded, copied to which endpoint and so on.



- Zoom in or out using your mouse. Right-click and move the chart left or right. Click 'Reset Zoom' to return to default view.
- Details of the icons is shown below the graph.
- Click an icon to view the trajectory details.



Browser Download ✖

Event Time
2018-05-23 18:55:02

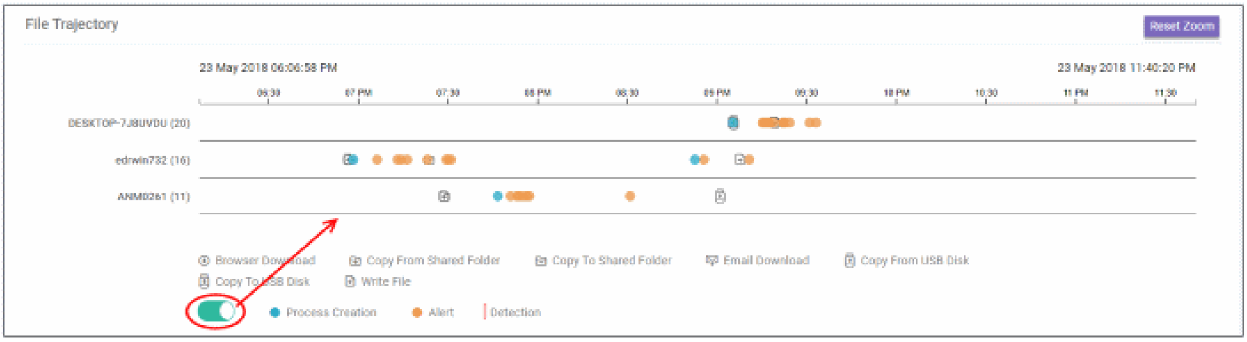
Process Hash
ef45d0c407d2987b2edb3dd76967e1b16bd6c1c8

Process Path
C:\Program Files\Mozilla Firefox\firefox.exe

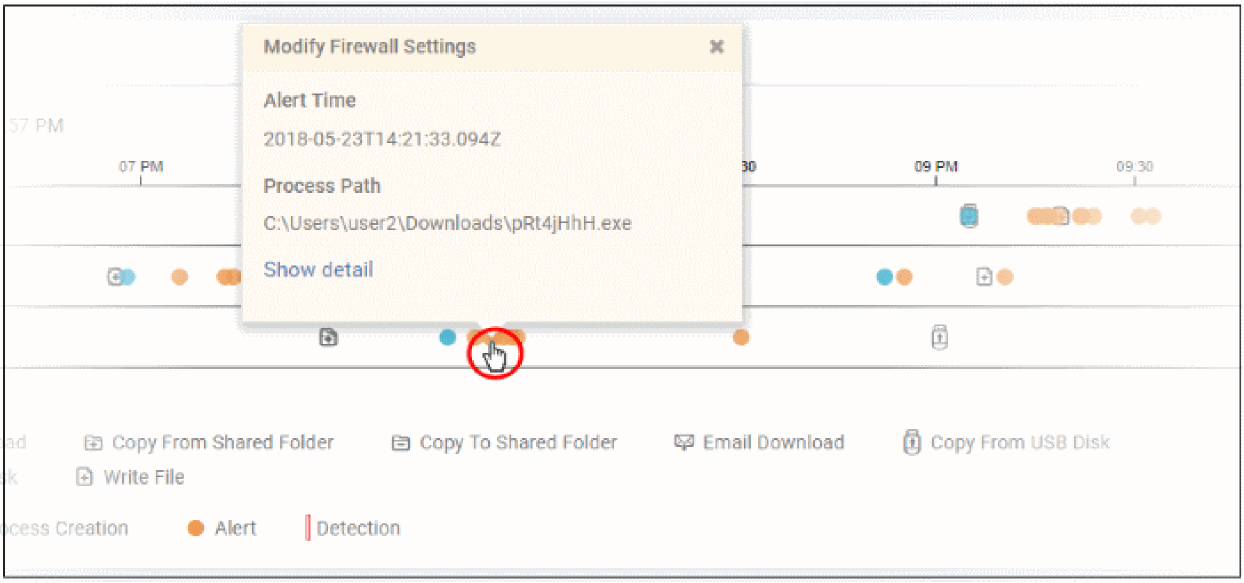
Path
C:\Users\user\Downloads\pRt4jHhH.exe

URL
https://bit.ly/2H9HZJR

- Click 'X' to close the dialog.
- Click 'Process Creation' button to view time of process creation, event detected and alert generated.



- Click an icon color code to view trajectory details.



Modify Firewall Settings ✖

Alert Time

2018-05-23T14:21:33.094Z

Process Path

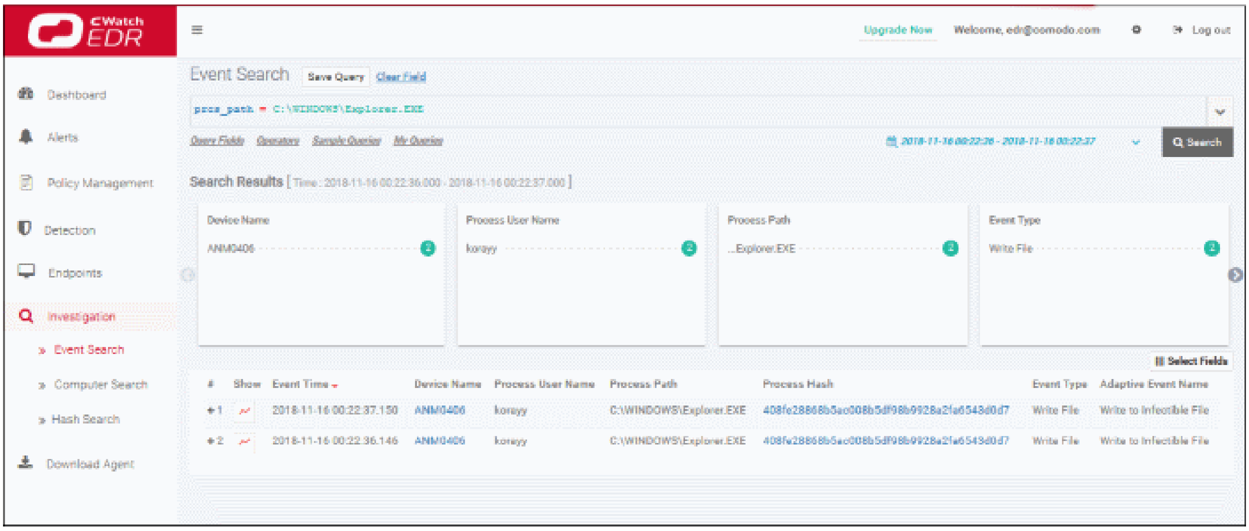
C:\Users\user2\Downloads\pRt4jHhH.exe

Show detail

- 'Show detail' link will be available for Alert dialog. Clicking the link will open the event details screen for which the alert was generated.
- Click 'X' to close the dialog.

Step 6 - Analyze Events

- The 'Event Search' interface lets you find specific events using built-in queries.
- cWatch ships with some useful sample queries, and you can construct your own queries.
- You have to create conditions for a search and configure the results table accordingly.
- You can also use the search results to construct another query.
- Click 'Investigation' on the left then 'Event Search' to open the interface:



proc_path = C:\WINDOWS\Explorer.EXE

2018-11-16 00:22:36 - 2018-11-16 00:22:37

Search Results [Time : 2018-11-16 00:22:36.000 - 2018-11-16 00:22:37.000]

Device Name: ANM0406 2

Process User Name: korayy 2

Process Path: ...Explorer.EXE 2

Event Type: Write File 2

#	Show	Event Time	Device Name	Process User Name	Process Path	Process Hash	Event Type	Adaptive Event Name
+ 1		2018-11-16 00:22:37.150	ANM0406	korayy	C:\WINDOWS\Explorer.EXE	408fe28868b5ac008b5df98b9928a2fa6543d0d7	Write File	Write to Infectible File
+ 2		2018-11-16 00:22:36.146	ANM0406	korayy	C:\WINDOWS\Explorer.EXE	408fe28868b5ac008b5df98b9928a2fa6543d0d7	Write File	Write to Infectible File

- By default, no custom queries are defined, allowing you search for all events that occurred during the last 3 days.
- Use the 'Query Fields' and 'Operator' links on the upper-left to build a custom event query.
- The first query field you add will automatically have the '=' operator appended to it (you can change this if required). You will need to enter the criteria after the operator.
- Any subsequent fields you add will automatically be prefixed with the 'AND' operator.
- All queries that you save will be listed under 'My Queries'
- 'Sample Queries' are pre-defined, example queries. These can be used as standalones, or adapted to produce a more complex search.
- 'Select Fields' on the right lets you configure the columns of the results table.
- You can change the date range using the link 2nd from the right.

The interface allows you to:

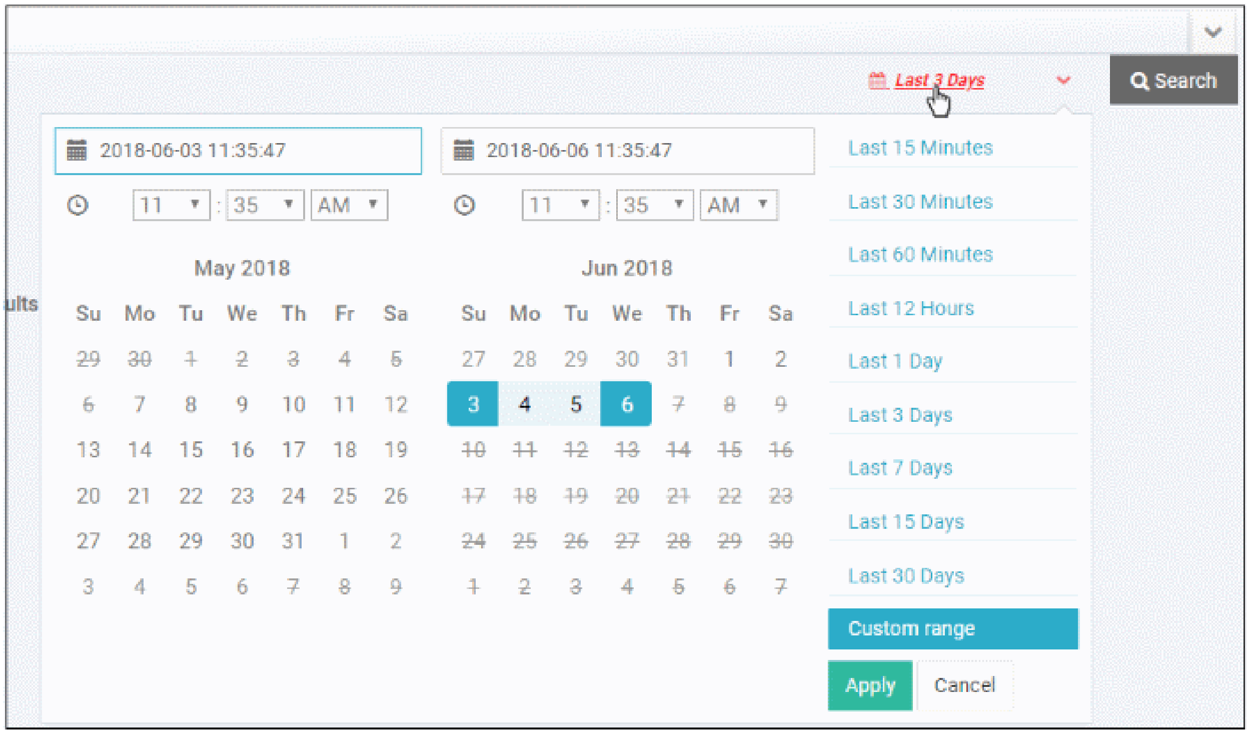
- **Run a general event search**
- **Configure and run a custom query search**
- **Use sample queries**
- **View query results**
- **Configure results table column headers for a query**

Run General Event Search

A general search returns all events recorded from all enrolled endpoints.

To run a general event search:

- Make sure the 'Search Box' field is blank.
- Use the time-range drop-down to pick a specific date or date range.



2018-06-03 11:35:47 — 11 : 35 AM

2018-06-06 11:35:47 — 11 : 35 AM

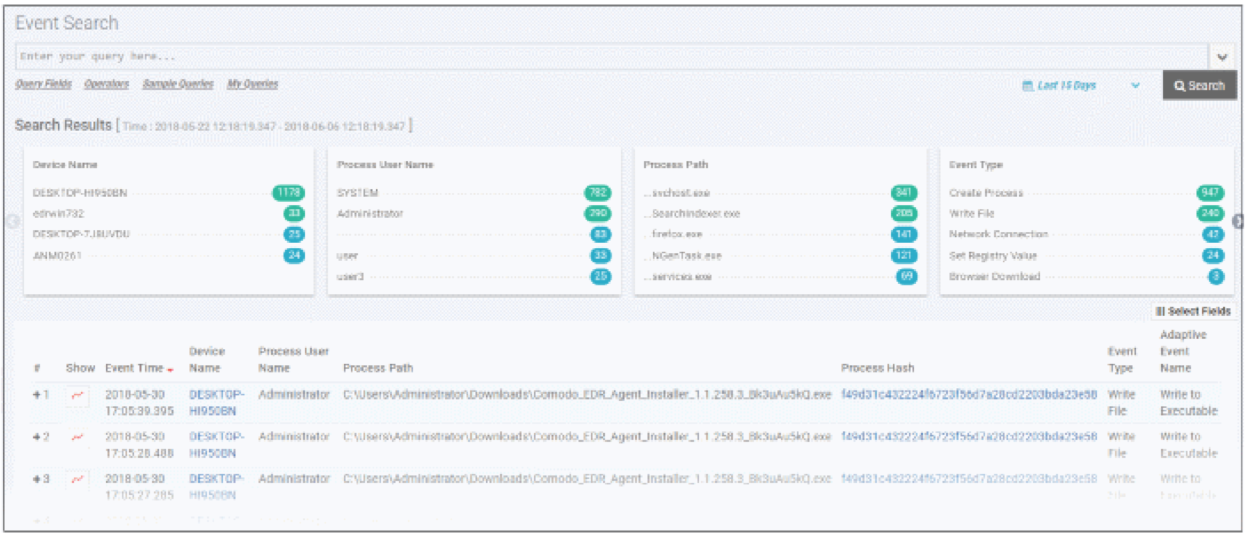
May 2018

Su	Mo	Tu	We	Th	Fr	Sa
~~29~~	~~30~~	~~1~~	~~2~~	~~3~~	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31	1	2
3	4	5	6	~~7~~	8	9

Jun 2018

Su	Mo	Tu	We	Th	Fr	Sa
27	28	29	30	31	1	2
3	4	5	6	~~7~~	~~8~~	~~9~~
~~10~~	~~11~~	~~12~~	~~13~~	~~14~~	~~15~~	~~16~~
~~17~~	~~18~~	~~19~~	~~20~~	~~21~~	~~22~~	~~23~~
~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	~~29~~	~~30~~
~~1~~	~~2~~	~~3~~	~~4~~	~~5~~	~~6~~	~~7~~

- Click 'Custom range' to choose specific dates:
- Click 'Apply', then 'Search'



Search Results [Time : 2018-05-22 12:18:19.347 - 2018-06-06 12:18:19.347]

Device Name	
DESKTOP-HI950BN	1178
edrwin732	33
DESKTOP-7J8UVDU	25
ANM0261	24

Process User Name	
SYSTEM	782
Administrator	290
	83
user	33
user3	25

Process Path	
...svchost.exe	341
...SearchIndexer.exe	205
...firefox.exe	141
...NGenTask.exe	121
...services.exe	69

Event Type	
Create Process	947
Write File	240
Network Connection	42
Set Registry Value	24
Browser Download	3

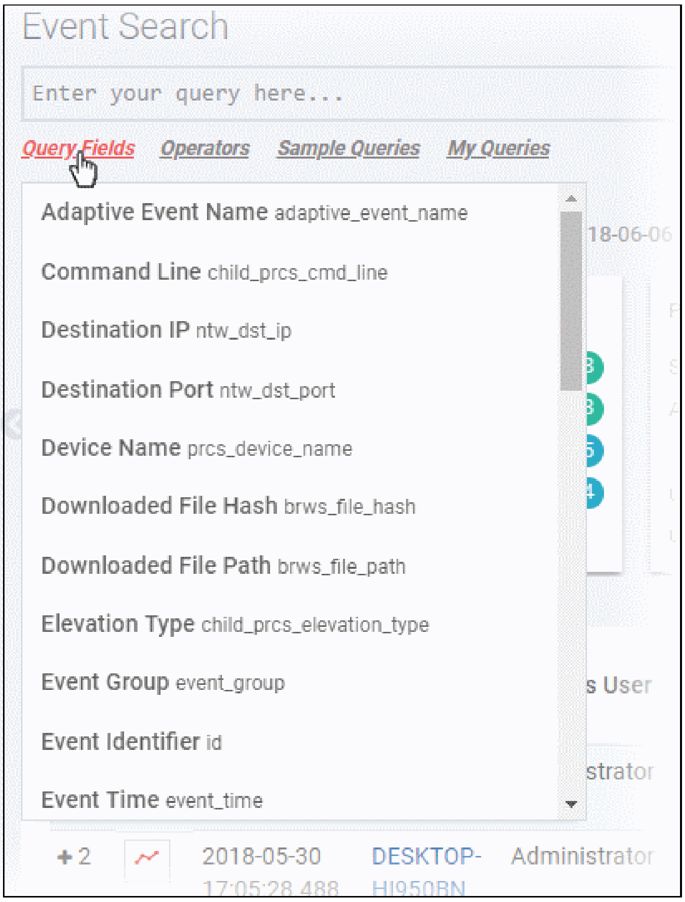
#	Show	Event Time	Device Name	Process User Name	Process Path	Process Hash	Event Type	Adaptive Event Name
+ 1		2018-05-30 17:05:39.395	DESKTOP-HI950BN	Administrator	C:\Users\Administrator\Downloads\Comodo_EDR_Agent_Installer_1.1.258.3_Bk3uAu5kQ.exe	f49d31c432224f6723f56d7a28cd2203bda23e58	Write File	Write to Executable
+ 2		2018-05-30 17:05:28.488	DESKTOP-HI950BN	Administrator	C:\Users\Administrator\Downloads\Comodo_EDR_Agent_Installer_1.1.258.3_Bk3uAu5kQ.exe	f49d31c432224f6723f56d7a28cd2203bda23e58	Write File	Write to Executable
+ 3		2018-05-30 17:05:27.285	DESKTOP-HI950BN	Administrator	C:\Users\Administrator\Downloads\Comodo_EDR_Agent_Installer_1.1.258.3_Bk3uAu5kQ.exe	f49d31c432224f6723f56d7a28cd2203bda23e58	Write File	Write to Executable

The results for the selected period will be displayed. See '**View Query Results**' for more information.

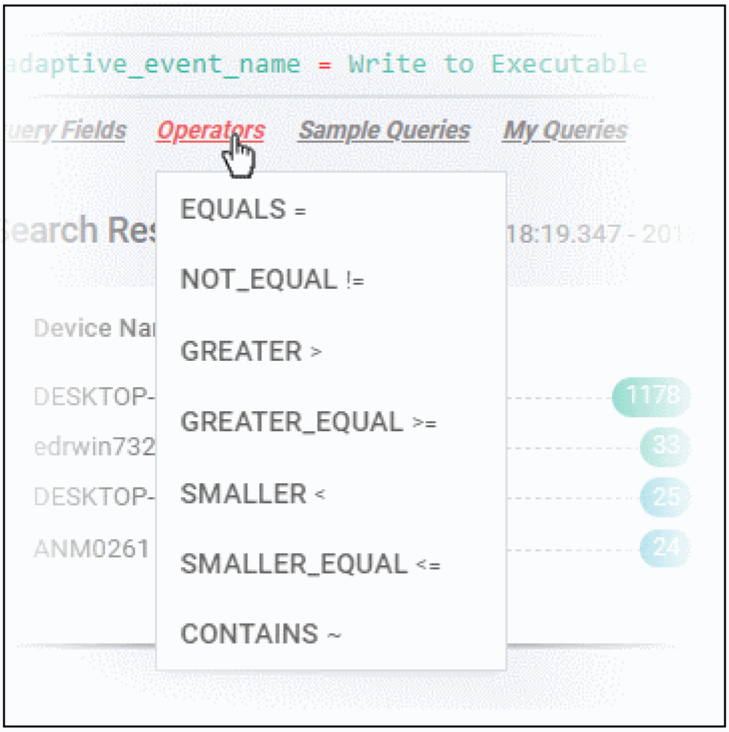
Configure and Run a Custom Query Search

You can search for particular events by building custom queries.

- Click 'Query Fields' then select an event type to begin constructing a custom event query:

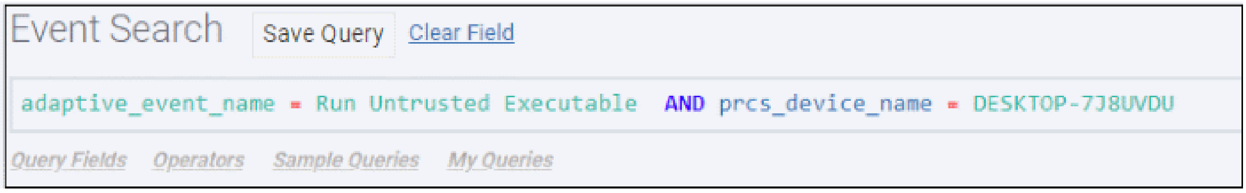

Event Search
Enter your query here...
Query Fields
Operators
Sample Queries
My Queries
Adaptive Event Name adaptive_event_name
Command Line child_prcs_cmd_line
Destination IP ntw_dst_ip
Destination Port ntw_dst_port
Device Name prcs_device_name
Downloaded File Hash brws_file_hash
Downloaded File Path brws_file_path
Elevation Type child_prcs_elevation_type
Event Group event_group
Event Identifier id
Event Time event_time
+2
2018-05-30 17:05:28.488
DESKTOP-HI950BN
Administrator

- Alternatively, click in the search box and use short cut keys 'Ctrl + space'. Select an event field from the list.
- Repeat the process to add more event fields for the query. The 'AND' operator will be automatically added to any subsequent fields you add.
- Click 'Operators' link and select the operator from the drop-down. You can also enter the operator manually.



- Enter the relevant details of the event fields.

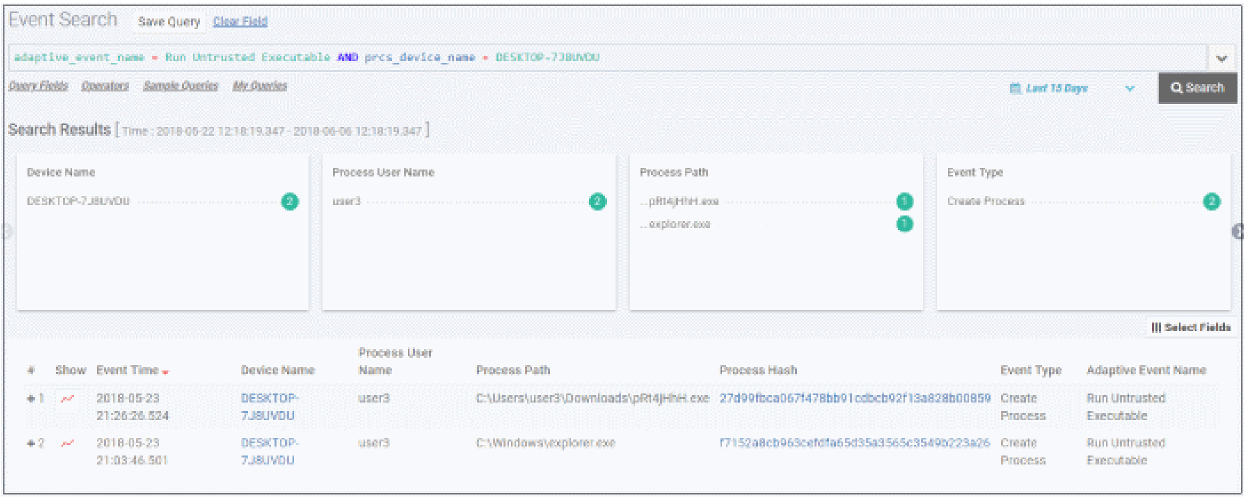
The following example shows a search for 'Adaptive Event Name' = 'Run Untrusted Executable' AND 'Device Name' = 'DESKTOP-7J8UVDU':



```
adaptive_event_name = Run Untrusted Executable  AND prcs_device_name = DESKTOP-7J8UVDU
```

- Next, select the time period for the custom query and click 'Search'

The search results for the custom query will be displayed:



```
adaptive_event_name = Run Untrusted Executable AND prcs_device_name = DESKTOP-7J8UVDU
```

Search Results [Time : 2018-05-22 12:18:19.347 - 2018-06-06 12:18:19.347]

Device Name	Process User Name	Process Path	Event Type
DESKTOP-7J8UVDU 2	user3 2	...pRt4jHhH.exe 1 ...explorer.exe 1	Create Process 2

#	Show	Event Time	Device Name	Process User Name	Process Path	Process Hash	Event Type	Adaptive Event Name
1		2018-05-23 21:26:26.524	DESKTOP-7J8UVDU	user3	C:\Users\user3\Downloads\pRt4jHhH.exe	27d99fbca067f478bb91cdbcb92f13a828b00859	Create Process	Run Untrusted Executable
2		2018-05-23 21:03:46.501	DESKTOP-7J8UVDU	user3	C:\Windows\explorer.exe	f7152a8cb963cefdfa65d35a3565c3549b223a26	Create Process	Run Untrusted Executable

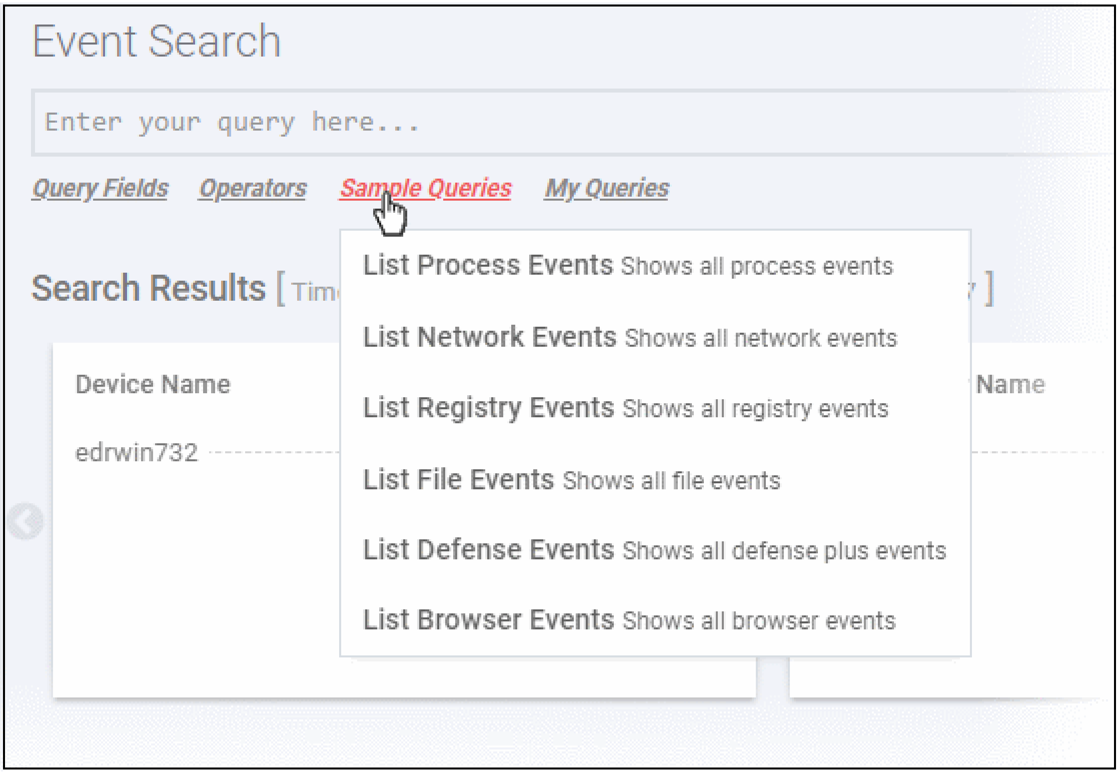
Please note the results for the query will also display details for other fields also. See '**View Query Results**' for more information.

You can also build custom queries using the search results. See the topic '**Event Search**' for more information.

Use Sample Queries

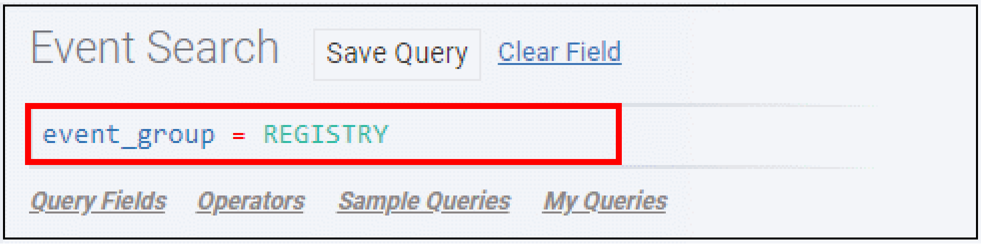
EDR ships with built-in sample queries that are often used. This also serves as examples for you to create more complex queries.

- Click 'Sample Queries' link below the search box



Event Search
Enter your query here...
Query Fields
Operators
Sample Queries
My Queries
Search Results [Tim
Device Name
edrwin732
Name
List Process Events Shows all process events
List Network Events Shows all network events
List Registry Events Shows all registry events
List File Events Shows all file events
List Defense Events Shows all defense plus events
List Browser Events Shows all browser events

The sample query will be automatically updated in the 'Search Box'.



```
event_group = REGISTRY
```

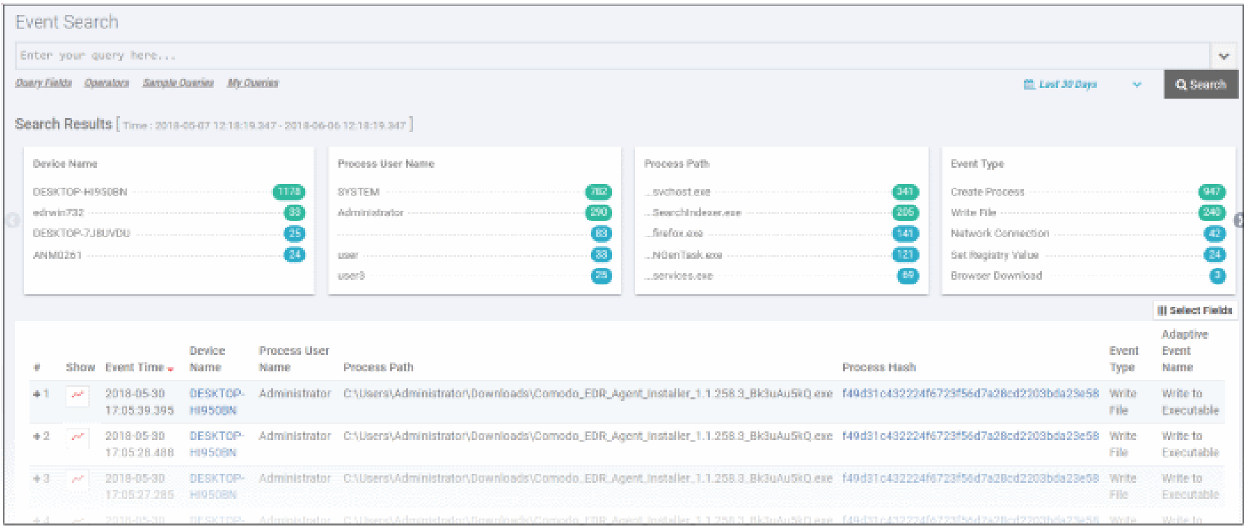
- Select the time-period and click 'Search'

Events matching the sample query will be displayed. See '**View Query Results**' for more information.

View Query Results

EDR stores the generated events on the cloud and these can be fetched anytime from anywhere using an internet browser. You can use these events for data analysis and take remedial actions on endpoints. The query results will be displayed depending on the type of query search.

A summary of the search results is shown on separate tiles at the top. Results for each event are displayed below.

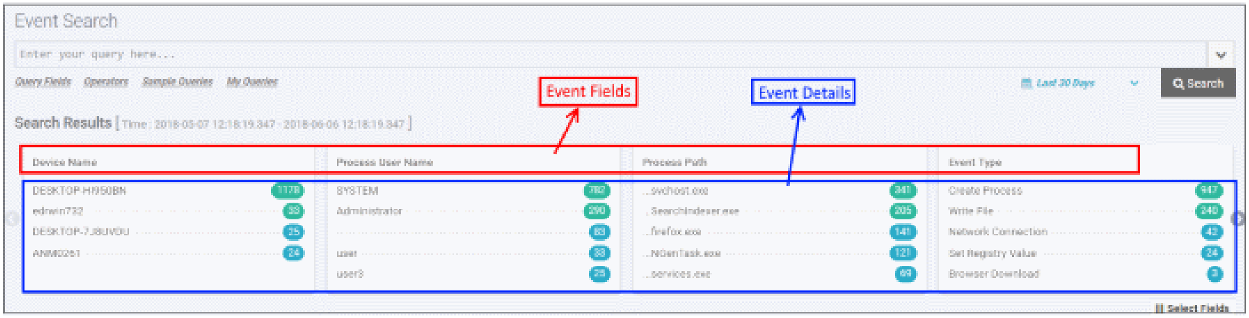


Search Results [Time : 2018-05-07 12:18:19.347 - 2018-06-06 12:18:19.347]

Device Name		Process User Name		Process Path		Event Type	
DESKTOP-HI950BN	1178	SYSTEM	782	...svchost.exe	341	Create Process	947
edrwin732	33	Administrator	290	...SearchIndexer.exe	205	Write File	240
DESKTOP-7J8UVDU	25		83	...firefox.exe	141	Network Connection	42
ANM0261	24	user	33	...NGenTask.exe	121	Set Registry Value	24
		user3	25	...services.exe	69	Browser Download	3

#	Show	Event Time	Device Name	Process User Name	Process Path	Process Hash	Event Type	Adaptive Event Name
+ 1		2018-05-30 17:05:39.395	DESKTOP-HI950BN	Administrator	C:\Users\Administrator\Downloads\Comodo_EDR_Agent_Installer_1.1.258.3_Bk3uAu5kQ.exe	f49d31c432224f6723f56d7a28cd2203bda23e58	Write File	Write to Executable
+ 2		2018-05-30 17:05:28.488	DESKTOP-HI950BN	Administrator	C:\Users\Administrator\Downloads\Comodo_EDR_Agent_Installer_1.1.258.3_Bk3uAu5kQ.exe	f49d31c432224f6723f56d7a28cd2203bda23e58	Write File	Write to Executable
+ 3		2018-05-30 17:05:27.285	DESKTOP-HI950BN	Administrator	C:\Users\Administrator\Downloads\Comodo_EDR_Agent_Installer_1.1.258.3_Bk3uAu5kQ.exe	f49d31c432224f6723f56d7a28cd2203bda23e58	Write File	Write to Executable

Summary Search Results



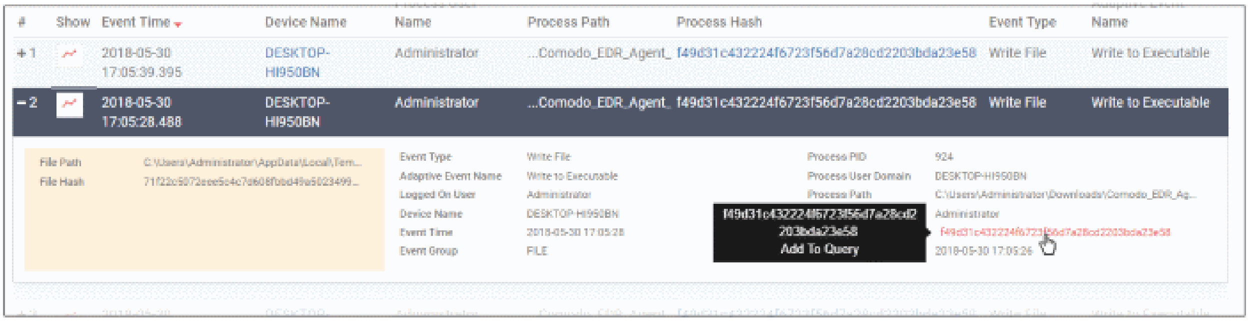
Search Results [Time : 2018-05-07 12:18:19.347 - 2018-06-06 12:18:19.347]

Device Name		Process User Name		Process Path		Event Type	
DESKTOP-HI950BN	1178	SYSTEM	782	...svchost.exe	341	Create Process	947
edrwin732	33	Administrator	290	...SearchIndexer.exe	205	Write File	240
DESKTOP-7J8UVDU	25		83	...firefox.exe	141	Network Connection	42
ANM0261	24	user	33	...NGenTask.exe	121	Set Registry Value	24
		user3	25	...services.exe	69	Browser Download	3

- The number beside each event detail indicates the total number of events recorded for that item.
- Clicking an event detail under an event field will display only the results pertaining to those items.

Event List

The lower section below the tiles displays the results for each event.



#	Show	Event Time	Device Name	Process User Name	Process Path	Process Hash	Event Type	Adaptive Event Name
+ 1		2018-05-30 17:05:39.395	DESKTOP-HI950BN	Administrator	...Comodo_EDR_Agent_	f49d31c432224f6723f56d7a28cd2203bda23e58	Write File	Write to Executable
− 2		2018-05-30 17:05:28.488	DESKTOP-HI950BN	Administrator	...Comodo_EDR_Agent_	f49d31c432224f6723f56d7a28cd2203bda23e58	Write File	Write to Executable

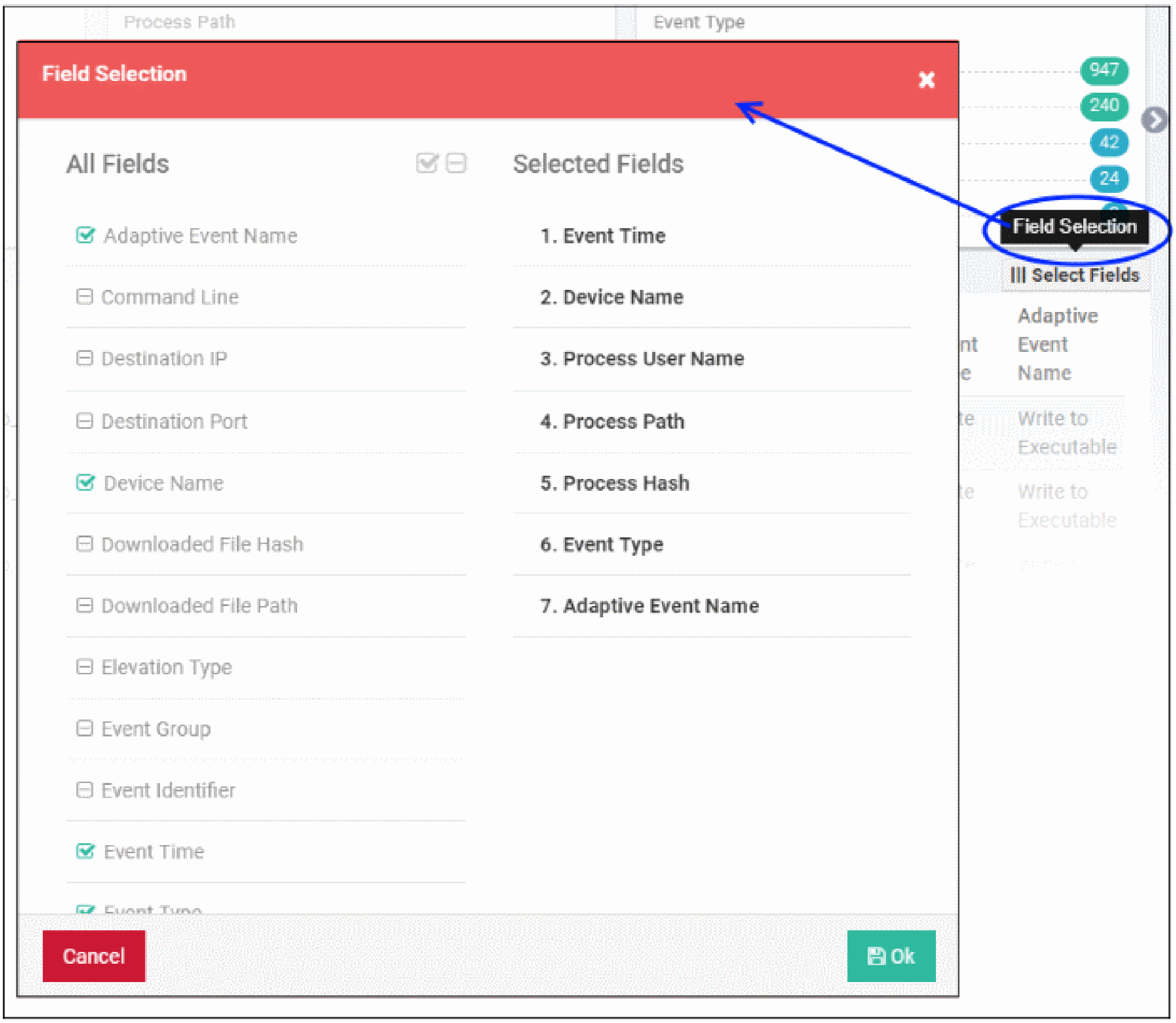
File Path	C:\Users\Administrator\AppData\Local\Tem...	Event Type	Write File	Process PID	924
File Hash	71f22c5072eee5c4c7d608fbbd49a5023499...	Adaptive Event Name	Write to Executable	Process User Domain	DESKTOP-HI950BN
		Logged On User	Administrator	Process Path	C:\Users\Administrator\Downloads\Comodo_EDR_Ag...
		Device Name	DESKTOP-HI950BN		Administrator
		Event Time	2018-05-30 17:05:28		f49d31c432224f6723f56d7a28cd2203bda23e58
		Event Group	FILE		2018-05-30 17:05:26

- Clicking an event row will display all the event fields for that event type. The number of event fields displayed depends on the event type.
- Clicking an event detail beside an event field will display only the results pertaining to those items.
- Clicking the icon in the 'Show' column for an event will display its timeline.

Configure Results Table Column Headers for a Query

You can configure the results table to show columns which are important to your custom query. You can also view all the event fields pertaining to your search by clicking the '+' sign beside a query result.

- Click 'Select Fields' on the right to configure the result table columns:



Field Selection

All Fields

- ☑ Adaptive Event Name
- ⊟ Command Line
- ⊟ Destination IP
- ⊟ Destination Port
- ☑ Device Name
- ⊟ Downloaded File Hash
- ⊟ Downloaded File Path
- ⊟ Elevation Type
- ⊟ Event Group
- ⊟ Event Identifier
- ☑ Event Time
- ☑ Event Type

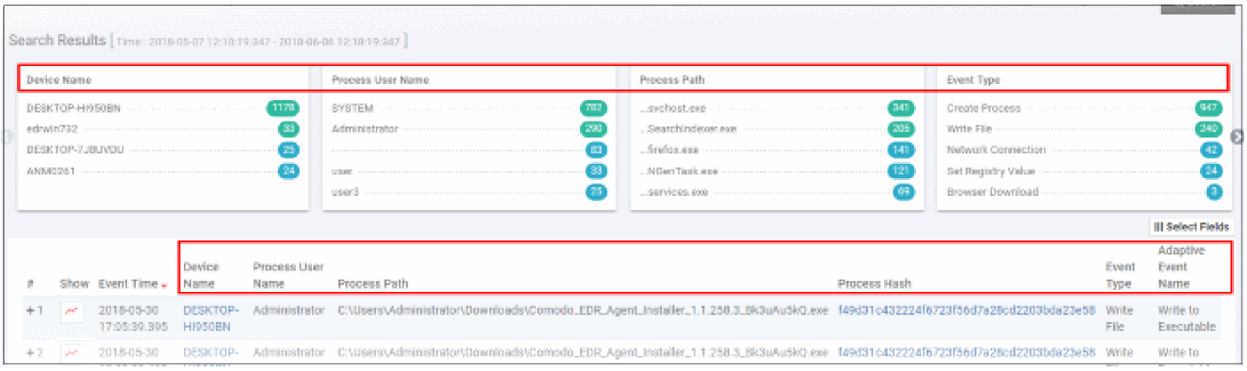
Selected Fields

1. Event Time
2. Device Name
3. Process User Name
4. Process Path
5. Process Hash
6. Event Type
7. Adaptive Event Name

A check-mark is shown next to currently enabled fields. A 'field' in this sense is a column in the results table.

- Click the checkbox beside an individual field to enable or disable it.
- To display all fields, click ☑ at the top
- To hide all fields, click ⊟ at the top.
- All enabled fields are shown on the right, with field # 1 being the first column on the left. Click and drag a particular field to re-position it in the table.
- Click 'Ok' when done.

Your selected fields will be shown as columns in the query search results. The same fields will also be shown for the results summary tiles above the 'Event List' results table. The results summary will not display the 'Event Time' field since this available beside 'Search Results' by default.



Search Results [Time : 2018-05-07 12:18:19.347 - 2018-06-06 12:18:19.347]

Device Name	
DESKTOP-HI950BN	1178
edwin732	33
DESKTOP-7J8UVDU	25
ANM0261	24

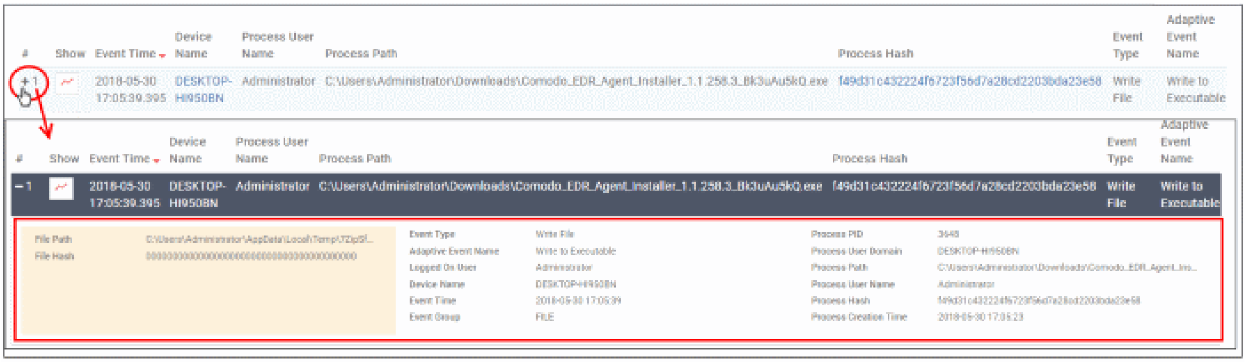
Process User Name	
SYSTEM	702
Administrator	290
	83
user	33
user3	25

Process Path	
...svchost.exe	341
...SearchIndexer.exe	205
...firefox.exe	141
...NGenTask.exe	121
...services.exe	69

Event Type	
Create Process	947
Write File	240
Network Connection	42
Set Registry Value	24
Browser Download	3

#	Show	Event Time	Device Name	Process User Name	Process Path	Process Hash	Event Type	Adaptive Event Name
+ 1		2018-05-30 17:05:39.395	DESKTOP-HI950BN	Administrator	C:\Users\Administrator\Downloads\Comodo_EDR_Agent_Installer_1.1.258.3_Bk3uAu5kQ.exe	f49d31c432224f6723f56d7a28cd2203bda23e58	Write File	Write to Executable
+ 2		2018-05-30	DESKTOP-	Administrator	C:\Users\Administrator\Downloads\Comodo_EDR_Agent_Installer_1.1.258.3_Bk3uAu5kQ.exe	f49d31c432224f6723f56d7a28cd2203bda23e58	Write	Write to

Tip. You can still view all event fields for a result by clicking the number beside a event result row:



#	Show	Event Time	Device Name	Process User Name	Process Path	Process Hash	Event Type	Adaptive Event Name
+ 1		2018-05-30 17:05:39.395	DESKTOP-HI950BN	Administrator	C:\Users\Administrator\Downloads\Comodo_EDR_Agent_Installer_1.1.258.3_Bk3uAu5kQ.exe	f49d31c432224f6723f56d7a28cd2203bda23e58	Write File	Write to Executable

#	Show	Event Time	Device Name	Process User Name	Process Path	Process Hash	Event Type	Adaptive Event Name
− 1		2018-05-30 17:05:39.395	DESKTOP-HI950BN	Administrator	C:\Users\Administrator\Downloads\Comodo_EDR_Agent_Installer_1.1.258.3_Bk3uAu5kQ.exe	f49d31c432224f6723f56d7a28cd2203bda23e58	Write File	Write to Executable

File Path	C:\Users\Administrator\AppData\Local\Temp\7ZipSf...
File Hash	0000000000000000000000000000000000000000

Event Type	Write File
Adaptive Event Name	Write to Executable
Logged On User	Administrator
Device Name	DESKTOP-HI950BN
Event Time	2018-05-30 17:05:39
Event Group	FILE

Process PID	3648
Process User Domain	DESKTOP-HI950BN
Process Path	C:\Users\Administrator\Downloads\Comodo_EDR_Agent_Ins...
Process User Name	Administrator
Process Hash	f49d31c432224f6723f56d7a28cd2203bda23e58
Process Creation Time	2018-05-30 17:05:23

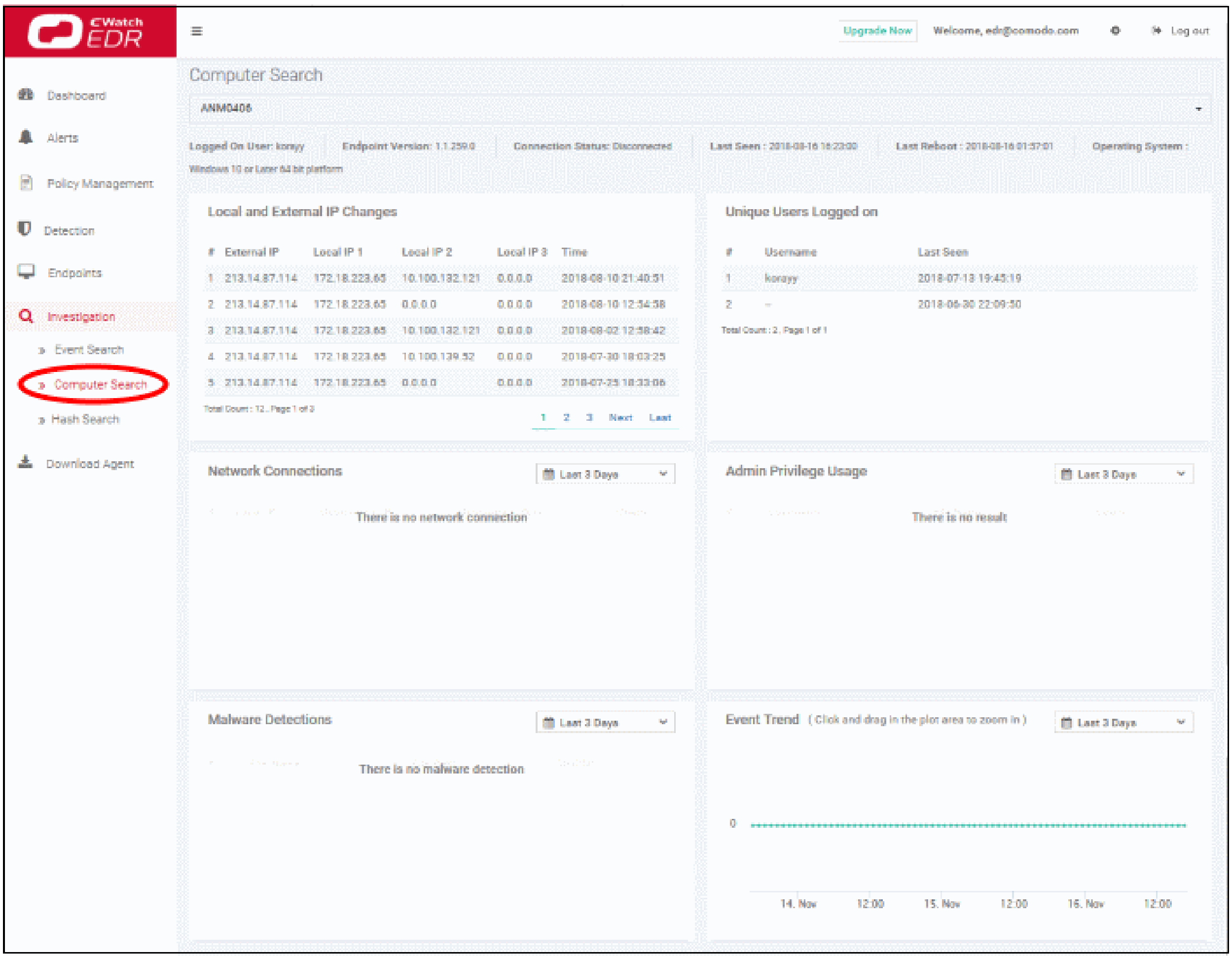
The number of event fields displayed in the detailed results depends on the event type.

See '**Event Search**' topic if you need more help with this.

Step 7 - Investigate Events on Computers

The 'Computer Search' screen shows events recorded on all endpoints added to EDR. Details include event trends, network connection events, malware detection events and so on.

- Click 'Investigation' on the left then 'Computer Search' to open the interface



Computer Search

ANM0406

Logged On User: korayy | Endpoint Version: 1.1.259.0 | Connection Status: Disconnected | Last Seen : 2018-08-16 18:23:00 | Last Reboot : 2018-08-16 01:57:01 | Operating System : Windows 10 or Later 64 bit platform

Local and External IP Changes

#	External IP	Local IP 1	Local IP 2	Local IP 3	Time
1	213.14.87.114	172.18.223.65	10.100.132.121	0.0.0.0	2018-08-10 21:40:51
2	213.14.87.114	172.18.223.65	0.0.0.0	0.0.0.0	2018-08-10 12:54:58
3	213.14.87.114	172.18.223.65	10.100.132.121	0.0.0.0	2018-08-02 12:58:42
4	213.14.87.114	172.18.223.65	10.100.139.52	0.0.0.0	2018-07-30 18:03:25
5	213.14.87.114	172.18.223.65	0.0.0.0	0.0.0.0	2018-07-25 18:33:06

Total Count : 12 , Page 1 of 3

Unique Users Logged on

#	Username	Last Seen
1	korayy	2018-07-13 19:45:19
2	-	2018-06-30 22:09:50

Total Count : 2 , Page 1 of 1

Network Connections

There is no network connection

Admin Privilege Usage

There is no result

Malware Detections

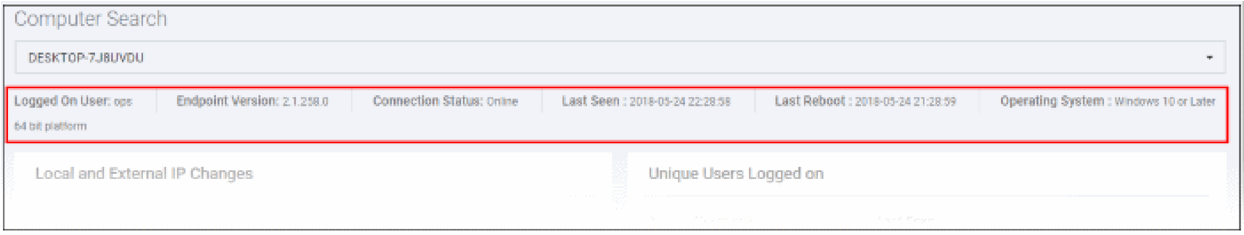
There is no malware detection

Event Trend (Click and drag in the plot area to zoom in)

By default, the screen will be empty with the search range set for the past 3 days.

- Click inside the search field above the data tiles, then:
  - Select an endpoint from the list from the list to view data about the device.
  - You can search for specific endpoints if required
- Use the time-range drop-down to show event info for specific dates (applies to Network Connections, Admin Privilege Usage, Malware Detections and Event Trend tiles).
- Click 'Apply'.

Information about the selected endpoint is shown directly below the search box:


Computer Search

DESKTOP-7J8UVDU

Logged On User: ops | Endpoint Version: 2.1.258.0 | Connection Status: Online | Last Seen : 2018-05-24 22:28:58 | Last Reboot : 2018-05-24 21:28:59 | Operating System : Windows 10 or Later 64 bit platform

Local and External IP Changes

Unique Users Logged on

The six tiles in the main section contain data about events on the endpoint:

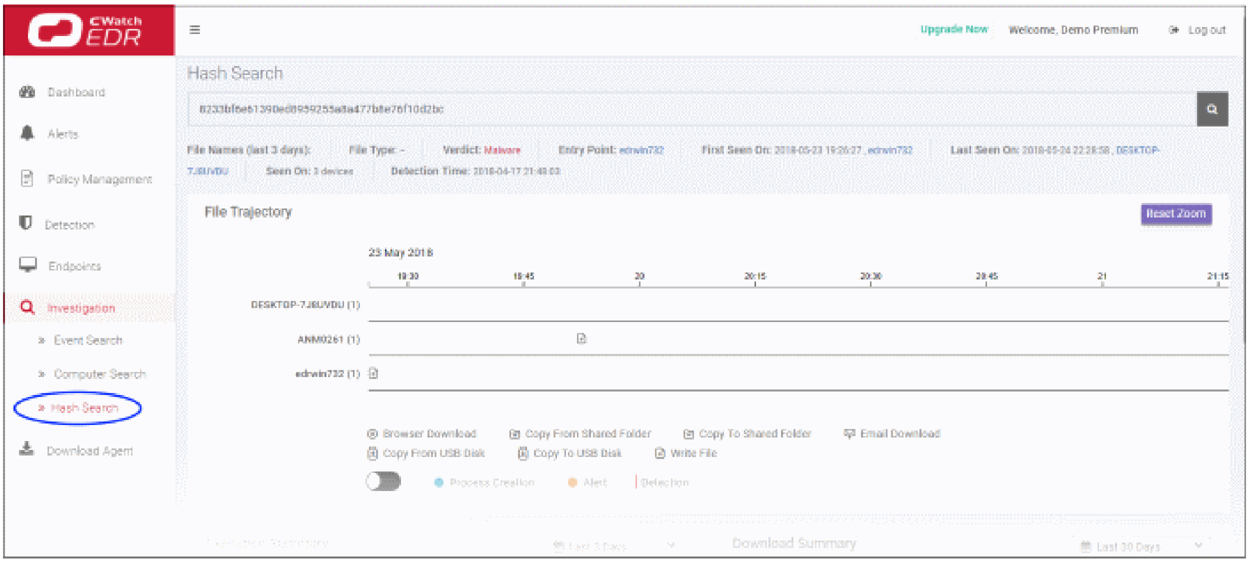
- **Local and External IP Changes -** Changes to the endpoint's local IP and external IP.
- **Event Trend -** Number of events on the endpoint for the selected time-period. You can zoom the timeline by clicking and dragging on the graph. Place your mouse cursor on a point in the line to see events for a specific day.
- **Unique Users Logged on -** Most recent login times of every user that has logged onto the endpoint.

- **Admin Privilege Usage -** Events that required admin privileges.
- **Network Connections -** Network connection events for the selected time-period.
- **Malware Detections -** Threat detection events on the endpoint. Click a hash signature to view full details in the 'Hash Search' interface.

See '**Computer Search**' topic if you need more help with this.

Step 8 - Analyze Files by Hash Values

- A hash search lets you locate files by their MD5 or SHA-1 hash value. Visibility, execution trend, file history and execution summary are listed for each file.
- Unlike the 'Event' and 'Computer' interfaces, you cannot simply search for a hash. You must either
  - (i) Copy and paste a hash value from the dashboard, detection or event search interfaces, or
  - (ii) Click a hash-value link in the dashboard or 'Computer Search' screens. This will auto-populate the search interface.
- Click 'Investigation' on the left then 'Hash Search' to open the interface.

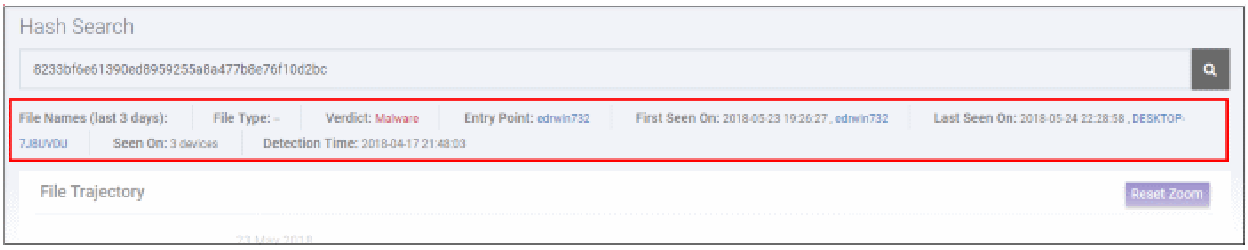


8233bf6e61390ed8959255a8a477b8e76f10d2bc

File Names (last 3 days): File Type: - Verdict: Malware Entry Point: edrwin732 First Seen On: 2018-05-23 19:26:27, edrwin732 Last Seen On: 2018-05-24 22:28:58, DESKTOP-7J8UVDU Seen On: 3 devices Detection Time: 2018-04-17 21:48:03

- By default, the screen will be blank
- Enter the hash value of the file you wish to analyze. Hash values of malware and safe files can be copied from various interfaces such as:
  - 'Dashboard' > 'Malware & Suspicious Activity' tile > under 'Most Found Malware' and 'Last Found Malware'
  - 'Detection' > in the 'Sha1' column
  - 'Investigation' > 'Event Search' > in the 'Process Hash' column
- Click a hash value on any of the screens above to automatically populate the search box here.
- Use the time-range drop-down to show event information for a specific date range (applies to 'Execution Summary', 'Download Summary', 'Creation Summary' and 'Execution Trend' tiles)

Results are shown below the search box:



8233bf6e61390ed8959255a8a477b8e76f10d2bc

File Names (last 3 days): | File Type: - | Verdict: Malware | Entry Point: edrwin732 | First Seen On: 2018-05-23 19:26:27 , edrwin732 | Last Seen On: 2018-05-24 22:28:58 , DESKTOP-7J8UVDU | Seen On: 3 devices | Detection Time: 2018-04-17 21:48:03

File Trajectory

The results screen shows the following details about the file:

- **File Trajectory -** The movement of the file - where it was downloaded from, where it was copied to, and so on.
- **Execution Summary -** Devices on which the file was executed. Details include the file path and the number of times it was executed.
- **Download Summary -** Which endpoints the file was downloaded to ('Entry Point'), the URL it was downloaded from, and the number of times it was downloaded.
- **Creation Summary -** Endpoints on which the file created processes, and the file location.
- **Execution Trend -** The number of times the file was executed during the selected period. Zoom into specific hours by dragging any point on the graph.

See '**Hash Search**' if you need more help with this.

Step 9 - View Process Timeline of Events

The 'Process Timeline' shows all processes spawned by an event.

You can view the timeline in two ways:

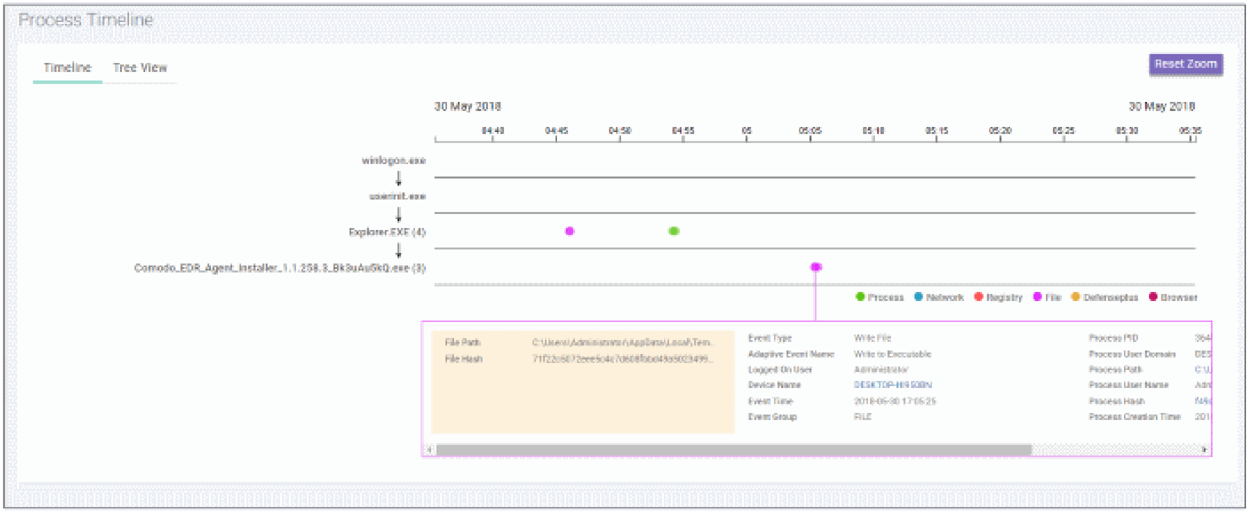
Event Search

- Go to 'Investigation' > 'Event Search', select a time-period and click 'Search'.
- Click the timeline icon in the 'Event List' section.
- Alternatively, enter an event ID manually to view its timeline.

Alerts

- Go to 'Alerts' then click 'Show Alerts' in a row.
- Click the timeline icon in the 'Event List' section.

The timeline of the selected event will be shown:



File Path: C:\Users\Administrator\AppData\Local\Tem...
File Hash: 71f22c6072eee5c4c7d608fbbd49a5023499...

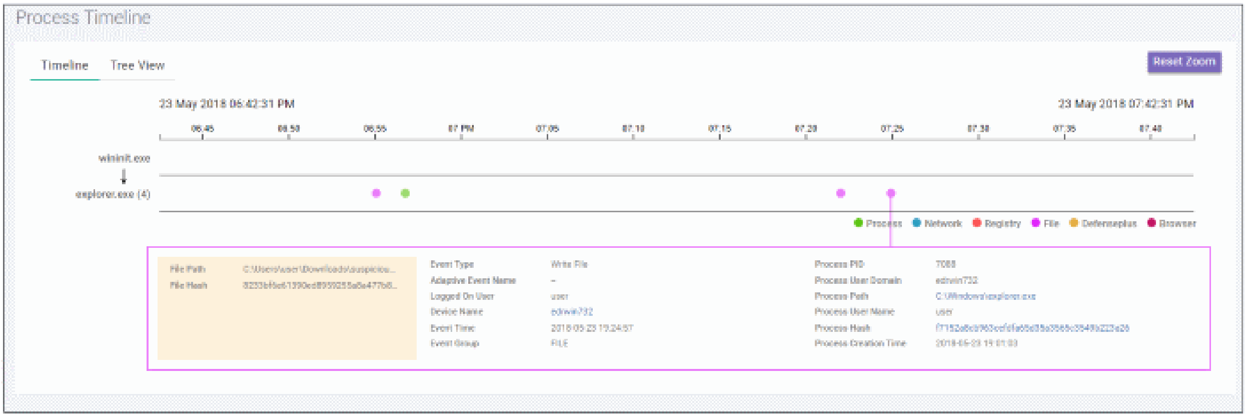
Event Type: Write File
Adaptive Event Name: Write to Executable
Logged On User: Administrator
Device Name: DESKTOP-HH9S0BN
Event Time: 2018-05-30 17:05:25
Event Group: FILE

Process PID: 364
Process User Domain: DES
Process Path: C:\U
Process User Name: Adm
Process Hash: f4fe
Process Creation Time: 201

You can view the details in timeline or tree view.

Timeline View

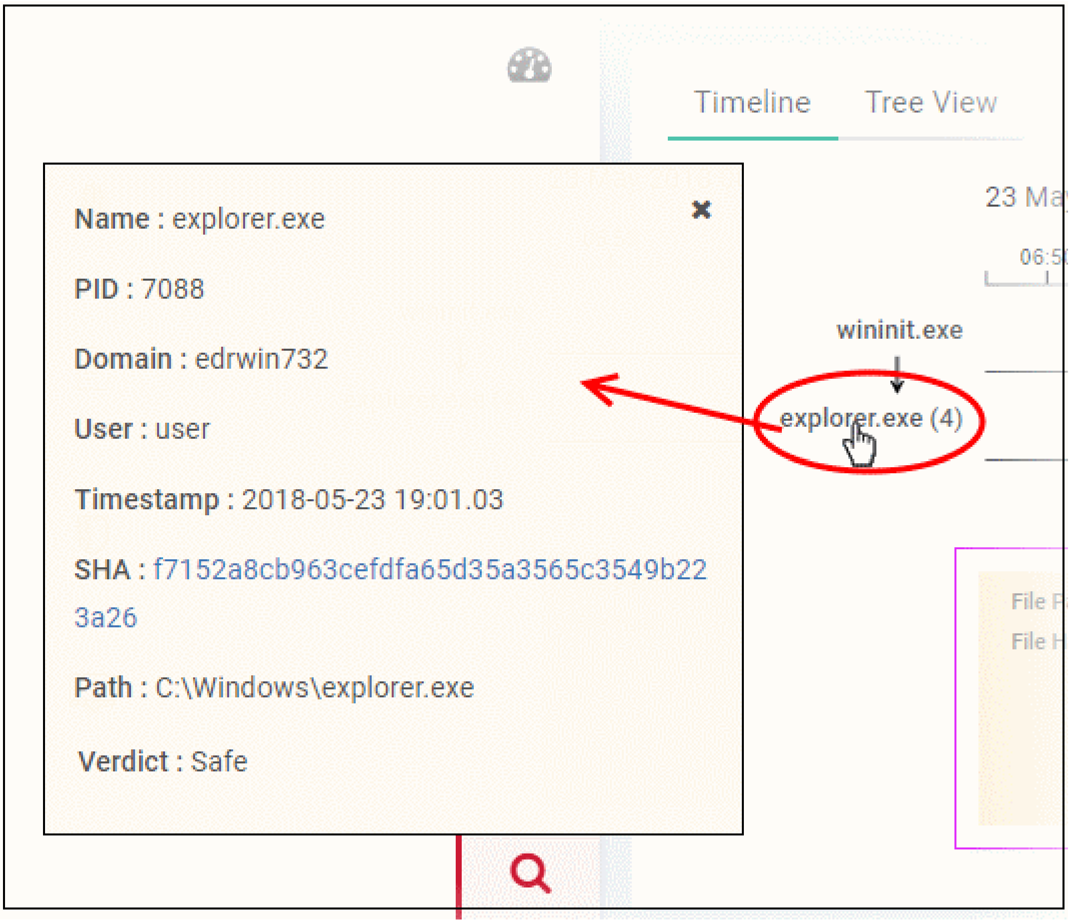
The timeline view is the default view:



File Path	C:\Users\user\Downloads\suspicio...
File Hash	8233bf6e61390ed8959255a6e477b6...

Event Type	Write File	Process PID	7088
Adaptive Event Name	-	Process User Domain	edrwin732
Logged On User	user	Process Path	C:\Windows\explorer.exe
Device Name	edrwin732	Process User Name	user
Event Time	2018-05-23 19:24:57	Process Hash	f7152a8cb963cefdfa65d35a3565c3549b223a26
Event Group	FILE	Process Creation Time	2018-05-23 19:01:03

- The time-line shows processes generated by the event over time.
  - Results are shown for processes generated 30 minutes before and after the event.
  - For example, if an event started at 11.00 AM, results are shown from 10.30 AM to 11.30 AM
  - The timeline of the event is shown at the top with date and time preselected.
- Executables opened by the event are shown by the down arrow on the left.
  - The number beside a process name shows the quantity of events created by the process.
  - Click on a process to view process name, time-stamp, hash, path and verdict:



Name : explorer.exe

PID : 7088

Domain : edrwin732

User : user

Timestamp : 2018-05-23 19:01.03

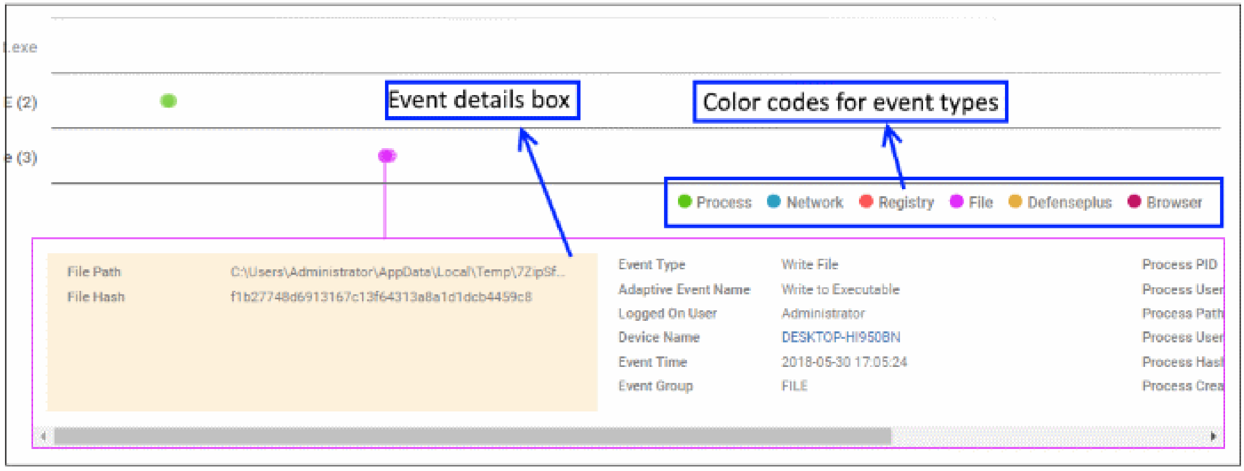
SHA : f7152a8cb963cefdfa65d35a3565c3549b223a26

Path : C:\Windows\explorer.exe

Verdict : Safe

- Details about the event (created by the process) are shown in the box below the process path.

- The event types are color coded and displayed above the event details box.


t.exe
E (2)
e (3)
Event details box
Color codes for event types
● Process ● Network ● Registry ● File ● Defenseplus ● Browser

File Path C:\Users\Administrator\AppData\Local\Temp\72ipSf...
File Hash f1b27748d6913167c13f64313a8a1d1dcb4459c8

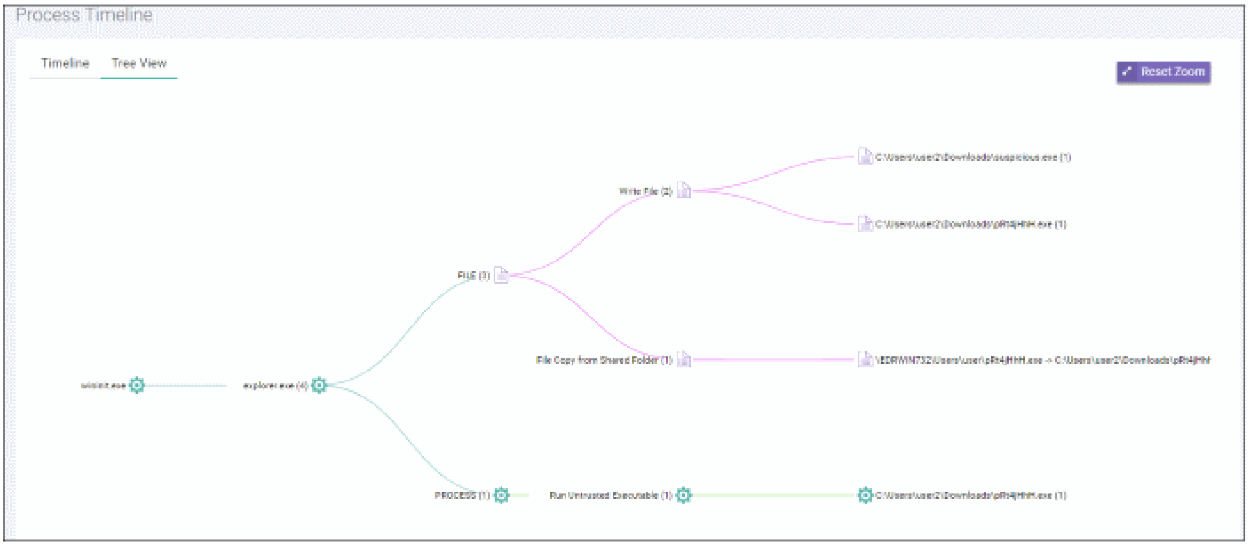
Event Type Write File
Adaptive Event Name Write to Executable
Logged On User Administrator
Device Name DESKTOP-HI950BN
Event Time 2018-05-30 17:05:24
Event Group FILE

Process PID
Process User
Process Path
Process User
Process Hash
Process Crea

- Event details show all event fields for that event type. The number of event fields displayed depends on the event type.

Tree View

- Click the 'Tree View' tab.
- The view shows process activity as a sequence of parent/child events:


Process Timeline
Timeline
Tree View
Reset Zoom
wininit.exe
explorer.exe (4)
FILE (3)
Write File (2)
C:\Users\user2\Downloads\suspicious.exe (1)
C:\Users\user2\Downloads\pRt4jHhH.exe (1)
File Copy from Shared Folder (1)
\EDRWIN732\Users\user\pRt4jHhH.exe -> C:\Users\user2\Downloads\pRt4jHhH
PROCESS (1)
Run Untrusted Executable (1)
C:\Users\user2\Downloads\pRt4jHhH.exe (1)

- Use mouse to zoom in and zoom out. Click 'Reset Zoom' to default view.
- The number beside a process name indicates the number of events generated by the process.
- Click a process name to view full details about it in the '**Event Search**' screen.

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 cyber-attacks 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**