



# Comodo EDR

Software Version 1.7

### Administrator Guide

Guide Version 1.1.071619

Comodo Security Solutions 1255 Broad Street Clifton, NJ 07013

#### **Table of Contents**

1 Introduction to Comodo EDR	3
1.1 Purchase Licenses	4
1.2 Login to the Admin Console	7
2 The Admin Console	9
3 The Dashboard	10
4 MSP Dashboard	12
5 Add Endpoints to EDR	16
6 View Enrolled Endpoints	19
7 Manage EDR Policies	20
8 View Event Details on Endpoints	33
9 Alerts	
10 Investigation	42
10.1 Event Search	43
10.2 Computer Search	53
10.3 Hash Search	60
10.4 Process Timeline	66
Appendix 1 - Default Comodo Security Policy Details	70
Appendix 2 - Agent Firewall Ports, IPs and Domains	78
About Comodo Security Solutions	80

## 1 Introduction to Comodo EDR

Comodo Endpoint Detection and Response (EDR) is a powerful event analysis tool that provides real-time monitoring and detection of malicious events on Windows endpoints. EDR allows you to visualize threats in a detailed timeline while instantaneous alerts keep you informed if an attack occurs.

EDR's cloud-based admin console can be accessed anytime using an internet browser.

- You can enroll for a free EDR account at https://edr.cwatch.comodo.com
- You can login to the EDR admin console at https://edr.cwatch.comodo.com/login
- You can also access EDR through your Comodo One/ Comodo Dragon / ITarian account. Login then click 'Applications' > 'cWatch EDR'.
- You must install the EDR agent on all endpoints you wish to monitor. After logging-in, click 'Download Agent' to get started.

Image: Adverting Process   Matt Adverting Process   Image: Adver	Malware &	Suspicious Activity			Endpoint Overview	Show Details
USHJCGS7 Most Alersed Endpoint   Most Alersed Endpoint Most Alersed Endpoint   Most 181559600D057DC6831A88190D7F475301A3425E Most 5556A9D0616ED7161A889192E253180DA85AD10   Last Found Malwere Disconnected   Endpoint Health Status Most Found Malwere   Safe 23   Detections 1   Needs Agent Update 21	Q <sub>0</sub>	powershell exe Most Alerting Process	A	1262 Total # of Alerts		4 Office
IstE596000057DC6B31A3B100TF4F75301A3425F   Most Found Mahware   Most Found Mahware   Endpoint Health Status   Sale   0   Bale   28   0   0   Bale   28   0   1   Reseda Agent Update   21	Ģ	USNJCS7 Moar Aleraed Endpoint	<b>å</b>	ozerm Most Alerted User	тота	24 L DEVICES
Endpoint Health Status   Sale   23   Email   Derections   1   Reserts Luptans   21   Shared Fulder   Resonable Media	₩ <sup>1</sup>	81E59600D057DC6B31A3B19D7F4F753D1A3425E Most Found Maiware	ж. <sup>с</sup>	45356A9DD616ED7161A389192E2F318DDA85AD10 Last Found Malware	20 Disconnected	
Endpoint Health Status Attack Vectors   Safe 23   Detections 1   Needs Agent Update 21   Shared Folder 05   Removable Media 05						Disconnected Offine Drine
Safe     28     Email     0%       Detections     1     Enumer     0%       Reeds Agent Update     21     Shared Folder     0%       Removable Media     0%     0%	Endpoint H	lealth Status			Attack Vectors	
Detections 1 Browser 04	Safe.			23	Email	0%
Needs Agent Update 21 Shared Folder 04 Removable Media 04	Detections	-			Browser	04
Removable Media	Needs Agent U	Ipdate		21	Shared Folder	02
					Removable Media	05
Other (100%)					Other	(10%)

#### Features

- · Continuous threat monitoring of managed endpoints
- Advanced search capabilities for file hashes and detection
- · Real-time visibility into what's happening in your environment
- Policy customization
- Unrivaled process timeline visualization
- · Retrospective analysis of events
- Centralized cloud hosted architecture
- · Human analysis of unknown file and event types
- · Compatible with other endpoint security tools
- Multi tenancy Support

#### **Guide Structure**

This guide is intended to take you through the configuration and use of EDR and is broken down into the following main sections. The guide can also be navigated using the bookmarks on the left.

COMODO Creating Trust Online\*

- Introduction
  - Purchase Licenses
  - Login to the Administrative Console
- The Admin Console
- The Dashboard
- MSP Dashboard
- Add Endpoints to EDR
- View Enrolled Endpoints
- Manage EDR Policies
- View Event Details on Endpoints
- Alerts
- Investigation
  - Event Search
  - Computer Search
  - Hash Search
  - Process Timeline
- Appendix 1 Default Comodo Security Policy Details
- Appendix 2 Agent Firewall Ports, IPs and Domains

#### 1.1 Purchase Licenses

There are two ways you can sign up for cWatch EDR.

- From cWatch EDR website as stand-alone application
- From your Comodo One / Comodo Dragon / ITarian portal as an integrated application

#### **Stand-alone application**

It only takes a few steps to subscribe to the EDR service:

- Visit https://edr.cwatch.comodo.com/
- · Select your plan and click 'Protect your Endpoints Now'

The purchase page will be displayed:

#### COMODO Creating Trust Online\*

сомор	O Creating Trust Online <sup>™</sup>	Need Assistance? 888-351-7956	
		•	
Shop	pping Cart	Account Details	Complete Order
~	cWatch EDR FREE 1 year		
cWatch			\$ 0.00
Cruch	cWatch EDR FREE 1 year		
ENTER CU	Odo User	Register a new Comodo acco	unt with your e-mail address.
New Comodo	User	E-mail address * :	
		Password *:	
I have read a	nd agree to the End User license/Se	rvice Agreement	Continue »
	Terms & Condition	s   Conditions of Use   Privacy Notice	

- Select a subscription plan. A free,1 year is also available. You have to provide your credit card details for a paid subscription.
  - Subscribing for EDR without Comodo Account
  - Subscribing for EDR with Comodo Account

#### If you do not have a Comodo account:

- Select 'New Comodo User'
- · Enter your email address and password in the respective fields
- Provide credit card details if you select a paid subscription
- · Click 'End User license / Service Agreement' link, read the EULA fully and select the check-box
- Click 'Continue'

Your order will be processed and a confirmation message will be displayed:

#### COMODO Creating Trust Online\*

COMODO Creating Trust Online"	() Need Assistance 888-351-795	6 CHAT NOW!
Shonning Cart Ac	count Details	Complete Order
Congratulations! Your	Order is complet	te.
CWatch EDR FREE 1 year	on has already been sent to y	our email.
ORDER NUMBER 36250177-1	SUBSCRIPTION ID	30fac9af78
» cWatch EDR FREE 1 year		
Getting Started		
How do I login to my account?		
Login		
You can download your agent software by following the or	"Download Agent" link in EDR	web application.
Your system administrator can set up the agent softwa	re using GPO	
or		
You can deploy cWatch EDR using COMODO ITSM vi	a script execution	

You will also receive a confirmation message to your email address. A new Comodo account (CAM) will be created for you at https://accounts.comodo.com/. You can subscribe to various Comodo products using this account. See 'Comodo Accounts Manager' help guide for more details about how to manage your account.

#### If you have a Comodo account:

- Select 'Existing Comodo User'
- Enter your 'Comodo Accounts Manager' (CAM) username and password in the respective fields
- Provide credit card details if you chose a paid subscription
- · Click 'End User license / Service Agreement' link, read the EULA fully and select the check-box
- Click 'Continue'

Your order will be processed and a confirmation message will be displayed and a notification sent to your registered email also. Comodo EDR will be added to your subscribed products list. See 'Comodo Accounts Manager' help guide for more details about how to manage your account.

#### Comodo One / Comodo Dragon / ITarian customers

#### To subscribe for EDR via Comodo One / Comodo Dragon / ITarian portal

- Login to your Comodo One / Comodo Dragon / ITarian account
  - The purchase process is same for Comodo One / Comodo Dragon and ITarian. Comodo One portal is shown below as an example.
- Click 'Store' in the top-menu
- Click 'Buy' or 'Free' on the EDR tile.

	agement - 🗃 reports 🐂 store 💼 tools		😵 Roome e 🗄 🗄 🛛 v 💿 v 💐 🙆 herculespopulær v
Acronis Cloud Backup can help you securely migrate, protect and recover critical data whenever it madate in your physical, which are cloud environments. Its innovative solutions are designed L.	CWatch is a managed Breach Prevention and Compliance solution that leverages a modular Security as Service platform to monitor the data from various sensors spread across your private and public.	Comodo Dome Is a revolutionary Cloud Delivered Secure Web Pietform that to delivered as a Security as a-Service (Sack) solution that provides fully comprehensive web c	Comodo Dome Shield PLATINUM is a package designed to improve your Dome Shield experience with advanced and exclusive features! Meet Dome Shield PUATINUM, the.
Bay	Free	30 Days Free Trial Buy	30 Days Free Trial Buy
CRM	CONODO DOME WETUM	compile games	
Customer Relationship Manager Tool (CRW) is a powerful tool designed to manage all field and contacts by campaigns and opportunities prepare quotes involves so that you can grow your sales, impr	Dome Prewall Virtual Appliance is a free of charge Unified Threat Nonagement solution that can be Installed into any hardware or virtualization solution within your company network. Dome Riewa	Comodo Dome Antispam is an enterprise antispam and threat prevention appliance that uses a sophisticated array of spam filters, anti-irus scanners and content analysis engines to prevent uncol	Dome Frewall Central Manager is a free of charge Central Management Solution for Dome Firewall Virtual Appliances that ca
Free	Free	30 Days Free Foat Buy	Free
CWatch			
C EDR			
cWwtchiDR is a cloud-based endpoint detection and response solution thetgives unrivalled visibility into what's happening in yourenvironment.			
free			

- You will be taken to the respective subscription page.
- Complete the purchase process. See https://help.comodo.com/topic-457-1-981-14357-Add-cWatch-EDR.html for more details.

#### 1.2 Login to the Admin Console

There are two methods to login to EDR:

- Stand-alone EDR customers
- Comodo One / Comodo Dragon / ITarian portal customers

#### Stand-alone EDR portal

 Customers that subscribed for stand-alone EDR application should login at http://edr.cwatch.comodo.com/



ſ		Can't Wait? Call Now +1 (844) 260-2204 Login
	CWatch EDR	rs Who needs cWatch EDR? Help Guide
	Welcome to EDR	
s Fir	🛎 Email	always be FREE!
	& Password	No. Contraction of the state of the
s abou ns too	SIGN IN Forgot Password?	ints need protection against file- s, memory exploits, abuse of powershell?
the attac	Don't have an account? Sign Up	anced event definitions
it the full att	ack chain is	COMODO's Recommended Security Policy

Enter your credentials and click 'Sign in'. If you have forgotten your password, click 'Forgot Password' to reset it.

After successful verification, the 'EDR Dashboard' page will be displayed:

Malware & Suspicious Activity		Endpoint Overview	Show Details
Dowershell.exe Most Alerting Process	Total *	1262 di Alersa	4 Office
USNJCS7 Most Alerael Endpoint	Most Aler	ozerm ed User TOTAL D	4 IEVICES
181E50600D057DC6B31A3B1907F4F75501A3425 Most Found Malware	45356A9DD616ED7161A389192E257318DD Last Found I	ABSAD10 Jalware 20 Disconnected	
			Disconnected Offline Online
Endpoint Health Status		Attack Vectors	
Safe	— 23	Email	er
Detections	1	Browser	01
Needs Agent Update	21	Shared Folder	(m)
		Removable Media	0%
		Other	100%

#### Comodo One / Comodo Dragon / ITarian customers:

- Login to your Comodo One / Comodo Dragon / ITarian account
- Click 'Applications' > 'cWatch EDR' to open the EDR interface

COMODO Creating Trust Online\*

ONC		t ~ 🖶 reports 🍹	STORE 🚔 TOOLS	Facome Fartner	• =0 · @ · 💐 🛛 ·
ENROLL NEW DEVIC	Endpoint Manager		ENROLL DEVICES IN BULK		REW QUOTE
	RMM				
Customer: All	Patch Management				o: Customize
Help Actions	Device Management Procedures	1	Ticket Data		1
¥	Endpoint Protection Service Desk	@=	0 High Priority	3 Open	3 Overdue
Help Guides	Dome Shield	Email Support			
4	CWatch EDR				
	Quote Manager		Assigned	Unassigned	Iotal Tickets
R	All Applications			-	
Contact Information	1		0	2	

## 2 The Admin Console

- The EDR admin console allows you to enroll endpoints, create polices, view and analyze events and more.
- You need to install the EDR agent on all endpoints you wish to manage. Click 'Download Agent' to get started.

Malware & S	Suspicious Activity			Endpoint Overview	Show Details
00	powershell exe Most Alerting Process	A	1262 Total # of Alexa		4 Othine
Ģ	USNJCS7 Moan Alerted Endpoint	4	ozern Most Alented User	то	24 TAL DEVICES
∰ <sup>18</sup>	1E59600D057DC6B31A3B19D7E4E75301A3425E Most Found Malware	<del>Ж</del>	45356A9DD616ED7161A389192E2F318DDA85AD10 Last Found Malware	20 Disconnected	
					Disconnected Offline Online
Endpoint He	ealth Status			Attack Vectors	
Safe			23	Email	0%
Detections	-		1	Browser	(***
Needs Agent Up	pdate		21	Shared Folder	0%
				Removable Media	or
				Other	100%

The buttons at the top of the interface allow you to:

Expand / collapse the left-hand menu.

Upgrade Now

Allows you to purchase a higher subscription plan. The available plans are:

- Free for 1 year 3 days data retention/history
- Premium 30 days data retention/history
- Platinum 90 days data retention/history

➡ Log out Log out of the EDR admin console.

The menu on the left contains links to the main areas of the console:

- **Dashboard** A top level overview of events on your managed endpoints. The dashboard shows the number of online, offline and disconnected devices, a summary of detected malware and the most attacked/ most recently attacked endpoints. See 'The Dashboard' for more details.
- Alerts A list of warnings generated by a policy breach. Alert details include name of the event, time of the breach and more. See 'Alerts' for more details.
- **Policy Management** EDR ships with default policy that will monitor and generate alerts for numerous attack types and activities. You can also configure custom policies according to your requirements. See **Manage EDR Policies** for more details.
- Endpoints A list of Windows devices enrolled to EDR. Each row shows various details about the endpoint, including computer name, operating system, connection status and more. See 'Viewing Enrolled Endpoints' for more details.
- Detection Displays more detailed information about the malware found on your endpoints. See 'Viewing Event Details on Endpoints' for more details.
- Investigation Allows you to search for, identify and analyze events by event type, by computer or by hash value. See 'Investigation' for more details.
- **Download Agent** Download the endpoint agent. You need to install this agent on your target Windows machines in order for EDR to monitor them. See 'Adding Endpoints to EDR' for more details.

## 3 The Dashboard

The dashboard is an at-a-glance summary of the security and connection status of enrolled endpoints. Each dashboard tile shows vital information about detected malware and allows you to drill-down further on areas of interest. Statistics include most the attacked endpoint, the quantity of malware found, the number of enrolled devices and so on.

Click 'Dashboard' on the left to view the EDR dashboard

COMODO Creating Trust Online\*

<b>E</b> Watch EDR	=	Upgrade Now Welcome, edi@comodo.com 94 Log out
Dashboard	Malware & Suspicious Activity	Endpoint Overview Show Details
Alets	powershell.exe         1262           Most Alerting Process         Total # of Alerts	-2 Online
Policy Management     Detection	USNJCS7 Carem Most Alerted Endpoint Most Alerted User	24
Endpoints      Investigation	181E59600D057DC6B31A3B19D7F4F75301A325E 45356A9D0616ED7161A3B9192E2F318D0A	18 Disconnected
<ul> <li>Event Search</li> <li>Computer Search</li> </ul>		Disconnected Offine Online
» Hash Search		
A Download Agent	Endpoint Health Status	Attack Vectors
	Safe 23	Email
	Detections - 1	Browser 0%
	Needs Agent Update 21	Shared Folder 0%
		Removable Media
		Other

- Stand-alone and Comodo One / Comodo Dragon / ITarian enterprise customers You can view endpoint statistics of your company.
- Comodo One / Comodo Dragon / ITarian MSP customers You can view endpoint statistics of all companies managed by you. See MSP Dashboard to to learn more.

#### **Dashboard Tiles**

- Malware & Suspicious Activity
  - Most Alerting Process Name of the application process that generated most alerts. Click the
    process name to open the 'Alerts' interface which shows more details. See 'Alerts' for more
    information.
  - Most Alerted Endpoint The name of the device for which the most number of alerts were generated. Click the name of the endpoint to open the 'Alerts' interface which shows more details. See 'Alerts' for more information.
  - **Most Found Malware** The hash value of the most prevalent malware on all your managed endpoints. Click the hash value to view malware details, including the endpoints that triggered the events, the date and time of the event and so on. See 'Hash Search' for more details.
  - **Total number of Alerts** The total number of alerts generated for all enrolled endpoints. Click the alert number to open the 'Alerts' interface. See 'Alerts' for more information.
  - Most Alerted User The device user for whom the most alerts were generated.
  - Last Found Malware The hash value of the malware that was detected most recently. Click the hash
    value to view malware details, including the endpoints that triggered the events, the date and time of
    the event and so on. See 'Hash Search' for more details.
- Endpoint Overview
  - Total Devices The total number of endpoints you have added to EDR
  - Online Devices The number of devices that are currently active.
  - Offline Devices The number of endpoints that are currently shut down and not connected to EDR.
  - **Disconnected Devices** Enrolled devices that are logged off. Disconnected devices includes endpoints that were not shut down properly or crashed.



- Click 'Show Details' to open the 'Endpoints' interface to view information about the endpoint. See 'View Enrolled Endpoints' for more details.
- Endpoint Health Status
  - Safe The number of endpoints where no malicious activities were detected.
  - Detections The number of devices on which malicious and suspicious activities were detected.
  - Needs Agent Update The number of endpoints which are using an outdated version of the EDR agent. EDR supports auto-update. Whenever an endpoint with outdated agent version goes online, it gets the latest update.
- Attack Vectors The channel via which malicious activities originated on the endpoints.

### 4 MSP Dashboard

Comodo One / Comodo Dragon and ITarian MSP customers can view endpoint statistics of all companies managed by them.

- Login to your Comodo One / Comodo Dragon / ITarian account
- Click 'Applications' > 'cWatch EDR'

.

- Click 'Store' if you haven't yet activated EDR. You can install the free version from the 'CWatch EDR' tile.
- Click 'MSP Dashboard' on the left of the EDR interface to view statistics for all companies on your account.

Top 10 Endpoints with	Most Alerts		Tip 10 Users with I	Nost Alerts		Total Number Of Alerts: 4850 (Last 90 Days)
Endpoint Plane	Companya Passina	maniper tri niert	Unersame	CONCIATS Plante	Number Of Alert	
VEROEVPC	Witness Sizell' American	18503	Webster	Distaine Marth Adventure	10403	
001085	Gramon tapath Januaroa	12508	abbreak	Tadenali	6-407	Tadouat: 25.95
049-01-00	Tedenari	11400	admin	Wirnes North America	11015	
TM PURCHTREY	Trailement	9287	in section 1	Testemati	8187	
Charles of sets	Tradamark	4479	therear.	diverses hereb Jenaries	1074-1 I	
INCOMPANYING INCOMPANY	Mining Roll America	8208		Tedenah	0.011	
Adverte Persona da	Trailements	621.5	A fedaration	Receive Intell America	60223	
dute-en-ler	'madamash	0.044	rand	trachemark	10.044	
ADMAGDIOTANTPO	Writeway Nurth American	801.8	12 millioner	Drives North America	80234	
ADDITE HIPSIDE	Trademark	4198	Adminute and	Trademach	0001	
Tro If Provenue all	h binat ällerin		Ment Duard Malaca			Total Newtow / Halasam Detertion: 16.0 art 90 Taxet
Top To Processes with	D MORE ANETS		NOT POUR MANY			India realizar of realizaria orbectable. In (Last 1/ Last
Preserves Harrison	Contraining Nation	Rasilar-O'Abria	DAA .	Carriptory	Nature Hash Previdence	A Andrew Manual 1 1 1
Explore D41	Trademark	44675	1010-2018-2018-2018-2018-2018-2018-2018-	(7.) Tydenai		
mitter verspirerere	Taberak	18265	DIRACHING CONCERN	trademant		
subargasa.	Ohimuu Narih Javariaa	16468				- Seiner Harth James
Capitone DAT	Fademark	-400				
0.00010101000	Tuderat	11308				
Operita esta a su a	Tradewark	10070				
dyame.exe	Instemark	wate				
Paldarciant/platerare	Thirty Play in Array ins	8339				
MedProfil and	Albieves Narih America	1000 C				
Continuous	Memor reach whereas	1004				
						Tudenast, 71.85
Newerl Delections						Endpoints (Tencement) (Second
		Total and the second				

Top 10 Endpoints with Most Alerts - List of endpoints which caused the most alerts to be generated (all time).

#### Top 10 Endpoints with Most Alerts Number Of Alert Endpoint Name Company Name WEBDEV-PC 18605 Shimco North America SRVSBS Shimco North America 12505 SAF-X1-ED Trademark 11465 TMI-PURCH-TREV Trademark 9237 **IT-THINK-SPARE** Trademark 8672 ENGINEERING3 Shimco North America 8503 ADM-HP800G3-SS Trademark 8213 ELEC-X1-RD Trademark 6244 Shimco North America ADMASSISTANT-PC 6014 ACCT2-HPZ200 Trademark 5198

Top 10 Users with Most Alerts - List of users who caused the most alerts to be generated (all time).

UsernameCompany NameNumber Of AlertWebdevShimco North America18605edabrowskiTrademark11457adminShimco North America11015bverrietTrademark9187SForrestShimco North America8961sherrisTrademark8498O_indieserveShimco North America6522ryandTrademark6244KSivathasanShimco North America6014AdministratorTrademark5601	Top 10 Users with Most Alerts				
WebdevShimco North America18605edabrowskiTrademark11457adminShimco North America11015bverrietTrademark9187SForrestShimco North America8961aherrisTrademark84980_indieserveShimco North America6522ryandTrademark6244KSivathasanShimco North America6014AdministratorTrademark5601	Username	Company Name	Number Of Alert		
edabrowskiTrademark11457adminShimco North America11015bverrietTrademark9187SForrestShimco North America8961aherrisTrademark8498O_indieserveShimco North America6522ryandTrademark6244KSivathasanShimco North America6014AdministratorTrademark5601	Webdev	Shimco North America	18605		
adminShimco North America11015bverrietTrademark9187SForrestShimco North America8961sherrisTrademark8498O_indieserveShimco North America6522ryandTrademark6244KSivathasanShimco North America6014AdministratorTrademark5601	edabrowski	Trademark	11457		
bverrietTrademark9187SForrestShimco North America8961sherrisTrademark8498O_indieserveShimco North America6522ryandTrademark6244KSivathasanShimco North America6014AdministratorTrademark5601	admin	Shimco North America	11015		
SForrestShimco North America8961sherrisTrademark8498O_indieserveShimco North America6522ryandTrademark6244KSivathasanShimco North America6014AdministratorTrademark5601	bverriet	Trademark	9187		
sherrisTrademark84980_indieserveShimco North America6522ryandTrademark6244KSivathasanShimco North America6014AdministratorTrademark5601	SForrest	Shimco North America	8961		
0_indieserve     Shimco North America     6522       ryand     Trademark     6244       KSivathasan     Shimco North America     6014       Administrator     Trademark     5601	sherris	Trademark	8498		
ryand     Trademark     6244       KSivathasan     Shimco North America     6014       Administrator     Trademark     5601	0_indieserve	Shimco North America	6522		
KSivathasan     Shimco North America     6014       Administrator     Trademark     5601	ryand	Trademark	6244		
Administrator Trademark 5601	KSivathasan	Shimco North America	6014		
	Administrator	Trademark	5601		

**Total Number of Alerts (Last 90 Days) -** Amount of alerts generated by all users and all endpoints in the previous 90 days. Alerts are broken down by company responsible:

Total Number Of Alerts: 4650 (Last 90 Days)

Top 10 Processes with Most Alerts - The 10 processes and applications that triggered the most alerts (all time).

Top 10 Processes with Most Alerts			
Process Name	Company Name	Number Of Alerts	
Explorer.EXE	Trademark	33575	
RdrServicesUpdater.exe	Trademark	18386	
taskeng.exe	Shimco North America	16468	
Explorer.EXE	Trademark	14889	
explorer.exe	Trademark	11308	
CpmService.exe	Trademark	10373	
chrome.exe	Trademark	9136	
RdrServicesUpdater.exe	Shimco North America	8339	
WmiPrvSE.exe	Shimco North America	8031	
CpmService.exe	Shimco North America	6868	

Most Found Malware - The most prevalent malware on your protected endpoints (all time).

- SHA1 = hash of the malware.
- Hash prevalence = how many instances of the hash were found on endpoints which belong to the company

COMODO Creating Trust Online

#### shown in the middle column.

2606176752009510917		
2100170703000310017	Trademark	2
3B420466FC91CC29A6C	Trademark	1

**Total Number of Malware Detections:**(Last 90 Days) - Quantity of malware found on your protected endpoints in the previous 90 days. Malware is broken down by company affected:



#### **Attack Vectors -**

Shows the methods by which threats were launched on your companies. Each bar shows the % of each type in relation to all threats.

Y axis - Company affected by the threat

- X axis Percentage of total threats
- Legend Method used to deliver the threat. Examples include 'Email', 'Browser' and 'Shared Folder'.



### 5 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 interface
  - · Install the agent on every target machine
  - Click here to view a tutorial on this process
- 2. Use Group Policy Management (GPO). See https://help.comodo.com/topic-444-1-910-11939-Introduction-to-Agent-Deployment-via-GPO.html for help with this
- 3. Use script execution via Endpoint Manager. You can also deploy the .msi agent by executing scripts via procedures in Endpoint Manager. The script can be accessed from the link below: https://scripts.comodo.com/frontend/web/topic/enroll-comodo-edr-agent

		PPLICATIONS - <b>°O</b> MANAGEMENT - E	🖥 REPORTS 🍃 STORE 🚔 TOOLS		Steamer E 🛛 - 🞯 - 😫 🕲 -
Endpoint Manager		Procedures		License Options	Logout (herculespopular22@gmail.com)
Endpoint Manager  Austication  Configuration templates  Profiles  Profiles  Austications  Applications  Applications  Security sub-systems  Security sub-s	· · · · · · · · · · · · · · · · · · ·			License Options C	Logout (herculespopular22@gmail.com)   CREATED ON LAST MODIFIED BY   UPDATED ON   2018/09/22   2018/09/22   2018/09/22   2018/09/22   2018/09/22
			Uninstall ESET End. Productived Approved E     Deckup and restore. Predefined Approved E     Latential and initiat Predefined Approved E	Seript Seript Seript	2018/59/22. 2018/59/22. 2018/59/22.

- To run the script, create a custom procedure. Login to your Comodo One / Comodo Dragon / ITarian
   account
- Click 'Applications' > 'Endpoint Manager'
- Click 'Configuration Templates' > 'Procedures'

 To create script to install .msi package on multiple endpoints, see 'Create a custom Procedure' in the 'Endpoint Manager – Administrator Guide' guide for help.

#### Add endpoints individually

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

♣ : 🖓 📴 ᆕ	Application Tools Downloads	-	
File Home Sh	are View Manage		~ 😲
← → → ↑ 🕹 >	This PC → Downloads $\checkmark$ 한	Search Downloads	م
Ouick access	^ Name	Date modified	Туре
Deckton d	Scomodo_EDR_Agent_Installer_1.1.258.3_Bk3uAu5kQ	5/29/2018 12:47 PM	Application
	ComodoRemoteControl	5/23/2018 1:48 PM	Application
🕂 Downloads 🚿	Sirefox Installer (1)	5/30/2018 2:53 PM	Application
Shared Space 🖈	Sirefox Installer	5/29/2018 2:10 PM	Application
🔮 Documents 🖈	😽 itsm_E1bYJR4J_installer	5/22/2018 5:20 PM	Windows Installer
📰 Pictures 🛛 🖈	🙀 itsm_zZTWucmT_installer	5/23/2018 11:08 AM	Windows Installer
h Music	nevosetup	5/22/2018 12:44 PM	Application
Videos	Ng wordweb8	5/29/2018 1:08 PM	Application
ineDrive 🍊 🍊			
🛄 This PC	v <		>
8 items 1 item select	ed 5.38 MB		

Open the setup file to start the installer



• The default installation location is C:\Program Files (x86)\COMODO\cWatchEDRAgent\. Click 'Browse...' to

COMODO Creating Trust Online

choose a different installation location.

Click 'Next' to continue the installation



You must restart the endpoint to complete the installation:



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

That's it. The endpoint now is enrolled to EDR and can be monitored.

## 6 View Enrolled Endpoints

- · Click 'Endpoints' on the left to view and manage all endpoints you have added to EDR
- Details include the endpoint name, connection status, IP address, operating system, alerts and more.

EDR	-					Upgrade	Now Welcome,	ednjicamoda.com 🛛 🛤	Logar
	Endpoints								
250 Dashboard	Search with endpoint versi	on, local tp address, comp	suter name, logged on user ar	id connection status					9
Alerts	Endpoint Search Result								
Policy Management	# Endpoint Version	Local IP Address	Computer Name	Operating System	Logged On User	Connection Status	Detection	Last Update Time 🗸	
Detection	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	
$\sim$	2 1.1.260.2	10.104.69.60	USNJCS7	Windows 10 or Later 64 bit platform	azerm	Online	No	2018-11-13 18:15:47	
🖵 Endpoints	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-SHOSLIRR15BG	Windows II or Later 64 bit platform		Disconnected	No	2010-11-12 16:49:50	
Q Investigation	5 1.1.260.2	10.100.182.117	AND0414	Windows 10 or Later 64 bit platform		Disconnected	No	2018-11-13 13:57:36	
> Event Search	6 11,260.2	10.108.51,209	DESKTOP-TTPO9PR	Windows 10 or Later 64 bit platform		Disconnected	No	2018-11-13 11:23:02	
a Computer Search	7 1.1.260.2	192.168.1.159	OZER PC	Windows 8 or Later 64 bit platform	Mehmet@zer	Disconnected	No	2018-11-12 06:29:41	
	8 1.1.259.0	192,168,38,130	DESKTOP-AU048VH	Windows 10 or Later 64 bit platform	CMD-CHINAGA	Disconnected	Support	2018-10-24 01:14:54	
Hash Search	9 1.1.259.D	172.18.223.65	ANMD406	Windows 10 or Later 64 bit platform	konwyy	Office	No	2018-08-16 16:40:13	
Download Agent	10 1.1.253.3	127.0.0.1	ANM123	Windows 7 64 bit platform	yash	Disconnected	No	2018-02-13 21:59:17	
warminana riguna	11 1.1.253.2	192.168.1.242	WIN-J7BDRE7034U	Windows 10 or Later 64 bit platform	SYSTEM	Disconnected	No	2018-02-08 08:25:43	
	12 1.1.253.3	10.100.129.141	EDRWING132	Windows B or Later	ndr	Office	No	2010-01-19 10:53:30	
	13 1.1.253.8	10.100.136.238	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	10.100.186.226	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 18:53:55	
	17 1.1.105.0	192.168.1.151	ANM0091	Windows 7 64 bit platform	SYSTEM	Disconnected	No	2017-09-18 05:10:00	

Endpoints - Table of Column Descriptions			
Column Header	Description		
Endpoint Version	The version number of the EDR agent.		
Local IP Address	The internal IP address of the endpoint		
Computer Name	The endpoint label. Click this name to view events on the endpoint. See 'Computer Search' for more information.		
Operating System	The endpoint's OS		
Logged On User	The user currently using the machine		
Connection Status	Whether or not the endpoint is connected to EDR		
Detection	<ul><li>Whether or not there have been malicious events on the endpoint.</li><li>A yellow bar indicates a malware event.</li></ul>		
	Click 'Suspend Alarm' to remove the alert. You may want to do this if the event has been dealt with and no longer poses a concern.		
Last Update Time	The most recent update sent from the endpoint agent to the EDR console.		

- Use the search box above the table to find specific items. You can filter by agent version, local IP, active user, computer name and connection status
- Clear the data to view the full list again.



### 7 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 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:

EDR EVatch	=	Upgrade Now	Welcome, edrc1@yopmail.com	00	Log out
B Dashboard	Policy List				
Alerts	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 acces scale is 0-10.				
Policy Management	Events with scores 6-10 are High Risk Events.				
Detection	✓ Comodo Recommended Security Policy				
Endpoints					
Q investigation					
» Event Search					
» Computer Search					
» Hash Search					
🛓 Cownicad Agent					
	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.
- From this interface you can:
  - Create a new policy
  - View and edit the default Comodo security policy
  - Activate a policy
  - Delete a policy

#### Create a new policy

- Click 'Policy Management' on the left
- Click 'Create Policy':

**EDR** Upgrade Now Welcome, edrc1@yopmail.com E Log out Policy List Dashboard 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 ۸ Alerts Event score scale is 0-10. Events with score 0-5 are Low Risk Events. Events with scores 6-10 are High Risk Events Policy Mana Detection Comodo Recommended Security Policy Endpoints Q Investigation » Event Search » Computer Search » Hash Search 2018 @ EDR by Comodo 📥 Download Agent

#### 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
U	Chennal Site Policy Cancel

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

Ē	✓ Comodo Recommended Security Policy	
U	Chennal Site Policy	Edit Policy
	+ Create Policy	

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

COMODO Creating Trust Online

 $\mathbf{O}$ = D Log out Chennai Site Policy Activite Delete ß Company Rules Endpoint Rules 4 OB Process Events Add New Registry Events Add New Create Process Set Registry Value E Suspicious System Process Creat Disable User Account Co ØG ØÐ WHEN pros. verdict not, equal Safe V HEN reg\_key\_path equal HKEY\_LOC reg value name equal EnableLUA V D ote Powershell Execution 5  $\oslash \ominus$ able Task Manager 9 ØΘ EN child, prcs, path matches hws eg, key. path equal HKEY\_CURRENT\_USER\SOFTV \_value\_rame equal DisableTaskd/gr WHEN reg\_va Stop Service 5 ØΘ HEN child\_pros\_cmd\_line matches %s stallation of Drivers 8 00 Q Suspicious Powershell Flag 5 HEN reg.key.path matches HKEY.LOCAL\_MACHINE/SYSTEM/OurrentCont al Type OR/WHEN reg\_value\_data equal 1 OR WHEN reg\_value\_data equal 2 Ø WHEN child, pres, emd, line matches "power hild pres, emd, line matches "powershell"-wi ± Add New File Events Add New (a) Download Events

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' lat the top of an event category:

COMODO Creating Trust Online



#### The 'Add Condition' dialog will open:

,	Add Condition				
8	Event Type				
	– Choose Event Type –	۳			
	- 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	
AND OR Add rule • Add group	
× Delete	
Save Cancel	

- 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	
AND OR	+ Add rule • Add group
L O	× Delete
Process Path Process Verdict Registry Value Name	Save Cancel
owershe Registry Value Data Registry Key Path	d_line matches *powershell*-NonInteractive* WHEN chil Add Active Setup Value In Registry 7

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
AND OR Add group
Registry Key Path   equal  HKEY_LOCAL_MACHINE  Content of the second sec
Save Cancel

- 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			
AND OR			+ Add rule O Add group
- Registry Key Path 🔹	equal	HKEY_LOCAL_MACHINE	X Delete
Registry Value Name 🔻	equal	• EnableLUA	× Delete
Registry Value Data 🔻	equal	• 0	× Delete
			Save Cancel

• 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	
AND OR	+ Add rule • Add group
Registry Key Path   matches  HKEY_LOCAL_MACHINE	X Delete
Registry Value Name 🔻 equal 🔻 Type	X Delete
AND OR	+ Add rule Add group X Delete
Registry Value Data 🔻 equal 💌 1	🗙 Delete
Registry Value Data 🔻 equal 🔻 2	× Delete
	Save Cancel

- 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.
- To remove a rule, click the delete icon beside it.



Click 'Yes, delete it!' to confirm removal.

#### **Endpoint Rules**

Click 'Policy Management' on the left then the 'Endpoint Rules' tab

	<b>EDR</b>	=	Upgrade Now	Welcome, Demo Premium	0+ Log out
ß	Dashboard	Comodo Recommended Security Policy Active Policy	_		unu nev
	Alerts	Company Rule Endpoint Rules Choose Endpoint:	o	5	10 10
e	Policy Management	- Choose Endpoint			•
U	Detection				
-	Endpoints				

Select the endpoint from the drop-down

•

C = Welcome, Demo Premium B Log out Comodo Recommended Security Policy 6 Company Rules Endpoint Rules Choose Endpoint: 4 DESKTOP-HI950BN - Administrator -- Choose Endpoint --ANM0261 - butch DESKTOP-7J8UVDU - ops ₿ edrwin732 -- vincent Create Process U Suspicious System Process Creation 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.



- · 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'

COMODO Creating Trust Online

olicy
olicy
Θ

- 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.
- To remove a rule, click the delete icon beside it.



Click 'Yes, delete it!' to confirm removal.

#### View and edit the default Comodo security policy

- Comodo EDR ships with a default security policy that is automatically applied to enrolled endpoints.
- · Click 'Policy Management' on the left, then 'Comodo Recommended Security Policy'

EDR	≡	Upgrade Now	Welcome, Demo Premium	0+ Log out
B Daribbarri	Policy List			
Alerts	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.			
Policy Management	Events with scores 6-10 are High Risk Events.			
Detection	Comodo Recommended Security Policy			Edit Policy
Endpoints	Test Techwriting			
Q Investigation	+ Create Policy			
» Event Search				
» Computer Search				

The policy interface is similar to the 'Create a new policy' interface. See 'Company Rules' and 'Endpoint Rules' under 'Create a new policy' section.

#### Activate a policy

- You can add as many security policies as required but any one only can be active at a time.
- The active policy has a green check mark next to it.
- Click 'Policy Management' on the left then the security policy that you want to active.

EDR	≡	Upgrade Now	Welcome, Demo Premium	🕪 Log out
R Dashboard	Policy List			
Alerts	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.			
Policy Management	Events with scores 6-10 are High Risk Events.			
Detection	✓ Comodo Recommended Security Policy			
Endpoints	Test Techwriting			Edit Policy
Q Investigation	+ Create Policy			
» Event Search				
Computer Search				
» Hash Search				
a Downoad Agent				

Click 'Activate' at the top

Company Rules
 Company Rules
 Company Rules
 Endpoint Rules
 Policy Management
 Detection

Click 'Yes, activate' to confirm



The policy will be activated and its rules will be applied to the enrolled endpoints.

#### **Delete a policy**

- You cannot delete an active policy
- · Click 'Policy Management' on the left then the security policy that you want to delete

COMODO Creating Trust Online

**EDR** = Upgrade Now Welcome, Demo Premium 6 Log out Policy List 🚯 Dashboard 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. Alerts Events with score 0-5 are Low Risk Events. Events with scores 6-10 are High Risk Events. Policy Management Detection Comodo Recommended Security Policy Endpoints Ċ Q Investigation + Create Policy » Event Search

• Click 'Delete' at the top

<b>EDR</b>	≡
🚯 Dashboard	Test Techwriting Activate Delete
Alerts	Company Rules Endpoint Rules
Policy Management	Process Events
Detection	Create Process

Click 'Yes, delete it!' to confirm

COMODO Creating Trust Online



A confirmation dialog will be shown:



Click 'OK' to close the dialog.



### 8 View Event Details on Endpoints

The 'Detection' screen provides an 'at-a-glance' summary of malicious events on your endpoints. The table shows detailed information about each malware incident.

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

EDR	Ξ		Upgrade Now	Welcome, Demo Pro	emium 😁 Logiout
🚳 Deshboard	Detection Search with user, computer or hash			∰ 2018-05-03 - 2	1018-06-01 ¥ Q
<ul> <li>Alerts</li> <li>Policy Management</li> </ul>	Detection Search Results [ Time : 2018-05-03 16:47:45:442 - 2018-06-01 16:47:45:442 ]				
Detection	# Computer Name         User         Sha1           1         DESKTOP-7J8UVDU         user3         27D99FBCA067F478BB91CDBcB92F13A828B00859	Count 1	First Event - 2018-05-24 22:28:58	Last Event 2018-05-24 22:28:58	Valkyrie Report See Report
Endpoints     Investigation	2         DESKTOP-7,80/VDU         user3         82338F6661390ED8959255A8A47788E76F1002BC           3         ANM0261         user2         27D99FBCA067F478BB01CDBC802F13A826B00859           4         ANM0261         user2         27D99FBCA067F478BB01CDBC802F13A826B00859	1	2018-05-24 22:28:58 2018-05-24 22:28:58	2018-05-24 22:28:58 2018-05-24 22:28:58	See Report
<ul> <li>Event Search</li> <li>Computer Search</li> </ul>	4         Hermitizer         Lose 2         623307060133062095234064475062741002205           5         edrwin732         User         27099FBCA067F4788891C0BC892F13A828800859           6         edrwin732         user         82338F65613906D8959255A8A47788E76F10028C	1	2018-05-24 22:28:58 2018-05-24 22:28:58	2018-05-24 22:28:58 2018-05-24 22:28:58	See Report
<ul> <li>Hash Search</li> </ul>	Total Court : 6, Page 1 of 1				
🏝 Download Agent					

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 full details of the file analysis. See <a href="https://help.comodo.com/topic-397-1-773-9563-Introduction-to-Comodo-Valkyrie.html">https://help.comodo.com/topic-397-1-773-9563-Introduction-to-Comodo-Valkyrie.html</a> for more information about Valkyrie.				

#### Search and Sorting options

•

- Search option The 'Search' boxes above the table allow you to 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.
- Sorting option 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.

1018-05-03 - 2018-06-01 ملله الم Q Last 15 Minutes 2018-05-02 16:47:45 2018-06-01 16:47:45 Last 30 Minutes \* : 47 \* PM \* • : 47 • PM • G Last 60 Minutes < May 2018 Jun 2018 Last 12 Hours Su Mo Tu We Th Fr Sa Su Mo Tu We Th Fr Sa Last 1 Day Last 3 Days б Last 7 Days  $\frac{21}{21}$ Last 15 Days Last 30 Days Last 45 Days Last 60 Days Last 90 Days Last 1 Year Custom range Apply Cancel

- Click 'Custom range' to choose specific dates:
- · Click 'Apply'. The results for the selected period will be displayed.

COMODO Creating Trust Online

### 9 Alerts

Alerts are generated 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

0	=				<u>.</u>				Upgra	de Nov
	Alerts									
M	Alert Search	Po	licies	Device	St	atue	Soore			
m			- Select Policy -	- Select Device	e- ~	- Select Status - 🗸	8	15 Ap	ply Cl	ear
-	Alert Lis	ıt								
	Score	Alert Name	Alert Time	Process Name		Device	Policy	User Verdict	Alert	
-	Q 🚺	Run Untrusted Executable	2018-11-13 13:44:36	C:\WINDOWS\Explorer.EXE		DESKTOP- TTPO9PR	Comodo Recommended Security Policy	N/A	New	0
Ē	Q 5	Write to Executable	e 2018-11-13 13:33:26	C:\WINDOWS\Explorer.EXE		DESKTOP- TTPO9PR	Comodo Recommended Security Policy	N/A	New	0
	Q 4	Run Untrusted Executable	2018-11-13 13:27:56	C:\WINDOWS\Explorer.EXE		DESKTOP- TTPO9PR	Comodo Recommended Security Policy	N/A	New	0
U	Q, 🚺	Run Untrusted Executable	2018-11-13 13:18:08	C:\WINDOWS\Explorer EXE		DESKTOP- TTPO9PR	Comodo Recommended Security Policy	N/A	New	0
Ţ	Q 10	Write to Infectible File	2018-11-13 13:18:08	C:\WINDOWS\Explore: EXE		DESKTOP- TTPO9PR	Comodo Recommended Security Policy	N/A	New	0
0	@ 10	Write to Infectible File	2018-11-13 13:15:03	C:\WINDOWS\Explore: EXE		DESKTOP- TTPO9PR	Comodo Recommended Security Policy	N/A	New	0
ų	Q. 5	Write to Infectible File	2018-11-13 12:32:00	C:\WINDOWS\Explorer.EXE		DESKTOP- TTPO9PR	Comodo Recommended Security Policy	N/A	New	0
*	۹ 🔺	Run Untrusted Executable	2018-11-13 12:18:12	C:\Users\Vega\AppData\Local\Terr	np\JNIS2ECD.tm	p DESKTOP- TTPO9PR	Comodo Recommended Security Policy	N/A	New	0
	۹ 🖪	Run Untrusted Executable	2018-11-13 12:12:13	C:\WINDOWS\Explorer.EXE		DESKTOP- TTPO9PR	Comodo Recommended Security Policy	N/A	New	0
	Q 5	Write to Executable	e 2018-11-13 12:12:10	C:\Usera\Vega\AppData\Local\Tem p\AWFT\aetup.exe	np\Temp1_AWF	T.zi DESKTOP- TTPO9PR	Comodo Recommended Security Policy	N/A	New	0
	Q 10	Write to Infectible File	2018-11-13 12:08:49	C:\WINDOWS\Explorer.EXE		DESKTOP- TTPO9PR	Comodo Recommended Security Policy	N/A	New	C
	Q 5	Write to Executable	e 2018-11-13 12:08:49	C:\WINDOWS\Explores EXE		DESKTOP- TTPO9PR	Comodo Recommended Security Policy	N/A.	New	0
	0.00									

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!		Upgrade No	
			1	
	licer Verdice	Alart Statur		
Security Policy	N/A	In Progress	0	
d Security Policy	True Positive	Resolved	co	
d Security Policy	N/A	New	Ó	
d Security Policy	N/A	In Progress	0	
d Security Policy	N/A	New	0	
	N/A	New	0	

The alert status will change to 'In progress'

Click the progress icon to submit the verdict


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

					Upgrade Now
					1
Apply Cle	Nar				
	Device	Policy	User Verdict	Alert Status	
	DESKTOP-TTPO9PR	Comodo Recommended Security Policy	N/A	In Progress	0
			True Positive	Resolved	CO
	/	$\frown$	N/A	New	0
	(	i)	UA.	New	0
			N/A	New	0
		Г	N/A	New	0
	Are y	ou sure?	N/A	New	0
Th	is alert will be opened	again. Reopening an alert will	N/A	New	0
	delete it	s user verdict.	N/A	New	0
			N/A	New	0
	Yes, reopen	it! Cancel	N/A	New	0

- · 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:

сомодо

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

0	=											Epgrade Now
	Explorer.E	XE - Write to	Infectible File o									
Μ	Alert Tarse: 201 Sole Use	eri-sitisti mane inge	Policy: Canada Recommended Security Policy User Weeklet: 1971	Computer Name: DOX:109-1190	Pit Opera	ling Bysteen: Windows 18 or Later 16 bit platfor	n 13	en lines. 2010-11-14 16 17 AB	that announcements	winencount?	Pade C INNOVIDALANNESS	wedat:
8	Events										Lim	Tree View
		Show	Adaptive Even	Name				Evant Type			Scare	
	+	*	Write to briech	ble File				Witte File			1	
		100	Write in Expense	aabiw				Weie File			10	
臣												
	.File Troje	clary										Reset Zoom
U			13 Nevember 2018								54	November 2018
				1	28	WHITE	4	-	10		1	
-		SESCOP TROOPS										
Q			(8) Deswaar Deveningel (8) Cept Promit	Chanad Paider (E): Copy To Share	éToléar 19	Erral Develoari 🛛 🔞 Copy Prem US	5 Olak	Copy To USE Disk B	Write File			
			Present Departure	ther) Demodian								
*												

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

pRt4jHhH.exe - Suspic	cious 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 l	ater 64 bit platform
Last Seen: 2018-05-24 22:28:59	Sha1: 27d99fbca067f478bb91cdbcb92f13a828b00859	Path: C:\Users\user3\Downloads\pR	4jHhH.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:

Event	s			List View	Tree View
*	Show	Adaptive Event Name	Event Type	Score	
+	11	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 Na	<i>ae</i>		Event Type		Score		
-	11	Write to infectible	File		Write File				
File Path File Heat		Children Magel AppCland Rosaning Microsoft Windows Reven. 21 ad Januar Noedd Church 21 Sold CN 1788 Net	Formi Tigge Adaptive Swent Harne Logged On User Derive Hanne Event Time Event Group	Minine File Minine to Infectibile File Vega Distantical-YTHICHAR 2010-11-12 12:12:52 FILE	Process PID Process User Domain Process Path Process Dath Process Hash Process Creation Time	SANA DESKTOR-TTPOPPR Christionen SUS Tinger 4004/2014/06/2015/07/06/2015/94/54/2017 2014/15/13/11/48/20			
+	11	Write to Executable	e		Write File		8		

#### Tree View

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



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

meline Tree View									Reset
	13 November 2018	12.50	12.58	0		01.05	DI:10	ours	01,20
winlogan.exe ↓ userinit.exe ↓ Explorer.EXE (14)								•	
-							Process Stebucit	Registry File	Defenseplus Inow
	File Path File Heath	C1Users/Wegal/AppData/Roaming/Mit	2000*/Win_ 6774819cb	Event Type Adaptive Event Norse Logged On Uper Device Name Event Time	Write File Write to Infectible File Vega DESKTOP-TTPOSPR 2016-11-13 12:12:52 File		Process PID Process User Domain Process User Name Process User Name Process Hash	5464 DEBKTOP-TTPO4PR C*WINDOWS/Explorer 2 Vegs 4094c2058555cc50855 3058-11-15-11-48-26	0/E #7966093842%65434047

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.

e Trajectory							Reset Zoom
	23 May 2018 06:55:02 P	м					23 May 2018 09.
	07 PM	07:15 07:30	07;45 08	PM 66;15	00:00	00:45	09 PM
DESKTOP-7J8UVDU (4)							Ø
edrwin732 (4)	Ð	Ð					Ð
ANM0261 (3)		۵					0
	<ul> <li>Browser Download</li> <li>Copy To USB Disk</li> </ul>	<ul> <li>Copy From Shared Folder</li> <li>Write File</li> </ul>	Copy To Shared Fold	ier 🛛 🖗 Email Downloa	ad 🛛 🗄 Copy From U	ISB Disk	
	Process	s Creation 🛛 🗧 Alert 🔤 De	stection				

- 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	^	Adaptive Event Name
Event Time	t Noo	Logged On User
2018-05-23 18:55:02	35 -In	Device Name
Process Hash		Event Time Event Group
ef45d0c407d2987b2edb3dd76967e1b16bd6c1	c8	
Process Path		
C:\Program Files\Mozilla Firefox\firefox.exe		
Path		
C:\Users\user\Downloads\pRt4jHhH.exe		
URL 🔥		07;30
https://bit.ly/2H9HZJR		
edrwin732 (4)		)
ANM0261 (3)		۵
Browser Download	🔁 Copy I	From Shared Folder
Copy To USB Disk	🕑 Write F	ile

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

#### COMODO Creating Trust Online



#### · Click an icon color code to view trajectory details.

	Modify Firewall Settings	×		
7 PM 07 PM	Alert Time 2018-05-23T14:21:33.094Z Process Path C:\Users\user2\Downloads\pRt4jHhH.exe	30	09 PM 09:	30
<b>(</b>	Bhow detail		• • •	
	• • (The second		Ť	
<ul> <li>Copy From State</li> <li>Write File</li> </ul>	om Shared Folder 🛛 🖻 Copy To Shared Folder	罕 Email Download	Copy From USB Disk	
ess Creation	Alert Detection			

- '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.

# 10 Investigation

The 'Investigation' section allows you to identify analyze events by event type, computer or hash value. For example, you can query events generated by a certain browser on specific devices.

COMODO Creating Trust Online\*

EDR	Ξ	Upgrade Now Welcome, Demo Premium 🕞 Log out
	Computer Search	
Dashboard	DESKTOP-HI950BN	
Alerts	Logged On User: Administrator Endpoint Version: 1.1.250.3 Connection	Status: Online Last Scon : 2018-05-00 17:09:50 Last Reboot : 2018-05-00 20:02:46
Policy Management	Operating System : Windows 10 or Later 64 bit platform	
Detection	Local and External IP Changes	Unique Users Logged on
_	Local IP Local IP	# Username Last Seen
Endpoints	# External IP Local IP 1 2 3 Time	1. SYSTEM 2017-06-23 12:46:20
	1 182.74.23.22 10.0.2.15 0.0.0.0 0.0.0.0 2018-05-29 12:32:16	2 Administrator 2018-05-29 12:49:16
C Investigation	2 52 41 147 167 10 108 51 211 0.0.0.0 0.0.0.0 2017-06-23	3 2018-05-29 12:48:09
» Event Search	12:46:20	Total Count : 1 , Page 1 of 1
» Computer Search » Hash Search	Total Count : 2, Page 1 of 1	
🎄 Download Agent	Network Connections 🖀 Last 15 Days 🗸	Admin Privilege Usage 🗎 Last 3 Days 🗸
	P A Local IP Destination IP Destination Port Count	

- Event Search Search for events according to specific parameters. Parameters include event ID, device name, logged on user and so on. You can use operators to concatenate parameters and build granular queries. See 'Event Search' for details.
- Computer Search Search for events that were recorded on a specific endpoint. The search results
  include items such as network connections, malware detections, event trends and so on. See 'Computer
  Search' for details.
- Hash Search Search for events based on the hash value of the file. The search results include file name and type, point of entry, execution trend, file history and more. See 'Hash Search' for details.
- Process Timeline View a timeline of processes initiated by events. See 'Process Timeline' for details.

### 10.1 Event Search

- 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:

EDR	Ξ	Upgrade Now Welcome, edr@comodo.com Ø 54 Log out
Deshboard	Event Search Save Query Clastified	
<ul> <li>Alerts</li> <li>Policy Management</li> </ul>	Deers Fields Generators Senado Doction Mr Generics Search Results [ Time: 2018-11-16 00:22:36.000 - 2018-11-16 00:22:37.000 ]	₫ 2018-11-16 00:22:36 - 2018-11-16 00:22:37
Detection     Endooints	Device Name Process User Name ANMAD406	Process Path Event TypeExplorer.EXE
Q Investigation		
» Event Search		🔢 Select Fields
» Computer Search	# Show Event Time - Device Name Process User Name Process Path	Process Hash Event Type Adaptive Event Name
> Hash Search	+1  2018-11-16-00-22-37.150 ANM0406 koreyy C:\WINDOWS\Explor 2  2018-11-16-00-22-36.146 ANM0406 koreyy C:\WINDOWS\Explor	er.EXE 408fe28868b5ar008b5df98b9928a2fe654360d7 Write File Write to Infectible File wr.EXE 408fe28868b5ar008b5df98b9928a2fe654380d7 Write File Write to Infectible File
Lownload Agent		

- 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 to the query 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.

	Event Search Interface - Table of controls
Select Fields	Allows you to configure the 'Results' table for the query results displayed at the lower pane.
🏥 Last 3 Days 🛛 🗸	Allows you choose the time period for which events are fetched. Periods range from 15 minutes to 1 month. You can also specify a custom period.
<b>Q</b> Search	Allows you to run a search operation based on the configured / general query.
<u>Query Fields</u>	Allows you to add query fields for a custom query
<u>Operators</u>	Allows you to add conditions for a custom query.
Sample Queries	Built-in sample event queries that are most often used.
Clear Field	Allows you to remove queries entered in the search field
Save Query	Allows you to save a custom query
<u>My Queries</u>	Saved custom queries will be listed here.

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 a 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.

														<u> Last 3 Days</u> ✓	Q Search
2	018-0	5-03 <sup>-</sup>	11:35:	47			2	018-0	6-06	11:35:	47			Last 15 Minutes	
0	11	٣	: 35	٣	AM	٣	0	⊙ 11 ▼: 35 ▼ AM ▼				AM	٣	Last 30 Minutes	
		М	ay 20	18					J	un 20 <sup>-</sup>	18			Last 60 Minutes	
Su	Mo	Tu	We	Th	Fr	Sa	Su	Мо	Tu	We	Th	Fr	Sa	Last 12 Hours	
<del>29</del>	<del>30</del>	1	2	3	4	5	27	28	29	30	31	1	2	Last 1 Day	
6	7	8	9	10	11	12	3	4	5	6	7	8	9	Last 3 Days	
13	14	15	16	17	18	19	<del>10</del>	11	<del>12</del>	<del>13</del>	<del>14</del>	<del>15</del>	<del>16</del>	Last 7 Days	
20	21	22	23	24	25	26	17	<del>18</del>	<del>19</del>	20	21	22	23	Last 15 Days	
27	28	29	30	31	1	2	24	<del>25</del>	<del>26</del>	27	<del>28</del>	<del>29</del>	<del>30</del>	246110 00,0	
3	4	5	6	7	8	9	1	2	3	4	5	6	7	Last 30 Days	
														Custom range	
														Apply Cancel	

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

Even	it Sea	arch								
Enter	your	query here								~
<b>Query F</b>	ields s	oevators <u>Samp</u>	e Querles My	Ø <u>veries</u>				🗮 Last 15 Days	~	Q Search
Searc	h Res	ults [ Time : 20	18-05-22 12:18:1	19.347 - 2018-06-1	6 12:18:19:347					
Dev	ice Nar				Process User Name	Priscess Path		Event Type		
DES	DESKTOP-HI950BN			(1178)	SYSTEM	svchost.exe		Create Process		
edn	win732			•	Administrator 290	Bearchindexet.exe	205	Write File		
DES	RETOR-1	JBUVDU				. firefox.exe	[14]	Network Connection		
AN	M0261				user	NGenTask.exe	121	Set Registry Value		
					Ciecu Ciecu			Browser Download		•••••
										III Select Fields
,	Sho	w Event Time	Device Name	Process User Name	Process Path		Process Hash		Event Type	Adaptive Event Name
+1	~	2018-05-30 17:05:39.39	DESKTOP-	Administrator	C:\Users\Administrator\Downloads\Comodo_EDR_Age	ent_Installer_1.1.258.3_Bk3uAu5kQ.exe	f49d31c432224f67	23f56d7a28cd2203bda23e58	Write File	Write to Executable
+2	2	2018-05-30 17:05:28.48	DESKTOP- HI950BN	Administrator	C:\Users\Administrator\Downloads\Comodo_EDR_Age	ent_Installer_11.258.3_8k3uAu5kQ.exe	149d31c432224/67	23f56d7a28cd2203bda23e58	Write File	Write to Executable
+3	"	2018-05-30 17:05:27:28	DESKTOP- HI950BN	Administrator	C:\Users\Administrator\Downloads\Comodo_EDR_Age	ent_Installer_1.1.258.3_Bk3uAu5kQ.exe	f49d31c432224f67	23156d7a28cd2203bda23e58	Write 2114	Write to Encounted by

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. Custom queries can be configured in two ways:

Configure a custom event query manually

COMODO Creating Trust Online

#### Using the search results

#### To configure a custom event query

· Click 'Query Fields' below the search box and select an event from the list.

Event Search	
Enter your query here	
<u>Query Fields</u> <u>Operators</u> <u>Sample Queries</u> <u>My Queries</u>	
Adaptive Event Name adaptive_event_name	18-06-06
Command Line child_prcs_cmd_line	
Destination IP ntw_dst_ip	P
Destination Port ntw_dst_port	
Device Name prcs_device_name	5
Downloaded File Hash brws_file_hash	<b>)</b>
Downloaded File Path brws_file_path	
Elevation Type child_prcs_elevation_type	
Event Group event_group	s User
Event Identifier id	
Event Time event_time	strator ▼
+2 → 2018-05-30 DESKTOP- Adn	ninistrator

- 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.

COMODO Creating Trust Online

ery Fields (	<u>Operators</u> <u>Sample Queries</u>	<u>My Queries</u>
earch Res	EQUALS =	<b>18:19.347</b> - 2
	NOT_EQUAL !=	
Device Na	GREATER >	
DESKTOP- edrwin732	GREATER_EQUAL >=	
DESKTOP-	SMALLER <	
ANM0261	SMALLER_EQUAL <=	
	CONTAINS ~	

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':

Event Search Save Query Clear Field adaptive event name = Run Untrusted Executable AND prcs device name = DESKTOP-738UVDU Query Fields Operators Sample Queries My Queries

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

The search results for the custom query will be displayed:

.

Eve	nt	Sea	rch Save Query	Clear Field							
ada	riv	/e_evi	ent_name = Run Un	trusted Executabl	e AND prcs_device_n	ame = DESKTOP-738UVDU					~
<i>9</i> 10079	Fiel	ds _0)	verators Sample Over	ies My.Ounties						🛄 Levi 15 D	nyv 👻 Q. Search
Seal	ch	Resu	<b>ilts</b> [Time: 2018-05-2	2 12:18:19.347 - 2018	06-06 12:18:19.347 ]						
D	evice	e Name	e		Process User Name		Process Path		Event Ty	pe	
D	ESKI	FOP-7.			user3		pRt4jHhH.ex		Create P	DCR35	
							explorer.exe	•			6
					Process User						Select Fields
	\$	show	Event Time 🗸	Device Name	Name	Process Path		Process Hash		Event Type	Adaptive Event Name
+	1	~	2018-05-23 21:26:26.524	DESKTOP- 7J8UVDU	user3	C:\Users\user3\Download:	\pRt4JHhH.exe	27d99fbca067f478bb91cdbcb92f13a	828600859	Create Process	Run Untrusted Executable
+	2	P	2018-05-23 21:03:46.501	DESKTOP- 7J8UVDU	user3	C:\Windows\explorer.exe		f7152a8cb963cefdfa65d35a3565c35	490223a26	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.

• Click 'Save Query' for future use. The saved query will be listed under 'My Queries'.

#### To configure a custom query using the search results

In addition to manually providing the event field details for creating a custom query, you can also query for a particular event from the search results.

The following example shows the general search results for a selected time-period.

Searc	h Box								
Ente	r your	query here							
Query	Fields (	Operators Sample Que	volens.			Select Fields	2017-06-04 14:54-00:000 - 2017	05-30 14:59:0	0.000 👻 Q Sewich
Sear	ch Resu	ilts [ Time: 2017-06-04	14:34:00.000 - 20	17-08-30 14-59:00.000 ]					
Devic	e Name		Current Pro	cess User Name	Current Process Path	Current Process Image Hash	Current Process Verdict		Event Type
DESK	TOP-HI93	0BN (1503	Administrate	ar (15065)	C.\\Windows\\System3 4327	a2d14508b3edddr80d (4327)	Safe	10009	Create Registry Key
DESK	TOP-TTP	09PR	NETWORK S	ERVICE	C:\\Program Files (x86) 4203	c1939e8c702979c330e 4203	Unknown ·····		Network Connection
			SYSTEM ····	2262	C:WUsersWAdministrat	2f0b217263bcd4d7d89	Malware ·····		Orop File
					C:\\Users\\Administrat	df3328f9944867c3c5e			Exit Process
			LOCAL SERV	ICE	F/\All tests\//Ghost\/Gh	3437369w6b75021f57d			Write Portable Execute
Even	t List								
,	Show	Event Time 🗸	Device Name	Current Process User Name	Current Process Path	Current Process Ima	ge Hash	Current Process Verdict	Event Type
+1	[معر]	2017-06-30 14:58:32.851	DESKTOP- HI9500N	Administrator	C:\\Program Files (x86)\\Google\\Chrome\\Application\\ch	c1939e8c702979c330 rome.exe	ie0c5734b7952c9676b45a6	Safe	Network Connection
+2	an'	2017-06-30 14:58:31.850	DE5KTOP- HI950BN	Administrator	C:\\Program Files (x86)\\Google\\Chrome\\Application\\ch	c1939e8c702979c33i rome.exe	se0c5734b7952c9676b45a6	Safe	Network Connection
+3									

#### **Summary Results section**

The results summary section at the top shows results for all endpoints and events. You can select particular fields to build a custom query from the results.

Search Box											
Enter your query here											
Query Fields Operators Sample Queries			III Select Fields	2017-06-04 14:34:00.000 - 2017-06-30 14:59:0	0.000 👻 Q. Search						
Search Results [ fime : 2017-06-04 14	34:00.000 - 2017-06-30 14:59:00.000 ]										
Device Name	Current Process User Name	Current Process Path	Current Process Image Hash	Current Process Verdict	Event Type						
DE5KTOP-HI950BN 15935	Administrator	C:\\Windows\\\System3	a2d14508b3edddf86d (4327)	Safe	Create Registry Key						
DESKTOP-TTPO9PR . 4985	NETWORK SERVICE 2702	C://Program Files (xB6) 4355	c1930eBc702979c336e 4203	Unknown 5258	Network Connection						
	SYSTEM	C/\Users\\Administrat	2f0b217263bcd4d7d89 2168	Malware 5123	Drop File · · · · · · · ·						
		C:\\Users\\Administrat	df3328f9044867c3c5e 1934		Exit Process						
	LOCAL SERVICE 340	F/WAII tests/WGhost/VGh 978	3437369e6b75021f57d (1042)		Write Portable Executa.						
Event List											
	Current Process User			Current Process							

The result columns depend on the **selected event fields**. For example if you want to search for run untrusted executable events for an endpoint:

- First, click the endpoint under 'Device Name'. The query will be automatically entered in the 'Search Box' and EDR will provide all results for the endpoint.
- Click 'Run Untrusted Executable' under 'Adaptive Event Name'. The query will be automatically updated in the 'Search Box' and the results for the untrusted executable events on the endpoint will be displayed:

COMODO Creating Trust Online\*

Event Search save Query Clear Field				
prcs_device_name = DESKTOP-738UVDU AND adapt	<pre>ive_event_name = Run</pre>	Untrusted Executable		~
Query Fields Operators Simple Queries My Queries		The second secon	🏥 Last 30 Days	V Q Search
Search Results [ 7me : 2018-05-07 12:18:19.347 - 2010	3-06-06 12:18:19.347 ]			
Device Name		ProcessUser Name	Proces	s Path
DESKTOP-7JØUVDU	•••••••••••••••••••••••••••••••••••••••	user3		Hhillexe
3		Adaptive EventName		0
Create Process		Run Untrusted Executable		
				III Select Fields
n - Store Kern finter - Device Name	Process User Name	Process Path Process Hash	Event Type Ada	ptive Event Name

#### **Event List section**

The details shown in the summary results depend on the **selected event fields**. You can, of course, also choose fields from the 'Event List' section.

Click the number beside a event list row from which you want to build a custom query

#	Show	Event Time 🗸	Device Name	Process User Name	Process Path	Process Hash	Event Type	Adaptive Event Name
+1	~	2018-05-23 20:24:23.296	edrwin732	user	chrome.exe	87a567f54537e5d2335fc226f44e4fb35067ed0	3 Browser Download	T
+2	*	2018-05-23 20:04:07.138	edrwin732	user	firefox.exe	ef45d0c407d2987b2edb3dd76967e1b16bd6c1	c8 Browser Download	-
(-3 1-3	~	2018-05-23 18:55:02.370	edrwin732	user	firefox.exe	ef45d0c407d2987b2edb3dd76967e1b16bd6c1	c8 Browser Download	Download Executable
0	JRL Downloade Downloade	https://bit.lg/2H9HZJR c.:USersiuseri/Downloads/g 27d99fbce067f478bb91cdb	Ever PR16] Ada Icb92 Logi Devi Ever Ever	nt Type Brown ptive Event Name Down ged On User user ce Name edrw nt Time 2018 nt Group BROY	ter Download nload Executable 1n732 +05-23 18:55:02 ASER	Process PID I Process User Domain Process Path C Process User Name Process User Name Process User Name Process Creation Time 2	756 drwin732 :\Program Files\Mozilla Firefox 8er f45d0c407d296752edb3dd769 018-05-23 19-01-11	∿∫meTox.exe 167e1b16bd6c1c8

• Click the event field(s) details that you want to use to build a custom query.

#	Show	Event Time 🗸	Device Name	Process User Name	Process Path	Process Hash	Event Type	Adaptive Event Name
+1	~	2018-05-23 20:24:23.296	edrwin732	user	chrome.exe	87a567f54537e5d2335fc226f44e4fb35067ed03	Browser Download	-
+2	*	2018-05-23 20:04:07.138	edrwin732	user	firefox.exe	ef45d0c407d2987b2edb3dd76967e1b16bd6c1c	8 Browser Download	-
- 3	~	2018-05-23 18:55:02.370	edrwin732	user	firefox.exe	ef45d0c407d2987b2edb3dd76967e1b16bd6c1c	8 Browser Download	Download Executable
	URL Downloade Downloade	https://bit.ly/2H9H2JR C.Wsers!wser!/Downloads/g 27d99fbca067f478bb91cdb	Even Rt/lj Adaj cb92 Logo Devi Even Even	n Type Brow stive Event Name Dow red On User user oe Name ednv n Time 2016 n Group BRO	vser Download nload Executable vin732 9-05-23 18:55:02 WSER	Process PID 87 Process Discr Domain ed Process Path C: ef45d0c407d2987b2edb3dd76967 49 e115d6d6c1c8 20 Add To Query 20	56 win732 Program Files\Mozilla Firefos er 45d0c407d2987b2edb3dg76 18-05-23 19:01:11	Afrefox.exe 967e1b16bd6c1c8

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



Event Search save query clear Field								
event_type = Browser Download AND prcs_hash = ef45d8c487d2987b2edb3dd76967e1b16bd6c1c8			~					
Query.Eields Operators Sample.Queries My.Queries	🏥 Last 30 Days	~	<b>Q</b> Search					

Select the time-period and click 'Search'

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

#### **Run Sample Queries**

.

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

E	vent Search											
[	Enter your query here											
Q	uery Fields <u>Operators</u>	Sample Queries My Queries										
S	earch Results [ Time	List Process Events Shows all process events	7]									
	-	List Network Events Shows all network events										
	Device Name	List Registry Events Shows all registry events	Name									
	edrwin732 ·····	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 Search save Query Clear Field	
<pre>event_group = REGISTRY</pre>	
Query Fields Operators Sample Queries My Queries	

· 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. Administrators 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. See 'Configure results table column headers for a query', 'Run a general event search', 'Configure and run a custom query search' and 'Use sample queries' for more details.

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

E	vent	Sear	ch								
E	nter	your q	uery here								~
Qu	ary:Eia	ta Qa	calaca Sacople.	Queries My C	Sweeting				🛄 Last 30 Days	*	Q Search
Se	arch	Resul	<b>ts</b> [ Time : 2018	-05-07 12:18:1	9.347 - 2018-06-0	6 12:18:19.347 ]					
	Devio	e Name				Process User Name	Process Path		Event Type		
	DESK	TOP-HIS	508N		1178	SYSTEM	svchost.exe	341	Create Process		947
	edrwi	n732 ···				Administrator	Searchindexer.exe	205	Write File		240
	DESK	T0P-7J8	SUVDU		(2)		firefox.exe		Network Connection		
	ANM	0261				Liser	NGenTask.exe		Set Registry Velue		
						user3 🔤	services.exe		Browser Download		
											Select Fields
											Adaptive
		Show	Event Time 🗸	Device Name	Process User Name	Process Path		Process Hash		Event Type	Event Name
	+1	"	2018-05-30 17:05:39.395	DESKTOP- HI9508N	Administrator	C:\Users\Administrator\Downloads\Comodo_EDR_Agent	t_installer_1.1.258.3_Bk3uAu5kQ.exe	f49d31c432224f67	723f56d7a28cd2203bda23e58	Write File	Write to Executable
	<b>\$</b> 2	*	2018-05-30 17:05:28:488	DESKTOP- HI950BN	Administrator	C:\Users\Administrator\Downloads\Comodo_EDR_Agent	t_installer_1.1.258.3_Bk3uAu5kQ.exe	f49d31c432224f67	723456d7a28cd2203bda23e58	Write File	Write to Executable
	+3	~	2018-05-30 17:05:27:285	DESKTOP- HI9508N	Administrator	C:\Users\Administrator\Downloads\Comodo_EDR_Agent	t. Installer, 1.1.258.3, Bk3uAu5k0, exe	f49d31c432224f67	723f56d7a28cd2203bda23e58	Write File	Write to Executable

#### **Summary Search Results**

E	vent Search						
	inter your query here						~
9	very.Fields Operators Sample Overles My.Overles	Even	at Fields	Ever	t Datails	🗮 Last 30 Days	Q, Search
s	earch Results [ Time : 2018-05-07 12:18:19.347 - 2018-06	06 12:18:19.347 ]			1		1
	Device Name	Process User Name		Process Path		Event Type	1
	DESKTOP-HIV50BN	SYSTEM	712	svchost.exe	341	Create Process	907
0	edrwin732 ···· 83	Administrator	-230	.Searchindeser.exe · · · · ·		Write File	
	DESKTOP-7JBUVDU			firefox.exe		Network Connection	43 1
	ANIM0261	1298f		NGenTask.exe		Set Registry Value	
		user3	•	services.exe	63	Browser Download	•
	L						

- 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. This is similar to creating a **custom query**.

#### **Event List**

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

ŧ	Show	Event Time	Device Name	Current Process Use Name	r Curren Path	t Process	Current Process I	mage Hash		Cur Pro Ver
+1	~	2017-06-30 14:58:32.851	DESKTOP- HI950BN	Administrate	or C:\\Pro; (x86)\\C	gram Files Google\\Chro	c1939e8c702979c	336e0c5734b7952	c9676b45a6	Saf
-2	~	2017-06-30 14:58:31.850	DESKTOP- HI950BN	Administrato	or C:\\Pro; (x86)\\C	gram Files Google\\Chro	c1939e8c702979c	336e0c5734b7952	c9676b45a6	Saf
Bas Cur	e Event Ty rent Proce	pe Network Con sss C2017-06-28 1	nection 0:41:58.002	c	ustomer Ider levice Name	ntifid975c2b6-db7 DESKTOP-HI9	0-473f-be27-bc39cec2 50BN	Logged On User Destination IP	Administrator 127.0.0.1	
Cur	rent Proce	ess ID 3300		E	ndpoint Iden	tifierVBOXHARDD	5K-7130340531357875	Source IP	10.108.51.118	
Cur	rent Proce	ess I c1939e8c702	979c336e0c573	467952 E	ndpoint Inter	mal0.0.0.0	C-WDroarom E	Source Port	64843	
Cur	rent Proce	ess PC:\\Program	Files (x86)\\Goo	gle\\Chr E	vent Group	NETWORK	C.wrtogram P	ication//chromo.ov	UDP	
Cur	rent Proce	ess UDESKTOP-HIS	350BN	E	vent Time	2017-06-30 14	:58:31	o	. C:\\Program Fi	iles (x8
Cur	rent Proce	ess UAdministrato	e	E	vent Type	Network Conn	oction Add	lo Querv	SUCCESS	
Cur	root Proce	ere V. Safo		la la	Institut	ExtETATE COR	/du	io query		

 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. This is similar to creating a custom query.
- Clicking the icon in the 'Show' column for an event will display its timeline. See 'Process Timeline' for more details.

#### 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:

All Fields	80	Selected Fields		
☑ Adaptive Event Name		1. Event Time		Field Selection
🖯 Command Line		2. Device Name		III Select Fiel Adaptive
Destination IP		3. Process User Name	nt e	Event Name
□ Destination Port		4. Process Path	te	Write to
C Device Name		5. Process Hash	te	Write to
□ Downloaded File Hash		6. Event Type	20	
Downloaded File Path		7. Adaptive Event Name		
□ Elevation Type				
🖯 Event Group				
🖯 Event Identifier				
🕑 Event Time				

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 S 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.

COMODO Creating Trust Online

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.

Sean	ch Resu	<b>ilts</b> [ Time : 2018	-05-07 12:18:1	9.347 - 2018-06-0	6 12:18:19:247 ]					
De	vice Name	0			Process User Name	Process Path		Event Type		
DE ed DE AN	SKTOP-HP win732 - SKTOP-7J M0261	950BN			SYSTEM 100 Administrator 200 User 200 User 200 User 200	svchost.exe _Searchindexet.exe _Srafoz.exe _NDerTiesk.exe services.exe		Create Process Write File Nerwark Connection Set Registry Value Browser Download		
										III Select Fields
,	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_Ag	ent_Installer_1.1.258.3_Bk3uAu5kQ.exe	f49d31c432224f6	723f56d7a28cd2203bda23e58	Write File	Write to Executable
+:	20	2018-05-30	DESKTOP-	Administrator	C:\Users\Administrator\Downloads\Comodo_EDR_Ag	ent_Installer_1.1.258.3_Bk3uAu5kQ.exe	f49d31c432224f6	723f56d7a28cd2203bda23e58	Write	Write to

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

4		Show	Event Time 🚽	Device Name	Process User Name	Process Path				Process Hash		Event Type	Event Name
G	P	~	2018-05-30 17:05:39.395	DESKTOP- HI950BN	Administrator	C:\Users\Adm	ninistrator\Downloads\C	Comodo_EDR_Agent_Installer_1	.1.258.3_8k3uAu5kQ.ex	f49d31c432224f6	723f56d7a28cd2203bda23e58	Write File	Write to Executable
4	<b>\</b>	how	Event Time 🗸	Device Name	Process User Name	Process Path				Process Hash		Event Type	Adaptive Event Name
-1	ľ	<i>~</i>	2018-05-30 17:05:39.395	DESKTOP- HI950BN	Administrator	C:\Users\Admi	inistrator\Downloads\Co	omodo_EDR_Agent_Installer_1.	1.258.3_Bk3uAu5kQ.exe	f49d31c432224f67	23/56d7a28cd2203bda23e58	Write File	Write to Executable
	rile F	Path Hash	C:\Ue 00001	ersl.Administrati 10000000000000	or'AppDeta'(Loceh) 100666000000000000	lemp(721p5i	Event Type Adaptive Event Name Logged On Oser Device Name Event Time Event Oroup	Write File Write to Executable Administrator DESKT0P+44908N 2018-05-00 17:05:39 FILE	Pao Pao Pao Pao Pao	coss PD coss User Domain coss Path coss User Name coss Hash coss Creation Time	3648 DESKTOP-HISSEEN C.WaershAdministrator/Downloads/Con Administrator Mirkd3164122245723556478286422038 2018-05-50 17:05:23	nodo_EDR.J ida23e58	4gentins

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

### 10.2 Computer Search

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

EDR EWatch ≡ 9 Log out 0 Computer Search Dashboard ANM0405 Alerts Logged On User: korayy Endpoint Version: 1.1.259.0 Last Seen : 2018-08-16 16:22:00 Last Reboot : 2018-08-16 01:57:01 Ope to Syst Windows 10 or Later 64 bit plat Policy Managemy Local and External IP Changes Unique Users Logged on Detection # External IP Local IP1 Local IP2 Local IP3 Time Username Last See . Endpoints 2018-07-13 19:45:19 1 213.14.87.114 172.18.223.65 10.100.132.121 0.0.0.0 2018.08.10.21:40.51 1 korayy 2 213.14.87.114 172.18.223.65 0.0.0.0 0.0.0.0 2018-08-10 12:54:58 2018-05-30 22:09:50 2 Q Investigation 3 213.14.87.114 172.18.223.65 10.100.132.121 0.0.0.0 2018-08-02.12:38:42 Total Count : 2, Page 1 of 1 ent Search 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 2018-07-25 18:33:06 Total Count: 12. Page 1 of 3 1 2 3 Next Last » Hash Search Download Agent Network Connections Admin Privilege Usage M Last 3 Dave 📋 Last 3 Days ~ There is no network connection There is no result Event Trend (Click and drag in the plot area to zoom in ) Mahware Detections 🛗 Laat 3 Daya 🛛 👻 There is no malware detection 14. Nov 12:00

- By default, the screen will be blank with search time range pre-selected for the last 3 days.
- Please note the search field will be auto-populated and results displayed for the endpoint that is clicked from the dashboard.

#### **Search and Sorting options**

- Search option The 'Search' box above the table allows you to filter the list.
  - · Click anywhere on the row and select from the device list

OR

Click anywhere on the row and enter full or partial endpoint name in the search box and select from the suggestion

Use the time-range drop-down to show event information for a specific date or date range (applies to Network Connections, Admin Privilege Usage, Malware Detections and Event Trend tiles).

COMODO Creating Trust Online

		000010		an F	<sup>&gt;</sup> rivil	ege Us	age							tast 3 Days ✓
2	018-06	6-03 1	5:34:0	)3			2	018-0	6-06 1	15:34:	03			Last 15 Minutes
۲	3	Ŧ	: 34	Ŧ	PM	Ŧ	٩	3	٣	: 34	٣	PM	Ŧ	Last 30 Minutes
		M	ay 20	18					Ju	un 20 <sup>.</sup>	18			Last 60 Minutes
Su	Мо	Tu	We	Th	Fr	Sa	Su	Мо	Tu	We	Th	Fr	Sa	Last 12 Hours
<del>29</del>	<del>30</del>	7	2	3	4	5	27	28	29	30	31	1	2	Last 1 Day
6	7	8	9	10	11	12	3	4	5	6	7	8	9	Last 3 Days
13	14	15	16	17	18	19	<del>10</del>	11	<del>12</del>	<del>13</del>	14	<del>15</del>	<del>16</del>	Last 7 Days
20	21	22	23	24	25	26	17	<del>18</del>	<del>19</del>	<del>20</del>	<del>21</del>	<del>22</del>	23	Last 15 Days
27	28	29	30	31	1	2	<del>24</del>	<del>25</del>	<del>26</del>	27	<del>28</del>	<del>29</del>	<del>30</del>	
3	4	5	6	7	8	9	1	2	3	4	5	6	7	Last 30 Days
														Custom range
														Apply Cancel

- Click 'Custom range' to choose specific dates.
- Click 'Apply'. The results for the selected period will be displayed.

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

Computer Search						
DESKTOP-7J8UVDU						•
Logged On User: ops 64 bit platform	Endpoint Version: 2.1.258.0	Connection Status: Online	Last Seen : 2018-0:	1-24 22:28:58	Last Reboot : 2018-05-24 21:28:59	Operating System : Windows 10 or Later
Local and External	IP Changes		Un	ique Users L	ogged on	

- Logged On User Endpoint username at the time of event logging
- Endpoint Version Software version of the EDR agent
- Connection Status Indicates whether the endpoint is connected to EDR. The statuses are:
  - Online Indicates the endpoint is normally sending message to the EDR server
  - Offline Indicates that the agent sent last message to the server along with the information that it would of offline
  - Disconnected Indicates the agent was not able to send the message that it would go offline.
- Last Seen Indicates the latest date and time the EDR agent on the endpoint updated EDR
- Last Reboot Date and time the endpoint was rebooted last
- Operating System The details of endpoint's OS.

The six tiles below the endpoint info provide the details of events recorded for the selected endpoint.

- Local and External IP Changes
- Event Trend
- Unique Users Logged on
- Admin Privilege Usage

COMODO Creating Trust Online

COMODO Creating Trust Online

- Network Connections
- Malware Detections

### Local and External IP Changes

This tile lists any changes in the endpoint's local IP and external IP.

	External IP	Local IP 1	Local IP 2	Local IP 3	Time
	182.74.23.22	10.0.2.15	0.0.0	0.0.00	2018-05-29 12:32:16
,	52 41 147 167	10 100 51 011	0.0.0.0	0.0.0.0	2017-06-23 12:46:20

- External IP The current external IP through which the endpoint connects to other external networks.
- Local IP 1 The current local IP of the endpoint.
- Local IP 2 and 3 Details of the previous local IPs (for example, the endpoint is moved from one network to another and allotted different IPs)
- Time The date and time of last recorded change.

#### **Event Trend**

This tile displays the number of events that were recorded from the endpoint for the selected time-period.

COMODO Creating Trust Online\*

Event	Trend (Click	and drag in th	ne plot area to	o zoom in )		🛗 Las	t 15 Days	~
300								
200				_				
100				had				
0	24. May	26. May	28. May	30. May	1. Jun	3. Jun	5. Jun	

- Select the time-period for which the event trend should be shown. The period ranges from last 15 minutes to 30 days.
- The X-axis displays the selected date range and Y-axis provides the number of events.

Event	Trend (Click	and drag in th	ne plot area to	zoom in )		🛗 Las	t 15 Days	~
300 -								
200			Tuesda • Ever	y, May 29, 15:3 nt Count: <b>14</b> 3	0 3			
100				C <sub>8</sub>				
0	24. May	26. May	28. May	30. May	1. Jun	3. Jun	5. Jun	
0	24. May	26. May	28. May	30. May	1. Jun	3. Jun	5. Jun	-

• Placing the mouse cursor on a particular point on the graph displays the number of events.

• To view the number of events for a particular of time, click on the graph and drag to zoom. You can view the number of recorded events by hourly basis. Zoom in again if required.

COMODO Creating Trust Online\*



- Place your mouse cursor on a point in the line to see events for a specific day.
- Click 'Reset Zoom' to view the original graph.

#### **Unique Users Logged on**

Displays the most recent login times of every user that has logged onto the endpoint.

#	Username	Last Seen	
1	SYSTEM	2017-06-23 14:20:19	
2	Administrator	2017-07-03 16:04:49	

- Username The name of the user that is currently logged in and last communicated time to EDR. SYSTEM indicates the date and time the endpoint was first connected to EDR.
- Last Seen Date and time the endpoint communicated to EDR.

#### Admin Privilege Usage

Displays details of events that required admin privileges.

COMODO Creating Trust Online\*

	dmin Privile	ege Usage	🛗 Last 15 Days	~
#	Username	File Name		Count
1	user3	C:\Windows\System32\WindowsPowerShell\v1.0\powershell	.exe	3
2	user3	C:\LIsers\user3\Downloads\pRt4iHbH exe		1

- Select the time-period for which the data should be shown. The period ranges from last 15 minutes to 30 days. You can configure custom range also.
- Username The name of the user that used the admin level privileges on the endpoint.
- File Name The name of the application that was used.
- Count The number of times the event was recorded. Clicking the number will display the event details in the 'Event Search' interface.

### **Network Connections**

Displays the details of network connection events for the selected time-period.

#	Local IP	Destination IP	Destination Port	Count
TT	Local IF	Destination IP	Destination Fort	count
1	10.0.2.15	46.144.122.248	1433	1
2	10.0.2.15	43.249.131.101	443	1
3	10.0.2.15	121.54.162.115	443	1
4	10.0.2.15	121.54.162.116	443	1

- Select the time-period for which the data should be shown. The period ranges from last 15 minutes to 30 days. You can configure custom range also.
- · Local IP The internal IP address of the endpoint.
- Destination IP The destination IP details to which the connection was established.
- Destination Port The destination port to which the connection was established.
- Count The number of time the connection to the destination IP and port was established from the endpoint. Clicking the number will provide the event details in the 'Event Search' interface.
- View more records by clicking 'Next', 'Last', 'First', 'Previous' or any number.

#### **Malware Detections**

Displays the malware detected events on the endpoint for the selected period.

#	File Name	File Path	Sha256
1	suspicious.exe	C:\Users\user3\Downloads\suspicious.exe	8233bf6e61390ed8959255a8a477b8e76f10
2	pRt4jHhH.exe	C:\Users\user3\Downloads\pRt4jHhH.exe	27d99fbca067f478bb91cdbcb92f13a828b0
1			•

- Select the time-period for which the data should be shown. The period ranges from last 15 minutes to 30 days. You can configure custom range also.
- File Name The name of the file that was detected as malware by EDR.
- File Path The location of the malware file.
- Sha256 The hash signature of the malware file. Clicking a hash signature will provide the full details in the 'Hash Search' interface.
- View more records by clicking 'Next', 'Last', 'First', 'Previous' or any number.

### 10.3 Hash Search

- A hash search allows you to 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 (ii) click a hash-value link in various screens such as the dashboard or 'Computer Search' screens. The latter will auto-populate the search interface.
- Click 'Investigation' on the left then 'Hash Search' to open the interface.

COMODO Creating Trust Online\*

	CWatch						Up	prade Now Welco	ome. Demo Premium	9 Los out
_	EDR	_								
an	Provide a second	Hash Search								
0210	Dashboard	8233bfbeb1390ed8959255a8a43	7b8e76f10d2bc							Q
	Alerts	File Names (last 3 days) Elle	a Tumor Unceller	Malazan Baliya	Doint: anata720	First Page fire 2018 of a	111-01-01	Lost Feen On 10	0.05.04.00.05.05.0	_
Ð	Policy Management	7.BIVDU Seen Dn: 2 devices	Detection Time: 2	018-04-17 21:49:03	Point Brinning	This are on 21700	of 19.00.27 , Borniniae	Carl aven de 20	1979724222830, BESKIN	
U	Detection	File Trajectory								leset Zoom
	Endpoints		23 May 2018							
			19:30	19:45	20	20:15	20:30	20.45	21	21-15
۹	Investigation	DESKTOP-7JBUVDU (1)								
3	Event Search	ANM0261 (1)		Ð	1					
3	Computer Search	edrwin732 (1)	9							
0	Mash Search									
			Browser Download	E Copy From 5	Shared Folder	Copy To Shared Folder	尋 Email Download	đ		
*	Download Agent		Copy From USB Dis	ik 🛛 🖺 Copy To U	SB Disk 🛛 🖻 Writ	File				
			Proce	es Creation 💦 😑	Alert Detection					
		Electron Samany		题 Lat	4.3 Davis V	Download Su	mmary		🏥 Last 30 Da	15 01 9

- 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 or date-range (applies to 'Execution Summary', 'Download Summary', 'Creation Summary' and 'Execution Trend' tiles)

Results are shown below the search box:

Hash Search	
8233bf6e61390ed8959255a8a477b8e76f10d2bc	٩
File Names (last 3 days):         File Type: -         Verdict: Ma/ware         Entry Point: edmin732         First Seen On: 2018/05/23 19/26/27, edmin732           7.38UVDU         Seen On: 3 devices         Detection Time: 2018/04/17 21:48/03         First Seen On: 2018/05/23 19/26/27, edmin732	Last Seen On: 2018/05/24 22:28:58 , DESKTOP-
File Trajectory	Reset Zoom

- File Name Hash value's file name
- File Type The nature of file. For example, an executable.
- Verdict Displays the file's trust rating after EDR analysis.
- Entry Point The name of the device on which the file was first detected. Click the device name to open the 'Computer Search' screen with the device name auto-populated in the search box.
- First Seen On The date and time of the event was first logged and the name of the device on which it was detected. Click the device name to open the 'Computer Search' screen with the device name auto-populated in the search box.
- Last Seen On The date and time of the last event logged for the same file and the name of the device on which it was detected. Click the device name to open the 'Computer Search' screen with the device name auto-populated in the search box.
- Seen On The number of devices on which the file was found.
- Detection Time The date and time the trust verdict was awarded to the file. This may be some time in the past if Valkyrie has already encountered the file and has a database entry for it.

The results screen provides the following details about the file:

- File Trajectory
- Execution Summary
- Download Summary
- Creation Summary
- Execution Trend

#### **File Trajectory**

The first tile below the hash file info screen displays the movement of the file, that is from where it was downloaded, copied to which endpoint and so on.

File Trajectory									Reset Zoom
	23 May 2018 06:55:02 P 07 PM	9M 07;15	07;30	07;45	00 PM	66:15	60,30	00,45	23 May 2018 09
DESKTOP-7J8UVDU (4)					•				Ø
edrwin732 (4)	۲	Ð							۲
ANM0261 (3)			Ð						茵
	Browser Download     Copy To USB Disk     Process	<ul> <li>Copy From Copy From Cop</li></ul>	m Shared Folder Alert Oct	Copy To:	Shared Folder	ଡ଼ି Email Download	🗍 Copy From U	SB Disk	

- 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.

Event Time Logge   2018-05-23 18:55:02 3s In   Process Hash Event   ef45d0c407d2987b2edb3dd76967e1b16bd6c1c8   Process Path   C:\Program Files\Mozilla Firefox\firefox.exe   Path   C:\Users\user\Downloads\pRt4JHhH.exe   URL   https://bit.ly/2H9HZJR	ged On User	mapping Life	A PA	
2018-05-23 18:55:02 Is -In Device Event i ef45d0c407d2987b2edb3dd76967e1b16bd6c1c8 Process Path C:\Program Files\Mozilla Firefox\firefox.exe Path C:\Users\user\Downloads\pRt4jHhH.exe URL 0 https://bit.ly/2H9HZJR 0	50 St 10/00 St 50 St	Logged On U	Loo.	ime
Process Hash ef45d0c407d2987b2edb3dd76967e1b16bd6c1c8 Process Path C:\Program Files\Mozilla Firefox\firefox.exe Path C:\Users\user\Downloads\pRt4jHhH.exe URL 0 https://bit.ly/2H9HZJR	ice Name	Device Name	as In De	5-23 18:55:02
ef45d0c407d2987b2edb3dd76967e1b16bd6c1c8 Process Path C:\Program Files\Mozilla Firefox\firefox.exe Path C:\Users\user\Downloads\pRt4JHhH.exe URL 0 https://bit.ly/2H9HZJR edrwin732 (2)	nt Lime nt Group	Event Lime Event Group	E	s Hash
Process Path C:\Program Files\Mozilla Firefox\firefox.exe Path C:\Users\user\Downloads\pRt4JHhH.exe URL https://bit.ly/2H9HZJR edrwin732 (4)			-	c407d2987b2edb3dd76967e1b16bd6c1c8
C:\Program Files\Mozilla Firefox\firefox.exe Path C:\Users\user\Downloads\pRt4JHhH.exe URL othttps://bit.ly/2H9HZJR edrwin732 (2015)				s Path
Path C:\Users\user\Downloads\pRt4JHhH.exe URL 0 https://bit.ly/2H9HZJR edrwin732 (4				ram Files\Mozilla Firefox\firefox.exe
C:\Users\user\Downloads\pRt4JHhH.exe URL 0 https://bit.ly/2H9HZJR edrwin732 (				
URL 0 https://bit.ly/2H9HZJR E				s\user\Downloads\pRt4jHhH.exe
edrwin732 (4 )	07:30	07:30		٨
edrwin732 (4 G				bit.ly/2H9HZJR
				edrwin732 (A B)
ANM0261 (3)	b	•		ANM0261 (3)
Browser Download	hared Folder	rom Shared	Copy From	<ul> <li>Browser Download</li> </ul>
🗄 Copy To USB Disk 🛛 🗈 Write File		le	Write File	Copy To USB Disk

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

File Trajectory											Reset Zoom
	23 May 2018 06:06:58	8 PM								23 May 201	8 11:40:20 PM
	06,30	67 PM	07;30	08 PM	08,30	CS PM	09,30	18 PM	10,30	11 PM	11,30
DESKTOP-7J8UVDU (20)											
edrwin732 (16)		<b>@ • •</b>				•• 🕞					
ANM0261 (11)			۵	• • • • •	٠	Ē					
		1									
	Browser Download	E Copy Fi	rom Shared Fold	er 🖻 Copy	To Shared Folder	💷 Email 🛙	beoinwoo	Copy From USE	3 Disk		
	Copy To SB Disk	Write Fil	e								
(	Proci	ess Creation	Alert	Detection							

	Modify Firewall Settings	×		
57 PM 07 PM	Alert Time 2018-05-23T14:21:33.094Z Process Path C:\Users\user2\Downloads\pRt4jHhH.exe	30	09 PM 09 30	
<b>G</b>	General Show detail		• • •	
	B • (7)		ŧ	
ad 😰 Copy From K 🗈 Write File	Shared Folder 🖻 Copy To Shared Folder	역 Email Download	🕄 Copy From USB Disk	
ocess Creation 🛛 🔴	Alert Detection			

Click an icon color code to view trajectory details.

- '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.

#### **Execution Summary**

A summary of the devices on which the file was executed. Details include the file path and the number of times it was executed.

COMODO Creating Trust Online\*

Execution Summa	у	🛗 Last 30 Days 🔷 🗸
Executed On	Execution Path	Execution Count
DESKTOP-7J8UVDU	C:\Users\user3\Downloads\suspicious.exe	1
edrwin732	C:\Users\user\Downloads\suspicious.exe	1
ANM0261	C:\Users\user2\Downloads\suspicious.exe	1

- Select the time-period for which the event trend should be shown. The period ranges from last 15 minutes to 30 days.
- View more records by clicking 'Next', 'Last', 'First', 'Previous' or any number.
- Executed On The device on which the file was run.
- Execution Path The location of the file on the device. Clicking the path link will open the 'Event Search' screen with the query pre-populated.
- Execution Count The number of times the event has occurred.

#### **Download Summary**

Shows the details on which endpoint the file was downloaded (aka 'Entry Point'), the URL from where it was downloaded and the number of times it was downloaded.

Downloaded On edrwin732 Fotal Count : 1 , Page 1 of 1	Downloaded From https://bit.ly/2H9HZJR	Downloaded Count
edrwin732 fotal Count : 1 , Page 1 of 1	https://bit.ly/2H9HZJR	1
Fotal Count : 1 , Page 1 of 1		

- Select the time-period for which the download summary should be shown. The period ranges from last 15 minutes to 30 days.
- View more records by clicking 'Next', 'Last', 'First', 'Previous' or any number.
- Downloaded On The device on which the file was first downloaded
- Downloaded From The location from which the file was downloaded
- Downloaded Count The number of times the file was downloaded

#### **Creation Summary**

Details of endpoints on which the file has created processes and the location of file from where it was run.

COMODO Creating Trust Online

Last 30 Da						
Created On	Location	Process				
DESKTOP- 7J8UVDU	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\pRt4j HhH.exe	pRt4jHhH.exe				
DESKTOP- 7J8UVDU	C:\Users\user3\AppData\Microsoft\Windows\Start Menu\Programs\Start up\pRt4jHhH.exe	pRt4jHhH.exe				
edrwin732	C:\windows\system32\pRt4jHhH.exe	pRt4jHhH.exe				
DESKTOP- 7J8UVDU	C:\Users\user3\Downloads\pRt4jHhH.exe	explorer.exe				
ANM0261	C:\Users\user2\Downloads\pRt4jHhH.exe	explorer.exe				
otal Count : 6 , Pag	e 1 of 2 1 2	Next Last				

- Select the time-period for which the creation summary should be shown. The period ranges from last 15 minutes to 30 days.
- View more records by clicking 'Next', 'Last', 'First', 'Previous' or any number.
- · Created On The device on which the file was run
- Location The path of the file from where it was run
- Process The name of the application that was run

#### **Execution Trend**

The number of times the file ran during the selected time-period.

xecutior	n Trend			🏥 Last 30 Days	~
3					
2					
1					
0	14 44-11	21. 14	28 Mar	4	
	It. May	21. May	28. May	4. jun	

- Select the time-period for which the creation summary should be shown. The period ranges from last 15 minutes to 30 days.
- X-axis displays the selected date range and Y-axis provides the number of file execution counts.
- Place you mouse cursor on a particular point on the graph to see the number of executions.

COMODO Creating Trust Online

Execution	Trend			🛗 Last 30 Days	~
3					
2		Wednesday, May Execution (	(23, 18:30 Count: 1		
1			8		
0	14 Mari	21 Ман	28 Mar	4	
	14. May	21. May	20. May	4. jun	

• You can zoom in by dragging any point on the graph. This lets you, for example, more clearly see the hours of the day when the file ran.

Execution Trend				🏥 Last 30 Days	~
3 Reset zoom					
1 Wednesday, May 23, 20 • Execution Count:	2:30 2				
20:00	24. May	04:00	08:00	12:00	•

- Place your mouse cursor on a point in the line to see the number of counts.
- Click 'Reset Zoom' to view the original graph.

### 10.4 Process Timeline

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

You can view the timeline in two ways:

#### **Event Search**

Auto-populate the event ID from the 'Event Search' results interface. Go to 'Investigation' > 'Event Search', select the time-period and click 'Search'. Under the 'Event List' section, click the process timeline icon beside an event in the 'Show column.

• Alternatively, you can provide the event ID manually in the field to view its timeline.

#### Alerts

Go to 'Alerts' then click 'Show Alerts' in an Alert row. Under 'Events' section, click the process timeline icon
 beside an event in the 'Show column.

The timeline of the selected event will be displayed.

rocess rimeline												
Timeline Tree View											Rese	t Zoom
	30 May 2018										30 May 20	018
	04.40	04:45	04:50	04.55	05	05:05	05,10	05 15	05:20	65.25	05:30	05:35
wink	ogon.exe											
	erinit.eze											
Explore	r.EXE (4)	•		•								_
	+					-						
Comodo EDR Agent Installer 1,1,258,3 Bk3uAu5ki	0.448.225					_						
	u.cec (0)											
	u.cee.toy					-	Process	Network	Registry	🖲 file 😑 D	vefenseptus 🔍 Bro	ASet
	File Pach	Cillikensijäde	inistano (, App)	atalLocal\Tem.	Event Type	Ī	Process     Write File	Network	Registry	O File O D	Process P1D	NSET
	File Park File Hash	C:WsensijAde 71f22o5672e	sinistore/sApp1 ee5o4c7d608fb	atali.ocali,Tem bd43a5023499	Event Type Adaptive Eve	ent Name	Process     Write File     Write to Exect     Approximation	• Network	Registry	● file ● D	efenseptus	364 DES Chui
	File Pach File Hash	C:WsensUAdr 71f22o6872e	sinistoste ("Apol ee 504c7d608fo	ata/Local/Tem	Event Type Adaptive Eve Logget On U Device Name	cri Narse Jser	Process     Write file     Write to Exec     Apministrato     DESKTOP-Hill	Nedwork	Registry	● file ● D	Process P1D Process P1D Process User Domain Process Path Process Litter Name	364 085 034 034
	File Pach File Hash	C:\Users\\Adr 71f22o6872e	ninistrato (J. Apol ee 504 c 7060810	anail.ocail.Tem. bol43a5023499	Event Type Adaptive Exc Logget On U Device Name Event Time	ent Name Jser	Process     Write File     Write to Exec     Apministratio     DESKTOP-HIS     2018-06-30 1	Network usable Koon 20625	<ul> <li>Registry</li> </ul>	● file ● D	Minimipius Ibor Process PtD Process User Domain Process Path Process Liter Name Process Rash	264 DES 030 Adm 7450
	File Pach File Hash	C Weens Under 71 ft 22:050 72e	ninistorto (, Appl ee 504c 7060810	ima(Local),Tem. 	Event Type Adaptive Eve Logged On U Device Name Event Time Event Goog	cri Narsc Jser	Process     Write Pile     Write In Energy     Administratio     DESKTOP-HIS     2018-06-30 1     FILE	Network utable / Isonn 20625	<ul> <li>Registry</li> </ul>	• fin • D	Minimiplus III or Process P3D Process User Domain Process Path Process Rash Process Rash Process Creation Time	364 065 031 Adm 6490 201

You can view the details in timeline or tree view.

#### **Timeline View**

By default, the timeline view of the event will be displayed:

											RESE
	23 May 2018	06:42:31 PM								23 May 20	18 07:42:31
	06,45	08.50	06,55	67 (94	07,05 07	10 07,15	07,20	07,25	07,30	07:35	07,40
wininit.exe											
explorer.exe (4)			• •				•	+			
								Process	Network 🔴 Registry	r 🔍 File 🔍 Defen	seplus 🔶 Brox
Г	His Puth	C.Wsers/user/Downlo	ads/guspicios_	Event Type	Write File		Process	<ul> <li>Process</li> <li>Process</li> </ul>	Network Registry	r 🔍 Flie 🧶 Defen	seplus 🔎 Brox
Γ	Hic Huth File Heah	C.Users/user/Dowrlig 8233bf8e61390es895	ed9/auspicios 9255a5e47765	Event Type Adaptive Event Name	Write File		Process	Process	Network Registry 7088 edmin732	y 🖤 File 🧶 Defen	seplus 🔍 Brow
[	Hie Puth File Heah	G.Wsers/wsert/Downlo 82233649e61390ed895	eds/auspicios 9255e8e47768	Event Type Acleptive Event Name Logged On User	Write File - user		Process Process Process	Process	Network Registry 7068 edmin732 C:Windownicspiere	r 🗣 File 🔍 Defen	seplus 🔍 Brow
	Hic Puth Hic Hosh	G.Wsers/aser/Downlo 8233bHse51390ed895	edo'suspicios 7255e0e477b0	Event Type Adaptive Event Name Logged On User Device Name	Write File - user ediwin732		Process Process Process Process	Process	Network Begistry 7088 edmin732 C.Windowsheapfore User	r 🗣 File 🔍 Defen	seplus 🔎 Bron

- The search time here indicates the processes that the event generated. The results are displayed for processes generated 30 minutes preceding and after the event. For example, for an event that started at 11.00.00, the results will displayed for processes generated by the event from 10.30.00 to 11.30.00.
- The timeline of the event is shown at the top with date and time preselected.
- The processes path initiated by the event is indicated by the down arrow.
- The number beside a process name indicates the number of events generated by the process.
- · Click on a process to view process name, time-stamp, hash, path and verdict.

COMODO Creating Trust Online



- The event (created by the process) details are shown in the box below the process path.
- The event types are color coded and displayed above the event details box.

.e	xe					
E (	2)	•	Event details box	Color	codes for event types	]
e (	3)		• 1		1	
				Process	Network Registry File	🔴 Defenseplus 🔎 Browser
		File Path File Hash	C:\Users\Administrator\AppData\Local\Temp\72ipSf f1b27748d6913167c13f64313a8a1d1dcb4459c8	Event Type Adaptive Event Name Logged On Uaer Device Name Event Time Event Group	Write File Write to Executable Administrator DESKTOP-H19508N 2018-05-30 17:05:24 FILE	Process PID Process User Process Path Process User Process Has Process Crea
	4					,

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

#### **Tree View**

You can view the process hierarchy in tree view. In the 'Process Timeline' screen, click 'Tree View' tab.



- You can view the processes and event types with respective colors.
- 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.
- Clicking on a process name will open the 'Event Search' screen with the event search box populated with the selected process parameters.



# Appendix 1 - Default Comodo Security Policy Details

An EDR policy determines which events will generate an alert for you. Comodo EDR ships with a default security policy containing seven event categories. The table below contains details of the default rules in each event category.

The built-in event categories are:

- Process Events Rules to generate alerts if an application causes an event
- Registry Events Rules to alert you about changes to the Windows registry on your endpoints.
- File Events Rules that detect modifications to any system files and folders
- Download Events Rules to create alerts when applications are downloaded via browsers.
- Upload Events Rules to alert you about file uploads to shared folders or external drives.
- Defense+ Events No default rules are set for this event category.
- Network Events No default rules are set for this event category.

#### **Process Events**

	Event Category - Process Events						
Event Type - Creat	e Process						
Event Name	Score	Description					
Suspicious System Process Creation	6	Process verdict is not safe AND file path matches %systemroot%\*					
Remote Powershell Execution	5	File path matches *\wsmprovhost.exe					
Suspicious Powershell Flag	5	Command line matches any of the following: *powershell*-NoP* *powershell*-Win* *powershell*-ex* *powershell*-Exec* *powershell*-ex* *powershell*-ep* *powershell*-command* *powershell*-NoL* *powershell*-InputFormat* *powershell*-InputFormat* *powershell*-NonInteractive* *powershell*-nonI* *powershell*-nonI*					
Stop Service	5	Command line matches %systemroot%\system32\net*stop*					
Run Untrusted	4	Verdict is not safe					

Executable		
Suspicious Process Hierarchy	3	Process path does not match *\explorer.exe AND path matches *\powershell.exe OR patch matches *\cmd.exe
Start Service	2	Command line matches %systemroot%\system32\net*start*

### **Registry Events**

	Event Category - Registry Events						
Event Type - Set	Registyry V	alue					
Event Name	Score	Description					
Disable User Account Control	9	Registry key path is equal to HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\S ystem AND registry value name is equal to EnableLUA0 AND registry value data is equal to 0.					
Disable Task Manager	9	Registry key path is equal to HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policie s\System AND registry value name is equal to DisableTaskMgr AND registry value data is equal to 1					
Installation of Drivers	8	Registry key path matches HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\* AND registry value name is equal to Type AND Registry value data is equal to 1 OR registry value data is equal to 2					
Add Service to svchost	7	Registry key path matches HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\* AND registry value name is equal to ImagePath AND registry value data matches *svchost.exe* OR Registry key path matches HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\*\Parameters AND registry value name is equal to ServiceDII AND registry matches *.dll					
Add Active Setup Value In Registry	7	Registry key path matches HKEY_LOCAL_MACHINE\Software\Microsoft\Active Setup\Installed Components\*					
Modify Powershell Execution Policy	7	Registry key path is equal to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PowerShell\1\ShellIds\Microsoft. PowerShell AND registry value name is equal to ExecutionPolicy					
Modify Firewall Settings	6	Registry key path matches HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\P arameters\FirewallPolicy\StandardProfile*					
Disable Registry Editing Tool	6	Registry key path is equal to HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policie s\System AND registry value name is equal to DisableRegistryTools AND registry value data is equal to 1.					



COMODO Creating Trust Online


		HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate AND registry value name is equal to DisableWindowsUpdateAccess AND registry value data is equal to 1 OR Registry key path is equal to HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Wi ndowsUpdate AND registry value name is equal to DisableWindowsUpdateAccess AND registry value data is equal to 1
Disable Service	5	Registry key path matches HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\* AND registry value name is equal to Start AND registry value data is equal to 4
Create Explorer Entry	5	Registry key path matches any of the following: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\PROTOCOLS\Filter* HKEY_LOCAL_MACHINE\SOFTWARE\Classes\PROTOCOLS\Filter* HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Desktop\Components* HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellS erviceObjectDelayLoad* HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellS erviceObjectDelayLoad* HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellS erviceObjectDelayLoad* HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellS erviceObjectDelayLoad* HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\S hellExecuteHooks* HKEY_LOCAL_MACHINE\Software\Classes\*\ShellEx\ContextMenuHandlers* HKEY_LOCAL_MACHINE\Software\Classes\AllFileSystemObjects\ShellEx\Context MenuHandlers* HKEY_LOCAL_MACHINE\Software\Classes\Directory\ShellEx\ContextMenuHandl ers* HKEY_LOCAL_MACHINE\Software\Classes\Directory\ShellEx\ContextMenuHandl ers* HKEY_LOCAL_MACHINE\Software\Classes\Directory\ShellEx\ContextMenuHandl ers* HKEY_LOCAL_MACHINE\Software\Classes\Directory\ShellEx\ContextMenuHandl ers* HKEY_LOCAL_MACHINE\Software\Classes\Directory\Shellex\DragDropHandlers* HKEY_LOCAL_MACHINE\Software\Classes\Directory\Shellex\DragDropHandlers* HKEY_LOCAL_MACHINE\Software\Classes\Directory\Shellex\DragDropHandlers* HKEY_LOCAL_MACHINE\Software\Classes\Directory\Shellex\DragDropHandlers* HKEY_LOCAL_MACHINE\Software\Classes\Directory\Shellex\ContextMenuHandl ers* HKEY_LOCAL_MACHINE\Software\Classes\Directory\Shellex\CopyHookHandlers* HKEY_LOCAL_MACHINE\Software\Classes\Directory\Shellex\CopyHookHandlers* HKEY_LOCAL_MACHINE\Software\Classes\Directory\Shellex\CopyHookHandlers* HKEY_LOCAL_MACHINE\Software\Classes\Directory\Shellex\ColumnHandlers* HKEY_LOCAL_MACHINE\Software\Classes\Directory\Shellex\ColumnHandlers* HKEY_LOCAL_MACHINE\Software\Classes\Directory\Shellex\ColumnHandlers* HKEY_LOCAL_MACHINE\Software\Classes\Folder\Shellex\ColumnHandlers*
		HKEY_CURRENT_USER\Software\Classes\Folder\ShellEx\ContextMenuHandlers *

#### COMODO Creating Trust Online

## Comodo EDR - Admin Guide

		$\label{eq:hkey_local_MACHINE} Kare\Classes\Folder\ShellEx\ContextMenuHandlers^*$
		HKEY_CURRENT_USER\Software\Classes\Directory\Background\ShellEx\Contex tMenuHandlers*
		HKEY_LOCAL_MACHINE\Software\Classes\Directory\Background\ShellEx\ContextMenuHandlers*
		HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\S hellIconOverlayIdentifiers*
		HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\S hellIconOverlayIdentifiers*
		HKEY_CURRENT_USER\Software\Microsoft\Ctf\LangBarAddin*
		HKEY_LOCAL_MACHINE\Software\Microsoft\Ctf\LangBarAddin*
		HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Approved*
		HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Approved*
		OR
		Registry key path is equal to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explor er\SharedTaskScheduler
Disable Windows Application	5	Registry key path is equal to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policie s\Explorer\DisallowRun
Disable Command Prompt	5	Registry key path is equal to HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System AND registry value name is equal to DisableCMD AND registry value data is equal to 2
Disable Show Hidden Files	4	Registry key path is equal to HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\A dvanced AND registry value data is equal to 2
		AND
		Registry value name is equal to Hidden OR registry value name is equal to ShowSuperHidden
Share Folder	4	Registry key path is equal to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Lanmanserver\S hares
Addition of DNS Server	3	Registry key path matches HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters \Interfaces\* AND registry value name is equal to NameServer
Modify Hosts File Registry	3	Registry key path is equal HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters AND registry value name equal to DataBasePath

#### **File Events**

Event Category - File Events						
Event Type - Write File						
Event Name	Score	Description				
Add Scheduled Task	6	File path matches %systemroot%\System32\Tasks* OR %systemroot%\Tasks*				
Write Fake System File	6	File path matches *svch0st.exe OR *svhost.exe				
Write to System Directory	5	File path matches %systemroot%*				
Add Startup File or Folder	5	File path matches any of the following: %appdata%\Microsoft\Windows\Start Menu\Programs\Startup\* %programdata%\Microsoft\Windows\Start Menu\Programs\Startup\* %systemroot%\system\iosubsys\* %systemroot%\system\vmm32\* %systemroot%\Tasks\* OR File path equals any of the following: %systemdrive%\autoexec.bat %systemdrive%\config.sys %systemroot%\winstart.bat %systemroot%\winstart.bat %systemroot%\win.ini %systemroot%\system.ini %systemroot%\dosstart.bat				
Modify Host File	4	File path is equal to %systemroot%\system32\drivers\etc\hosts				
Write to Executable	4	File type is equal to PORTABLE_EXECUTABLE AND Process path doesn't match *\explorer.exe				
Write to Infectible File	4	Process path doesn't match *\explorer.exe AND File path matches any of the following: *.lnk *.wsf *.hta *.hta *.mhtml *.html *.doc *.docm *.xls				

		*.xlsm *.ppt
		^.pptm * abre
		*.vbs
		*.js
		*.bat
		*.pif
		*.pdf
		*.jar
		*.sys
Modify Group Policy Settings	1	File path matches %systemroot%\system32\grouppolicy\* OR %systemroot %\Sysvol\sysvol\*\Policies\*
Write to Program Files Directory	1	File path matches %programfiles%\*

#### **Download Events**

Event Category - Download Events				
Event Type - Browser Download				
Event Name	Score	Description		
Download Infectible File	3	File path matches any of the following: *.Ink		
		*.wsf		
		*.hta		
		*.mhtml		
		*.html		
		*.doc		
		*.docm		
		*.xls		
		*.xlsm		
		*.ppt		
		*.pptm		
		*.chm		
		*.vbs		
		*.js		
		*.bat		
		*.pif		
		*.pdf		
		*.jar		
		*.sys		



Download Executable	2	File type is equal to PORTABLE_EXECUTABLE
------------------------	---	---

#### **Upload Events**

Event Category - Upload Events				
Event Type - File Copy to Shared Folder				
Event Name	Score	Description		
Write Executable to Shared Folder	5	File type is equal to PORTABLE_EXECUTABLE		
to Shared Folder Write Infectible to Shared Folder	5	File path matches any of the following: *.Ink *.wsf *.hta *.mhtml *.html *.html *.doc *.docm *.xls *.xls *.xls *.xls *.xlsm *.ppt *.ppt *.ppt *.pptm *.chm *.vbs *.js *.bat *.pdf *.pdf		
		*.sys		

#### **Defense+ Events**

No default rules for this event category.

#### **Network Events**

No default rules for this event category.

# Appendix 2 - Agent Firewall Ports, IPs and Domains

We can capture DNS queries from network packets with Wireshark, and extract domain information.

Domain	IPs and Ports	Purpose	Miscellaneous
Valkyrie.comodo.com	52.60.56.170:443, 52.60.198.77:443	Valkyrie query and upload	Valkyrie server domain hardcoded
p10.fls.security.comodo.com	199.66.201.16:4448	FLS query	FLS server domain hardcoded
licensing.security.comodo.com	178.255.87.18:443	Register and security logs.	Hardcoded in the code, Wireshark capture traces during installation phase.
cmc.comodo.com	178.255.85.135:443	Acquire Valkyrie encrypted key from server	Hardcoded in the code, Wireshark capture traces during installation phase.
oscp.comodoca.com ocsp.comodoca.com.edgesuite.net	184.50.87.41:443 184.50.87.75:443	Encrypted communications (optional)	Wireshark capture traces during installation phase. Not defined in the solution code.
wtfibam2s5.execute-api.us-west- 2.amazonaws.com	13.33.231.28:443, 13.33.231.89:443, 13.33.231.27:443, 13.33.231.45:443 (variable)	Policy, settings and heartbeat	EDR production server domain hardcoded in solution
6ynhsugqeg.execute-api.us-west- 2.amazonaws.com	13.33.231.65:443, 13.33.231.105:443, 13.33.231.109:443, 13.33.231.39:443 (variable)	Policy, settings and heartbeat	EDR development server domain from edragentsettings.conf
h7tsgu3aej.execute-api.us-west- 2.amazonaws.com	13.33.231.80:443, 13.33.231.90:443, 13.33.231.52:443, 13.33.231.25:443 (variable)	Policy, settings and heartbeat	EDR staging server domain from edragentsettings.conf
firehose.us-west- 2.amazonaws.com	52.119.165.138:443 52.119.162.196:443 52.119.162.43:443	Upload event logs to AWS	SDK encapsulate the domain information. Extract the domain information from Wireshark monitor.



52.119.169.95:443	
52.119.168.237:443 (variable)	

The EDR agent uses port 443 to communicate over HTTPS with all servers *except* the Comodo FLS server, which uses port 4448.

There are only three server communications during installation - licensing.security.comodo.com, cmc.comodo.com, oscp.comodoca.com (ocsp.comodoca.com.edgesuite.net). The oscp.comodoca.com server domain is optional.

## **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