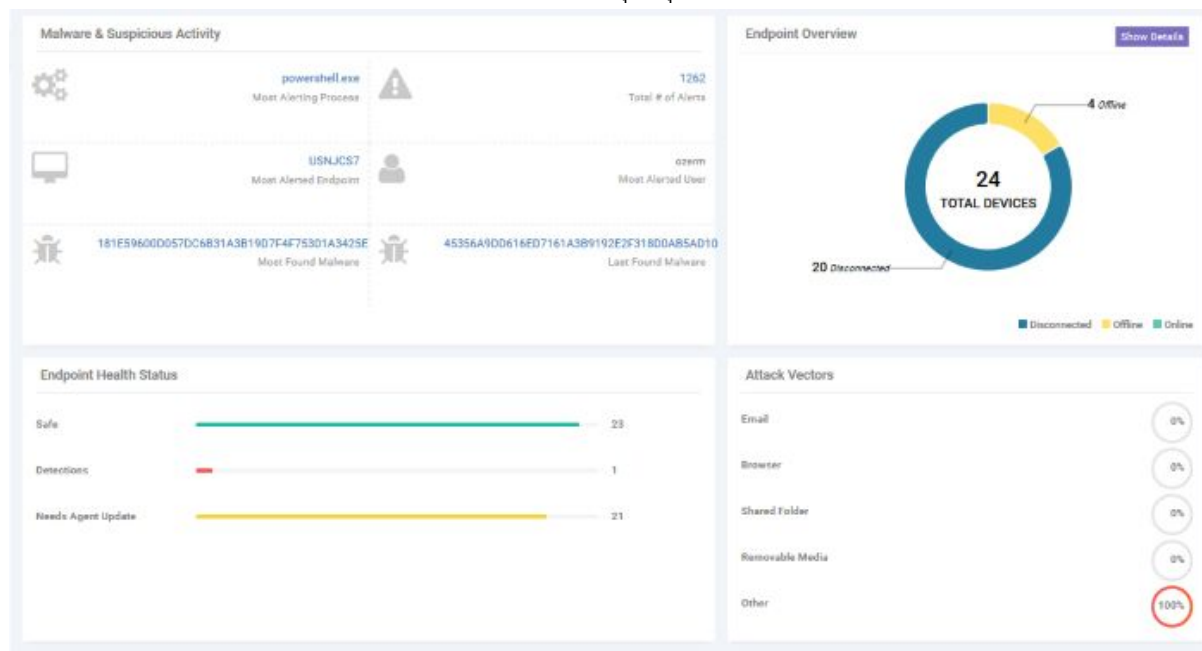


Comodo EDR

Comodo Endpoint Detection and Response (EDR) เป็นเครื่องมือวิเคราะห์เหตุการณ์ให้การตรวจสอบแบบเรียลไทม์ และตรวจจับเหตุการณ์ที่เป็นอันตรายการตรวจจับเหตุการณ์และการตอบสนองช่วยให้คุณเห็นภาพการคุกคามแบบใหม่และแบบละเอียดหากมีการโจมตีจะมีการแจ้งเตือนแบบให้คุณทราบ

Console Comodo EDR เป็นระบบบนคลาวด์สามารถเข้าถึงได้ทุกที่ทุกเวลาโดยใช้อินเทอร์เน็ตเบราว์เซอร์



Admin Console

1. สามารถลงทะเบียนอุปกรณ์ปลายทาง สร้างนโยบายและวิเคราะห์เหตุการณ์และอื่น ๆ
2. สามารถติดตั้ง Agent Comodo EDR บนเครื่องปลายทางทั้งหมดที่คุณต้องการจัดการ โดยการดาวน์โหลด Agent

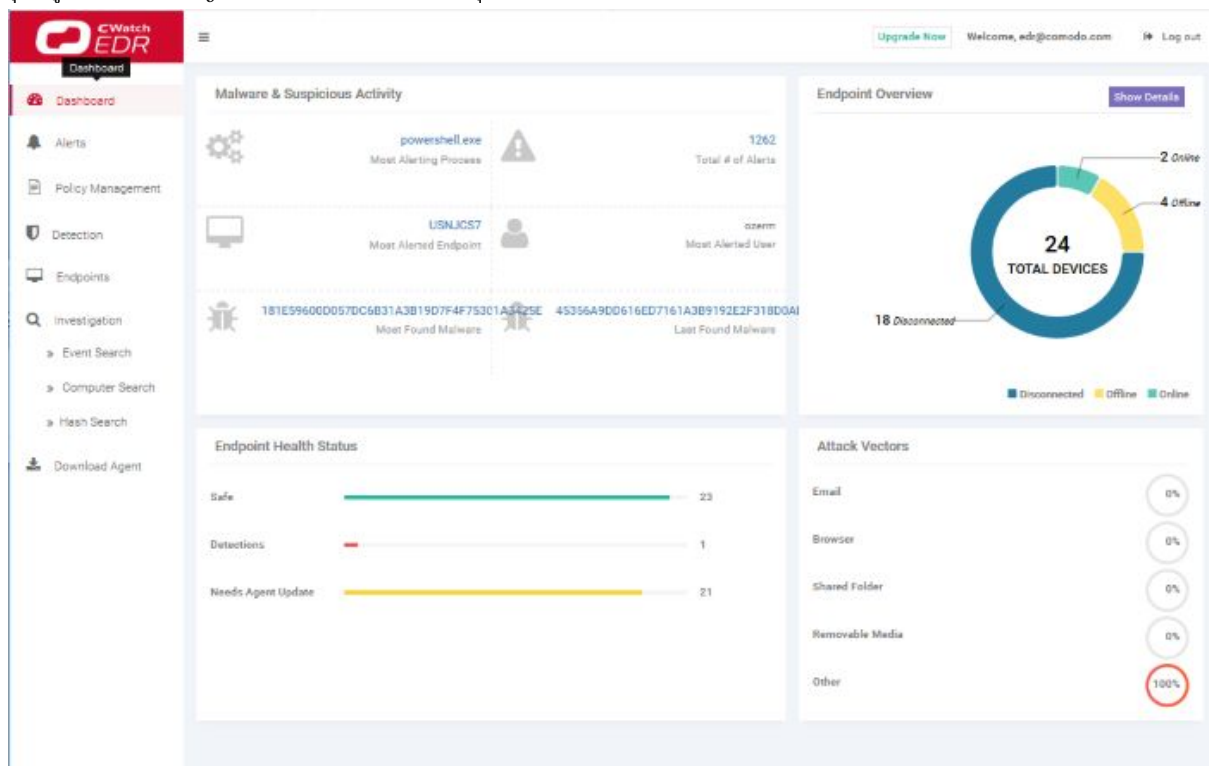
Features

1. Continuous threat monitoring of managed endpoints
การตรวจสอบภัยคุกคามอย่างต่อเนื่องบนเครื่องปลายทาง
2. Advanced search capabilities for file hashes and detection
ความสามารถในการค้นหาขั้นสูง สำหรับการแฮชไฟล์และการตรวจจับ
3. Real-time visibility into what's happening in your environment
การมองเห็นสิ่งที่เกิดขึ้นในสภาพแวดล้อมของคุณแบบเรียลไทม์
4. Policy customization
การปรับแต่งนโยบาย
5. Unrivaled process timeline visualization
กระบวนการสร้างภาพ ข้อมูลกระบวนการ
6. Retrospective analysis of events
การวิเคราะห์เหตุการณ์ย้อนหลัง
7. Centralized cloud hosted architecture
สถาปัตยกรรมโฮสต์บนคลาวด์ส่วนกลาง
8. Human analysis of unknown file and event types
การวิเคราะห์โดยมนุษย์เกี่ยวกับไฟล์ที่ไม่รู้จักและเหตุการณ์
9. Compatible with other endpoint security tool
เข้ากันได้กับเครื่องมือรักษาความปลอดภัยปลายทางอื่น ๆ

The Dashboard

แดชบอร์ดเป็นบทสรุปโดยย่อของความปลอดภัยและสถานะการเชื่อมต่อของจุดสิ้นสุดที่ลงทะเบียนแล้วแดชบอร์ด

แต่ละอันจะแสดงข้อมูลสำคัญเกี่ยวกับมัลแวร์ที่ตรวจพบและช่วยให้คุณสามารถเจาะลึกลงไปในพื้นที่ที่น่าสนใจ สถิติรวมถึงจุดสิ้นสุดที่ถูกโจมตีส่วนใหญ่ปริมาณมัลแวร์ที่พบจำนวนอุปกรณ์ที่ลงทะเบียนเป็นต้น



☰	ขยาย / ยุมเมนูซ้ายมือ
Upgrade Now	<p>ช่วยให้คุณซื้อแผนการสมัครสมาชิกที่สูงขึ้น แผนการที่มีอยู่คือ:</p> <ul style="list-style-type: none"> • พรีเมียม - การเก็บรักษาข้อมูล / ประวัติ 30 วัน • Platinum - การเก็บรักษาข้อมูล / ประวัติ 90 วัน
🚪 Log out	ออกจากระบบของคอนโซลผู้ดูแลระบบ EDR

Malware & Suspicious Activity

1. Most Alerting Process ชื่อของกระบวนการแอปพลิเคชันที่สร้างการแจ้งเตือนส่วนใหญ่ คลิกชื่อกระบวนการเพื่อเปิดอินเทอร์เฟซ 'การแจ้งเตือน' ซึ่งแสดงรายละเอียดเพิ่มเติม ดู 'การแจ้งเตือน' สำหรับข้อมูลเพิ่มเติม
2. Most Alerted Endpoint ชื่อของอุปกรณ์ที่สร้างการแจ้งเตือนได้มากที่สุด คลิกชื่อของจุดสิ้นสุดเพื่อเปิดอินเทอร์เฟซ 'การแจ้งเตือน' ซึ่งแสดงรายละเอียดเพิ่มเติม ดู 'การแจ้งเตือน' สำหรับข้อมูลเพิ่มเติม
3. Most Found Malware

ค่าแฮชของมัลแวร์ที่แพร่หลายมากที่สุดในอุปกรณ์ปลายทางที่คุณจัดการทั้งหมดคลิกที่ค่าแฮชเพื่อดูรายละเอียดมัลแวร์รวมถึงจุดสิ้นสุดที่ทริกเกอร์เหตุการณ์วันที่และเวลาของเหตุการณ์และอื่น ๆ ดู 'HashSearch' สำหรับรายละเอียดเพิ่มเติม

4. Total number of Alerts

จำนวนการแจ้งเตือนทั้งหมดที่สร้างขึ้นสำหรับจุดสิ้นสุดที่ลงทะเบียนไว้ทั้งหมด คลิกหมายเลขการแจ้งเตือนเพื่อเปิดอินเทอร์เฟซ 'การแจ้งเตือน' ดู 'การแจ้งเตือน' สำหรับข้อมูลเพิ่มเติม

5. Most Alerted User

ผู้ใช้อุปกรณ์ที่สร้างการแจ้งเตือนมากที่สุด

6. Last Found Malware

ค่าแฮชของมัลแวร์ที่ตรวจพบล่าสุด คลิกที่ค่าแฮชเพื่อดูรายละเอียดมัลแวร์รวมถึงจุดสิ้นสุดที่ทริกเกอร์เหตุการณ์ วันที่และเวลาของเหตุการณ์และอื่น ๆ ดู 'Hash Search' สำหรับรายละเอียดเพิ่มเติม

Endpoint Overview

1. Total Devices จำนวนจุดสิ้นสุดทั้งหมดที่คุณเพิ่มลงใน EDR
2. Online Devices จำนวนอุปกรณ์ที่ใช้งานในปัจจุบัน
3. Offline Devices จำนวนของจุดปลายที่กำลังปิดและไม่ได้เชื่อมต่อกับ EDR
4. Disconnected Devices อุปกรณ์ที่ลงทะเบียนแล้วซึ่งออกจากระบบ อุปกรณ์ที่ตัดการเชื่อมต่อรวมถึงจุดปลายที่ไม่ได้ปิดอย่างถูกต้องหรือผิดพลาด

Endpoint Health Status

1. Safe จำนวนจุดสิ้นสุดที่ไม่พบกิจกรรมที่เป็นอันตราย
2. Detections จำนวนอุปกรณ์ที่ตรวจพบกิจกรรมที่เป็นอันตรายและน่าสงสัย
3. Needs Agent Update จำนวนของจุดปลายที่ใช้เอเจนต์ EDR รุ่นที่ล้าสมัย การตรวจหาปลายทางและการตอบสนองรองรับการอัปเดตอัตโนมัติ เมื่อใดก็ตามที่ปลายทางที่มีรุ่นตัวแทนที่ล้าสมัยเข้าสู่สถานะออนไลน์จะได้รับการอัปเดตล่าสุด

Attack Vectors ช่องทางที่กิจกรรมที่เป็นอันตรายเกิดขึ้นที่จุดสิ้นสุด

Alerts

การแจ้งเตือนจะถูกสร้างขึ้นเมื่อกิจกรรมในเครือข่ายของคุณตรงกับกฎในนโยบาย EDR ของคุณ ดู 'จัดการนโยบาย EDR' หากคุณต้องการเรียนรู้เกี่ยวกับนโยบายและกฎ

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

Alerts - ตารางคำอธิบาย

Column Header	Description
Score	คะแนนที่คุณตั้งไว้สำหรับเหตุการณ์เมื่อสร้างกฎ คุณสามารถใช้คะแนนระหว่าง 0 ถึง 10 โดยพิจารณาจากความรุนแรงของเหตุการณ์ ดู 'จัดการนโยบาย EDR'
Alert Name	ป้ายกำกับที่คุณให้กับเงื่อนไขเมื่อสร้างกฎ การแจ้งเตือนจะถูกสร้างขึ้นเมื่อมีการทริกเกอร์เงื่อนไขของกฎ ดู 'จัดการนโยบาย EDR'
Alert Time	วันที่และเวลาที่คำเตือนถูกสร้างขึ้น
Process Name	เส้นทางของแอปพลิเคชันที่เกิดขึ้นของเหตุการณ์
Device	ชื่อของจุดปลายที่บันทึกเหตุการณ์
Policy	ชื่อของนโยบายความปลอดภัยที่สร้างการแจ้งเตือน

User Verdict	สถานะที่กำหนดให้กับการแจ้งเตือนโดยผู้ดูแลระบบที่จัดการกับปัญหา ตัวเลือกรวมถึง: False Positive - ผู้ดูแลระบบไม่พิจารณาเหตุการณ์ที่เกิดขึ้นว่าเป็นภัยคุกคามความปลอดภัย True Positive - Admin ยืนยันเหตุการณ์ที่เกิดขึ้น 'จะแนบ' ที่แนบมากับเหตุการณ์ควรเป็นคำตอบที่ต้องการ
Alert Status	ความคืบหน้าของการแจ้งเตือน สถานะรวมถึง: new - งานยังไม่ได้เริ่มแจ้งเตือน In progress - ผู้ดูแลระบบกำลังเข้าร่วมการแจ้งเตือน Resolved - ผู้ดูแลระบบได้ส่งคำตัดสินของการแจ้งเตือน

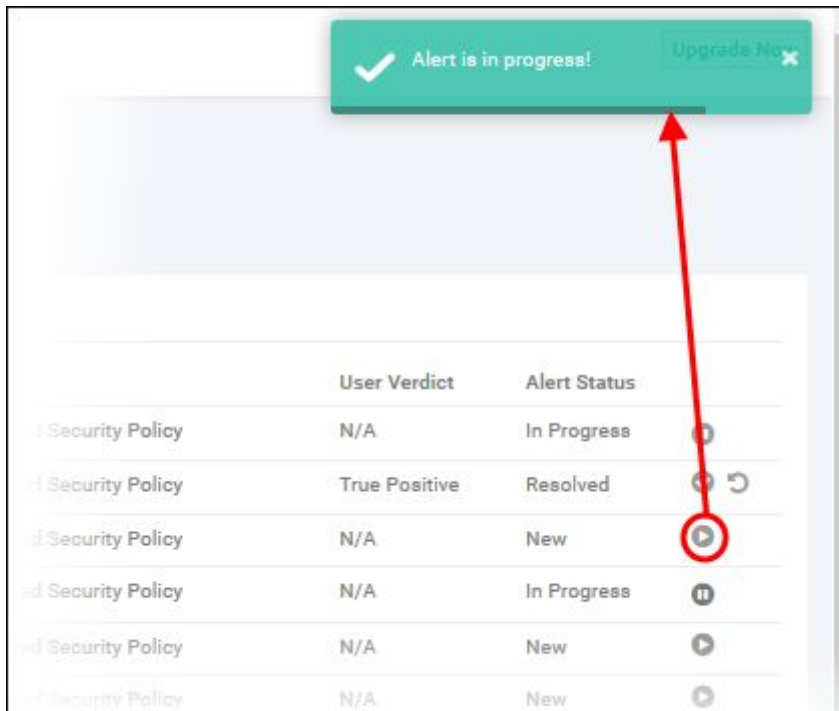
Filter options

คุณสามารถค้นหาการแจ้งเตือนเฉพาะโดยใช้ตัวกรองต่อไปนี้:

- Alert Name – ค้นหาตามป้ายเตือน
- Alert Time – ค้นหาเมื่อสร้างการแจ้งเตือน
- Process Name – ค้นหาตามชื่อกระบวนการ
- Devices – เลือกอุปกรณ์ที่เหตุการณ์เกิดขึ้น
- Policy – กรองตามนโยบายที่เรียกใช้การแจ้งเตือน
- User Verdict – กรองตามสถานะที่ได้รับจากการแจ้งเตือนโดยผู้ดูแลระบบ
- Alert Status – กรองตามระดับความคืบหน้า 3 ระดับ - 'new', 'In progress' หรือ 'Resolved'

คุณสามารถกำหนดค่าตัวกรองหลายตัวเพื่อค้นหาการแจ้งเตือนที่เฉพาะเจาะจง ตัวอย่างเช่นคุณสามารถค้นหาเหตุการณ์ด้วยชื่อการแจ้งเตือนนโยบายและปลายทาง

- คลิก ไอคอนเล่นข้างสถานะการแจ้งเตือน 'ใหม่' เพื่อส่งคำตัดสิน



สถานะการแจ้งเตือนจะเปลี่ยนเป็น 'กำลังดำเนินการ'

- คลิกที่ไอคอนความคืบหน้าเพื่อส่งคำตัดสิน

Change Status for Run Untrusted Executable

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

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

True Positive False Positive

Please give us feedback on this alert. (Optional)

Submit

- คลิก 'ส่ง' เพื่อแก้ไขการแจ้งเตือน
- คลิกไอคอนเปิดใหม่หากคุณต้องการเปลี่ยนคำตัดสิน

Upgrade Now

Apply Clear

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

Are you sure?

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

Yes, reopen it! Cancel

- คลิก 'ใช่เปิดใหม่อีกครั้ง!' เพื่อเปลี่ยนคำตัดสิน
- คลิก 'ยกเลิก' เพื่อไม่เปลี่ยนแปลงคำตัดสิน

View Event Details

คลิก 'แสดงรายละเอียด' ในคอลัมน์ 'คะแนน'

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

เปิดหน้าจอข้อมูลสำหรับเหตุการณ์นั้น:

Explorer.EXE - Write to Infectible File

Alert Time: 2018-11-13 13:18:08 | Policy: Comodo Recommended Security Policy | Computer Name: DESKTOP-11Q2W9R | Operating System: Windows 10 or Later 64 bit platform | Last Seen: 2018-11-14 18:17:02 | SHA1: 27099fbc9067478bb91cdccb92f13a828b00859 | Path: C:\Users\user3\Downloads\pRt4jHhH.exe | Verdict: Malware | User name: user3

Time	Adaptive Event Name	Event Type	Score
13:18:08	Write to Infectible File	Write File	10
13:18:08	Write to Executable	Write File	5

File Trajectory

13 November 2018 | 14 November 2018

DESKTOP-11Q2W9R

Browser Download | Copy From Shared Folder | Copy To Shared Folder | Email Download | Copy From USB Disk | Copy To USB Disk | Write File

Prevent Execution | Alerts | Disinfect

ส่วนบนของหน้าจอแสดงรายละเอียดเช่นชื่อการแจ้งเตือนและแอปพลิเคชันที่สร้างกิจกรรม:

pRt4jHhH.exe - Suspicious System Process Creation

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

Last Seen: 2018-05-24 22:28:59 | Sha1: 27099fbc9067478bb91cdccb92f13a828b00859 | Path: C:\Users\user3\Downloads\pRt4jHhH.exe | Verdict: Malware | User name: user3

- ชื่อการแจ้งเตือนและแอปพลิเคชันจะแสดงที่ด้านบน
- Alert Time - วันที่และเวลาของการแจ้งเตือน
- Policy - ชื่อของนโยบายความปลอดภัย คลิกชื่อของนโยบายเพื่อเปิดหน้าจอการจัดการนโยบาย ดู 'จัดการนโยบาย EDR'
- Computer Name - ชื่อของจุดสิ้นสุดที่บันทึกเหตุการณ์ การคลิกจุดสิ้นสุดจะเป็นการเปิดหน้าจอ 'การค้นหาคอมพิวเตอร์' ด้วยการเลือกจุดสิ้นสุดไว้ล่วงหน้า ดู 'การค้นหาคอมพิวเตอร์'
- operating System - รายละเอียดของระบบปฏิบัติการของอุปกรณ์ปลายทางที่บันทึกเหตุการณ์ไว้

Last Seen - วันที่และเวลาสุดท้ายที่จุดปลายทางสื่อสารกับ EDR

- Sha 1 - ค่าแฮชของไฟล์ การคลิกที่ค่าแฮชจะเปิดหน้าจอ 'ค้นหาแฮช' พร้อมกับไฟล์ที่เลือกไว้ล่วงหน้า ดู 'Hash Search' สำหรับข้อมูลเพิ่มเติม
- Path - เส้นทางกระบวนการทั้งหมดของเหตุการณ์ที่บันทึกไว้ การคลิกที่เส้นทางกระบวนการจะเปิดหน้าจอ 'การค้นหากิจกรรม' ที่มีการเติมข้อความค้นหาเหตุการณ์ในฟิลด์ค้นหาโดยอัตโนมัติ
- Verdict - ผลลัพธ์หลังจากการวิเคราะห์

- User name - ชื่อผู้ใช้ที่ล็อกอินของปลายทาง การคลิกที่ชื่อจะเปิดหน้าจอ 'การค้นหากิจกรรม' ด้วยการเติมคำค้นหาเหตุการณ์ในฟิลด์ค้นหา
- User Verdict - ชื่อสรุปของผู้ดูแลระบบเกี่ยวกับลักษณะของการแจ้งเตือน ตัวเลือกที่ให้ไว้เพื่อประกาศผลลัพธ์คือ 'True Positive' และ False Positive'

Events

รายละเอียดของกิจกรรมจะแสดงในบานหน้าต่างหลัก:

#	Show	Adaptive Event Name	Event Type	Score
+		Suspicious System Process Creation	Create Process	8

ตามคำเริ่มต้น 'มุมมองรายการ' จะปรากฏขึ้น

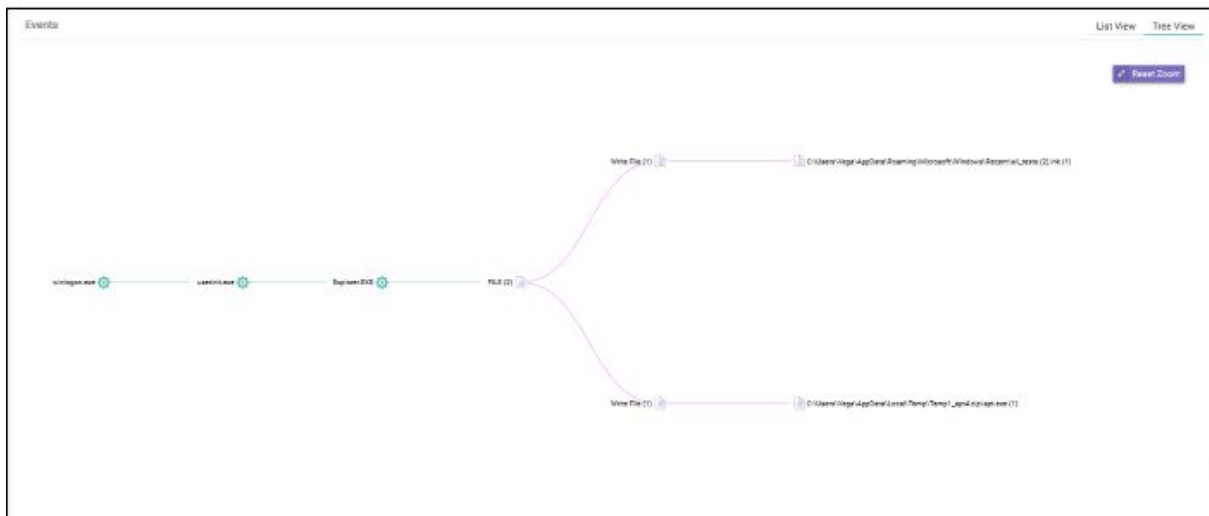
List View

- Show - Click Icon เพื่อดูลำดับเหตุการณ์ ดู 'ระยะเวลาดำเนินการ' สำหรับรายละเอียดเพิ่มเติม
- Adaptive Event Name เลเบลที่กำหนดให้กับเหตุการณ์เมื่อสร้างกฎความปลอดภัย
- Event Type หมวดหมู่ของเหตุการณ์
- Score ความรุนแรงของเหตุการณ์ สิ่งนี้ถูกระบุเมื่อสร้างกฎ
- Click ที่ใดก็ได้ในแถวเพื่อดูฟิลด์กิจกรรมทั้งหมดสำหรับประเภทกิจกรรมนั้น จำนวนฟิลด์กิจกรรมที่แสดงขึ้นอยู่กับประเภทเหตุการณ์:

#	Show	Adaptive Event Name	Event Type	Score																																				
-		Write to Executable File	Write File	8																																				
<table border="1"> <thead> <tr> <th>File Path</th> <th>Process PID</th> <th>Event Type</th> <th>Write File</th> <th>Process PID</th> <th>RAM</th> </tr> </thead> <tbody> <tr> <td>C:\Users\jagpr\AppData\Local\Microsoft\Windows\Recent\... C:\Users\jagpr\AppData\Local\Temp\2154a9c7274813db</td> <td>...</td> <td>Adaptive Event Name</td> <td>Write to Executable File</td> <td>Process User Domain</td> <td>5547D24-77D24F4</td> </tr> <tr> <td>...</td> <td>...</td> <td>Logged On User</td> <td>Write</td> <td>Process Path</td> <td>C:\WINDOWS\system32\cmd.exe</td> </tr> <tr> <td>...</td> <td>...</td> <td>Device Name</td> <td>2688C3A7D0696</td> <td>Process User Name</td> <td>jagpr</td> </tr> <tr> <td>...</td> <td>...</td> <td>Event Time</td> <td>2019-11-13 12:12:52</td> <td>Process Hash</td> <td>409a28049efac030e59f82923a37d5424c7</td> </tr> <tr> <td>...</td> <td>...</td> <td>Event Group</td> <td>FILE (1)</td> <td>Process Creation Time</td> <td>2019-11-12 11:48:26</td> </tr> </tbody> </table>					File Path	Process PID	Event Type	Write File	Process PID	RAM	C:\Users\jagpr\AppData\Local\Microsoft\Windows\Recent\... C:\Users\jagpr\AppData\Local\Temp\2154a9c7274813db	...	Adaptive Event Name	Write to Executable File	Process User Domain	5547D24-77D24F4	Logged On User	Write	Process Path	C:\WINDOWS\system32\cmd.exe	Device Name	2688C3A7D0696	Process User Name	jagpr	Event Time	2019-11-13 12:12:52	Process Hash	409a28049efac030e59f82923a37d5424c7	Event Group	FILE (1)	Process Creation Time	2019-11-12 11:48:26
File Path	Process PID	Event Type	Write File	Process PID	RAM																																			
C:\Users\jagpr\AppData\Local\Microsoft\Windows\Recent\... C:\Users\jagpr\AppData\Local\Temp\2154a9c7274813db	...	Adaptive Event Name	Write to Executable File	Process User Domain	5547D24-77D24F4																																			
...	...	Logged On User	Write	Process Path	C:\WINDOWS\system32\cmd.exe																																			
...	...	Device Name	2688C3A7D0696	Process User Name	jagpr																																			
...	...	Event Time	2019-11-13 12:12:52	Process Hash	409a28049efac030e59f82923a37d5424c7																																			
...	...	Event Group	FILE (1)	Process Creation Time	2019-11-12 11:48:26																																			
+		Write to Executable	Write File	8																																				

Tree View

Click ลิงก์ 'Tree View' ที่ด้านบนขวาของส่วน 'กิจกรรม'




หน้าจอแสดงเส้นทางกระบวนการทั้งหมดของเหตุการณ์ การคลิกที่ป้ายกระบวนการใด ๆ จะเปิดหน้าจอ 'การค้นหากิจกรรม' ที่มี การเติมข้อความค้นหาเหตุการณ์ในฟิลด์ค้นหาโดยอัตโนมัติ

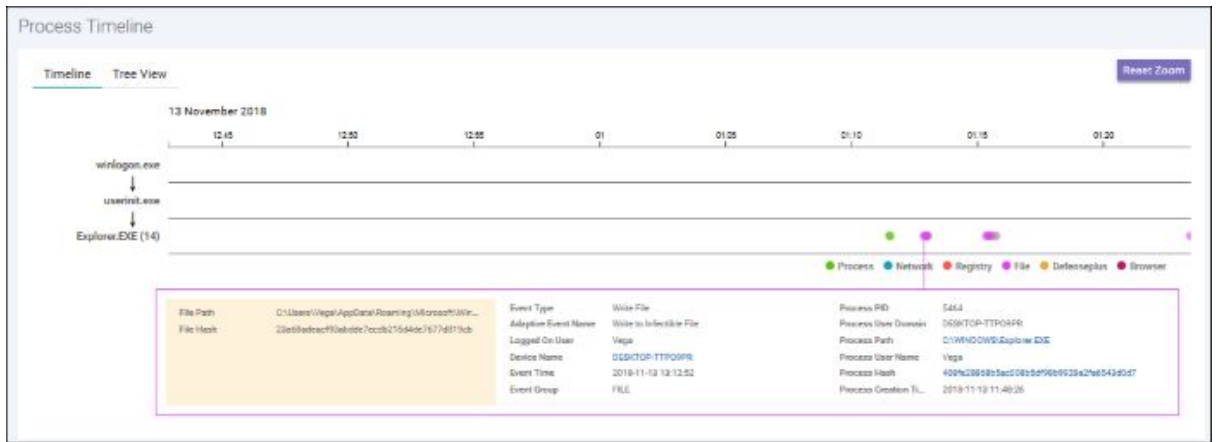
- ซ่อมเข้าหรือซ่อมออกโดยใช้เมาส์ คลิกขวาและเลื่อนแผนภูมิไปทางซ้ายหรือขวา คลิก 'รีเซ็ตการย่อ / ขยาย' เพื่อกลับสู่มุมมองเริ่มต้น

Process Timeline of the Event

แสดงกิจกรรมต่าง ๆ ที่เกิดขึ้นในเหตุการณ์สำหรับไฟล์แต่ละประเภท

Process View

- **Click**  แสดงในไอคอน 'ระยะเวลาดำเนินการ' ของเหตุการณ์



หน้าจอ 'Process Timeline' จะเปิดขึ้น

หน้าจอแสดงเวลาที่เกิดเหตุการณ์แต่ละเหตุการณ์ ดู 'Process Timeline' สำหรับรายละเอียดเพิ่มเติม

Process View

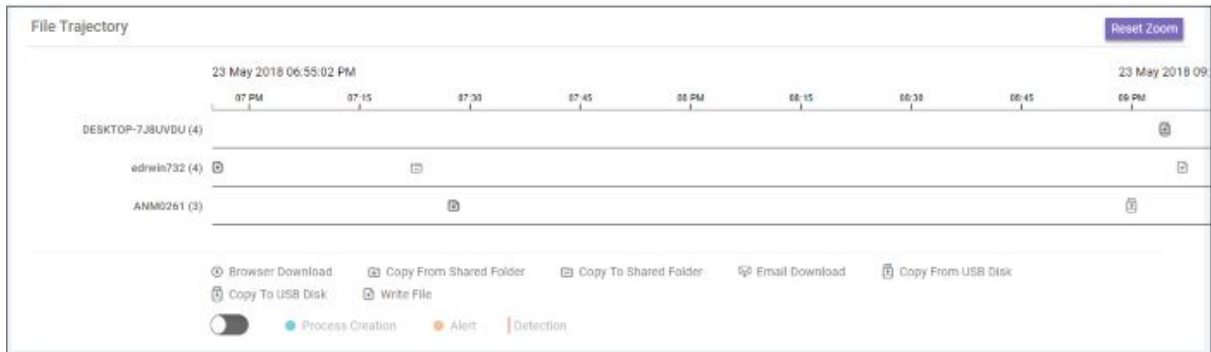
- คลิกที่ไอคอน 'Show in Process Timeline' ของกิจกรรม
- คลิก '**Tree View**'



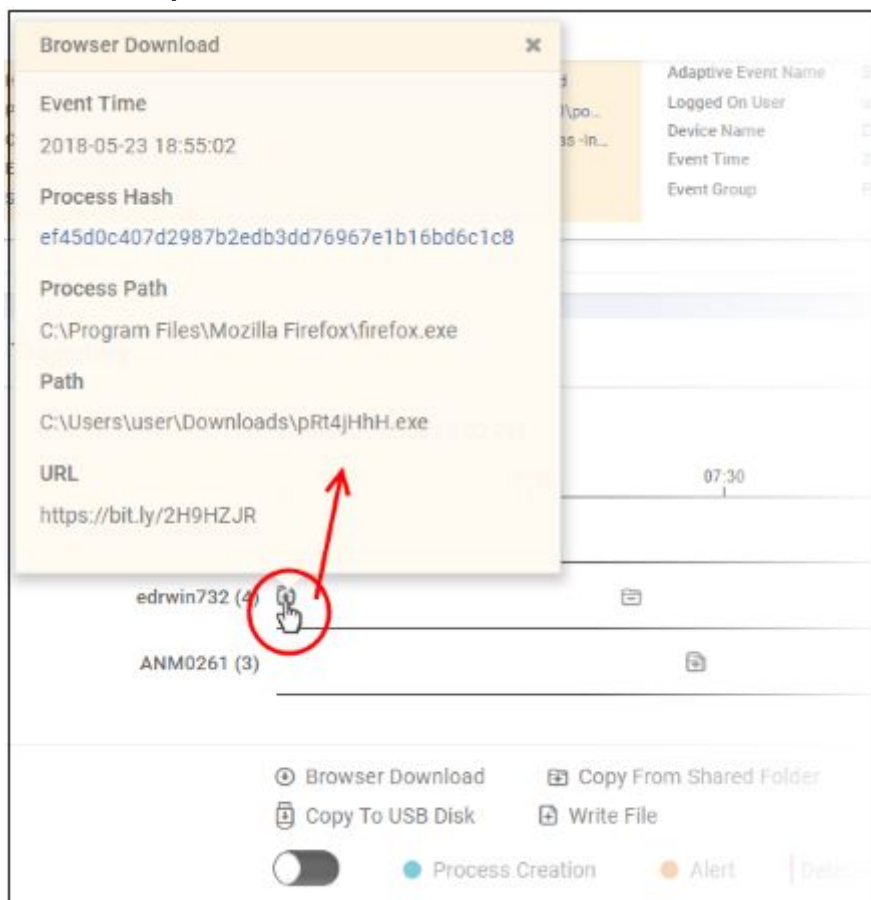
หน้าจอแสดงมุมมองต้นไม้ของเหตุการณ์ที่เกิดขึ้น ดู Process Timeline

File Trajectory

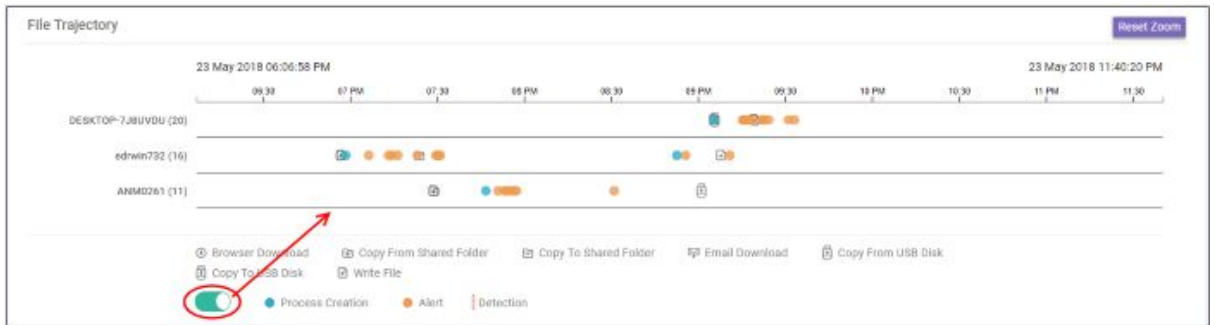
ส่วนด้านล่างของหน้าจะแสดงการเคลื่อนไหวของไฟล์ซึ่งมาจากที่ที่มันถูกดาวน์โหลดไปยังจุดสิ้นสุดและอื่น ๆ



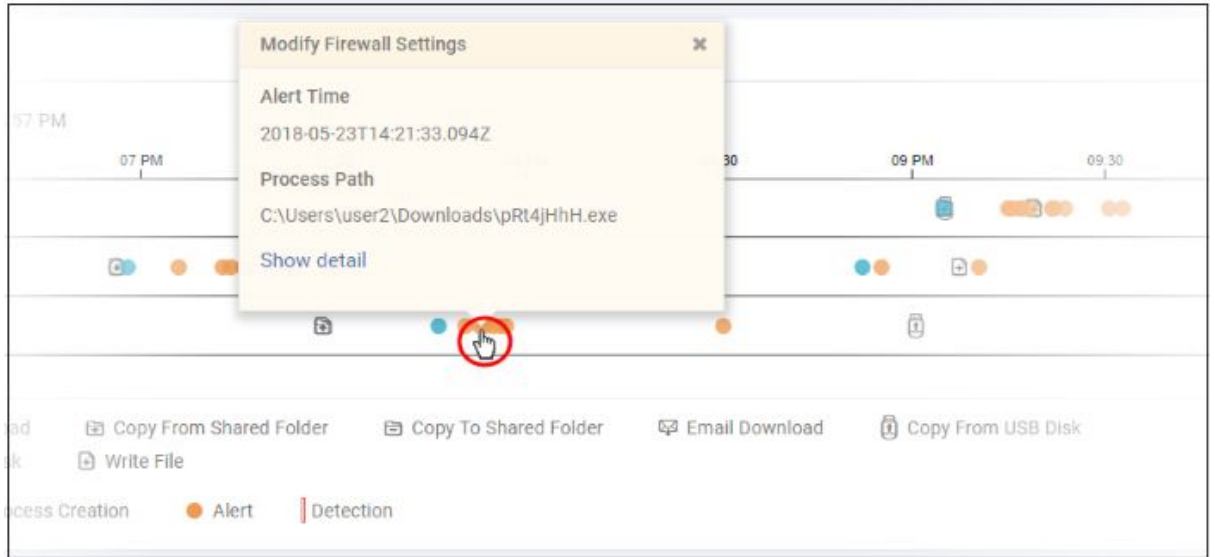
- ซุมเข้าหรือซุมออกโดยใช้เมาส์ คลิกขวาและเลื่อนเมนูไปทางซ้ายหรือขวา คลิก "รีเซ็ตการย่อ / ขยาย" เพื่อกลับสู่มุมมองเริ่มต้น
- รายละเอียดของไอคอนแสดงอยู่ด้านล่างกราฟ
- คลิกที่ไอคอนเพื่อดูรายละเอียดเส้นทาง



- คลิก 'X' เพื่อปิดกล่องโต้ตอบ
- คลิกปุ่ม 'Process Creation' เพื่อดูเวลาของการสร้างกระบวนการตรวจพบเหตุการณ์และสร้างการแจ้งเตือน



- คลิกที่สวิตช์ไอคอนเพื่อดูรายละเอียดเส้นทาง



- ลิงก์ 'แสดงรายละเอียด' จะพร้อมใช้งานสำหรับกล่องโต้ตอบการแจ้งเตือน การคลิกลิงก์จะเปิดหน้าจอรายละเอียดกิจกรรมที่สร้างการแจ้งเตือน
- คลิก 'X' เพื่อปิดกล่องโต้ตอบ

View Enrolled Endpoints

- คลิก 'จุดปลาย' ทางด้านซ้ายเพื่อดูและจัดการจุดปลายทั้งหมดที่คุณเพิ่มลงใน EDR
- รายละเอียดรวมถึงชื่อจุดปลายสถานะการเชื่อมต่อที่อยู่ IP ระบบปฏิบัติการการแจ้งเตือนและอื่น ๆ

#	Endpoint Version	Local IP Address	Computer Name	Operating System	Logged On User	Connection Status	Detection	Last Update Time
1	1.1.250.2	172.17.104.17	ANM0406	Windows 10 or Later 64 bit platform	korayy	Online	No	2018-11-13 18:20:05
2	1.1.250.2	10.104.89.80	USRJCS7	Windows 10 or Later 64 bit platform	ozam	Online	No	2018-11-13 18:15:47
3	1.1.250.2	10.100.130.8	WIN101	Windows 10 or Later 64 bit platform		Disconnected	No	2018-11-13 17:40:32
4	1.1.250.2	10.0.2.15	WIN-91C5LJRR1580	Windows 8 or Later 64 bit platform		Disconnected	No	2018-11-13 18:48:58
5	1.1.250.2	10.100.102.117	AND0414	Windows 10 or Later 64 bit platform		Disconnected	No	2018-11-13 13:07:26
6	1.1.250.2	10.108.51.209	DESKTOP-TTPO3PR	Windows 10 or Later 64 bit platform		Disconnected	No	2018-11-13 11:23:02
7	1.1.250.2	192.168.1.159	OZER-PC	Windows 8 or Later 64 bit platform	Admin1@22r	Disconnected	No	2018-11-12 06:29:41
8	1.1.259.0	192.168.38.130	DESKTOP-AUQ49VH	Windows 10 or Later 64 bit platform	CMD-CHNAGA	Disconnected	Endpoint	2018-10-24 01:14:54
9	1.1.259.0	172.16.223.65	ANM0406	Windows 10 or Later 64 bit platform	korayy	Offline	No	2018-05-16 16:42:13
10	1.1.253.3	127.0.0.1	ANM123	Windows 7 64 bit platform	ysai	Disconnected	No	2018-02-13 21:59:17
11	1.1.253.3	192.168.1.242	WIN-J78DRBTG38J	Windows 10 or Later 64 bit platform	SYSTEM	Disconnected	No	2018-02-08 08:26:43
12	1.1.253.3	10.100.129.141	EDRW08132	Windows 8 or Later	mr	Offline	No	2018-01-19 18:33:38
13	1.1.253.3	10.100.136.238	ANM0189	Windows 10 or Later 64 bit platform	SYSTEM	Offline	No	2018-01-04 18:04:46
14	1.1.253.5	10.100.152.55	AND0623	Windows 10 or Later 64 bit platform	rand	Offline	No	2017-12-22 13:36:17
15	1.1.106.0	10.100.136.226	AND0148	Windows 10 or Later 64 bit platform	SYSTEM	Disconnected	No	2017-10-16 21:29:25
16	1.1.253.0	10.100.132.170	ANM0133	Windows 10 or Later 64 bit platform	SYSTEM	Disconnected	No	2017-09-27 18:51:58
17	1.1.106.0	192.168.1.151	ANM0091	Windows 7 64 bit platform	SYSTEM	Disconnected	No	2017-09-18 03:10:02
18	1.1.106.0	10.100.136.136	AND0013	Windows 10 or Later 64 bit platform	SYSTEM	Disconnected	No	2017-09-13 20:58:05

Endpoints - Table of Column Descriptions	
Column Header	Description
Endpoint Version	หมายเลขเวอร์ชันของเอเจนต์ EDR
Local IP Address	ที่อยู่ IP ภายในของจุดสิ้นสุด
Computer Name	ฉลากจุดสิ้นสุด คลิกชื่อนี้เพื่อดูเหตุการณ์ในจุดสิ้นสุด ดู 'การค้นหาคอมพิวเตอร์' สำหรับข้อมูลเพิ่มเติม
Operating System	ระบบปฏิบัติการของอุปกรณ์ปลายทาง
Logged On User	ผู้ใช้ที่ใช้งานเครื่องอยู่ในขณะนี้
Connection Status	ปลายทางเชื่อมต่อกับ EDR หรือไม่
Detection	จุดสิ้นสุดหรือไม่ว่ามีเหตุการณ์ที่เป็นอันตรายหรือไม่ <ul style="list-style-type: none"> • แดชบอร์ดหมายถึงถึงเหตุการณ์มีลแวร์ • คลิก 'ระบุสัญญาณเตือน' เพื่อลบการแจ้งเตือน คุณอาจต้องการทำเช่นนี้หากกิจกรรมได้รับการจัดการและไม่มีข้อกังวลอีกต่อไป

Last Update Time	อัปเดตล่าสุดที่ส่งจากเอเจนต์ endpoint ไปยังคอนโซล EDR

- ใช้ข้อมูลค้นหาบนตารางเพื่อค้นหารายการเฉพาะ คุณสามารถกรองตามเวอร์ชันตัวแทน, IP ที่ท้องถิ่น, ผู้ใช้ที่ใช้งาน, ชื่อคอมพิวเตอร์และสถานะการเชื่อมต่อ
- ล้างข้อมูลเพื่อดูรายการทั้งหมดอีกครั้ง

Default Comodo Security Policy Details

นโยบาย EDR กำหนดกิจกรรมที่จะสร้างการแจ้งเตือน ตารางด้านล่างประกอบด้วยรายละเอียดของกฎเริ่มต้นในแต่ละประเภทกิจกรรม

The built-in event categories are:

- Process Events -กฎเพื่อสร้างการแจ้งเตือนหากแอปพลิเคชันทำให้เกิดเหตุการณ์
- Registry Events -กฎเพื่อแจ้งเตือนคุณเกี่ยวกับการเปลี่ยนแปลงในรีจิสทรีของ Windows ที่จุดสิ้นสุดของคุณ
- File Events -กฎที่ตรวจพบการแก้ไขไฟล์และไฟล์เดอรับบบใด ๆ
- Download Events -กฎเพื่อสร้างการแจ้งเตือนเมื่อมีการดาวน์โหลดแอปพลิเคชันผ่านเบราว์เซอร์
- Upload Events -กฎที่จะเตือนคุณเกี่ยวกับการอัปโหลดไฟล์ไปยังไฟล์เดอรับบบที่แชร์หรือไดรฟ์ภายนอก
- Defense+ Events -ไม่มีการตั้งค่ากฎเริ่มต้นสำหรับหมวดหมู่กิจกรรมนี้
- Network Events -ไม่มีการตั้งค่ากฎเริ่มต้นสำหรับหมวดหมู่กิจกรรมนี้

Process Events

Event Category – Process Events		
Event Type – Create 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 *wsmpvhost.exe
Suspicious Powershell Flag	5	Command line matches any of the following: *powershell*-NoP* *powershell*-Win* *powershell*-w* *powershell*-Exec* *powershell*-ex* *powershell*-ep* *powershell*-command* *powershell*-NoL* *powershell*-InputFormat* *powershell*-Enc* *powershell*-NonInteractive* *powershell*-nonI* *powershell*-file*
Stop Service	5	Command line matches %systemroot%system32net*stop*.
Run Untrusted Executable	4	Verdict is not safe.
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%system32net*start*.

Registry Events

Event Category – Registry Events		
Event Type – Set Registry Value		
Event Name	Score	Description
Disable User Account Control	9	Registry key path is equal to HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System 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_USERSOFTWARE\Microsoft\Windows\CurrentVersion\Policies\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 ServiceDll 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\PowerShell1\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\Parameters\FirewallPolicy\StandardProfile*
Disable Registry Editing Tool	6	Registry key path is equal to HKEY_CURRENT_USERSOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System AND registry value name is equal to DisableRegistryTools AND registry value data is equal to 1.

Modify Applnit_DLLs in Registry	6	Registry key path is equal to HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows AND registry value name is equal to Applnit_DLLs
Add Service	6	Registry key path matches HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services* AND registry value name is equal to ImagePath AND registry value data matches *.exe* AND registry value data doesn't match *svchost.exe*
Layered Service Provider installation	6	Registry key path matches HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries*
Add Autorun In Registry	5	Registry key path matches any of the following: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\System\Scripts\Startup* HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System\Scripts\Logon* HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System* HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx* HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce* HKEY_CURRENT_USER\Software\Microsoft\Windows\NT\CurrentVersion\Windows* HKEY_CURRENT_USER\Software\Microsoft\Windows\NT\CurrentVersion\WindowsRun* HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\ExplorerRun* HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\ExplorerRun* HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System\Scripts\Logoff* HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\System\Scripts\Shutdown* OR Registry key path equals any of the following: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
Booting Time Execution	5	Registry key path is equal to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager AND registry value name is equal to BootExecute
Disable Auto Update	5	Registry key path is equal to HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU AND registry value name is equal to NoAutoUpdate AND registry value data is equal to 1 OR Registry key path is equal to 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\WindowsUpdate AND registry value name is equal to DisableWindowsUpdateAccess AND registry value data is equal to 1

Disable Service	5	<p>Registry key path matches HKEY_LOCAL_MACHINESystemCurrentControlSetServices* AND registry value name is equal to Start AND registry value data is equal to 4</p>
Create Explorer Entry	5	<p>Registry key path matches any of the following: HKEY_LOCAL_MACHINESOFTWAREClassesPROTOCOLSFilter* HKEY_LOCAL_MACHINESOFTWAREClassesPROTOCOLSHandler* HKEY_CURRENT_USERSOFTWAREMicrosoftInternet ExplorerDesktopComponents* HKEY_LOCAL_MACHINESOFTWAREMicrosoftActive SetupInstalled Components* HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionShellServiceObjectDelayLoad* HKEY_CURRENT_USERSOFTWAREMicrosoftWindowsCurrentVersionShellServiceObjectDelayLoad* HKEY_LOCAL_MACHINESoftwareMicrosoftWindowsCurrentVersionExplorerShellExecuteHooks* HKEY_CURRENT_USERSoftwareClasses*ShellExContextMenuHandlers* HKEY_LOCAL_MACHINESoftwareClasses*ShellExContextMenuHandlers* HKEY_CURRENT_USERSoftwareClassesAllFileSystemObjectsShellExContextMenuHandlers* HKEY_LOCAL_MACHINESoftwareClassesAllFileSystemObjectsShellExContextMenuHandlers* HKEY_CURRENT_USERSoftwareClassesDirectoryShellExContextMenuHandlers* HKEY_LOCAL_MACHINESoftwareClassesDirectoryShellExContextMenuHandlers* HKEY_CURRENT_USERSoftwareClassesDirectoryShellExDragDropHandlers* HKEY_LOCAL_MACHINESoftwareClassesDirectoryShellExDragDropHandlers* HKEY_CURRENT_USERSoftwareClassesDirectoryShellExPropertySheetHandlers* HKEY_LOCAL_MACHINESoftwareClassesDirectoryShellExPropertySheetHandlers* HKEY_CURRENT_USERSoftwareClassesDirectoryShellExCopyHookHandlers* HKEY_LOCAL_MACHINESoftwareClassesDirectoryShellExCopyHookHandlers* HKEY_CURRENT_USERSoftwareClassesFolderShellExColumnHandlers* HKEY_LOCAL_MACHINESoftwareClassesFolderShellExColumnHandlers* HKEY_CURRENT_USERSoftwareClassesFolderShellExContextMenuHandlers* HKEY_LOCAL_MACHINESoftwareClassesFolderShellExContextMenuHandlers* HKEY_CURRENT_USERSoftwareClassesDirectoryBackgroundShellExContextMenuHandlers* HKEY_LOCAL_MACHINESoftwareClassesDirectoryBackgroundShellExContextMenuHandlers* HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionExplorerShellIconOverlayIdentifiers* HKEY_LOCAL_MACHINESoftwareMicrosoftWindowsCurrentVersionExplorerShellIconOverlayIdentifiers* HKEY_CURRENT_USERSoftwareMicrosoftCtfLangBarAddin* HKEY_LOCAL_MACHINESoftwareMicrosoftCtfLangBarAddin* HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionShellExtensionsApproved* HKEY_LOCAL_MACHINESoftwareMicrosoftWindowsCurrentVersionShellExtensionsApproved* OR Registry key path is equal to HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionExplorerSharedTaskScheduler</p>

Disable Windows Application	5	Registry key path is equal to HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionPoliciesExplorerDisallowRun
Disable Command Prompt	5	Registry key path is equal to HKEY_CURRENT_USERSoftwarePoliciesMicrosoftWindowsSystem 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_USERSoftwareMicrosoftWindowsCurrentVersionExplorerAdvanced 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_MACHINESYSTEMCurrentControlSetServicesLanmanserverShares
Addition of DNS Server	3	Registry key path matches HKEY_LOCAL_MACHINESYSTEMCurrentControlSetServicesTcpipParametersInterfaces* AND registry value name is equal to NameServer
Modify Hosts File Registry	3	Registry key path is equal HKEY_LOCAL_MACHINESYSTEMCurrentControlSetServicesTcpipParameters 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%System32Tasks* 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%MicrosoftWindowsStart MenuProgramsStartup* %programdata%MicrosoftWindowsStart MenuProgramsStartup* %systemroot%systemiosubsys* %systemroot%systemvmm32* %systemroot%Tasks* OR File path equals any of the following: %systemdrive%autoexec.bat %systemdrive%config.sys %systemroot%wininit.ini %systemroot%winstart.bat %systemroot%win.ini %systemroot%system.ini %systemroot%dosstart.bat
Modify Host File	4	File path is equal to %systemroot%system32driversetchosts
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 *.mhtml *.html *.doc *.docm *.xls *.xlsm *.ppt *.pptm *.chm *.vbs *.js *.bat *.pif *.pdf *.jar *.sys

Modify Group Policy Settings	1	File path matches %systemroot%system32grouppolicy* OR %systemroot%Sysvolsysvol*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	<p>File path matches any of the following:</p> <ul style="list-style-type: none"> *.lnk *.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
Write Infectible to Shared Folder	5	File path matches any of the following: *.lnk *.wsf *.hta *.mhtml *.html *.doc *.docm *.xls *.xlsm *.ppt *.pptm *.chm *.vbs *.js *.bat *.pif *.pdf *.jar *.sys