



ที่ สก ๐๐๑๙/ว๖๕๕๖

ศาลากลางจังหวัดสระแก้ว  
ถนนสุวรรณศรี สก ๒๗๐๐๐

๑๙ เมษายน ๒๕๖๖

เรื่อง การดำเนินงานโครงการระบบรักษาความปลอดภัยคอมพิวเตอร์แม่ข่ายและคอมพิวเตอร์ลูกข่าย (Antivirus) ปีงบประมาณ พ.ศ. ๒๕๖๖

เรียน นายอำเภอ ทุกอำเภอ

สิ่งที่ส่งมาด้วย	๑. คู่มือการติดตั้งและใช้งานโปรแกรม ESET Endpoint Security	จำนวน ๑ ชุด
	๒. ข้อมูลการตั้งชื่อเครื่องคอมพิวเตอร์	จำนวน ๑ ฉบับ
	๓. แบบรายงานทะเบียนข้อมูลคอมพิวเตอร์	จำนวน ๑ ฉบับ

ด้วย กรมการพัฒนาชุมชน ได้ดำเนินงานโครงการระบบรักษาความปลอดภัยคอมพิวเตอร์แม่ข่ายและคอมพิวเตอร์ลูกข่าย (Antivirus) ปีงบประมาณ พ.ศ. ๒๕๖๖ โดยจัดซื้อซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์ที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย และสามารถป้องกันไวรัสคอมพิวเตอร์ได้อย่างมีประสิทธิภาพ สำหรับรักษาความมั่นคงปลอดภัยคอมพิวเตอร์แม่ข่ายและคอมพิวเตอร์ลูกข่าย รวมทั้งป้องกันความเสียหายหรือการสูญหายของข้อมูลสารสนเทศจากภัยคุกคามต่าง ๆ และโปรแกรมที่ไม่พึงประสงค์ให้กับเครื่องคอมพิวเตอร์ของหน่วยงาน

เพื่อให้การดำเนินการดังกล่าวเป็นไปด้วยความเรียบร้อย จังหวัดสระแก้วขอให้อำเภอ มอบหมายสำนักงานพัฒนาชุมชนอำเภอ ดำเนินการ ดังนี้

๑. ศึกษาคู่มือการติดตั้งและใช้งานโปรแกรมป้องกันไวรัสคอมพิวเตอร์ ESET Endpoint Security เวอร์ชัน ๙.๐ และ ๑๐

๒. ตั้งชื่อคอมพิวเตอร์ (Computer Name) และกำหนดเวิร์กกรุป (Workgroup) ตามแนวทางที่กรมฯ กำหนด

๓. จัดทำทะเบียนเครื่องคอมพิวเตอร์และติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ ESET Endpoint Security ตามแนวทางที่กรมฯ กำหนด รายงานให้จังหวัดทราบภายในวันที่ ๒๗ เมษายน ๒๕๖๖

สามารถศึกษาคู่มือการติดตั้งและใช้งานโปรแกรมป้องกันไวรัสคอมพิวเตอร์ ESET Endpoint Security ประจำปี ๒๕๖๖ โดยดาวนโหลดคู่มือฯ ได้ที่เว็บไซต์ [sakaao.cdd.go.th](http://sakaao.cdd.go.th) หัวข้อคู่มือสำหรับเจ้าหน้าที่ ทั้งนี้มอบหมายให้นางสาวสุจินดา แก้วอำไพ ตำแหน่งนักวิชาการพัฒนาชุมชนชำนาญการ หมายเลขโทรศัพท์ ๐๘๘-๒๕๑๙๔๑๔ เป็นผู้ประสานงาน

จึงเรียนมาเพื่อพิจารณาดำเนินการ

ขอแสดงความนับถือ

(นายสุชาติ ภัคพานิชย์)  
พัฒนาการจังหวัด ปฏิบัติราชการแทน  
ผู้ว่าราชการจังหวัดสระแก้ว

สำนักงานพัฒนาชุมชนจังหวัด  
กลุ่มงานสารสนเทศการพัฒนาชุมชน  
โทร./โทรสาร. ๐-๓๗๔๒-๕๐๕๗-๘

ข้อมูลการตั้งชื่อเครื่องคอมพิวเตอร์ (Computer Name) และกำหนดเวิร์กกรุป (Workgroup)

สำนักงานพัฒนาชุมชนอำเภอ สังกัดสำนักงานพัฒนาชุมชนจังหวัดสระแก้ว

ที่	อำเภอ	ชื่อเครื่องคอมพิวเตอร์		เวิร์กกรุป (Workgroup)
		ภาษาไทย	ภาษาอังกฤษ	
1	เมืองสระแก้ว	สก_6201	SKW_6201	CDDSAKAO
2	คลองหาด	สก_6202	SKW_6202	CDDSAKAO
3	ตาพระยา	สก_6203	SKW_6203	CDDSAKAO
4	วังน้ำเย็น	สก_6204	SKW_6204	CDDSAKAO
5	วัฒนานคร	สก_6205	SKW_6205	CDDSAKAO
6	อรัญประเทศ	สก_6206	SKW_6206	CDDSAKAO
7	เขาฉกรรจ์	สก_6207	SKW_6207	CDDSAKAO
8	โคกสูง	สก_6208	SKW_6208	CDDSAKAO
9	วังสมบูรณ์	สก_6209	SKW_6209	CDDSAKAO

หมายเหตุ

สำหรับอำเภอให้ใช้รหัสตามพื้นที่การจัดเก็บข้อมูล จปฐ. หรือดูจากรหัสเลขหนังสือของอำเภอ 2 ตัวแรก เช่น อำเภอเมืองสระแก้ว รหัสอำเภอเมืองฯ 01 ชื่อเครื่องคอมพิวเตอร์ คือ สก\_620101 หรือ SKW\_620101 (ส่วนเลข 01 (2ตัวหลัง)) คือการเรียงลำดับเครื่องคอมพิวเตอร์

ความหมายของชื่อเครื่องคอมพิวเตอร์

สก\_620101

สก\_62 = ชื่อย่อภาษาไทยและรหัสจังหวัด

01 = รหัสอำเภอ

01 = ลำดับเครื่องคอมพิวเตอร์ใน สพอ.

SKW\_620101

SKW\_62 = ชื่อย่อภาษาอังกฤษและรหัสจังหวัด

01 = รหัสอำเภอ

01 = ลำดับเครื่องคอมพิวเตอร์ใน สพอ.



1331



ศาลากลางจังหวัดสระแก้ว
เลขรับที่..... 5447
วันที่..... 3 เม.ย. 2566
เวลา..... น.

ที่ มท ๐๔๐๕.๕/ว ๑๓๓/๗

กรมการพัฒนาชุมชนพัฒนาชุมชนจังหวัดสระแก้ว  
 ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา 1331  
 ๕ ธันวาคม ๒๕๕๐ อาคารรัฐประศาสนภักดี  
 ถนนแจ้งวัฒนะ เขตหลักสี่ กทม. ๑๐๒๑๐

๓๑ มีนาคม ๒๕๖๖

เวลา.....

อ.  ย.  ส.  สท

เรื่อง การดำเนินงานโครงการระบบรักษาความปลอดภัยคอมพิวเตอร์แม่ข่ายและคอมพิวเตอร์ลูกข่าย (Antivirus) ปีงบประมาณ พ.ศ. ๒๕๖๖

เรียน ผู้ว่าราชการจังหวัด ทุกจังหวัด

- |                                      |              |
|--------------------------------------|--------------|
| สิ่งที่ส่งมาด้วย ๑. กำหนดการฝึกอบรมฯ | จำนวน ๑ ฉบับ |
| ๒. แผนสนับสนุนการติดตั้งโปรแกรมฯ     | จำนวน ๑ ชุด  |

ด้วยกรมการพัฒนาชุมชน ได้ดำเนินงานโครงการระบบรักษาความปลอดภัยคอมพิวเตอร์แม่ข่ายและคอมพิวเตอร์ลูกข่าย (Antivirus) ปีงบประมาณ พ.ศ. ๒๕๖๖ โดยจัดซื้อซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์ที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย และสามารถป้องกันไวรัสคอมพิวเตอร์ได้อย่างมีประสิทธิภาพ สำหรับรักษาความมั่นคงปลอดภัยให้กับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่าย รวมทั้งป้องกันความเสียหายหรือการสูญหายของข้อมูลสารสนเทศจากภัยคุกคามต่าง ๆ และโปรแกรมที่ไม่พึงประสงค์ ให้กับเครื่องคอมพิวเตอร์ของหน่วยงานส่วนกลางและส่วนภูมิภาค โดยมีบริษัท ณะณิชา ดีไซน์ จำกัด เป็นคู่สัญญา กับกรมการพัฒนาชุมชน

เพื่อให้การดำเนินงานโครงการฯ เป็นไปด้วยความเรียบร้อยและบรรลุตามวัตถุประสงค์ รวมทั้งบุคลากรกรมการพัฒนาชุมชนมีความเข้าใจแนวทางการดำเนินงานโครงการฯ กรมการพัฒนาชุมชน จึงขอให้จังหวัดแจ้งสำนักงานพัฒนาชุมชนจังหวัด มอบหมายเจ้าหน้าที่ผู้รับผิดชอบงานด้านเทคโนโลยีสารสนเทศระดับจังหวัด จำนวน ๑ คน เข้าร่วมการฝึกอบรมให้ความรู้เกี่ยวกับระบบรักษาความปลอดภัยคอมพิวเตอร์แม่ข่ายและคอมพิวเตอร์ลูกข่าย (Antivirus) ปีงบประมาณ พ.ศ. ๒๕๖๖ ในวันพุธที่ ๕ เมษายน ๒๕๖๖ เวลา ๐๙.๐๐ - ๑๖.๐๐ น. ผ่านระบบการประชุมวีดิทัศน์ทางไกล (Video Conference) และอำนวยความสะดวกในการติดตั้งโปรแกรมป้องกันไวรัส (Remote Support) ตามแผนสนับสนุนการติดตั้งโปรแกรมฯ รายละเอียดตามสิ่งที่ส่งมาด้วย ทั้งนี้ กรมการพัฒนาชุมชนมอบหมายให้นางสาวอัจฉริย์ มานะกิจ ตำแหน่งนักวิชาการพัฒนาชุมชนชำนาญการ หมายเลขโทรศัพท์ ๐ ๒๑๔๑ ๓๐๕๗ เป็นผู้ประสานงาน

จึงเรียนมาเพื่อโปรดพิจารณาดำเนินการต่อไป

ขอแสดงความนับถือ

(นายชูชีพ พงษ์ไชย)

รองอธิบดี ปฏิบัติราชการแทน  
อธิบดีกรมการพัฒนาชุมชน

ศูนย์สารสนเทศเพื่อการพัฒนาชุมชน

กลุ่มงานพัฒนาระบบเทคโนโลยีสารสนเทศ

โทร. ๐ ๒๑๔๑ ๖๒๘๒ / โทรสาร ๐ ๒๑๔๓ ๘๙๒๑

ไปรษณีย์อิเล็กทรอนิกส์ saraban@cdd.mail.go.th

## กำหนดการ

ฝึกอบรมให้ความรู้เกี่ยวกับการใช้งานระบบรักษาความปลอดภัยคอมพิวเตอร์แม่ข่าย  
และคอมพิวเตอร์ลูกข่าย (Antivirus) ปีงบประมาณ พ.ศ. ๒๕๖๖  
ผ่านระบบการประชุมวิดีโอทัศนังทางไกล (Video Conference) และ ทีวี พช.  
วันพุธที่ ๕ เมษายน ๒๕๖๖ เวลา ๐๙.๐๐ - ๑๖.๐๐ น.

- |                       |   |
|-----------------------|---|
| เวลา ๐๘.๓๐ - ๐๙.๐๐ น. | - เตรียมระบบการประชุมวิดีโอทัศนังทางไกล (Video Conference)  |
| เวลา ๐๙.๐๐ - ๐๙.๑๕ น. | - กล่าวเปิดการฝึกอบรมฯ<br>โดย ผู้อำนวยการศูนย์สารสนเทศเพื่อการพัฒนาชุมชน  |
| เวลา ๐๙.๑๕ - ๐๙.๓๐ น. | - โครงการระบบรักษาความปลอดภัยคอมพิวเตอร์แม่ข่าย<br>และคอมพิวเตอร์ลูกข่าย (Antivirus) ปีงบประมาณ พ.ศ. ๒๕๖๖<br>โดย ผู้อำนวยการกลุ่มงานพัฒนาระบบเทคโนโลยีสารสนเทศ  |
| เวลา ๐๙.๓๐ - ๑๒.๐๐ น. | - ฝึกอบรมให้ความรู้เกี่ยวกับการใช้งานระบบรักษาความปลอดภัยคอมพิวเตอร์<br>แม่ข่ายและคอมพิวเตอร์ลูกข่าย (Antivirus) ปีงบประมาณ พ.ศ. ๒๕๖๖<br>โดย เจ้าหน้าที่บริษัท ณะณิษา ดีไซน์ จำกัด (บริษัทคู่สัญญา)       |
| เวลา ๑๒.๐๐ - ๑๓.๐๐ น. | - พักรับประทานอาหาร   |
| เวลา ๑๓.๐๐ - ๑๖.๐๐ น. | - ฝึกอบรมให้ความรู้เกี่ยวกับการใช้งานระบบรักษาความปลอดภัยคอมพิวเตอร์<br>แม่ข่ายและคอมพิวเตอร์ลูกข่าย (Antivirus) ปีงบประมาณ พ.ศ. ๒๕๖๖<br>โดย เจ้าหน้าที่บริษัท ณะณิษา ดีไซน์ จำกัด (บริษัทคู่สัญญา) (ต่อ) |
|                       | - ถาม/ตอบข้อซักถาม  |

**กลุ่มเป้าหมาย :** เจ้าหน้าที่ผู้รับผิดชอบงานด้านเทคโนโลยีสารสนเทศระดับจังหวัด ศูนย์ศึกษาและพัฒนาชุมชน  
วิทยาลัยการพัฒนารัฐบาล และส่วนกลาง กรมการพัฒนารัฐบาล



## สารบัญ

เรื่อง	หน้า
วิธีการใช้งาน ESET PROTECT	
๑. การเข้าเว็บไซต์	๑
๒. การเข้าใช้งาน (Login) การกรอก User และ Password	๒
๓. หน้า Dashboard สำหรับตรวจสอบสถานะเครื่องคอมพิวเตอร์แบบเรียลไทม์	๒
๔. การตรวจสอบสถานะเครื่องคอมพิวเตอร์	๖
๕. การตรวจสอบเครื่องคอมพิวเตอร์ที่ผิดปกติหรือมีปัญหา	๑๐
๖. การสั่งสแกนเครื่องคอมพิวเตอร์	๑๒
๗. การ Update Modules	๑๓
๘. การเรียกดูเครื่องคอมพิวเตอร์ที่มีรายงานตัวในระบบ Web Console	๑๔
๙. การตรวจสอบเมนู Detections	๑๖
๑๐. การเลือกช่วงเวลาที่จะตรวจสอบไวรัสบนเครื่องคอมพิวเตอร์ในแต่ละ Group	๑๖
๑๑. การแสดงรายงานเมนู Report	๑๗

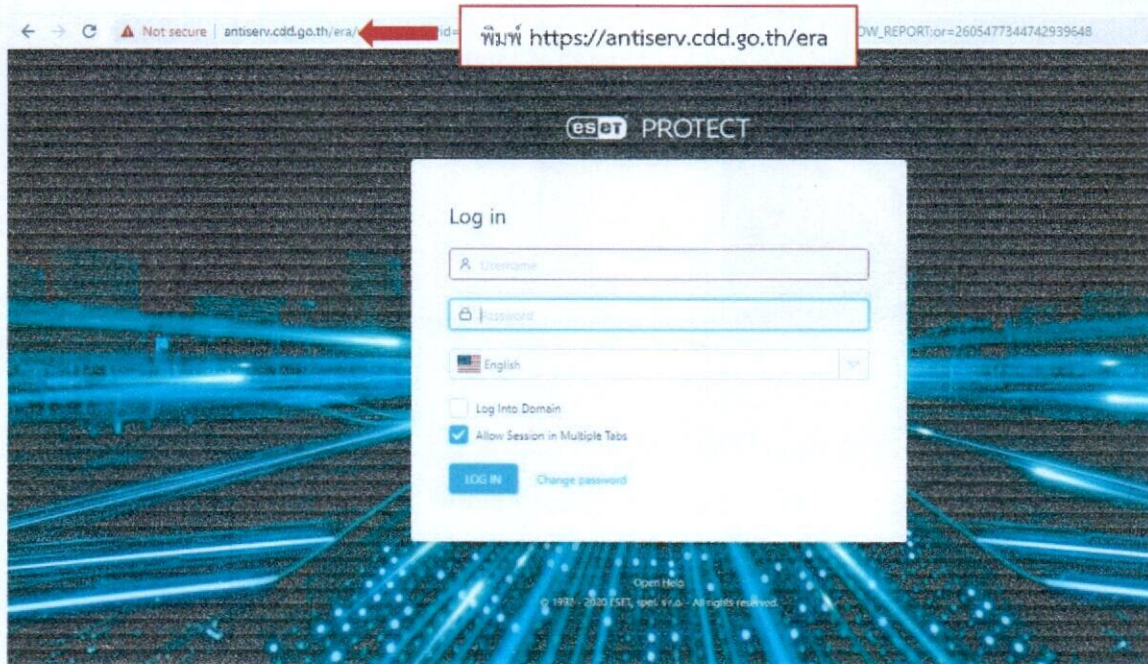
## สารบัญ

เรื่อง	หน้า
วิธีการใช้งาน ESET PROTECT	
๑. การเข้าเว็บไซต์	๑
๒. การเข้าใช้งาน (Login) การกรอก User และ Password	๒
๓. หน้า Dashboard สำหรับตรวจสอบสถานะเครื่องคอมพิวเตอร์แบบเรียลไทม์	๒
๔. การตรวจสอบสถานะเครื่องคอมพิวเตอร์	๖
๕. การตรวจสอบเครื่องคอมพิวเตอร์ที่ผิดปกติหรือมีปัญหา	๑๐
๖. การสั่งสแกนเครื่องคอมพิวเตอร์	๑๒
๗. การ Update Modules	๑๓
๘. การเรียกดูเครื่องคอมพิวเตอร์ที่มีรายงานตัวในระบบ Web Console	๑๔
๙. การตรวจสอบเมนู Detections	๑๖
๑๐. การเลือกช่วงเวลาที่จะตรวจสอบไวรัสบนเครื่องคอมพิวเตอร์ในแต่ละ Group	๑๖
๑๑. การแสดงรายงานเมนู Report	๑๗

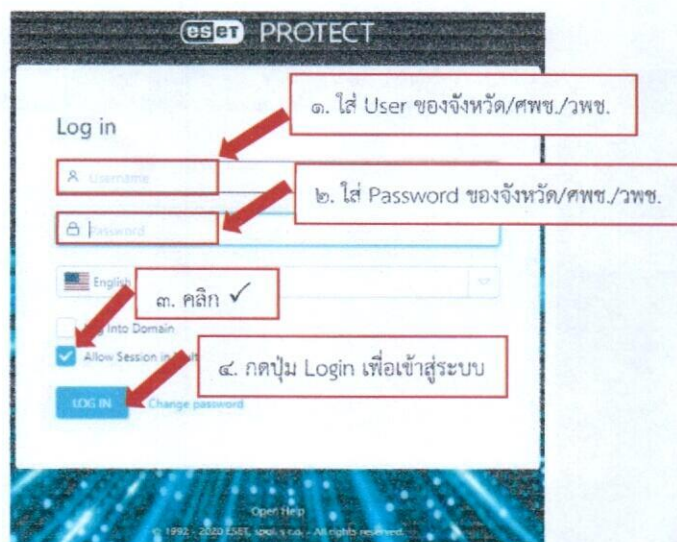
## คู่มือการใช้งาน ESET PROTECT

โปรแกรมป้องกันไวรัส ESET Endpoint Security กำหนดให้มีเว็บไซต์สำหรับบริหารจัดการโปรแกรมป้องกันไวรัส เช่น การตรวจสอบจำนวนเครื่องคอมพิวเตอร์ลูกข่ายที่ติดตั้งโปรแกรมป้องกันไวรัส การตรวจสอบการโจมตีของไวรัสคอมพิวเตอร์ การรายงานผล (Report) การอัปเดตฐานข้อมูลไวรัส เป็นต้น เพื่อให้การใช้งานโปรแกรมป้องกันไวรัสเป็นไปอย่างมีประสิทธิภาพ สามารถบริหารจัดการโปรแกรมป้องกันไวรัส ได้สะดวกมากยิ่งขึ้น จึงได้จัดทำคู่มือการใช้งาน ESET PROTECT ให้กับผู้รับผิดชอบงานด้านเทคโนโลยีสารสนเทศ ใช้เป็นแนวทางในการปฏิบัติงาน โดยมีขั้นตอน ดังนี้

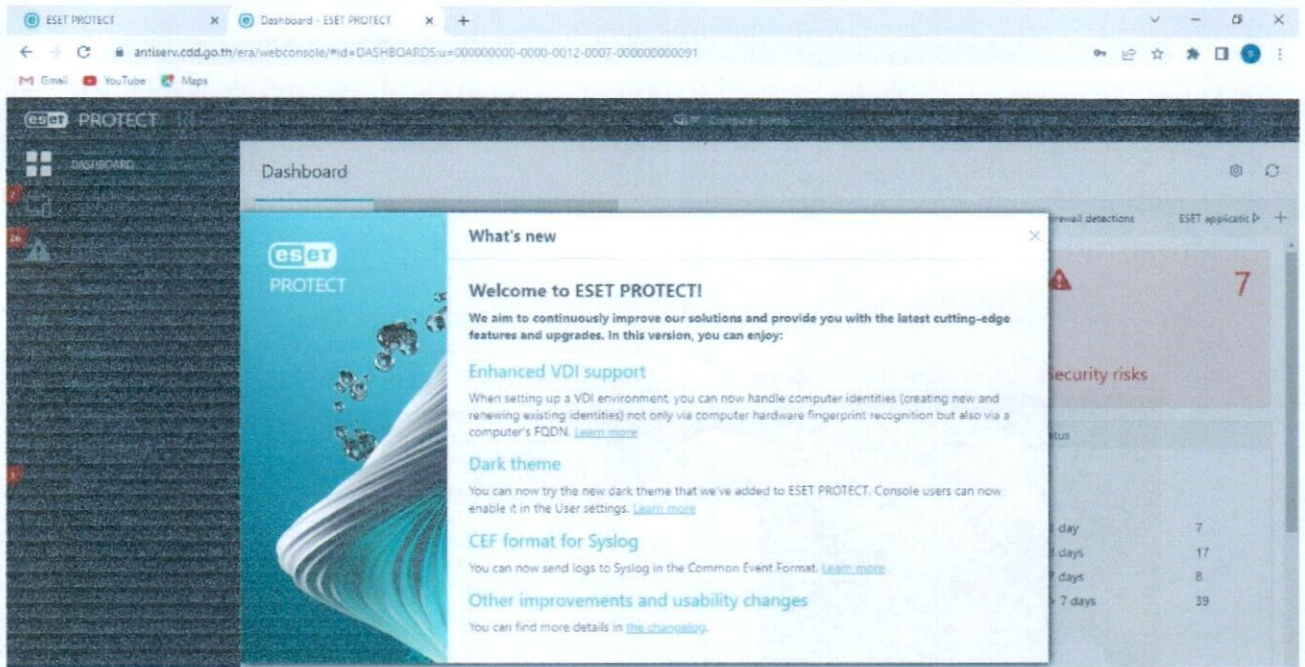
๑. เข้าสู่เว็บไซต์โดยเปิดเว็บเบราว์เซอร์แล้วพิมพ์ URL > <https://antiser.v.cdd.go.th/era> เพื่อเข้าสู่หน้า Login



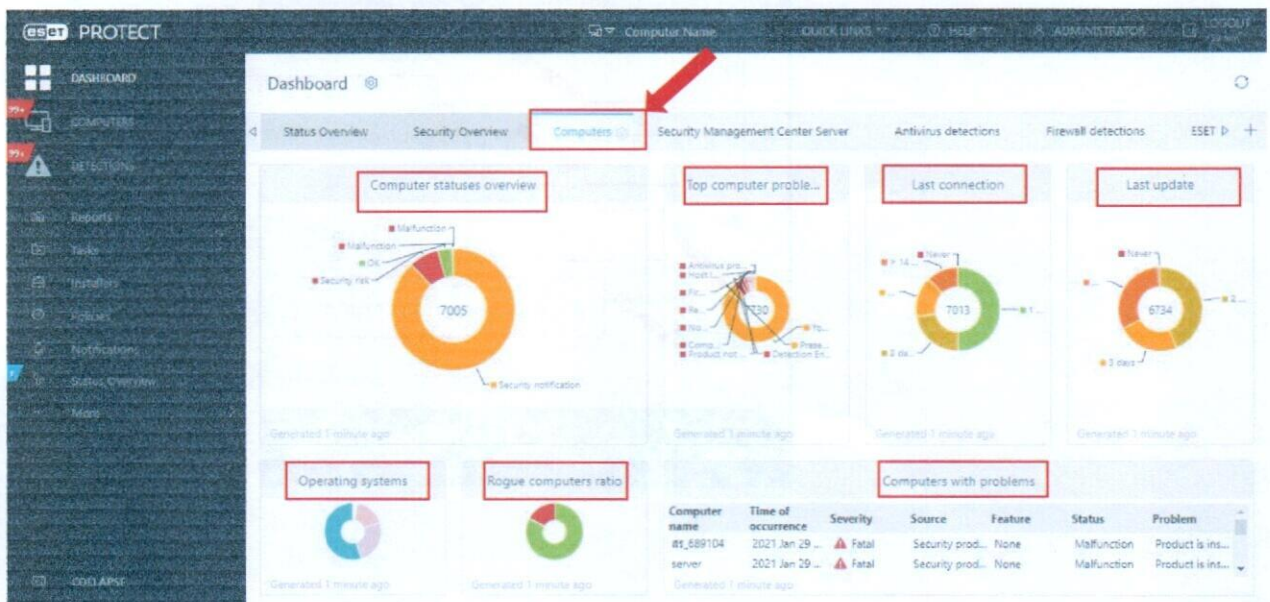
๒. กรอก User และ Password ของแต่ละจังหวัด/ศูนย์ศึกษา/วิทยาลัย แล้วกดปุ่ม  เพื่อเข้าสู่ระบบ



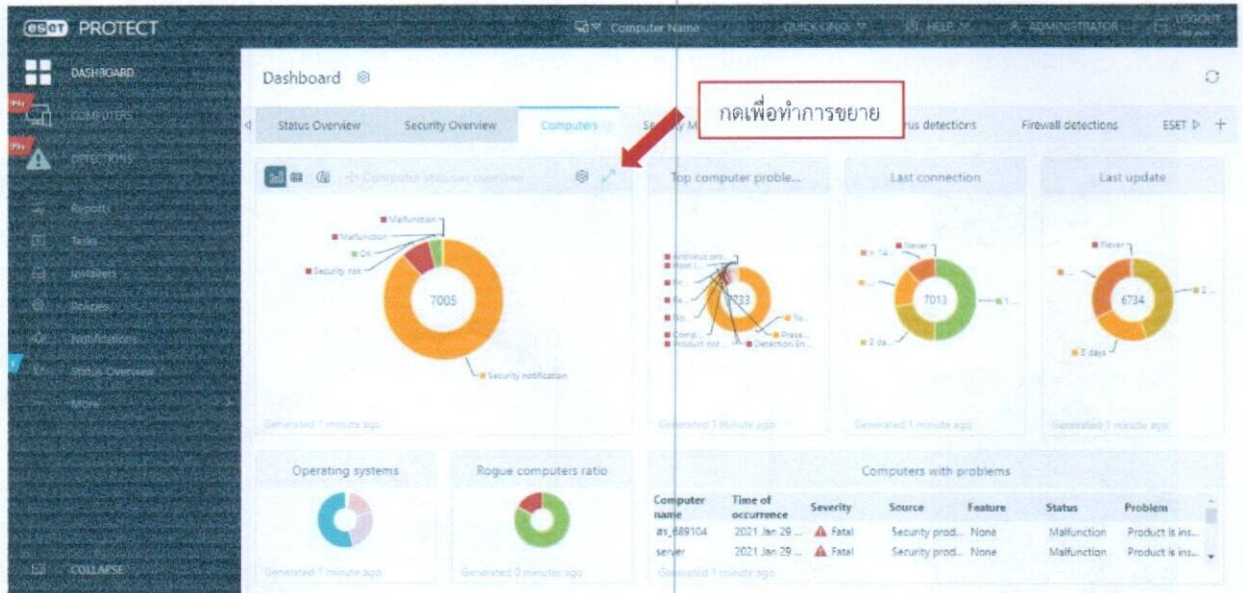
- เมื่อ Login เข้าสู่ระบบแล้วปรากฏหน้าจอดังภาพ ให้กดที่ปุ่ม X



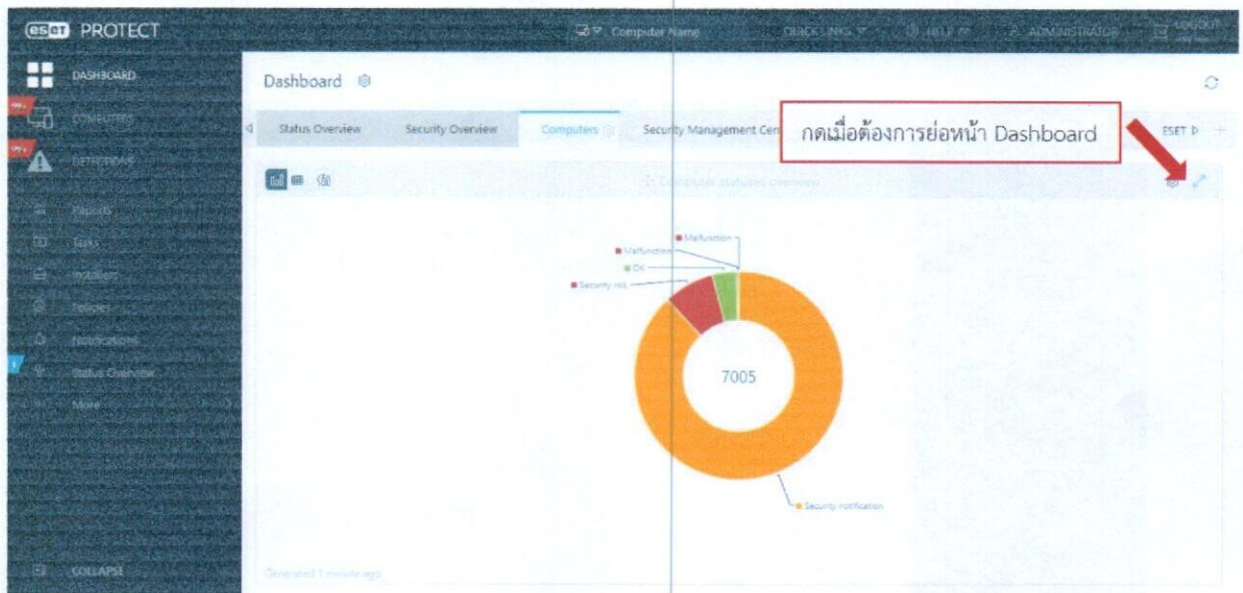
๓. เมื่อ Login เข้าสู่ระบบแล้วจะปรากฏหน้า Dashboard : ในหน้า Dashboard ใช้สำหรับตรวจสอบสถานะ เครื่องคอมพิวเตอร์แบบเรียลไทม์ ให้คลิก Computer จะแสดง template ให้ตรวจสอบสถานะโปรแกรมหลายรูปแบบ เช่น หัวข้อ Computer statuses overview เป็นการตรวจสอบสถานะการอัปเดตของเครื่องว่ามีความผิดปกติหรือไม่สังเกตได้จากสีของกราฟ โดยแบ่งออกเป็น สีเขียว - การอัปเดตปกติ สีส้ม - ไม่ได้มีการอัปเดตมาซักระยะหนึ่งหรือมีการใช้ Presentation mode และสีแดง - ฟังก์ชันไม่สมบูรณ์หรือไม่ได้อัปเดตมานานมาก และผู้ดูแลโปรแกรมสามารถคลิกดูแต่ละ template เพื่อตรวจสอบข้อมูล คือ Top Computer problem, Last connection, Last update, Operating system, Rogue computer ratio และ Computer with problem ดังภาพ




๓.๑ ในการขยายดูหน้าตาต่างสถานะของ Dashboard แต่ละ template สามารถทำได้โดยการกดปุ่ม  ดูข้อมูลของ Dashboard นั้นๆ ดังภาพ

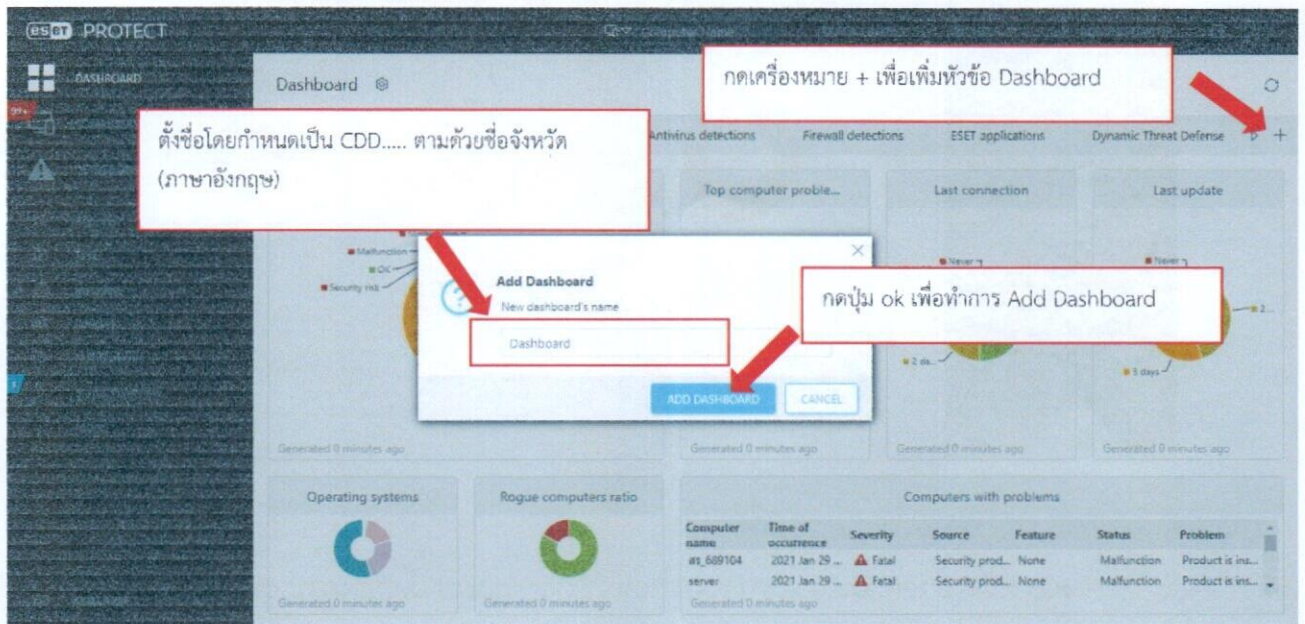


๓.๒ หน้าจอ template แสดงการขยายหน้า Dashboard เมื่อต้องการย่อหน้า Dashboard กลับไปเป็นหน้าเดิมให้กดปุ่ม  อีกครั้ง

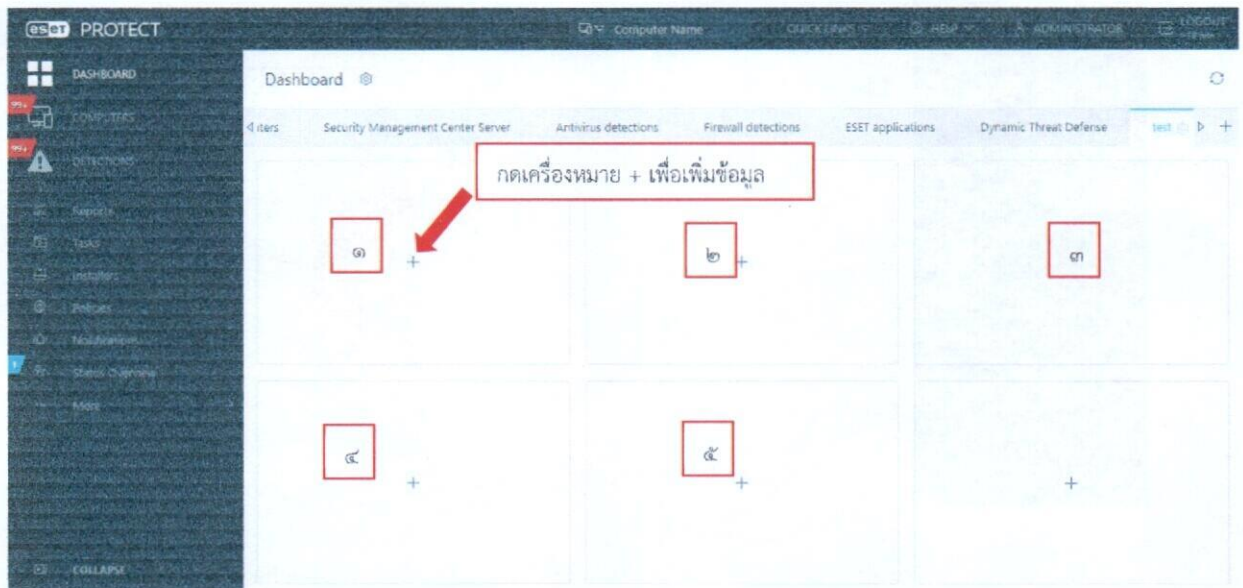


๓.๓ ในขั้นตอนนี้ผู้ดูแลโปรแกรมจะต้องเพิ่มหัวข้อ Dashboard เพื่อแสดงผลการรายงาน (Report) ของแต่ละจังหวัดมีขั้นตอน ดังนี้

๑) กดเครื่องหมาย + เพื่อเพิ่มหัวข้อ Dashboard จะมีช่อง Add Dashboard ให้ตั้งชื่อโดยพิมพ์ CDD.... ตามด้วยชื่อจังหวัด (ภาษาอังกฤษตัวพิมพ์ใหญ่) เสร็จแล้วกดปุ่ม  เพื่อ Add Dashboard ดังภาพ

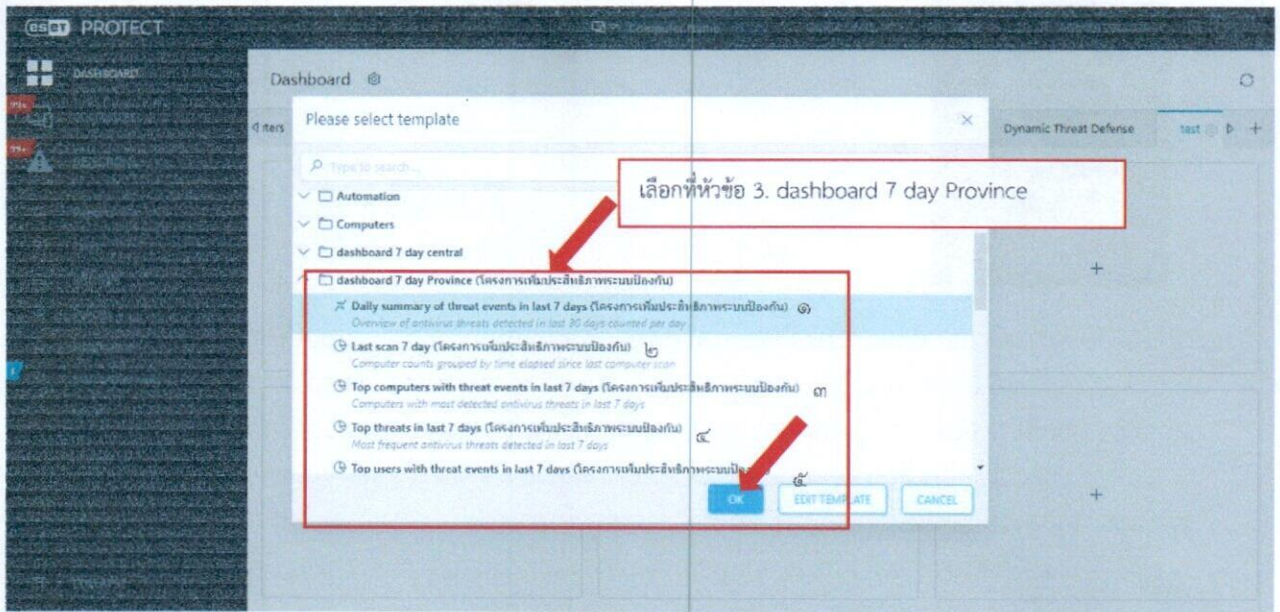


๒) เมื่อกดปุ่ม ok แล้ว จะแสดงหน้าต่างการเพิ่ม Dashboard ให้กดเครื่องหมาย + ดังภาพ เมื่อกดเครื่องหมาย + แล้วจะพบ report template สำหรับจังหวัด โดยเลือกที่หัวข้อ “3. dashboard 7 day Province”

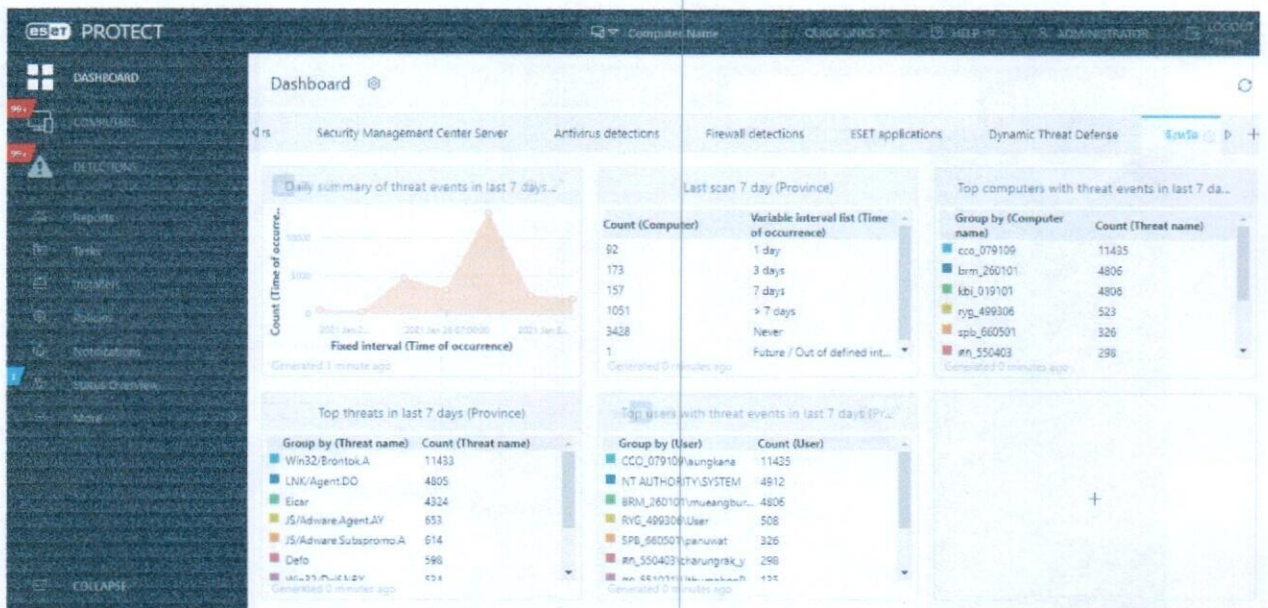



๓) ให้คลิกเลือกหัวข้อเรียงตามลำดับหมายเลขให้ครบ ๕ หัวข้อ ดังนี้

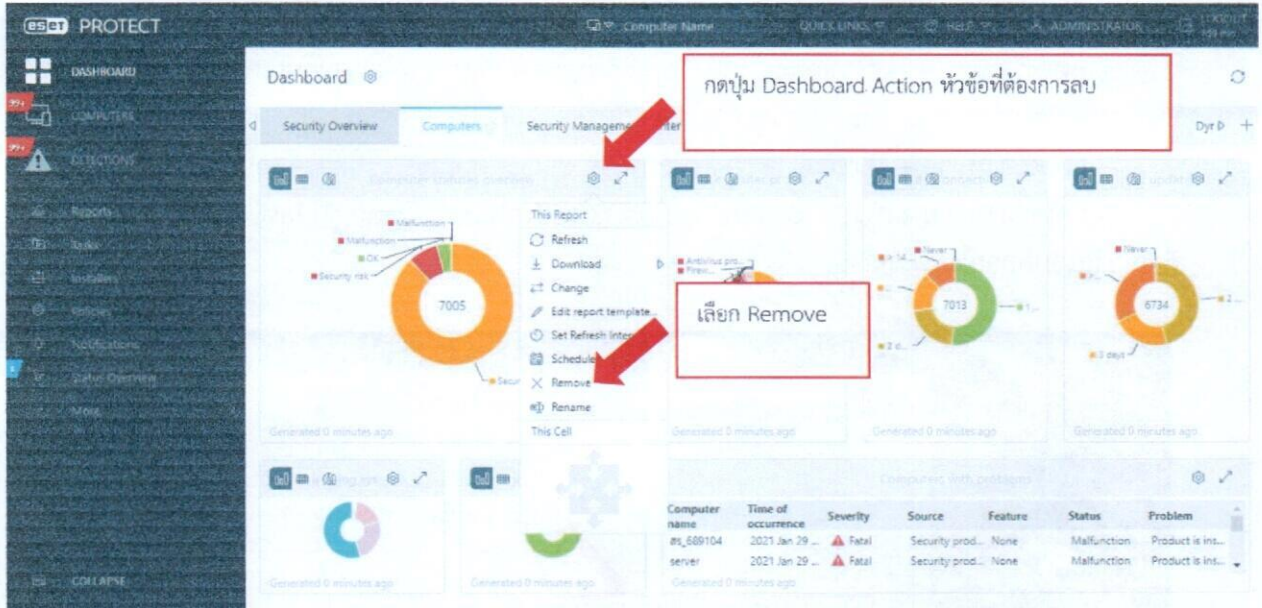
- กดเครื่องหมาย + หัวข้อ ๑ เลือก Daily summary of threat event in ๗ days - ใช้ตรวจสอบจำนวนไวรัสที่เข้ามาโจมตีในแต่ละวัน ภายใน ๗ วัน
- กดเครื่องหมาย + หัวข้อ ๒ เลือก Last scan ๗ days - ใช้ตรวจสอบการสแกนของเครื่องแต่ละเครื่องภายใน ๗ วัน
- กดเครื่องหมาย + หัวข้อ ๓ เลือก Top computer with threat event in last ๗ days - ใช้ตรวจสอบว่ามีเครื่องคอมพิวเตอร์เครื่องไหนติดไวรัส ภายใน ๗ วัน
- กดเครื่องหมาย + หัวข้อ ๔ เลือก Top threat in last ๗ days - ใช้ตรวจสอบไวรัสที่เข้ามาโจมตีภายใน ๗ วัน
- กดเครื่องหมาย + หัวข้อ ๕ เลือก Top users with threat events in last ๗ days - ใช้ตรวจสอบ users ที่ถูกไวรัสโจมตีภายใน ๗ วัน



๔) แสดงหน้าจอหลังจากเพิ่มข้อมูล Dashboard ทั้ง ๕ หัวข้อ และแสดงการรายงานข้อมูล



๕) หากต้องการลบ Dashboard ที่ไม่จำเป็นต้องใช้งาน สามารถลบออกได้โดยกดเครื่องหมาย  และเลือก Remove ยืนยันการลบ Dashboard โดยการกดปุ่ม ok หรือยกเลิกการลบ Dashboard โดยการกดปุ่ม CANCEL



๔. การตรวจสอบสถานะเครื่องคอมพิวเตอร์ โดยกดเลือกหัวข้อ Computer ด้านซ้ายมือ

หัวข้อ Computer เป็นเมนูสำหรับดูจำนวนเครื่องคอมพิวเตอร์ที่เข้ามารายงานตัวในระบบและตรวจสอบสถานะของเครื่องคอมพิวเตอร์ เช่น สถานะเครื่อง, ชื่อเครื่อง, IP ของเครื่อง, Last connection เป็นต้น

๔.๑ ให้คลิกเลือก Computer แล้วให้กดปุ่มเครื่อง + หน้าหัวข้อ Province กดปุ่มโฟลเดอร์ชื่อจังหวัด เพื่อแสดงรายละเอียดของเครื่องคอมพิวเตอร์ที่เชื่อมต่อเข้ามาในระบบของแต่ละจังหวัด

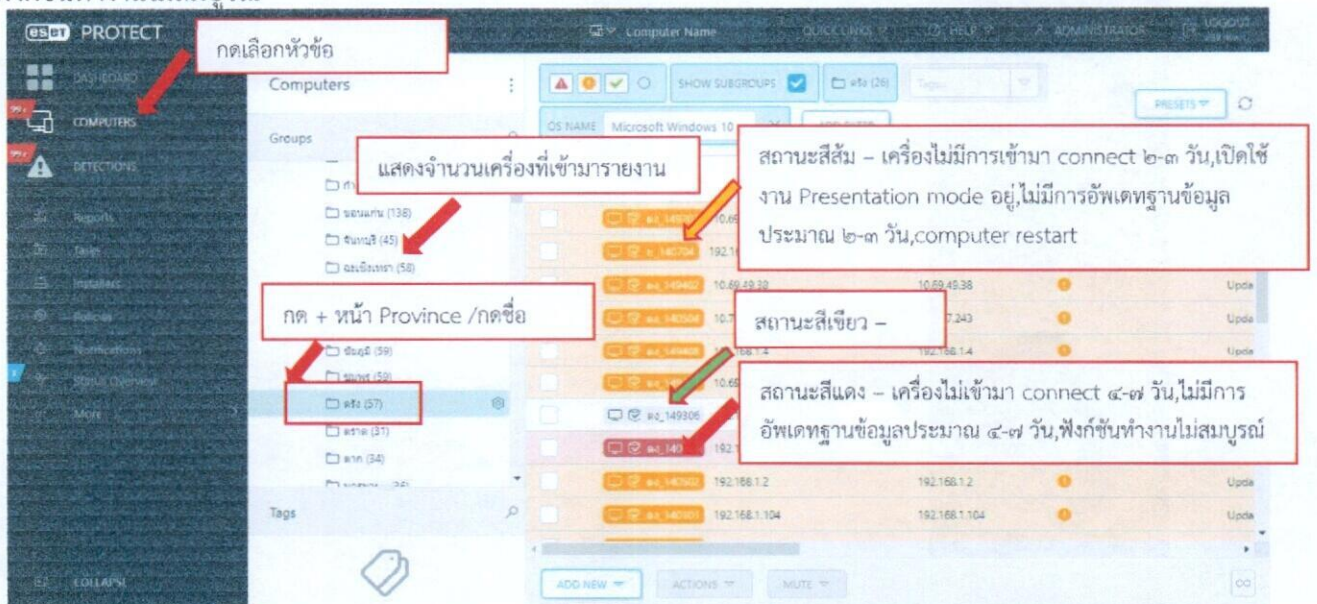
๔.๒ เครื่องคอมพิวเตอร์แต่ละเครื่องจะมีการแสดงสถานการณ์แจ้งเตือน คือ

- สถานะสีเขียว : เครื่องปกติ
- สถานะสีส้ม : เครื่องไม่มีการเข้ามา connect หรือเปิดใช้งาน Presentation mode อยู่ หรือไม่มี

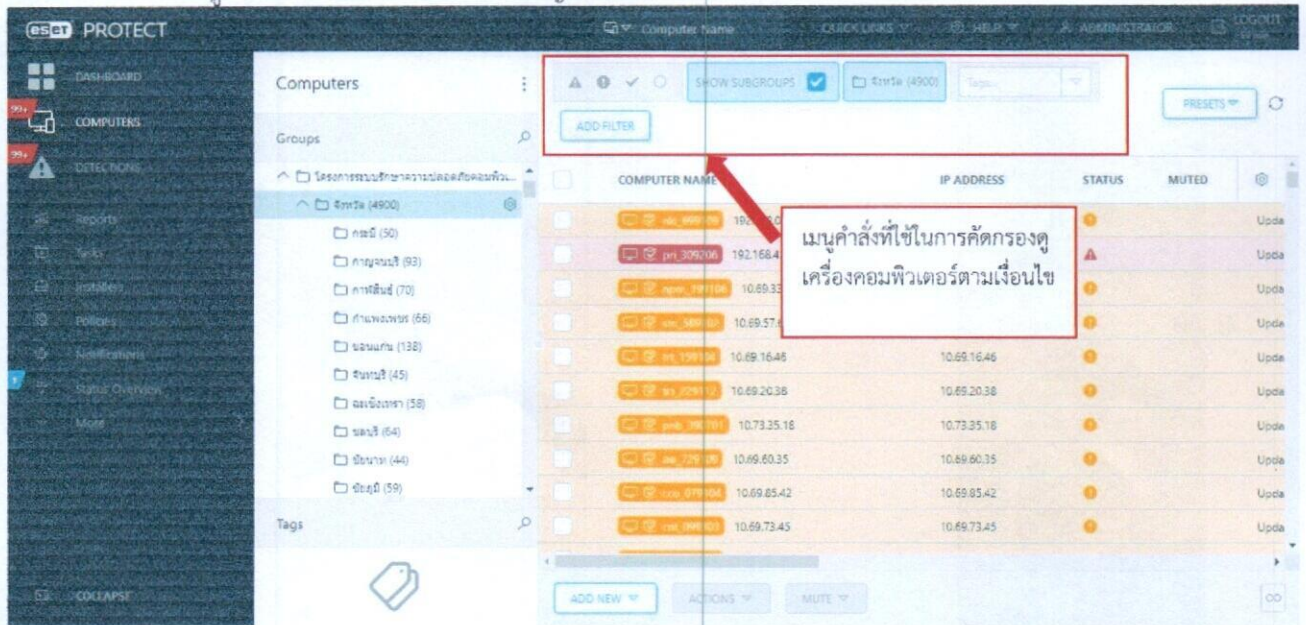
การอัปเดตฐานข้อมูลไวรัส ประมาณ ๒-๓ วัน

- สถานะสีแดง : เครื่องไม่เข้ามา connect หรือไม่มีการอัปเดตฐานข้อมูลไวรัส ประมาณ ๔-๗ วัน หรือ

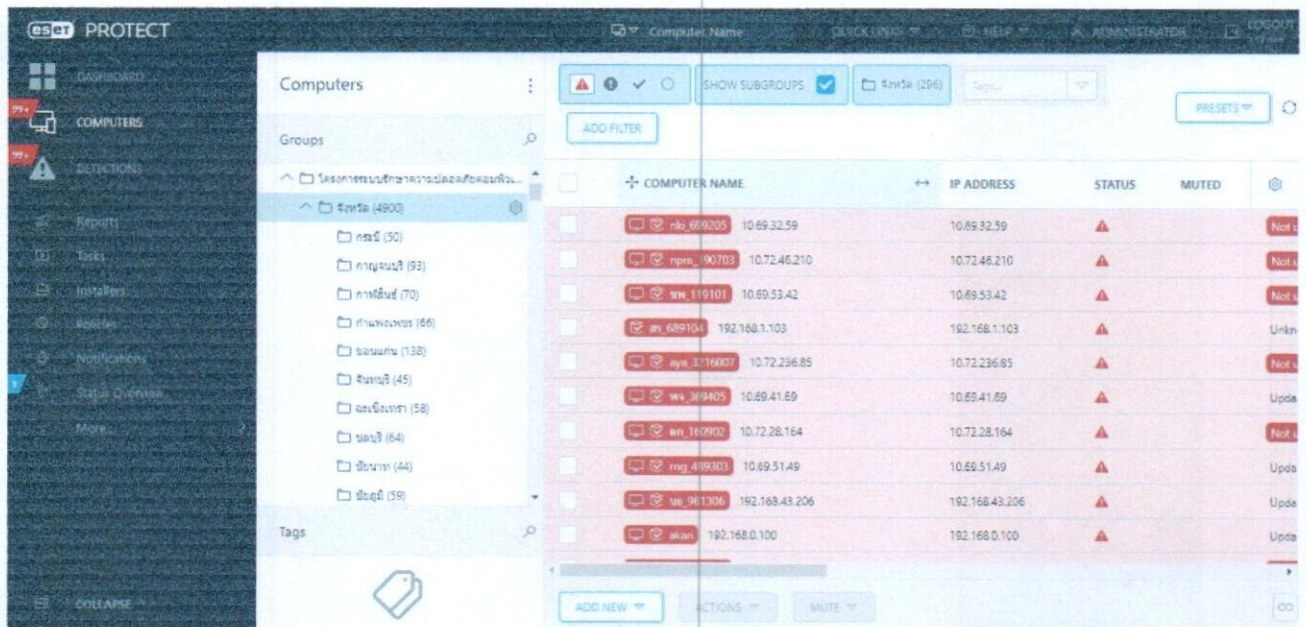
ฟังก์ชันทำงานไม่สมบูรณ์



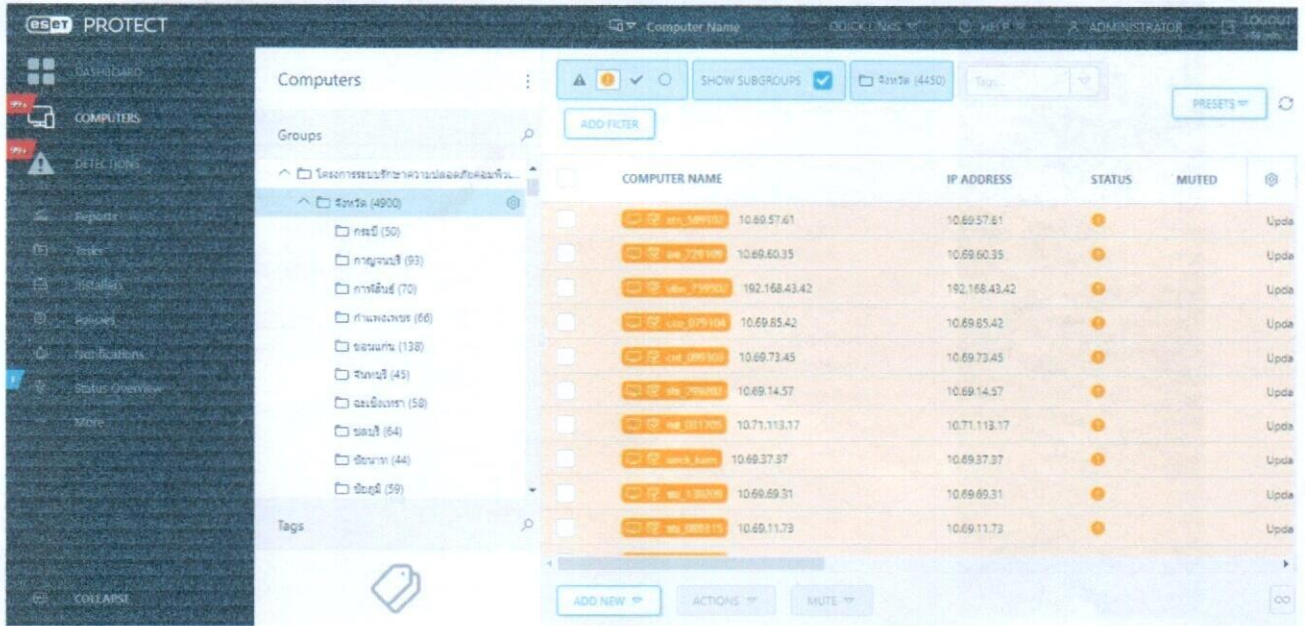
๔.๓ เมนู Computer ผู้ดูแลโปรแกรม สามารถที่จะคัดกรองดูข้อมูลเครื่องคอมพิวเตอร์เฉพาะส่วนที่ต้องการได้ จากเมนูตามภาพ โดยคลิกเลือกตามสัญลักษณ์ ดังนี้



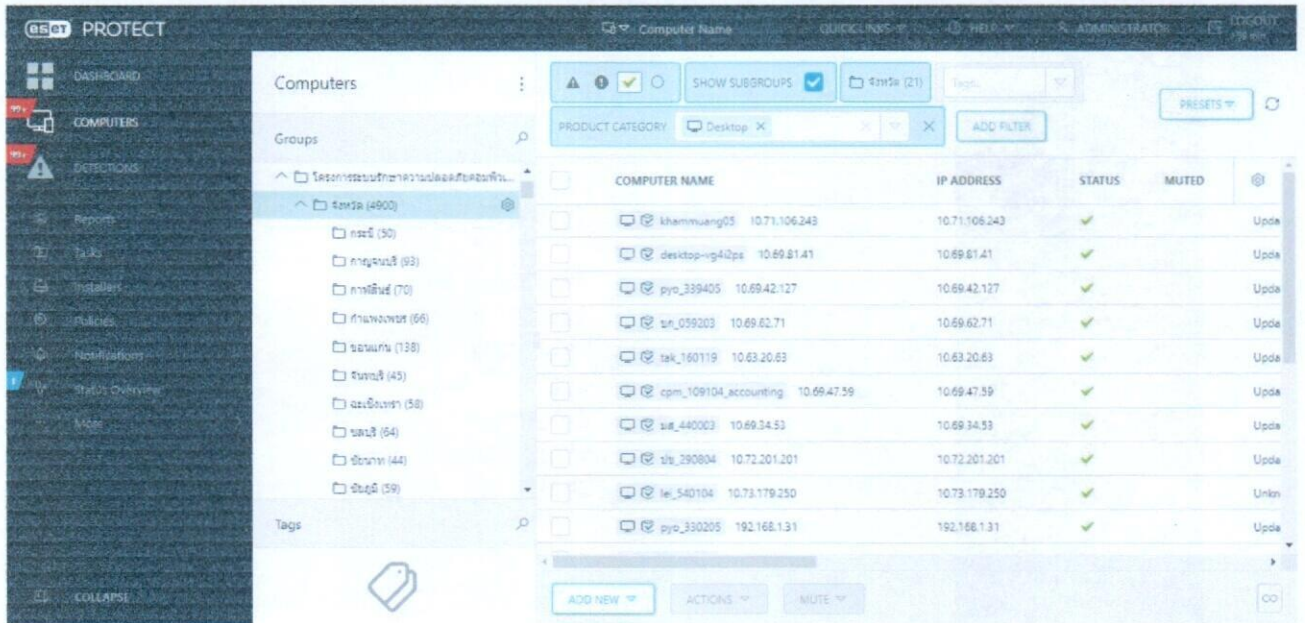
๔.๓.๑ แสดงการคัดกรองเฉพาะเครื่องคอมพิวเตอร์ที่แจ้งสถานะเป็นสีแดง



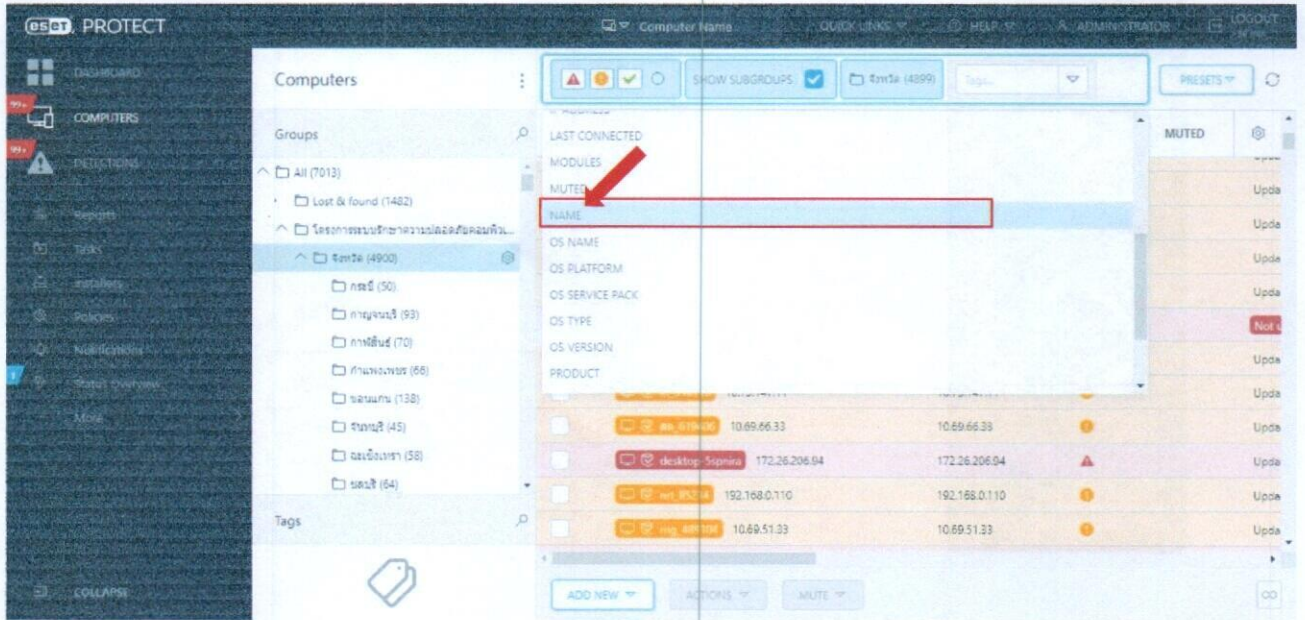
๔.๓.๒ แสดงการคัดกรองเฉพาะคอมพิวเตอร์ที่แจ้งสถานะเป็นสีเขียว



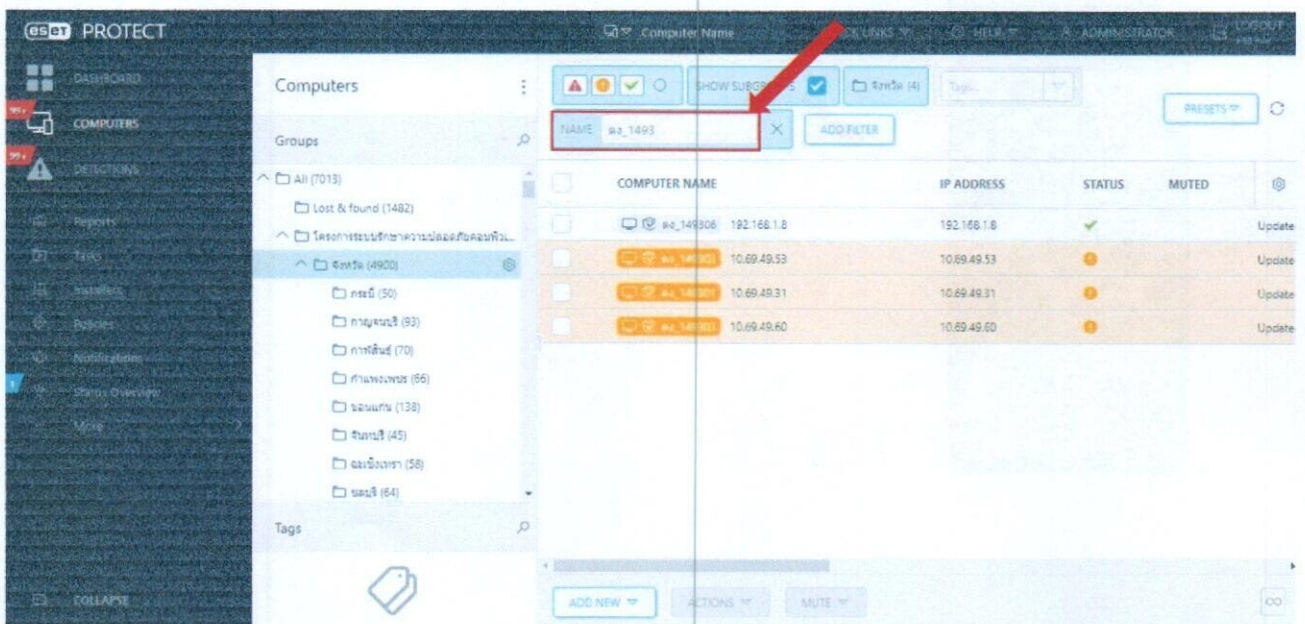
๔.๓.๓ แสดงการคัดกรองเฉพาะคอมพิวเตอร์ที่แจ้งสถานะเป็นสีเขียว



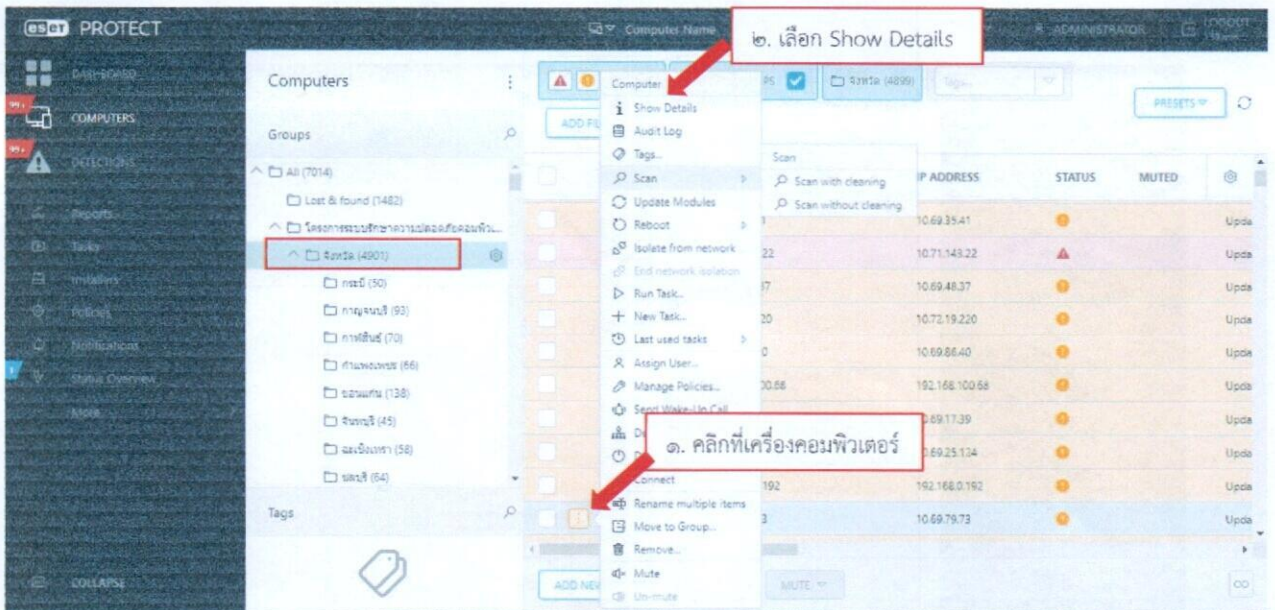
๔.๓.๔ ในกรณีที่ต้องการคัดกรองเครื่องคอมพิวเตอร์โดยระบุเงื่อนไขอื่นๆ ให้คลิกที่ปุ่ม **ADD FILTER** จะปรากฏตัวเลือกในการคัดกรองเพิ่มเติม ดังตัวอย่าง แสดงการคัดกรองเครื่องคอมพิวเตอร์ที่ชื่อ ตง\_1493 โดยให้เลือกที่ Name



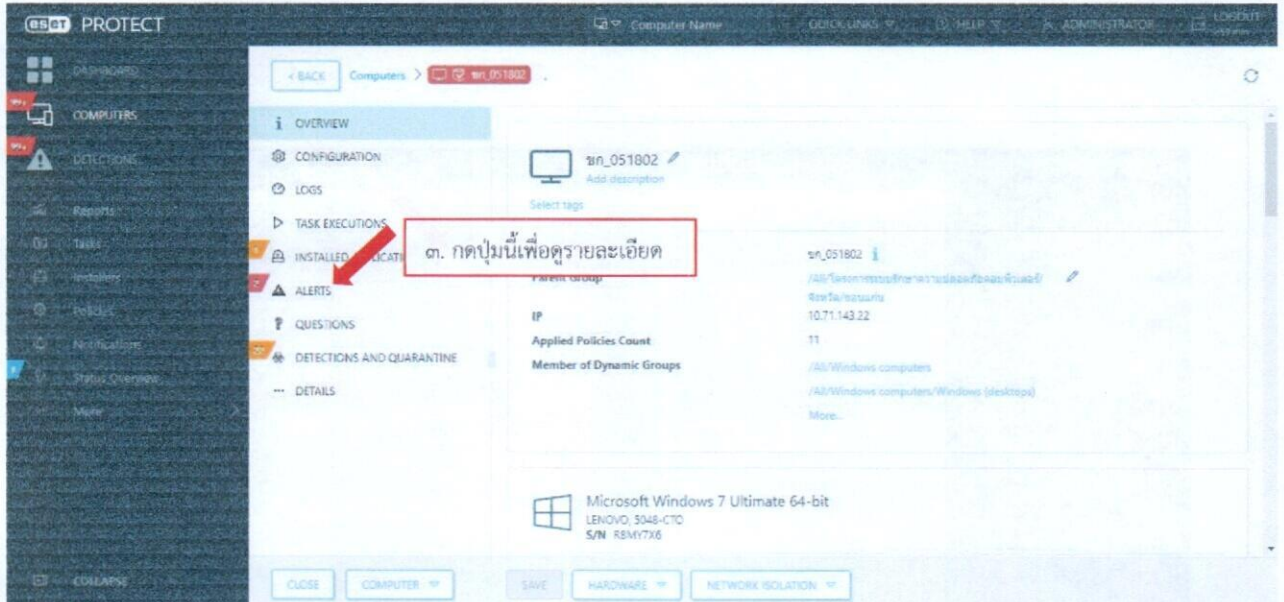
- ปรากฏหน้าจอดังภาพ ให้ใส่ชื่อเครื่องคอมพิวเตอร์ ตง\_1493 เสร็จแล้วกด Enter หน้าจอจะแสดงเครื่องคอมพิวเตอร์ชื่อ ตง\_1493 ทุกเครื่อง หากจะกลับสู่หน้าจอเดิมให้กด **X** ปิดที่



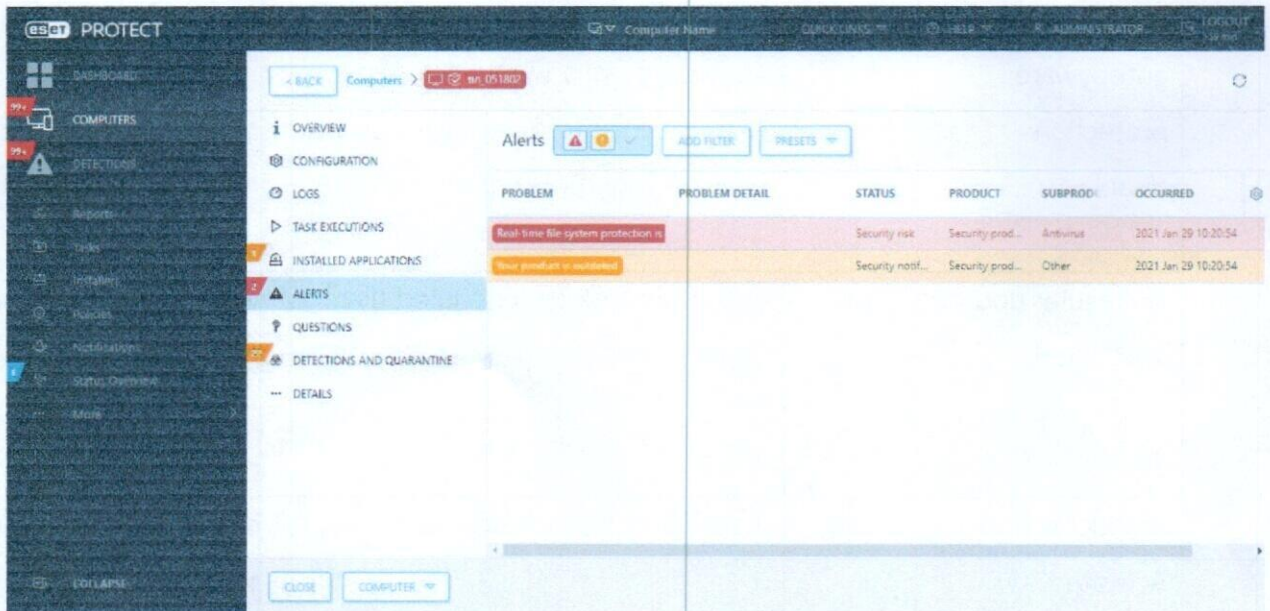
๕. การตรวจสอบเครื่องคอมพิวเตอร์ที่ผิดปกติหรือมีปัญหา เพื่อให้ผู้ดูแลโปรแกรมตรวจสอบเครื่องคอมพิวเตอร์ที่มีความผิดปกติ และวิธีแก้ไขโดยเลือกที่เครื่องคอมพิวเตอร์ที่มีปัญหา (สีแดง) แล้วเลือก Show Details ดังภาพ



หลังจากนั้นจะปรากฏหน้าจอนี้ ให้คลิกที่หัวข้อ ALERTS ดังภาพ



หน้าจจะแสดงปัญหาที่เกิดขึ้นภายในเครื่องคอมพิวเตอร์ ดังภาพ

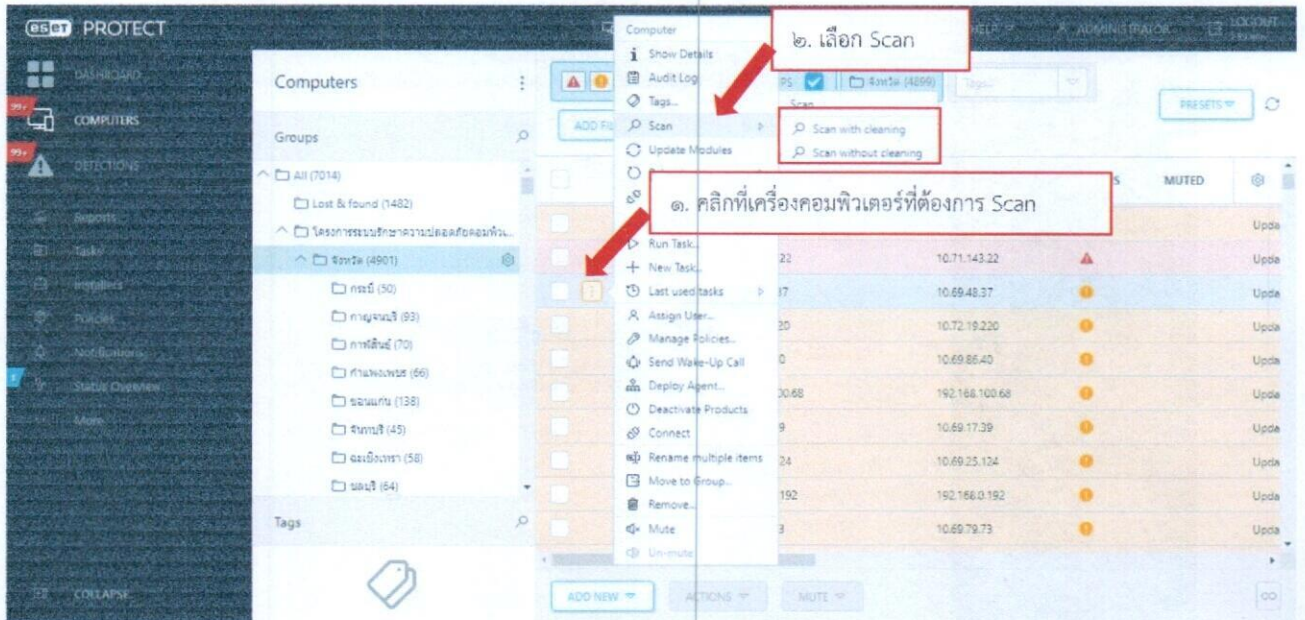


รายละเอียดแจ้งเตือนปัญหาที่อาจเกิดขึ้นภายในเครื่องคอมพิวเตอร์ และวิธีแก้ไขปัญหา ดังนี้

ข้อมูลแจ้งสถานะ	สีสถานะ	ความหมาย	วิธีแก้ไข
Antivirus and antispyware protection disabled	แดง	อาจมีการปิดการใช้งานโปรแกรม Antivirus ชั่วคราว หรือโปรแกรมทำงานไม่สมบูรณ์ทำให้ฟังก์ชัน antivirus and spyware ไม่ถูกเปิดใช้งาน	<ul style="list-style-type: none"> <li>- หากฟังก์ชันถูกปิดอยู่ให้ทำการเปิดใช้งานได้ทันที</li> <li>- หากฟังก์ชันไม่สมบูรณ์ให้ทำการถอนการติดตั้งออกโดยใช้ Tools uninstaller และติดตั้งใหม่อีกครั้ง</li> </ul>
No regular update scheduled	แดง	คือ system task ใน scheduled อาจมีปัญหา	<ul style="list-style-type: none"> <li>- ต้องทำการกำหนด scheduler update ใหม่</li> <li>- ถอนการติดตั้งโดยใช้ tools uninstaller และ ติดตั้งใหม่อีกครั้ง</li> </ul>
Product is not Activated	แดง	เครื่องยังไม่การ active license	<ul style="list-style-type: none"> <li>- รอกการส่ง task จาก server</li> <li>- หากรอนานเกิน ๒๔ ชม. ให้ติดต่อเจ้าหน้าที่บริษัทได้โดยตรง</li> </ul>
Virus signature database is out date	แดง	ฐานข้อมูลไวรัสไม่ได้รับการอัปเดต	<ul style="list-style-type: none"> <li>- สั่ง task update database</li> <li>- หากสั่งแล้วติดให้ activation license ให้รอหากเกิน ๒๔ ชม. ให้ติดต่อเจ้าหน้าที่บริษัทได้โดยตรง</li> </ul>
Firewall not function	แดง	ฟังก์ชัน Firewall มีปัญหา	<ul style="list-style-type: none"> <li>- เนื่องจากผลิตภัณฑ์ของทางกรมพัฒนาชุมชนไม่ได้ใช้ Product firewall ต้องทำการถอนการติดตั้งโดย Tools uninstaller และติดตั้งใหม่อีกครั้ง</li> </ul>
Protocol filtering not functional	แดง	ฟังก์ชันเกี่ยวกับการสแกนการใช้งานอินเทอร์เน็ต โปรโตคอล มีปัญหา มักเกิดจากการติดตั้งโปรแกรมทับโปรแกรมป้องกันไวรัส ของเดิมบนเครื่องคอมพิวเตอร์นั้น ๆ	<ul style="list-style-type: none"> <li>- ถอนการติดตั้งโดยใช้ tools uninstaller และติดตั้งใหม่อีกครั้ง</li> </ul>
Presentation Mode is enabled	เหลือง	มีการเปิดใช้งานหน้าจอแบบ Full screen เช่น PowerPoint หรือการเปิดไฟล์ภาพยนตร์แบบเต็มหน้าจอ	<ul style="list-style-type: none"> <li>- หลังจากผู้ใช้ออกจากการใช้งานแบบเต็มหน้าจอ สถานะจะหายไปเอง</li> </ul>
Recent update attempts failed	เหลือง	โปรแกรมป้องกันไวรัส ไม่สามารถอัปเดตฐานข้อมูลไวรัสได้ในช่วงเวลานั้นๆ เกิน ๓ ครั้งขึ้นไป	<ul style="list-style-type: none"> <li>- สั่ง task update database</li> <li>- หากสั่งแล้วไม่อัปเดตให้ activation license ให้รอหากเกิน ๒๔ ชม. ให้ติดต่อเจ้าหน้าที่บริษัทได้โดยตรง</li> </ul>

ข้อมูลแจ้งสถานะ	สถานะ	ความหมาย	วิธีแก้ไข
Product is not connected. No connection attempt occurred.	เหลือง	เครื่องคอมพิวเตอร์ดังกล่าว ยังไม่ได้มีการติดตั้งโปรแกรมป้องกันไวรัส เวอร์ชัน ๘ และโปรแกรมป้องกันไวรัสเดิมเวอร์ชัน ๕ มักจะมีการแจ้งเกี่ยวกับการทำงานที่ไม่สมบูรณ์ ถ้าหากเครื่องไม่เคยลงโปรแกรมป้องกันไวรัส แสดงว่าการเขียน registry ของโปรแกรมอาจไม่สมบูรณ์	- ถอนการติดตั้งโปรแกรมป้องกันไวรัส เวอร์ชัน ๘ โดยใช้ tools uninstaller และติดตั้งโปรแกรมป้องกันไวรัส เวอร์ชัน ๘ ใหม่อีกครั้ง
Product is installed but it is not running	เหลือง	เครื่องคอมพิวเตอร์ดังกล่าว ยังไม่ได้มีการติดตั้งโปรแกรมป้องกันไวรัส เวอร์ชัน ๘ และโปรแกรมป้องกันไวรัสเดิมเวอร์ชัน ๕ มักจะมีการแจ้งเกี่ยวกับการทำงานที่ไม่สมบูรณ์หรือเกิดจากการติดตั้งโปรแกรมป้องกันไวรัส เวอร์ชัน ๘ ที่ไม่สมบูรณ์	- ถอนการติดตั้งโปรแกรมป้องกันไวรัส โดยใช้ tools uninstaller และ ติดตั้งโปรแกรมป้องกันไวรัส เวอร์ชัน ๘ ใหม่อีกครั้ง

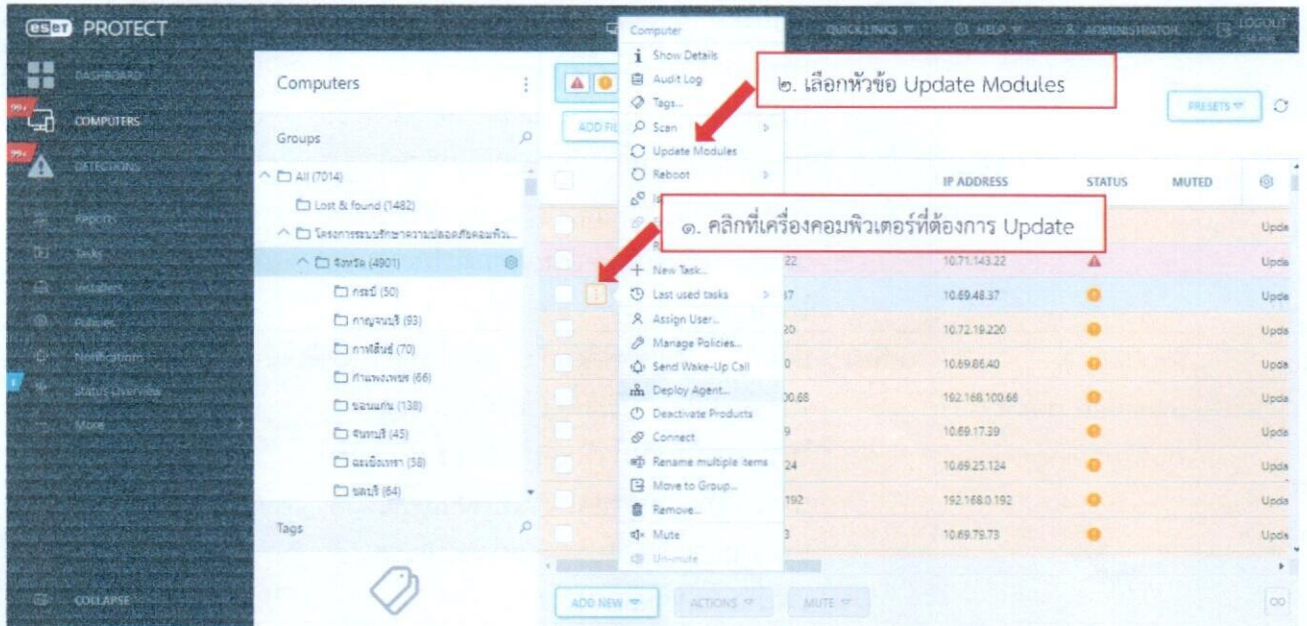
๖. การสั่งสแกนเครื่องคอมพิวเตอร์ กรณีที่เครื่องคอมพิวเตอร์ไม่ได้มีการสแกน ให้คลิกที่เครื่องคอมพิวเตอร์ที่ต้องการสแกน แล้วเลือกหัวข้อ Scan ดังภาพ



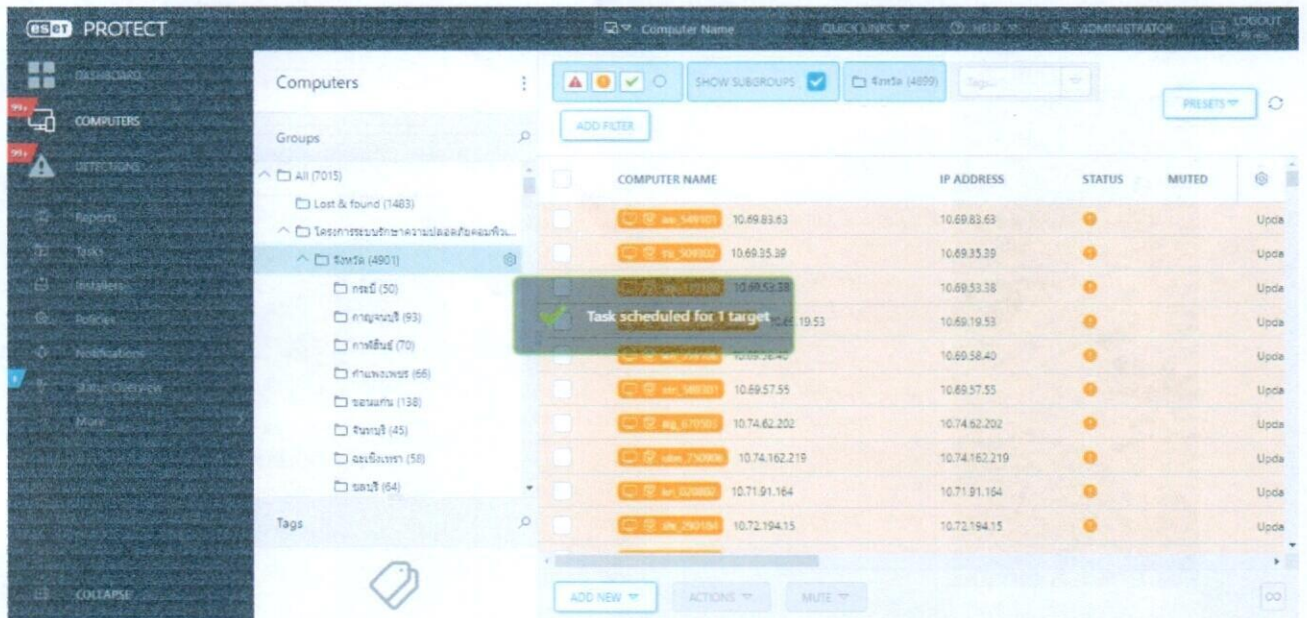
การสแกนสามารถสแกนได้ ๒ แบบดังนี้

- scan with cleaning - โปรแกรมจะทำการสแกนไวรัสให้ทั้งหมดเมื่อตรวจพบก็จะทำการ clean ทันที
- scan without cleaning - โปรแกรมจะทำการสแกนไวรัสให้ทั้งหมดแต่เมื่อตรวจพบก็จะไม่ทำการ clean

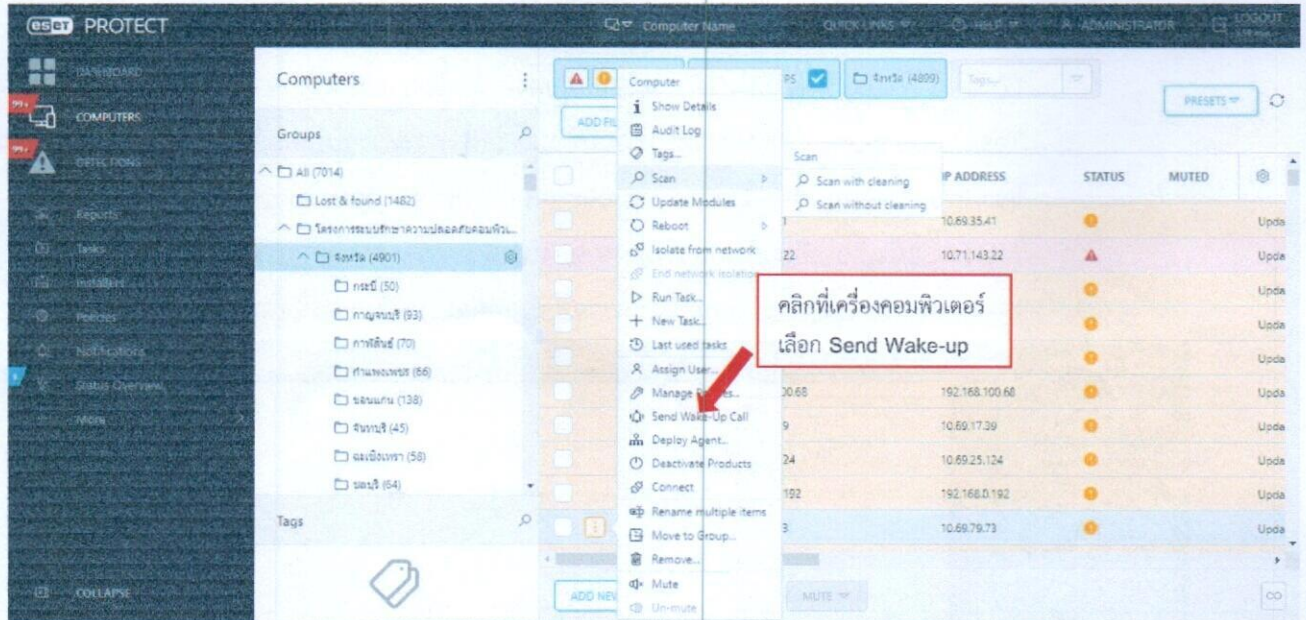
๗. การ Update Modules เป็นการสั่ง Update เครื่องคอมพิวเตอร์หากพบว่าเครื่องที่อยู่ใน Group ไม่มีการ Update โดยคลิกเครื่องที่ไม่มีการ Update และเลือกหัวข้อ Update Modules



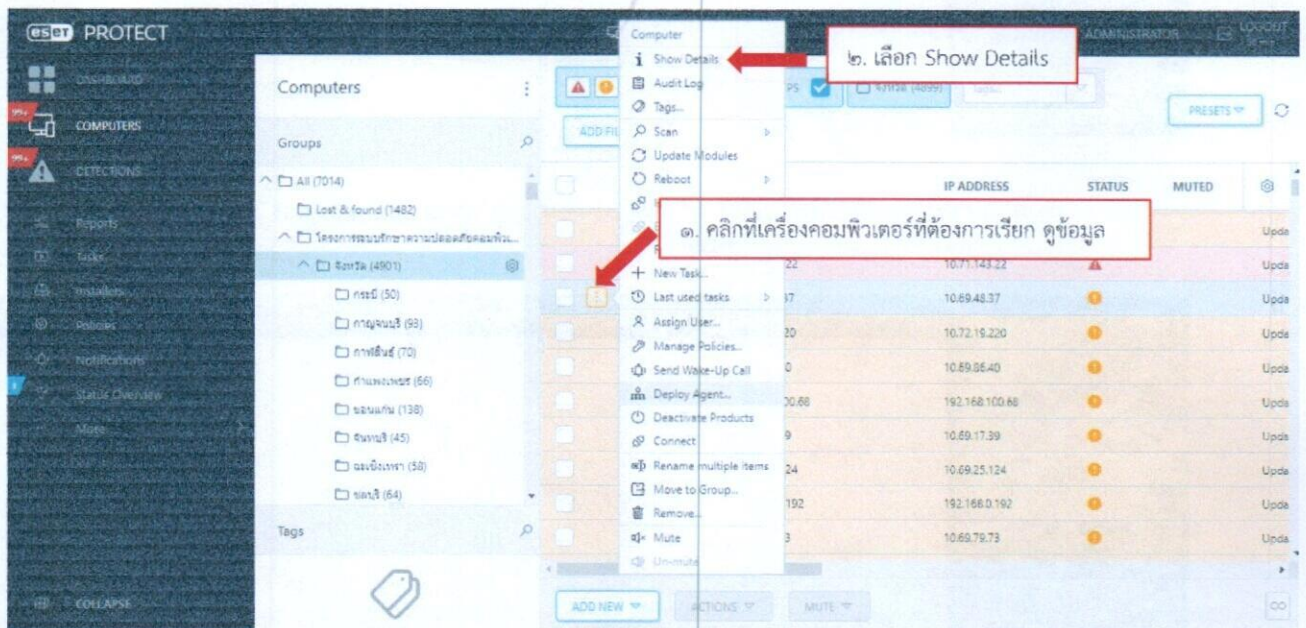
๗.๑ หลังจากสั่งการทำงานไปแล้ว ไม่แสดงการสแกนหรือการอัปเดต ระบบจะมีหน้าจอแจ้งข้อมูลว่าคำสั่งมีการส่งออกไปยังเครื่องลูกข่ายเรียบร้อยแล้ว แต่ไม่ได้หมายความว่าเครื่องลูกข่ายจะดำเนินการตามคำสั่งในทันที



๗.๒ เนื่องจากเครื่องลูกข่ายทุกเครื่อง จะได้รับการตั้งค่าให้มารายงานตัวกับเครื่องแม่ข่ายทุกๆ ๒๐ นาที หากต้องการให้เครื่องมารายงานตัวเป็นกรณีเร่งด่วน สามารถใช้คำสั่ง Send Wake-up call เพื่อลดระยะเวลาการรายงานตัวของเครื่องลูกข่ายได้ (ระยะเวลารายงานตัวจะเหลือประมาณ ๑ นาที ในการสั่งการทำงานครั้งนั้นๆ)

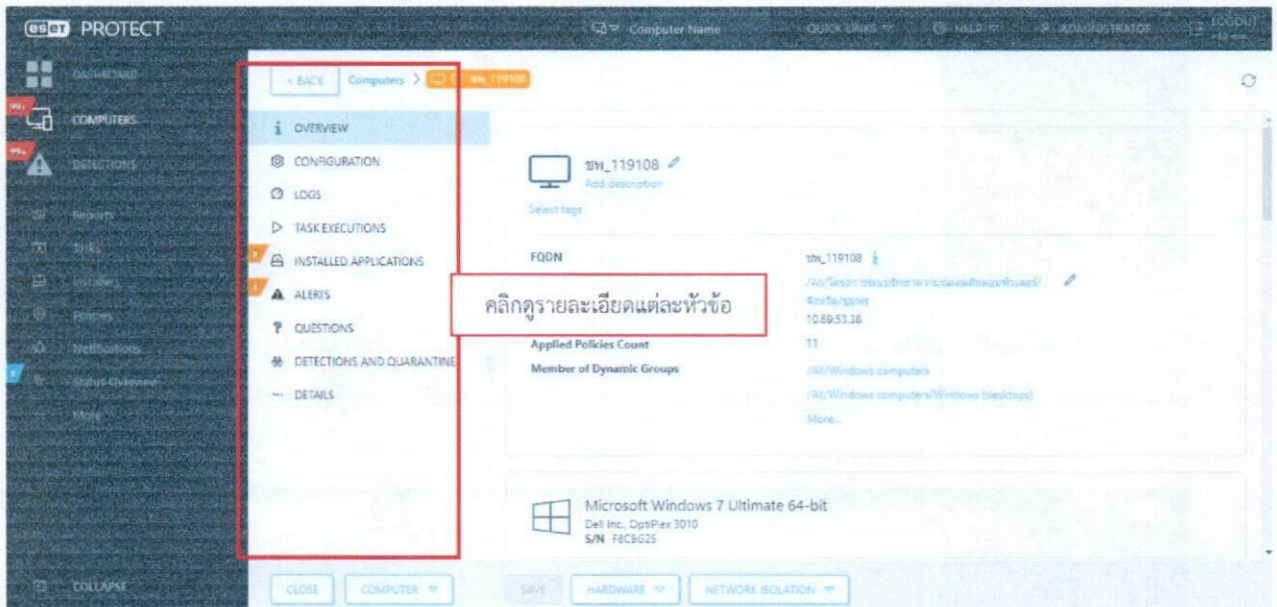


๘. ผู้ดูแลโปรแกรม สามารถเรียก ดูรายละเอียดข้อมูลเครื่องคอมพิวเตอร์แต่ละเครื่องที่มารายงานตัวในระบบ Web Console โดยคลิกที่เครื่องคอมพิวเตอร์ที่ต้องการดูข้อมูล แล้วเลือกหัวข้อ Show Details ดังภาพ

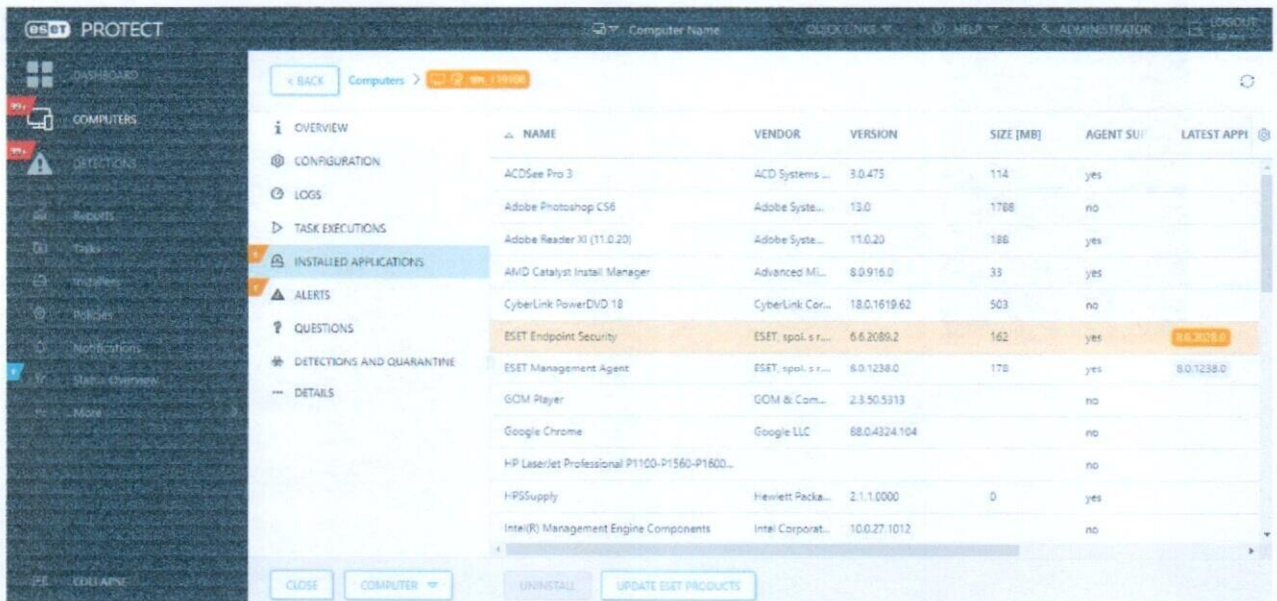


แสดงรายละเอียดข้อมูลเครื่องคอมพิวเตอร์ที่มารายงานตัวในระบบ Web Console ข้อมูลที่ปรากฏจะแสดงตามหัวข้อที่เลือก ซึ่งสามารถคลิกดูรายละเอียดแต่ละหัวข้อได้ ดังนี้

- Basic - ใช้ตรวจสอบข้อมูลเครื่องคอมพิวเตอร์, IP Address, Computer Name, OS Name, Work Group
- Configuration - ใช้ตรวจการตั้งค่า configuration ที่ใช้กับเครื่องคอมพิวเตอร์
- Logs - ใช้ในการวิเคราะห์หาความผิดปกติของเครื่องในกรณีเกิดปัญหาต่างๆ
- Task Executions - ใช้ในการตรวจสอบข้อมูล task การทำงานที่เคยสั่งกับเครื่องคอมพิวเตอร์นั้น ๆ
- Install Applications - ใช้ตรวจสอบและถอนการติดตั้ง Applications ที่ติดตั้งในเครื่อง
- Alerts - แจ้งเตือนเกี่ยวกับปัญหาต่างๆ ของโปรแกรม
- Detection And Quarantine - ใช้ตรวจสอบข้อมูลไวรัสที่เคยตรวจพบบนเครื่องคอมพิวเตอร์



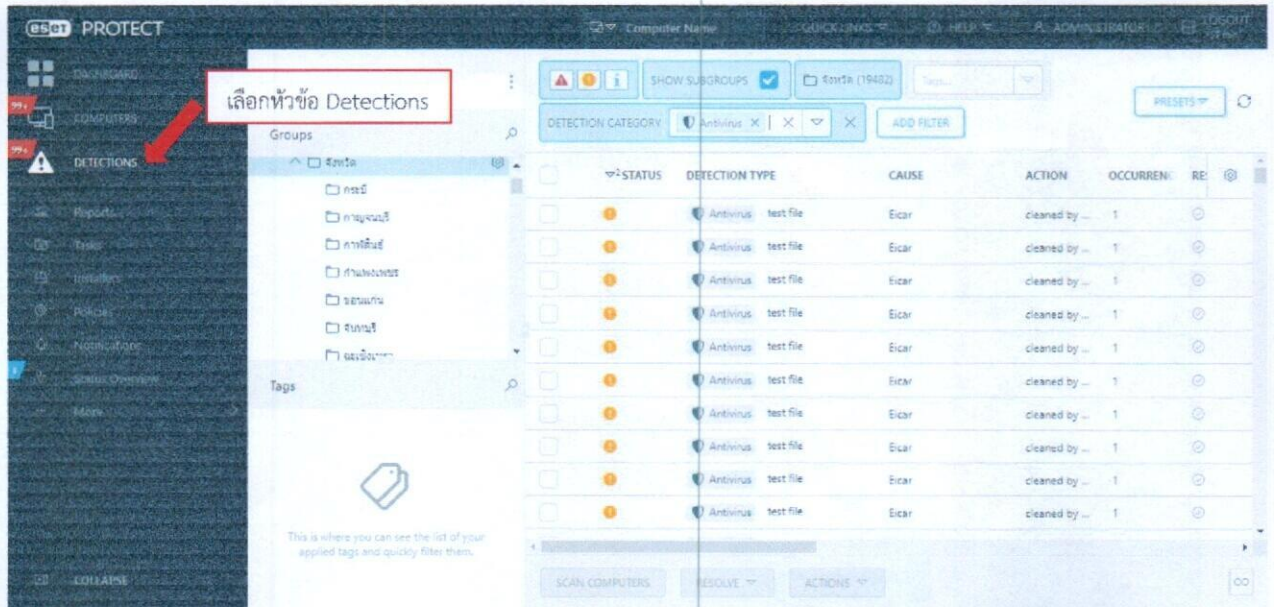
ตัวอย่างแสดงรายละเอียดข้อมูล Install Applications ชื่อเครื่อง ชพ\_119108



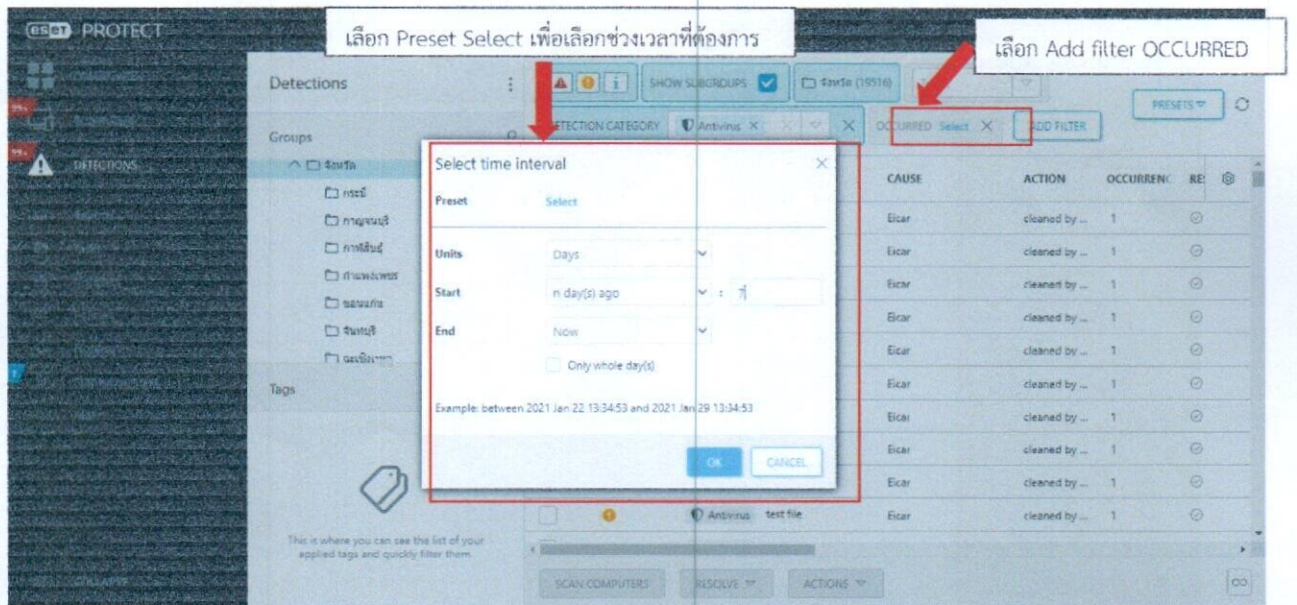
๙. เมนู Detections ใช้สำหรับตรวจสอบไวรัสที่พบทั้งหมดบนเครื่องคอมพิวเตอร์ในแต่ละ Group และระบุได้ว่าสามารถจัดการได้หรือไม่โดยดูจาก Action และสามารถระบุช่วงเวลาที่ต้องการดู Threats Log ได้ ถ้าสถานะเครื่องสีเหลือง คือ โปรแกรมสามารถ clean, delete หรือ quarantine ได้ปกติ แต่ถ้าสถานะเครื่องสีแดง คือ โปรแกรมไม่สามารถ delete ได้

สถานะเครื่องสีแดง เกิดได้หลายสาเหตุที่ไม่สามารถ delete ได้คือเนื่องจากไวรัสที่ถูกตรวจจับได้ไปฝังตัวอยู่ใน system หรือ Application ที่กำลัง running อยู่ จึงไม่สามารถ delete ได้

วิธีแก้ไขให้ทำการ Scan computer ใน safe mode หรือทำ USB Sysrescue เพื่อนำมาสแกน วิธีทำ Sysrescue Scan เข้าเว็บไซต์ <https://www.eset.com/int/support/sysrescue/>



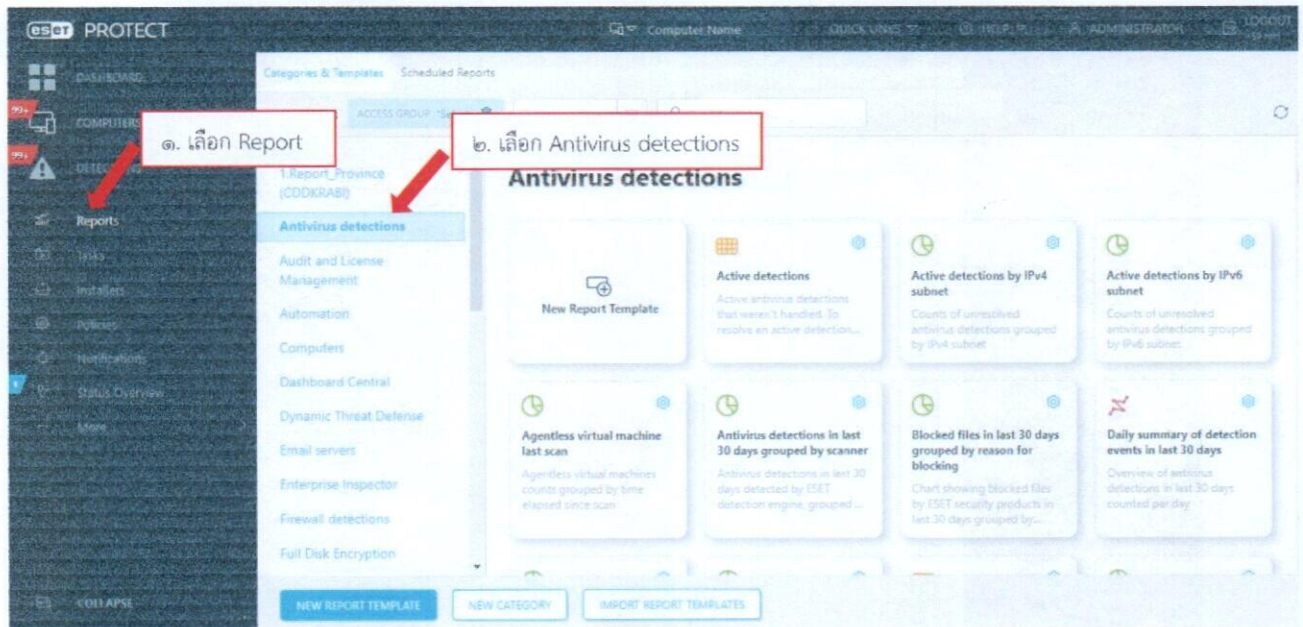
๑๐. การเลือกช่วงเวลาที่จะตรวจสอบไวรัสบนเครื่องคอมพิวเตอร์ในแต่ละ Group สามารถคลิกเลือกหัวข้อ OCCURRED แล้วเลือกช่วงระยะเวลา ตั้งตัวอย่างเลือก ๗ วัน



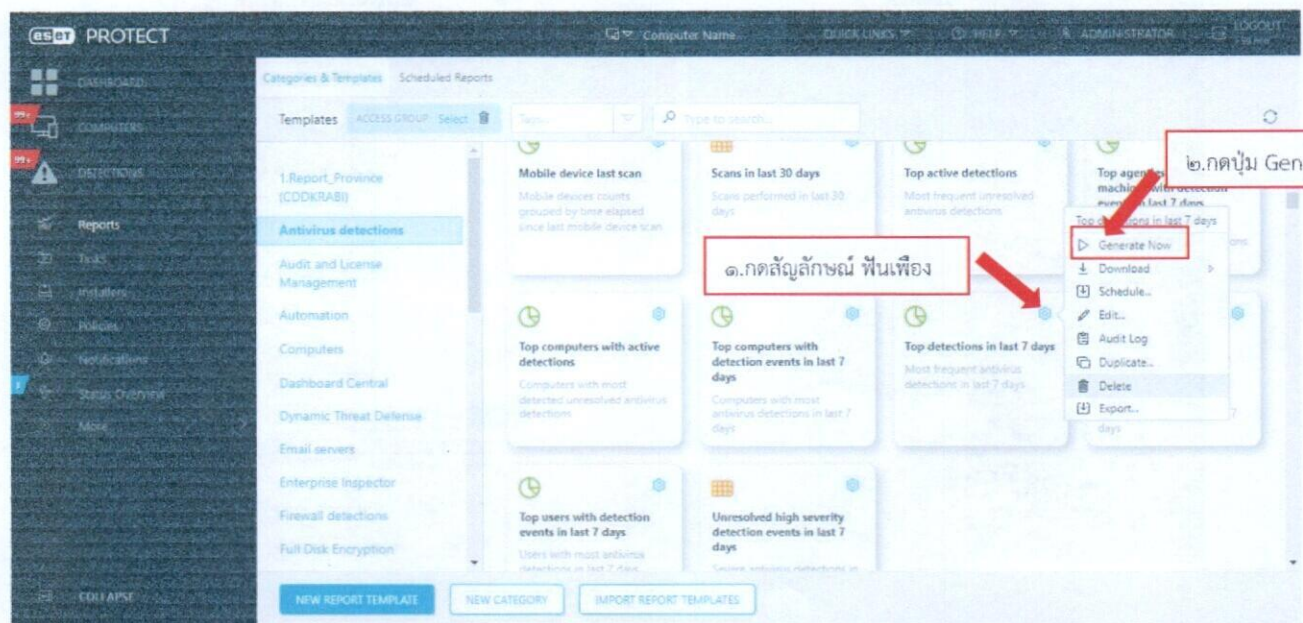
\* ข้อมูลที่แสดงผลการตรวจพบไวรัสบนเมนู Detections จะแสดงชื่อเครื่องคอมพิวเตอร์,ประเภทไวรัส,สถานะการกำจัด ซึ่งสถานะสีแดงคือไม่สามารถลบไฟล์ที่ติดไวรัสได้เพราะ Process อาจจะมีการใช้งานอยู่และสถานะสีเหลืองคือสามารถคลีนไวรัสได้

\*\* ข้อมูลจะมีอายุการจัดเก็บบนระบบ ๖ เดือน หลังจากนั้นจะมีการถูกลบอัตโนมัติ โดยผู้ดูแลระบบส่วนกลาง

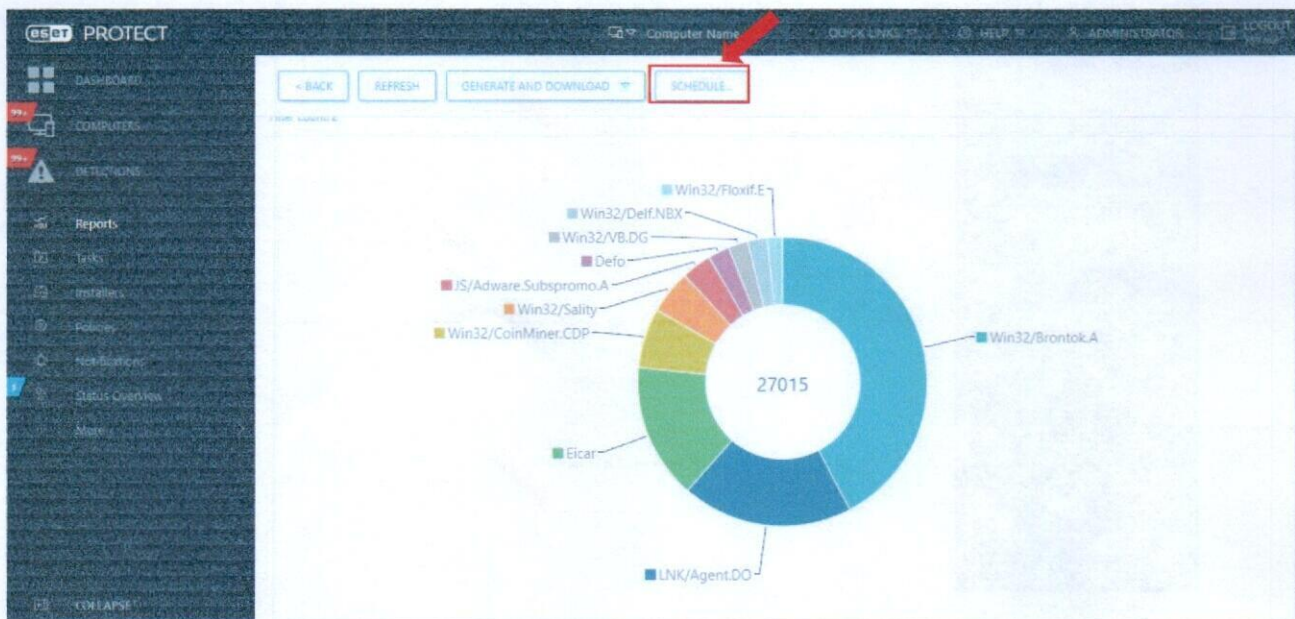
๑๑. เมนู Report ใช้สำหรับแสดงรายงานเกี่ยวกับการโจมตีของไวรัสที่โจมตีเครื่องคอมพิวเตอร์ในระบบ Web Console ให้เลือกหัวข้อ Report Antivirus detections ดังภาพ



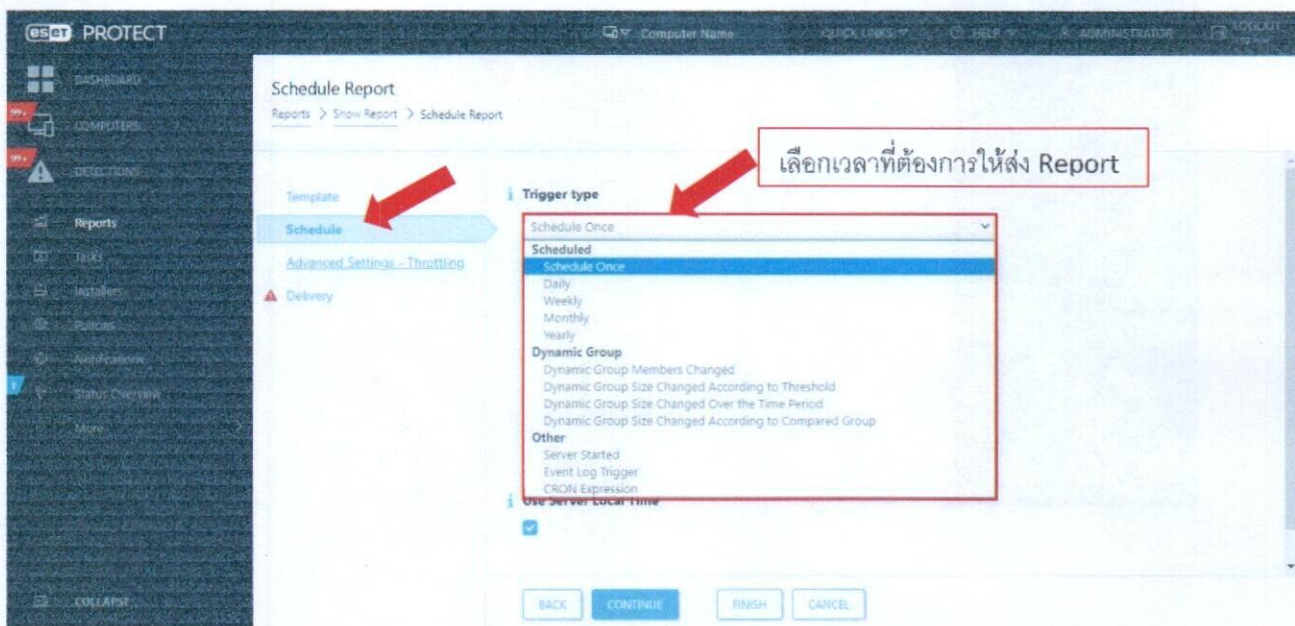
๑๑.๑ จะแสดงรายละเอียด Report ของแต่ละหัวข้อ โดยการเลือกหัวข้อ Report ที่ต้องการแสดง จากนั้น กดปุ่ม Generate Now (ตรวจสอบการโจมตีของไวรัสคอมพิวเตอร์และรายงานผลตามหัวข้อที่เลือก)



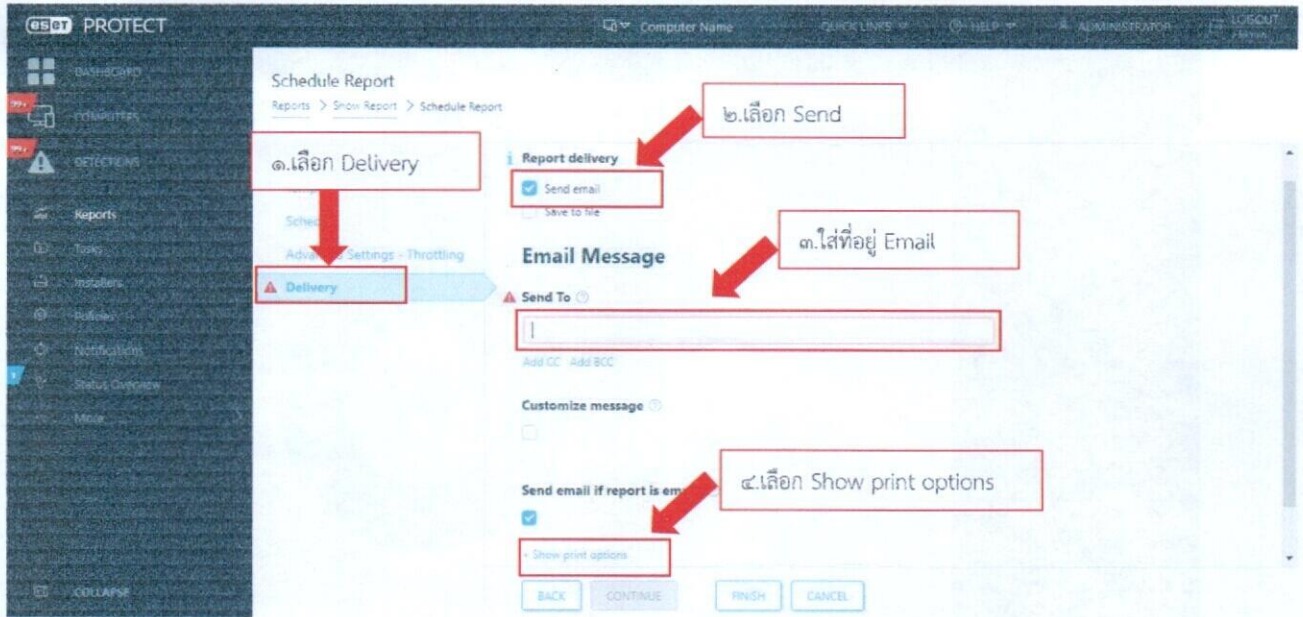
๑๑.๒ แสดง Report หลังจากทำการ Generate report เรียบร้อยจะได้ Report ตามภาพ Report หัวข้อ “Top threats in last 30 days” จากนั้นเลือกทำ Schedule... เพื่อให้ระบบการทำส่ง report ไปยังที่อยู่ email



๑๑.๓ เมื่อกดปุ่ม Schedule... เรียบร้อยแล้ว ให้เลือก Schedule เลือกตั้งเวลาในการส่ง Report อีกครั้ง



๑๑.๔ คลิก Delivery และเลือก Send email ใส่ที่อยู่ email เรียบร้อยแล้ว สามารถเลือกได้ว่าจะรับรายงานเป็นไฟล์รูปแบบไหน โดย คลิกที่ +SHOW PRINT OPTIONS



๑๑.๕ สามารถจะเลือกแสดงรายงานเป็นไฟล์ได้ ๒ รูปแบบคือ PDF, CSV ตามภาพ หลังจากนั้น กดปุ่ม Finish เพื่อทำการส่ง Report ไปยัง E-mail ของผู้รับ

