คู่มือการใช้งานเครื่องมือบริหารจัดการเครื่องลูกข่าย
“ESET Remote Administrator Web console”
เวอร์ชั่น 6.4.2014.0
ปีงบประมาณ ๒๕๖๑
สำหรับผู้รับผิดชอบงานเทคโนโลยีสารสนเทศ
ระดับสำนักงานพัฒนาชุมชนจังหวัด

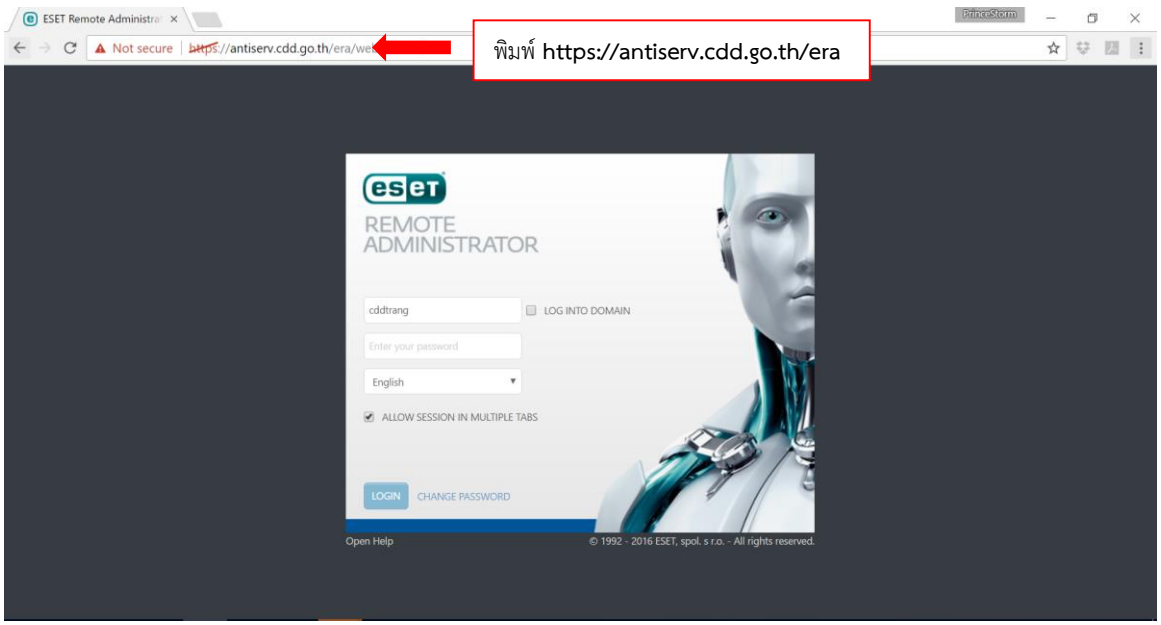
กรมการพัฒนาชุมชน ศูนย์สารสนเทศเพื่อการพัฒนาชุมชน
กลุ่มงานพัฒนาระบบเครือข่าย
โทร. ๐-๒๑๔๑-๖๒๕๒, ๐-๒๑๔๑-๖๒๘๑
www.gn.cdd.go.th

สารบัญ

คู่มือการใช้งาน ESET Remote Administrator Web Console

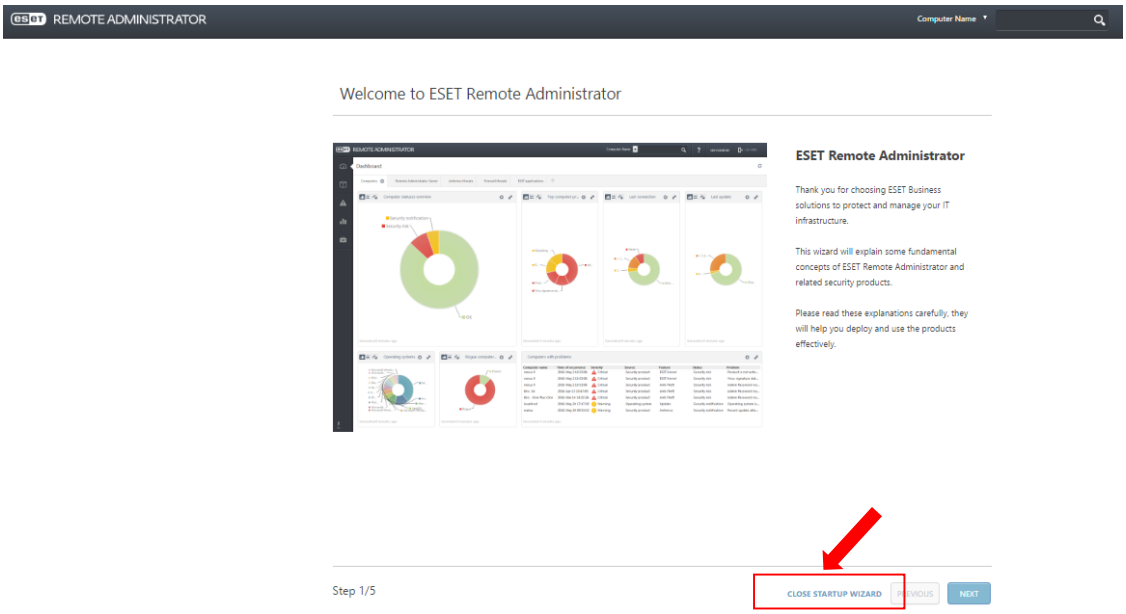
โปรแกรมป้องกันไวรัส ESET Endpoint Version 6.4.2014.0 กำหนดให้มีเว็บไซต์สำหรับบริหารจัดการโปรแกรมป้องกันไวรัส เช่น การตรวจสอบจำนวนเครื่องคอมพิวเตอร์ลูกข่ายที่ติดตั้งโปรแกรมป้องกันไวรัส การตรวจสอบการโจมตีของไวรัสคอมพิวเตอร์ การรายงานผล (Report) การอัพเดทฐานข้อมูลไวรัส เป็นต้น เพื่อให้การใช้งานโปรแกรมป้องกันไวรัสเป็นไปอย่างมีประสิทธิภาพ สามารถบริหารจัดการโปรแกรมป้องกันไวรัส ได้สะดวกมากยิ่งขึ้น จึงได้จัดทำคู่มือการใช้งาน ESET Remote Administrator Web Console ให้กับผู้รับผิดชอบงานด้านเทคโนโลยีสารสนเทศ ใช้เป็นแนวทางในการปฏิบัติงาน โดยมีขั้นตอน ดังนี้

๑. เข้าสู่เว็บไซต์โดยเปิดเว็บบราวเซอร์แล้วพิมพ์ URL > https://antiserv.cdd.go.th/era เพื่อเข้าสู่หน้า Login

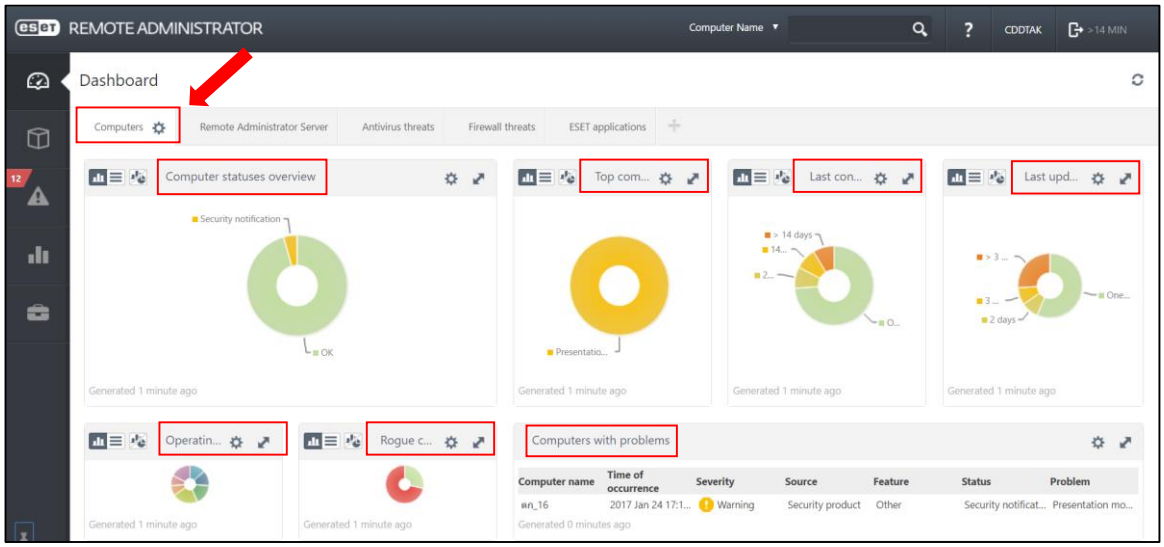


๒. กรอก User และ Password ของแต่ละจังหวัด/ศูนย์ศึกษา/วิทยาลัย แล้วกดปุ่ม  เพื่อเข้าสู่ระบบ

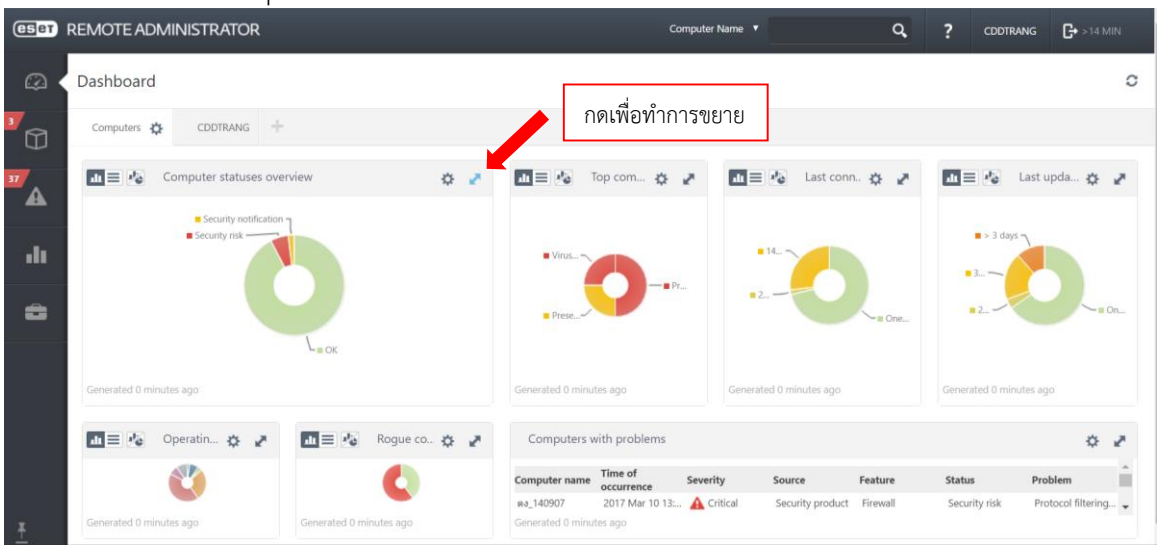
- เมื่อ Login เข้าสู่ระบบแล้วปรากฏหน้าจอดังภาพ ให้กดที่ปุ่ม CLOSE STARTUP WIZARD



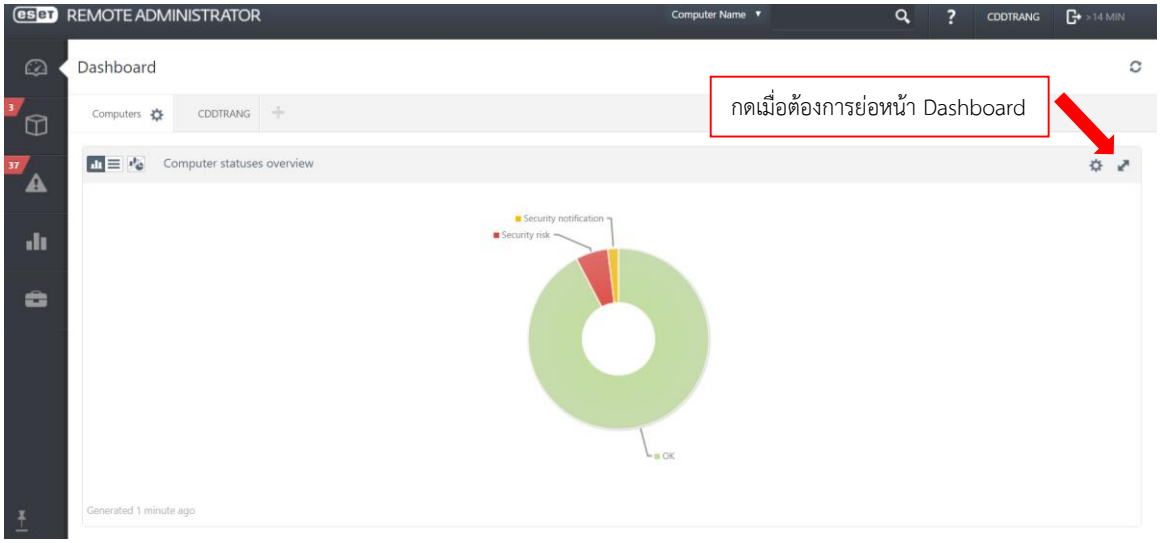
๓. เมื่อ Login เข้าสู่ระบบแล้วจะปรากฏหน้า Dashboard : ในหน้า Dashboard ใช้สำหรับตรวจสอบสถานะเครื่องคอมพิวเตอร์แบบเรียลไทม์ ให้คลิก Computer จะแสดง template ให้ตรวจสอบสถานะโปรแกรมหลายรูปแบบ เช่น หัวข้อ Computer statuses overview เป็นการตรวจสอบสถานะการอัพเดทของเครื่องว่ามีความผิดปกติหรือไม่สังเกตได้จากสีของกราฟ โดยแบ่งออกเป็น สีเขียว - การอัพเดทปกติ สีส้ม - ไม่ได้มีการอัพเดทมา ซักระยะหนึ่งหรือมีการใช้ Presentation mode และสีแดง - ฟังก์ชันไม่สมบูรณ์หรือไม่ได้อัพเดทมานานมาก และผู้ดูแลโปรแกรมสามารถคลิกดูแต่ละ template เพื่อตรวจสอบข้อมูล คือ Top Computer problem, Last connection, Last update, Operating system, Rague computer ratio และ Computer with problem ดังภาพ



๓.๑ ในการขยายดูหน้าต่างสถานะของ Dashboard แต่ละ template สามารถทำได้โดยการกดปุ่ม  ดูข้อมูลของ Dashboard นั้นๆ ดังภาพ

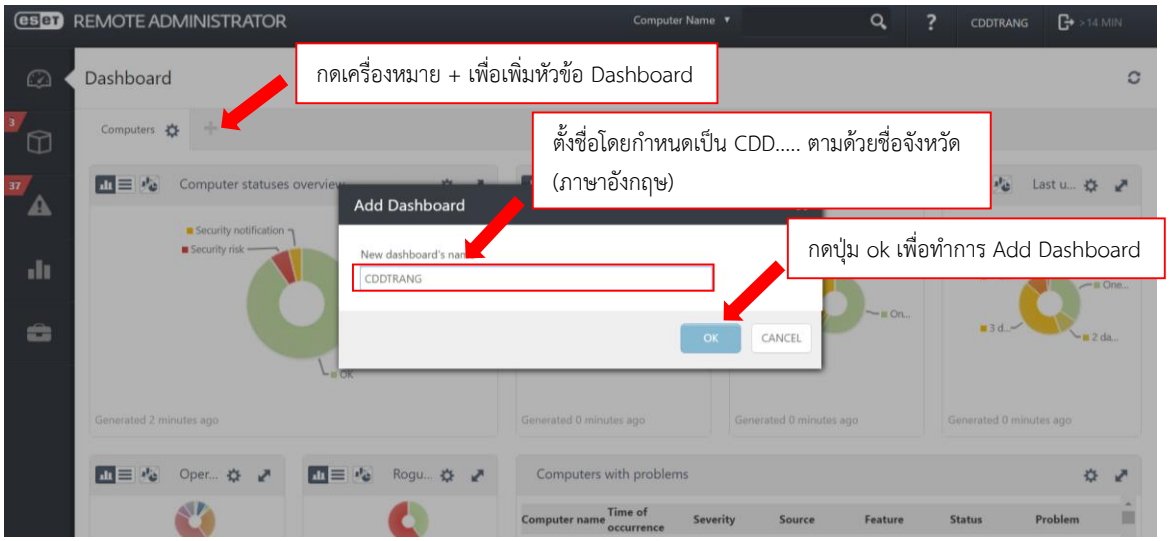


๓.๒ หน้าจอ template แสดงการขยายหน้า Dashboard เมื่อต้องการย่อหน้า Dashboard กลับไปเป็นหน้าเดิมให้กดปุ่ม  อีกครั้ง

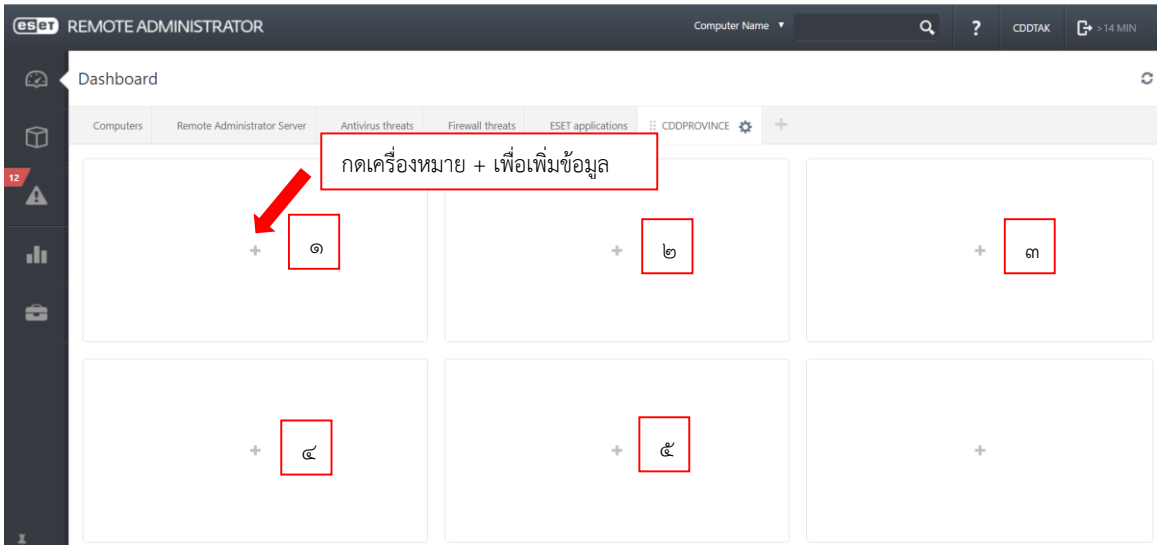


๓.๓ ในขั้นตอนนี้ผู้ดูแลโปรแกรมจะต้องเพิ่มหัวข้อ Dashboard เพื่อแสดงผลการรายงาน (Report) ของแต่ละจังหวัดมีขั้นตอน ดังนี้

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

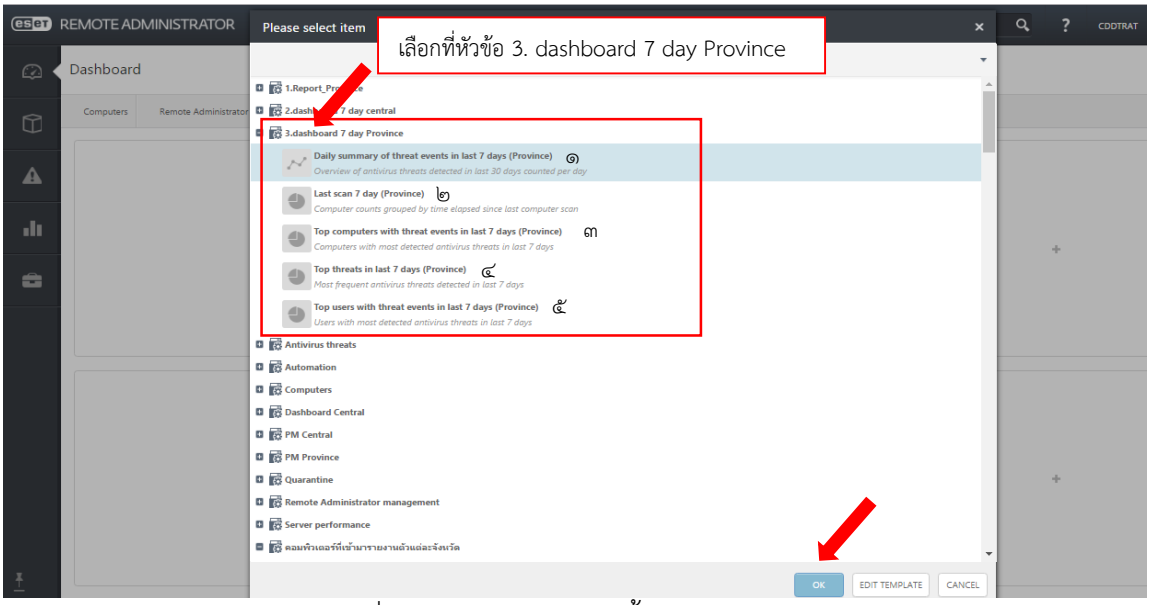


๒) เมื่อกดปุ่ม ok แล้ว จะแสดงหน้าต่างการเพิ่ม Dashboard ให้กดเครื่องหมาย + ดังภาพ เมื่อกดเครื่องหมาย + แล้วจะพบ report templete สำหรับจังหวัด โดยเลือกที่หัวข้อ “3. dashboard 7 day Province”

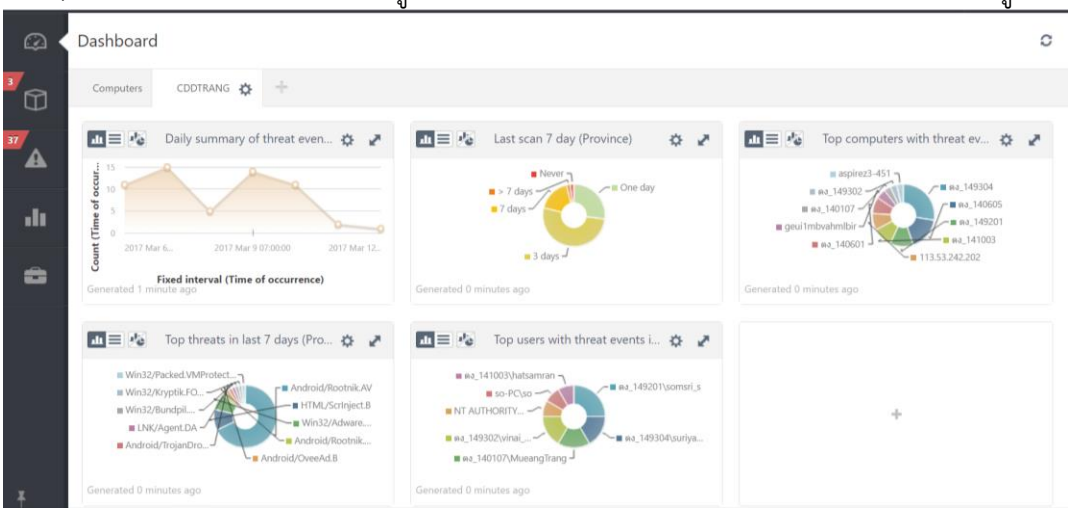


๓) ให้คลิกเลือกหัวข้อเรียงตามลำดับหมายเลขให้ครบ ๕ หัวข้อ ดังนี้

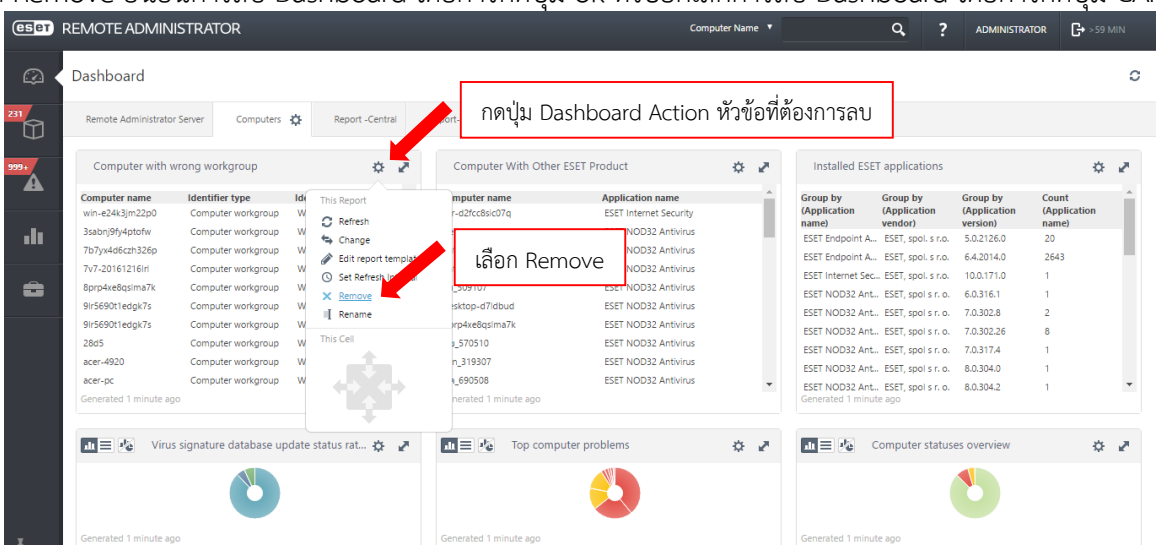
- กดเครื่องหมาย + หัวข้อ ๑ เลือก Daily summary of threat event in ๗ days - ใช้ตรวจสอบจำนวนไวรัสที่เข้ามาโจมตีในแต่ละวัน ภายใน ๗ วัน
- กดเครื่องหมาย + หัวข้อ ๒ เลือก Last scan ๗ days - ใช้ตรวจสอบการสแกนของเครื่องแต่ละเครื่องภายใน ๗ วัน
- กดเครื่องหมาย + หัวข้อ ๓ เลือก Top computer with threat event in 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



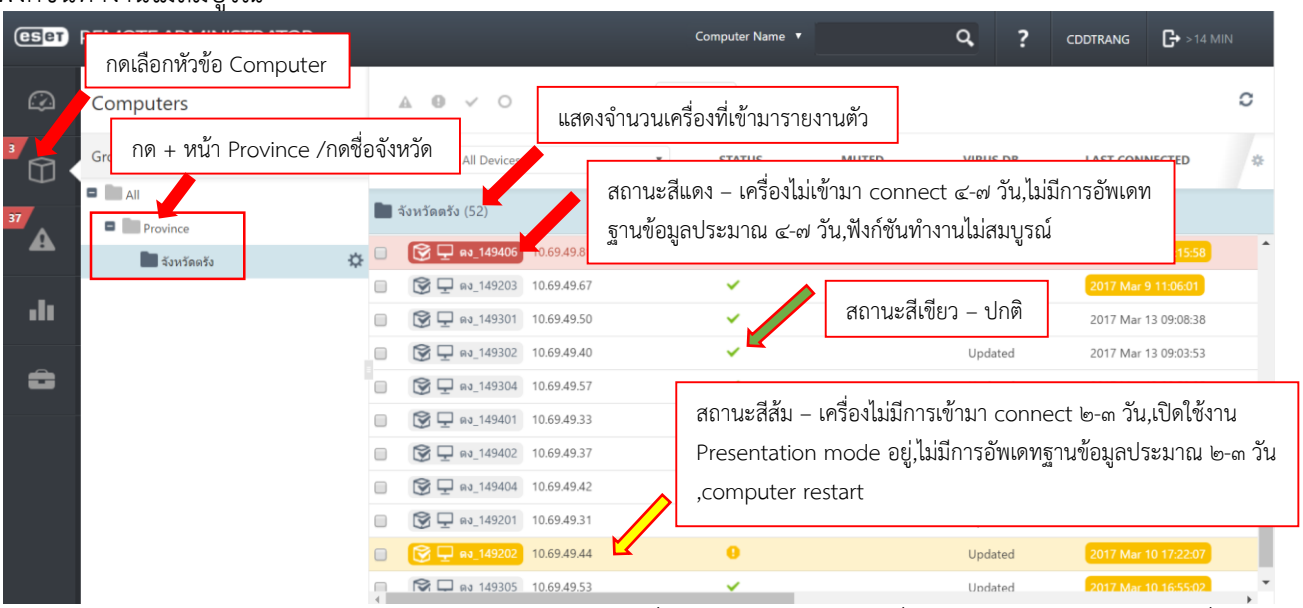
๔. การตรวจสอบสถานะเครื่องคอมพิวเตอร์ โดยกดเลือกหัวข้อ Computer ด้านซ้ายมือ

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

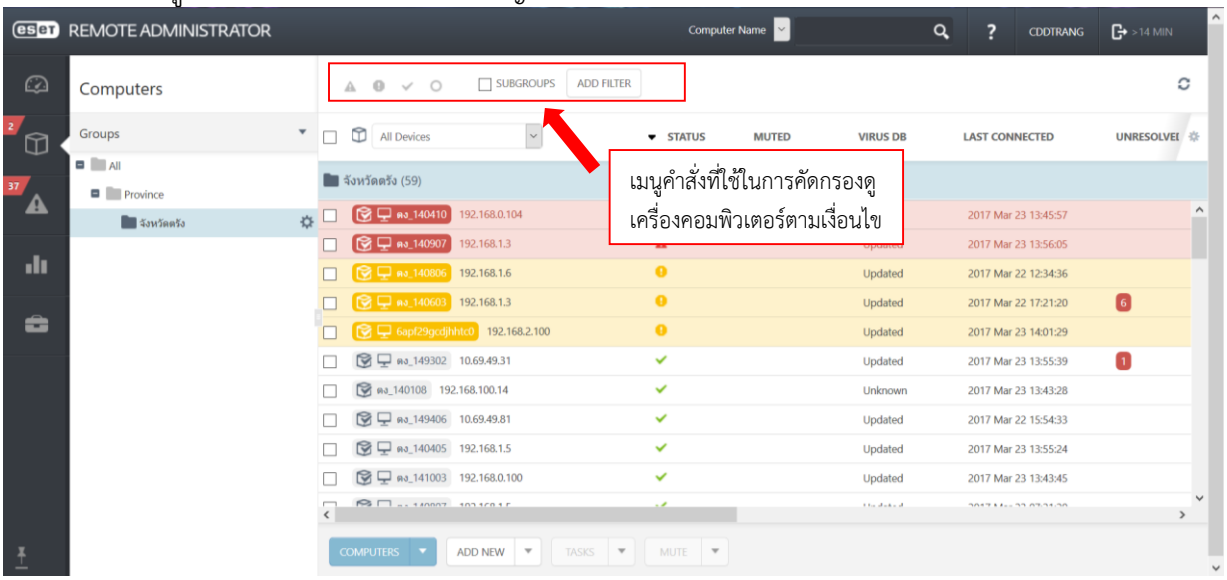
๔.๑ ให้คลิกเลือก Computer แล้วให้กดปุ่มเครื่อง + หน้าหัวข้อ Province กดปุ่มโฟลเดอร์ชื่อจังหวัด เพื่อแสดงรายละเอียดของเครื่องคอมพิวเตอร์ที่เชื่อมต่อเข้ามาในระบบของแต่ละจังหวัด

๔.๒ เครื่องคอมพิวเตอร์แต่ละเครื่องจะมีการแสดงสถานการณ์แจ้งเตือน คือ

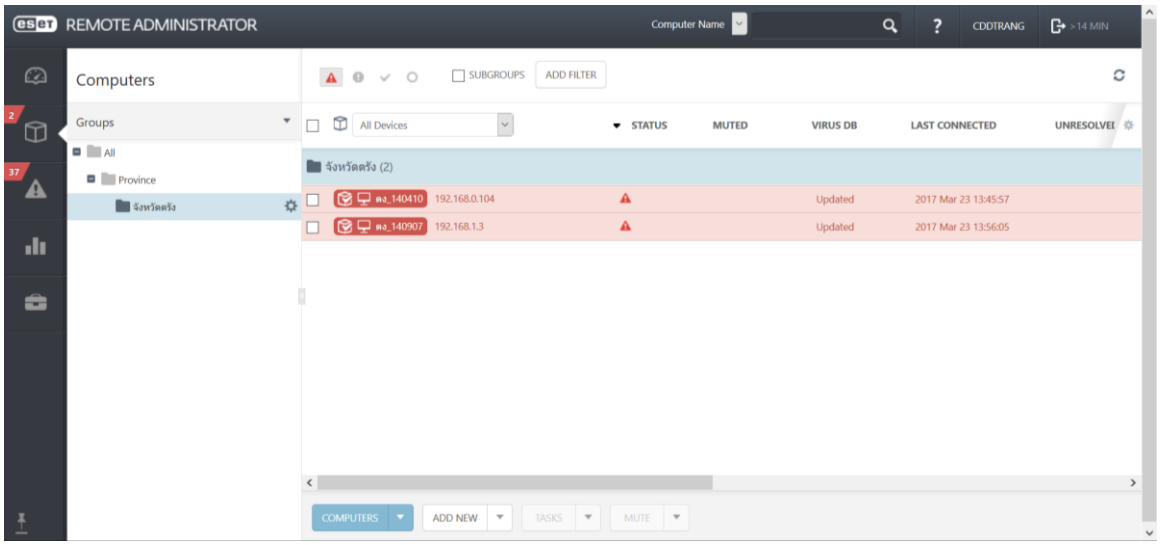
- สถานะสีเขียว : เครื่องปกติ
- สถานะสีส้ม : เครื่องไม่มีการเข้ามา connect หรือเปิดใช้งาน Presentation mode อยู่ หรือไม่มีการอัพเดทฐานข้อมูลไวรัส ประมาณ ๒-๓ วัน
- สถานะสีแดง : เครื่องไม่เข้ามา connect หรือไม่มีการอัพเดทฐานข้อมูลไวรัส ประมาณ ๔-๗ วัน หรือฟังก์ชันทำงานไม่สมบูรณ์



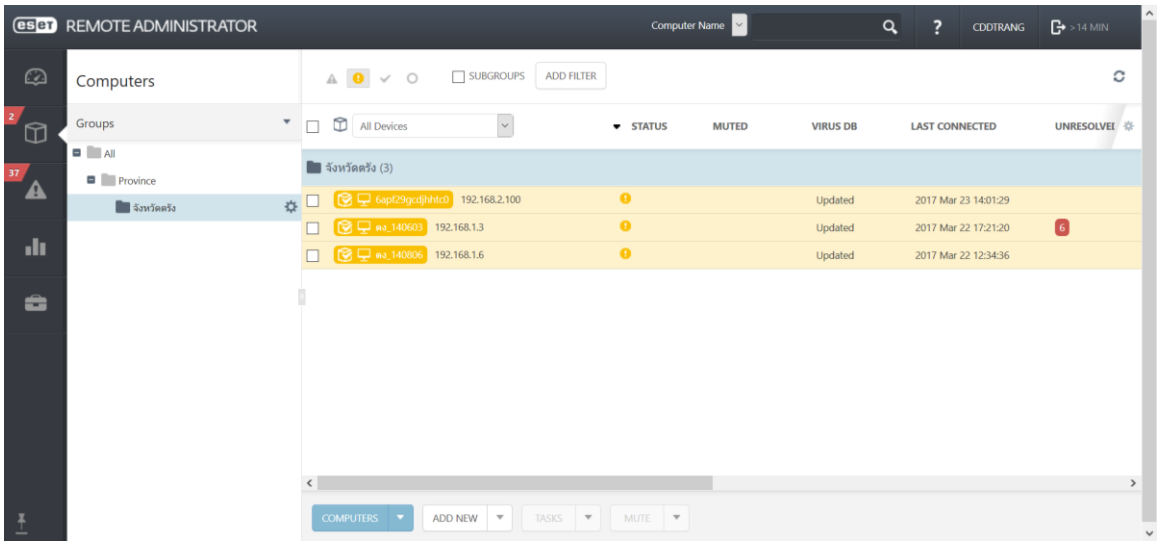
๔.๓ เมนู Computer ผู้ดูแลโปรแกรม สามารถที่จะคัดกรองดูข้อมูลเครื่องคอมพิวเตอร์เฉพาะส่วนที่ต้องการได้ จากเมนูตามภาพ โดยคลิกเลือกตามสัญลักษณ์ ดังนี้



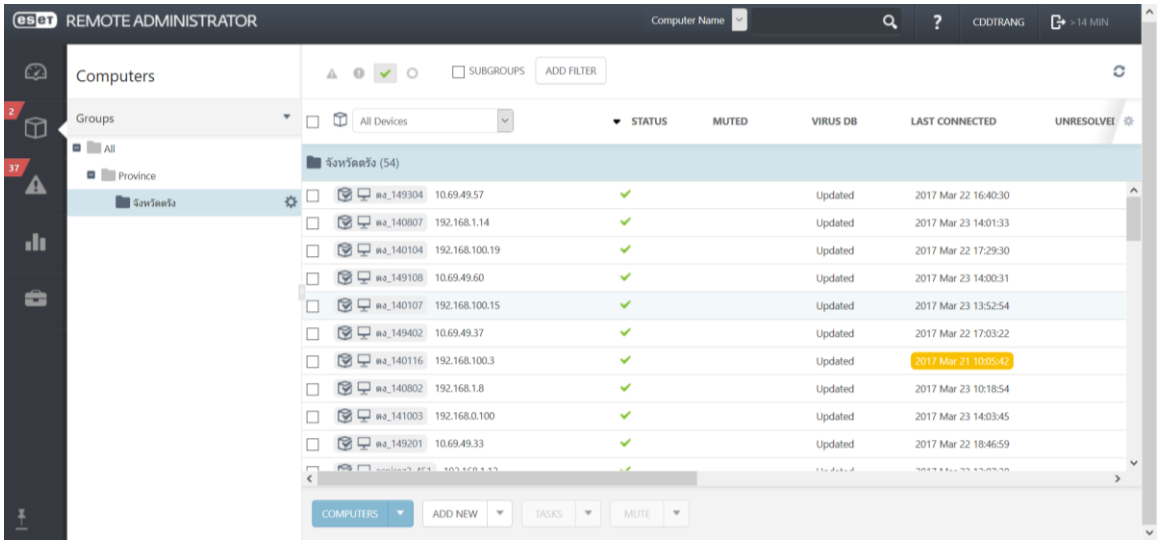
๔.๓.๑ แสดงการคัดกรองเฉพาะเครื่องคอมพิวเตอร์ที่แจ้งสถานะเป็นสีแดง



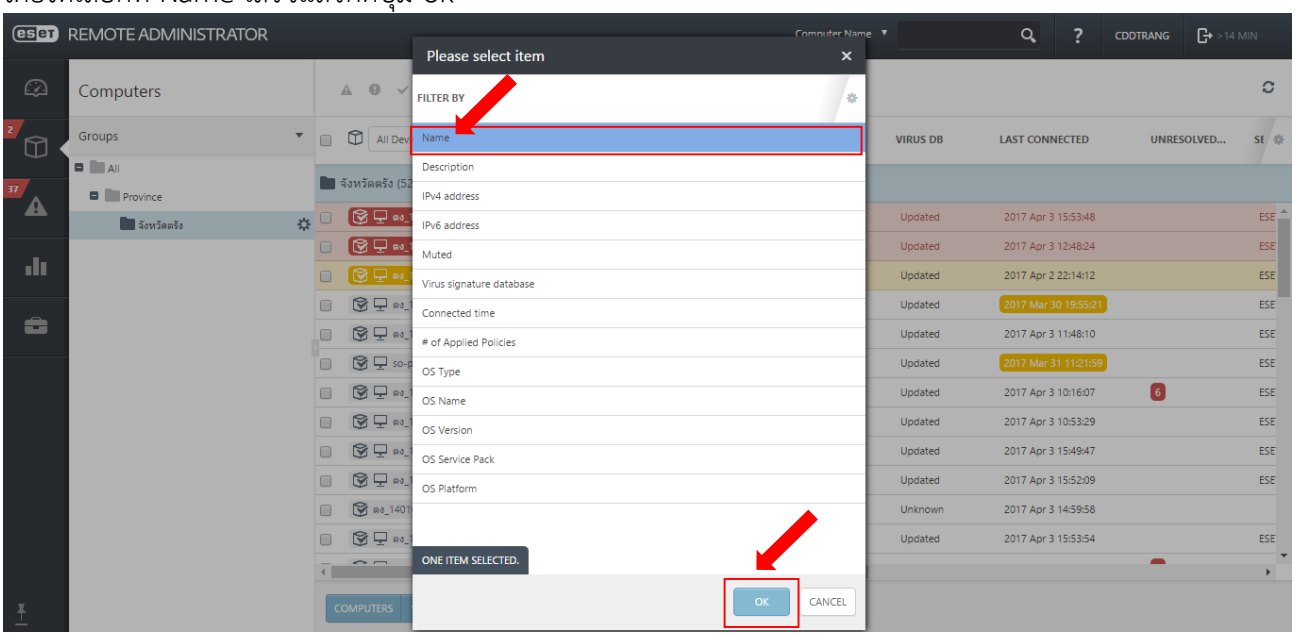
๔.๓.๒ แสดงการคัดกรองเฉพาะเครื่องคอมพิวเตอร์ที่แจ้งสถานะเป็นสีเหลือง



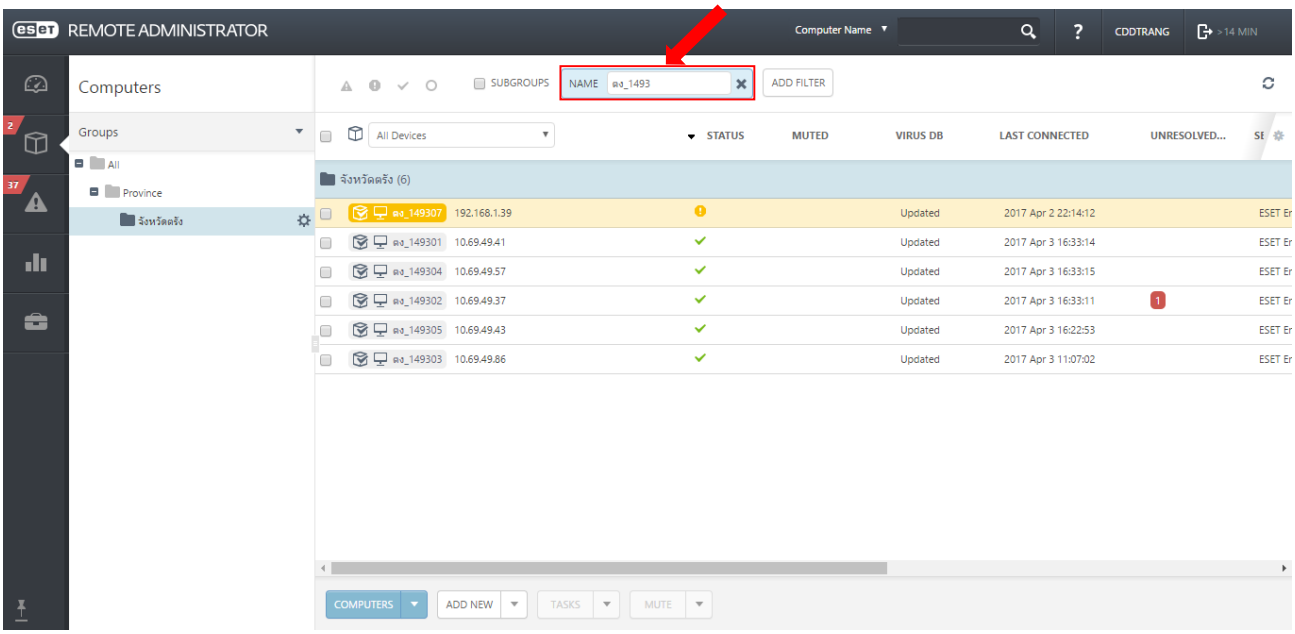
๔.๓.๓ แสดงการคัดกรองเฉพาะเครื่องคอมพิวเตอร์ที่แจ้งสถานะเป็นสีเขียว



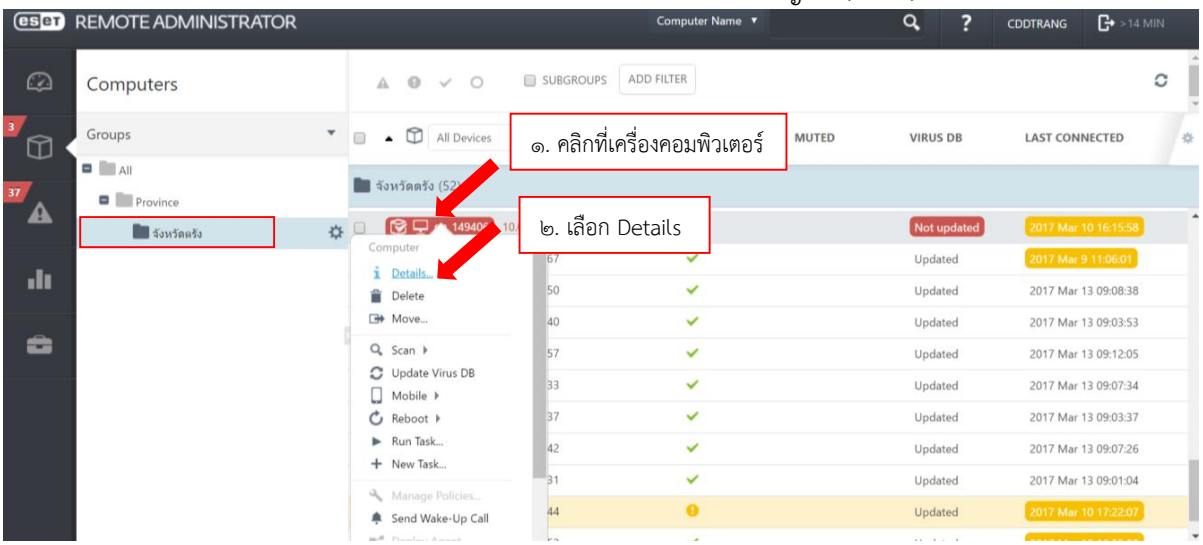
๔.๓.๔ ในกรณีที่ต้องการคัดกรองเครื่องคอมพิวเตอร์โดยระบุเงื่อนไขอื่นๆ ให้คลิกที่ปุ่ม ADD FILTER จะปรากฏตัวเลือกในการคัดกรองเพิ่มเติม ดังตัวอย่าง แสดงการคัดกรองเครื่องคอมพิวเตอร์ที่ชื่อ ตง_1493 โดยให้เลือกที่ Name เสร็จแล้วกดปุ่ม ok



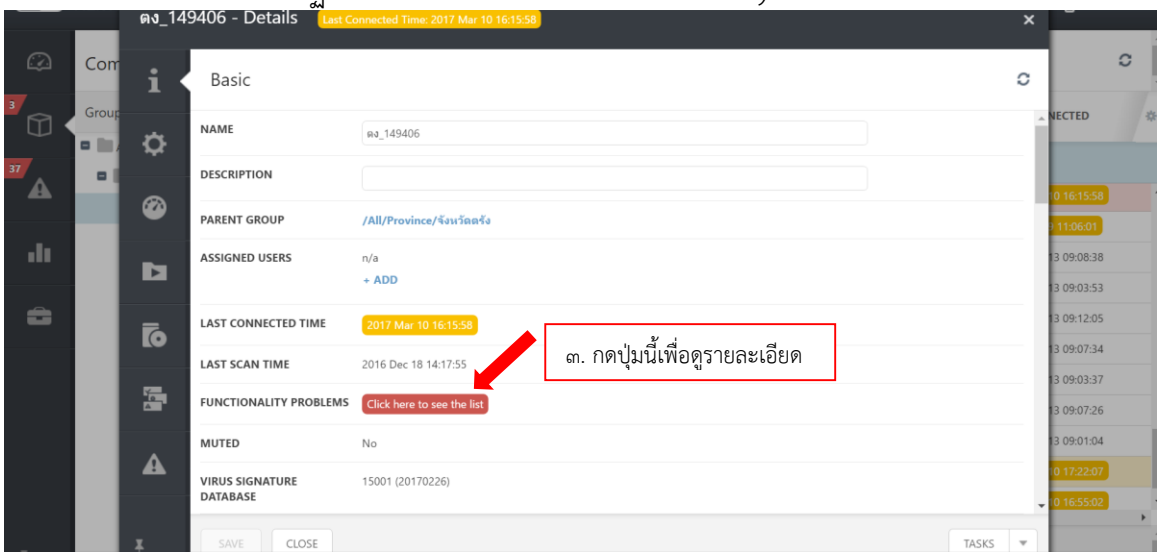
- ปรากฏหน้าจอดังภาพ ให้ใส่ชื่อเครื่องคอมพิวเตอร์ ตง_1493 เสร็จแล้วกด Enter หน้าจอจะแสดงเครื่องคอมพิวเตอร์ชื่อ ตง_1493 ทุกเครื่อง หากจะกลับสู่หน้าจอเดิมให้กดปิดที่ ✖



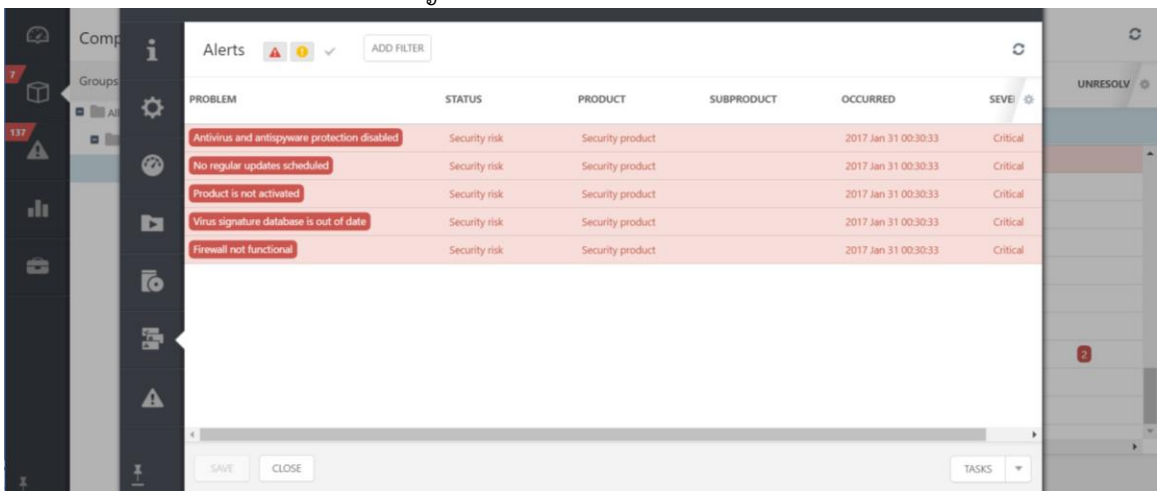
๕. การตรวจสอบเครื่องคอมพิวเตอร์ที่ผิดปกติหรือมีปัญหา เพื่อให้ผู้ดูแลโปรแกรมตรวจสอบเครื่องคอมพิวเตอร์ที่มีความผิดปกติ และวิธีแก้ไขโดยเลือกที่เครื่องคอมพิวเตอร์ที่มีปัญหา (สีแดง) แล้วเลือก Details ดังภาพ



หลังจากนั้นจะปรากฏหน้าจอนี้ ให้คลิกที่หัวข้อ Functionality Problems ดังภาพ



หน้าจอจะแสดงปัญหาที่เกิดขึ้นภายในเครื่องคอมพิวเตอร์ ดังภาพ

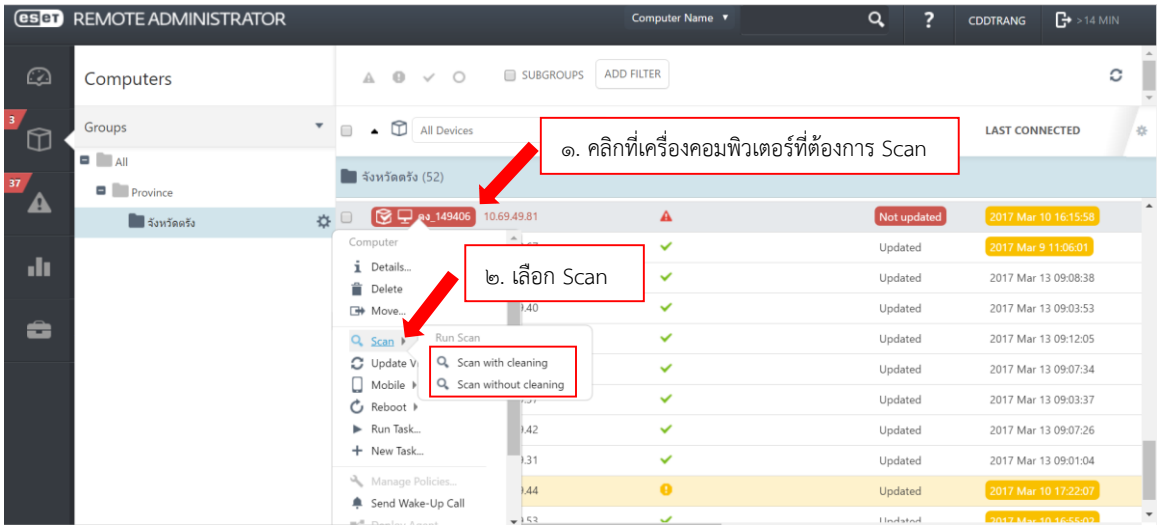


รายละเอียดแจ้งเตือนปัญหาที่อาจเกิดขึ้นภายในเครื่องคอมพิวเตอร์ และวิธีแก้ไขปัญหา ดังนี้

ข้อมูลแจ้งสถานะ	สีสถานะ	ความหมาย	วิธีแก้ไข
Antivirus and antispyware protection disabled	แดง	อาจมีการปิดการใช้งานโปรแกรม Antivirus ชั่วคราว หรือโปรแกรมทำงานไม่สมบูรณ์ทำให้ฟังก์ชั่น antivirus and spyware ไม่ถูกเปิดใช้งาน	- หากฟังก์ชั่นถูกปิดอยู่ให้ทำการเปิดใช้งานได้ทันที - หากฟังก์ชั่นไม่สมบูรณ์ให้ทำการถอนการติดตั้งออกโดยใช้ Tools uninstaller และติดตั้งใหม่อีกครั้ง
No regular update scheduled	แดง	คือ system task ใน scheduled อาจมีปัญหา	- ต้องทำการกำหนด scheduler update ใหม่ - ถอนการติดตั้งโดยใช้ tools uninstaller และ ติดตั้งใหม่อีกครั้ง
Product is not Activated	แดง	เครื่องยังไม่การ active license	- รอการส่ง task จาก server - หากรอนานเกิน ๒๔ ชม. ให้ติดต่อเจ้าหน้าที่บริษัทได้โดยตรง
Virus signature database is out date	แดง	ฐานข้อมูลไวรัสไม่ได้รับการอัพเดท	- สั่ง task update database - หากสั่งแล้วติดให้ activation license ให้รอหากเกิน ๒๔ ชม. ให้ติดต่อเจ้าหน้าที่บริษัทได้โดยตรง
Firewall not function	แดง	ฟังก์ชั่น Firewall มีปัญหา	- เนื่องจากผลิตภัณฑ์ของทางกรมพัฒนาชุมชนไม่ได้ใช้ Product firewall ต้องทำการถอนการติดตั้งโดย Tools uninstaller และติดตั้งใหม่อีกครั้ง
Protocol filtering not functional	แดง	ฟังก์ชั่นเกี่ยวกับ การสแกนการใช้งานอินเตอร์เน็ต โปรโตคอล มีปัญหา มักเกิดจากการติดตั้งโปรแกรมทับโปรแกรมป้องกันไวรัสของเดิมบนเครื่องคอมพิวเตอร์นั้น ๆ	- ถอนการติดตั้งโดยใช้ tools uninstaller และติดตั้งใหม่อีกครั้ง
Presentation Mode is enabled	เหลือง	มีการเปิดใช้งานหน้าจอแบบ Full screen เช่น PowerPoint หรือการเปิดไฟล์ภาพยนตร์แบบเต็มหน้าจอ	- หลังจากผู้ใช้ออกจากการใช้งานแบบเต็มหน้าจอ สถานะจะหายไปเอง
Recent update attempts failed	เหลือง	โปรแกรมป้องกันไวรัส ไม่สามารถอัพเดทฐานข้อมูลไวรัสได้ในช่วงเวลานั้นๆ เกิน ๓ ครั้งขึ้นไป	- สั่ง task update database - หากสั่งแล้วไม่อัพเดทให้ activation license ให้รอหากเกิน ๒๔ ชม. ให้ติดต่อเจ้าหน้าที่บริษัทได้โดยตรง

ข้อมูลแจ้งสถานะ	สีสถานะ	ความหมาย	วิธีแก้ไข
Product is not connected. No connection attempt occurred.	เหลือง	เครื่องคอมพิวเตอร์ดังกล่าว ยังไม่ได้มีการติดตั้งโปรแกรมป้องกันไวรัส เวอร์ชั่น ๖ และโปรแกรมป้องกันไวรัสเดิมเวอร์ชั่น ๕ มักจะมีการแจ้งเกี่ยวกับการทำงานที่ไม่สมบูรณ์ ถ้าหากเครื่องไม่เคยลงโปรแกรมป้องกันไวรัสแสดงว่าการเขียน registry ของโปรแกรมอาจไม่สมบูรณ์	- ถอนการติดตั้งโปรแกรมป้องกันไวรัส เวอร์ชั่น ๕ โดยใช้ tools uninstaller และติดตั้งโปรแกรมป้องกันไวรัส เวอร์ชั่น ๖ ใหม่อีกครั้ง
Product is installed but it is not running	เหลือง	เครื่องคอมพิวเตอร์ดังกล่าว ยังไม่ได้มีการติดตั้งโปรแกรมป้องกันไวรัส เวอร์ชั่น ๖ และโปรแกรมป้องกันไวรัสเดิมเวอร์ชั่น ๕ มักจะมีการแจ้งเกี่ยวกับการทำงานที่ไม่สมบูรณ์หรือเกิดจากการติดตั้งโปรแกรมป้องกันไวรัส เวอร์ชั่น ๖ ที่ไม่สมบูรณ์	- ถอนการติดตั้งโปรแกรมป้องกันไวรัส โดยใช้ tools uninstaller และ ติดตั้งโปรแกรมป้องกันไวรัส เวอร์ชั่น ๖ ใหม่อีกครั้ง

๖. การสั่งสแกนเครื่องคอมพิวเตอร์ กรณีที่เครื่องคอมพิวเตอร์ไม่ได้มีการสแกน ให้คลิกที่เครื่องคอมพิวเตอร์ที่ต้องการสแกน แล้วเลือกหัวข้อ Scan ดังภาพ

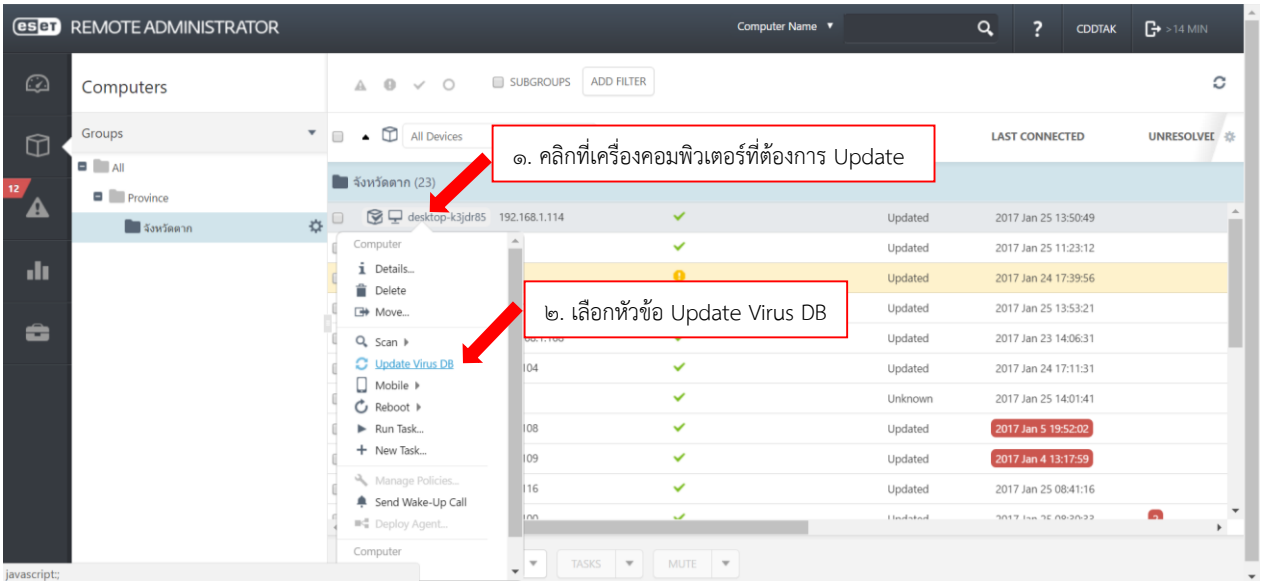


การสแกนสามารถสแกนได้ ๒ แบบดังนี้

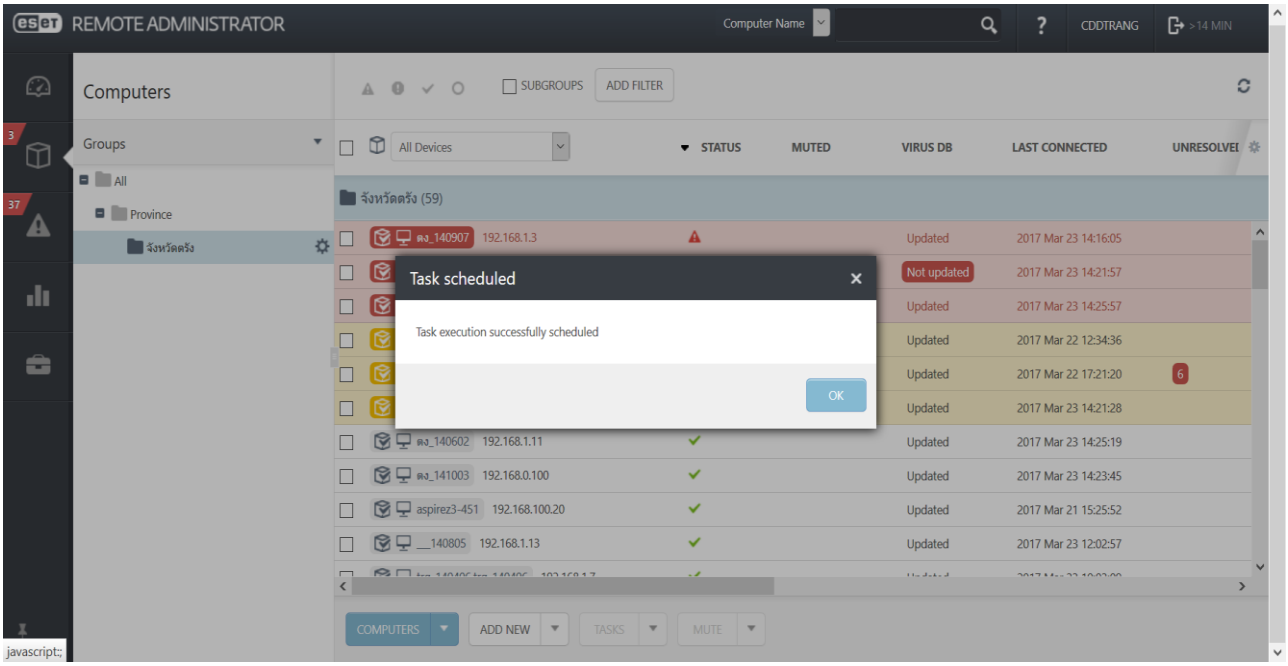
☐ scan with cleaning - โปรแกรมจะทำการสแกนไวรัสให้ทั้งหมดเมื่อตรวจพบก็จะทำการ clean ทันที

☐ scan without cleaning - โปรแกรมจะทำการสแกนไวรัสให้ทั้งหมดแต่เมื่อตรวจพบก็จะไม่ทำการ clean

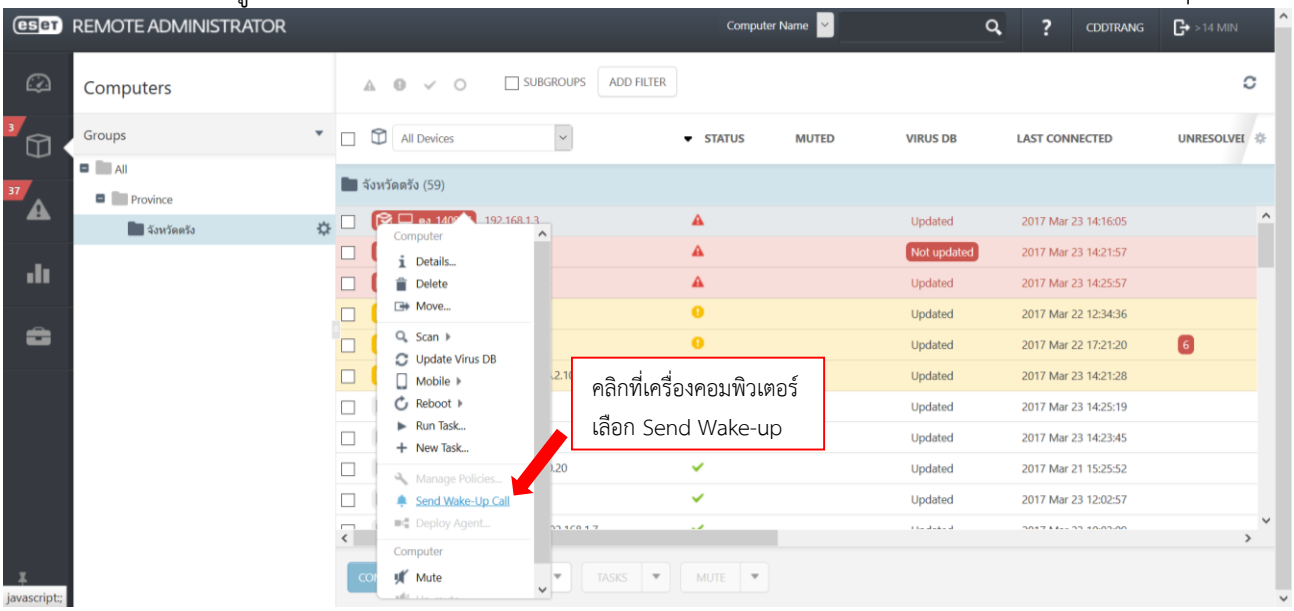
๗. การ Update Virus DB เป็นการสั่ง Update เครื่องคอมพิวเตอร์หากพบว่าเครื่องที่อยู่ใน Group ไม่มีการ Update โดยคลิกเครื่องที่ไม่มีการ Update และเลือกหัวข้อ Update Virus DB



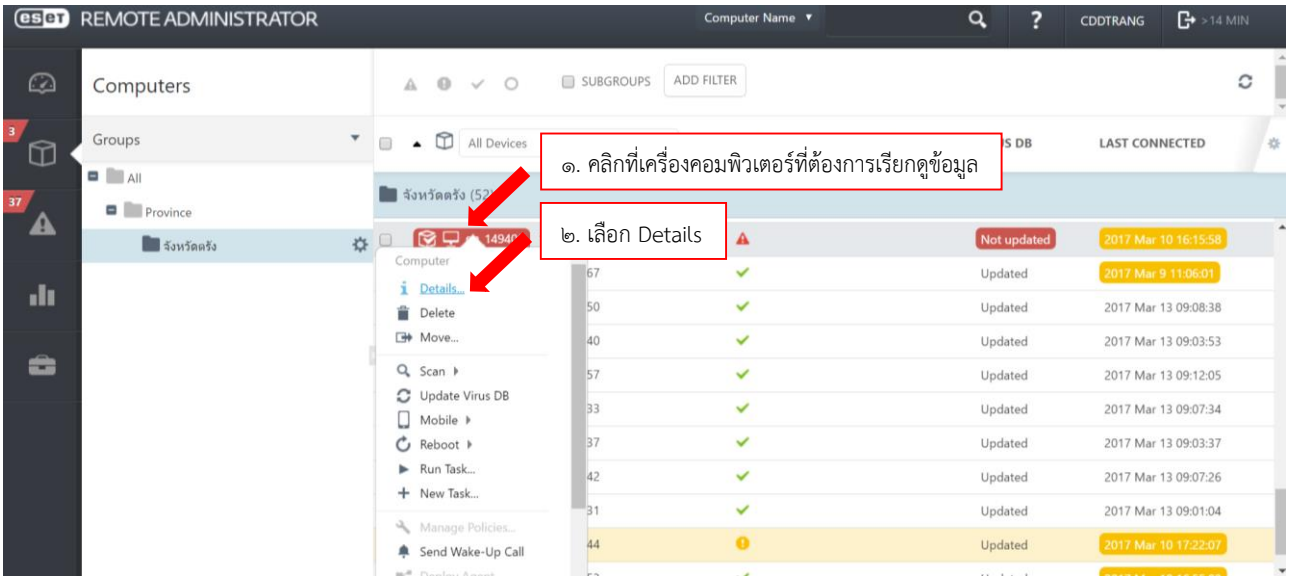
๗.๑ หลังจากสั่งการทำงานไปแล้ว ไม่แสดงการสแกนหรือการอัพเดท ระบบจะมีหน้าจอแจ้งข้อมูลว่าคำสั่งมีการส่งออกไปยังเครื่องลูกข่ายเรียบร้อยแล้ว แต่ไม่ได้หมายความว่าเครื่องลูกข่ายจะดำเนินการตามคำสั่งในทันที



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

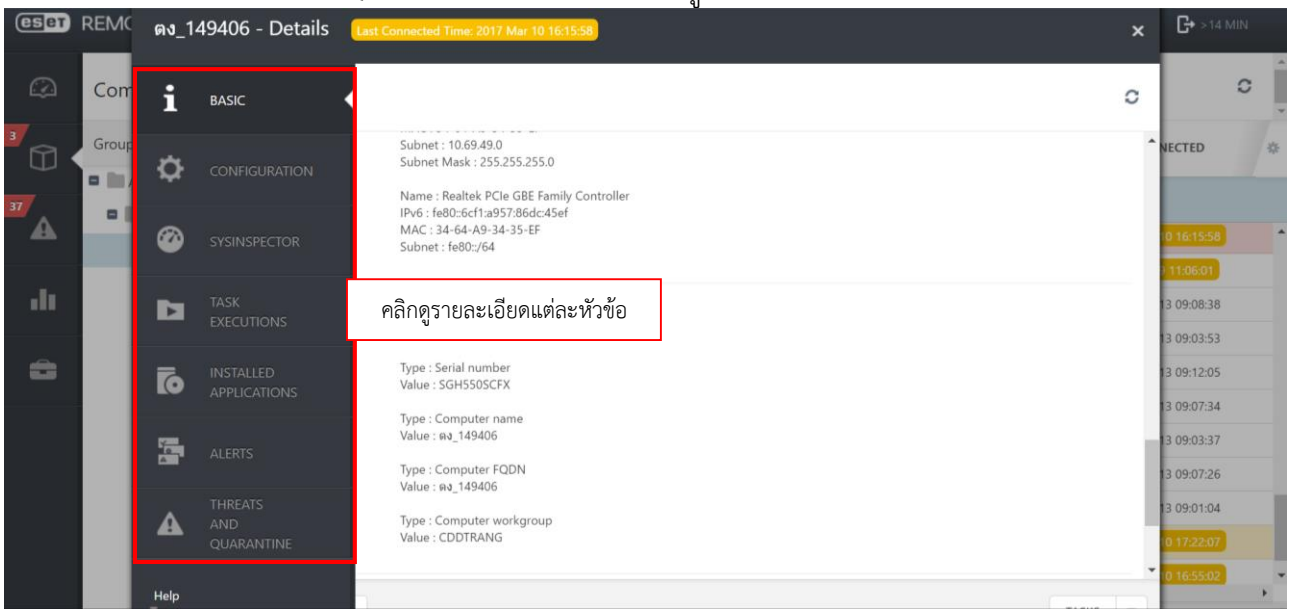


๘. ผู้ดูแลโปรแกรม สามารถเรียกดูรายละเอียดข้อมูลเครื่องคอมพิวเตอร์แต่ละเครื่องที่มารายงานตัวในระบบ Web Console โดยคลิกที่เครื่องคอมพิวเตอร์ที่ต้องการดูข้อมูล แล้วเลือกหัวข้อ Details ดังภาพ

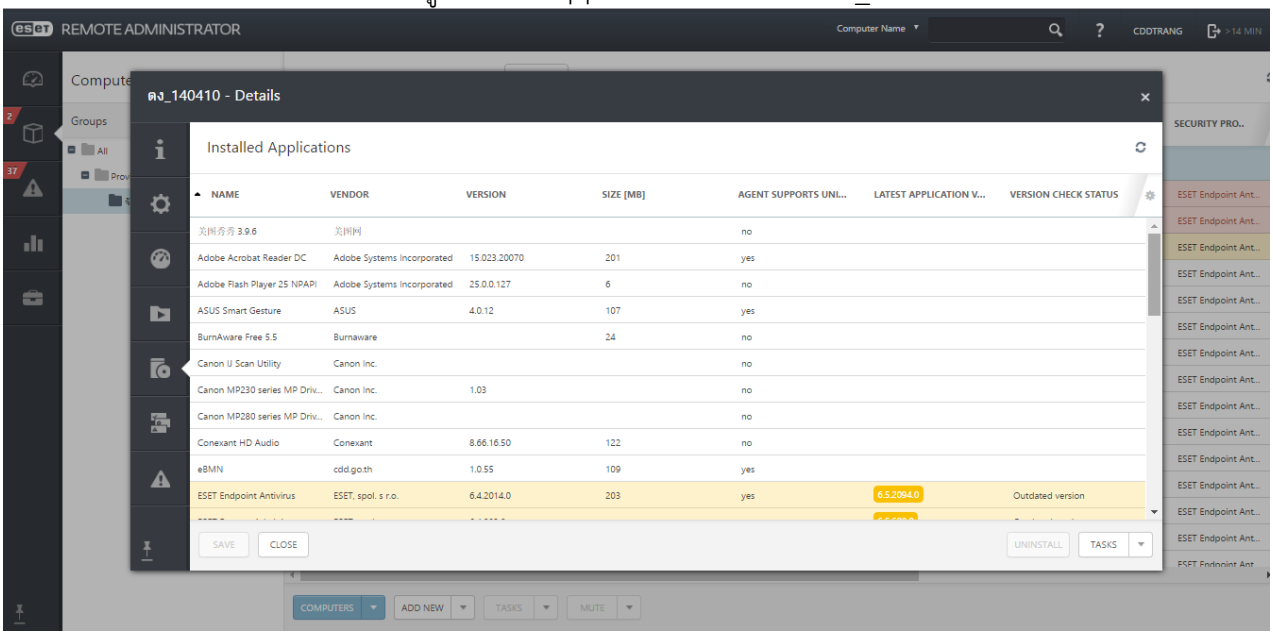


แสดงรายละเอียดข้อมูลเครื่องคอมพิวเตอร์ที่มารายงานตัวในระบบ Web Console ข้อมูลที่ปรากฏจะแสดงตามหัวข้อที่เลือก ซึ่งสามารถคลิกดูรายละเอียดแต่ละหัวข้อได้ ดังนี้

- Basic - ใช้ตรวจสอบข้อมูลเครื่องคอมพิวเตอร์, IP Address, Computer Name, OS Name, Work Group
- Configuration - ใช้ตรวจการตั้งค่า configuration ที่ใช้กับเครื่องคอมพิวเตอร์
- Sysinspector - ใช้ในการวิเคราะห์หาความผิดปกติของเครื่องในกรณีเกิดปัญหาต่างๆ
- Task Executions - ใช้ในการตรวจสอบข้อมูล task การทำงานที่เคยสั่งกับเครื่องคอมพิวเตอร์นั้น ๆ
- Install Applications - ใช้ตรวจสอบและถอนการติดตั้ง Applications ที่ติดตั้งในเครื่อง
- Alert - แจ้งเตือนเกี่ยวกับปัญหาต่างๆ ของโปรแกรม
- Threats And Quarantine - ใช้ตรวจสอบข้อมูลไวรัสที่เคยตรวจพบบนเครื่องคอมพิเตอร์



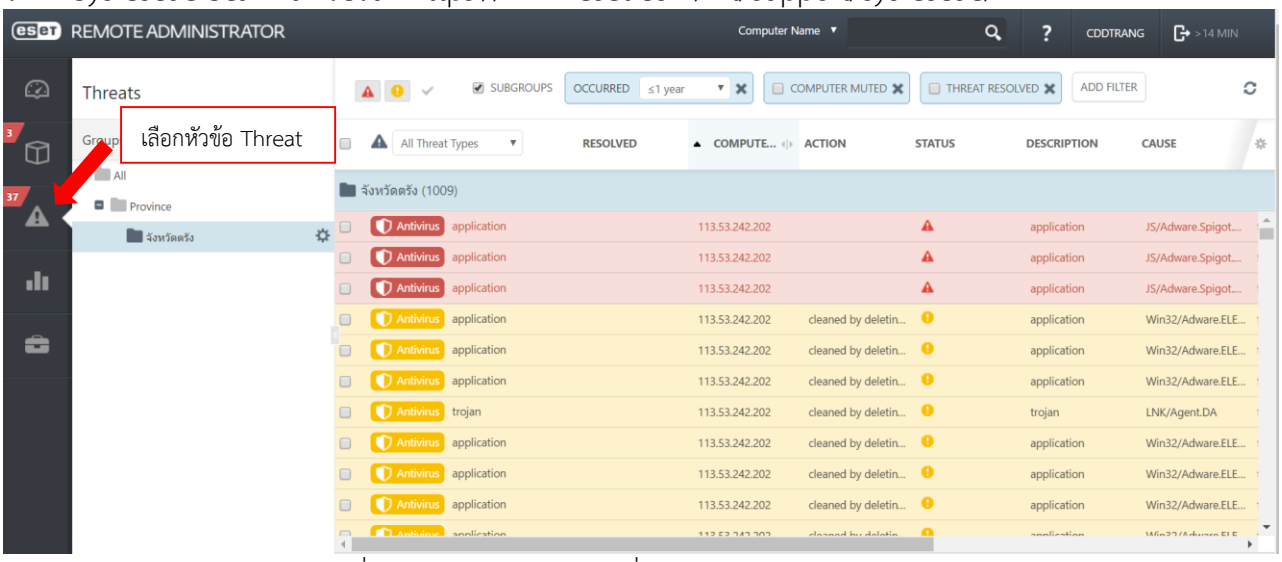
ตัวอย่างแสดงรายละเอียดข้อมูล Install Applications ชื่อเครื่อง ตง_140410



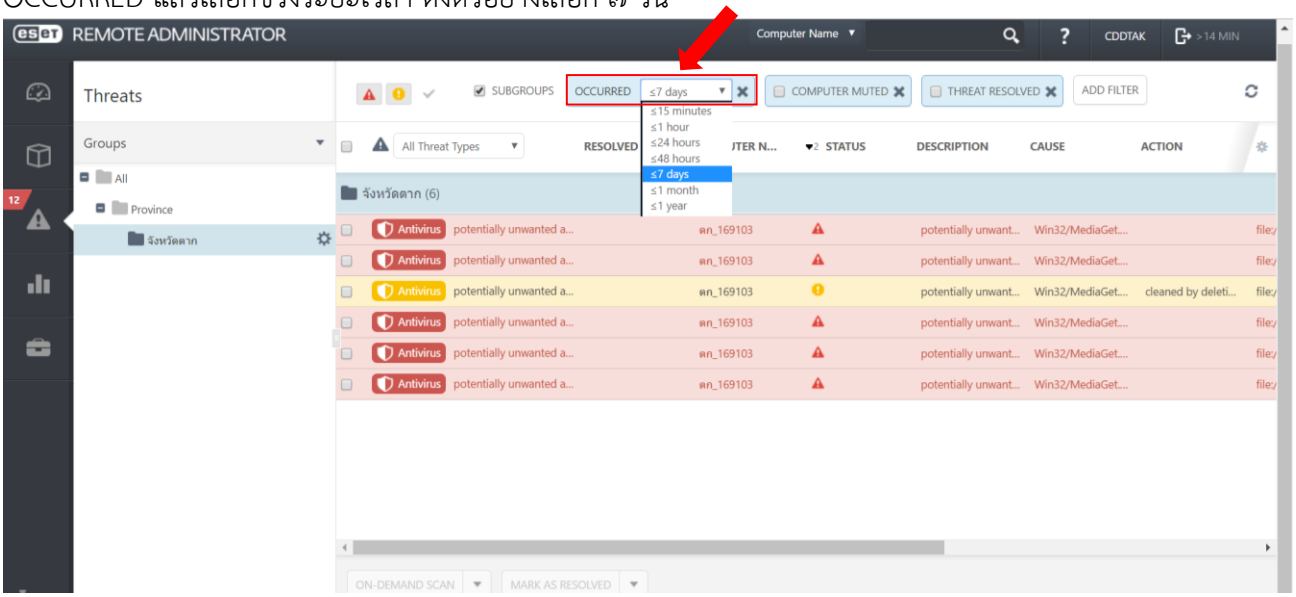
๙. เมนู Threats ใช้สำหรับตรวจสอบไวรัสที่พบทั้งหมดบนเครื่องคอมพิวเตอร์ในแต่ละ Group และระบุได้ว่าสามารถจัดการได้หรือไม่โดยดูจาก Action และสามารถระบุช่วงเวลาที่ต้องการดู Threats Log ได้ ถ้าสถานะเครื่องสีเหลือง คือ โปรแกรมสามารถ clean, delete หรือ quarantine ได้ปกติ แต่ถ้าสถานะเครื่องสีแดง คือ โปรแกรมไม่สามารถ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



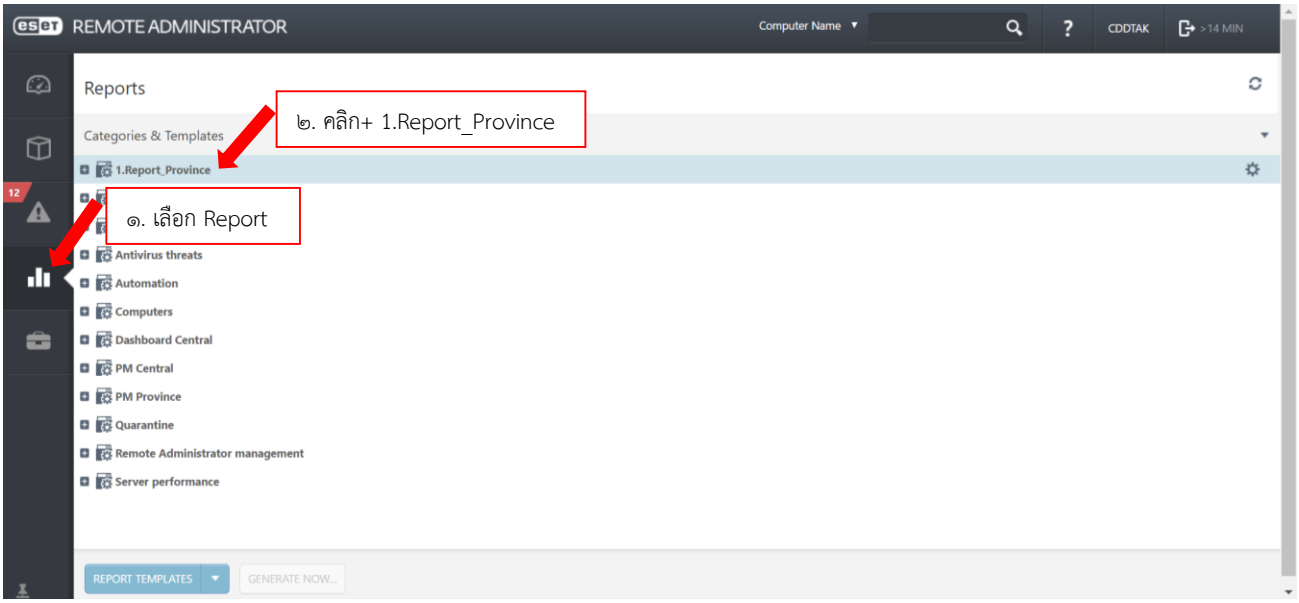
๑๐. การเลือกช่วงเวลาที่จะตรวจสอบไวรัสบนเครื่องคอมพิวเตอร์ในแต่ละ Group สามารถคลิกเลือกหัวข้อ OCCURRED แล้วเลือกช่วงระยะเวลา ดังตัวอย่างเลือก ๗ วัน



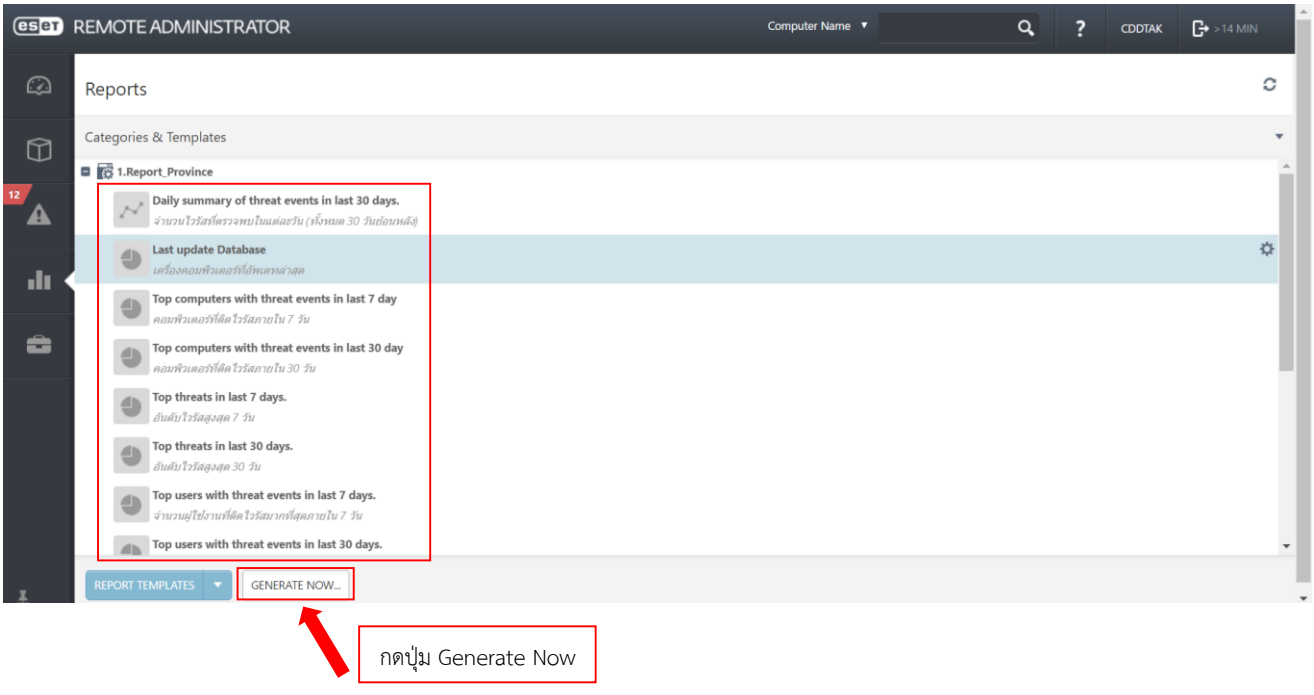
* ข้อมูลที่แสดงผลการตรวจพบไวรัสบนเมนู Threat จะแสดงชื่อเครื่องคอมพิวเตอร์,ประเภทไวรัส,สถานะการกำจัด ซึ่งสถานะสีแดงคือไม่สามารถลบไฟล์ที่ติดไวรัสได้เพราะ Process อาจจะมีการใช้งานอยู่และสถานะสีเหลืองคือสามารถคลีนไวรัสได้

** ข้อมูลจะมีอายุการจัดเก็บบนระบบ ๖ เดือน หลังจากนั้นจะมีการถูกลบอัตโนมัติ โดยผู้ดูแลระบบส่วนกลาง

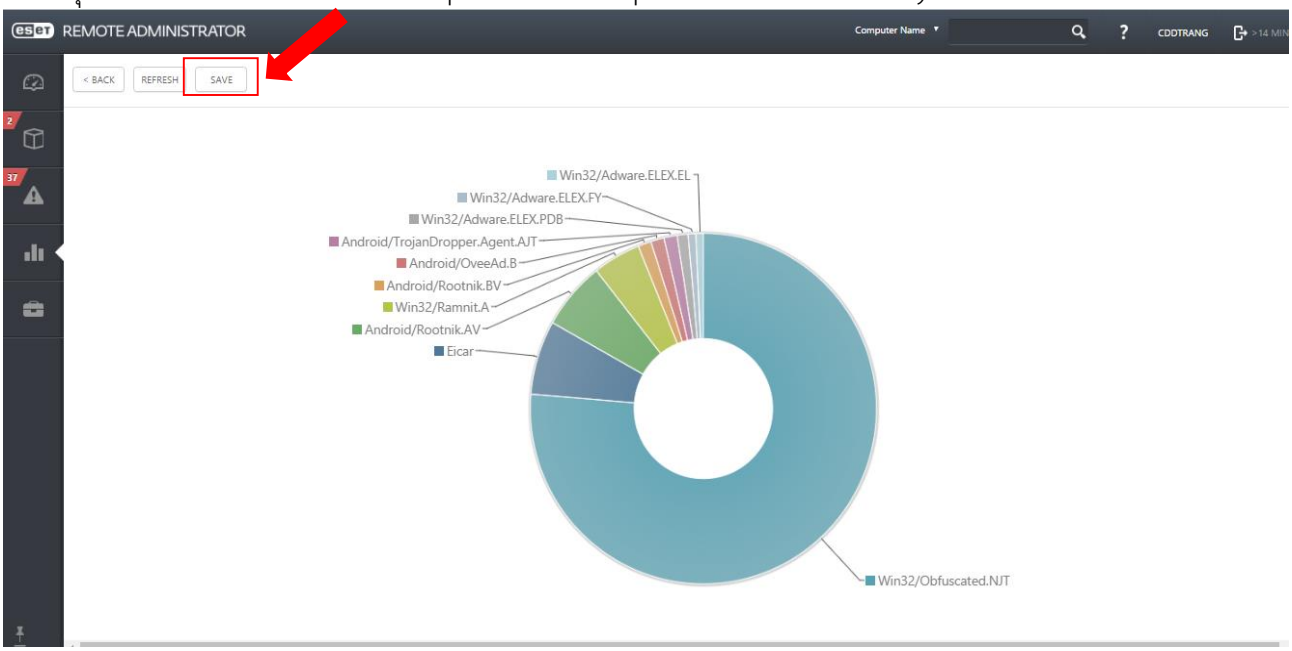
๑๑. เมนู Report ใช้สำหรับแสดงรายงานเกี่ยวกับการโจมตีของไวรัสที่โจมตีเครื่องคอมพิวเตอร์ในระบบ Web Console ให้เลือกหัวข้อ Report คลิกเครื่องหมาย + ข้างหน้า 1.Report_Province ดังภาพ



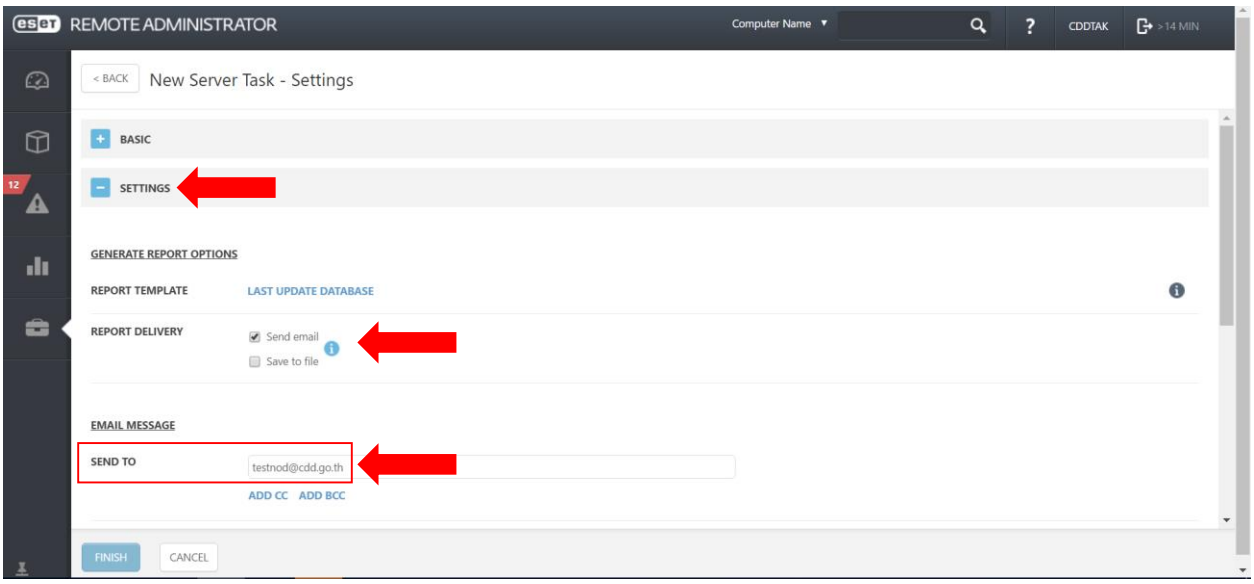
๑๑.๑ จะแสดงรายละเอียด Report ของแต่ละหัวข้อ โดยการเลือกหัวข้อ Report ที่ต้องการแสดง จากนั้นกดปุ่ม Generate Now (ตรวจสอบการโจมตีของไวรัสคอมพิวเตอร์และรายงานผลตามหัวข้อที่เลือก)



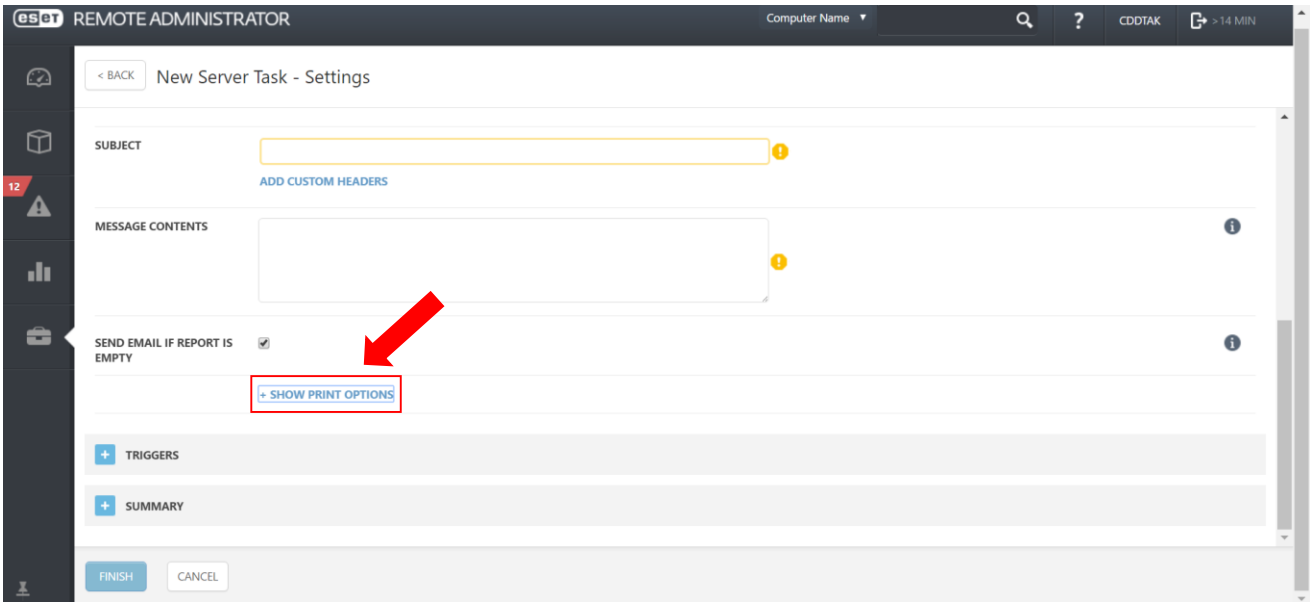
๑๑.๒ แสดง Report หลังจากทำการ Generate report เรียบร้อยจะได้ Report ตามภาพ จากนั้นให้กดปุ่ม save ดังภาพเป็นการแสดง Report หัวข้อ “Top threats in last 30 days”



๑๑.๓ เมื่อกดปุ่ม save เรียบร้อยแล้ว ให้เลือกรับ Report ผ่าน E-mail โดยเลือกที่ Send email และกรอก e-mail ผู้รับตามภาพ



๑๑.๔ หลังจากใส่ E-mail เรียบร้อยแล้ว สามารถเลือกได้ว่าจะรับรายงานเป็นไฟล์รูปแบบไหน โดยคลิกที่ +SHOW PRINT OPTIONS



๑๑.๕ สามารถจะเลือกแสดงรายงานเป็นไฟล์ได้ ๓ รูปแบบคือ PDF, PS, CSV ตามภาพ หลังจากนั้นกดปุ่ม Finish เพื่อทำการส่ง Report ไปยัง E-mail ของผู้รับ