ฝ่ายโครงสร้างพื้นฐานและระบบเครือข่าย

รายงานการใช้งานระบบเครือข่ายคอมพิวเตอร์ ประจำเดือน พฤศจิกายน 67

- ระบบเครือข่ายคอมพิวเตอร์
- ระบบ Internet Data Center
- ระบบโทรคมนาคม

รายงานจำนวนผู้ใช้งานผ่านระบบเครือข่าย (LAN)
(ไม่รวมห้องปฏิบัติการคอมฯ)

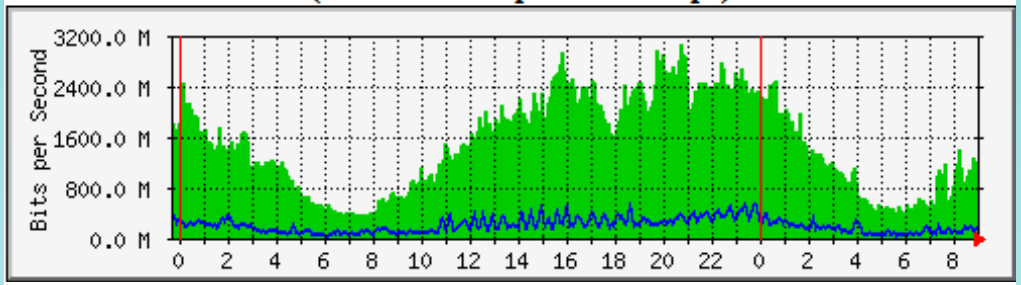
วิธีการ	จำนวน
วิธีการแบบ ISE (802.1x)	116 คน

ที่มา (ise) https://203.158.4.207

รายงานการใช้งานระบบเครือข่าย

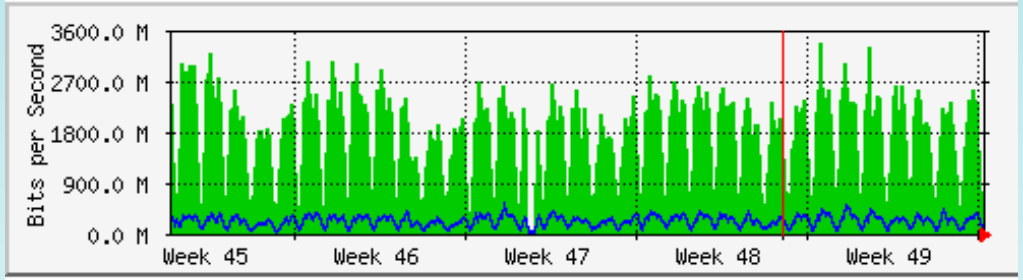
Internet Gateway Traffic

Link to True Internet (Domestic 6Gbps/Inter 3Gbps)



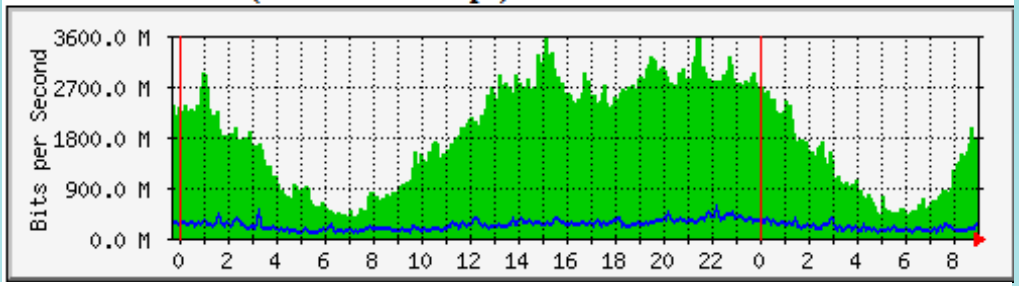
	Max	Average	Current
In	3049.0 Mb/s (30.5%)	1461.9 Mb/s (14.6%)	1075.2 Mb/s (10.8%)
Out	531.2 Mb/s (5.3%)	185.9 Mb/s (1.9%)	152.9 Mb/s (1.5%)

`Monthly' Graph (2 Hour Average)



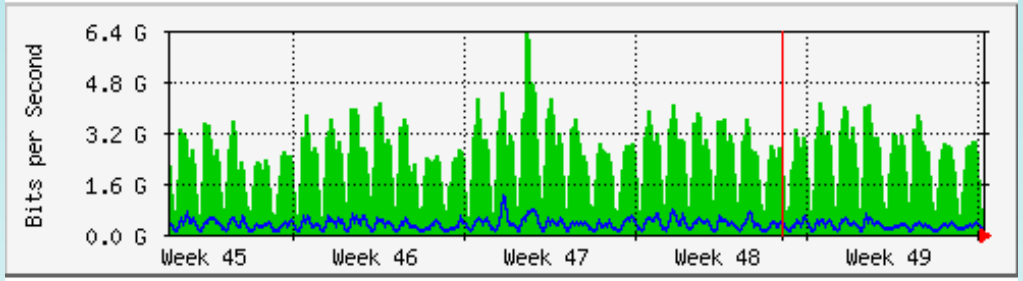
	Max	Average	Current
In	3367.6 Mb/s (33.7%)	1688.2 Mb/s (16.9%)	476.6 Mb/s (4.8%)
Out	504.2 Mb/s (5.0%)	205.3 Mb/s (2.1%)	67.6 Mb/s (0.7%)

Link to UNINET (Domestic 10Gbps)



	Max	Average	Current
In	3581.1 Mb/s (35.8%)	1784.2 Mb/s (17.8%)	1713.6 Mb/s (17.1%)
Out	540.2 Mb/s (5.4%)	215.9 Mb/s (2.2%)	182.3 Mb/s (1.8%)

`Monthly' Graph (2 Hour Average)

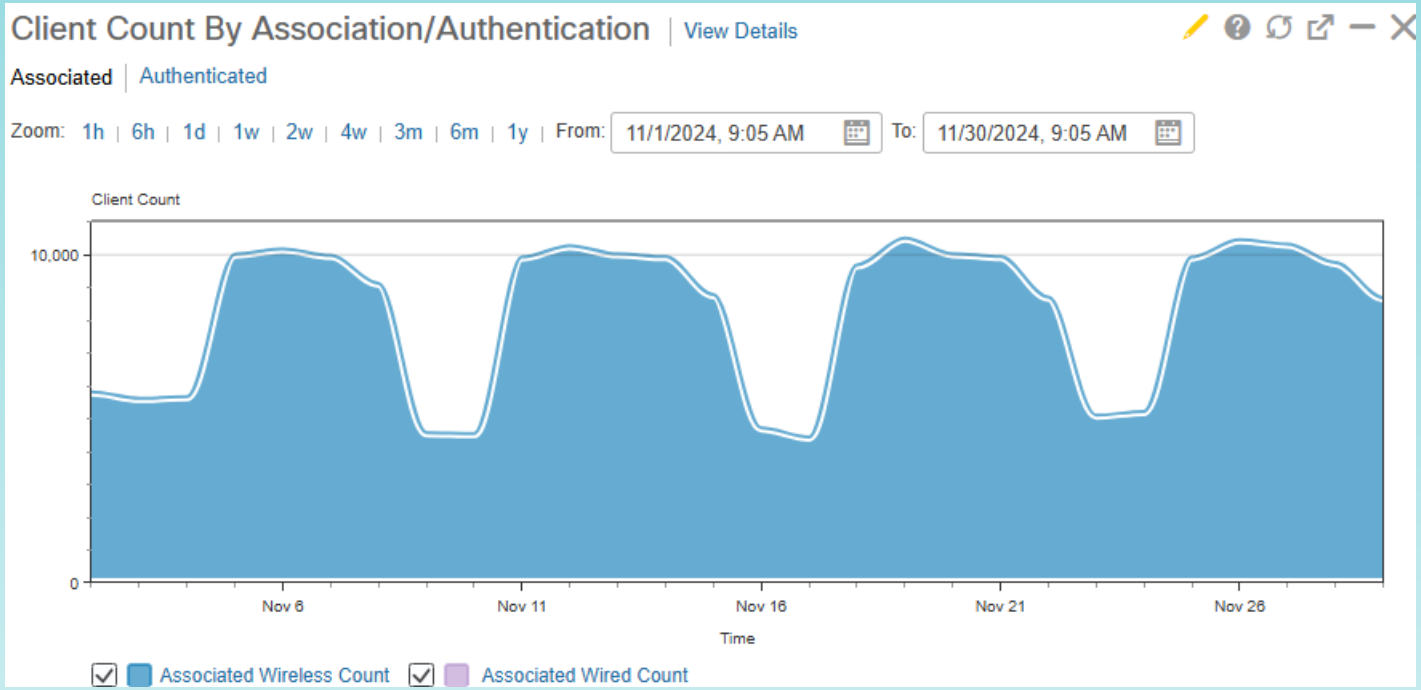


	Max	Average	Current
In	6312.3 Mb/s (63.1%)	2312.8 Mb/s (23.1%)	506.9 Mb/s (5.1%)
Out	1207.2 Mb/s (12.1%)	286.9 Mb/s (2.9%)	134.2 Mb/s (1.3%)

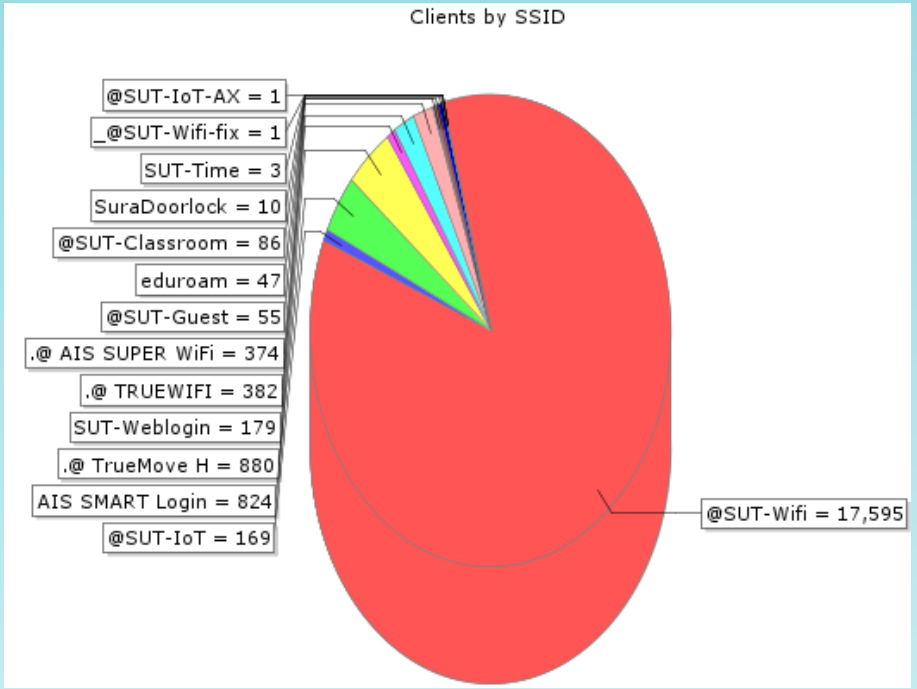
รายงานจำนวนผู้ใช้งานผ่านระบบเครือข่ายไร้สาย

สรุปสถิติจำนวนผู้ใช้งานผ่านระบบ wireless ทั้งหมด

สรุปปริมาณผู้ใช้งานต่อวัน



แบ่งตาม SSID สถิติย้อนหลัง 1 เดือน



- ผู้ใช้งานผ่านระบบ wireless สูงสุด 10,509 คน/วัน
- ผู้ใช้งานผ่านระบบ wireless, ต่ำสุด 4,446 คน/วัน
- ผู้ใช้งานผ่านระบบ wireless เฉลี่ย 8,291 คน/วัน

สรุปการดำเนินการบนระบบเครือข่ายคอมพิวเตอร์

01/11/2024	ตรวจสอบเครื่อง router ปล่อยสัญญาณ wifi ใช้งานไม่ได้ สถานที่ : ในและหน้าอาคารผีเสื้อ อาคาร : อาคารสุรพัฒน์ 6 ชั้น : 1 พบว่าอุปกรณ์ Adapter ชำรุด จึงได้ประสานงานแจ้งให้ทราบเป็นที่เรียบร้อย
04/11/2024	อาคารสุรพัฒน์ 5 เข้าตรวจสอบ พบสาย lan มีปัญหา ดำเนินการแก้ไข และ เปลี่ยนหัวท้าย ใหม่ พร้อม port ใหม่ ไม่สามารถใช้งานได้ แก้ไขเบื้องต้นให้ใช้ ap เสียบกับอุปกรณ์ภายในห้อง office สามารถใช้งานได้ปกติ
04/11/2024	internet โรงกัญชา ใช้งานไม่ได้ เข้าไปตรวจสอบ พบ fiber โดนหนูกัดสายขาด ดำเนินการเปลี่ยนสาย fiber ใช้งานได้ปกติ
04/11/2024	Set config switch D1-FL1-MainRoom1 เนื่องจากมีผู้ใช้งานระบบเครือข่าย LAN ไม่ได้ เพราะมีการต่อ hub และ loop ภายใน hub ทำให้ switch disable port จึงไม่สามารถใช้ LAN ได้ หลังตรวจเช็ค loop แล้วจึงได่แก้ไข config switch ใหม่
04/11/2024	ได้รับแจ้ง บริเวณโรงนม ไม่มีสัญญาณ internet เข้าไปตรวจสอบ พบสาย lan และ ap ไม่สามารถใช้งานได้ เข้าไปตรวจสอบ ดำเนินการทำความสะอาด หนีบหัว rj45 ใหม่ สามารถใช้งานได้เรียบร้อยแล้ว

สรุปการดำเนินการบนระบบเครือข่ายคอมพิวเตอร์

05/11/2024	Set config switch C1-FL2-Food-1 [172.16.1.51] set config disable dot1x (not save)
05/11/2024	ดำเนินการตรวจสอบอุปกรณ์ Ap ณ.ลานหมอลำ / ภายในอาคารสุรพัฒน์ 2
06/11/2024	สืบเนื่องระบบ authen ยืนยันตัวตน เกิดปัญหา ไม่สามารถใช้งานทั้งหมดภายใน มหาวิทยาลัย ได้ทำการประสาน ตรวจสอบ และแก้ไข port sw อาคารที่ได้รับผลกระทบ เพื่อให้กลับมาใช้งานเป็นการชั่วคราว ในระหว่างตรวจซ่อม ระบบ authen ซึ่งไม่สามารถ boot และทำงานได้ตามปกติ
06/11/2024	บริษัท เรื่องการเข้า MA datacenter UPS water leak pdu sofeware manage
06/11/2024	อาคารเครื่องมือ F11 ไม่สามารถใช้งาน ระบบ เครือข่ายได้ และไม่สามารถดูกล้อง cctv เข้าไปตรวจสอบพบมีการ ติดตั้ง ย้าย อุปกรณ์กล้อง และ ระบบคอมพิวเตอร์ใหม่ จึงแก้ไข เนื่องจาก ไม่ได้รับแจ้งก่อนหน้าว่าจะมีการ ย้าย หรือ ปรับเปลี่ยน ติดตั้งอุปกรณ์กล้อง พร้อมทั้งระบบ lan เพื่อใช้งานกล้องวงจรปิด
06/11/2024	ตรวจสอบอุปกรณ์ AP โซนหอพักนักศึกษา (หอพักสุรนิเวศ 18) ให้สัญญาณ Internet กลับมาใช้งานได้ปกติ
06/11/2024	ดำเนินการติดตั้งอุปกรณ์ AP เพิ่มเติม 1 จุด อาคารสุรพัฒน์ 2 ชั้น 1

สรุปการดำเนินการบนระบบเครือข่ายคอมพิวเตอร์

06/11/2024	ดำเนินการติดตั้งอุปกรณ์ AP เพิ่มเติม จำนวน 1 จุด อาคารสุรพัฒน์ 2 ชั้น 2
06/11/2024	ดำเนินการติดตั้ง AP จำนวน 2 จุดที่ประจำห้องเรียน ฟาร์มมหาวิทยาลัย หน่วยงานเครื่องจักรกล
06/11/2024	ตรวจสอบอุปกรณ์ AP โซนหอพักนักศึกษา (หอพักสุรนิเวศ 18) ให้สัญญาณ Internet กลับมาใช้งานได้ปกติ
07/11/2024	ระบบ .dot1x ไม่สามารถใช้งานได้ จึงจำเป็นต้องปลด config port switch ตามกลุ่มอาคารที่ใช้งาน เพื่อให้การใช้งานเป็นการชั่วคราว
08/11/2024	ตรวจสอบสาย fiber optic อาคารเพราะฟัก (งานประมง) พบว่าสายFIBER Optic ขาดที่ระยะ 215เมตร จากอาคารเพราะฟัก (งานประมง)
11/11/2024	ตรวจสอบอุปกรณ์ AP ภายในสำนักงานสวนพฤษศาสตร์ และได้ดำเนินการแก้ไขให้กับมาใช้งานได้ตามปกติเป็นที่เรียบร้อย
11/11/2024	ตรวจสอบอุปกรณ์ AP และสายสัญญาณ Fiber Optic ภายในสำนักงานโรงกัญชา และได้ดำเนินการแก้ไขให้กับมาใช้งานได้ตามปกติเป็นที่เรียบร้อย

สรุปการดำเนินการบนระบบเครือข่ายคอมพิวเตอร์

13/11/2024	user zone F9 ชั้น 4 ไม่สามารถใช้งานได้ และประสาน พูดคุยผ่าน line และโทรศัพท์ พบ user พบการตั้งค่า .dot1x ผิด และแนะนำ สามารถใช้งานได้ปกติ
12/11/2024	ตรวจสอบสาย fiber optic อาคารเกษตรภิวัฒน์ สนง ฟาร์ม สาย OFC ขาด ส่งผลกระทบ พืชทดลอง โรงไฟฟ้าย่อย 1 (สายไฟเบอร์ตก มาจากการเปลี่ยนเสาไฟฟ้านานแล้ว)
13/11/2024	องไฟฟ้า ชั้น 1 อาคารบรรณสาร 2 เพื่อติดตั้ง UPS แทนเครื่องเดิม (UPS ของศูนย์บรรณสาร) ใช้ต่อเข้าใช้งานที่ RACK Switch ชั้น 1, 2 และ 3 (แทนเครื่องเดิมที่ไม่ boot system เมื่อแบตเตอรี่หมด)
14/11/2024	ดำเนินการตรวจสอบอุปกรณ์ AP ประจำส่วนกิจการนักศึกษา
18/11/2024	เชื่อมต่อ Fiber Patch Cord จำนวน 6 ช่อง สัญญาณขนาด 12 Core ที่ห้องเซิร์ฟเวอร์เครือข่ายกับอุปกรณ์ Core Switch และขอเปิดใช้ช่องสัญญาณ SEP Module
18/11/2024	เชื่อมต่v CCTV เข้ากับ SUTnet ติตตั้งกล้องวงจรปิดจุดจำหน่ายสินค้าฟาร์มมาร์ทและคลังสินค้า ซึ่งทั้ง 2 จุดตั้งอยู่ ณ ฟาร์มมหาวิทยาลัย เพื่อให้สามารถดูกล้องวงรจรปิดให้ตลอดเวลา โดยผ่าน Open VPN

สรุปการดำเนินการบนระบบเครือข่ายคอมพิวเตอร์

18/11/2024	ตรวจสอบอุปกรณ์ UPS ไม่ทำงาน บริเวณ หอพักสุรนิเวศ 12, 13
19/11/2024	ระบบ monitor ตรวจพบ ไม่สามารถ monitor switch ที่โรงเรียนสุรวิวัฒน์ จำนวน 1 ตัว ได้ทำการแก้ไข หรือทดสอบผ่าน shell& อื่นๆ ไม่สามารถแก้ไขได้ จึงเข้าไปตรวจสอบ console และ ตรวจพบว่า มีอุปกรณ์ switch ของหน่วยงาน รปภ. เชื่อมต่อ และ อุปกรณ์ดังกล่าวมี uplink เป็น fiber อุปกรณ์ดังกล่าว ส่งผลให้ switch ทีต่อพ่วงกับอุปกรณ์ไม่สามารถทำงานได้ จึงดำเนินการปลด link จากหน่วยงาน รปภ. ออก จึงทำให้ระบบกลับมาทำงานปกติ สาเหตุ เกิดจาก loop อุปกรณ์ดังกล่าวมี uplink fiber และ lan ที่ต่อพ่วงกับ switch cisco ส่งผลให้อุปกรณ์ switch cisco ของโรงเรียนไมสามารถทำงานได้ ได้แก้ไข เรียบร้อยแล้ว
19/11/2024	ตรวจสอบอุปกรณ์ AP หอพักนักศึกษา สุรนิเวศ 11 และได้แก้ไขอุปกรณ์ AP ให้กลับมาใช้งานได้ ปกติ เป็นที่เรียบร้อย
21/11/2024	ตรวจสอบอุปกรณ์ AP หอพักนักศึกษา หอพักสุรนิเวศ 5, 6
26/11/2024	ตรวจสอบระบบสัญญาณ Internet และอุปกรณ์ AP ห้องคณบดี สำนักพยาบาล
27/11/2024	Set config rounter 4G WIFI-LAN เพื่อนำไปใช้งานที่ อพ.สธ คลองไผ่

สรุปการดำเนินการบนระบบเครือข่ายคอมพิวเตอร์

29/11/2024	ติดตั้ง AP เพิ่ม จำนวน 1 เครื่อง ที่สำนักงาน S9-10 ชั้น 1 เป็นการชั่วตราว โดย ต่อสายจาก outlet ชั้น 2 ลงมาห้องอ่านหนังสือ ชั้น 1 เจาะยึดเพลทในห้องฯ เพื่อติดตั้ง AP จำนวน 1 จุด ติดตั้ง AP พร้อมเช็คการทำงานว่า AP ทำงานแล้ว
29/11/2024	ระบบเครือข่าย อาคารเครื่องมือ 7 และห้องปฏิบัติการ remote sensing ไม่สามารถใช้งานได้ เข้าไปตรจสอบพบอุปกรณ์ ups ไม่ทำงาน และปัญหาแบตเตอรี่เสื่อมสภาพ ดำเนินการแก้ไข ต่อตรงเข้ากับไฟฟ้าหลักของอาคาร เพื่อให้สามารถใช้งานได้

สรุปการดำเนินการบนระบบ Internet Data Center

01/11/2024	แก้ไขปัญหา Email Account (SUTMail) อาจารย์แจ้งว่าไม่สามารถส่งไฟล์จาก Line เข้าเมลได้
05/11/2024	รายงานผลการตรวจสอบและแก้ไขภัยคุกคาม แก่ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ศปช.) สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
06/11/2024	สร้างบัญชีผู้ใช้งานระบบ SUT VPN (OpenVPN) สำหรับโรงพยาบาลศูนย์แพทย์ฯ และโรงพยาบาลแหล่งฝึก
06/11/2024	ตรวจสอบ Email พนักงานไม่ได้รับเมล PR ทำการตรวจสอบ Department ของพนักงาน และแก้ไข Department
06/11/2024	จัดทำรายงานภัยคุกคามระบบเครือข่าย ประจำปีงบประมาณ 2567
08/11/2024	จัดทำข้อมูลเพื่อประชาสัมพันธ์แจ้งเตือนภัยคุกคามทางไซเบอร์ ประเภทการหลอกลวงเพื่อขโมยข้อมูล (Data Theft) และการแพร่ระบาดของอีเมลหลอกลวง (Phishing Mail)
08/11/2024	จัดสรรทรัพยากร Virtual Server ให้กับหน่วยตรวจสอบภายใน สำหรับ ติดตั้งโปรแกรม DSPACE

สรุปการดำเนินการบนระบบ Internet Data Center

11/11/2024	สร้าง Email Account (SUT G.dot) สำหรับโรงเรียนสุรวิวัฒน์
12/11/2024	จัดสรรพื้นที่เว็บไซต์ http://personal.sut.ac.th/vijittra
12/11/2024	เปิดสิทธิ์การใช้งาน SMTP Service Mail ของสถาบันวิจัย
12/11/2024	Upgrade RAM บน Virtual Server ศูนย์บริการการศึกษา (cesdata01)
12/11/2024	ประชุมคณะกรรมการดำเนินงานเกี่ยวกับการคุ้มครองส่วนบุคคลของมหาวิทยาลัยเทคโนโลยีสุรนารี ครั้งที่ 4/2567
14/11/2024	จัดสรร virtual server สำหรับรองรับระบบสารสนเทศ (contactdir.sut.ac.th)
14/11/2024	จัดส่ง Certificate SSL สำหรับ Web Server ให้กับผู้ดูแล Web server : iaudsp

สรุปการดำเนินการบนระบบ Internet Data Center

18/11/2024	จัดสรรพื้นที่เว็บไซต์ https://scischolarship.sut.ac.th
18/11/2024	เชื่อมต่อ Fiber Patch Cord จำนวน 6 ช่อง สัญญาณขนาด 12 Core ที่ห้องเซิร์ฟเวอร์เครือข่ายกับอุปกรณ์ Core Switch และขอเปิดใช้ช่องสัญญาณ SEP Module
18/11/2024	เชื่อมต่อ CCTV เข้ากับ SUTnet ติดตั้งกล้องวงจรปิดจุดจำหน่ายสินค้าฟาร์มมาร์ทและคลังสินค้า ซึ่งทั้ง 2 จุดตั้งอยู่ ณ ฟาร์มมหาวิทยาลัย เพื่อให้สามารถดูกล้องวงรจรปิดให้ตลอดเวลา โดยผ่าน Open VPN
19/11/2024	จัดทำข้อมูลส่งให้สำนักวิศวกรรมศาสตร์ เกี่ยวกับระบบ Internet Data Center มทส. เนื่องจากสำนักฯทำ EdPEx300
20/11/2024	สรุปการทดสอบ Phishing Email ส่งให้สำนักวิศวะทราบถึงความคืบหน้าในการดำเนินการ
27/11/2024	ให้ข้อมูลเพิ่มเติมในการจักทำ EdPex สำนักวิศวกรรมศาสตร์ เกี่ยวกับจำนวนชั่วโมงในการกู้คืนเกินเป้าหมายที่ตั้งไว้ (3 ชม.), การ downtime ของระบบเครือข่าย, การยับยั้งการโจมตีระบบเครือข่าย
28/11/2024	จัดสรรพื้นที่เว็บไซต์ https://dfct2025.sut.ac.th

สรุปการดำเนินการบนระบบโทรคมนาคม

04/11/2024	แก้ไขโทรศัพท์ หมายเลข 5185 ของ สำนักงาน หอพักโรงเรียนสุรวิวัฒน์ สาเหตุจากสายมีความชื้น แก้ไขโดย เปลี่ยนสายเข้าหัวเครื่องเส้นใหม่ สามารถใช้งานได้เป็นปกติไม่มีสัญญาณแทรกซ้อน
04/11/2024	แก้ไขหมายเลขของห้องปฏิบัติการ f 6127 อาการไม่มีสัญญาณตรวจสอบสายขาดระยะ 85 เมตรสาเหตุจากเกิดออกไซด์ทำให้สายสัญญาณขาด ใช้งานได้แก้ไขโดยการตัดต่อสายใหม่ใช้งานได้เป็นปกติ
04/11/2024	ติดตั้งโทรศัพท์ตั้งโต๊ะพร้อมและเบอร์ภายในแก่พนักงานใหมา นายสัมฤทธิ์ ลิ้มเจริญ ส่วนงานบริหารสินทรัพย์
04/11/2024	ติดตั้งเครื่องโทรศัพท์และหมายเลขโทรศัพท์ภายในให้กับพนักงานใหม่ นางสาว สุดารัตน์ รุ่งเรือง หน่วยตรวจสอบภายใน
04/11/2024	การเชื่อมต่อวงจรสัญญาณ E1 ปกติ ใช้งานได้
05/11/2024	ซ่อมหมายเลข 3429 อาการไม่มีสัญญาณตรวจสอบแล้วเนื่องจากหนูกัดสายขาดทำการต่อ connector ใหม่ ใช้งานได้ปกติ
12/11/2024	ย้ายสายสัญญาณโทรศัพท์ อาคารเครื่องมือ 12 จากห้องสำนักงานไปยังห้องปรับปรุงชั่วคราว แต่ไม่สามารถดำเนินการได้เนื่องจากไม่มี Outlet ที่จะปล่อยหมายเลขได้จึงเสนอให้ใช้ระบบยูนิแทคแทนซึ่งพูดใช้จะทำการ บันทึกของ อีกครั้งหนึ่ง

สรุปการดำเนินการบนระบบโทรคมนาคม

19/11/2024	ย้ายหมายเลขโทรศัพท์ภายใน สำนักวิชาวิศวกรรมศาสตร์ อาคารวิชาการ1ชั้น1
19/11/2024	เปลี่ยนคู่สายภายเบอร์4392 สาขาวิชาวิศวกรรมโทรคมนาคมอาคารวิชาการ1ชั้น2
21/11/2024	โทรศัพท์มีเสียงแทรก รบกวนขณะคุยสาย 5805-001-01/53/101-3040000 ถอดทำความสะอาดเครื่องเปลี่ยนหัว RJ11 ใช้งานได้ปกติ
26/11/2024	ย้ายเบอร์โทรศัพท์ 3805 สำนักวิชาสาธารณสุขศาสตร์อาคารเฉลิมพระเกียรติ

สรุปการดำเนินการบนระบบโทรคมนาคม

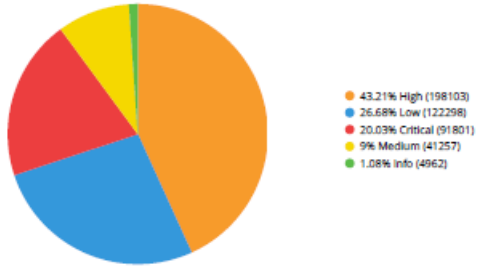
25/10/2024	ตรวจสอบอุปกรณ์ยืม-คืนวิทยุสื่อสาร จำนวน 10 เครื่อง ของค่ายวิชาทหาร ตรวจสอบตัวเครื่องหลังจากการใช้งานแล้ว และชาร์จแบต และเก็บเพื่อเตรียมพร้อมใช้งานต่อไป
25/10/2024	เช็ครายชื่อผู้ขอยืมเครื่องโทรศัพท์ อ.นพ.ธีรทัศน์ ชมบัณฑิตย์ สำนักวิชาแพทยศาสตร์ ลาออกวันที่1 พฤศจิกายน 2567
25/10/2024	1.ประชุมสำรวจพื้นที่เตรียมความพร้อม งานประชุมวิชาการ อพสธ คลองไผ่ สีคิ้ว 2.ตรวจสอบพื้นที่เตรียมรับเสด็จ อพสธ คลองไผ่ 3. จัดเตรียมวางแผนงานระบบสื่อสาร
28/10/2024	ทดสอบโทรเข้าเบอร์ 044223000 ติดระบบตอบรับอัตโนมัติ กดเบอร์ต่อเลขหมายภายในได้ สัญญาณและระบบการทำงานปกติ
28/10/2024	ทดสอบกด 8 โทรออก ได้ปกติ สัญญาณและระบบเชื่อมต่อใช้งานได้ปกติ
29/10/2024	ได้ทำการตรวจเช็คพบว่าตัวเครื่องมีปัญหา และเนื่องจากไม่ม่เครื่องเปลี่ยนผู้แจ้งซ่อมยินดีรอเครื่องจัดสรรใหม่

ภัยคุกคามระบบเครือข่าย

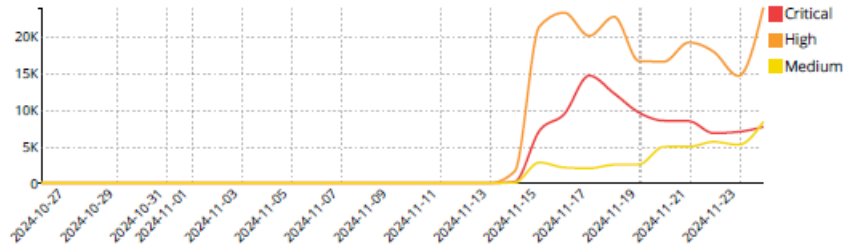
การยับยั้งการโจมตีบนระบบเครือข่าย โดย อุปกรณ์ Next Gen Firewall : Fortinet
(ข้อมูล 1 เดือนย้อนหลัง)

Summary

Intrusions By Severity



Critical High and Medium Intrusions Timeline



Intrusions By Types

#	Intrusion Type	Counts
1	Path Traversal	85,451
2	Malware	80,163
3	Anomaly	72,309
4	OS Command Injection	60,193
5	Code Injection	46,250
6	SQL Injection	27,082
7	Other	20,408
8	Permission/Privilege/Access Control	9,085
9	Buffer Errors	5,074
10	XSS	4,756
11	DoS	1,601
12	Information Disclosure	1,447
13	Improper Authentication	674
14	CSRF	2
15	Resource Management Errors	1

Intrusions Detected

Critical Severity Intrusions

#	Attack Name	CVE-ID	Intrusion Type	Counts
1	Hikvision.Products.SDK.Web Language.Tag.Command.Injection	CVE-2021-36260	OS Command Injection	34,963
2	PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	CVE-2017-9841	Code Injection	24,171
3	Andromeda.Botnet			5,194
4	Apache.Struts.2.DefaultActionMapper.Remote.Command.Execution	CVE-2013-2251	Other	3,515
5	NETGEAR.DGN1000.CGI.Unauthenticated.Remote.Code.Execution		Code Injection	2,104
6	DZS.GPON.Remote.Code.Execution	CVE-2018-10561,CVE-2018-10562	OS Command Injection	2,064
7	D-Link.Devices.HNAP.SOAPAction-Header.Command.Execution	CVE-2015-2051,CVE-2019-10891	OS Command Injection	1,978
8	Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution	CVE-2017-5638	Code Injection	1,824
9	Bladabindi.Botnet			1,423
10	TP-Link.Devices.userRpmNatDebugRpm.Authentication.Bypass		Permission/Privilege/Access Control	1,091
11	Apache.Log4j.Error.Log.Remote.Code.Execution	CVE-2021-4104,CVE-2021-44228,CVE-2021-45046	Permission/Privilege/Access Control	1,027
12	Gh0st.Rat.Botnet			926
13	OpenSSL.Heartbleed.Attack	CVE-2014-0160	Information Disclosure	891
14	Joomla!.Core.Session.Remote.Code.Execution	CVE-2015-8562	Code Injection	819
15	njRAT.Botnet			812
16	WIFICAM.P2P.GoAhead.Multiple.Remote.Code.Execution	CVE-2017-8221,CVE-2017-8223,CVE-2017-8225,CVE-2017-18377	Code Injection	798
17	Amadey.Botnet			690
18	WordPress.HTTP.Path.Traversal	CVE-2019-9618,CVE-2022-4101,CVE-2018-16283,CVE-2018-16299,CVE-2020-11738	Path Traversal	580
19	Telerik.Web.UI.RadAsyncUpload.Handling.Arbitrary.File.Upload	CVE-2017-11317,CVE-2017-11357,CVE-2019-18935	Improper Authentication	510
20	Remote.CMD.Shell		Malware	484

การยับยั้งการโจมตีบนระบบเครือข่าย โดย อุปกรณ์ Next Gen Firewall : Fortinet
(ข้อมูล 1 เดือนย้อนหลัง)

Intrusion Victims

#	Attack Victim	Counts	Critical	High	Medium	Percent of Total Attacks
1	192.168.31.131				35,179	30.12%
2	203.158.7.61				24,229	20.75%
3	202.28.42.71				8,969	7.68%
4	202.28.42.38				8,258	7.07%
5	202.28.42.25				7,384	6.32%
6	202.28.42.26				6,975	5.97%
7	10.1.63.32				5,177	4.43%
8	203.158.4.150				2,149	1.84%
9	18.208.156.248				1,771	1.52%
10	185.208.158.202				1,745	1.49%
11	185.237.207.107				1,736	1.49%
12	176.10.111.126				1,611	1.38%
13	194.62.105.143				1,607	1.38%
14	79.132.128.13				1,605	1.37%
15	203.158.7.95				1,515	1.30%
16	203.158.4.100				1,458	1.25%
17	173.234.13.50				1,439	1.23%
18	173.234.13.48				1,401	1.20%
19	203.158.6.44				1,342	1.15%
20	173.234.13.47				1,241	1.06%

Intrusion Sources

#	Attack Source	Counts	Critical	High	Medium	Percent of Total Attacks
1	92.255.57.58				45,874	29.05%
2	5.147.173.168				23,826	15.09%
3	149.50.96.45				14,343	9.08%
4	31.220.1.88				12,450	7.88%
5	194.50.16.198				10,061	6.37%
6	10.1.56.178				8,730	5.53%
7	95.214.52.254				7,786	4.93%
8	184.105.192.2				5,192	3.29%
9	192.168.127.161				3,835	2.43%
10	103.215.25.250				3,483	2.21%
11	45.202.35.17				3,413	2.16%
12	185.78.165.153				2,618	1.66%
13	194.87.216.228				2,413	1.53%
14	141.98.11.178				2,207	1.40%
15	179.43.191.98				2,025	1.28%
16	154.213.187.20				2,015	1.28%
17	95.214.55.43				1,941	1.23%
18	8.222.152.112				1,929	1.22%
19	46.19.138.234				1,892	1.20%
20	47.239.102.166				1,866	1.18%

การยับยั้งการโจมตีบนระบบเครือข่าย โดย อุปกรณ์ Next Gen Firewall : Fortinet
(ข้อมูล 1 เดือนย้อนหลัง)

Intrusions Blocked

#	Intrusion Name	Intrusion Type	Severity	Counts
1	Hikvision.Products.SDK.WebLanguage.Tag.Command.Injection	OS Command Injection	Critical	34,963
2	PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	Code Injection	Critical	24,171
3	Andromeda.Botnet		Critical	5,194
4	Apache.Struts.2.DefaultActionMapper.Remote.Command.Execution	Other	Critical	3,515
5	NETGEAR.DGN1000.CGI.Unauthenticated.Remote.Code.Execution	Code Injection	Critical	2,104
6	DZS.GPON.Remote.Code.Execution	OS Command Injection	Critical	2,064
7	D-Link.Devices.HNAP.SOAPAction-Header.Command.Execution	OS Command Injection	Critical	1,978
8	Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution	Code Injection	Critical	1,824
9	Bladabindi.Botnet		Critical	1,423
10	TP-Link.Devices.userRpmNatDebugRpm.Authentication.Bypass	Permission/Privilege/Access Control	Critical	1,091
11	Apache.Log4j.Error.Log.Remote.Code.Execution	Permission/Privilege/Access Control	Critical	1,027
12	Gh0st.Rat.Botnet		Critical	926
13	OpenSSL.Heartbleed.Attack	Information Disclosure	Critical	891
14	Joomla!.Core.Session.Remote.Code.Execution	Code Injection	Critical	819
15	njRAT.Botnet		Critical	812
16	WIFICAM.P2P.GoAhead.Multiple.Remote.Code.Execution	Code Injection	Critical	798
17	Amadey.Botnet		Critical	690
18	WordPress.HTTP.Path.Traversal	Path Traversal	Critical	580
19	Telerik.Web.UI.RadAsyncUpload.Handling.Arbitrary.File.Upload	Improper Authentication	Critical	510
20	Remote.CMD.Shell	Malware	Critical	484

การยับยั้งการโจมตีบนระบบเครือข่าย โดย อุปกรณ์ Next Gen Firewall : Fortinet
(ข้อมูล 1 เดือนย้อนหลัง)

Security and Threat Prevention

High Risk Applications

Risk	Application Name	Category	Technology	User	Bytes	Session
5	Cloudflare.1.1.1.1.VPN	Proxy	Client-Server	3	274.99 MB	299,630
5	Proxy.HTTP	Proxy	Network-Protocol	110	3.71 GB	198,701
5	Hola.Unblocker	Proxy	Client-Server	9	4.86 MB	2,488
5	Hotspot.Shield	Proxy	Client-Server	1	4.24 MB	1,186
5	SOCKS4	Proxy	Network-Protocol	1	290.28 KB	741
5	SOCKS5	Proxy	Network-Protocol	1	240.37 KB	645
5	VeePN.VPN	Proxy	Client-Server	2	1.00 MB	220
5	Turbo.VPN	Proxy	Client-Server	1	344.52 KB	199
5	Surfshark.VPN	Proxy	Client-Server	3	624.06 KB	170
5	TunnelBear	Proxy	Client-Server	1	340.75 KB	92
5	Psiphon	Proxy	Client-Server	4	1.02 MB	90
5	Tor	Proxy	Client-Server	1	94.34 KB	66
5	Touch.VPN	Proxy	Client-Server	1	273.30 KB	53
5	CryptoTab.Mining	General.Interest	Client-Server	2	25.57 MB	52
5	Bitcoin.Cryptocurrency.Miner	General.Interest	Client-Server	3	99.82 MB	36
5	SkyVPN	Proxy	Client-Server	6	28.26 MB	27
5	Monero.Cryptocurrency.Miner	General.Interest	Client-Server	6	19.21 MB	24
5	Ethereum.Cryptocurrency.Miner	General.Interest	Client-Server	2	1.27 MB	11
5	Opera.VPN	Proxy	Client-Server	1	38.00 KB	8
4	BitTorrent	P2P	Peer-to-Peer	20	55.23 MB	33,362

Top Application Vulnerability Exploits Detected

Severity	Threat Name	Type	CVE-ID	Victim	Source	Count
5	Hikvision.Products.SDK.WebLanguage.Tag.Command.Injection	OS Command Injection	CVE-2021-36260	2	14	34,961
5	PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	Code Injection	CVE-2017-9841	1,137	105	24,076
5	Andromeda.Botnet			4	1	5,192
5	Apache.Struts.2.DefaultActionMapper.Remote.Command.Execution	Other	CVE-2013-2251	1,137	4	3,473
5	NETGEAR.DGN1000.CGI.Unauthenticated.Remote.Code.Execution	Code Injection		877	1,560	1,782
5	DZS.GPON.Remote.Code.Execution	OS Command Injection	CVE-2018-10561,CVE-2018-10562	873	1,544	1,724
5	D-Link.Devices.HNAP.SOAPAction-Header.Command.Execution	OS Command Injection	CVE-2015-2051,CVE-2019-10891	868	1,507	1,641
5	Bladabindi.Botnet			599	384	1,370
5	Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution	Code Injection	CVE-2017-5638	860	33	1,265
5	Apache.Log4j.Error.Log.Remote.Code.Execution	Permission/Privilege/Access Control	CVE-2021-4104,CVE-2021-44228,CVE-2021-45046	91	15	1,026
5	OpenSSL.Heartbleed.Attack	Information Disclosure	CVE-2014-0160	26	16	877
5	TP-Link.Devices.userRpmNatDebugRpm.Authentication.Bypass	Permission/Privilege/Access Control		605	1	826
5	Joomla!.Core.Session.Remote.Code.Execution	Code Injection	CVE-2015-8562	5	35	819
5	njRAT.Botnet			1	1	812
5	WIFICAM.P2P.GoAhead.Multiple.Remote.Code.Execution	Code Injection	CVE-2017-8221,CVE-2017-8223,CVE-2017-8225,CVE-2017-18377	6	17	798

การยับยั้งการโจมตีบนระบบเครือข่าย โดย อุปกรณ์ Next Gen Firewall : Fortinet
(ข้อมูล 1 เดือนย้อนหลัง)

Web Usage : Top Web Applications

Application	Sessions	Bytes
YouTube	47,558,202	89.82 TB
HTTPS.BROWSER	192,102,486	76.55 TB
TikTok	111,514,247	63.29 TB
Facebook	110,748,714	32.41 TB
Instagram	104,792,377	27.11 TB
Apple.Store	15,497,411	25.64 TB
Netflix	5,746,462	12.83 TB
Google.Services	87,069,907	12.82 TB
iCloud	48,378,019	10.91 TB
Apple.Services	25,255,488	9.82 TB
Microsoft.Windows.Update	2,446,779	8.04 TB
Twitch	984,971	4.49 TB
Twitter	5,992,830	3.85 TB
Microsoft.Portal	29,448,450	3.41 TB
HTTP.BROWSER	20,268,718	3.40 TB
Riot.Games	1,082,610	3.25 TB
SSL	10,342,126	2.50 TB
Amazon.CloudFront	591,764	2.49 TB
OneDrive	994,950	2.30 TB
Google.Photos	301,232	1.70 TB
Telegram	1,018,862	1.69 TB
Amazon.AWS	1,615,445	1.65 TB
HTTP.Download.Accelerator	132,631	1.61 TB
HTTP.Segmented.Download	184,648	1.36 TB
Google.Services	4,528,295	1.34 TB

การยับยั้งการโจมตีบนระบบเครือข่าย โดย อุปกรณ์ Next Gen Firewall : Fortinet สำหรับโซน REG และ Finance

Top Applications by Bandwidth

#	Application	Bandwidth (Sent / Received)
1	HTTPS.BROWSER	24.56 GB
2	tcp/21064	8.68 GB
3	SMB	3.89 GB
4	DTLS	3.63 GB
5	HTTP.BROWSER	1.62 GB
6	Microsoft.Windows.Update	1.06 GB
7	Apple.iPhone	507.54 MB
8	Facebook	494.23 MB
9	YouTube	376.47 MB
10	SSL	353.63 MB

Top Applications by Sessions

#	Application	Sessions
1	HTTP	590,150
2	HTTPS.BROWSER	107,769
3	HTTP.BROWSER	35,883
4	Web Management	30,222
5	DNS	19,798
6	SSL	12,903
7	HTTPS	12,006
8	udp/5353	9,472
9	DHCP6	8,965
10	Endpoint Control Registration	5,698

การยับยั้งการโจมตีบนระบบเครือข่าย โดย อุปกรณ์ Next Gen Firewall : Fortinet สำหรับโซน REG และ Finance

Intrusions Detected

No matching log data for this report

Events by Severity