ฝ่ายโครงสร้างพื้นฐานและระบบเครือข่าย

รายงานการใช้งานระบบเครือข่ายคอมพิวเตอร์ ประจำเดือน ธันวาคม 67

ระบบเครือข่ายคอมพิวเตอร์

ระบบ Internet Data Center

ระบบโทรคมนาคม

รายงานจำนวนผู้ใช้งานผ่านระบบเครือข่าย (LAN)
(ไม่รวมห้องปฏิบัติการคอมฯ)

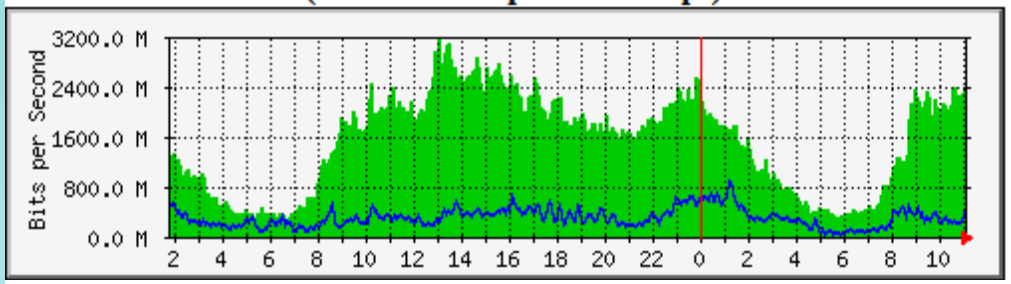
วิธีการ	จำนวน
วิธีการแบบ ISE (802.1x)	116 คน

ที่มา (ise) https://203.158.4.207

รายงานการใช้งานระบบเครือข่าย

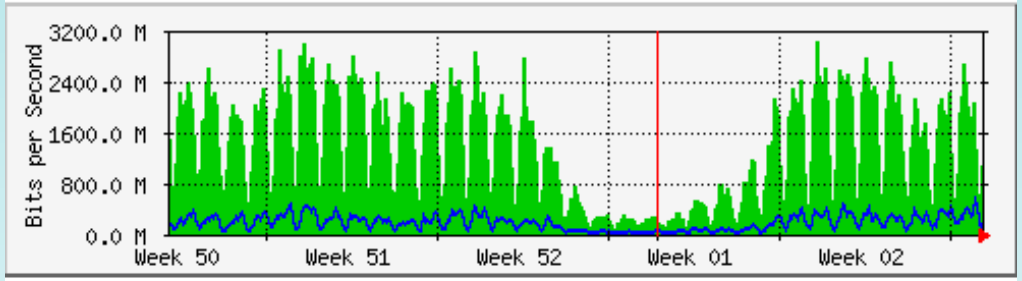
Internet Gateway Traffic

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



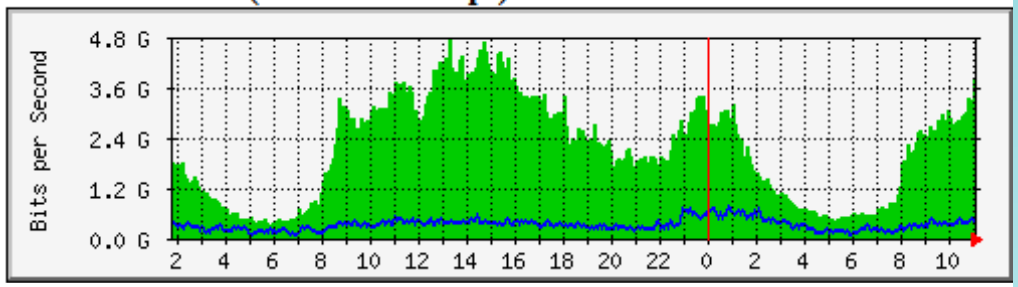
	Max	Average	Current
In	3148.9 Mb/s (31.5%)	1489.8 Mb/s (14.9%)	2379.6 Mb/s (23.8%)
Out	879.3 Mb/s (8.8%)	287.7 Mb/s (2.9%)	482.9 Mb/s (4.8%)

`Monthly' Graph (2 Hour Average)



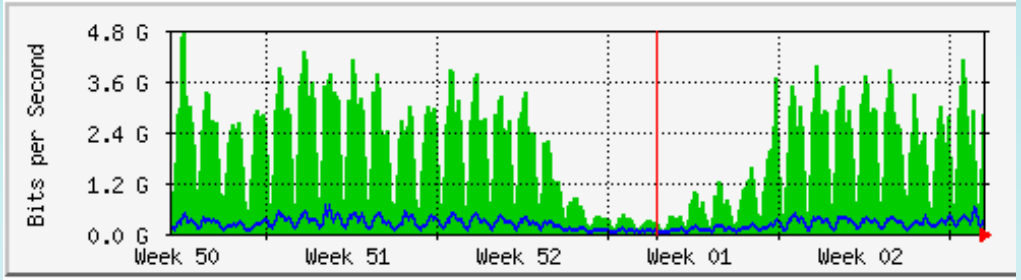
	Max	Average	Current
In	3022.5 Mb/s (30.2%)	1306.2 Mb/s (13.1%)	1062.9 Mb/s (10.6%)
Out	574.4 Mb/s (5.7%)	169.9 Mb/s (1.7%)	262.3 Mb/s (2.6%)

Link to UNINET (Domestic 10Gbps)



	Max	Average	Current
In	4790.5 Mb/s (47.9%)	2096.0 Mb/s (21.0%)	3800.5 Mb/s (38.0%)
Out	734.4 Mb/s (7.3%)	308.0 Mb/s (3.1%)	548.3 Mb/s (5.5%)

`Monthly' Graph (2 Hour Average)

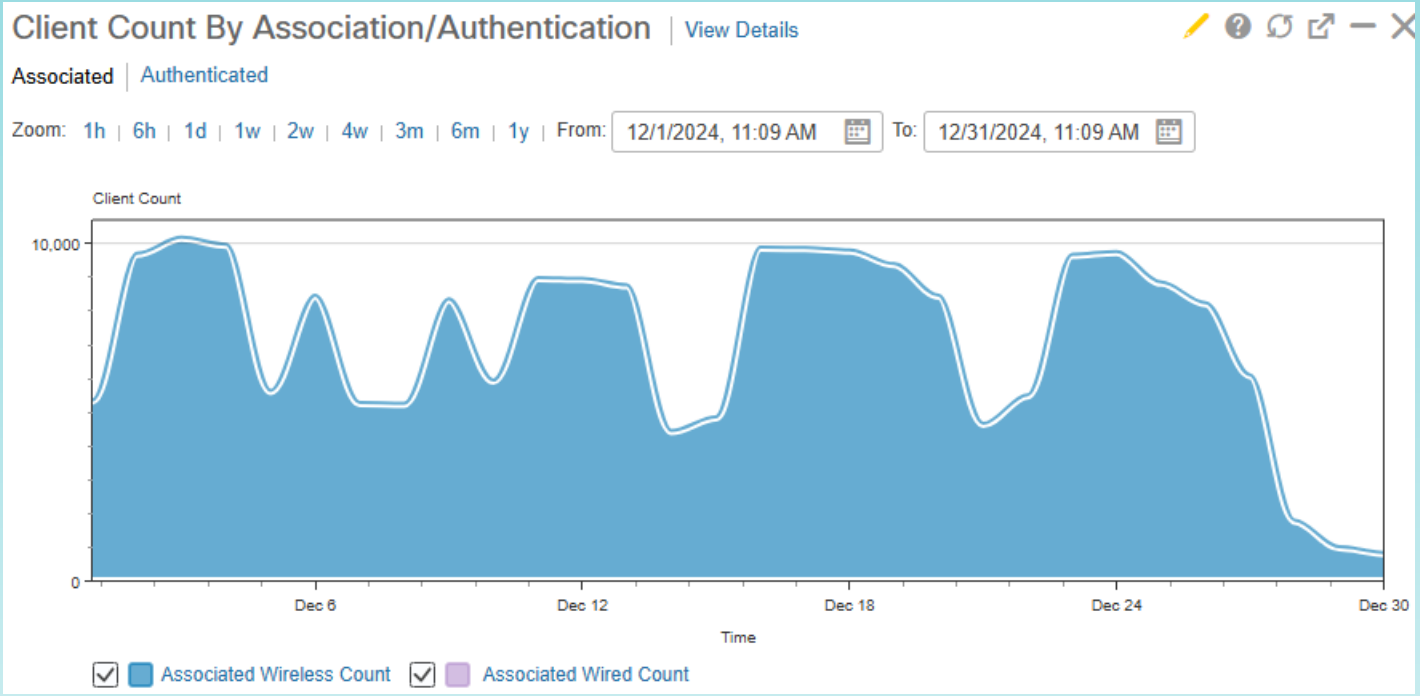


	Max	Average	Current
In	4752.5 Mb/s (47.5%)	1781.6 Mb/s (17.8%)	2805.5 Mb/s (28.1%)
Out	646.1 Mb/s (6.5%)	211.2 Mb/s (2.1%)	358.5 Mb/s (3.6%)

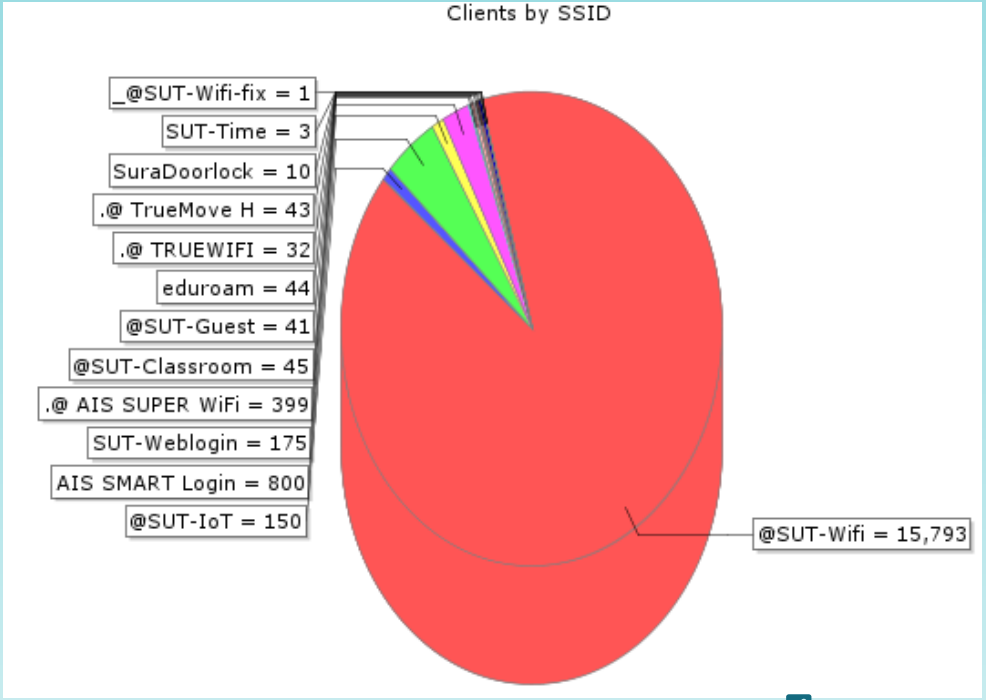
รายงานจำนวนผู้ใช้งานผ่านระบบเครือข่ายไร้สาย

สรุปสถิติจำนวนผู้ใช้งานผ่านระบบ wireless ทั้งหมด

สรุปปริมาณผู้ใช้งานต่อวัน



แบ่งตาม SSID สถิติย้อนหลัง 1 เดือน



- ผู้ใช้งานผ่านระบบ wireless สูงสุด 10,182 คน/วัน
- ผู้ใช้งานผ่านระบบ wireless, ต่ำสุด 869 คน/วัน
- ผู้ใช้งานผ่านระบบ wireless เฉลี่ย 7,145 คน/วัน

สรุปการดำเนินการบนระบบเครือข่ายคอมพิวเตอร์

02/12/2024	ตรวจสอบ wire lan อาคารวิชาการ 1 ชั้น 4 เกิดไฟฟ้าดับ และ ไฟฟ้ามา ก็ใช้งานไม่ได้ ตรวจสอบเบื้องต้น อุปกรณ์เครือข่ายทำงานปกติ เข้าไปตรวจสอบพบสายขาด ดำเนินการเปลี่ยน patch panel และ หนีบหัว rj45 สายของ user ใหม่ สามารถใช้งานได้ปกติ
02/12/2024	ดำเนินการตรวจสอบอุปกรณ์ AP หอพักนักศึกษา 9 ตรวจสอบพบว่า มี มด เข้ามาทำรังในอุปกรณ์ทำให้อุปกรณ์ AP ชำรุดเสียหาย จึงได้ดำเนินการแจ้งเจ้าหน้าที่หอพักให้ทราบถึงปัญหาเบื้องต้นเป็นที่เรียบร้อย
03/12/2024	ดำเนินการตรวจสอบอุปกรณ์ AP ภายในเรือนพักสุขนิวาส 1 ชั้น 3 จำนวน 1 จุด ที่ไม่สามารถใช้งานได้ จึงได้ดำเนินการแก้ไขให้กับมาใช้งานได้ตามปกติเป็นที่เรียบร้อย
04/12/2024	ตรวจสอบอุปกรณ์ UPS ไม่จ่ายไฟ ทำให้สัญญาณอุปกรณ์ AP ภายในหอพักนักศึกษาใช้งานไม่ได้ จึงได้ดำเนินการแก้ไขให้กับมาใช้งานเป็นปกติเป็นที่เรียบร้อยแล้ว ตรวจสอบอุปกรณ์ AP และตู้ Control ภายในหอพักนักศึกษา 6
04/12/2024	ตรวจสอบอุปกรณ์ AP ภายในอาคารเรียนรวม 1

สรุปการดำเนินการบนระบบเครือข่ายคอมพิวเตอร์

09/12/2024	ตรวจสอบอุปกรณ์ AP อาคารเรียนรวม 1 ชั้น 1-2 อุปกรณ์เครือข่าย switch ดับ และมีการปรับปรุงอาคารเรียนรวมทั้ง 1-2 และ lan ตามห้องเรียนชั้น 1-2 ตรวจพบ อุปกรณ์ switch ไม่ติด และ ห้องเรียนปรับปรุงไม่มีสาย lan แจ้ง ผู้คุมงานรับทราบ กรณี wifi ไม่สามารถแก้ไขได้ แต่ละห้องมีสอบ
11/12/2024	ดำเนินการตรวจสอบอุปกรณ์ AP อาคารเรียนรวม 1 ชั้น 1 ที่ไม่สามารถใช้งานได้และดำเนินการแก้ไข ให้กลับมาใช้งานได้ตามปกติ เป็นที่เรียบร้อย
11/12/2024	ดำเนินการตรวจสอบอุปกรณ์ AP โซนหอพักนักศึกษาสุรนิเวศ 18
11/12/2024	ดำเนินการเปลี่ยนอุปกรณ์ AP เพื่อทดสอบสัญญาณ wifi โซนหอพักนักศึกษาสุรนิเวศ 18 บริเวณชั้น 4 จำนวน 1 ตัว
12/12/2024	ได้ดำเนินการตรวจสอบ เรื่อง : ขอความอนุเคราะห์ตรวจเช็คสัญญาณWiFi เนื่องจากได้รับร้องเรียนจากนักศึกษาว่า มีปัญหาในการเชื่อมต่อ ติดๆดับๆ โดยเฉพาะการใช้ใน LabTop เครื่องส่งสัญญานหน้าห้อง 10210-10209 อาคาร : หอพักสุรนิเวศ 10 ชั้น : ชั้น 2 จากการเข้าตรวจสอบพบว่า สัญญาณ wifi บริเวณหน้าห้อง ปกติ และได้ทำการ Reset อุปกรณ์ AP สัญญาณ wifi ใหม่ พร้อมตรวจสอบเครื่องและสัญญาณ wifi ภายในห้องพัก พบว่าสัญญาณ ปกติ โดยแจ้งผู้ใช้งานให้ทราบถึงปัญหาในการใช้งานเบื้องต้นเป็นที่เรียบร้อย

สรุปการดำเนินการบนระบบเครือข่ายคอมพิวเตอร์

16/12/2024	Set config switch เพื่อทดแทนเครื่องเดิมที่เสีย สำหรับใช้กับ AP ที่ชั้น 1 อาคารสุรเริงไชย (โซน 3)
16/12/2024	ดำเนินการเปลี่ยน sw ที่อาคารสุรเริงไชย ทดแทนตัวเดิมที่ชำรุดเสียหาย เนื่องจากการใช้งานมานาน เพื่อให้ ap สามารถใช้งานได้ตามปกติ
17/12/2024	ดำเนินการตรวจสอบตู้อุปกรณ์เครือข่ายโซนหอพักสุรนิเวศ 16 และได้ดำเนินการแก้ไขให้กลับมาใช้งานได้ตามปกติ
17/12/2024	ดำเนินการเปลี่ยนอุปกรณ์ AP เพื่อทดสอบสัญญาณ wifi โซนหอพักนักศึกษาสุรนิเวศ 18 บริเวณชั้น 4 จำนวน 1 ตัว
17/12/2024	ดำเนินการตรวจสอบอุปกรณ์ AP หอพักสุรนิเวศ 2 บริเวณชั้น 2 เนื่องจากใช้งานไม่ได้ และได้ดำเนินการแก้ไขให้กลับมาใช้งานได้ตามปกติเป็นที่เรียบร้อย
17/12/2024	ดำเนินการเปลี่ยนอุปกรณ์เครือข่าย SW บริเวณหน้าห้อง polymer จำนวน 1 ตัว เพื่อให้ระบบเครือข่ายทำงานได้ตามปกติ
18/12/2024	ดำเนินการตรวจสอบอุปกรณ์ AP ที่อาคารเครื่องมือ 9 ชั้น 3
18/12/2024	set switch อุปกรณ์เครือข่าย โซนหน้าห้อง polymer บริเวณ C1 ชั้น 4

สรุปการดำเนินการบนระบบเครือข่ายคอมพิวเตอร์

19/12/2024	ดำเนินการตรวจสอบสัญญาณ Internet ห้องพักอาจารย์สำนักวิชาวิศวกรรมโยธา อาคารวิชาการ 1 ชั้น 4
19/12/2024	ดำเนินการตรวจสอบ อุปกรณ์ AP บริเวณอาคารเรียนรวม 1 ชั้น 2
23/12/2024	ดำเนินการตรวจสอบอุปกรณ์ AP บริเวณหอพักนักศึกษา หอพักสุรนิเวศ 15

สรุปการดำเนินการบนระบบ Internet Data Center

04/12/2024	สร้างบัญชีผู้ใช้งานระบบเครือข่ายคอมพิวเตอร์ สำหรับอาจารย์ประจำโรงพยาบาลร่วมผลิต
04/12/2024	เปลี่ยนที่อยู่เว็บไซต์ และขอเพิ่ม User ของผู้ดูแล Server จาก cste-dev.sut.ac.th/cste เป็น https://cste.sut.ac.th
06/12/2024	ได้รับหนังสือ อว.7434(4) ต้องการให้ภายนอกสามารถเข้ามาในระบบ cctv private ip 192.168.144.250 ระบบ scan หน้าของนักเรียน โครงการนักเรียน ราชสีมา เพื่อตรวจสอบ เข้า ออก ผ่านระบบตรวจสอบหน้าตา โดยแจ้ง public ip 203.158.7.129/25 และแจ้ง ผู้ประสานงานทราบ
06/12/2024	ทดสอบจับสัญญาณ @SUT-Guest ตามที่ผู้รับบริการแจ้ง พบว่า Account ที่ขอข้ามปีไม่สามารถใช้งานได้ และ Account ที่ขอถึง 31 ธันวาคม 67 สามารถใช้งานได้ แนะนำให้ผู้รับบริการ Gen Account ใหม่ ให้อยู่ภายในปี 67 และทดสอบการใช้งาน สามารถใช้งานได้
12/12/2024	อว 7402(3)/5626 ขอ vm เพื่อพัฒนาระบบสอบ online ดำเนินการ และ ส่งข้อมูลให้ user ตามความต้องการเรียบร้อย
17/12/2024	จัดทำไฟล์สื่อรูปภาพประชาสัมพันธ์ลงทะเบียนอีเมลสำรอง
24/12/2024	เชื่อมต่อ Radius Server ให้กับสำนักแพทย์

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

สรุปการดำเนินการบนระบบโทรคมนาคม

04/12/2024	ติดรหัสครุภัณฑ์โทรศัพท์ จำนวน 30 เครื่อง ตามใบสั่งซ์อที่ PO-6744-006 จัดทำใบยืมครุภัณฑ์จำนวน 30 เครื่อง
04/12/2024	ติดรหัสครุภัณฑ์โทรศัพท์ จำนวน 30 เครื่อง ตามใบสั่งซ์อที่ PO-6744-006
06/12/2024	โทรศัพท์ไม่มีสัญญาณรหัสครุภัณฑ์5805-001-37-00069-3040000,5805-001-37/00063-3040000 ตรวจแล้วว่ามีเจ้าหน้าที่คุณปัทมา เจ้าหน้าที่บริหารงานทั่วไปมาซ่อมให้แล้ว
06/12/2024	ขอเบิกโทรศัพท์สำนักงาน เครื่องใหม่ให้กับพนักงานใหม่(เจ้าหน้าที่ไม่สะดวกรับบริการ ขอนัดวันจัทร์10 ธค 67)
06/12/2024	ขอแจ้งวันเริ่มปฏิบัติงานของพนักงานประจำ (น.ส. ภัทริกา ลับดีพะเนาว์)สำนักวิชาศาสตร์และศิลป์ดิจิทัล เจ้าหน้าที่ขอเลื่อนวันรับบริการ
06/12/2024	โทรศัพท์ห้องอาจารย์ สุดเขตเสีย รหัสครุภัณฑ์5805-001-01/54/162-3040000 Outlet เสียบติดผนังชำรุด ดำเนินการแก้ไข ใช้งานได้ปกติ
09/12/2024	ติดตั้งเครื่องโทรศัพท์อาคารศูนย์เครื่องมือวิทยาศาสตร์และเทคโนโลยี5 ห้อง5104 นายจักกฤษณ์ ธนะมณีวุฒิ

สรุปการดำเนินการบนระบบโทรคมนาคม

09/12/2024	ตรวจสอบอุปกรณ์ยืม-คืนเฉพาะกิจวิทยุสื่อสาร จำนวน 15 เครื่อง (อพ.สธ. ส่วนกิจฯ) เลขใบงานE67/1728
11/12/2024	ตรวจสอบอุปกรณ์ยืม-คืนเฉพาะกิจ วิทยุสื่อสาร จำนวน 10 เครื่อง (อพ.สธ.ยานพาหนะ) เลขใบงาน E67/1735
11/12/2024	ตรวจสอบอุปกรณ์ยืม-คืนเฉพาะกิจ วิทยุสื่อสาร จำนวน 3 เครื่อง (อพ.สธ.การแสดง) เลขใบงาน E67/1729
11/12/2024	โทรศัพท์สำนักงานเสีย รหัสครุภัณฑ์ 5805-001-01/55/00384-3040000ห้องหัวหน้าสถานนวัตกรรมวิศวศึกษา ดำเนินการเปลี่ยนเครื่อง
12/12/2024	โทรศัพท์เสีย มีเสียงซ่าๆ รหัสครุภัณฑ์ :5805-001-12/57/00061-3040000 สถานที่ :วิชาการ 1 อาคาร : C1 ชั้น : 4 ห้องCME04
18/12/2024	ศูนย์บริการการศึกษา ศบก. ขอความอนุเคราะห์ย้ายหมายเลขโทรศัพท์ 3017 จากเคาน์เตอร์ 1 ไปที่ เคาน์เตอร์ 4
18/12/2024	ตรวจสอบอุปกรณ์วิทยุสื่อสาร จำนวน 16 เครื่อง (ค่ายภาวะผู้นำครั้งที่8)

สรุปการดำเนินการบนระบบโทรคมนาคม

18/12/2024	ขอแจ้งเปลี่ยนเครื่องโทรศัพท์ ผศ.ดร.คธา วาทกิจ รหัสครุภัณฑ์5805-001-01/57/00017-3040000ห้อง AE08 อาคาร วิชาการ 1 ชั้น2
19/12/2024	โทรศัพท์ เสียงซ่า ตลอดเวลารหัสครุภัณฑ์ :5805-01/55/00466-3040000 สถานที่ : ส่วนการเงินและบัญชี อาคาร : บริหาร ชั้น : 1 แก้ไขโดยการเปลี่ยนเครื่องโทรศัพท์รหัส 5805-001-01/68/00017-3040000
23/12/2024	แจ้งซ่อมหัว RJเข้าเครื่องโทรศัพท์ชำรุด 5805-001-01/62/00036-3040000สถานกีฬาและสุขภาพ เข้าดำเนินการเปลี่ยนเรียบร้อย
24/12/2024	สัญญานโทรศัพท์เสีย งานยานพาหนะ ส่วนอาคารสถานที่ อาคาร : ขนส่งชั้น : 1
24/12/2024	ตรวจสอบครุภัณฑ์ พนักงานที่ลาออก1ท่านมียืมเครื่องโทรศัพท์5805-001-01/66/00024-3040000เปลี่ยนชื่อผู้ยมเครื่อง
24/12/2024	สายสัญญาณโทรศัพท์พอยกจะรับโทรศัพท์แล้วสายหลุด สาขาวิศวกรรมเครื่องกล
24/12/2024	โทรศัพท์ห้องทำงานของ ผศ.ดร.ปรัชญา เทพณรงค์ใช้งานไม่ได้ รหัสครุภัณฑ์ 5805-001-01/48/047-3040000เปลี่ยนเครื่องใหม่ให้แล้ว

สรุปการดำเนินการด้านอื่น ๆ

02/12/2024	ประชุมคณะทำงานสำรวจครุภัณฑ์ ประจำหน่วยงาน ครั้งที่ 7/2567
09/12/2024	จัดทำรายงานผลการดำเนินงานฝ่ายโครงสร้างฯ ประจำเดือน พ.ย. 2567
11/12/2024	ประชุมจัดเตรียม การดำเนินการจัดโครงการประชุมบุคลากรและรายงานผลการดำเนินการ (ครึ่งปีหลัง)
12/12/2024	จัดดทำเอกสารจัดซื้ออุปกรณ์ระบบโทรศัพท์และการสื่อสาร จำนวน 1 ระบ
12/12/2024	สร้าง Account (SUT-Guest) ให้วิศวกรรมเมคคาทรอนิกส์ เนื่องจากมีผู้มาอบรม
20/12/2024	จัดทำเอกสารจ้างซ่อมสายเคเบิลใยแก้วนำแสง (Fiber Optic) ฟาร์มมหาวิทยาลัย
23/12/2024	ประชุมคณะทำงานการจัดการความรู้ ประจำศูนย์คอมพิวเตอร์ ครั้งที่ 4/2567

สรุปการดำเนินการด้านอื่น ๆ

23/12/2024	ประชุมคณะกรรมการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์ (e-bidding) - จ้างบำรุงรักษาอุปกรณ์เครือข่ายและระบบบริหารจัดการ จำนวน 1 ระบบ - ซื้ออุปกรณ์ประจำเครือข่ายหลัก ดาต้าเซนเตอร์ และเครือข่ายย่อย จำนวน 1 ระบบ
24/12/2024	ประชุมคณะกรรมการดำเนินงานเกี่ยวกับการคุ้มครองส่วนบุคคลของมหาวิทยาลัยเทคโนโลยีสุรนารี ครั้งที 5/2567
25/12/2024	จัดทำรายงานประชุมคณะกรรมการดำเนินงานเกี่ยวกับการคุ้มครองส่วนบุคคลของมหาวิทยาลัยเทคโนโลยีสุรนารี ครั้งที่ 5/2567

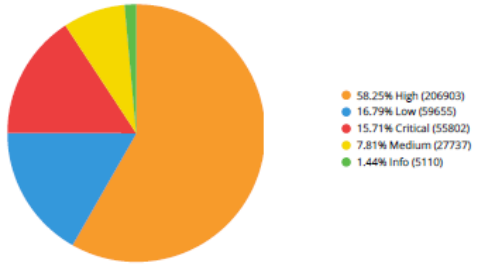
ภัยคุกคามระบบเครือข่าย

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

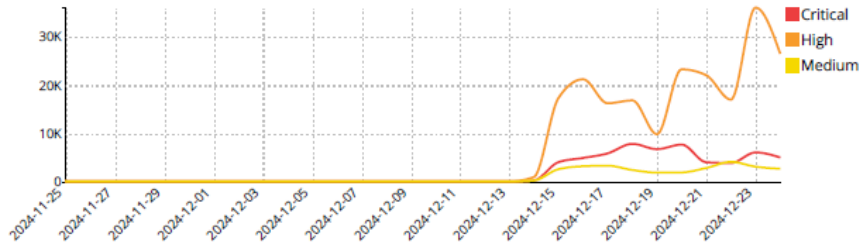
SUT Gatway of IPS Report

Summary

Intrusions By Severity



Critical High and Medium Intrusions Timeline



Intrusions By Types

#	Intrusion Type	Counts
1	Code Injection	71,627
2	Anomaly	62,436
3	Path Traversal	47,638
4	SQL Injection	45,046
5	Permission/Privilege/Access Control	26,539
6	OS Command Injection	21,185
7	Other	17,382
8	Malware	7,816
9	Buffer Errors	7,411
10	XSS	1,935
11	Information Disclosure	1,749
12	DoS	863
13	Improper Authentication	644
14	CSRF	45

Intrusions Detected

Critical Severity Intrusions

#	Attack Name	CVE-ID	Intrusion Type	Counts
1	PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	CVE-2017-9841	Code Injection	23,389
2	Andromeda.Botnet			4,742
3	Bladabindi.Botnet			2,611
4	NETGEAR.DGN1000.CGI.Unauthenticated.Remote.Code.Execution		Code Injection	2,167
5	DZS.GPON.Remote.Code.Execution	CVE-2018-10561,CVE-2018-10562	OS Command Injection	2,154
6	D-Link.Devices.HNAP.SOAPAction-Header.Command.Execution	CVE-2015-2051,CVE-2019-10891,CVE-2022-37056,CVE-2024-33112	OS Command Injection	2,066
7	Drupal.Core.REST.Module.Remote.Code.Execution	CVE-2019-6340	OS Command Injection	2,019
8	WIFICAM.P2P.GoAhead.Multiple.Remote.Code.Execution	CVE-2017-8221,CVE-2017-8223,CVE-2017-8225,CVE-2017-18377	Code Injection	1,895
9	Gh0st.Rat.Botnet			1,515
10	TOTOLINK.Devices.cstecgi.Command.Injection		OS Command Injection	1,241
		CVE-2024-0295,CVE-2024-7160,CVE-2024-7171,CVE-2024-7174,CVE-2024-7175,CVE-2024-7177,CVE-2024-7214,CVE-2024-7215,CVE-2024-8574,CVE-2021-42888,CVE-2022-25134,CVE-2022-26186,CVE-2022-26187,CVE-2022-26188,CVE-2022-26189,CVE-2022-26206,CVE-2022-26207,CVE-2022-26208,CVE-2022-26209,CVE-2022-26210,CVE-2022-26211,CVE-2022-26212,CVE-2022-26213,CVE-2022-26214,CVE-2022-27003,CVE-2022-27004,CVE-2022-27005,CVE-2022-28575,CVE-2022-28577,CVE-2022-28578,CVE-2022-28579,CVE-2022-28580,CVE-2022-28581,CVE-2022-28582,CVE-2022-28583,CVE-2022-28584,CVE-2022-28905,CVE-2022-28906,CVE-2022-28907,CVE-2022-28908,CVE-2022-28909,CVE-2022-28910,CVE-2022-28911,CVE-2022-28912,CVE-2022-28913,CVE-2022-28935,CVE-2022-32449,CVE-2022-38308,CVE-2022-38826,CVE-2022-38827,CVE-2022-38828,CVE-2022-41518,CVE-2022-41525,CVE-2023-24154,CVE-2023-24236,CVE-2023-24238,CVE-2023-24276,CVE-2023-25395,CVE-2023-26848,CVE-2023-31569,CVE-2023-31569,CVE-2023-31729,CVE-2023-33487,CVE-2023-33556,CVE-2023-46484,CVE-2023-46485,CVE-2023-46574,CVE-2023-46976,CVE-2023-46993,CVE-2023-49417,CVE-2023-49418,CVE-2023-50651,CVE-2023-51014,CVE-2023-51034,CVE-2023-51035,CVE-2023-52026,CVE-2023-52027,CVE-2023-52028,CVE-2023-52029,CVE-2023-52030,CVE-2023-52031,CVE-2023-52038,CVE-2023-52039,CVE-2023-52040,CVE-2023-52041,CVE-2023-52042,CVE-2024-22942,CVE-2024-23057,CVE-2024-23058,CVE-2024-23059,CVE-2024-23060,CVE-2024-23061,CVE-2024-24325,CVE-2024-24326,CVE-2024-24327,CVE-2024-24328,CVE-2024-24330,CVE-2024-24331,CVE-2024-24332,CVE-2024-24333,CVE-2024-25468,CVE-2024-31807,CVE-2024-31808,CVE-2024-31809,CVE-2024-31811,CV		

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

SUT Gatway of IPS Report

Intrusion Victims

#	Attack Victim	Counts	Critical	High	Medium	Percent of Total Attacks
1	202.28.42.26	20,158				24.66%
2	203.158.4.150	7,145				8.74%
3	202.28.42.71	6,580				8.05%
4	10.0.11.4	4,351				5.32%
5	203.158.3.42	4,031				4.93%
6	202.28.42.60	3,583				4.38%
7	203.158.3.125	3,505				4.29%
8	94.247.42.28	3,408				4.17%
9	77.220.212.54	3,399				4.16%
10	185.237.206.129	3,395				4.15%
11	45.155.250.224	3,393				4.15%
12	203.158.4.111	3,348				4.10%
13	202.28.42.40	2,613				3.20%
14	185.196.9.67	2,344				2.87%
15	203.158.3.44	2,268				2.77%
16	203.158.7.70	2,210				2.70%
17	203.158.7.63	2,011				2.46%
18	10.1.20.128	1,592				1.95%
19	202.28.42.30	1,518				1.86%
20	203.158.7.71	892				1.09%

Intrusion Sources

#	Attack Source	Counts	Critical	High	Medium	Percent of Total Attacks
1	92.255.57.58	45,158				24.11%
2	31.220.1.144	20,850				11.13%
3	31.220.1.88	18,581				9.92%
4	185.224.128.43	18,098				9.66%
5	203.86.235.18	16,156				8.62%
6	10.1.149.170	15,918				8.50%
7	180.188.198.140	7,225				3.86%
8	203.86.235.12	6,439				3.44%
9	180.188.198.112	4,807				2.57%
10	184.105.192.2	4,742				2.53%
11	195.3.223.52	4,691				2.50%
12	119.82.255.34	4,145				2.21%
13	180.188.198.109	3,783				2.02%
14	95.214.55.74	3,664				1.96%
15	180.188.198.132	2,451				1.31%
16	141.98.11.155	2,333				1.25%
17	180.188.198.116	2,264				1.21%
18	47.76.72.62	2,035				1.09%
19	38.61.1.134	1,999				1.07%
20	95.214.53.211	1,980				1.06%

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

Intrusions Blocked

SUT Gatway of IPS Report

#	Intrusion Name	Intrusion Type	Severity	Counts
1	PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	Code Injection	Critical	23,389
2	Andromeda.Botnet		Critical	4,742
3	Bladabindi.Botnet		Critical	2,611
4	NETGEAR.DGN1000.CGI.Unauthenticated.Remote.Code.Execution	Code Injection	Critical	2,167
5	DZS.GPON.Remote.Code.Execution	OS Command Injection	Critical	2,154
6	D-Link.Devices.HNAP.SOAPAction-Header.Command.Execution	OS Command Injection	Critical	2,066
7	Drupal.Core.REST.Module.Remote.Code.Execution	OS Command Injection	Critical	2,019
8	WIFICAM.P2P.GoAhead.Multiple.Remote.Code.Execution	Code Injection	Critical	1,895
9	Gh0st.Rat.Botnet		Critical	1,515
10	TOTOLINK.Devices.cstecgi.Command.Injection	OS Command Injection	Critical	1,241
11	Remote.CMD.Shell	Malware	Critical	1,180
12	Cisco.IOS.XE.Web.UI.Unauthorized.Account.Creation	Permission/Privilege/Access Control	Critical	1,035
13	Aigital.Wireless.Devices.formSysCmd.Command.Injection	OS Command Injection	Critical	1,025
14	OpenSSL.Heartbleed.Attack	Information Disclosure	Critical	880
15	Bash.Function.Definitions.Remote.Code.Execution	OS Command Injection	Critical	606
16	ThinkPHP.Controller.Parameter.Remote.Code.Execution	Code Injection	Critical	496
17	Mega.MSNSwitch.ExportSettings.Remote.Code.Execution	OS Command Injection	Critical	496
18	TVT.DVR.Remote.Code.Execution	Permission/Privilege/Access Control	Critical	481
19	Amadey.Botnet		Critical	474
20	Telesquare.SDT-CW3B1.Command.Injection	OS Command Injection	Critical	375

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	705.80 MB	767,150
5	Proxy.HTTP	Proxy	Network-Protocol	104	3.63 GB	192,231
5	Hola.Unblocker	Proxy	Client-Server	8	18.31 MB	9,358
5	Monero.Cryptocurrency.Miner	General.Interest	Client-Server	10	28.69 MB	6,543
5	Turbo.VPN	Proxy	Client-Server	2	1.93 MB	1,301
5	Hotspot.Shield	Proxy	Client-Server	1	1.44 MB	351
5	Touch.VPN	Proxy	Client-Server	2	864.60 KB	202
5	CryptoTab.Mining	General.Interest	Client-Server	4	84.14 MB	142
5	OKHTTP.Library.VPN	Proxy	Client-Server	2	3.44 MB	123
5	Psiphon	Proxy	Client-Server	1	355.99 KB	71
5	VeePN.VPN	Proxy	Client-Server	1	297.67 KB	58
5	Tor	Proxy	Client-Server	3	76.79 KB	53
5	Bitcoin.Cryptocurrency.Miner	General.Interest	Client-Server	1	112.19 MB	30
5	WindScribe	Proxy	Client-Server	1	101.57 KB	26
5	VPN.Master	Proxy	Client-Server	1	94.91 KB	15
5	SkyVPN	Proxy	Client-Server	3	9.58 MB	7
5	Bestline.VPN	Proxy	Client-Server	2	2.62 MB	2
4	BitTorrent	P2P	Peer-to-Peer	23	84.36 MB	440,162
4	RDP	Remote.Access	Client-Server	20	3.97 GB	16,068
4	SoftEther	Proxy	Peer-to-Peer	13	543.09 MB	6,318

Top Application Vulnerability Exploits Detected

Severity	Threat Name	Type	CVE-ID	Victim	Source	Count
5	PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	Code Injection	CVE-2017-9841	1,134	90	23,360
5	Andromeda.Botnet			2	1	4,742
5	Bladabindi.Botnet			1,102	529	2,597
5	NETGEAR.DGN1000.CGI.Unauthenticated.Remote.Code.Execution	Code Injection		942	1,848	2,083
5	DZS.GPON.Remote.Code.Execution	OS Command Injection	CVE-2018-10561,CVE-2018-10562	945	1,817	2,070
5	Drupal.Core.REST.Module.Remote.Code.Execution	OS Command Injection	CVE-2019-6340	1	6	2,019
5	D-Link.Devices.HNAP.SOAPAction-Header.Command.Execution	OS Command Injection	CVE-2015-2051,CVE-2019-10891,CVE-2022-37056,CVE-2024-33112	926	1,782	2,002
5	WIFICAM.P2P.GoAhead.Multiple.Remote.Code.Execution	Code Injection	CVE-2017-8221,CVE-2017-8223,CVE-2017-8225,CVE-2017-18377	7	16	1,895
5	Gh0st.Rat.Botnet			1,048	512	1,447
5	TOTOLINK.Devices.cstecgi.Command.Injection	OS Command Injection	CVE-2023-4412,CVE-2023-6612,CVE-2024-0295,CVE-2024-7160,CVE-2024-7171,CVE-2024-7174,CVE-2024-7175,CVE-2024-7177,CVE-2024-7214,CVE-2024-7215,CVE-2024-8574,CVE-2021-42888,CVE-2022-25134,CVE-2022-26186,CVE-2022-26187,CVE-2022-26188,CVE-2022-26189,CVE-2022-26206,CVE-2022-26207,CVE-2022-26208,CVE-2022-26209,CVE-2022-26210,CVE-2022-2	1,122	2	1,241

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

Web Usage : Top Web Applications

Application	Sessions	Bytes
YouTube	48,214,642	98.50 TB
HTTPS.BROWSER	186,200,317	83.92 TB
TikTok	116,817,382	69.25 TB
Facebook	109,957,115	30.94 TB
Instagram	114,478,974	26.92 TB
Apple.Store	16,504,722	18.73 TB
Netflix	5,588,859	13.19 TB
Google.Services	83,024,809	12.86 TB
iCloud	47,389,820	10.34 TB
Microsoft.Windows.Update	2,531,681	8.56 TB
Apple.Services	26,520,674	8.17 TB
SSL	14,195,594	5.57 TB
Twitter	5,936,415	5.46 TB
HTTP.BROWSER	21,889,666	4.93 TB
Microsoft.Portal	26,227,039	3.49 TB
Twitch	612,499	2.29 TB
Amazon.CloudFront	645,944	2.02 TB
Microsoft.365.Portal	746,179	1.94 TB
Amazon.AWS	1,292,730	1.88 TB
Riot.Games	846,815	1.77 TB
OneDrive	1,004,774	1.73 TB
Microsoft.SharePoint	2,180,406	1.60 TB
Telegram	1,093,438	1.58 TB
HTTP.Download.Accelerator	140,481	1.45 TB
Google.Cloud.Storage	375,702	1.38 TB

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

FIN-REG Security Analysis

Top Applications by Bandwidth

#	Application	Bandwidth	Sent	Received
1	HTTPS.BROWSER			70.68 GB
2	YouTube			39.38 GB
3	Facebook			32.46 GB
4	tcp/21064			26.30 GB
5	Netflix			16.25 GB
6	SMB			15.86 GB
7	Microsoft.Windows.Update			13.46 GB
8	SSL			10.76 GB
9	Microsoft.365.Portal			9.41 GB
10	Microsoft.Teams			7.48 GB

Top Applications by Sessions

#	Application	Sessions
1	DNS	719,668
2	HTTPS.BROWSER	560,342
3	SNMP	198,759
4	udp/5353	187,034
5	HTTP.BROWSER	149,177
6	Microsoft.Portal	147,968
7	SSL	131,430
8	HTTP	120,429
9	Endpoint Control Registration	114,615
10	Microsoft.365.Portal	100,385

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

Intrusions Detected

No matching log data for this report

Events by Severity