รายงานการใช้งานระบบเครือข่ายคอมพิวเตอร์ มหาวิทยาลัยเทคโนโลยีสุรนารี

1 ตุลาคม – 31 ธันวาคม 2559

1. <u>รายงานการดำเนินงานของฝ่ายเครือข่าย</u>

1.1 สรุปการดำเนินการบนระบบเครือข่าย SUTnet

- เริ่มใช้งาน internet service provider ใหม่ (3BB) แทน AIS ที่หมดสัญญาโดยมีความเร็ว internet เป็น 2 Gbps/1 Gbps (international/Domestic) (ความเร็วเท่าเดิม)
- Uninet เพิ่มความเร็ว internet ฝั่ง uninet จากเดิม 2 Gbps เป็น 3 Gbps วันที่ 31 ตุลาคม 2559
- ดำเนินการปรับเปลี่ยนระบบยืนยันตัวตน จาก cisco nac เป็น 802.1X เรียบร้อยแล้ว (ยังคงเหลือบางเครื่อง หรืออุปกรณ์ที่ยังไม่สามารถปรับเปลี่ยนได้ เช่น เครื่องที่ไม่สามารถรองรับการใช้งานแบบ 802.1x ได้ เป็นต้น)
- ปรับปรุงระบบสายส่งกระแสไฟฟ้า สำหรับห้อง data center ในวันศุกร์ที่ 11 พฤศจิกายน 2559 ตั้งแต่เวลา 20.00 - 24.00 น เนื่องด้วยสายไฟฟ้าหลักที่อาคารวิจัย ในส่วนที่ใช้งานระบบเครือข่ายและดาต้าเซนเตอร์ มีปัญหาจ่ายไฟเกินกำลังของสายส่ง ซึ่งอาจจะเกิดไฟฟ้าลัดวงจรได้ ทางส่วนอาคารสถานที่ (งานไฟฟ้า) มีความจำเป็นที่จะทำการปรับปรุงระบบสายส่งกระแสไฟฟ้า สำหรับห้อง data center อย่างเร่งด่วน เพื่อป้องกันและแก้ไขปัญหา
- ให้บริการขยายและแก้ไขจุดให้บริการเครือข่ายตามใบงานที่ได้รับแจ้งขอใช้บริการงานแจ้งซ่อมออนไลน์ (eccs.sut.ac.th) ดังนี้
    - ติดตั้ง Cisco 2960 ที่อัฒจันทร์สนามฟุตบอล จำนวน 2 เครื่อง (อุปกรณ์มากับการก่อสร้างอัฒจันทร์)
    - ติดตั้ง Cisco SG300 ที่อัฒจันทร์สนามฟุตบอล จำนวน 1 เครื่อง (อุปกรณ์มากับการก่อสร้างอัฒจันทร์)
    - ให้บริการชุดเครือข่ายฯ ชั่วคราวงานรายงานตัวนักศึกษาสำหรับงานพระราชทานปริญญาบัตร ประจำปีการศึกษา 2558 ที่อาคารสุรพัฒน์ 2
    - ให้บริการชุดเครือข่ายฯ ชั่วคราวตาม ศธ 5633(2)/294 งานกิจกรรมการสัมภาษณ์ผู้ผ่านการคัดเลือกประเภทโควตาวิชาเรียน ประจำปีการศึกษา 2560 ในวันที่ 17-18 ธันวาคม 2559 ที่อาคารเรียนรวม 1
    - แก้ไขจุดบริการระบบเครือข่ายฯ (Outlet LAN) จำนวน 1 จุด ที่ห้องคณบดี สำนักวิชาทันตแพทย์

- จัดทำสาย LAN เพื่อเชื่อมต่อกับจุดบริการเครือข่ายฯ ตามที่ได้รับแจ้งขอบริการ จำนวน 5 เส้น คือ ส่วนอาคารฯ (งานไฟฟ้า) จำนวน 1 เส้น, สำนักวิชาวิศวกรรมศาสตร์ จำนวน 2 เส้น, สาขาวิชาเทคโนโลยีการจัดการ จำนวน 1 เส้น และศูนย์เครื่องมือฯ อาคารเครื่องมือ 11 ชั้น 1 จำนวน 1 เส้น

1.2 สรุปการดำเนินการบนระบบเครือข่ายไร้สาย SUT-wifi

- ทดสอบระบบเครือข่ายไร้สายแบบปลอดภัย (ตามมาตราฐาน 802.1x) พร้อมระบบลงทะเบียน MAC Address อัตโนมัติ (โดยกำหนดให้ 1 บัญชี internet account สามารถใช้งานได้ 5 อุปกรณ์) ทดสอบปล่อยสัญญาณ @SUT-Wifi ที่อาคารวิจัย
- เปลี่ยน Access point แทนเครื่องเดิมเนื่องจากเครื่องรวนเพราะใช้งานหนักและติดตั้งนอกอาคาร ที่อาคารสุรพัฒน์ 2 จำนวน 1 เครื่อง
- ติดตั้ง Access point ชั่วคราวในงานพระราชทานปริญญาบัตรเพื่อรองรับความต้องการใช้งาน จำนวน 2 เครื่อง
- ตรวจรับการติดตั้งอุปกรณ์กระจายสัญญาณเครือข่าย Access point ที่อัฒจันทร์สนามฟุตบอล จำนวน 6 เครื่อง (อุปกรณ์มากับการก่อสร้างอัฒจันทร์)
- ติดตั้ง Access point เพิ่มที่ส่วนอาคาร(งานประปา) จำนวน 2 เครื่อง

1.3 สรุปการดำเนินการบนระบบ Internet Data Center

- MA storage Netapp FAS3140 (วันที่ 10/11/2559)
- MA storage Netapp FAS3140 (วันที่ 13/10/2559)
- เปลี่ยน harddisk storage Netapp FAS3140 1 unit (วันที่ 32/11/2559)
- ทดสอบการใช้งานระบบ VSAN / ติดตั้งระบบปฏิบัติการ VMware ESXi, 6.5.0 บนเครื่อง VmServer 33,34,35 และ config เพื่อใช้งาน VSAN

1.4 สรุปการดำเนินการบนระบบโทรศัพท์

- ย้ายตำแหน่งอุปกรณ์สำรองระบบโทรศัพท์ Voice Gateway ใหม่ ใช้งานชั่วคราวให้กับส่วนแผนงาน ย้ายมาทำงานที่อาคารเครื่องมือฯ 11 (F11) จำนวน 4 หมายเลข เนื่องจากห้องดังกล่าวไม่มีสายสัญญาณโทรศัพท์
- จัดสรรหมายเลขโทรศัพท์ให้กับอาจารย์และพนักงานที่เข้าใหม่ตามหนังสือแจ้งขอบริการ ดังนี้

เบอร์โทรศัพท์	ผู้ใช้งาน	ตำแหน่งใช้งาน
4741	ดร.สุกฤษฏิ์ สุขสมบัติ	สาขาวิทยาศาสตร์การกีฬา C2-217
4545	ดร.แหวพลอย จินากลูล	สาขาวิชาเทคโนโลยีการผลิตพืช C2-213
3316	นางสาวเพ็นพิสุทธิ์ จันทร์ขมภู	ศูนย์เชี่ยวชาญเฉพาะทางด้านนวัตกรรมเพื่อการพัฒนาโครงสร้างพื้นฐานอย่างยั่งยืน
4532	อ.ปทุมศิริ หุ่นทอง	เทคโนโลยีสังคม
3516	อ.ดร.วรรณวดี เนี่ยมสกุล	สาขาวิชาพยาบาลครอบครัวและการผดุงครรภ์ สำนักพยาบาลศาสตร์
5036	นางลำไพร ศรีธรรมมา	สังกัดฟาร์ม มทส. สำนักวิชาเทคโนโลยีการเกษตร
4695	ดร.สำราญ สันทาลุนัย	สาขาวิศวกรรมอิเล็กทรอนิกส์
4789	อ.ดร.มัณฑนา แจ่มกลาง	สาขาวิชาปรีคลีนิก
4721	อ.ดร.อรุณศรี นุชิตประสิทธิชัย	สาขาวิศวกรรมเคมี
4357	อ.จุฬาภรณ์ บัวขาว	สาขาวิชาศึกษาทั่วไป
4356	นางสาวนวิยา คำสระแก้ว	สาขาบูรณาการเทคโนโลยีการเกษตร
3396	นางปัญญา เกตุใหม่	งานตรวจติดตามการใช้เครื่องมือวัสดุและสนับสนุน
3296	รปภ. F11	F11
4853	นายอาทิตย์ อุดมชัย	ศูนย์เชี่ยวชาญเฉพาะทางด้านนวัตกรรมเพื่อการพัฒนาโครงสร้างพื้นฐานอย่างยั่งยืน
4834	นายอาทิตย์ อุดมชัย	ศูนย์เชี่ยวชาญเฉพาะทางด้านนวัตกรรมเพื่อการพัฒนาโครงสร้างพื้นฐานอย่างยั่งยืน
6020	ห้องเรียน F111-1 , ห้องเรียน F111-2 F 11	
6021	ห้องปฏิบัติการวิเคราะห์นา (Water Analysis Laboratory) F11205A	
6022	ห้องปฏิบัติการวิเคราะห์ไนโตรเจน (Total Kjeldahl Nitrogen (TKN) Analysis Laboratory) F11203A	
6023	ห้องเตรียมตัวอย่าง (Sample Preparation Room) F11204A	
6024	ห้องปฏิบัติการกล้องจุลทรรศน์เทคนิคฟลูออเรสเซ็นต์ (Fluorescence Microscope Laboratory) F11218A	
6025	ห้องปฏิบัติการจาแนกเชื อจุลินทรีย์ด้วยเทคนิคทางโมเลกุล (Microorganisms Identification by Molecular Biology Laboratory) F11216A	
6026	ห้องปฏิบัติการวิเคราะห์คุณภาพนมและผลิตภัณฑ์ (Milk and Dairy Product Analysis Laboratory) F11219A	

6027	ห้องปฏิบัติการวัดความหนืด (Viscosity Laboratory) F11220A
6028	ห้องปฏิบัติการวิเคราะห์ไนโตรเจน ไขมันและเยื่อใย (Nitrogen-Fat and Fiber Analysis Laboratory) F11221A
6029	ห้องปฏิบัติการเตรียมตัวอย่าง (Sample Preparation Laboratory) F11222A
6030	ห้องปฏิบัติการวิเคราะห์เชิงความร้อน (Thermal Analysis Laboratory) F11223A
6031	ห้องปฏิบัติการเตรียมปฏิกิริยาและตัวอย่างทางพันธุกรรม (Preparation and Reaction of Molecular biology Laboratory)F11231A

- แก้ไขปัญหาหัวเครื่องโทรศัพท์และสายสัญญาณที่ชำรุดตามใบงานแจ้งซ่อม

1.5การดำเนินการอื่นๆ

- จัดสรร internet account แก่โครงการโอลิมปิกวิชาการค่าย 1 ระหว่างวันที่ 10 - 21 ตุลาคม 2559
- จัดสรร internet account สำหรับคณะกรรมการประเมินฯ ระดับสถาบัน ระหว่างวันที่ 18-21 ต.ค. 59 โดยส่วนส่งเสริมวิชาการ
- จัดสรร internet account สำหรับนักศึกษาแลกปลี่ยนและอาจารย์จากมหาวิทยาลัยมิชิแกน 12 ท่าน โดยสำนักวิชาพยาบาลศาสตร์
- จัดสรร internet account สำหรับงานจัดแสดงและจำหน่ายหนังสือ (sut book fair 2016) โดยศูนย์บรรณสาร
- จัดสรร internet account สำหรับงานอบรม logistic หน่วยงานเทคโนธานี 150 account สำหรับใช้งานวันที่ 24-26 พย.59
- จัดสรรinternet account สำหรับงานประชุมวิชาการเทคโนโลยีกริด หน่วยงานเทคโนธานี 30 account สำหรับใช้งานวันที่ 30 พ.ย.- 2 ธ.ค .59
- จัดสรร internet account สำหรับงาน SUT IP & Innovation week หน่วยงานเทคโนธานี 553 account สำหรับใช้งานวันที่ 18-22 ธ.ค .59
- จัดสร้างตัววัด throughput web server โดยใช้ awstats

  http://www.sut.ac.th -> รันโปรแกรม **weblog expert** ที่หน้าจอ **desktop**

  http://its.sut.ac.th/awstats/awstats.pl

  http://student.sut.ac.th/awstats/awstats.pl

  http://202.28.42.25/awstats/awstats.pl?config=web.sut.ac.th

  http://202.28.42.26/awstats/awstats.pl?config=web.sut.ac.th

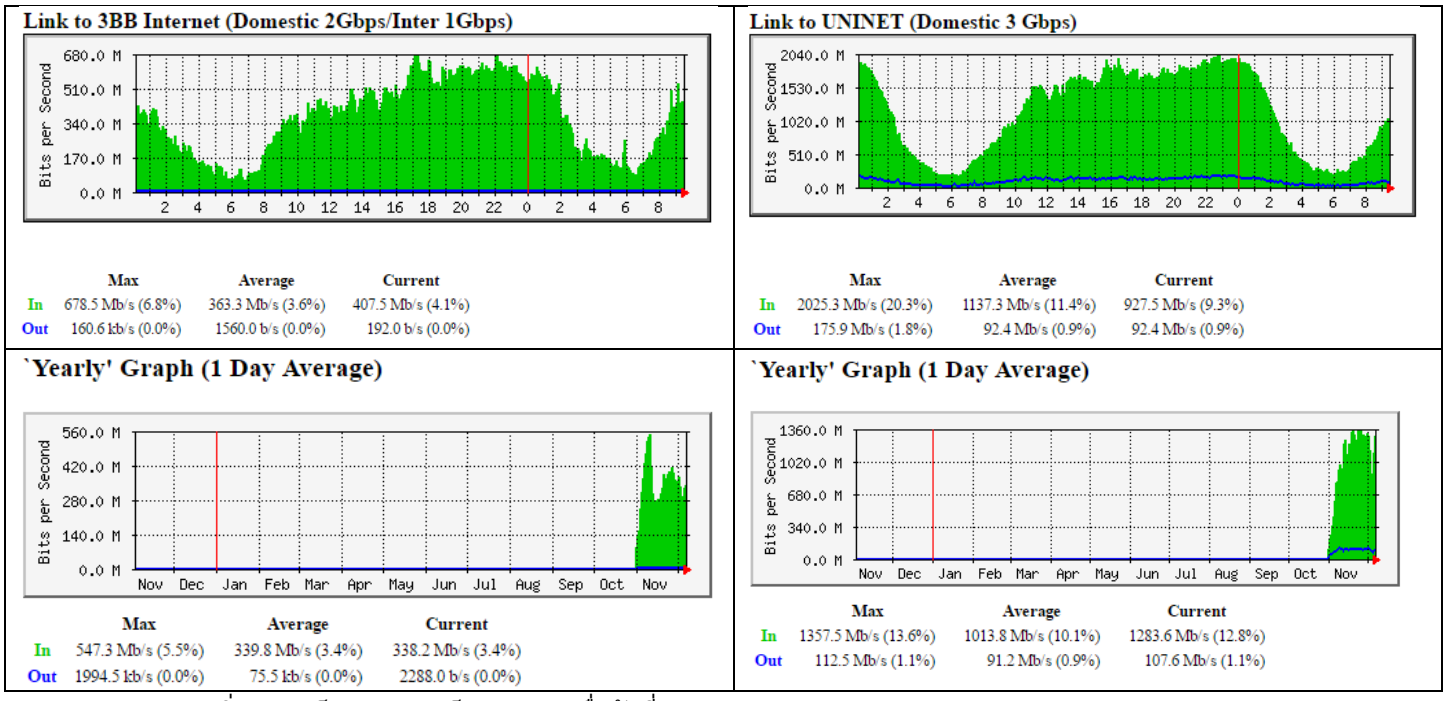
  http://202.28.42.27/awstats/awstats.pl?config=web.sut.ac.th

http://202.28.42.28/awstats/awstats.pl?config=web.sut.ac.th

- แจ้งเตือนเว็บไซต์ http://smart.sut.ac.th/inaudit/rbc/index.html โดน hack
- ตรวจพบการ hack เว็บไซต์ cia โดยมีสคริปฝังในเทมเพลต joomla ที่เปิด permission 777
- แจ้งเตือนเว็บไซต์ http://if.sut.ac.th โดน hack ถูกนำไฟล์แปลกปลอมเข้ามาวางใน server ในเบื้องต้น ได้ทำการลบไฟล์แปลกปลอมออกจาก Server และกำหนด Permission ใหม่
- จัดสรร domain http://reg-sws.sut.ac.th แก่ web server โรงเรียนสุรวิวัฒน์
- ตรวจพบการ hack email account ของบุคลากรโรงพยาบาลมทส. เนื่องจากมีการใช้รูปแบบ password แบบเดียวกัน จึงแจ้งเตือนเจ้าหน้าที่ IT โรงพยาบาลมทส.
- จัดสรรพื้นที่เว็บไซต์แก่งานกิจกรรมนักศึกษา เว็บไซต์ http://studentactivity.sut.ac.th
- จัดสรรพื้นที่เว็บไซต์แก่งานสัมนาวิชาการ http://icce2017.sut.ac.th/
- จัดสรรพื้นที่เว็บไซต์แก่หน่วยงานวิศวกรรมโยธา http://ceport.sut.ac.th
- จัดสรรพื้นที่เว็บไซต์แก่สำนักงานทรัพยืสินทางปัญญาและถ่ายทอดเทคโนโลยี http://tlo.sut.ac.th
- เพิ่มสมาชิกเว็บ vpn แก่สถาบันวิจัยแสงซินโครตรอน โดยปัจุบันมีสมาชิก 111 คน
- แก้ไขปัญหาเว็บไซต์ #kws=2shuvrqdovxwldf1wk2vxgmw โดยยิงสคริปโฆษณา โดยปิดการทำงานส่วน webboard
- จัดสรร virtual server : search.sut.ac.th ระบบปฏิบัติการ : windows 2008 r2 enterprise (64 bit) ram : 8Gb สำหรับศูนย์บรรณสาร
- ดำเนินการขอใบรับรอง certificates แก่ server : search.sut.ac.th

2.รายงานการใช้งานระบบเครือข่าย

Internet Gateway Traffic



*Uninet เพิ่มความเร็ว internet เป็น 3Gbps เมื่อวันที่ 31 ตุลาคม 2559

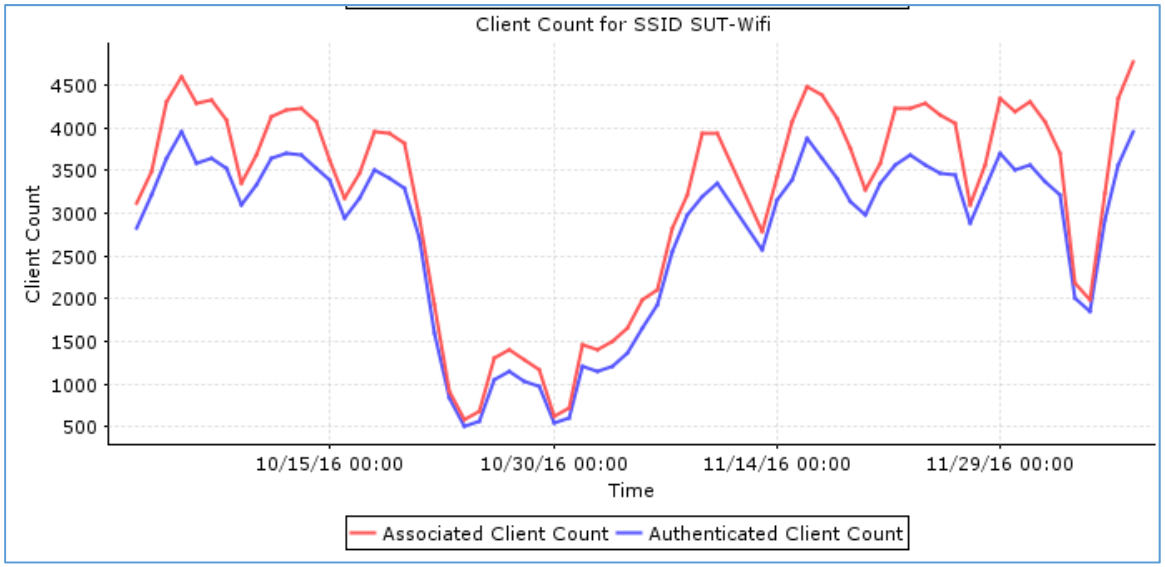
*เปลี่ยนผู้ให้บริการ internet Service Provider เป็น 3BB เมื่อวันที่ 1 ตุลาคม 2559 (ที่ความเร็วเท่าเดิม Domestic 2 Gbps/Inter 1 Gbps)

2.1 รายงานจำนวนผู้ใช้งานผ่านระบบเครือข่าย (LAN) (ไม่รวมห้องปฏิบัติการ)

วิธีการ	จำนวน
วิธีการแบบ 802.1x	1,162 คน
วิธีการแบบ NAC In-Band	149 คน
วิธีการแบบ NAC Out-Band	199 คน
รวมทั้งหมด	**1,510 คน**

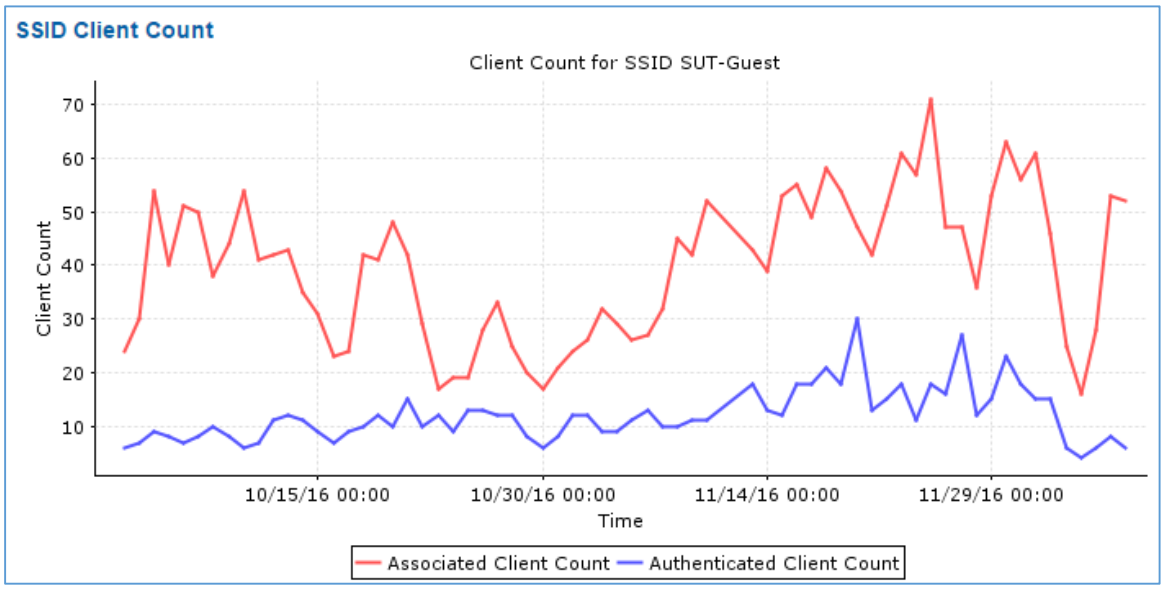
2.2 รายงานจำนวนผู้ใช้งานผ่านระบบเครือข่ายไร้สาย

SUT-Wifi Usage



SUT-AIS Wifi Usage

SUT-Guest Wifi Usage

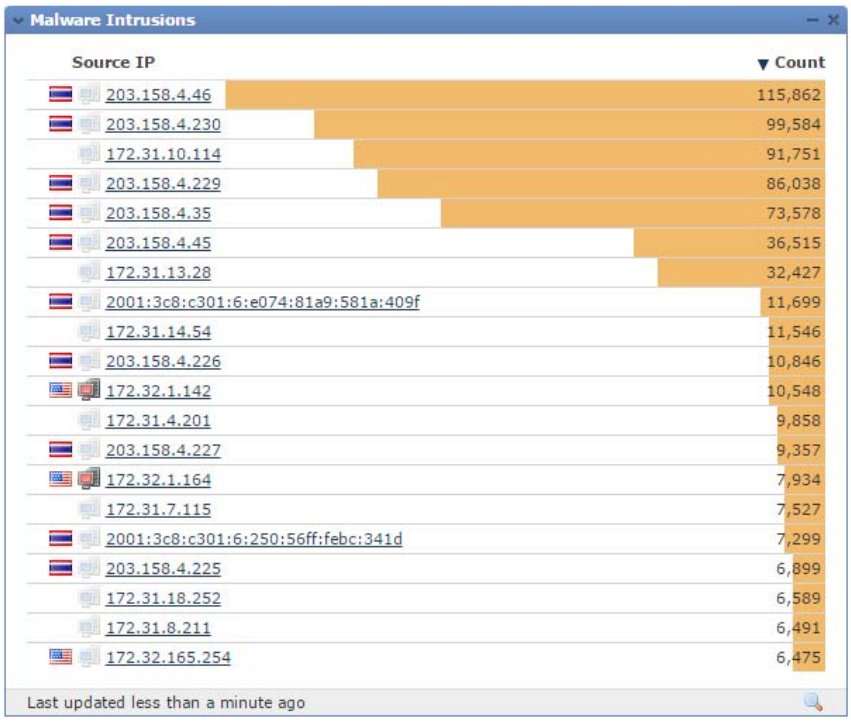


ข้อมูล 3 เดือนย้อนหลัง (1ต.ค.-8 ธ.ค.59) ที่มา 203.158.4.210 / 203.158.4.211

- ผู้ใช้งานผ่านระบบ wireless สูงสุด 7,005 คน/วัน
- ผู้ใช้งานผ่านระบบ wireless ต่ำสุด 752 คน/วัน
- ผู้ใช้งานผ่านระบบ wireless เฉลี่ย 4,801 คน/วัน

3. ภัยคุกคามระบบเครือข่าย

- **สถานะการณ์ไวรัสและมัลแวร์ที่แพร่ระบาดในมหาวิทยาลัย**



Malware Intrusions

Source IP	Count
203.158.4.46	115,862
203.158.4.230	99,584
172.31.10.114	91,751
203.158.4.229	86,038
203.158.4.35	73,578
203.158.4.45	36,515
172.31.13.28	32,427
2001:3c8:c301:6:e074:81a9:581a:409f	11,699
172.31.14.54	11,546
203.158.4.226	10,846
172.32.1.142	10,548
172.31.4.201	9,858
203.158.4.227	9,357
172.32.1.164	7,934
172.31.7.115	7,527
2001:3c8:c301:6:250:56ff:febc:341d	7,299
203.158.4.225	6,899
172.31.18.252	6,589
172.31.8.211	6,491
172.32.165.254	6,475

Last updated less than a minute ago

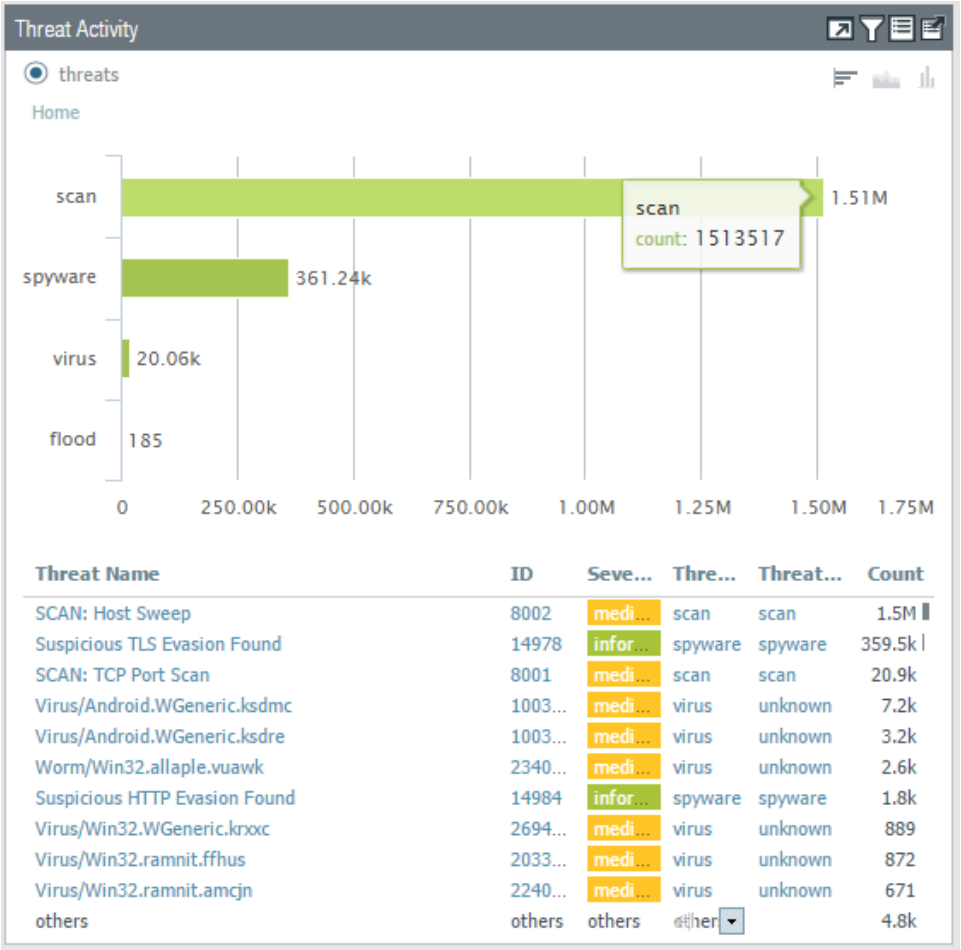
- การยับยั้งการโจมตีบนระบบเครือข่าย โดย อุปกรณ์ IPS

Dropped Intrusion Events

Classification	Count
A Network Trojan was Detected	1,039,816
Attempted Administrator Privilege Gain	4,967
Misc Activity	4,486
Web Application Attack	2,888
Attempted Information Leak	2,022
Attempted User Privilege Gain	770
Potential Corporate Policy Violation	330

Last updated 1 minute ago

- การยับยั้งการโจมตีบนระบบเครือข่าย โดย อุปกรณ์ Firewall



Threat Name	ID	Seve...	Thre...	Threat...	Count
SCAN: Host Sweep	8002	medi...	scan	scan	1.5M
Suspicious TLS Evasion Found	14978	infor...	spyware	spyware	359.5k
SCAN: TCP Port Scan	8001	medi...	scan	scan	20.9k
Virus/Android.WGeneric.ksdmc	1003...	medi...	virus	unknown	7.2k
Virus/Android.WGeneric.ksdre	1003...	medi...	virus	unknown	3.2k
Worm/Win32.allaple.vuawk	2340...	medi...	virus	unknown	2.6k
Suspicious HTTP Evasion Found	14984	infor...	spyware	spyware	1.8k
Virus/Win32.WGeneric.krxxc	2694...	medi...	virus	unknown	889
Virus/Win32.ramnit.ffhus	2033...	medi...	virus	unknown	872
Virus/Win32.ramnit.amcjn	2240...	medi...	virus	unknown	671
others	others	others	other		4.8k