รายงานการใช้งานระบบเครือข่ายคอมพิวเตอร์ มหาวิทยาลัยเทคโนโลยีสุรนารี

1 มิถุนายน – 30 มิถุนายน 2560

1. **<u>รายงานการดำเนินงานของฝ่ายเครือข่าย</u>**

1.1 สรุปการดำเนินการบนระบบเครือข่าย SUTnet

- ไฟดับวันที่ 24 มิถุนายน ตั้งแต่เวลา 7.00-9.00น. ส่งผลให้ระบบปรับอากาศไม่ทำงาน ทำให้อุณหภูมิสูงขึ้น จนทำให้ เครื่องคอมพิวเตอร์แม่ข่าย shutdown ตัวเอง ซึ่งมีอุปกรณ์เสียดังนี้
  - Harddisk net app เสีย 1 ลูก (300Gb)
  - เครื่องคอมพิวเตอร์แม่ข่าย vmserver 3 แจ้งสัญลักษณ์ระบบขัดข้อง ตรวจสอบพบ power supply มีปัญหา2ตัว ทำการ replacet ใหม่ จึงสามารถใช้งานได้ปกติ
- ทำการ reboot Firewall เมื่อวันที่ 22 มิถุนายน 60 เวลา 6.00 น. เพื่อ fix bug ทำให้ระบบมีความเสถียรมากขึ้น
- เดินสายระบบ internet-ระบบโทรศัพท์ อาคาร F12
- ซ่อมสาย Fiber Optic ที่เชื่อมระหว่างอาคารสุรสัมนาคาร1-2 เรียบร้อยแล้ว
- ซ่อมสาย Fiber Optic ที่เชื่อมระหว่างอาคาร Post-Harvest – ประมง เรียบร้อยแล้ว

1.2 สรุปการดำเนินการบนระบบเครือข่ายไร้สาย

- ย้ายตำแหน่งอุปกรณ์กระจายสัญญาณ (access point) จากจุดเดิม ศูนย์เครื่องมือ F1 ชั้น1 หน้าห้อง F1122 ไปติดตั้งหน้าห้อง F1107
- ตรวจสอบพบอุปกรณ์กระจายสัญญาณ เสีย 1 จุด ที่สุรสัมนาคาร ชั้น1 ประตูทางเข้า นำอุปกรณ์เปลี่ยนทดแทนเรียบร้อยแล้ว
- ติดตั้งอุปกรณ์กระจายสัญญาณเพิ่มเติม 1 จุด บริเวณสุรสัมนาคาร ชั้น2

1.3 สรุปการดำเนินการบนระบบ Internet Data Center

- Patch firmware vmserver3 (vsan 1) เพื่อให้ระบบมีเสถียรภาพ - แก้ไขปัญหาระบบจัดเก็บข้อมูลชนิด VSAN
- แก้ไขปัญหา vmserver0 (vsan2) ฟ้อง Disk มีปัญหาการจัดเก็บข้อมูล ตรวจสอบพบข้อมูล overload โดยมีการใช้ disk 135% ซึ่งมีโหลดมากเกินไป จึงทำการย้ายข้อมูลออกจาก vsan 2 และ

enter maintainance mode vm0 และ ลบ diskgroup vmserver0 และสร้างใหม่ทำให้ระบบ resync ข้อมูลใหม่ vmserver 0 จึงสามารถใช้งานได้ตามปกติ

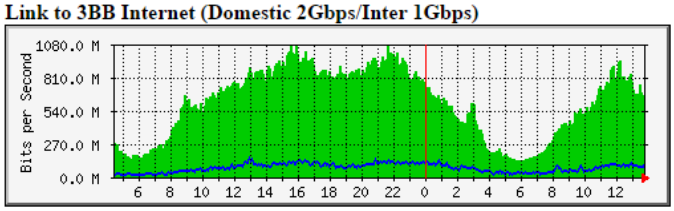
1.4การดำเนินการอื่นๆ

- สร้างระบบ DHCP cluster ประกอบด้วย server 2 ช่วยกันทำงานแบบ load balance
- แก้ไข student.sut.ac.th ทำการยิงเมลล์โฆษณาออกไปภานใน-ภายนอกจำนวนมาก
- สร้างระบบ mysql replication สำหรับฐานข้อมูลระบบ idm.sut.ac.th เพื่อพิ่มเสถียรภาพการใช้งานระบบ
- สร้างระบบ mysql cluster : mysql-web3.sut.ac.th เพื่อรองรับการใช้งานเว็บไซต์ที่มีการใช้งานฐานข้อมูลที่มากขึ้น
- Upgrade ระบบเมลล์มหาวิทยาลัย จากเดิม Exchange 2013 cu7 เป็น cu15 version สูงสุดของ Exchange 2013 เพื่อแก้ไข bug หลายรายการ
- ต้อนรับนักศึกษาดูงานห้อง Intertnet Data Center เมื่อวันที่ 5,9,16 มิถุนายน 2560
- จัดสรร internet account รองรับการประชุมเชิงปฏิบัติการ PANDA Computing Workshop 25 account
- จัดสรร internet account รองรับการอบรมเชิงปฏิบัติการครูผู้สอนเพื่อพัฒนาและส่งเสริมผู้มีความสามารถพิเศษทางวิทยาศาสตร์และเทคโนโลยีแบบห้องเรียนพิเศษ 265 account
- จัดสรร internet account ส่วนส่งเสริมวิชาการสำหรับงานอบรมวิชาการ 25 account
- จัดสรร internet account สำหรับการอบรมระยสั้น ของสำนักวิชาทันตแพทยศาสตร์ 7 account

2.รายงานการใช้งานระบบเครือข่าย

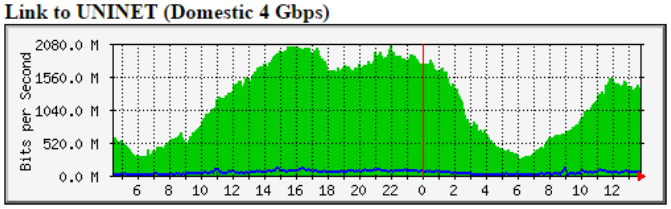
Internet Gateway Traffic

Link to 3BB Internet (Domestic 2Gbps/Inter 1Gbps)



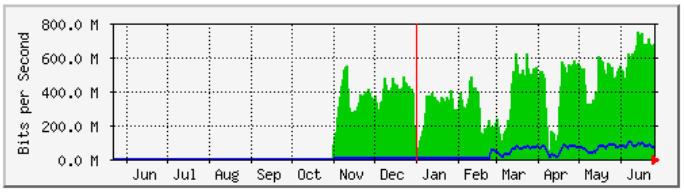
	Max	Average	Current
In	1065.1 Mb/s (10.7%)	602.2 Mb/s (6.0%)	669.0 Mb/s (6.7%)
Out	152.5 Mb/s (1.5%)	73.0 Mb/s (0.7%)	98.9 Mb/s (1.0%)

Link to UNINET (Domestic 4 Gbps)



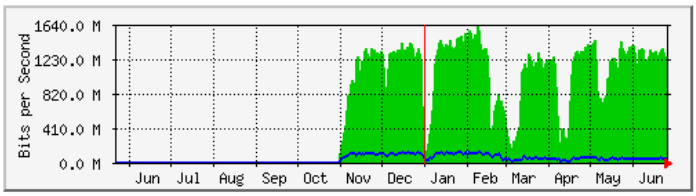
	Max	Average	Current
In	2075.9 Mb/s (20.8%)	1181.7 Mb/s (11.8%)	1424.8 Mb/s (14.2%)
Out	113.9 Mb/s (1.1%)	44.9 Mb/s (0.4%)	44.2 Mb/s (0.4%)

`Yearly' Graph (1 Day Average)



	Max	Average	Current
In	747.7 Mb/s (7.5%)	395.5 Mb/s (4.0%)	676.5 Mb/s (6.8%)
Out	100.6 Mb/s (1.0%)	31.2 Mb/s (0.3%)	66.5 Mb/s (0.7%)

`Yearly' Graph (1 Day Average)



	Max	Average	Current
In	1609.6 Mb/s (16.1%)	1082.5 Mb/s (10.8%)	1261.5 Mb/s (12.6%)
Out	126.6 Mb/s (1.3%)	67.0 Mb/s (0.7%)	40.8 Mb/s (0.4%)

*ทางออก Uninet 4Gbps / 3BB Domestic 2 Gbps,Inter 1 Gbps) / ข้อมูล ณ วันที่ 27 มิ.ย. 60

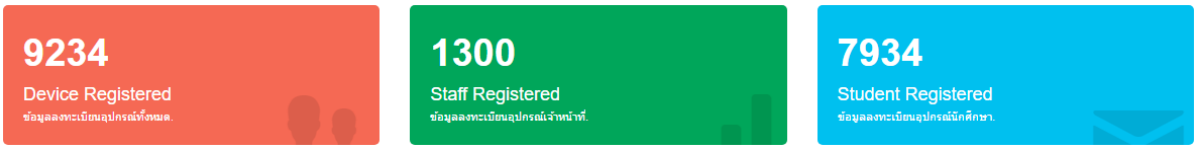
2.1 รายงานจำนวนผู้ใช้งานผ่านระบบเครือข่าย (LAN) (ไม่รวมห้องปฏิบัติการคอมฯ)

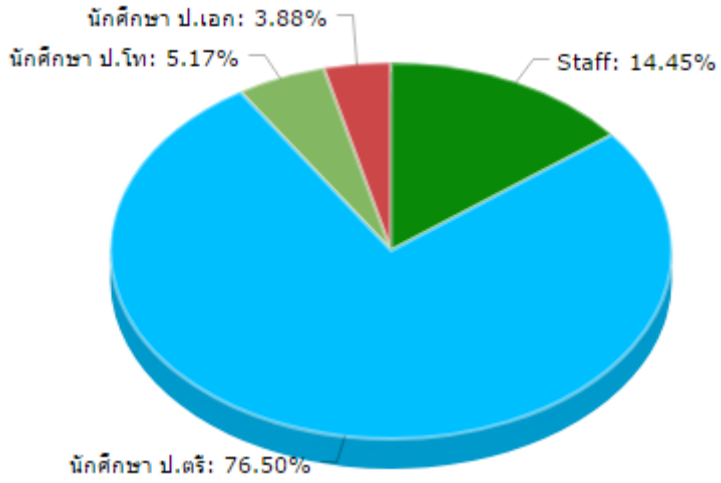
(ข้อมูล ณ วันที่ 27 มิ.ย. 60)

วิธีการ	จำนวน
วิธีการแบบ NAC In-Band	183 คน
วิธีการแบบ ISE	1,524 คน
รวมทั้งหมด	**1,707คน**

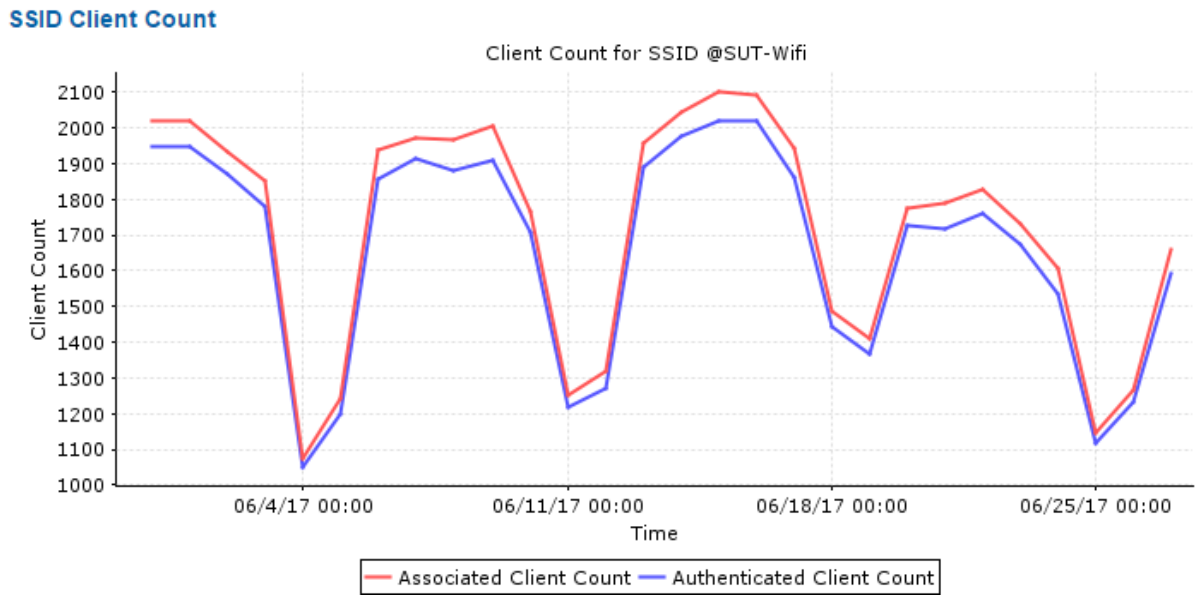
2.2 รายงานจำนวนผู้ใช้งานผ่านระบบเครือข่ายไร้สาย ที่มา https://203.158.4.211 (ข้อมูล 1 เดือนย้อนหลัง)

2.2.1 จำนวนผู้ใช้งานเครือข่ายไร้สาย @SUT-Wifi

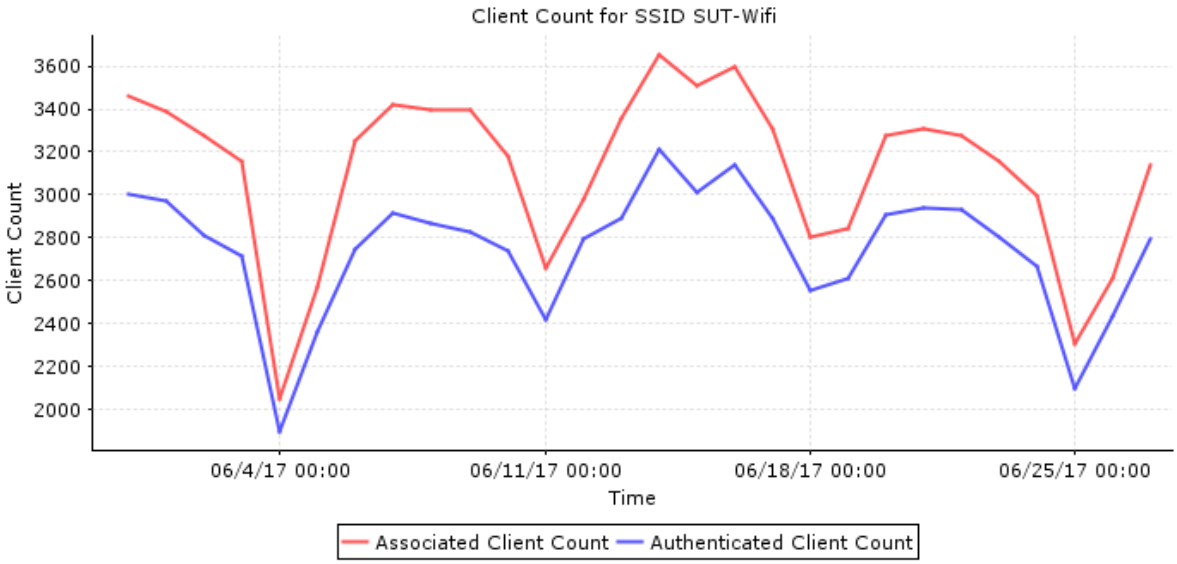




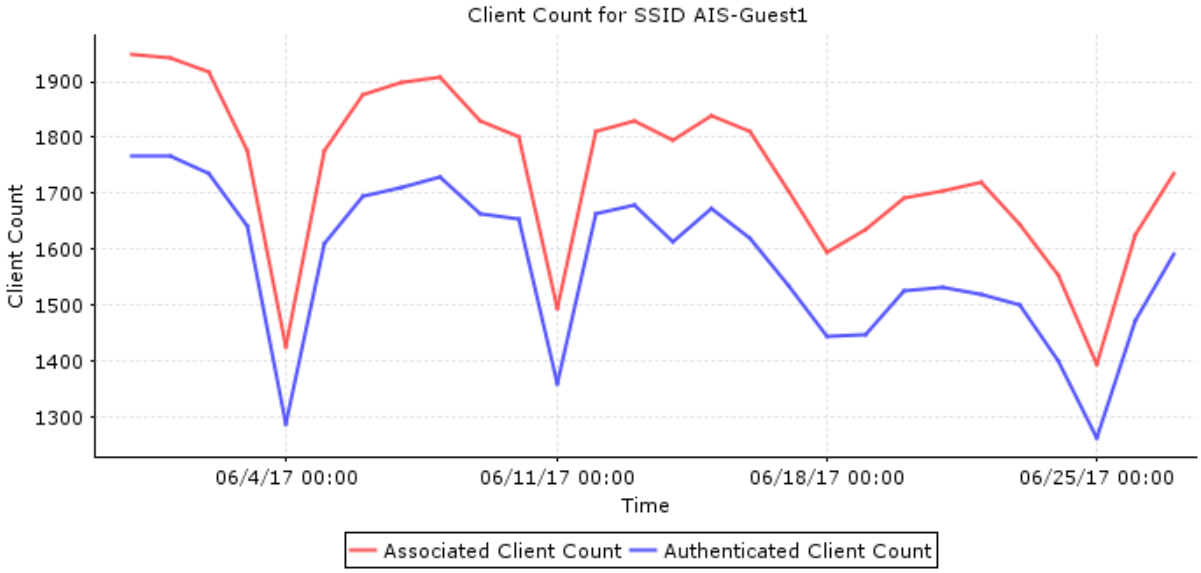
จำนวนผู้ใช้งานเครือข่ายไร้สาย @SUT-Wifi (ที่มา https://203.158.4.211) (ข้อมูล 1 เดือนย้อนหลัง)

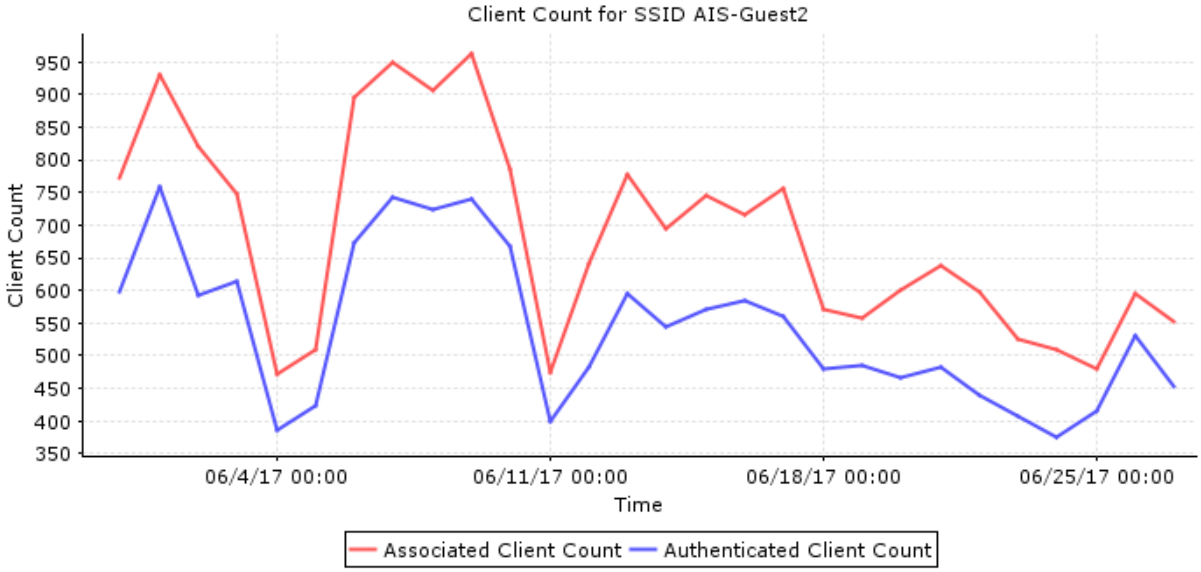


2.2.2 จำนวนผู้ใช้งานเครือข่ายไร้สาย SUT-Wifi

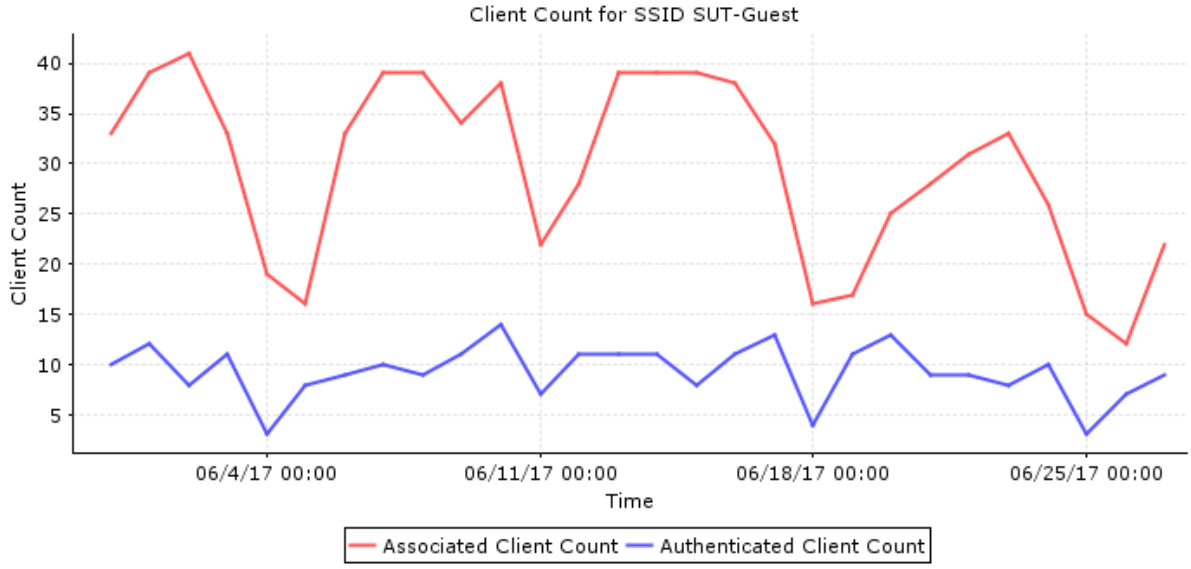


2.2.3 จำนวนผู้ใช้งานเครือข่ายไร้สาย SUT-AIS

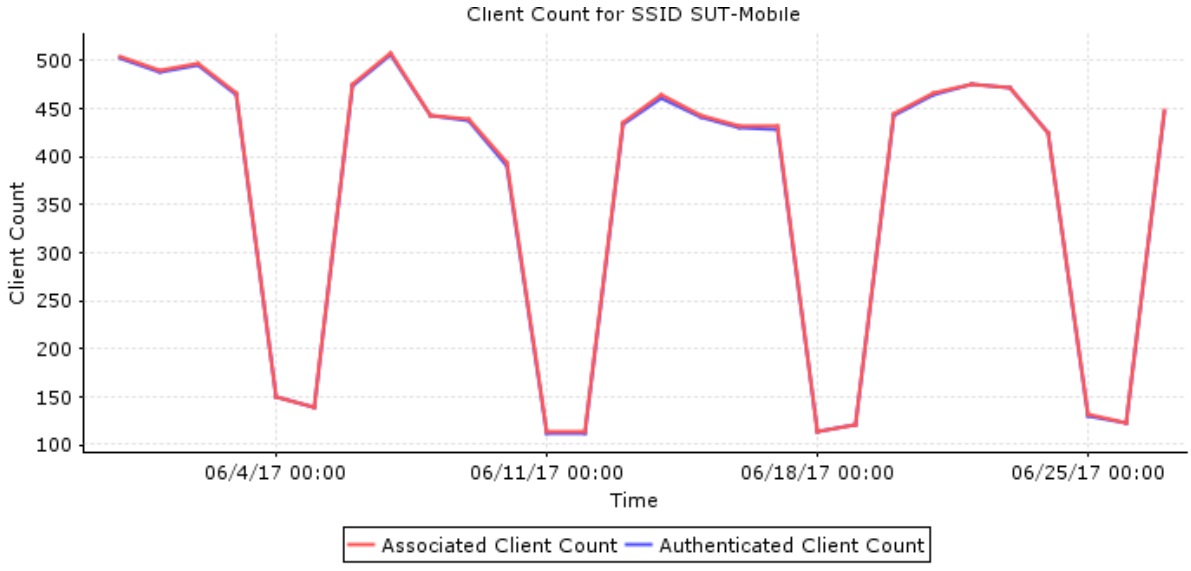




2.2.4 จำนวนผู้ใช้งานเครือข่ายไร้สาย SUT-Guest



2.2.5 จำนวนผู้ใช้งานเครือข่ายไร้สาย SUT-Mobile



2.2.6 สรุปสถิติจำนวนผู้ใช้งานผ่านระบบ wireless ทั้งหมด

- ผู้ใช้งานผ่านระบบ wireless สูงสุด 6,920 คน/วัน
- ผู้ใช้งานผ่านระบบ wireless ต่ำสุด 4,235 คน/วัน
- ผู้ใช้งานผ่านระบบ wireless เฉลี่ย 6,060 คน/วัน

3. ภัยคุกคามระบบเครือข่าย

- **สถานะการณ์ไวรัสและมัลแวร์ที่แพร่ระบาดในมหาวิทยาลัย** (ข้อมูล 1 เดือนย้อนหลัง)

  (ที่มา : Sourcefire 203.158.4.43)

Malware Intrusions

	Message	Count
	MALWARE-CNC Win.Trojan.Zeus variant outbound connection (1:35030:1)	152,077
+3	BLACKLIST suspicious .bit tcp dns query (1:42841:3)	85,910
+1	BLACKLIST suspicious .bit dns query (1:41083:1)	75,603
-2	MALWARE-CNC Win.Trojan.Zeus variant outbound connection (1:35549:1)	69,082
-2	MALWARE-CNC Win.Trojan.Njrat variant outbound connection (1:25100:5)	55,498
	MALWARE-CNC Win.Trojan.Andromeda variant outbound connection (1:33496:1)	40,952
	MALWARE-CNC Win.Trojan.Zeus variant outbound connection (1:35746:1)	32,741
+4	MALWARE-CNC Win.Trojan.Zbot variant in.php outbound connection (1:26023:3)	30,690
-1	MALWARE-CNC Win.Trojan.Pmabot outbound connection (1:37213:3)	19,597
-1	BLACKLIST DNS request for known malware domain rterybrstutnrsbberve.com	19,546
+6	BLACKLIST DNS request for known malware domain ltc.give-me-coins.com (1:31660:1)	19,291
-1	BLACKLIST DNS request for known malware domain erwbtkidthetcwerc.com (1:28058:1)	18,304
-3	BLACKLIST DNS request for known malware domain rvbwtbeitwjeitv.com (1:28060:1)	17,445
-1	BLACKLIST DNS request for known malware domain xa.yessearches.com -	17,135
+4	MALWARE-CNC Win.Trojan.Glupteba.M initial outbound connection (1:30288:2)	6,728
+4	MALWARE-CNC Win.Trojan.Nvbpass variant outbound connection (1:19864:5)	6,694
-2	MALWARE-CNC Torpig bot sinkhole server DNS lookup (1:16693:5)	5,384
-2	MALWARE-CNC Win.Trojan.Jaktinier outbound connection (1:31459:3)	4,904
	MALWARE-CNC Win.Trojan.Gamarue - Mozi1la User-Agent (1:27248:3)	4,260
	BLACKLIST DNS request for known malware domain wisenwizard.net -	3,861

Last updated less than a minute ago

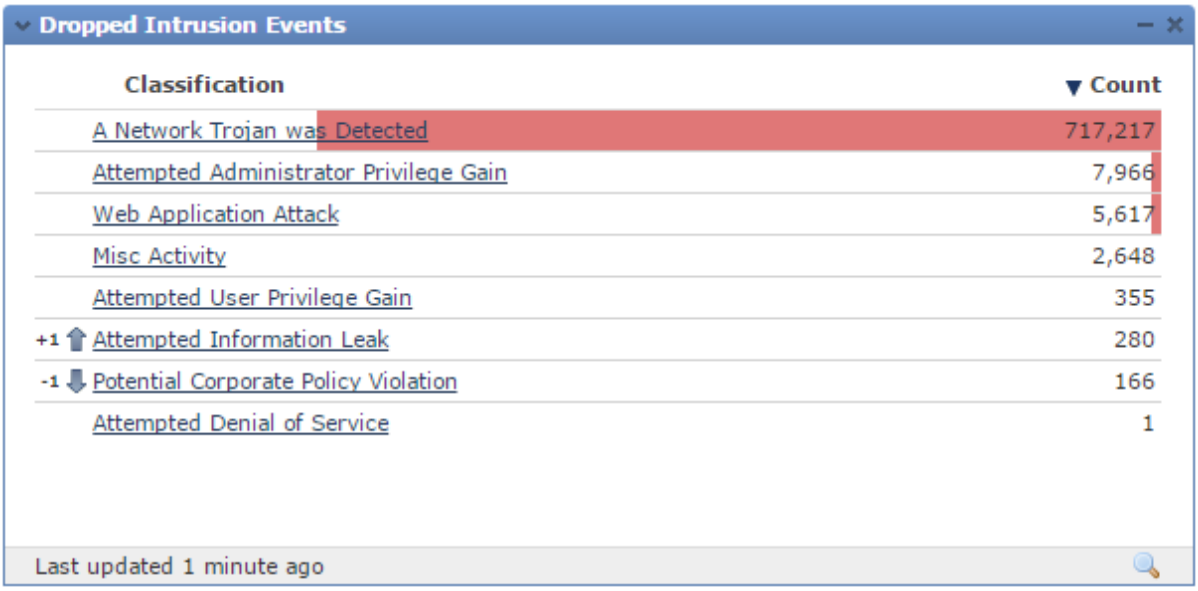
Top Attackers (High Impact Events)

	Source IP	Count
	203.158.4.46	81,588
	203.158.4.45	30,957
+1	203.158.4.229	22,185
+7	172.32.163.230	21,804
+5	2001:3c8:c301:6:250:56ff:febc:341d	18,679
	203.158.4.230	17,902
	203.158.4.225	15,290
	10.0.139.112	13,840
	172.30.1.69	13,657
-5	172.106.11.10	12,943
-8	172.31.26.156	12,912
-3	192.168.29.10	11,984
	172.31.16.88	11,221
	172.32.179.152	10,243
	172.31.8.93	10,062
+7	192.168.144.71	9,756
	172.31.16.152	9,248
+3	172.32.167.190	7,897
-3	172.32.68.197	7,884
+5	172.31.14.28	7,733

Last updated less than a minute ago

- **การยับยั้งการโจมตีบนระบบเครือข่าย โดย อุปกรณ์ IPS** (ข้อมูล 1 เดือนย้อนหลัง)

  (ที่มา : Sourcefire 203.158.4.43)



- **การยับยั้งการโจมตีบนระบบเครือข่าย โดย อุปกรณ์ Firewall** (ข้อมูล 1 เดือนย้อนหลัง)

  (ที่มา Paloalto:203.158.4.110)