รายงานการใช้งาน ระบบเครือข่ายคอมพิวเตอร์ ประจาเดือน เมษายน 2569

ฝ่ายโครงสร้างพื้นฐานและระบบเครือข่าย

รายงานจานวนผู้ใช้งานผ่านระบบเครือข่าย (LAN) (ไม่รวมห้องปฏิบัติการคอมฯ)

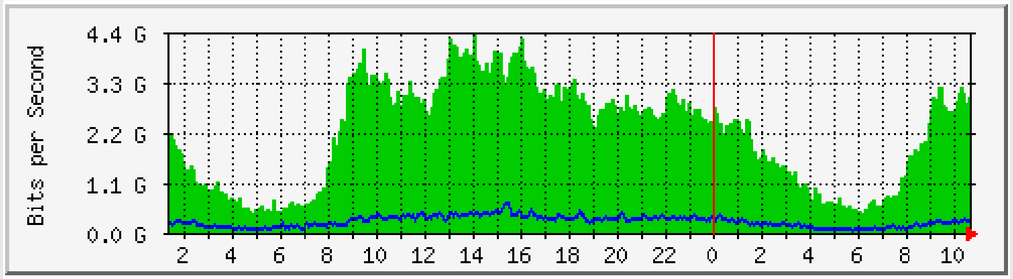
วิธีการ	จานวน
วิธีการแบบ ISE (802.1x)	298 คน

ที่มา https://203.158.4.207

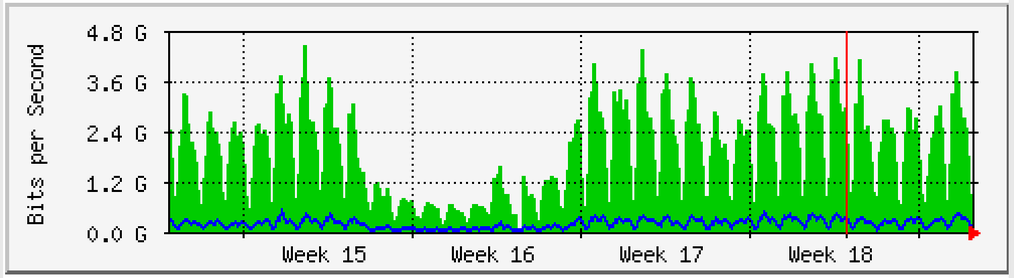
รายงานการใช้งานระบบเครือข่าย

Internet Gateway Traffic

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

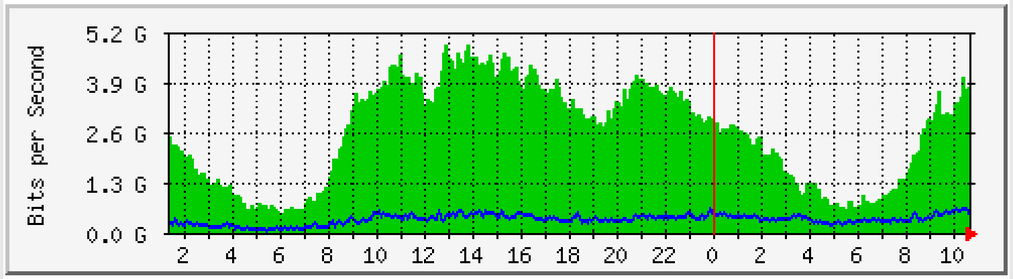


	Max	Average	Current
In	4353.2 Mb/s (43.5%)	2135.5 Mb/s (21.4%)	3078.6 Mb/s (30.8%)
Out	636.4 Mb/s (6.4%)	228.9 Mb/s (2.3%)	235.8 Mb/s (2.4%)

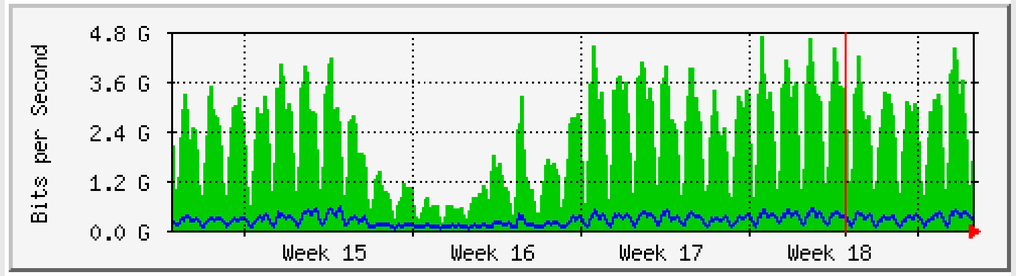


	Max	Average	Current
In	4431.2 Mb/s (44.3%)	1773.2 Mb/s (17.7%)	552.9 Mb/s (5.5%)
Out	505.9 Mb/s (5.1%)	175.8 Mb/s (1.8%)	60.2 Mb/s (0.6%)

Link to UNINET (Domestic 10Gbps)



	Max	Average	Current
In	4861.3 Mb/s (48.6%)	2537.8 Mb/s (25.4%)	3683.1 Mb/s (36.8%)
Out	611.7 Mb/s (6.1%)	322.7 Mb/s (3.2%)	478.2 Mb/s (4.8%)

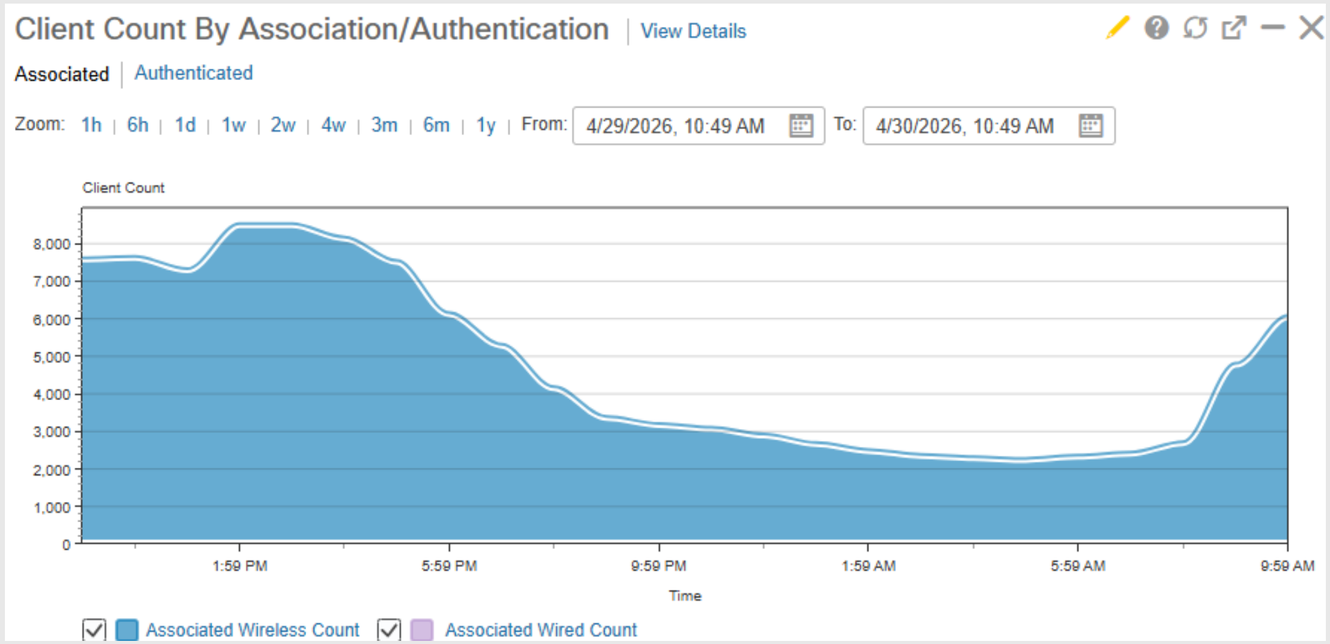


	Max	Average	Current
In	4676.4 Mb/s (46.8%)	2044.0 Mb/s (20.4%)	1677.0 Mb/s (16.8%)
Out	540.8 Mb/s (5.4%)	223.5 Mb/s (2.2%)	324.4 Mb/s (3.2%)

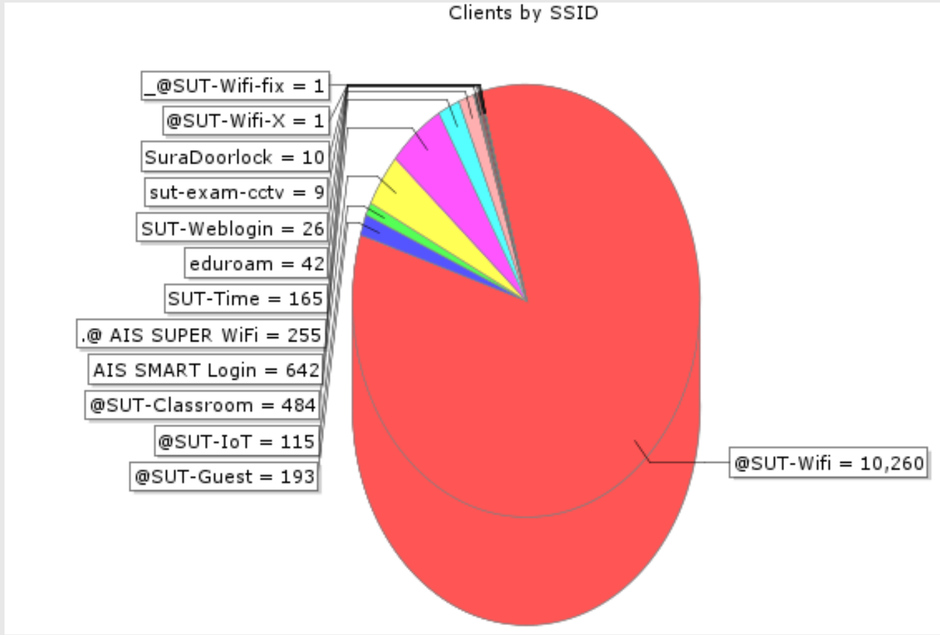
รายงานจานวนผู้ใช้งานผ่านระบบเครือข่ายไร้สาย

สรุปสถิติจานวนผู้ใช้งานผ่านระบบ Wirless ทั้งหมด

สรุปปริมาณผู้ใช้งานต่อวัน



แบ่งตาม SSID สถิติย้อนหลัง 1 เดือน



- ผู้ใช้งานผ่านระบบ wireless สูงสุด 8,532 คน/วัน
- ผู้ใช้งานผ่านระบบ wireless, ต่าสุด 2,281 คน/วัน
- ผู้ใช้งานผ่านระบบ wireless เฉลี่ย 4,767 คน/วัน

สรุปการดาเนินการบนระบบเครือข่ายคอมพิวเตอร์

หัวข้อ	จานวน (งาน)
ซ่อมแซมอุปกรณ์ Network (ผลกระทบในระดับอาคาร)	2
งานสารวจหน้างาน ประมาณราคาการจัดจ้าง ขยาย/ปรับปรุง/ซ่อมแซม/บารุงรักษาระบบ	13
การ Monitor/Standby ระบบ Network	100
ติดตั้ง/ซ่อมแซม สายสัญญาณ Network	22
งานให้คาแนะนาปรึกษาแก่ผู้ใช้บริการ	4

สรุปการดาเนินการบนระบบ INTERNET DATA CENTER

หัวข้อ	จานวน (งาน)
ติดตั้งอุปกรณ์ Data Center (ผลกระทบในระดับมหาวิทยาลัย)	-
บริหารจัดการระบบ Data Center	2
บริหารจัดการระบบ Network และ Security	13
จัดสรร VS/VM, Web	9
การ Monitor/Standby ระบบ Data Center	-
บริหารจัดการ Email Account / บริหารจัดการ Wifi Account / บริหารจัดการ G.dot Account	33
ตรวจสอบ/ปรับปรุงแก้ไข ด้านความปลอดภัยระบบสารสนเทศ	1

สรุปการดาเนินการบนระบบโทรคมนาคม

หัวข้อ	จานวน (งาน)
แก้ไขอุปกรณ์ Telephone (ผลกระทบในระดับอาคาร)	1
การ Monitor/Standby ระบบ Telephone	-
ติดตั้ง/ซ่อมแซม สายสัญญาณ Telephone	20
กากับดูแลการติดตั้ง เกบคืน อุปกรณ์/ครุภัณฑ์ และเอกสารประกอบที่เกี่ยวข้องให้ถูกต้องแล้วเสรจภายในเวลาที่กาหนด	4

สรุปการดาเนินการด้านอื่น ๆ

หัวข้อ	จานวน (งาน)
เข้าร่วมประชุม/เข้าร่วมกิจกรรมต่างๆของมหาวิทยาลัย	4
จัดทาเอกสารใบขอให้จัดซื้อ จัดจ้าง รวบรวมรายละเอียดต่าง ๆ ได้ถูกต้องครบถ้วน และบริหารจัดการส่งให้ส่วนพัสดุได้ทันตามกาหนด	1
คณะกรรมการจัดซื้อ/จัดจ้าง/ตรวจรับ/ร่างกาหนดคุณสมบัติ (TOR) วงเงินงบประมาณตั้งแต่ 100,001 - 499,999 บาท (งานจัดซื้อจัดจ้าง)	3
จัดทาเอกสารการจัดซื้อจัดจ้างตามแบบฟอร์มของพัสดุ	-
สรุปรายงานผลการดาเนินงานของหน่วยงานประจาเดือน/ประจาไตรมาส และรายงานต่อคณะกรรมการของมหาวิทยาลัย หรือระบบออนไลน์	4
ร่างหนังสือแบบฟอร์มพื้นฐานทั่วไป	2

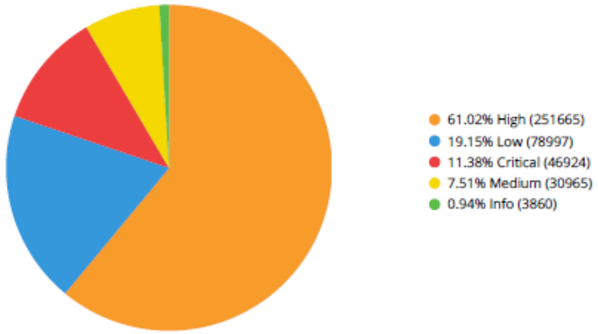
ภัยคุกคามระบบเครือข่าย

การยับยั้งการโจมตีบนระบบเครือข่าย โดยอุปกรณ์ Next Gen Firewall : Fortinet

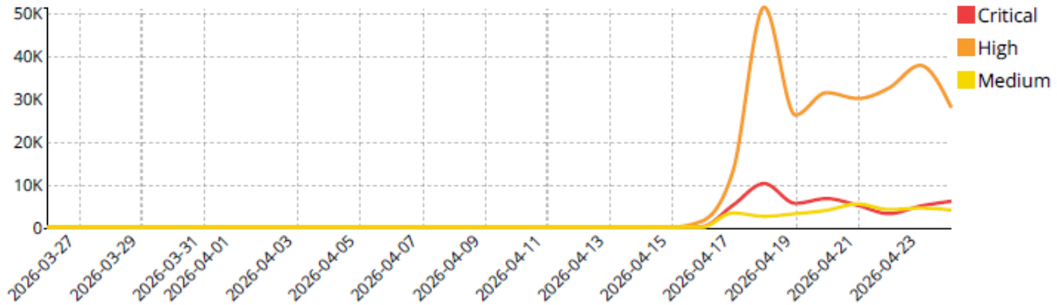
SUT Gatway of IPS Report

Summary

Intrusions By Severity



Critical High and Medium Intrusions Timeline



Intrusions By Types

#	Intrusion Type	Counts
1	Anomaly	95,798
2	Permission/Privilege/Access Control	42,487
3	Path Traversal	39,352
4	OS Command Injection	38,243
5	SQL Injection	30,322
6	Code Injection	22,287
7	Other	16,343
8	Malware	7,035
9	DoS	2,357
10	Improper Authentication	983
11	XSS	490
12	Information Disclosure	462
13	Buffer Errors	298
14	Resource Management Errors	10
15	CSRF	2

การยับยั้งการโจมตีบนระบบเครือข่าย โดยอุปกรณ์ Next Gen Firewall : Fortinet

SUT Gatway of IPS Report

Intrusion Victims

#	Attack Victim	Counts	Critical	High	Medium	Percent of Total Attacks
1	172.67.161.65				15,860	11.88%
2	172.67.175.87				15,853	11.88%
3	172.67.199.217				15,853	11.88%
4	117.18.127.179				14,172	10.62%
5	172.67.157.210				13,786	10.33%
6	203.158.3.42				11,838	8.87%
7	202.28.42.36				6,485	4.86%
8	203.158.5.129				5,943	4.45%
9	203.158.7.48				5,454	4.09%
10	203.158.7.63				5,418	4.06%
11	203.158.7.180				3,169	2.37%
12	23.197.202.166				2,758	2.07%
13	172.234.199.15				2,533	1.90%
14	203.158.3.112				2,202	1.65%
15	104.26.9.74				2,158	1.62%
16	172.67.75.242				2,100	1.57%
17	44.244.22.128				2,048	1.53%
18	172.237.145.27				2,042	1.53%
19	203.158.3.131				1,914	1.43%
20	203.158.3.129				1,883	1.41%

Intrusion Sources

#	Attack Source	Counts	Critical	High	Medium	Percent of Total Attacks
1	203.158.7.23				63,444	29.30%
2	79.124.40.174				38,341	17.71%
3	45.205.1.20				21,193	9.79%
4	10.0.187.99				11,195	5.17%
5	10.1.143.32				9,698	4.48%
6	193.32.162.28				8,378	3.87%
7	165.245.176.249				6,537	3.02%
8	10.15.0.164				5,928	2.74%
9	152.42.208.87				5,907	2.73%
10	5.61.209.107				5,712	2.64%
11	159.223.94.178				5,438	2.51%
12	10.1.173.157				4,487	2.07%
13	10.0.214.70				4,063	1.88%
14	51.79.128.217				4,005	1.85%
15	45.32.116.140				3,969	1.83%
16	109.104.155.28				3,910	1.81%
17	92.118.205.122				3,817	1.76%
18	185.237.185.6				3,812	1.76%
19	209.97.171.198				3,598	1.66%
20	185.186.78.170				3,087	1.43%

การยับยั้งการโจมตีบนระบบเครือข่าย โดยอุปกรณ์ Next Gen Firewall : Fortinet

Intrusions Blocked

SUT Gatway of IPS Report

#	Intrusion Name	Intrusion Type	Severity	Counts
1	PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	Code Injection	Critical	16,407
2	Hikvision.Products.SDK.WebLanguage.Tag.Command.Injection	OS Command Injection	Critical	5,735
3	D-Link.Realtek.SDK.Miniigd.UPnP.SOAP.Command.Execution	OS Command Injection	Critical	5,391
4	D-Link.DSL-2750B.CLI.OS.Command.Injection	OS Command Injection	Critical	2,336
5	NETGEAR.DGN1000.CGI.Unauthenticated.Remote.Code.Execution	Code Injection	Critical	2,045
6	D-Link.Devices.HNAP.SOAPAction-Header.Command.Execution	OS Command Injection	Critical	1,945
7	DZS.GPON.Remote.Code.Execution	OS Command Injection	Critical	1,939
8	Amadey.Botnet		Critical	1,524
9	udp_flood	Anomaly	Critical	1,394
10	Apache.Struts.2.DefaultActionMapper.Remote.Command.Execution	Other	Critical	1,195
11	njRAT.Botnet		Critical	1,186
12	PTZOptics.PT30X.param.Authentication.Bypass	Improper Authentication	Critical	798
13	Babar		Critical	798
14	Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution	Code Injection	Critical	590
15	Java.Debug.Wire.Protocol.Insecure.Configuration	Permission/Privilege/Access Control	Critical	506
16	Spring.Framework.SerializationUtils.Insecure.Deserialization	Permission/Privilege/Access Control	Critical	357
17	ThinkPHP.Controller.Parameter.Remote.Code.Execution	Code Injection	Critical	316
18	Bash.Function.Definitions.Remote.Code.Execution	OS Command Injection	Critical	182
19	F5.BIG-IP.iControl.REST.Authentication.Bypass	Permission/Privilege/Access Control	Critical	158
20	WIFICAM.P2P.GoAhead.Multiple.Remote.Code.Execution	Code Injection	Critical	151

การยับยั้งการโจมตีบนระบบเครือข่าย โดยอุปกรณ์ Next Gen Firewall : Fortinet

SUT Gateway Cyber Threat Assessment

High Risk Applications

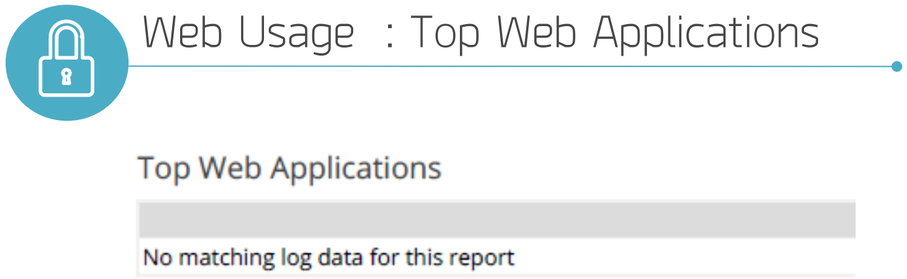
High Risk Applications

No matching log data for this report

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	1,127	32	14,089
5	Hikvision.Products.SDK.WebLanguage.Tag.Command.Injection	OS Command Injection	CVE-2021-36260	18	3	5,020
5	D-Link.Realtek.SDK.Miniigd.UPnP.SOAP.Command.Execution	OS Command Injection	CVE-2014-8361	891	7	1,926
5	D-Link.DSL-2750B.CLI.OS.Command.Injection	OS Command Injection	CVE-2016-20017	805	214	1,495
5	Amadey.Botnet			2	1	1,462
5	NETGEAR.DGN1000.CGI.Unauthenticated.Remote.Code.Execution	Code Injection		794	1,249	1,416
5	D-Link.Devices.HNAP.SOAPAction-Header.Command.Execution	OS Command Injection	CVE-2015-2051,CVE-2019-10891,CVE-2022-37056,CVE-2023-35723,CVE-2024-33112,CVE-2025-63932	793	1,221	1,373
5	DZS.GPON.Remote.Code.Execution	OS Command Injection	CVE-2018-10561,CVE-2018-10562	763	1,184	1,349
5	udp_flood	Anomaly		56	85	1,325
5	njRAT.Botnet			1	1	1,186
5	Apache.Struts.2.DefaultActionMapper.Remote.Command.Execution	Other	CVE-2013-2251	717	2	1,110
5	Babar			1	1	798
5	PTZOptics.PT30X.param.Authentication.Bypass	Improper Authentication	CVE-2024-8956	179	14	622
5	Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution	Code Injection	CVE-2017-5638	484	3	492

การยับยั้งการโจมตีบนระบบเครือข่าย โดยอุปกรณ์ Next Gen Firewall : Fortinet



การยับยั้งการโจมตีบนระบบเครือข่าย โดยอุปกรณ์ Next Gen Firewall : Fortinet สาหรับ REG และ Finance

FIN-REG Security Analysis

Top Applications by Bandwidth

Top Applications by Sessions

Top Applications by Bandwidth

No matching log data for this report

Top Applications by Sessions

No matching log data for this report

การยับยั้งการโจมตีบนระบบเครือข่าย โดยอุปกรณ์ Next Gen Firewall : Fortinet สาหรับ REG และ Finance

FIN-REG Security Analysis

Intrusions Detected

Events by Severity

Intrusions Detected

No matching log data for this report

Events by Severity

No matching log data for this report

การยับยั้งการโจมตีบนระบบเครือข่าย โดยอุปกรณ์ Next Gen Firewall : Fortinet สาหรับ REG และ Finance

FIN-REG Cyber Threat Assessment

Security and Threat Prevention
High Risk Applications

Top Application Vulnerability Exploits Detected

High Risk Applications

No matching log data for this report

Top Application Vulnerability Exploits Detected

No matching log data for this report

การยับยั้งการโจมตีบนระบบเครือข่าย โดยอุปกรณ์ Next Gen Firewall : Fortinet สาหรับ REG และ Finance

FIN-REG Cyber Threat Assessment

Top Web Applications

Top Web Applications

No matching log data for this report