รายงานการใช้งานระบบเครือข่ายคอมพิวเตอร์

โครงสร้างพื้นฐานและระบบเครือข่าย ประจำเดือน ธันวาคม 66

- ระบบเครือข่ายคอมพิวเตอร์
- ระบบ Internet Data Center
- ระบบโทรคมนาคม

สรุปการดำเนินการบนระบบเครือข่ายคอมพิวเตอร์

7 Dec 66	สำรวจระบบเครือข่ายที่อาคารสุรพัฒน์ 2 เพื่อรองรับงานพระราชทานปริญญาบัตร
11-12 Dec 66	ตรวจเช็ค Fiber optic จาก อาคารบริหาร ไป ยังป้าย LED ถนน 304 Fiber optic สามารถใช้งานได้ปกติ
12 Dec 66	UPS อาคารวิชาการ 2 มีปัญหา ทำให้ Switch ชั้น 3, 4 ใช้งานไม่ได้
13 Dec 66	ตรวจสอบสาย UTP สำนักงานหอ 7-8 สำหรับตู้คืนหนังสือ สายเสื่อมตามสภาพใช้งาน แก้ไขเรียบร้อย
18 Dec 66	ดำเนินการติดตั้งอุปกรณ์ระบบเครือข่ายที่อาคารสุรพัฒน์ 2 เพื่อรองรับงานพระราชทานปริญญาบัตร
18 Dec 66	ยูนิเน็ตเข้าตรวจสอบ Fiber Optic ที่ห้อง IDC อาคารวิจัย
22 Dec 66	เนื่องจากไฟตกหลายครั้งทำให้ Switch Core C1-Floor3 เสีย 1 ตัว
23 Dec 66	ทีม Ais แจ้งว่าอุปกรณ์ที่ลานน้ำพุใช้งานไม่ได้ ขอเข้ามาเช็คสายไฟเบอร์

รายงานจำนวนผู้ใช้งานผ่านระบบเครือข่าย (LAN)
(ไม่รวมห้องปฏิบัติการคอมฯ)

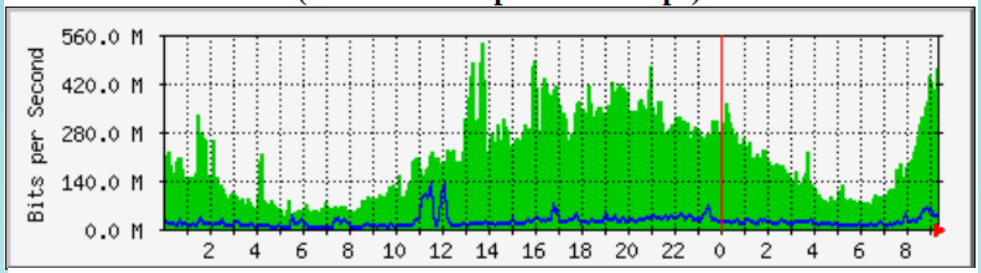
วิธีการ	จำนวน
วิธีการแบบ ISE (802.1x)	1,041 คน

ที่มา (ise) https://203.158.4.207

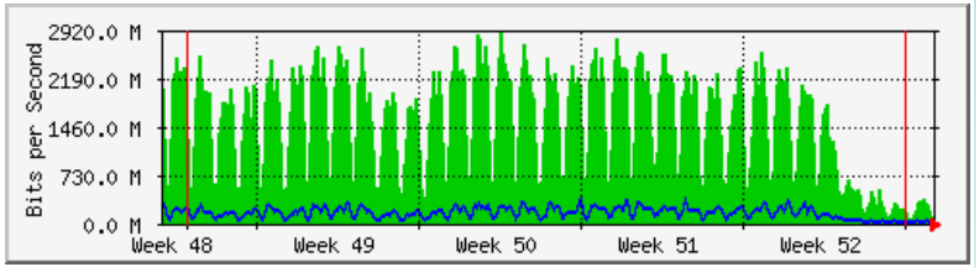
รายงานการใช้งานระบบเครือข่าย

Internet Gateway Traffic

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

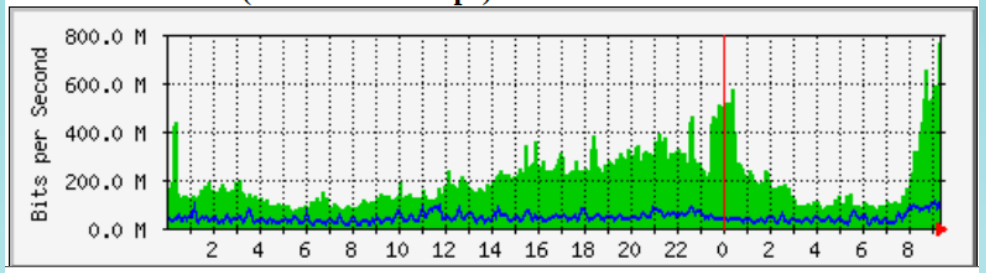


	Max	Average	Current
In	536.4 Mb/s (5.4%)	203.0 Mb/s (2.0%)	460.2 Mb/s (4.6%)
Out	130.3 Mb/s (1.3%)	19.7 Mb/s (0.2%)	43.0 Mb/s (0.4%)

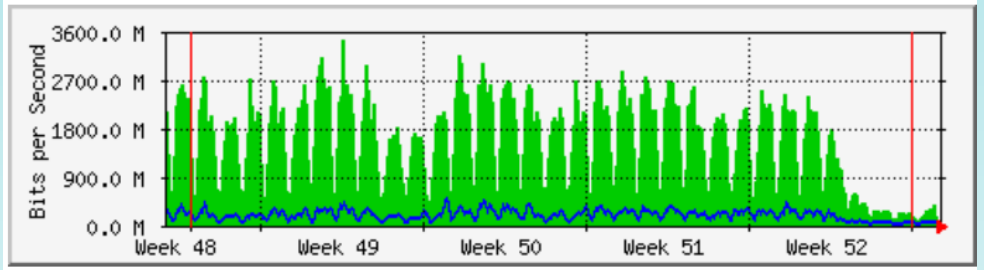


	Max	Average	Current
In	2891.7 Mb/s (28.9%)	1469.7 Mb/s (14.7%)	84.3 Mb/s (0.8%)
Out	368.5 Mb/s (3.7%)	147.7 Mb/s (1.5%)	10.3 Mb/s (0.1%)

Link to UNINET (Domestic 10Gbps)



	Max	Average	Current
In	767.1 Mb/s (7.7%)	194.7 Mb/s (1.9%)	723.3 Mb/s (7.2%)
Out	112.2 Mb/s (1.1%)	40.3 Mb/s (0.4%)	104.8 Mb/s (1.0%)

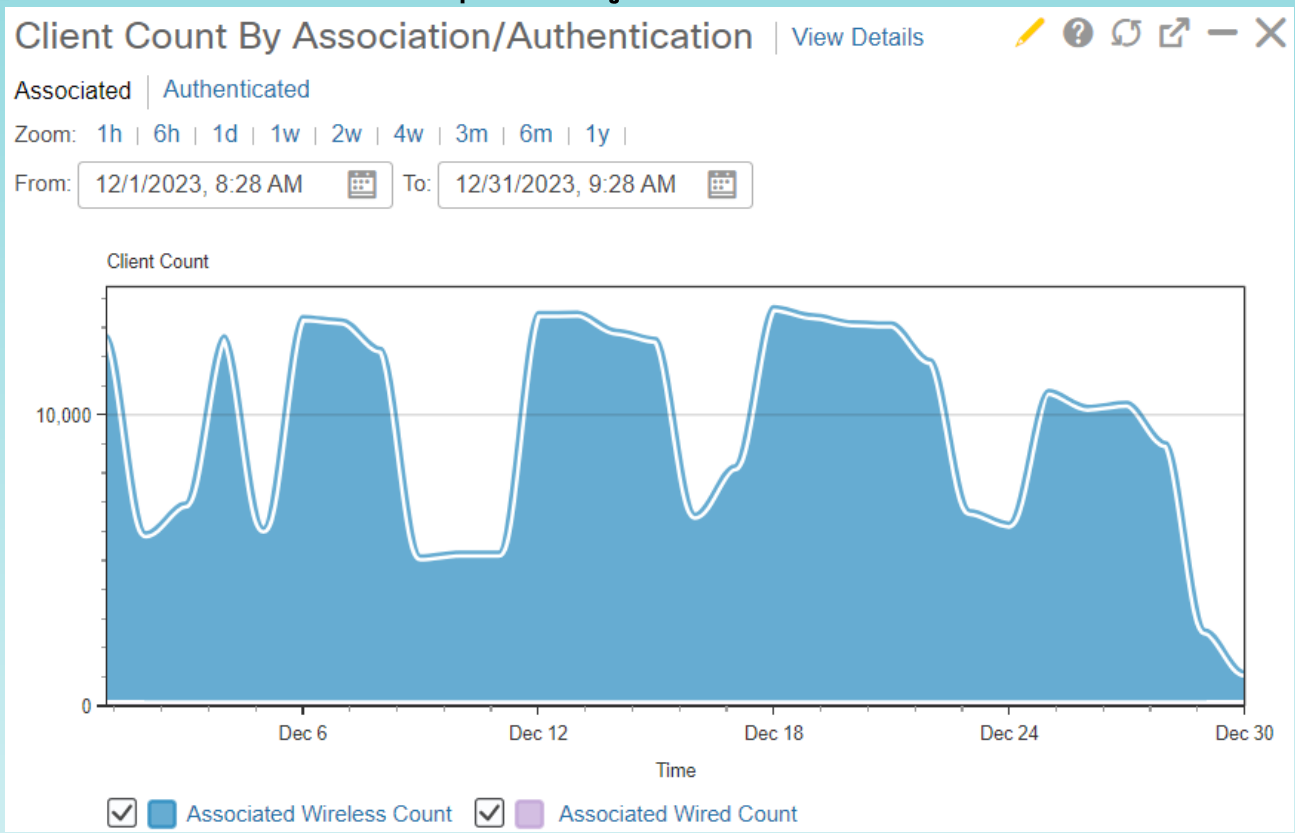


	Max	Average	Current
In	3435.9 Mb/s (34.4%)	1495.2 Mb/s (15.0%)	95.0 Mb/s (1.0%)
Out	496.1 Mb/s (5.0%)	179.4 Mb/s (1.8%)	33.4 Mb/s (0.3%)

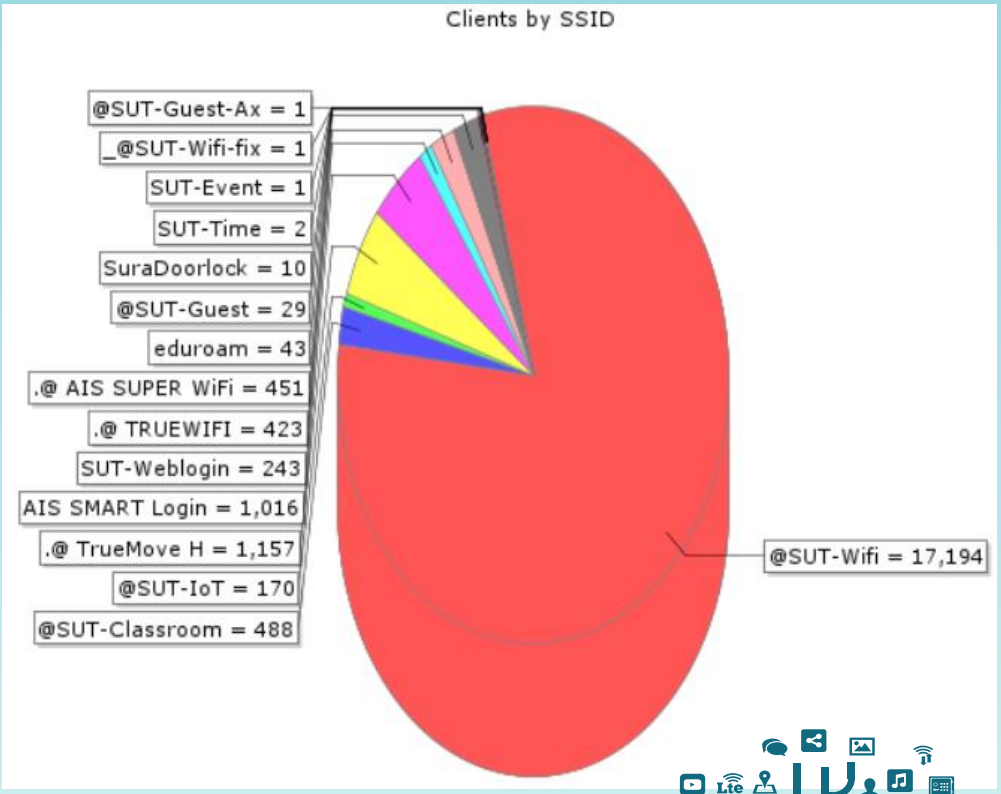
รายงานจำนวนผู้ใช้งานผ่านระบบเครือข่ายไร้สาย

สรุปสถิติจำนวนผู้ใช้งานผ่านระบบ wireless ทั้งหมด

สรุปปริมาณผู้ใช้งานต่อวัน



แบ่งตาม SSID สถิติย้อนหลัง 1 เดือน



- ผู้ใช้งานผ่านระบบ wireless สูงสุด 13,714 คน/วัน
- ผู้ใช้งานผ่านระบบ wireless, ต่ำสุด 1,160 คน/วัน
- ผู้ใช้งานผ่านระบบ wireless เฉลี่ย 9,636 คน/วัน

สรุปการดำเนินการบนระบบ Internet Data Center

15 Dec 66	upgrade vcenter
18 Dec 66	บำรุงรักษาเครื่องปรับอากาศ ห้องเมน และห้องเครือข่าย งวดที่ 1/4
19 Dec 66	บำรุงรักษาอุปกรณ์ ห้อง IDC ชั้น 4 อยู่ในการรับประกัน UPS/Air/Monitoring/Water Leak ครั้งที่ 5/8
22 Dec 66	อาคารวิจัยไฟฟ้าดับ Gen ทำงาน ยกเว้นตัวเล็กสีเขียว แจ้งงานไฟฟ้าเข้าตรวจสอบ
26 Dec 66	บำรุงรักษาระบบ FM-200 ห้อง IDC ชั้น 4 อยู่ในการรับประกันครั้งที่ 2/3

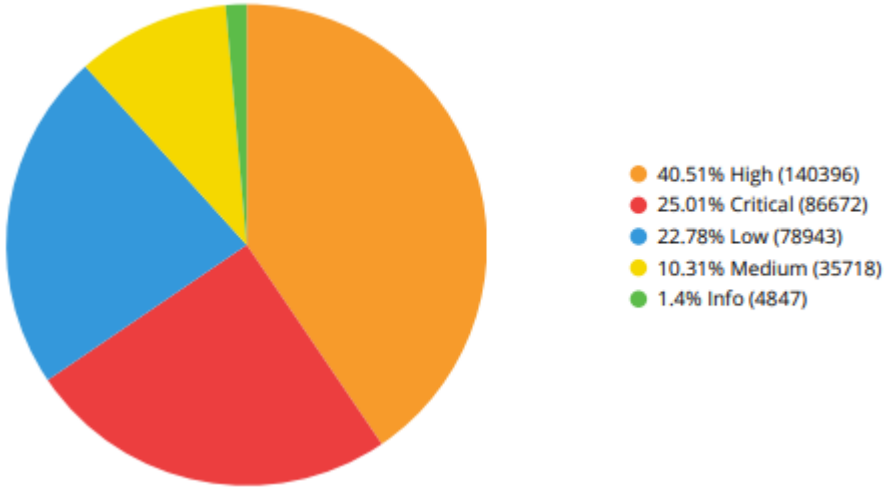
สรุปการดำเนินการบนระบบโทรคมนาคม

8 Dec 66	เวลา 15:00 น. ประชุมเรื่องงานโทรศัพท์ของดิจิเทค
12 Dec 66	ดำเนินการติดตั้ง switch เพื่อรองรับ IP Phone ชั้น 5 อาคารดิจิทัล สำนักวิชาดิจิเทค
14 Dec 66	หมายเลขโทรศัพท์สำนักวิชาดิจิเทค ขอจัดสรรเพิ่มเติม และของเดิมมีการเปลี่ยนแปลงชั้น 5 จำนวน 13 เลขหมาย และชั้น 1 ดำเนินการแล้วเสร็จ

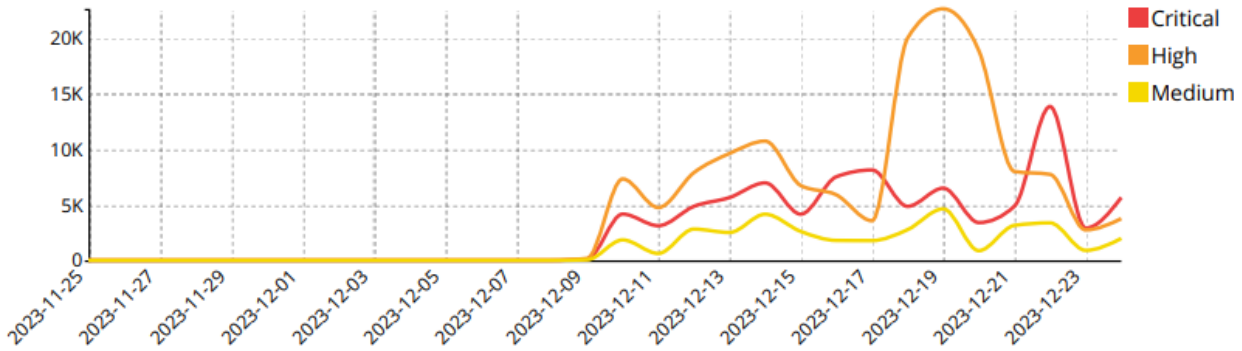
ภัยคุกคามระบบเครือข่าย

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

Intrusions By Severity



Critical High and Medium Intrusions Timeline



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

Intrusions By Types

#	Intrusion Type	Counts
1	Anomaly	82,869
2	SQL Injection	56,828
3	Code Injection	49,234
4	OS Command Injection	22,065
5	Malware	20,459
6	Other	19,086
7	Path Traversal	16,192
8	DoS	11,014
9	Buffer Errors	8,614
10	Permission/Priviledge/Access Control	5,364
11	Improper Authentication	3,428
12	XSS	2,342
13	Information Disclosure	1,454
14	CSRF	8
15	Resource Management Errors	6
16	Format String	1

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	28,616
2	WIFICAM.P2P.GoAhead.Multiple.Remote.Code.Execution	CVE-2017-8221,CVE-2017-8223, CVE-2017-8225,CVE-2017-18377	Code Injection	15,300
3	Bladabindi.Botnet			7,784
4	Gh0st.Rat.Botnet			5,861
5	Andromeda.Botnet			3,167
6	Zyxel.zhttpd.Webserver.Command.Injection		OS Command Injection	2,879
7	Zivif.PR115-204-P-RS.Web.Cameras.Credentials.Disclosure	CVE-2018-5726,CVE-2017-17106	Improper Authentication	1,785
8	Hikvision.Product.SDK.WebLanguage.Tag.Command.Injection	CVE-2021-36260	OS Command Injection	1,679
9	Babar			1,546
10	Apache.Log4j.Error.Log.Remote.Code.Execution	CVE-2021-4104,CVE-2021-44228 ,CVE-2021-45046	Permission/Priviledge/Access Control	1,393
11	Dasan.GPON.Remote.Code.Execution	CVE-2018-10561,CVE-2018-10562	OS Command Injection	1,369
12	RedLineStealer			1,265
13	Zyxel.Firmware.error.message.Command.Injection			1,173
14	Telerik.Web.UI.RadAsyncUpload.Handling.Arbitrary.File.Upload	CVE-2017-11317,CVE-2017-11357,CVE-2019-18935	Improper Authentication	1,099
15	Linksys.DirecTV.WVB.HTTP.Header.Remote.Command.Execution	CVE-2017-17411	Code Injection	1,097
16	D-Link.Devices.HNAP.SOAPAction-Header.Command.Execution	CVE-2015-2051,CVE-2019-10891	OS Command Injection	768
17	OpenSSL.Heartbleed.Attack	CVE-2014-0160	Information Disclosure	765
18	MS.Windows.HTTP.sys.Request.Handling.Remote.Code.Execution	CVE-2015-1635	Buffer Errors	640
19	ThinkPHP.Controller.Parameter.Remote.Code.Execution	CVE-2019-9082,CVE-2018-20062	Code Injection	612
20	Drupal.Core.REST.Module.Remote.Code.Execution	CVE-2019-6340	OS Command Injection	577

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

High Severity Intrusions

#	Attack Name	CVE-ID	Intrusion Type	Counts
1	HTTP.URI.SQL.Injection		SQL Injection	54,435
2	ALFA.TEaM.Web.Shell		Malware	14,048
3	malicious-url			13,518
4	Multiple.Routers.GPON.form Login.Remote.Command.Injecti on		OS Command Injection	13,151
5	Generic.XXE.Detection	CVE-2012-3363,CVE-2013-4295, CVE-2013-5015,CVE-2014-3490, CVE-2016-9563,CVE-2018-8527, CVE-2018-8532,CVE-2018-8533, CVE-2019-0537,CVE-2019-0948, CVE-2019-2647,CVE-2019-2648, CVE-2019-2649,CVE-2019-2650, CVE-2020-0765,CVE-2021-2400, CVE-2022-1018,CVE-2018-13415 ,CVE-2018-13416,CVE-2018-134 17,CVE-2018-15444,CVE-2018-1 8471,CVE-2019-17554,CVE-2019 -18227,CVE-2019-18227,CVE-20 20-15418,CVE-2020-15419,CVE- 2020-26981,CVE-2021-21658,CV E-2021-21659,CVE-2021-21672, CVE-2021-29447,CVE-2021-3120 7,CVE-2022-24463,CVE-2022-28 219,CVE-2022-43473,CVE-2022- 45468,CVE-2022-45876,CVE-202 2-46286,CVE-2022-46300,CVE-2 023-32567	Other	12,816
6	SystemBC.Botnet			8,746
7	AndroxGh0st.Malware		Malware	5,750
8	Mirai.Botnet			4,279
9	Linux.Kernel.TCP.SACK_Panic .DoS	CVE-2019-11477,CVE-2019-1147 8,CVE-2019-11479	DoS	2,326
10	MySQL.Login.Brute.Force	CVE-2012-2122	Anomaly	2,188
11	MS.IIS.FTP.IAC.Remote.Code. Execution	CVE-2010-3972	Buffer Errors	1,887
12	Web.Server.Password.File.Ac cess		Permission/Priviledge/Access Control	1,826
13	Generic.XXE.Detection	CVE-2012-3363,CVE-2013-4295, CVE-2013-5015,CVE-2014-3490, CVE-2016-9563,CVE-2018-8527, CVE-2018-8532,CVE-2018-8533, CVE-2019-0537,CVE-2019-0948, CVE-2019-2647,CVE-2019-2648, CVE-2019-2649,CVE-2019-2650, CVE-2020-0765,CVE-2021-2400, CVE-2022-1018,CVE-2018-13415 ,CVE-2018-13416,CVE-2018-134 17,CVE-2018-15444,CVE-2018-1 8471,CVE-2019-17554,CVE-2019 -18227,CVE-2019-18227,CVE-20 20-15418,CVE-2020-15419,CVE- 2020-26981,CVE-2021-21658,CV E-2021-21659,CVE-2021-21672, CVE-2021-29447,CVE-2021-3120 7,CVE-2022-24463,CVE-2022-28 219,CVE-2022-43473,CVE-2022- 45468,CVE-2022-45876,CVE-202 2-46286,CVE-2022-46300	Other	1,174
14	HTTP.Header.SQL.Injection		SQL Injection	860

Medium Severity Intrusions

#	Attack Name	CVE-ID	Intrusion Type	Counts
1	Apache.Solr.SolrResourceLoade r.Directory.Traversal	CVE-2013-6397	Path Traversal	13,541
2	WordPress.xmlrpc.Pingback.Do S		DoS	7,098
3	OpenSSL.DTLS.dtls1.buffer.reco rd.Function.DoS	CVE-2015-0206	Buffer Errors	6,023
4	Cross.Site.Scripting	CVE-2007-1355,CVE-2007-6316, CVE-2008-2165,CVE-2008-3305, CVE-2008-3726,CVE-2008-4393, CVE-2008-4918,CVE-2009-1524, CVE-2010-2370,CVE-2010-3266, CVE-2010-4828,CVE-2011-0508, CVE-2011-0959,CVE-2011-0961, CVE-2011-1772,CVE-2011-2179, CVE-2011-2938,CVE-2011-3010, CVE-2011-3390,CVE-2011-4340, CVE-2016-3212,CVE-2016-9500, CVE-2018-2791,CVE-2018-5550, CVE-2018-8006,CVE-2018-17441 ,CVE-2018-17443	XSS	2,151
5	Apache.HTTP.Server.mod_rpaf.X _Forwarded_For.DoS	CVE-2012-3526	DoS	1,465
6	HTTP.Referer.Header.SQL.Injecti on	CVE-2007-1061	SQL Injection	1,407
7	HTTP.GET.Request.Directory.Tra versal	CVE-2004-2112,CVE-2005-2020, CVE-2008-1145,CVE-2008-2938, CVE-2008-3727,CVE-2008-3938, CVE-2008-4243,CVE-2011-4714, CVE-2014-0780,CVE-2020-5410	Path Traversal	1,185
8	WordPress.xmlrpc.php.system. multicall.Amplification.Attack		Anomaly	966
9	TCP.Split.Handshake		Anomaly	572
10	WordPress.REST.API.Username. Enumeration.Information.Disclo sure	CVE-2017-5487	Information Disclosure	465
11	PHP.Diescan		Anomaly	272
12	RealNetworks.Helix.Universal.Se rver.DoS	CVE-2004-0389	DoS	110
13	LibreNMS.UserController.php.U sername.Stored.XSS	CVE-2022-4068	XSS	64
14	Apache.Axis2.Default.Password. Access	CVE-2010-0219	Other	33
15	HTTP.URI.XSS	CVE-2015-6099	XSS	30
16	Atlassian.Server.S.Endpoint.Info rmation.Disclosure	CVE-2021-26085,CVE-2021-2608 6	Information Disclosure	29
17	WordPress.DragAndDrop.Multi. File.Uploader.Arbitrary.File.Uplo ad	CVE-2020-12800	Permission/Priviledge/Access Control	26
18	Phpweb.CMS.appcode.Informati on.Disclosure		Information Disclosure	21
19	WS_FTP.Sensitive.File.Access		Information Disclosure	20
20	sqlmap.Scanner		Anomaly	19

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

Intrusion Victims

#	Attack Victim	Counts (Critical / High / Medium)	Percent of Total Attacks
1	203.158.7.71	26,677	23.71%
2	203.158.4.100	14,378	12.78%
3	10.1.40.80	8,683	7.72%
4	203.158.7.45	8,438	7.50%
5	204.11.56.48	8,205	7.29%
6	202.28.42.36	7,808	6.94%
7	203.158.7.39	5,301	4.71%
8	192.168.160.56	5,293	4.70%
9	202.28.42.29	4,860	4.32%
10	203.158.7.63	4,006	3.56%
11	202.28.42.71	3,278	2.91%
12	203.158.6.2	2,713	2.41%
13	202.28.42.25	2,014	1.79%
14	10.1.28.194	1,996	1.77%
15	192.168.31.131	1,922	1.71%
16	202.28.42.38	1,884	1.67%
17	202.28.42.60	1,419	1.26%
18	185.215.113.205	1,265	1.12%
19	203.158.4.150	1,189	1.06%
20	10.1.176.78	1,171	1.04%

Intrusion Sources

#	Attack Source	Counts (Critical / High / Medium)	Percent of Total Attacks
1	83.97.73.87	55,311	33.28%
2	52.139.173.129	43,035	25.89%
3	139.59.126.18	10,549	6.35%
4	66.240.205.34	7,984	4.80%
5	45.136.118.64	5,473	3.29%
6	31.7.58.42	5,337	3.21%
7	183.88.186.34	5,192	3.12%
8	185.134.22.149	4,872	2.93%
9	58.136.229.62	3,491	2.10%
10	91.92.250.63	3,393	2.04%
11	84.54.51.29	3,015	1.81%
12	94.130.164.87	2,904	1.75%
13	49.228.51.220	2,880	1.73%
14	131.159.24.205	2,297	1.38%
15	20.211.86.159	2,273	1.37%
16	4.178.122.242	1,950	1.17%
17	2.56.247.167	1,804	1.09%
18	179.43.183.170	1,785	1.07%
19	37.19.205.205	1,411	0.85%
20	10.0.28.20	1,265	0.76%

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

Intrusions Blocked

#	Intrusion Name	Intrusion Type	Severity	Counts
1	PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	Code Injection	Critical	28,616
2	WIFICAM.P2P.GoAhead.Multiple.Remote.Code.Execution	Code Injection	Critical	15,300
3	Bladabindi.Botnet		Critical	7,784
4	Gh0st.Rat.Botnet		Critical	5,861
5	Andromeda.Botnet		Critical	3,167
6	Zyxel.zhttpd.Webserver.Command.Injection	OS Command Injection	Critical	2,879
7	Zivif.PR115-204-P-RS.Web.Cameras.Credentials.Disclosure	Improper Authentication	Critical	1,785
8	Hikvision.Product.SDK.WebLanguage.Tag.Command.Injection	OS Command Injection	Critical	1,679
9	Babar		Critical	1,546
10	Apache.Log4j.Error.Log.Remote.Code.Execution	Permission/Priviledge/Access Control	Critical	1,393
11	Dasan.GPON.Remote.Code.Execution	OS Command Injection	Critical	1,369
12	RedLineStealer		Critical	1,265
13	Zyxel.Firmware.error.message.Command.Injection		Critical	1,173
14	Telerik.Web.UI.RadAsyncUpload.Handling.Arbitrary.File.Upload	Improper Authentication	Critical	1,099
15	Linksys.DirecTV.WVB.HTTP.Header.Remote.Command.Execution	Code Injection	Critical	1,097
16	D-Link.Devices.HNAP.SOAPAction-Header.Command.Execution	OS Command Injection	Critical	768
17	OpenSSL.Heartbleed.Attack	Information Disclosure	Critical	765
18	MS.Windows.HTTP.sys.Request.Handling.Remote.Code.Execution	Buffer Errors	Critical	640
19	ThinkPHP.Controller.Parameter.Remote.Code.Execution	Code Injection	Critical	612
20	Drupal.Core.REST.Module.Remote.Code.Execution	OS Command Injection	Critical	577

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

Top Applications by Bandwidth

#	Application	Sessions
1	HTTPS.BROWSER	243,747
2	Android	184,238
3	HTTP.BROWSER	85,138
4	DNS	42,248
5	Microsoft.MSN.Bing.Bot	17,105
6	Facebook	15,318
7	Microsoft.Portal	12,944
8	SSL	11,848
9	DHCP6	11,833
10	HTTP	10,996

Top Applications by Sessions

#	User (or IP)	Sessions
1	192.168.35.8	29,029
2	52.70.240.171	23,469
3	3.224.220.101	23,435
4	23.22.35.162	22,523
5	192.168.35.26	18,884
6	203.158.1.66	17,280
7	192.168.35.25	8,802
8	203.158.0.209	7,746
9	192.168.35.23	4,550
10	203.158.0.161	4,115

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

Intrusions Detected

#	Attack Name	Severity	CVE-ID	Counts
1	Mac.OSX.DSStore.Access.Content.Disclosure	Medium		1

Events by Severity