

รายงานการใช้งาน ระบบเครือข่ายคอมพิวเตอร์ ประจำเดือน ก.ค. 2569

ฝ่ายโครงสร้างพื้นฐานและระบบเครือข่าย





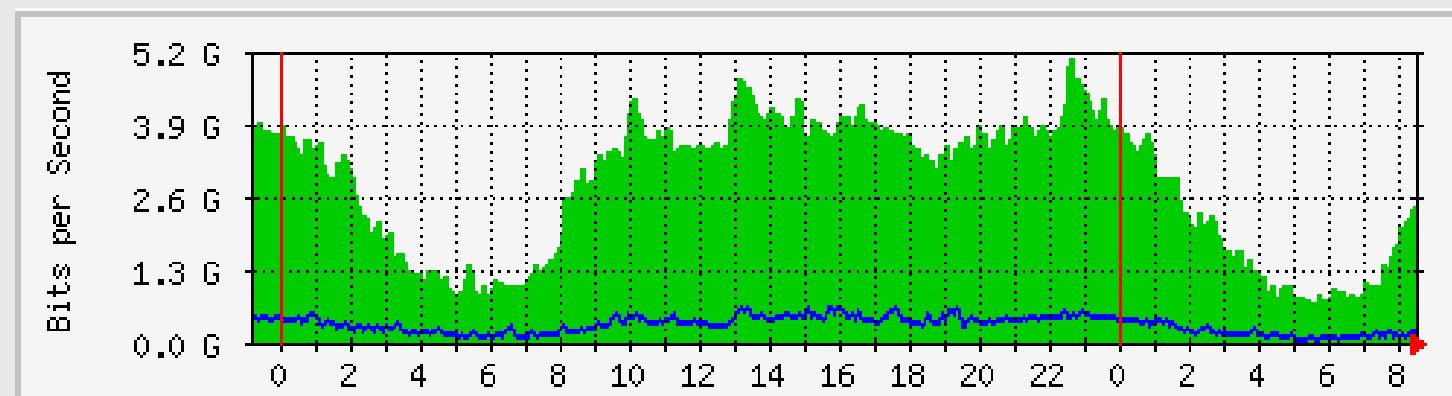
รายงานจำนวนผู้ใช้งานผ่านระบบเครือข่าย (LAN) (ไม่รวมห้องปฏิบัติการคอมพิวเตอร์)

วิธีการ	จำนวน
วิธีการแบบ ISE (802.1x)	309 คน

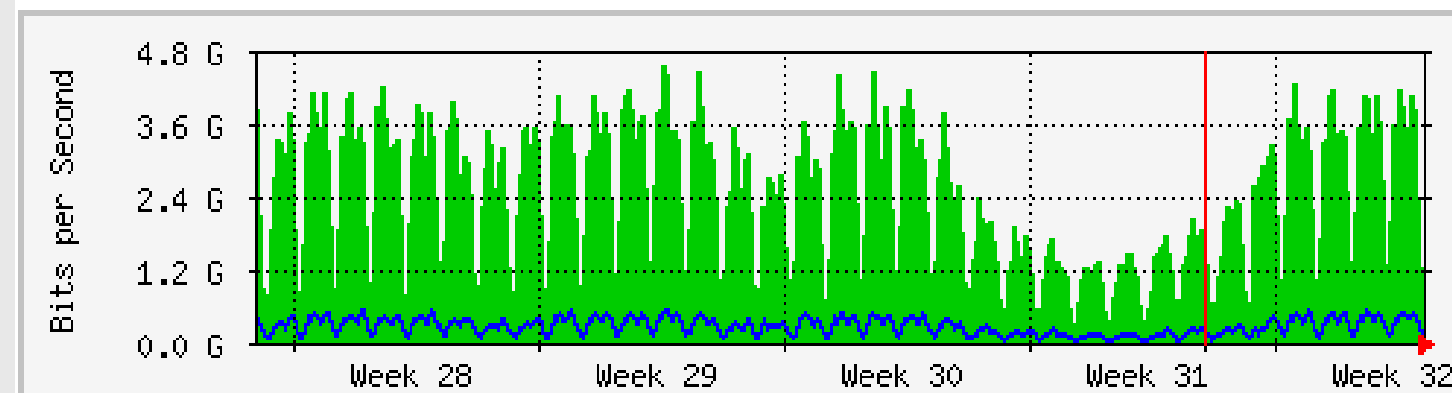
รายงานการใช้งานระบบเครือข่าย

Internet Gateway Traffic

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

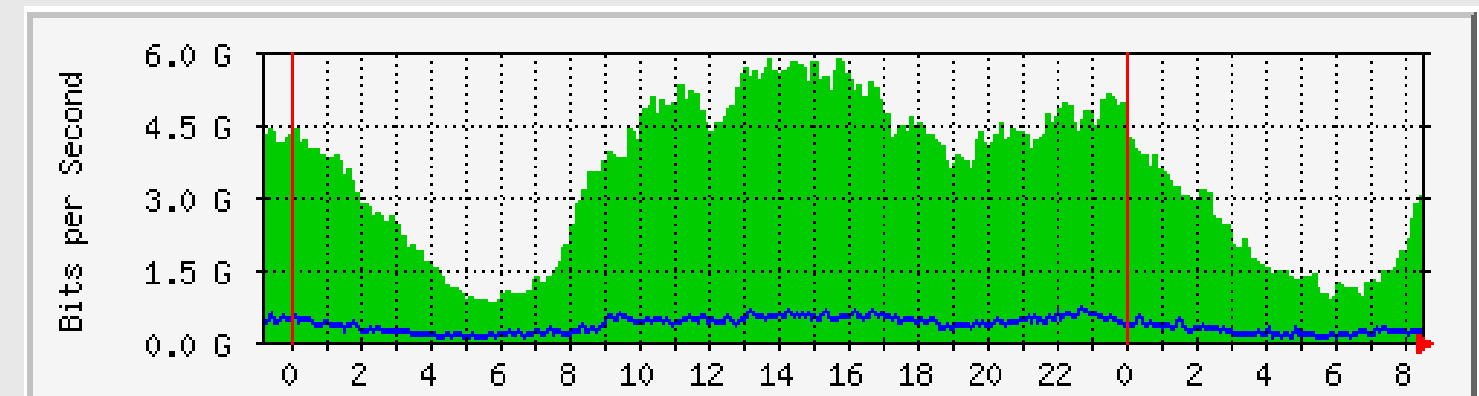


	Max	Average	Current
In	5053.3 Mb/s (50.5%)	2729.7 Mb/s (27.3%)	3155.6 Mb/s (31.6%)
Out	614.7 Mb/s (6.1%)	294.3 Mb/s (2.9%)	321.9 Mb/s (3.2%)

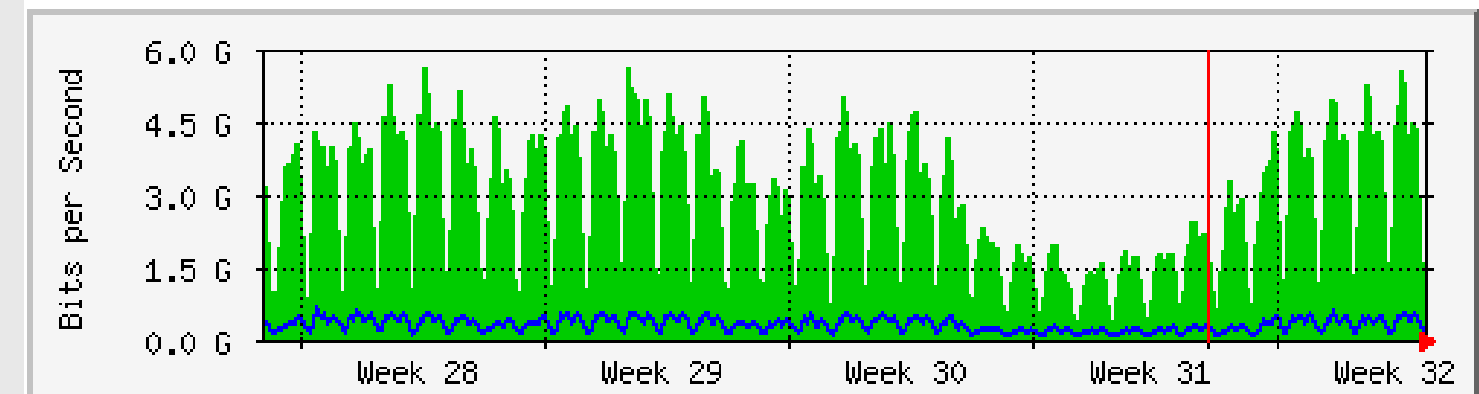


	Max	Average	Current
In	4532.4 Mb/s (45.3%)	2325.2 Mb/s (23.3%)	790.5 Mb/s (7.9%)
Out	526.9 Mb/s (5.3%)	248.9 Mb/s (2.5%)	68.4 Mb/s (0.7%)

Link to UNINET (Domestic 10Gbps)



	Max	Average	Current
In	5853.0 Mb/s (58.5%)	3332.1 Mb/s (33.3%)	3870.5 Mb/s (38.7%)
Out	689.2 Mb/s (6.9%)	324.7 Mb/s (3.2%)	345.8 Mb/s (3.5%)



	Max	Average	Current
In	5605.2 Mb/s (56.1%)	2733.1 Mb/s (27.3%)	1096.5 Mb/s (11.0%)
Out	621.7 Mb/s (6.2%)	293.1 Mb/s (2.9%)	141.0 Mb/s (1.4%)

สรุปการดำเนินการบนระบบเครือข่ายคอมพิวเตอร์

หัวข้อ	จำนวน (งาน)
ซ่อมแซมอุปกรณ์ Network (ผลกระทบในระดับอาคาร)	4
งานสำรวจหน้างาน ประมาณราคาการจัดจ้าง ขยาย/ปรับปรุง/ซ่อมแซม/บำรุงรักษาระบบ	2
การ Monitor/Standby ระบบ Network	2
ติดตั้ง/ซ่อมแซม สายสัญญาณ Network	41
งานให้คำแนะนำปรึกษาแก่ผู้ใช้บริการ	7

สรุปการดำเนินการบนระบบ INTERNET DATA CENTER

หัวข้อ	จำนวน (งาน)
ติดตั้งอุปกรณ์ Data Center (ผลกระทบในระดับมหาวิทยาลัย)	-
บริหารจัดการระบบ Data Center	1
บริหารจัดการระบบ Network และ Security	12
จัดสรร VS/VM, Web	16
การ Monitor/Standby ระบบ Data Center	2
บริหารจัดการ Active Directory Account	8
บริหารจัดการ Email Account / บริหารจัดการ Wifi Account / บริหารจัดการ G.dot Account / Manage Bulk Users	30
ตรวจสอบ/ปรับปรุงแก้ไข ด้านความปลอดภัยระบบสารสนเทศ	6

สรุปการดำเนินการบนระบบโทรคมนาคม

หัวข้อ	จำนวน (งาน)
แก้ไขอุปกรณ์ Telephone (ผลกระทบในระดับอาคาร)	2
การ Monitor/Standby ระบบ Telephone	-
ติดตั้ง/ซ่อมแซม สายสัญญาณ Telephone	31
จัดสรรหมายเลข/IP Phone/Soft Phone	-
กำกับดูแลการติดตั้ง เบบคีน อุปกรณ์/ครุภัณฑ์ และเอกสารประกอบที่เกี่ยวข้องให้ถูกต้องแล้ว เสร็จภายในเวลาที่กำหนด	5

สรุปการดำเนินงานด้านอื่น ๆ

หัวข้อ	จำนวน (งาน)
เข้าร่วมประชุม/เข้าร่วมกิจกรรมต่างๆของมหาวิทยาลัย	2
จัดการรายงานการประชุม /แจ้งเวียนรับรองรายงาน /แจ้งสรุปมติกับผู้ที่เกี่ยวข้องภายในระยะเวลาที่กำหนด	1
จัดทำเอกสารใบขอให้จัดซื้อ จัดจ้าง รวบรวมรายละเอียดต่าง ๆ ได้ถูกต้องครบถ้วน และบริหารจัดการส่งให้ส่วนพัสดุได้ทันตามกำหนด	-
จัดทำไฟล์นำเสนองานรูปแบบ PPT ออกแบบไฟล์สื่อประชาสัมพันธ์ รูปแบบ PDF, PNG ที่เกี่ยวข้องกับการกิจของฝ่าย/หน่วยงาน	2
รวบรวมข้อมูลและจัดทำกรอบค่างบประมาณประจำปีในภาพรวมของหน่วยงาน	-
สรุปรายงานผลการดำเนินงานของหน่วยงานประจำเดือน/ประจำไตรมาส และรายงานต่อคณะกรรมการของมหาวิทยาลัย หรือระบบออนไลน์	3
ร่างหนังสือแบบที่มีเนื้อหาลักษณะเฉพาะพิเศษ	1
ร่างหนังสือแบบฟอร์มพื้นฐานทั่วไป	2

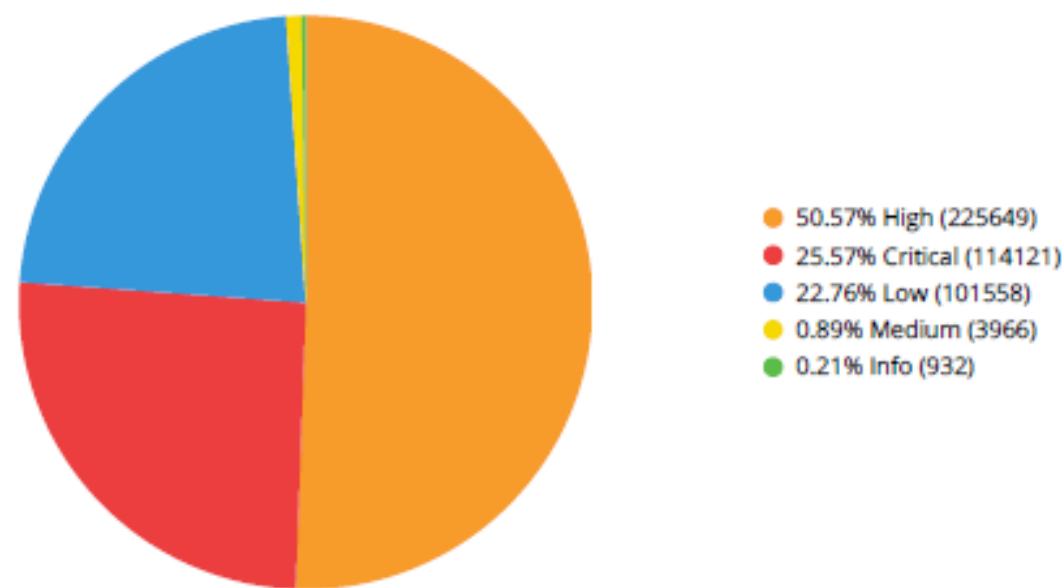
ภัยคุกคามระบบเครือข่าย



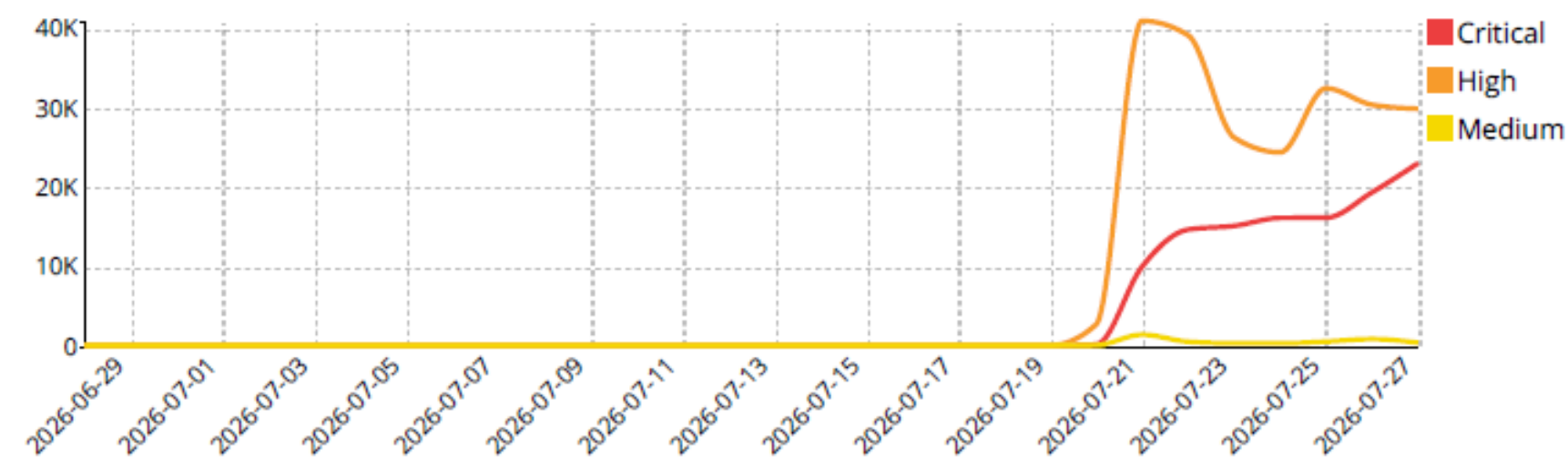
การยับยั้งการโจมตีบนระบบเครือข่าย โดยอุปกรณ์ Next Gen Firewall : Fortinet

SUT Gateway of IPS Report

Intrusions By Severity



Critical High and Medium Intrusions Timeline



การยับยั้งการโจมตีบนระบบเครือข่าย โดยอุปกรณ์ Next Gen Firewall : Fortinet

SUT Gateway of IPS Report

Intrusion Victims



#	Attack Victim	Counts	Critical	High	Medium	Percent of Total Attacks
1	203.158.5.129				88,455	40.02%
2	172.65.211.209				46,475	21.03%
3	117.18.127.179				19,073	8.63%
4	202.28.42.36				13,745	6.22%
5	202.28.42.26				11,796	5.34%
6	203.158.4.150				4,176	1.89%
7	202.28.42.38				3,562	1.61%
8	203.158.7.15				3,299	1.49%
9	65.20.83.65				3,287	1.49%
10	203.158.7.71				3,282	1.48%
11	49.228.131.165				3,266	1.48%
12	20.184.145.190				3,063	1.39%
13	202.28.42.39				2,572	1.16%
14	203.158.7.75				2,535	1.15%
15	203.158.7.92				2,456	1.11%
16	43.249.32.143				2,227	1.01%
17	202.28.42.23				2,212	1.00%
18	202.28.42.20				1,939	0.88%
19	203.158.7.70				1,830	0.83%
20	203.158.7.80				1,786	0.81%

Intrusion Sources



#	Attack Source	Counts	Critical	High	Medium	Percent of Total Attacks
1	203.158.7.23				46,475	19.89%
2	195.182.16.23				44,603	19.09%
3	144.172.99.164				25,949	11.10%
4	5.61.209.44				25,356	10.85%
5	94.154.43.243				11,848	5.07%
6	10.1.143.32				11,683	5.00%
7	10.1.96.233				7,392	3.16%
8	5.61.209.43				6,570	2.81%
9	10.0.53.36				6,117	2.62%
10	10.0.233.216				5,620	2.41%
11	10.1.155.141				5,493	2.35%
12	188.253.121.111				5,375	2.30%
13	197.248.76.230				5,252	2.25%
14	203.10.99.50				5,205	2.23%
15	103.52.212.114				3,894	1.67%
16	188.253.121.112				3,519	1.51%
17	188.253.121.110				3,423	1.46%
18	45.92.11.253				3,352	1.43%
19	10.0.144.250				3,286	1.41%
20	175.100.53.13				3,262	1.40%

การยับยั้งการโจมตีบนระบบเครือข่าย โดยอุปกรณ์ Next Gen Firewall : Fortinet



Intrusions Blocked

SUT Gateway of IPS Report

#	Intrusion Name	Intrusion Type	Severity	Counts
1	Hikvision.Products.SDK.WebLanguage.Tag.Command.Injection	OS Command Injection	Critical	88,380
2	njRAT.Botnet		Critical	3,266
3	Amadey.Botnet		Critical	3,063
4	Tofsee		Critical	2,997
5	Joomla!.Core.Session.Remote.Code.Execution	Code Injection	Critical	2,071
6	NETGEAR.DGN1000.CGI.Unauthenticated.Remote.Code.Execution	Code Injection	Critical	1,720
7	D-Link.Devices.HNAP.SOAPAction-Header.Command.Execution	OS Command Injection	Critical	1,651
8	DZS.GPON.Remote.Code.Execution	OS Command Injection	Critical	1,591
9	LB-LINK.goform.set_LimitClient_cfg.Command.Injection	Code Injection	Critical	1,523
10	WordPress.REST.API.batch-route.SQL.Injection	SQL Injection	Critical	1,201
11	PTZOptics.PT30X.param.Authentication.Bypass	Improper Authentication	Critical	885
12	Java.Debug.Wire.Protocol.Insecure.Configuration	Permission/Privilege/Access Control	Critical	640
13	WIFICAM.P2P.GoAhead.Multiple.Remote.Code.Execution	Code Injection	Critical	484
14	Remote.CMD.Shell	Malware	Critical	475
15	ThinkPHP.Controller.Parameter.Remote.Code.Execution	Code Injection	Critical	390
16	Apache.Log4j.Error.Log.Remote.Code.Execution	Permission/Privilege/Access Control	Critical	367
17	D-Link.DSL-2750B.CLI.OS.Command.Injection	OS Command Injection	Critical	273
18	Joomla!.SP.Page.Builder.Arbitrary.File.Upload	Code Injection	Critical	231
19	Apache.Struts.2.OGNLScript.Injection	Other	Critical	137
20	ASUS.Devices.infosvr.UDP.Broadcast.Command.Execution	OS Command Injection	Critical	131

การยับยั้งการโจมตีบนระบบเครือข่าย โดยอุปกรณ์ Next Gen Firewall : Fortinet

SUT Gateway Cyber Threat Assessment



การยับยั้งการโจมตีบนระบบเครือข่าย โดยอุปกรณ์ Next Gen Firewall : Fortinet



Web Usage : Top Web Applications

Application	Sessions	Bytes
YouTube	30,381,891	71.82 TB
SSL	171,975,838	69.33 TB
TikTok	101,821,649	54.79 TB
Instagram	101,841,155	48.42 TB
Facebook	93,023,933	30.48 TB
Apple.Store	23,283,224	17.04 TB
iCloud	35,741,792	10.09 TB
Twitter	3,509,637	9.60 TB
Netflix	5,095,439	7.86 TB
Google.Services	78,125,572	7.48 TB
Microsoft.Windows.Update	1,297,886	6.91 TB
Apple.Services	26,776,216	5.21 TB
Garena	2,300,499	3.37 TB
Riot.Games	1,267,728	2.29 TB
HTTPS	61,809,141	2.09 TB
Microsoft.Portal	18,763,540	1.68 TB
Telegram	1,000,330	1.54 TB
Microsoft.365.Portal	10,488,228	1.53 TB
HTTP.BROWSER	10,332,372	1.47 TB
Twitch	318,917	1.45 TB
HoYoverse.Genshin.Impact	28,822	1.43 TB
Naver.Line	7,259,280	1.23 TB
HTTP.Download.Accelerator	488,072	1.18 TB
Amazon.AWS	727,842	1.15 TB
HTTP.Segmented.Download	374,067	1.11 TB

การยับยั้งการโจมตีบนระบบเครือข่าย โดยอุปกรณ์ Next Gen Firewall : Fortinet

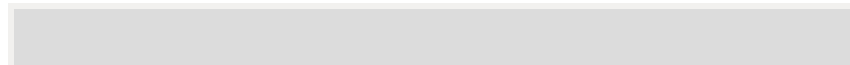
สำหรับ REG และ Finance

FIN-REG Security Analysis

Top Applications by Bandwidth



Top Applications by Bandwidth

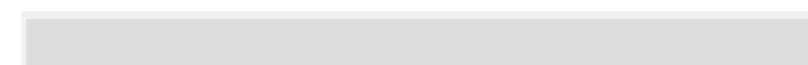


No matching log data for this report

Top Applications by Sessions



Top Applications by Sessions



No matching log data for this report

การยับยั้งการโจมตีบนระบบเครือข่าย โดยอุปกรณ์ Next Gen Firewall : Fortinet

สำหรับ 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

สำหรับ REG และ Finance

FIN-REG Cyber Threat Assessment

Security and Threat Prevention
High Risk Applications



High Risk Applications

No matching log data for this report

Top Application Vulnerability Exploits Detected



Top Application Vulnerability Exploits Detected

No matching log data for this report

การยับยั้งการโจมตีบนระบบเครือข่าย โดยอุปกรณ์ Next Gen Firewall : Fortinet สำหรับ REG และ Finance

FIN-REG Cyber Threat Assessment



Top Web Applications

Top Web Applications

No matching log data for this report