

รายงานการใช้งาน ระบบเครือข่ายคอมพิวเตอร์ ประจำเดือน ก.ย. 2569

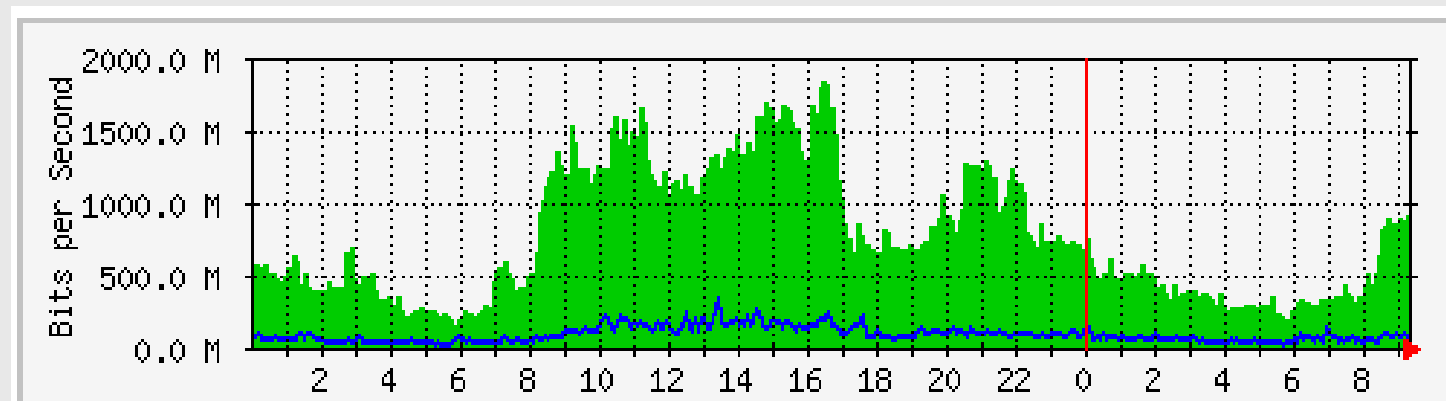
ฝ่ายโครงสร้างพื้นฐานและระบบเครือข่าย



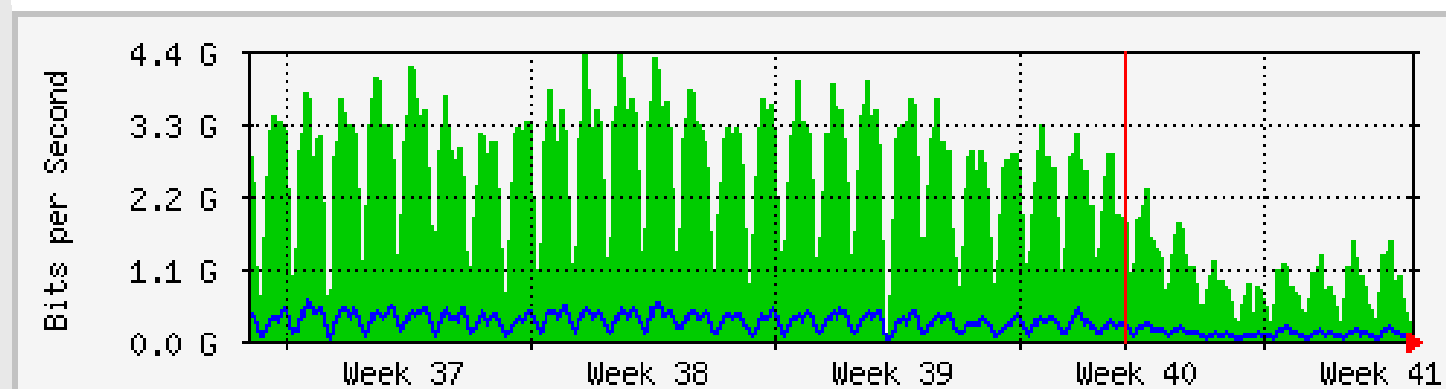
รายงานการใช้งานระบบเครือข่าย

Internet Gateway Traffic

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

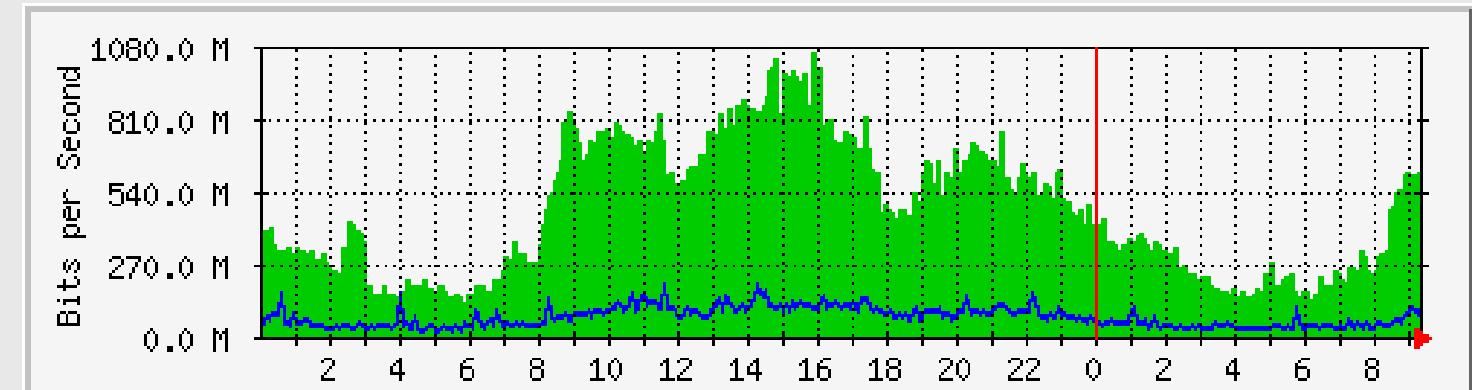


	Max	Average	Current
In	1821.0 Mb/s (18.2%)	731.7 Mb/s (7.3%)	912.0 Mb/s (9.1%)
Out	327.2 Mb/s (3.3%)	82.2 Mb/s (0.8%)	81.2 Mb/s (0.8%)

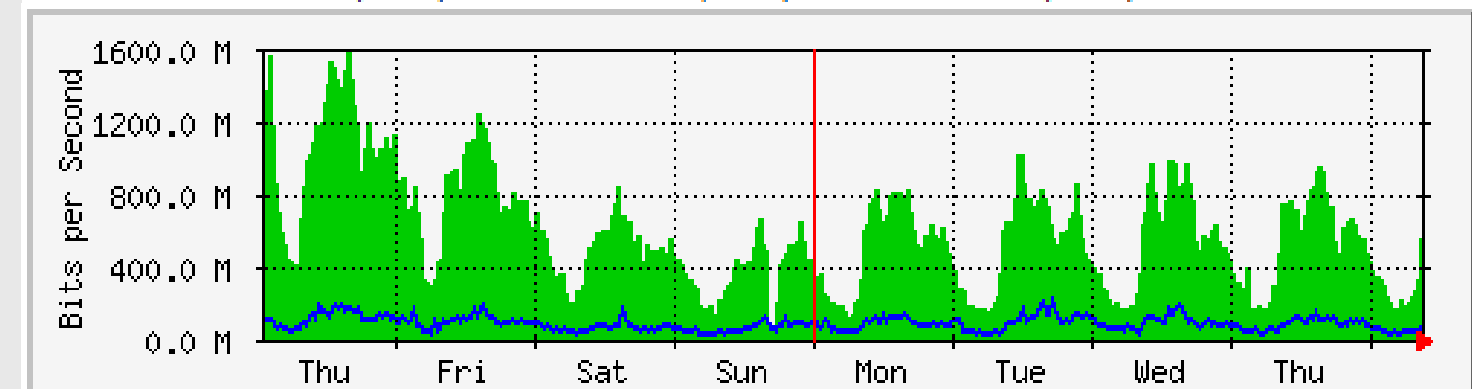


	Max	Average	Current
In	4369.0 Mb/s (43.7%)	2105.8 Mb/s (21.1%)	269.7 Mb/s (2.7%)
Out	574.3 Mb/s (5.7%)	240.1 Mb/s (2.4%)	46.0 Mb/s (0.5%)

Link to UNINET (Port-Channel20 - 20Gbps)



	Max	Average	Current
In	1050.6 Mb/s (10.5%)	453.9 Mb/s (4.5%)	608.0 Mb/s (6.1%)
Out	194.1 Mb/s (1.9%)	68.1 Mb/s (0.7%)	109.1 Mb/s (1.1%)



	Max	Average	Current
In	1572.8 Mb/s (15.7%)	573.5 Mb/s (5.7%)	549.4 Mb/s (5.5%)
Out	214.6 Mb/s (2.1%)	81.6 Mb/s (0.8%)	67.3 Mb/s (0.7%)

ภัยคุกคามระบบเครือข่าย

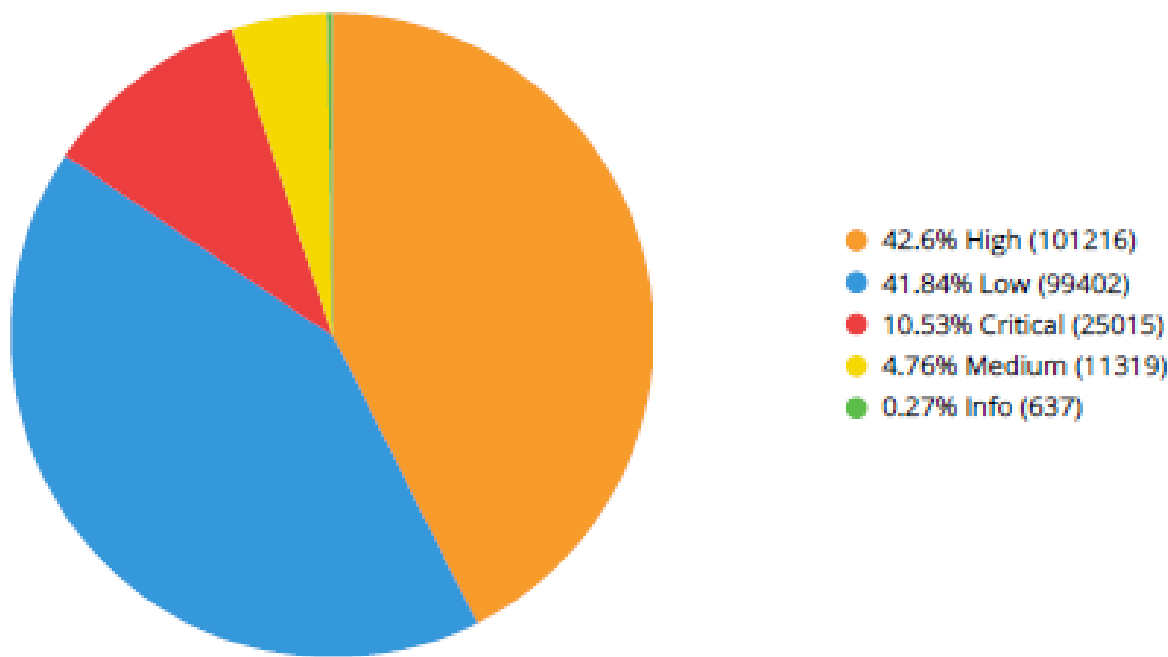


การยับยั้งการโจมตีบนระบบเครือข่าย โดยอุปกรณ์ Next Gen Firewall : Fortinet

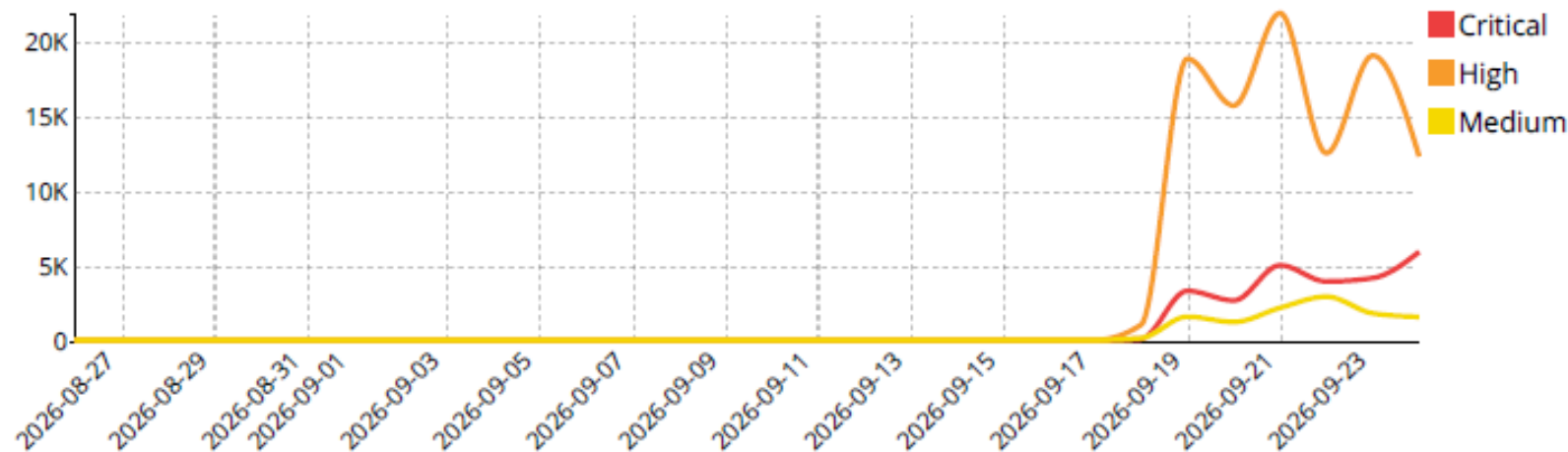
SUT Gateway of IPS Report

Summary

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	117.18.127.179				16,270	28.48%
2	202.28.42.36				10,112	17.70%
3	192.168.149.7				4,645	8.13%
4	203.158.5.129				2,904	5.08%
5	20.184.145.190				2,200	3.85%
6	150.171.110.102				2,122	3.71%
7	202.28.42.23				1,971	3.45%
8	203.158.3.157				1,685	2.95%
9	203.158.7.29				1,533	2.68%
10	203.158.4.150				1,394	2.44%
11	65.9.168.30				1,377	2.41%
12	65.9.168.101				1,326	2.32%
13	65.9.168.79				1,325	2.32%
14	65.9.168.99				1,294	2.27%
15	202.28.42.38				1,265	2.21%
16	202.28.42.20				1,215	2.13%
17	203.158.7.70				1,159	2.03%
18	202.28.42.39				1,153	2.02%
19	192.168.90.70				1,136	1.99%
20	202.28.42.40				1,043	1.83%

Intrusion Sources



#	Attack Source	Counts	Critical	High	Medium	Percent of Total Attacks
1	144.172.99.164				22,212	29.23%
2	10.1.143.32				9,464	12.46%
3	10.1.96.233				6,667	8.77%
4	184.105.192.2				4,640	6.11%
5	10.0.53.36				4,388	5.78%
6	156.253.11.220				3,694	4.86%
7	221.159.119.6				2,751	3.62%
8	195.182.16.23				2,750	3.62%
9	179.43.167.3				2,344	3.08%
10	148.66.59.214				2,339	3.08%
11	10.0.184.7				2,032	2.67%
12	45.92.11.253				1,885	2.48%
13	45.198.224.188				1,628	2.14%
14	222.122.224.114				1,557	2.05%
15	10.1.137.182				1,432	1.88%
16	203.158.7.1				1,397	1.84%
17	93.152.221.67				1,380	1.82%
18	51.79.194.123				1,323	1.74%
19	178.128.18.214				1,175	1.55%
20	10.1.121.52				924	1.22%

การยับยั้งการโจมตีบนระบบเครือข่าย โดยอุปกรณ์ Next Gen Firewall : Fortinet



Intrusions Blocked

SUT Gateway of IPS Report

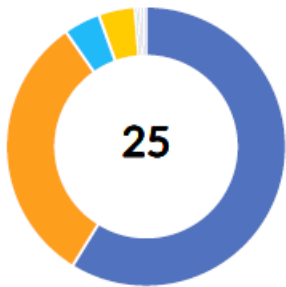
#	Intrusion Name	Intrusion Type	Severity	Counts
1	Andromeda.Botnet		Critical	4,645
2	Hikvision.Products.SDK.WebLanguage.Tag.Command.Injection	OS Command Injection	Critical	4,308
3	Apache.Log4j.Error.Log.Remote.Code.Execution	Permission/Privilege/Access Control	Critical	2,825
4	Amadey.Botnet		Critical	2,200
5	DZS.GPON.Remote.Code.Execution	OS Command Injection	Critical	1,826
6	NETGEAR.DGN1000.CGI.Unauthenticated.Remote.Code.Execution	Code Injection	Critical	1,614
7	D-Link.Devices.HNAP.SOAPAction-Header.Command.Execution	OS Command Injection	Critical	1,489
8	Joomla!.Core.Session.Remote.Code.Execution	Code Injection	Critical	980
9	PTZOptics.PT30X.param.Authentication.Bypass	Improper Authentication	Critical	586
10	Java.Debug.Wire.Protocol.Insecure.Configuration	Permission/Privilege/Access Control	Critical	456
11	PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	Code Injection	Critical	401
12	ASUS.Devices.infosvr.UDP.Broadcast.Command.Execution	OS Command Injection	Critical	263
13	WIFICAM.P2P.GoAhead.Multiple.Remote.Code.Execution	Code Injection	Critical	195
14	Dahua.Products.NetKeyboard.Authentication.Bypass	Improper Authentication	Critical	169
15	Gh0st.Rat.Botnet		Critical	160
16	Realtek.SDK.UDPServer.Command.Execution	OS Command Injection	Critical	138
17	Bash.Function.Definitions.Remote.Code.Execution	OS Command Injection	Critical	137
18	WordPress.REST.API.batch-route.SQL.Injection	SQL Injection	Critical	131
19	Remote.CMD.Shell	Malware	Critical	117
20	MS.Windows.HTTP.sys.Request.Handling.Remote.Code.Execution	Buffer Errors	Critical	106

การยับยั้งการโจมตีบนระบบเครือข่าย โดยอุปกรณ์ Next Gen Firewall : Fortinet

SUT Gateway Cyber Threat Assessment

RECOMMENDED ACTIONS

Total Detected



- Application Vulnerability Attacks: 15
- P2P and Filesharing Applications: 8
- Botnet Infections: 1
- Proxy Applications: 1
- Malicious Website: 0
- Malware Detected: 0
- Phishing Websites: 0
- Remote Access Applications: 0

SECURITY AND THREAT PREVENTION

Top 10 high risk applications

Risk	Application Name	Category	Technology	User	Total Bytes	Session
5	Proxy.HTTP	Proxy	Network-Protocol	1,390	335.19 MB	1,680
5	SOCKS4	Proxy	Network-Protocol	1	220.76 KB	235
5	SOCKS5	Proxy	Network-Protocol	1	219.38 KB	235
5	Google.Translate_Websites	General.Interest	Browser-Based	12	3.55 MB	37
4	Chrome.Remote.Desktop	Remote.Access	Client-Server	7	50.36 MB	540
4	RDP	Remote.Access	Client-Server	10	7.02 GB	264
4	Microsoft.Quick.Assist	Remote.Access	Client-Server	24	115.81 MB	149
4	AnyDesk	Remote.Access	Client-Server	6	29.19 MB	114

APPLICATION VULNERABILITY EXPLOITS

Risk	Threat Name	Type	CVE-ID	Victim	Source	Count
5	Java.Debug.Wire.Protocol.Insecure.Configuration	Permission/Privilege/Access Control	CVE-2017-6639	5	273	397
5	Vercel.Next.js.x-middleware-subrequest.Authentication.Bypass	Permission/Privilege/Access Control	CVE-2025-29927	6	10	19
4	Spring.Boot.Actuator.Unauthorized.Access	Permission/Privilege/Access Control		17	207	1,339
4	Generic.Path.Traversal.Detection	Path Traversal		17	140	792
4	Web.Server.Password.File.Access	Permission/Privilege/Access Control		17	139	621
4	malicious-url			7	2	19
4	Apache.HTTP.Server.cgi-bin.Path.Traversal	Path Traversal	CVE-2021-41773,CVE-2021-42013	4	3	6
4	PHP.Malicious.Shell	Malware		1	1	1
4	Winos.Botnet			1	1	1
3	Vite.server.fs.deny.raw.Arbitrary.File.Read	Information Disclosure	CVE-2025-30208	17	146	6,917
3	Vite.server.fs.deny.import.Arbitrary.File.Read	Information Disclosure	CVE-2024-45811	17	147	1,358

การยับยั้งการโจมตีบนระบบเครือข่าย โดยอุปกรณ์ Next Gen Firewall : Fortinet



TOP WEB CATEGORIES

WEB USAGE

TOP WEB CATEGORIES

No matching log data for this report

การยับยั้งการโจมตีบนระบบเครือข่าย โดยอุปกรณ์ Next Gen Firewall : Fortinet

สำหรับ REG และ Finance

FIN-REG Security Analysis

Top Applications by Bandwidth



#	Application	Bandwidth	Sent	Received
1	SSL			1.61 TB
2	HTTP.BROWSER			696.05 GB
3	YouTube			528.88 GB
4	Facebook			528.44 GB
5	MySQL			341.10 GB
6	SMB/445			178.39 GB
7	MIS-TCP/21064-21071			154.89 GB
8	tcp/21064			142.79 GB
9	DTLS			110.43 GB
10	Windows.File.Sharing			107.42 GB



Top Applications by Sessions

#	Application	Sessions
1	MMS	31,635,434
2	HTTP.BROWSER	25,613,666
3	SSL	18,455,156
4	DNS	7,741,264
5	SNMP	2,740,592
6	Google.Services	1,657,705
7	Microsoft.Portal	1,170,070
8	Facebook	1,158,621
9	MySQL	1,032,516
10	HTTP	959,442

การยับยั้งการโจมตีบนระบบเครือข่าย โดยอุปกรณ์ Next Gen Firewall : Fortinet

สำหรับ REG และ Finance

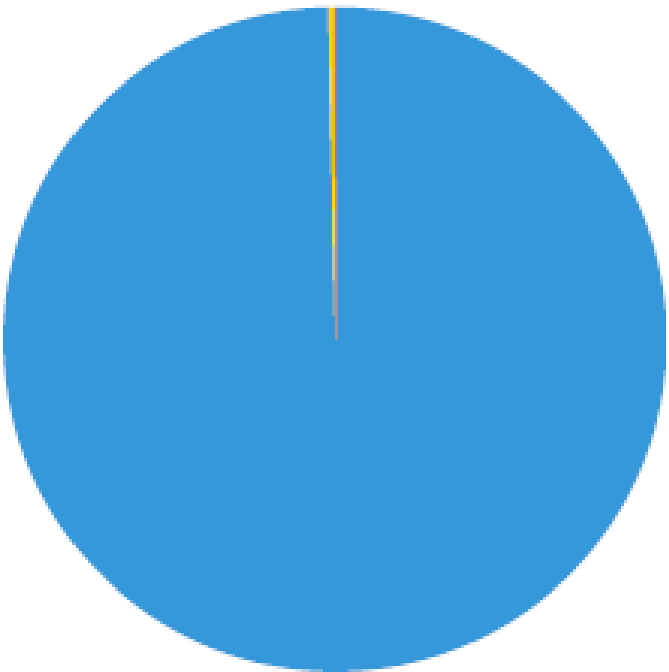
FIN-REG Security Analysis

Intrusions Detected



#	Attack Name	Severity	CVE-ID	Counts
1	Java.Debug.Wire.Protocol.Insecure.Configuration	Critical	CVE-2017-6639	397
2	Vercel.Next.js.x-middleware-subrequest.Authentication.Bypass	Critical	CVE-2025-29927	19
3	Spring.Boot.Actuator.Unauthorized.Access	High		1,339
4	Generic.Path.Traversal.Detection	High		792
5	Web.Server.Password.File.Access	High		621
6	malicious-url	High		19
7	Apache.HTTP.Server.cgi-bin.Path.Traversal	High	CVE-2021-41773,CVE-2021-42013	6
8	Winos.Botnet	High		1
9	PHP.Malicious.Shell	High		1
10	Vite.server.fs.deny.raw.Arbitrary.File.Read	Medium	CVE-2025-30208	6,917

Events by Severity



- 99.67% Low (11010)
- 0.29% Medium (32)
- 0.05% Critical (5)

การยับยั้งการโจมตีบนระบบเครือข่าย โดยอุปกรณ์ Next Gen Firewall : Fortinet

สำหรับ REG และ Finance

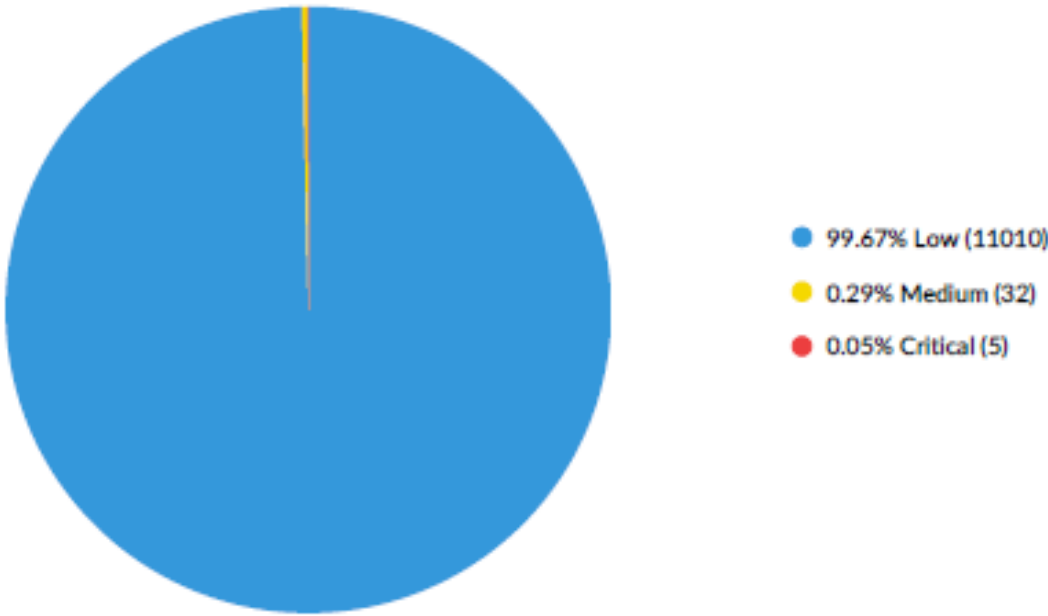
FIN-REG Security Analysis

Intrusions Detected



#	Attack Name	Severity	CVE-ID	Counts
1	Java.Debug.Wire.Protocol.Insecure.Configuration	Critical	CVE-2017-6639	397
2	Vercel.Next.js.x-middleware-subrequest.Authentication.Bypass	Critical	CVE-2025-29927	19
3	Spring.Boot.Actuator.Unauthorized.Access	High		1,339
4	Generic.Path.Traversal.Detection	High		792
5	Web.Server.Password.File.Access	High		621
6	malicious-url	High		19
7	Apache.HTTP.Server.cgi-bin.Path.Traversal	High	CVE-2021-41773,CVE-2021-42013	6
8	Winos.Botnet	High		1
9	PHP.Malicious.Shell	High		1
10	Vite.server.fs.deny.raw.Arbitrary.File.Read	Medium	CVE-2025-30208	6,917

Events by Severity



การยับยั้งการโจมตีบนระบบเครือข่าย โดยอุปกรณ์ Next Gen Firewall : Fortinet

สำหรับ REG และ Finance

FIN-REG Cyber Threat Assessment

High Severity Events



No matching log data for this report

Medium Severity Events



Medium Severity Events

#	Event Name (Description)	Level	Counts
1	Interface status changed	Medium	32

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