

當SOC遇見NOC

原來SIEM的使用也可以很簡單

Kevin Yang

kmyang@fortinet.com

從積極預防的角度來面對網路資訊安全

Shift Cybersecurity Investment to Detection and Response



FOUNDATIONAL

Refreshed: 03 May 2017 | Published: 07 January 2016 ID: G00292536

Analyst(s): *Ayal Tirosh* | *Paul E. Proctor*

“Organizations need to detect and respond to malicious behaviors and incidents, because even the best preventative controls will not prevent all incidents.”

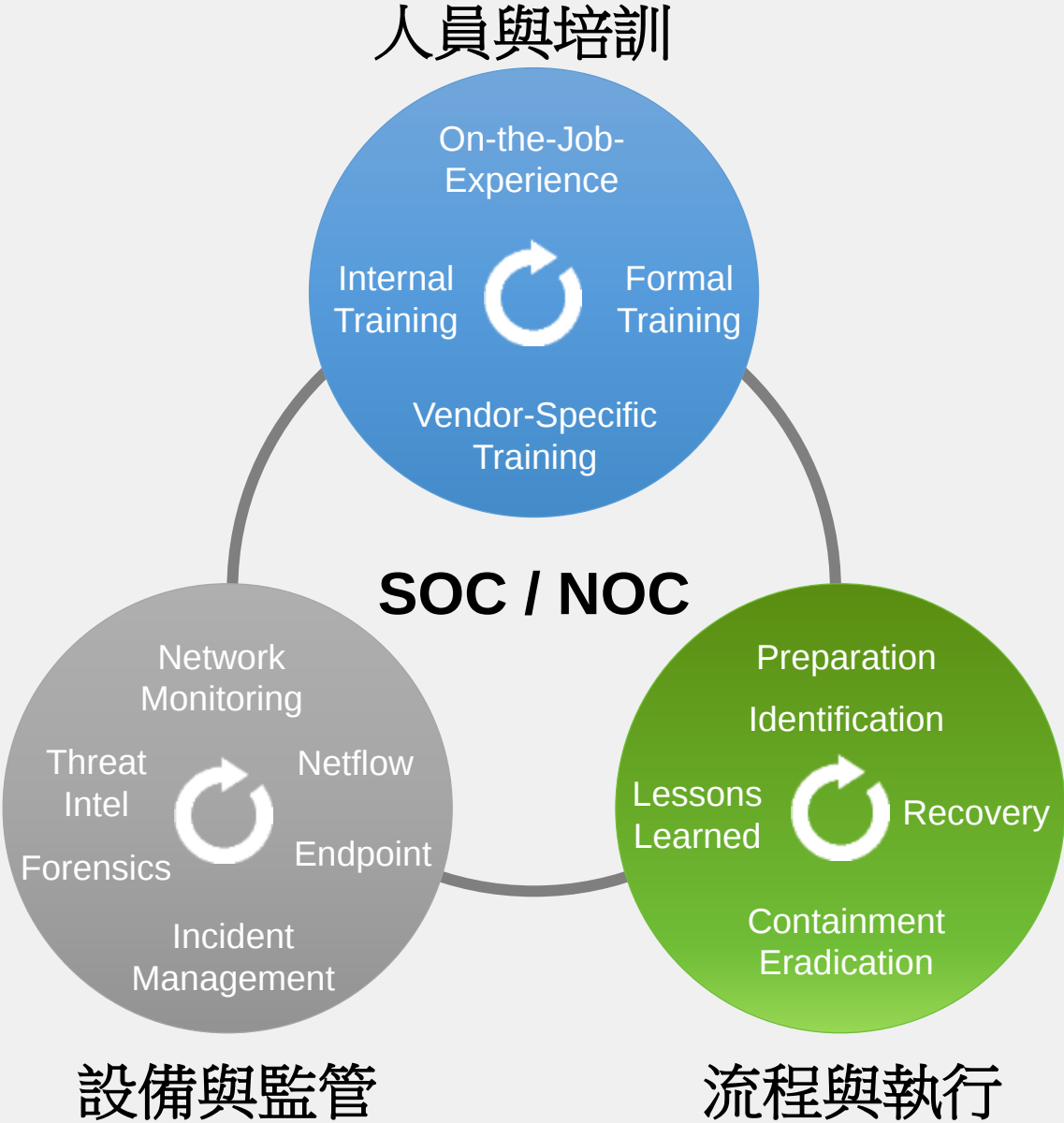
Application Performance Monitoring and Application Security Monitoring Are Converging

Published: 25 April 2017 ID: G00324828

Analyst(s): *Cameron Haight* | *Neil MacDonald*

“...an end user doesn't care if their application service problems are performance or security-related. In other words, high CPU utilization, a SQL injection attack or a denial of service (DoS) attack can result in service degradation.”





傳統的 SIEM vs. 新一代的 SIEM

NOC/SOC
TODAY

Skilled Personnel

Collect Logs

Reduce the Size if Possible

Transport to Central Location

Normalize / Enrich / Correlate

Enhanced Search Capabilities

Alert / Take Actions in Real-Time

Data Storage

Produce Reports

資安 (SOC) 與網維 (NOC) 融合式分析

設備資產、配置與效能管理 (CMDB)

可快速擴容的高彈性架構

支持多租戶管理環境

直覺式事件分析簡單易用

整合眾多設備與既有環境

單一的統合性介面管理平台

Traditional **SIEM** Capabilities

新一代的 SIEM 平台
更好的可視性 (**Visibility**) 與擴容性 (**Scalability**)
降低使用維運的複雜度 (**Less Complexity**)

資安 (SOC) 與網維 (NOC) 融合式分析

NOC/SOC
TODAY

資安 SOC 分析

Log Ingestion, Parsing and Storage

File Integrity Monitoring

Patented Log Analytics

Incident Management, Ticketing and Response

Dynamic Identity and Location Report

External Threat Feed Intelligence Integration

Reporting and Compliance – Built in/Custom

Rule and Statistical Anomaly Based Reporting

網維 NOC 分析

Real-Time Infrastructure Discovery CMDB

Network and Interface Utilization

CPU, Memory, Disk Performance Monitoring

Availability Monitoring

Storage Monitoring

Change monitoring – config., installed software

Infrastructure and User Application Monitoring

Synthetic Transaction Monitoring

Cross Correlated in Real-Time

設備資產、配置管理資料庫 (CMDB)

NOC/SOC
TODAY



設備識別分類



運行效能監控

Date	Type/File Name
03:49:00 04/26/2017	running-config
03:46:34 04/26/2017	running-config
03:46:34 04/26/2017	startup-config

設定配置保存



應用導向管理



威脅交查比對



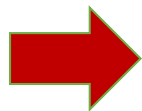
設備資產統整

新一代 SIEM 分散式架構主要構成元件

NOC/SOC
TODAY



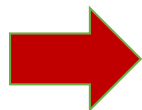
SUPERVISOR



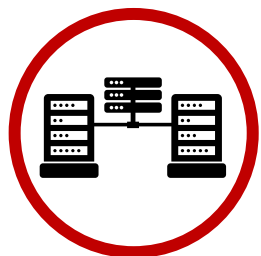
SIEM 系統核心功能，單一使用者介面、
CMDB 資料庫與報表管理



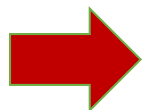
WORKERS



分散式運算協作節點，可橫向擴充 SIEM
系統，提升資料關聯分析效能



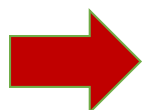
COLLECTORS



分散式資料收集節點，設備探索與分類，
資料解譯、正規化、壓縮與加密傳輸



WINDOWS AGENTS

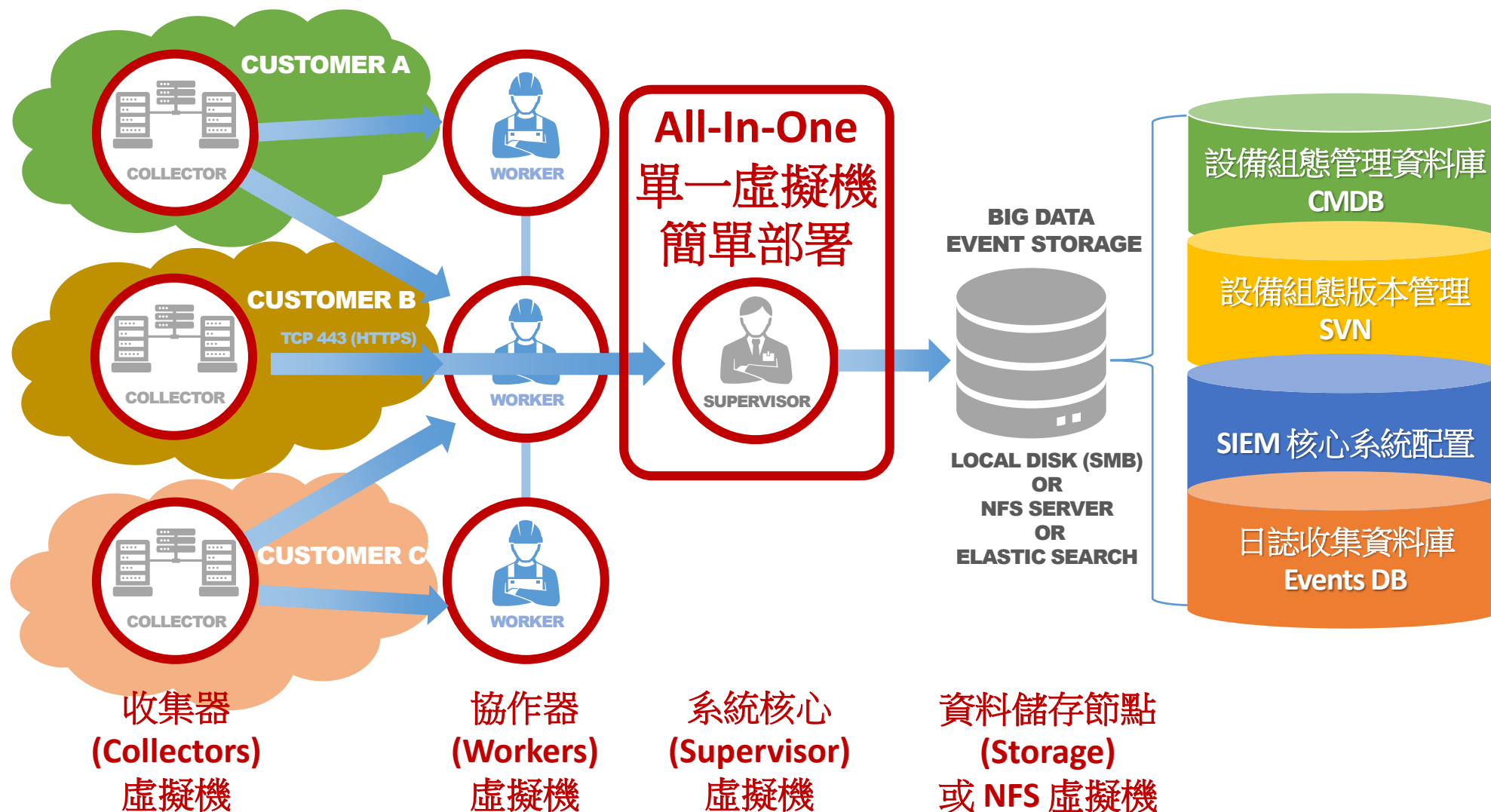


針對 WINDOWS 系統提供更方便有效的
日誌收集代理程式

可快速擴容的高彈性架構 Rapid Scale Architecture

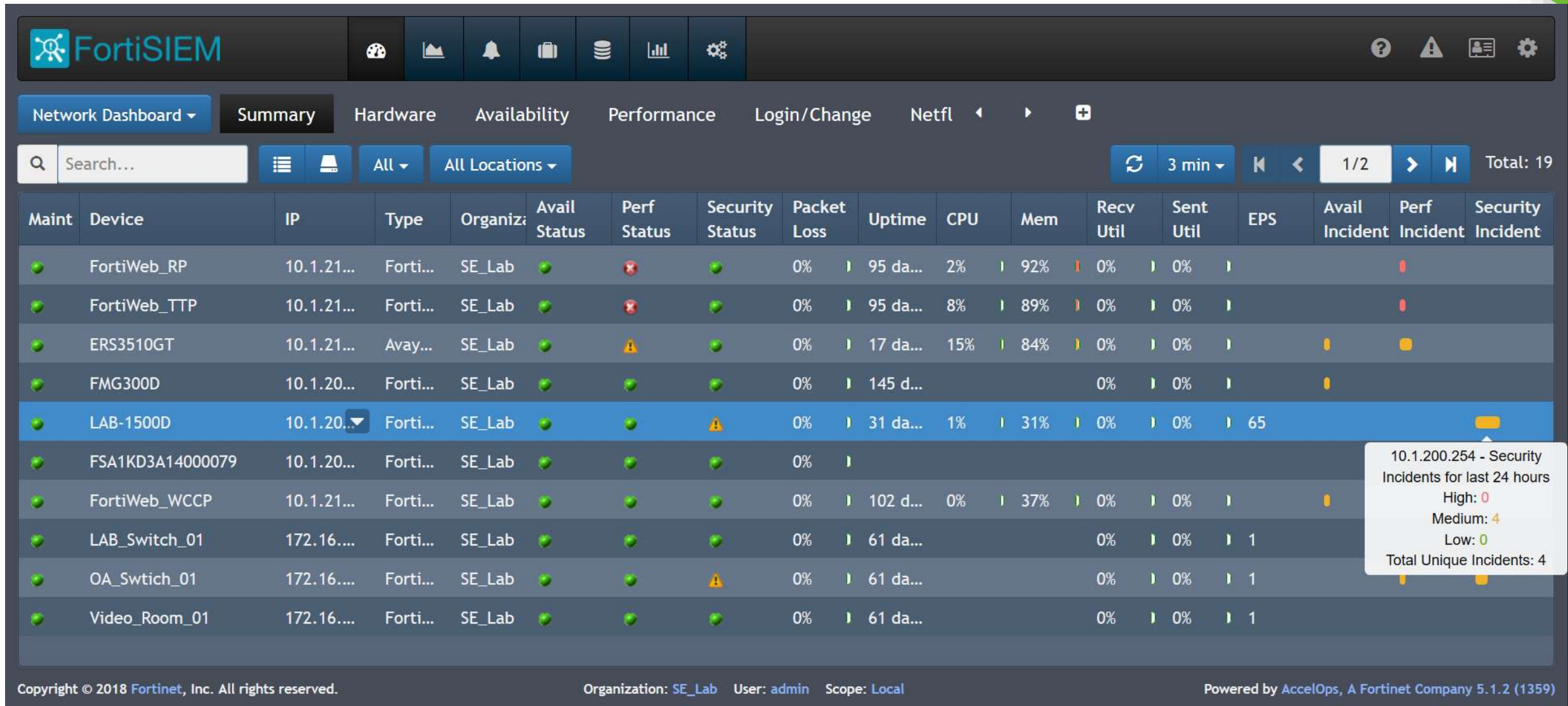
NOC/SOC
TODAY

- 支援多租戶資安服務管理部署 (Managed Security Service Provider)



SOC 與 NOC 的融合分析： 設備資安、效能狀態彙總表 (Network Summary Dashboard)

NOC/SOC
TODAY



SOC 與 NOC 的融合分析： 自動 IP、MAC、User、Location 關聯分析

NOC/SOC
TODAY

The screenshot shows the FortiSIEM Identity & Location Dashboard. The table displays network data with columns for IP Address, MAC Address, User, Host Name, Domain, VLAN ID, Connected to, First Seen, Last Seen, and Organization. Red boxes highlight specific columns, and red arrows point from text boxes to these columns, indicating data sources.

IP Address	MAC Address	User	Host Name	Domain	VLAN ID	Connected to	First Seen	Last Seen	Organization
10.10.1.120	98:E0:D9:8B:E3:23		JaniedeAir-2			OA-600D.fortinet.com .tw 192.168.1.254	Dec 26, 2018 2:24:45 PM	Jan 9, 2019 8:19:06 PM	SE_Lab
10.1.206.151	90:6C:AC:29:FE:28		FG800D3915800145				Dec 19, 2018 3:57:45 PM	Jan 9, 2019 8:19:36 PM	SE_Lab
10.1.200.242	00:50:56:ba:47:86	kevin (Domain)	WIN7B.fortinet.com.tw	FORTINET	1	ERS3510GT 10.1.210.35 (ifc4 (Slot: 1 Port: 4))	Dec 17, 2018 12:28:19 AM	Jan 9, 2019 8:34:30 PM	Super/Local
10.1.206.192	00:D9:1C:...						Dec 5, 2018 12:03:03 PM		SE_Lab
10.1.206.194	8:D6:9F:...						Dec 5, 2018 12:03:25 PM		SE_Lab
10.30.1.107	00:00:00:2e:05:68		LA-100-4PIG5MC0			00D.fortinet.com .tw 192.168.1.254	Jan 3, 2019 12:52:46 PM		SE_Lab
10.30.1.105	f0:18:98:50:ff:48		zhangheeMacBook			OA-600D.fortinet.com .tw 192.168.1.254	Jan 3, 2019 3:02:24 PM	Jan 3, 2019 3:02:24 PM	SE_Lab
10.30.1.105	F0:18:98:50:FF:48		zhangheeMacBook			OA-600D.fortinet.com .tw 192.168.1.254	Jan 7, 2019 5:12:21 PM	Jan 7, 2019 5:12:53 PM	SE_Lab
42.74.77.177		marty (VPN)		10.1.200.254			Jan 4, 2019 2:08:50 PM	Jan 4, 2019 2:08:50 PM	SE_Lab
10.30.1.102	34:36:3b:cd:f1:4a		Spencerteki-MBP			OA-600D.fortinet.com .tw 192.168.1.254	Jan 3, 2019 1:49:23 PM	Jan 3, 2019 2:44:01 PM	SE_Lab

From DHCP Logs

From AD Logon Logs

From L2 Switches Discovery

From ALL Relevant Logs

Copyright © 2018 Fortinet, Inc. All rights reserved. Organization: Super User: admin Scope: Global Powered by AccelOps, A Fortinet Company 5.1.1 (1357)

直覺式的事件關聯分析處理： 以人為本的操作邏輯，簡單易用，減輕人員負擔

NOC/SOC
TODAY

FortiSIEM

DASHBOARD ANALYTICS INCIDENTS CASES CMDB RESOURCES ADMIN

Actions [1] Raw Messages

Reporting IP IN Devices: Firewall AND Event Type

定義想關聯分析甚麼?

Filters

Paren	Attribute	Operator	Value	Paren	Next	Row
+	Reporting IP	IN	Devices: Firewall	+	AND	+
+	(			+	OR	+
+	Event Type	CONTAIN	FortiGate-auth	+	OR	+
+	Event Type	CONTAIN	FortiGate-webfilter	+	OR	+
+	Event Type	CONTAIN	FortiGate-event	+	OR	+
+	Event Type	CONTAIN	FortiGate-antivirus	+	OR	+
+	Event Type	CONTAIN	FortiGate-ips-	+	OR	+

Time: ☒ Real Time ☐ Relative Last 1 Hour ☐ Absolute

Save & Run Save Cancel

Organization: Super User: admin Scope: Global

Powered by AccelOps, A Fortinet Company 5.1.1 (1357)

直覺式的事件關聯分析處理： 以人為本的操作邏輯，簡單易用，減輕人員負擔

NOC/SOC
TODAY

FortiSIEM

DASHBOARD ANALYTICS INCIDENTS CASES CMDB RESOURCES ADMIN

Actions [1] Raw Messages

Edit Filters and Time Range...

Define how to display analysis results?

Display Fields

Clear All

Attribute	Order	Display As	Row	Move
Event Severity			+	↑
			-	↓
Source IP			+	↑
			-	↓
Destination IP			+	↑
			-	↓
COUNT(Matched Events)			+	↑
			-	↓

Save & Run Save Cancel

0/0 0

https://10.1.200.171/phoenix/html/#

Organization: Super User: admin Scope: Global

Powered by AccelOps, A Fortinet Company 5.1.1 (1357)

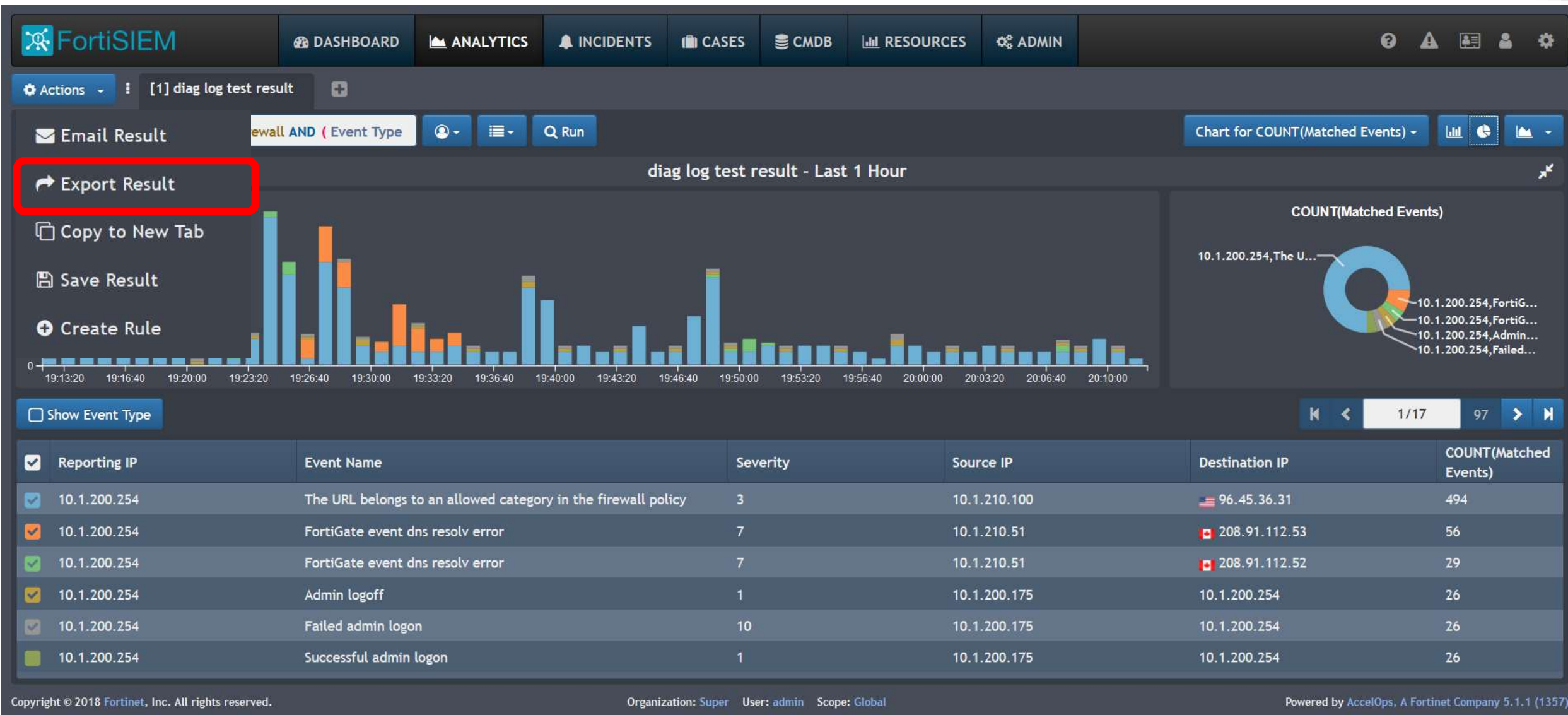
直覺式的事件關聯分析處理： 以人為本的操作邏輯，簡單易用，減輕人員負擔

NOC/SOC
TODAY



直覺式的事件關聯分析處理： 分析結果可輸出報表（手動或排程）

NOC/SOC
TODAY



直覺式的事件關聯分析處理： 分析結果可輸出報表（手動或排程）

NOC/SOC
TODAY



FORTINET



diag log test result - 11:19:40 PM Jan 08 2019

Organization : Super/Global

Report Start Time : Jan 08 2019, 10:25:43 PM CST

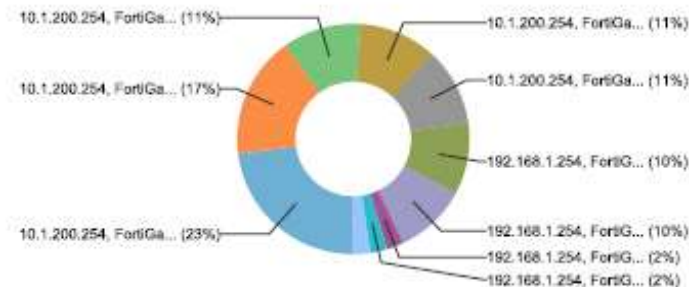
Report End Time : Jan 08 2019, 11:25:42 PM CST

Generated On : Jan 08 2019, 11:26:02 PM CST

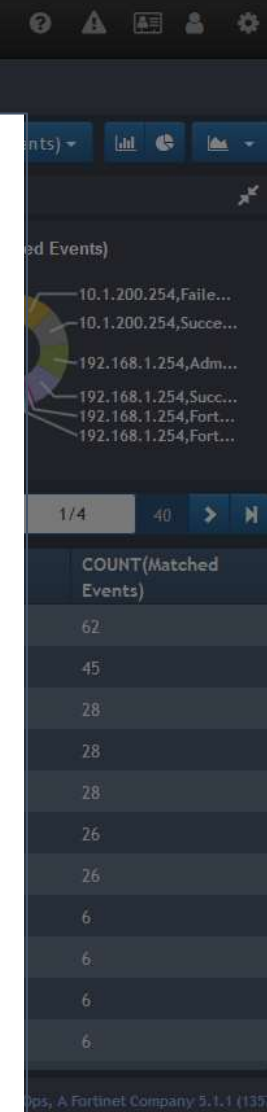
Device Time Zone : Asia/Taipei

1 log test events analysis

Donut Chart for COUNT(Matched Events) in diag log test result - 11:19:40 PM Jan 08 2019



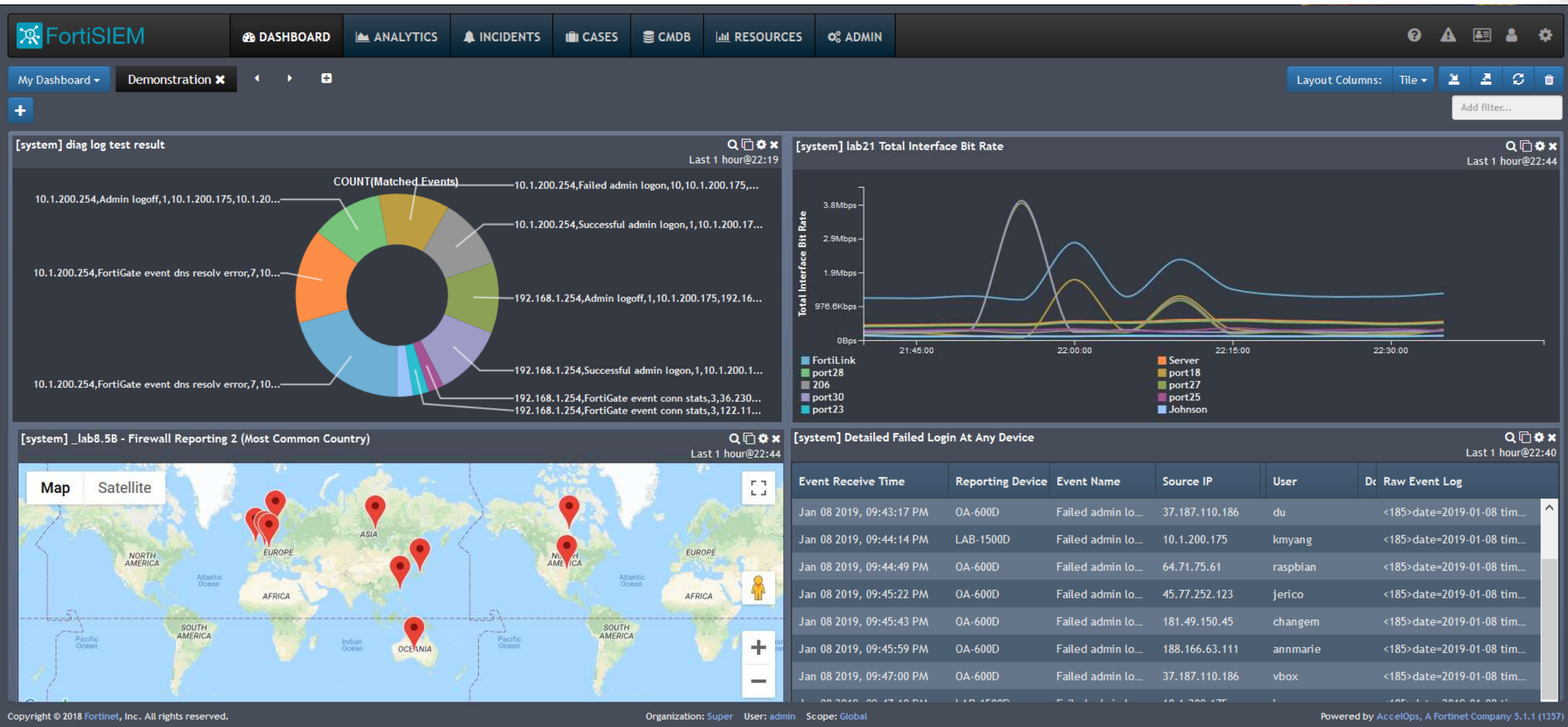
Rank	Reporting IP	Event Type	Event Name	Event Severity	Source IP	Destination IP	COUNT(Matched Events)
1	10.1.200.254	FortiGate event: dns resolve error	FortiGate event: dns resolve error	7	10.1.210.51	208.91.112.52	53
2	10.1.200.254	FortiGate event: dns resolve error	FortiGate event: dns resolve error	7	10.1.210.51	208.91.112.53	44
3	10.1.200.254	FortiGate event: admin logout	Admin logout	1	10.1.200.115	10.1.200.254	28
4	10.1.200.254	FortiGate event: login failure	Failed admin login	10	10.1.200.115	10.1.200.254	28
5	10.1.200.254	FortiGate event: login success	Successful admin login	1	10.1.200.115	10.1.200.254	28
6	192.168.1.254	FortiGate event: admin logout	Admin logout	1	10.1.200.115	192.168.190.1	26
7	192.168.1.254	FortiGate event: login success	Successful admin login	1	10.1.200.115	192.168.190.1	26
8	192.168.1.254	FortiGate event: conn status	FortiGate event: conn status	3	30.230.12.25	60.250.130.67	6
9	192.168.1.254	FortiGate event: conn status	FortiGate event: conn status	3	122.116.185.134	60.250.130.67	6
10	192.168.1.254	FortiGate event: conn status	FortiGate event: conn status	3	193.07.150.66	60.250.130.67	6



**NOC/SOC
TODAY**

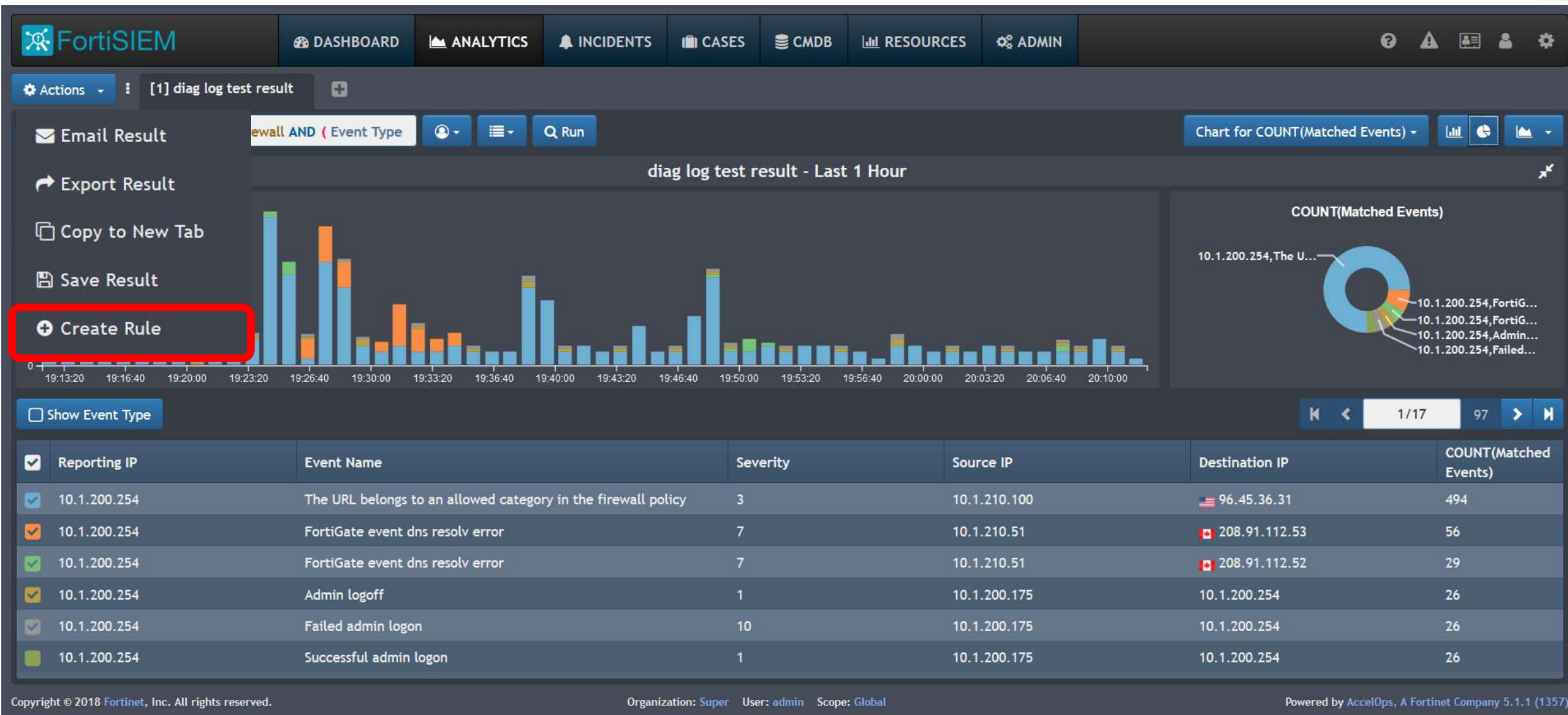
直覺式的事件關聯分析處理： 分析結果可轉成各式監看儀表板

NOC/SOC
TODAY



直覺式的事件關聯分析處理： 分析結果可產生規則，觸發事故告警

NOC/SOC
TODAY



直覺式的事件關聯分析處理： 分析結果可產生規則，觸發事故告警

NOC/SOC
TODAY

FortiSIEM

DASHBOARD

Actions

[1] diag log test result

Reporting IP IN Devices: Firewall AND (Event Type

22:16:40

22:20:00

22:23:20

22:26:40

22:30:00

Show Event Type

Reporting IP

Event N

10.1.200.254

FortiGat

10.1.200.254

FortiGat

10.1.200.254

Admin lo

10.1.200.254

Failed a

10.1.200.254

Success

192.168.1.254

Admin lo

192.168.1.254

Success

192.168.1.254

FortiGat

192.168.1.254

FortiGat

192.168.1.254

FortiGate e

192.168.1.254

FortiGate e

Create Rule

Edit SubPattern

Name: Filter_1

Filters:	Paren	Attribute	Operator	Value	Paren	Next	Row
	+ -	Reporting IP	IN	Devices: Firewall	+ -	AND	+ -
	+ -	(Event Type	CONTAIN	FortiGate-auth	+ -	OR	+ -
	+ -	Event Type	CONTAIN	FortiGate-webfilter	+ -	OR	+ -
	+ -	Event Type	CONTAIN	FortiGate-event	+ -	OR	+ -

Aggregate:	Paren	Attribute	Operator	Value	Paren	Next	Row
	+ -	COUNT(Matched Events)	>=	1	+ -		+ -

Group By:

Attribute	Row	Move
Reporting IP	+ -	↑ ↓
Event Type	+ -	↑ ↓
Event Severity	+ -	↑ ↓

Save

Save as Report

Run as Query

Cancel

自動帶入關聯
分析條件

關聯規則
觸發閥值

Chart for COUNT(Matched Events)

COUNT(Matched Events)

10.1.200.254,Admi...

10.1.200.254,Fail...

10.1.200.254,Succ...

192.168.1.254,Adm...

192.168.1.254,Succ...

192.168.1.254,Fort...

10.1.200.254,Forti...

192.168.1.254,Fort...

192.168.1.254,Fort...

10.1.200.254,Admi...

1.112.52

1.112.53

.254

.254

.254

.254

198.1

198.1

30.67

30.67

60.250.130.67

60.250.130.67

COUNT(Matched Events)

62

45

28

28

28

26

26

6

6

6

6

Copyright © 2018 Fortinet, Inc. All rights reserved.

Organization: Super User: admin Scope: Global

Powered by AccelOps, A Fortinet Company 5.1.1 (1357)

內建豐富的關聯規則與用戶終端行為分析 (UEBA) 以用戶登入模式異常為例 (Sudden User Login Pattern Change)

NOC/SOC
TODAY

FortiSIEM

DASHBOARDANALYTICSINCIDENTSCASESCMDBRESOURCESADMIN

ReportsRulesNetworksWatch ListsProtocolsEvent TypesMalware DomainsMalware IPsMalware URLsMalware ProcessesCountry GroupsMalware HashDefault PasswordAnonymity NetworkUser AgentsRemediations

Resources > Rules

NewEditDeleteCloneTestSearch...

ImportExportSystem37/46688

Active	Name	Description	Exceptions	Scope	Test Status
☒	(s) Sudden Increase in User Login Volume			System	
☒	(s) Sudden Increase in WMI Response Times	Detects a sudden 50% increase of WMI Response Times over a 30 minute time window		System	
☒	(s) Sudden User Location Change	Detects location change for a user unfeasible in the period of time. This may indicate a stolen credential.		System	
☒	(s) Sudden User Login Pattern Change	Detects daily user login distribution anomaly against profile. This may indicate suspicious user behaviors.		System	
☒	(s) Suspicious Botnet like End host DNS Behavior	Detects an end host meeting at least 3 requirements for suspicious use of DNS requests - this indicates that a bot is likely running on the end host		System	
☒	(s) Suspicious Control Panel DLL Load	Detects suspicious Rundll32 execution from control.exe as used by Equation Group and Exploit Kits. This rule requires Windows sysmon events collected via FortiSIEM Advanced Windows Agent.		System	
☒	(s) Suspicious Database Logon	Detects suspicious database logon - success or failure. This includes multiple login failures, privileged logins, brute force successful logins		System	
☒	(s) Suspicious Linux SSHD Errors	Detects suspicious SSH / SSHD error messages that indicate a fatal or suspicious error that could be caused by exploit attempts		System	
☒	(s) Suspicious Linux VSFTPD Errors	Detects suspicious VSFTPD error messages that indicate a fatal or suspicious error that could be caused by exploit attempts		System	
☒	(s) Suspicious Linux log entries	Detects suspicious entries in linux syslog		System	

Copyright © 2018 Fortinet, Inc. All rights reserved.

Organization: Super User: admin Scope: Global

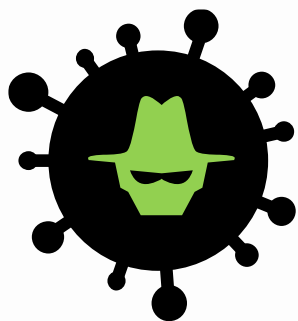
Powered by AccelOps, A Fortinet Company 5.1.1 (1357)

內建支援眾多廠牌設備

NOC/SOC
TODAY

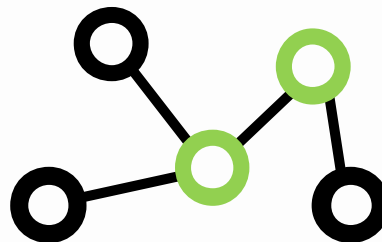


與外部威脅 情報整合



- Malware Domain, IP, File hash, User Agent, URL
- Real-time/Historical query
- Out-of-the-box support

與報修派工系統和 作業流程整合



- Build-in or Integrate with External Ticket System
- 2-way integration
- API / GUI based integration

與雲端應用 系統整合



- Okta – SSO
- Kafka – Big Data
- Box – Document sharing
- Salesforce – CRM Activity

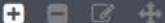
與外部威脅情資整合

NOC/SOC
TODAY









Resources > Malware IPs > Emerging Threat Malware IP

NewEditDeleteMore

 Search...

Last updated at Feb 18, 2019 4:06:01 PM

Active	Low IP	Update	Country	Description	Date Found
☒	1.10.16.0	Bulk enable			
☒	1.32.128.0	Bulk disable			
☒	100.42.20.148				
☒	101.187.14.253				
☒	101.192.0.0				
☒	101.200.81.187				
☒	101.202.0.0				
☒	101.203.128.0				
☒	101.248.0.0				
☒	101.252.0.0				

Event Types

Malware Domains

Malware IPs

- Emerging Threat Malware IP
 - Zeus Malware IP
 - ThreatStream Malware IP
 - Hail-A-TAXII Malware IP
 - FortiGuard Malware IP
 - Ungrouped

Malware URLs

Malware Processes

Country Groups

Copyright © 2018 Fortinet, Inc. All rights reserved.

Organization: Super User: admin Scope: Global

Powered by AccelOps, A Fortinet Company 5.1.2 (1359)

**NOC/SOC
TODAY**

即時事故反應與處理：以內網連線外部高風險 IP 地址告警為例 登入系統

NOC/SOC
TODAY



USER ID:

PASSWORD:

CUST/ORG ID:

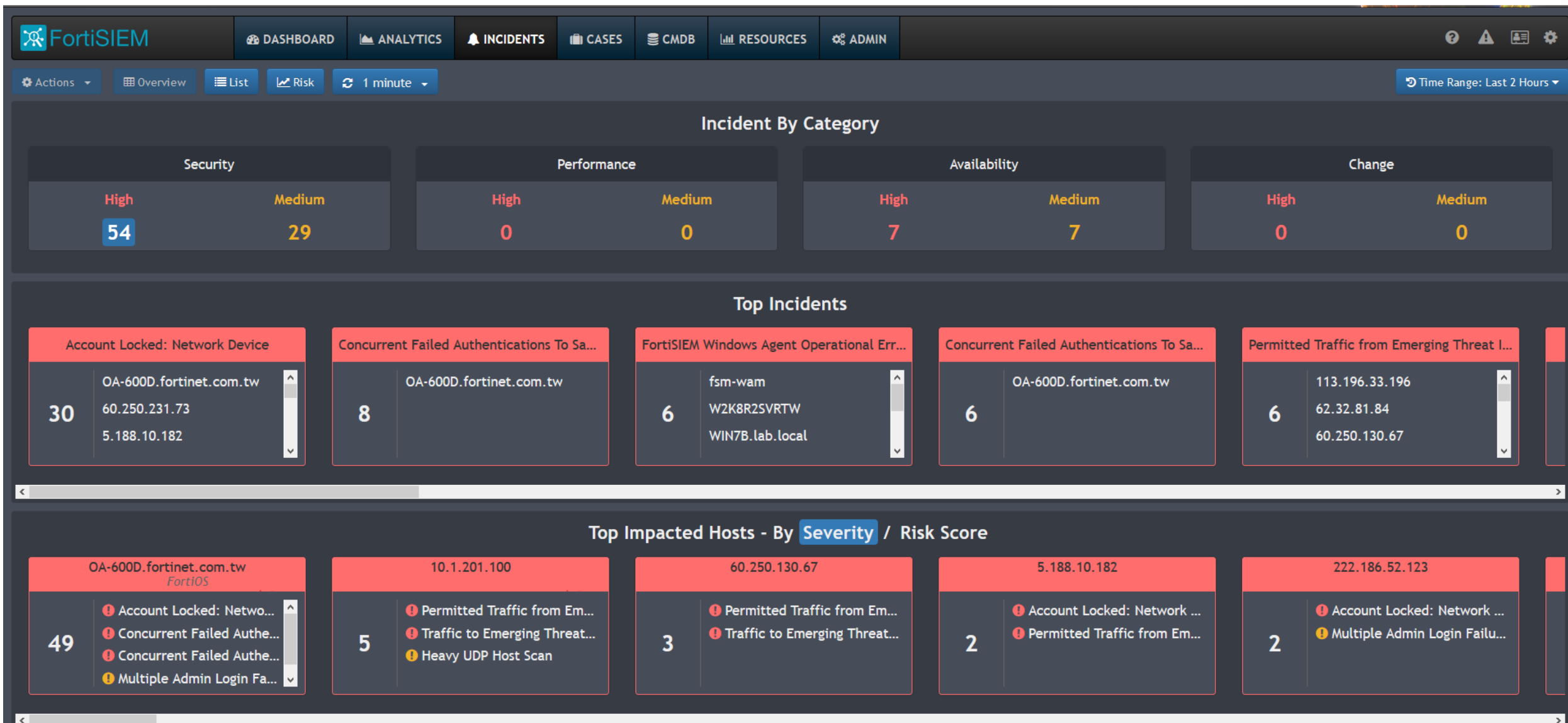
DOMAIN:

LOG IN



即時事故反應與處理：以內網連線外部高風險 IP 地址告警為例 事故彙整儀表板 (Incidents Overview Dashboard)

NOC/SOC
TODAY



即時事故反應與處理：以內網連線外部高風險 IP 地址告警為例

點擊進入查看事故詳情

NOC/SOC
TODAY

FortiSIEM

DASHBOARDANALYTICSINCIDENTSCASESCMDBRESOURCESADMIN

ActionsOverviewListRisk1 minute

2/352

Security Incidents: HIGH: 52MEDIUM: 29LOW: 0

	Last Occurred	Incident	Reporting	Source	Target	Detail
	Jul 19 2018, 11:48:30 PM	Concurrent Failed Authentications To Same Account From Multiple Countries	OA-600D		192.168.1.254 User: support	
	Jul 19 2018, 11:48:30 PM	Concurrent Failed Authentications To Same Account From Multiple Cities	OA-600D		OA-600D 192.168.1.254 User: support	
	Jul 19 2018, 11:45:00 PM	Account Locked: Network Device	OA-600D	212.253.83.214	OA-600D 192.168.1.254	Triggered Event Count: 1
	Jul 19 2018, 11:45:00 PM	Account Locked: Network Device	OA-600D	46.8.117.95	OA-600D 192.168.1.254	Triggered Event Count: 1
	Jul 19 2018, 11:44:30 PM	Concurrent Failed Authentications To Same Account From Multiple Cities	OA-600D		OA-600D 192.168.1.254 User: guest	
	Jul 19 2018, 11:42:30 PM	Permitted Traffic from Emerging Threat IP List		159.151.129.61	10.1.201.100	
	Jul 19 2018, 11:42:30 PM	Traffic to Emerging Threat IP List	LAB-1500D	10.1.201.100	159.151.129.61	
	Jul 19 2018, 11:38:00 PM	Account Locked: Network Device	OA-600D	60.250.246.222	OA-600D 192.168.1.254	Triggered Event Count: 1
	Jul 19 2018, 11:37:00 PM	Permitted Traffic from Emerging Threat IP List		5.188.10.182	113.196.33.196	
	Jul 19 2018, 11:37:00 PM	Account Locked: Network Device	OA-600D	5.188.10.182	OA-600D 192.168.1.254	Triggered Event Count: 1
	Jul 19 2018, 11:37:00 PM	Account Locked: Network Device	OA-600D	125.5.20.230	OA-600D 192.168.1.254	Triggered Event Count: 1
	Jul 19 2018, 11:36:30 PM	Account Locked: Network Device	OA-600D	201.68.109.61	OA-600D	Triggered Event Count: 1

DetailsEventsRuleAuto expand

即時事故反應與處理：以內網連線外部高風險 IP 地址告警為例 可開事故處理單進行處理

NOC/SOC
TODAY

FortiSIEM | DASHBOARD | ANALYTICS | INCIDENTS | CASES | CMDB | RESOURCES | ADMIN

Actions | Overview | List | Risk | 1 minute

Display

- Clear Incident
- Disable Rule
- Edit Comment
- Export Incident
- Edit Rule
- Edit Rule Exception
- Create Event Dropping Rule
- Notify via Email
- Remediate Incident
- Create Ticket**
- Show Notification History
- Show Ticket History
- External Integration...

Incident

HIGH: 52 MEDIUM: 52

New Ticket

Incident ID(s): 11587 Mode: Create a new ticket

Summary: Traffic to Emerging Threat IP List, In LAB-1500D(10.1.200.254)

State: Assigned Assignee: admin (knyang@fortinet.com)

Escalation: Ticket Delay Escalation Priority: Medium

Due Date: 07/21/2018 00:42:31 Attachment:

CC:

Description: Incident Name => Traffic to Emerging Threat IP List
Incident Source => IP Address:10.1.201.100,
Incident Target => LAB-1500D(10.1.200.254)
Incident Detail =>
Noted: Please follow SOP and take Incident Response immediately.

Cancel Save

Case overdue notification

預計完成時間

指派處理人員

自動帶入事故資訊

Event Type	Event
Concurrent Failed Authentication	10.1.200.254
Permitted Traffic from Emerging Threat IP List	10.1.201.100
Traffic to Emerging Threat IP List	10.1.201.100
Account Locked: Network Device	10.1.200.254

Raw Event Log

<189>date=2018-07-19 time=23:42:21 devname="LAB-1500D" devid="FG1K5D3114803"

即時事故反應與處理：以內網連線外部高風險 IP 地址告警為例 系統內建派工處理系統，可追蹤事故處理進度

NOC/SOC
TODAY



DASHBOARD

ANALYTICS

INCIDENTS

CASES

CMDB

RESOURCES

ADMIN

New

Edit

Add filter...

Time Range *LAST 30 Days*

↺

Export

Elapsed	State	Priority	Ticket ID	Summary	Assignee	Creator	Creation Date
Overdue	Assigned	Medium	4780051	Permitted Traffic from Emerging Threat IP List, in (1...	admin	admin <kmyang@fortinet.com>	Jul 11 2018, 08:20:58 PM
54 %	Assigned	High	4780052	Permitted Traffic from Emerging Threat IP List,destl...	admin	admin <kmyang@fortinet.com>	Jul 19 2018, 11:26:52 AM
0 %	Assigned	Medium	6156150	Traffic to Emerging Threat IP List, in LAB-1500D(10.1...	admin	admin <kmyang@fortinet.com>	Jul 20 2018, 12:46:12 AM

Detail

Incident ID: 11587

Organization: SE_Lab

Due Date: Jul 21 2018, 12:42:31 AM

Escalation Policy: Ticket Delay Escalation

CC:

Attachment:

Action History

SE_Lab/admin Jul 20 2018, 12:46:12 AM

Add notes: Incident Name => Traffic to Emerging Threat IP List
Incident Source => IP Address:10.1.201.100,
Incident Target => LAB-1500D(10.1.200.254)
Incident Detail =>

Noted: Please follow SOP and take Incident Response Immediately.

即時事故反應與處理：以內網連線外部高風險 IP 地址告警為例 被指派人員可迅速反應處理

NOC/SOC
TODAY

FortiSIEM

DASHBOARDANALYTICSINCIDENTSCASESCMDBRESOURCESADMIN

Actions

Overview

List

Risk

1 minute

Display

Clear Incident

Disable Rule

Edit Comment

Export Incident

Edit Rule

Edit Rule Exception

Create Event Dropping Rule

Notifv via Email

Remediate Incident

Create Ticket

Show Notification History

Show Ticket History

External Integration...

1/3

54

HIGH: 54

MEDIUM: 30

LOW: 0

Incident	Reporting	Source	Target	Detail
Account Locked: Network Device	OA-600D	222.186.52.123	OA-600D 192.168.1.254	Triggered Event Count: 1
Concurrent Failed Authentications To Same Account From Multiple Cities	OA-600D		OA-600D 192.168.1.254 User: admin	
Concurrent Failed Authentications To Same Account From Multiple Cities	OA-600D		OA-600D 192.168.1.254 User: root	
Account Locked: Network Device	OA-600D	60.250.246.222	OA-600D 192.168.1.254	Triggered Event Count: 1
Permitted Traffic from Emerging Threat IP List		111.37.21.69	113.196.33.196	
Traffic to Emerging Threat IP List	LAB-1500D	10.1.201.100	196.196.193.44	

Details

Events

Rule

Auto expand

Incident ID: 7402

Biz Service:

Notification Recipients:

First Occurred: May 29 2018, 10:05:30 PM

Notification:

External Resolve Time:

View Status: Read

Incident Type: PH_RULE_TO_EMERGING_THREAT_IP

Count: 48

Cleared Reason:

Reporting IP: 10.1.200.254

Cleared User:

External Ticket ID:

Raw Event Log:

Incident Status: Active

Cleared Time: N/A

Incident Comments:

Ticket ID:

External User:

External Ticket State:

Ticket Status: N/A

Ticket User:

Severity: 9

Organization: SE_Lab

External Cleared Time: N/A

External Ticket Type:

即時事故反應與處理：以內網連線外部高風險 IP 地址告警為例 被指派人員可迅速反應處理

NOC/SOC
TODAY

FortiSIEM

DASHBOARDANALYTICSINCIDENTSCASESCMDBRESOURCESADMIN

ActionsOverviewListRisk1 minute

Last OccurredIncident

	Jul 20 2018, 12:49:30 AM	Server Disk Latency Critical			
	Jul 20 2018, 12:48:30 AM	End User DNS Queries to Unauthorized DNS Ser			
	Jul 20 2018, 12:44:30 AM	Large Outbound Transfer	10.1.206.100		
	Jul 20 2018, 12:44:30 AM	Large Outbound Transfer To Outside My Country	10.1.206.100		
	Jul 20 2018, 12:43:30 AM	Account Locked: Network Device	OA-600D	60.250.246.222	
	Jul 20 2018, 12:43:30 AM	Permitted Traffic from Emerging Threat IP List		111.37.21.69	
	Jul 20 2018, 12:43:00 AM	Permitted Traffic from Emerging Threat IP List		196.196.193.44	
	Jul 20 2018, 12:43:00 AM	Traffic to Emerging Threat IP List	LAB-1500D	10.1.201.100	196.196.193.44

Run Remediation

Enforce On: Device: LAB-1500D

Remediation: Fortinet FortiOS - Block IP FortiOS 5.4

Run On: Super

RunCancel

3/6101

Target	Detail
10.1.200.242 WIN7B	Disk Name: C:\ Disk Read Latency ms: 68.76ms Disk Write Latency ms: 0.81ms
	Triggered Event Count: 10
208.91.113.183	Sent Bytes: 26.77 MB
208.91.113.183	Sent Bytes: 23.62 MB
OA-600D 192.168.1.254	Triggered Event Count: 1
113.196.33.196	
10.1.201.100	
196.196.193.44	

DetailsEventsRule

Auto expand

Incident ID: 7402

Biz Service:

Notification Recipients:

First Occurred: May 29 2018, 10:05:30 PM

Notification:

External Resolve Time:

View Status: Read

Incident Type: PH_RULE_TO_EMERGING_THREAT_IP

Count: 48

Cleared Reason:

Reporting IP: 10.1.200.254

Cleared User:

External Ticket ID:

Raw Event Log:

Incident Status: Active

Cleared Time: N/A

Incident Comments:

Ticket ID:

External User:

External Ticket State:

Ticket Status: N/A

Ticket User:

Severity: 9

Organization: SE_Lab

External Cleared Time: N/A

External Ticket Type:

即時事故反應與處理：以內網連線外部高風險 IP 地址告警為例 自動通報與設備自動聯防處理流程

NOC/SOC
TODAY

FortiSIEM

DASHBOARD ANALYTICS INCIDENTS CASES CMDB RESOURCES ADMIN

Setup Device Support Health License General Settings

System Analytics Discovery Monitoring Event Handling Notification Role Escalation

New Edit Delete Clone Search... Columns

Enabled

Notification Policy

Severity: ☒ Low ☒ Medium ☒ High

Rules: RULE:Traffic to Emerging Threat IP List

Time Range: ANY

Affected Items: ANY

Actions:

- ☒ Send Email/SMS to the target users.
- ☒ Run Remediation/Script.
- ☐ Send SNMP message to the destination set in Admin > General Settings > Analytics.
- ☐ Send XML file over HTTP(S) to the destination set in Admin > General Settings > Analytics.
- ☐ Open Remedy ticket using the configuration set in Admin > General Settings > Analytics.

Settings:

- ☐ Do not notify when an incident is cleared automatically.
- ☐ Do not notify when an incident is cleared manually.
- ☒ Do not notify when an incident is cleared by system.

Comments:

Save Cancel

自動通報設定

自動腳本執行設定

Copyright © 2018 Fortinet, Inc. All rights reserved. Organization: SE Lab User: admin Scope: Local Powered by AccelOps - A Fortinet Company 5.0.1 (1203)

1. 資安(SOC)與網維(NOC)融合式分析
2. 設備資產、配置與效能管理(CMDB)
3. 可快速擴容的高彈性架構
4. 直覺式事件分析簡單易用
5. 支持多租戶管理環境
6. 整合眾多設備與既有環境



7. 單一的統合性介面管理平台

The logo for FERTINET is displayed in a bold, white, sans-serif typeface. The letter 'F' is stylized with three horizontal bars. The letters 'E' and 'R' also feature horizontal bars. A registered trademark symbol (®) is positioned to the upper right of the final 'T'. The logo is centered horizontally against a solid blue background.

FERTINET®