Flowmon
Networks

Security Use-Case
User Account Compromise

1200+ customers in 45+ countries

orange™ SIEMENS EQUINIX SEGA® KBC

Gartner recognized in NPMD & NDR

Gartner peerinsights™ 4.9 / 5

Network Detection and Response

Gather

Flowmon collects network application telemetry data from a variety of sources including your existing network devices and our own sensors.

Analyze

The data is then processed using machine learning, heuristics and advanced algorithms.

Real-time

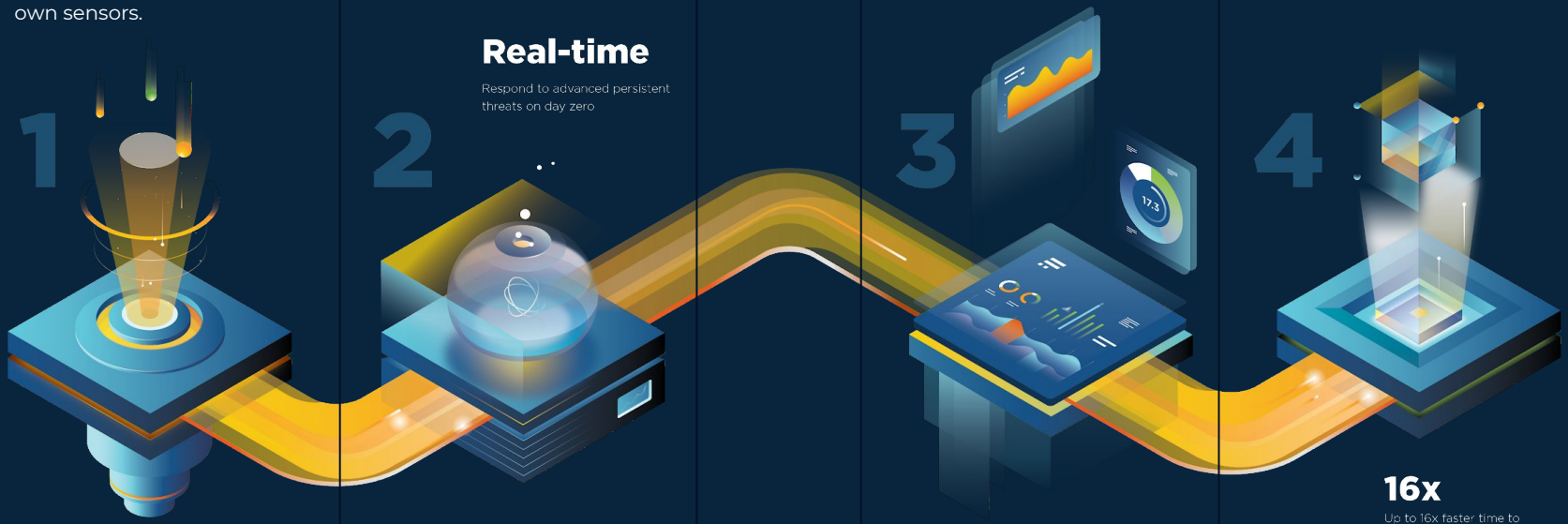
Respond to advanced persistent threats on day zero

Understand

Relevant information is extracted and visualized on the dashboard.

Act

The user sees the big picture. The most important and relevant information is clear and noise-free.



16x

Up to 16x faster time to resolution reported

Flowmon

Connected flow sources: 1 of 1

Last 24 hours (generic time span)

2020-09-08 10:00 - 2020-09-09 10:00

Excellent

Last 24 hours (generic time span)

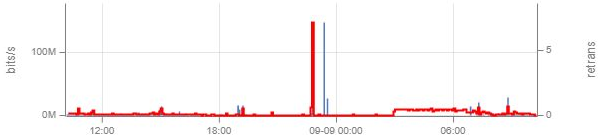
Hide details

ERP	99.812%
Intranet	97.773%

2020-09-08 10:15 - 2020-09-09 10:15

Structure of Overall Traffic

Last 24 hours (generic time span)



	Source	Maximal bits/s	Bits per second	Bytes	AVG RTR
1	127.0.0.1 (localhost)	148.0 M	2.0 M	20.29 GiB	0.1
	Total	**148.0 M**	**2.0 M**	**20.29 G...**	**0.1**

2020-09-08 10:15 - 2020-09-09 10:15

Structure of Overall Traffic

Last 24 hours (generic time span)

99.796%

Retransmission index

0% 90% 99% 99.9% 100%

Poor Excellent

AVG packets/s	AVG RTT
323.7	30.309 ms
AVG SRT	**AVG RTR**
89.557 ms	0.1

2020-09-08 10:15 - 2020-09-09 10:15

Application performance overview

Last 24 hours (generic time span)

ERP

99.812%

0% 70% 80% 90% 100%

Poor Excellent

AVG response time	Median of response time
3 ms	1 ms
95% response time	**99% response time**
16 ms	46 ms

2020-09-08 10:15 - 2020-09-09 10:15

Application performance overview

Last 24 hours (generic time span)

Intranet

97.773%

0% 70% 80% 90% 100%

Security status

Last 24 hours (generic time span)

Critical priority events: 5

Security issues

Hide details

Critical	5
High	36
Medium	31
Low	4
Info	3

Event overview by type

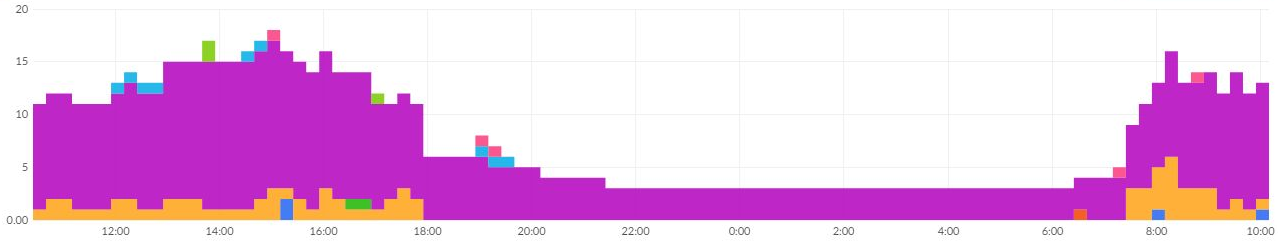
Last 24 hours (generic time span)

	Event type	Name	Number of events
1	UPLOAD	Detection of uploading data	4
2	DICTATTACK	Detection of dictionary attacks on various protocols.	1
3	DNSANOMALY	Detection of anomalies traffic	35
4	L3ANOMALY	Detection of anomalies on the third layer of OSI model.	1
5	TEAMVIEWER	Detection of TeamViewer	28
6	DNSQUERY	Detection of too many DNS queries	3
7	HIGHTRANSF	Detection of high data transfers in network	4
8	MULTICAST	Detection of IPv4 and IPv6 multicast traffic	3
	Others		**0**
	Total		**79**

Logs
About

EVENTS

Show: PRIORITIES METHODS



Methods

Type method name to filter

- UPLOAD
- DICTATTACK
- DNSANOMALY
- L3ANOMALY
- TEAMVIEWER
- DNSQUERY
- HIGHTRANSF
- MULTICAST

EVENTS BY PRIORITY

2020-09-08 10:25 - 2020-09-09 10:10

Overall events count: 79

UPLOAD

DICTATTACK 1

1 events of the type DICTATTACK from **1** source IP addresses detected

SOURCE IP ADDRESS	SOURCE IP FILTERS	EVENTS COUNT
192.168.0.33 (unknown)		

RELATED EVENTS

Detected **1** events of the type DICTATTACK from **192.168.0.33**

ID	DETECTION TIME	LAST UPDATE	DETAIL	TARGETS	DATA FEED	COMMENTS
#151715	2020-09-09 06:25:52	2020-09-09 06:30:52	Samba dictionary attack, attempts: 195, port(s): 445, attack duration: 22 s 902 ms, average time between attempts: 117 ms.	192.168.0.252	Default	

Showing 1 - 1 of 1

Showing 1 - 1 of 1

DNSANOMALY

Analysis
Events
Reports
Settings
Logs
About

Date: Custom | From: 2020-09-08 10:10 | To: 2020-09-09 10:10 | Perspective: Security issues | Data feed: -- Unspecified -- | Source IP:

ANALYSIS | EVENT #151715

Type: Dictionary attacks (DICTATTACK)

Subtype: SambaProtocol
Reports the password-guessing attacks (dictionary or brute-force based) on a Samba server. This may indicate an attacker's activity to get unauthorized access to a service or a misconfigured device that is continuously trying to authenticate to a service unsuccessfully.

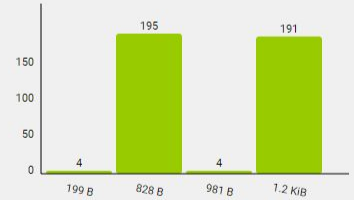
Detail: Samba dictionary attack, attempts: 195, port(s): 445, attack duration: 22 s 902 ms, average time between attempts: 117 ms.

Detection time:	2020-09-09 06:25:52	**Event source:**	192.168.0.33 (unknown)	**Probability:**	100 %
Last update:	2020-09-09 06:30:52	**Captured source hostname:**	N/A	**False positive:**	No
First flow:	2020-09-09 06:24:51	**MAC address:**	1c:75:08:04:7a:5f	**Detected by instance:**	Default
		User identity:	N/A	**Data feed:**	Default

TARGETS (1) | COMMENTS (0) | CATEGORIES (0) | ATTRIBUTES | EVENT EVIDENCE | RELATED IDS EVENTS (1) | TRAFFIC RECORDS

Flow count in relation to Transferred

Save as a text file
Query the Monitoring Center



2020-09-09 06:20:00 - 2020-09-09 06:30:00

Filter flows: Show all flows | APPLY

SOURCE IP	DESTINATION IP	TIMESTAMP	DURATION	PROTOCOL	SOURCE PORT	DESTINATION PORT	TRANSFERRED	PACKETS	FLAGS	TOS	SOURCE MAC	DESTINATION MAC	APP TAG	DATA FEED IP	TCP WINDOW SIZE
192.168.0.33 (unknown)	192.168.0.252 (unknown)	2020-09-09 06:24:51.114	0.123	TCP	64024	445	981	5	....APRS.	Best Effort & Default	1c:75:08:04:7a:5f	00:11:32:6c:b3:69	N/A	127.0.0.1	64240
192.168.0.252 (unknown)	192.168.0.33 (unknown)	2020-09-09 06:24:51.115	0.121	TCP	445	64024	828	6	....APS.	Routine (LD, NT, NR)	00:11:32:6c:b3:69	1c:75:08:04:7a:5f	N/A	127.0.0.1	N/A
192.168.0.33	192.168.0.252	2020-09-09	0	TCP	64024	445	199	1	....AP...	Best Effort &	1c:75:08:04:7a:5f	00:11:32:6c:b3:69	cifs	127.0.0.1	N/A

Analysis
Events
Reports
Settings
Logs
About

Date: Custom | From: 2020-09-08 10:10 | To: 2020-09-09 10:10 | Perspective: Security issues | Data feed: -- Unspecified -- | Source IP:

ANALYSIS | EVENT #151715

Type: Dictionary attacks (DICTATTACK)

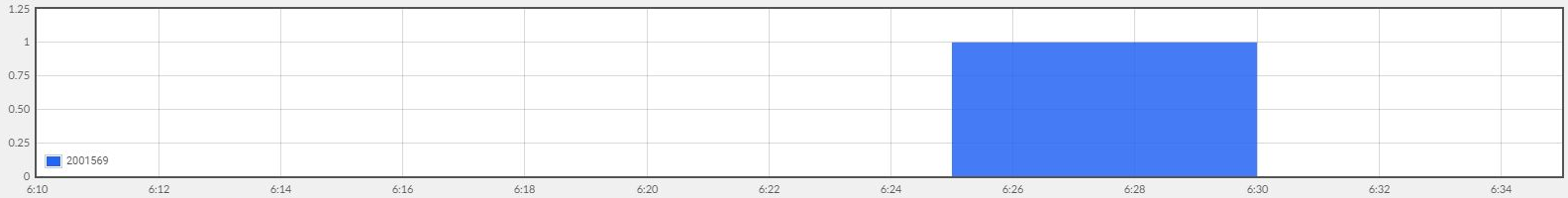
Subtype: SambaProtocol
Reports the password-guessing attacks (dictionary or brute-force based) on a Samba server. This may indicate an attacker's activity to get unauthorized access to a service or a misconfigured device that is continuously trying to authenticate to a service unsuccessfully.

Detail: Samba dictionary attack, attempts: 195, port(s): 445, attack duration: 22 s 902 ms, average time between attempts: 117 ms.

Detection time:	2020-09-09 06:25:52	**Event source:**	192.168.0.33 (unknown)	**Probability:**	100 %
Last update:	2020-09-09 06:30:52	**Captured source hostname:**	N/A	**False positive:**	No
First flow:	2020-09-09 06:24:51	**MAC address:**	1c:75:08:04:7a:5f	**Detected by instance:**	Default
		User identity:	N/A	**Data feed:**	Default

TARGETS (1) | COMMENTS (0) | CATEGORIES (0) | ATTRIBUTES | EVENT EVIDENCE | RELATED IDS EVENTS (1) | TRAFFIC RECORDS

Search by source IP | Search by destination IPs | VIEW



FIRST SEEN	LAST SEEN	SOURCE IP (BASE FOR AGGREGATION)	SOURCE PORT	DESTINATION IP (BASE FOR AGGREGATION)	DESTINATION PORT	SIGNATURE ID (BASE FOR AGGREGATION)	SIGNATURE (BASE FOR AGGREGATION)	LOG SOURCE IP	LOG SOURCE INTERFACE	COUNT	OTHER INFO
2020-09-09 06:25:10	2020-09-09 06:25:10	192.168.0.33	64102	192.168.0.252	445	2001569	ET SCAN Behavioral Unusual Port 445 traffic Potential Scan or Infection	127.0.0.1	eth2	1	**category:** Misc activity | **severity:** 3 | **action:** allowed | **groupID:** 1 | **rev:** 15

Analysis
Events
Reports
Settings
Logs
About

Date: Custom | From: 2020-09-08 10:10 | To: 2020-09-09 10:10 | Perspective: Security issues | Data feed: -- Unspecified -- | Source IP:

ANALYSIS | EVENT #151715

Type: Dictionary attacks (DICTATTACK)

Subtype: SambaProtocol
Reports the password-guessing attacks (dictionary or brute-force based) on a Samba server. This may indicate an attacker's activity to get unauthorized access to a service or a misconfigured device that is continuously trying to authenticate to a service unsuccessfully.

Detail: Samba dictionary attack, attempts: 195, port(s): 445, attack duration: 22 s 902 ms, average time between attempts: 117 ms.

Detection time:	2020-09-09 06:25:52	**Event source:**	192.168.0.33 (unknown)	**Probability:**	100 %
Last update:	2020-09-09 06:30:52	**Captured source hostname:**	N/A	**False positive:**	No
First flow:	2020-09-09 06:24:51	**MAC address:**	1c:75:08:04:7a:5f	**Detected by instance:**	Default
		User identity:	N/A	**Data feed:**	Default

TARGETS (1) | COMMENTS (0) | CATEGORIES (0) | ATTRIBUTES | EVENT EVIDENCE | RELATED IDS EVENTS (1) | TRAFFIC RECORDS

FPI SERVER	ID	STATE	START TIME	STOP	FILES	ACTION
localhost	5f58595087896	Analyzed	2020-09-09 06:19:51	2020-09-09 06:35:52	FPI_5f58595087896_192.168.2.4_eth2_history.pcap, FPI_5f58595087896_192.168.2.4_eth2_0002_20200909_063000.pcap, FPI_5f58595087896_192.168.2.4_eth2_0001_20200909_062554.pcap, FPI_5f58595087896_192.168.2.4_eth2_0003_20200909_063500.pcap	DOWNLOAD FILES

New PCAP
Recordings
Settings

Recordings

Group: All | From: 2000-01-01 00:00 | To: 2020-09-09 10:18
Traffic recording ID: | State: All | Segment: Custom
Show by source: All | Filtering rule:

1 2 3 4 5 6 ... 118 2 Go

STATE	TRAFFIC RECORDING ID	GROUP	START TIME	END TIME	ANALYSIS RESULT	ACTION	TOOLS
Recorded	5f58699555c62	FPI	2020-09-09 07:29:26	2020-09-09 07:45:17	-		EDIT ANALYSIS DETAIL DOWNLOAD DELETE
Recorded	5f5868a54336a	FPI	2020-09-09 07:25:42	2020-09-09 07:41:17	-		EDIT ANALYSIS DETAIL DOWNLOAD DELETE
Analyzed	5f58595087896	FPI	2020-09-09 06:19:51	2020-09-09 06:35:52	0 / 0 / 78		EDIT ANALYSIS DETAIL DOWNLOAD DELETE
Recorded	5f57a6a58b3bb	FPI	2020-09-08 17:37:44	2020-09-08 17:53:33	-		EDIT ANALYSIS DETAIL DOWNLOAD DELETE
Recorded	5f57a5b393e70	FPI	2020-09-08 17:33:50	2020-09-08 17:49:31	-		EDIT ANALYSIS DETAIL DOWNLOAD DELETE
Recorded	5f57a12c11ac5	FPI	2020-09-08 17:14:33	2020-09-08 17:30:12	-		EDIT ANALYSIS DETAIL DOWNLOAD DELETE
Recorded	5f57973b5e451	FPI	2020-09-08 16:30:58	2020-09-08 16:47:47	-		EDIT ANALYSIS DETAIL DOWNLOAD DELETE
Recorded	5f57904753982	FPI	2020-09-08 16:02:16	2020-09-08 16:18:07	-		EDIT ANALYSIS DETAIL

Network Detection and Response

Live Demo

Flowmon

Analysis detail

Source probe: 192.168.2.4 - eth2

Show the following protocols in the analysis report (1): SMB

EVENTS | STATISTICS

Tree options: PROPAGATE SEVERITY | COLLAPSE ALL | EXPAND ALL

Displayed root events: Information: 0 | Warning: 0 | Error: 78

- SMB: SMB request detected (TCP@192.168.0.33:64159-192.168.0.252:445)
  - SMB: SMB2 negotiation
    - SMB: SMB2 negotiation successful
      - SMB: Session with sign in
        - SMB: Server challenge sign in
          - SMB: Client credentials for sign in
            - SMB: SMB2 session setup error response
- SMB: SMB request detected (TCP@192.168.0.33:64205-192.168.0.252:445)
  - SMB: SMB2 negotiation
    - SMB: SMB2 negotiation successful
      - SMB: Session with sign in
        - SMB: Server challenge sign in
          - SMB: Client credentials for sign in
            - SMB: SMB2 session setup error response
- SMB: SMB2 request detected (TCP@192.168.0.33:64160-192.168.0.252:445)
  - SMB: SMB2 negotiation
    - SMB: SMB2 negotiation successful
      - SMB: Session with sign in
        - SMB: Server challenge sign in
          - SMB: Client credentials for sign in
            - SMB: SMB2 session setup error response
- SMB: SMB2 request detected (TCP@192.168.0.33:64161-192.168.0.252:445)

SMB2 session setup error response

Verify network connectivy. Check compatibility of client and server SMB protocol version. Check server log for error messages. You can try to restart the server.

Description	192.168.0.252 and 192.168.0.33 did not set up session - The attempted logon is invalid. This is either due to a bad username or authentication information (STATUS_LOGON_FAILURE, 0xC000006D).
Protocol	SMB
Severity	error
Flow	TCP@192.168.0.252:445-192.168.0.33:64243
TCP flow errors	No errors detected
Frame time	09.09.2020 06:28:15
Frame number	935
IP version	4
IP source	192.168.0.252
IP destination	192.168.0.33
IP proto	6
TCP source port	445
TCP destination port	64243
TCP stream	77
smb2.pid	0x0000feff
nt_status_decoded	The attempted logon is invalid. This is either due to a bad username or authentication information (STATUS_LOGON_FAILURE, 0xC000006D)
smb2.flags	0x00000001
smb2.sesid	0x000000001d1fdde8