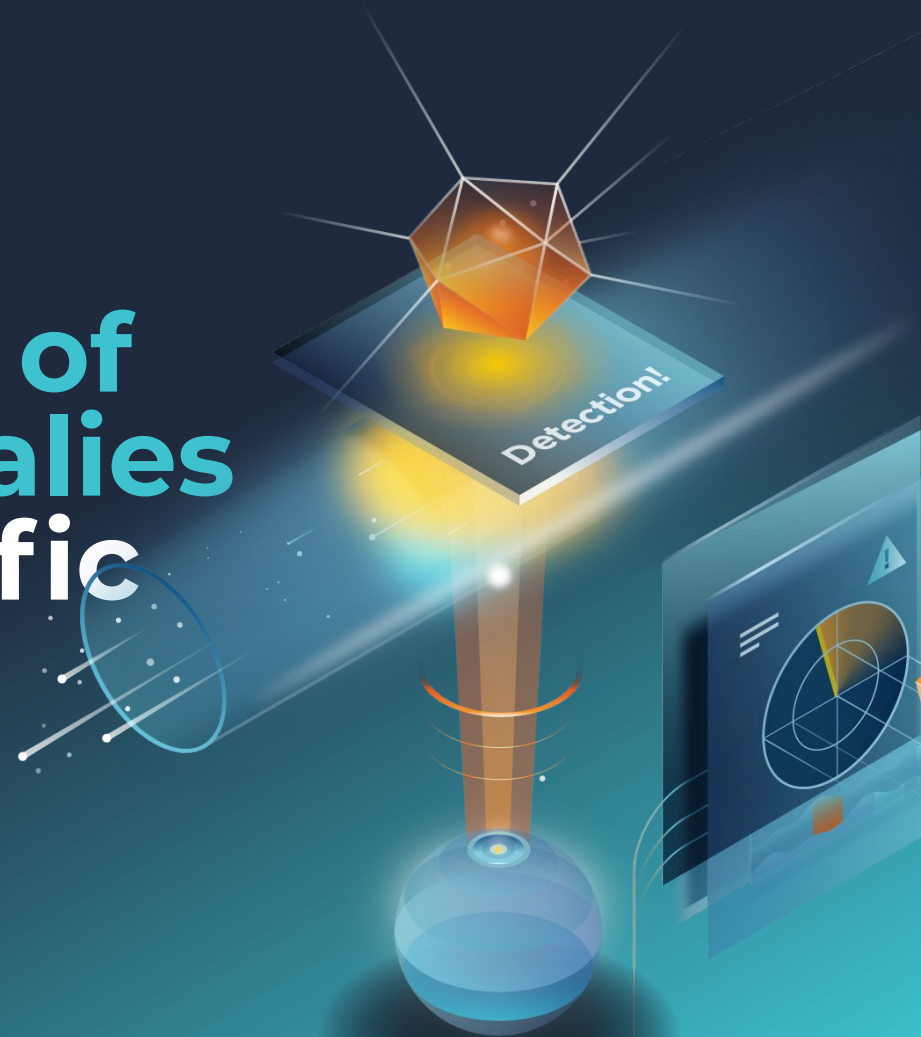


Early Detection of IoCs and Anomalies in Network Traffic

Pavel Minarik, Chief Technology Officer

Flowmon Networks



Prevention consumes 90% of budget

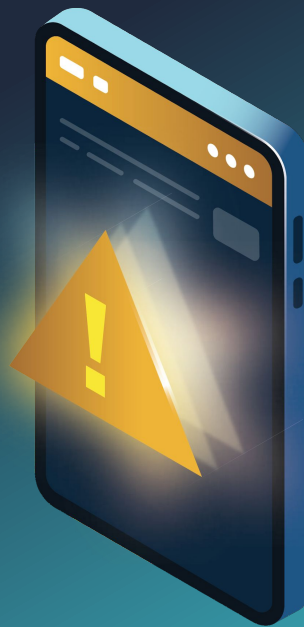
Firewall protects perimeter,
but what if it's bypassed?



Endpoint protection can be evaded

On average it takes 197 days to
identify a breach

Source: Cost of a Data Breach Study, Ponemon Institute



97 mil. CZK

Average cost of a breach

Healthcare

Highest average cost industry

USA

The most targeted country

280 days

Average time to contain a breach



Of the 240 GB of data allegedly stolen from University Hospital New Jersey, the attackers have leaked a 1.7 GB archive containing over 48,000 documents.


A source in the cybersecurity industry has told that an employee of UHNJ was infected with the TrickBot trojan at the end of August.

University Hospital New Jersey hit by SunCrypt ransomware, data leaked

By [Ax Sharma](#)

September 16, 2020 01:39 PM 0

Добавить Извлечь Тестировать Копировать Переместить Удалить Информация				
Legal\Shared\...				
Имя	Размер	Сжатый	Изменен	Атрибуты
Agri...	2 553 198 175	1 648 503 888	2020-07-30 15:16	DCI
Arch...	1 607 167 982	1 492 044 432	2019-12-05 11:30	DCI
Att...	4 416 704 344	1 524 319 728	2020-05-19 14:21	DCI
Bo...	73 873 690	0	2019-11-20 10:25	DCI
Cre...	770 762	0	2020-07-01 13:51	DCI
Em...	756 677 954	1 864 816 016	2020-08-25 13:17	DCI
Ins...	454 846 211	1 614 028 224	2020-09-04 12:31	DCI
Ins...	612 555 011	0	2020-08-17 14:49	DCI
Lav...	58 258	0	2020-08-25 13:04	DCI
Leg...	82 235 597	0	2020-08-28 12:15	DCI
Li...	17 967 285 550	14 620 174 304	2020-09-11 13:05	DCI
No...	590 362 810	0	2019-08-16 12:55	DCI
OP...	1 765 888 591	885 794 928	2020-05-06 11:39	DCI
P...	602 698	0	2020-01-22 16:50	DCI


UNIVERSITY HOSPITAL
 Newark, New Jersey

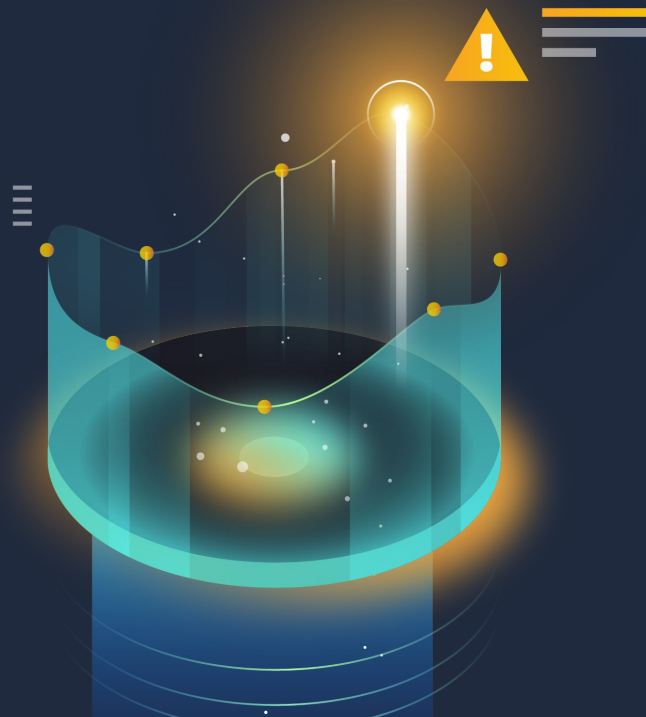
0 [REDACTED] 925
 Health Information Management
 150 Bergen Street, B417
 Newark, NJ 07101-6750
 (973) 972-5604

AUTHORIZATION FOR RELEASE OF PATIENT RECORDS

Please PRINT (except signature) and all sections must be completed.

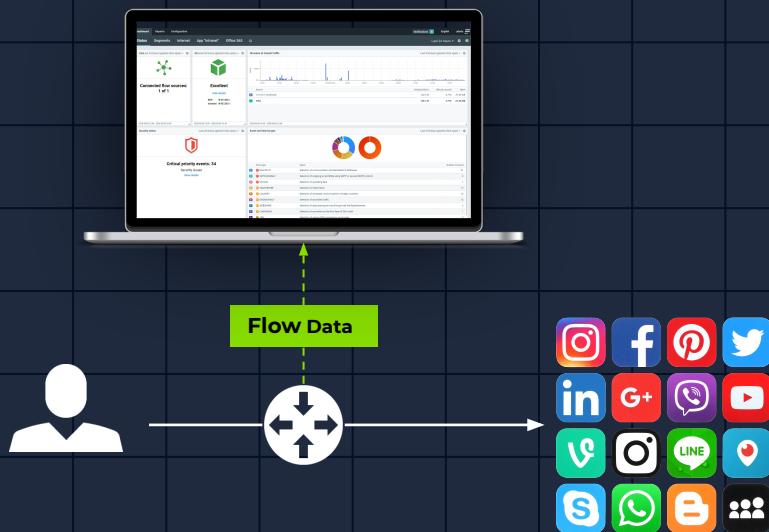
Scattered footprints

Threat actors constantly modify code and use advanced techniques to hide in network traffic. But they still leave footprints scattered all over the network. Enriched **network telemetry** is the key to discover those footprints.

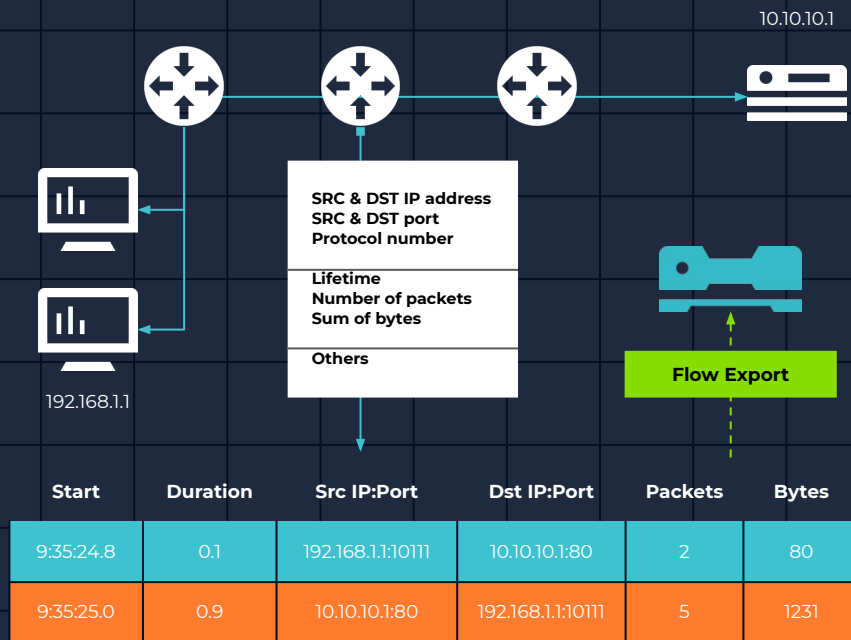


What is Flow Data?

- Standard network telemetry
- Cisco standard NetFlow v5/v9, IETF standard IPFIX
- Focused on L3/L4 information and volumetric parameters
- Network traffic to flow data reduction ratio from 250:1 to 500:1

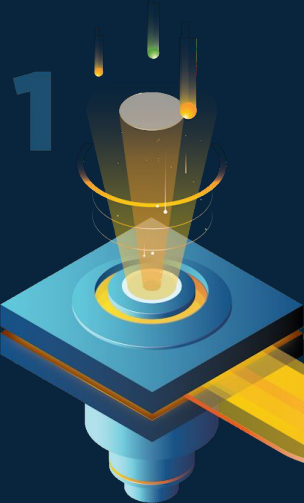


Principle of Flow Monitoring



Gather

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

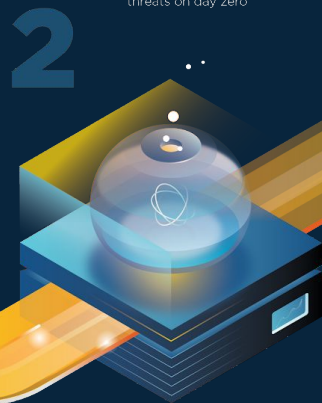


Analyze

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

Real-time

Respond to advanced persistent threats on day zero



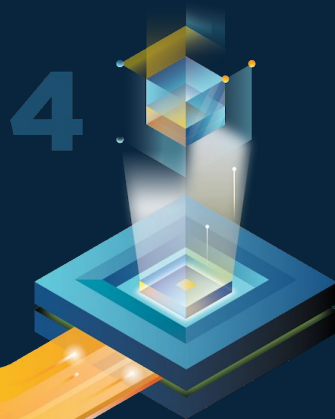
Understand

Relevant information is extracted and visualized on the dashboard.



Act

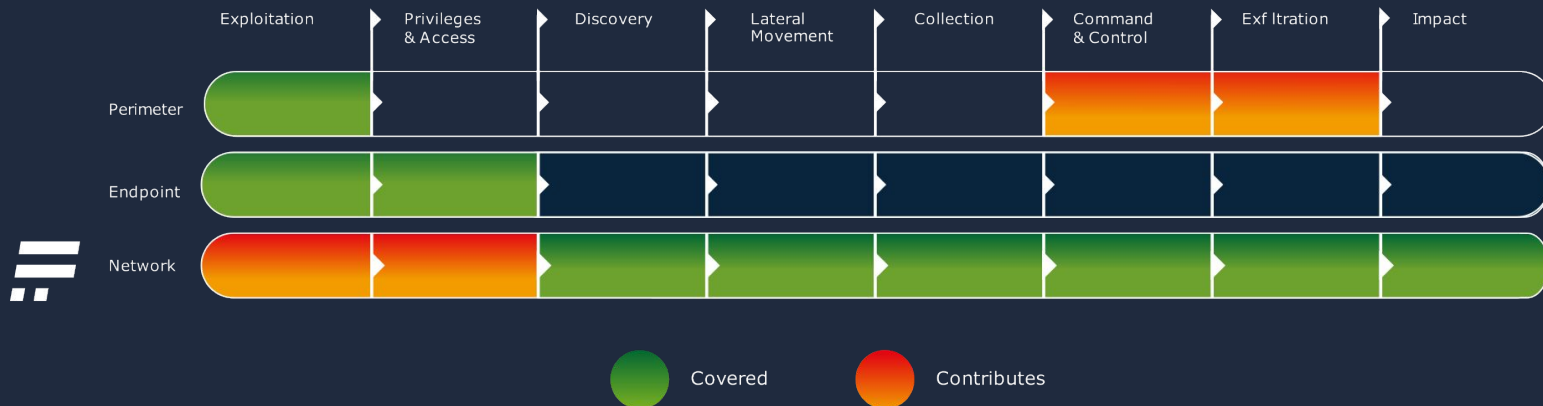
The user sees the big picture. The most important and relevant information is clear and noise-free.



16x

Up to 16x faster time to resolution reported


Multi-layered Security



Demonstration User Account Compromise




ConLast 24 hours (generic time span)



Connected flow sources:
1 of 1

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

AllLast 24 hours (generic time span)



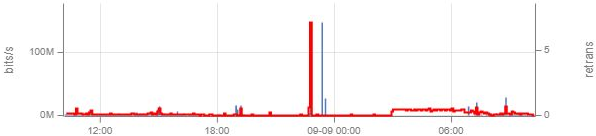
Excellent

Hide details

ERP99.812%
Intranet97.773%

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

Structure of Overall TrafficLast 24 hours (generic time span)

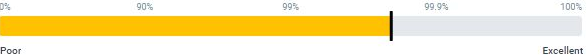


Source	Maximal bits/s	Bits per second	Bytes	AVG RTR
127.0.0.1 (localhost)	148.0 M	2.0 M	20.29 GiB	0.1
Total	148.0 M	2.0 M	20.29 G...	0.1

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

Structure of Overall TrafficLast 24 hours (generic time span)

99.796%
Retransmission index




AVG packets/s323.7
AVG SRT89.557 ms
AVG RTT30.309 ms
AVG RTR0.1

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

Application performance overviewLast 24 hours (generic time span)

ERP

99.812%




AVG response time3 ms
Median of response time1 ms
95% response time16 ms
99% response time46 ms

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


Application performance overviewLast 24 hours (generic time span)

Intranet

97.773%



Security statusLast 24 hours (generic time span)




Critical priority events: 5

Security issues

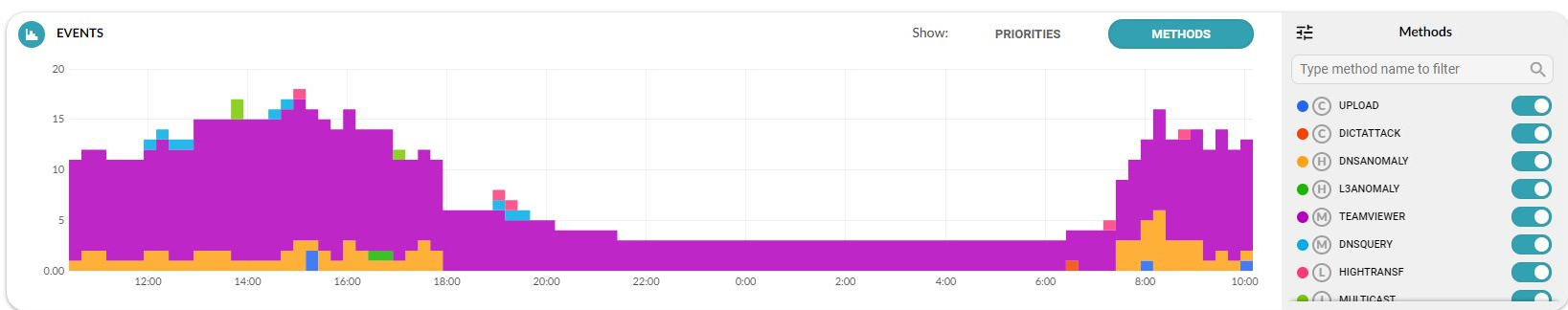
Hide details

Critical5
High36
Medium31
Low4
Info3

Event overview by typeLast 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



EVENTS BY PRIORITY 2020-09-08 10:25 - 2020-09-09 10:10 Overall events count: **79**

> **UPLOAD**

▼ **DICTATTACK**

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)		1

Detected 1 events of the type DICTATTACK from 192.168.0.33

Nighttime

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 From To Perspective Data feed Source IP

Custom 2020-09-09 10:10 2020-09-09 10:10 Security issues -- Unspecified --

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	5APRS.	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	6APS.	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 06:20:00	0	TCP	64024	445	199	1AP...	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

DateFromToPerspectiveData feedSource IP

Custom2020-09-08 10:102020-09-09 10:10Security issues-- Unspecified --

ANALYSIS

EVENT #151715

Type:Dictionary attacks (DICTATTACK)

Subtype:SambaProtocol

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

Last update:2020-09-09 06:30:52

First flow:2020-09-09 06:24:51

Event source:192.168.0.33 (unknown)

Captured source hostname:N/A

MAC address:1c:75:08:04:7a:5f

User identity:N/A

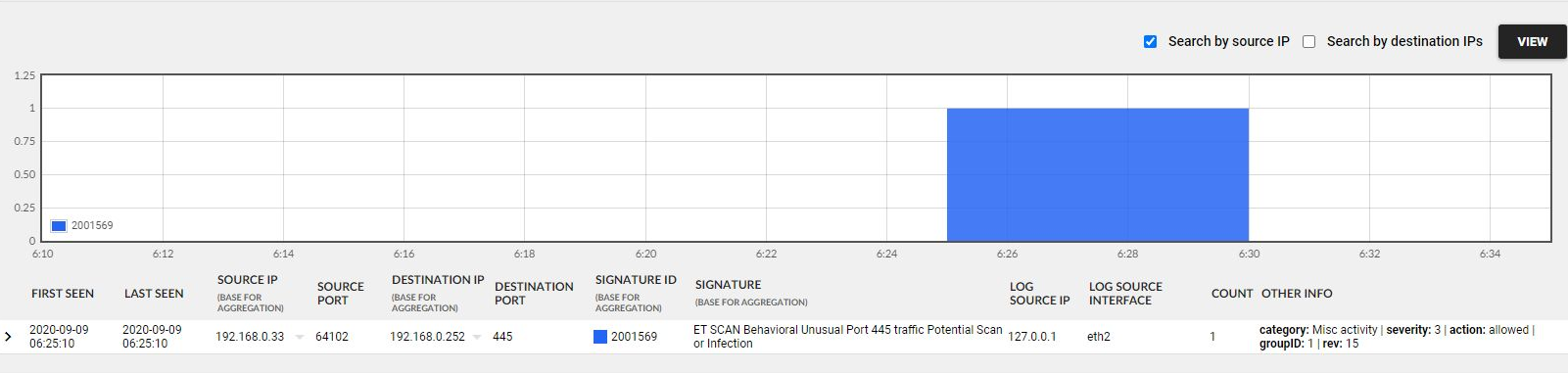
Probability:100 %

False positive:No

Detected by instance:Default

Data feed:Default

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



Analysis

Events

Reports

Settings

Logs

About

DateFromToPerspectiveData feedSource IP

Custom2020-09-08 10:102020-09-09 10:10Security issues-- Unspecified --

ANALYSIS

EVENT #151715

Type:Dictionary attacks (DICTATTACK)

Subtype:SambaProtocol

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

Last update:2020-09-09 06:30:52

First flow:2020-09-09 06:24:51

Event source:192.168.0.33 (unknown)

Captured source hostname:N/A

MAC address:1c:75:08:04:7a:5f

User identity:N/A

Probability:100 %

False positive:No

Detected by instance:Default

Data feed:Default

TARGETS (1)COMMENTS (0)CATEGORIES (0)ATTRIBUTESEVENT EVIDENCERELATED 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	<div>DOWNLOAD FILES</div>

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

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

Analysis detail

Source probe 192.168.2.4 - eth2 Show the following protocols in the analysis report (1)

SMB x

EVENTS

STATISTICS

Tree options

Displayed root events

PROPAGATE SEVERITY

COLLAPSE ALL

EXPAND ALL

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 connectivity. 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 login 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 login is invalid. This is either due to a bad username or authentication information (STATUS_LOGON_FAILURE, 0xC000006D)
smb2.flags	0x00000001
smb2.sesid	0x000000001d1fdde8

Incident summary

Input data



Network telemetry (flow data), reputation feeds, IDS signatures, full packet data.

Detection algorithms



Machine learning, adaptive baselining, behavior analysis, heuristics, reputation-based and signature-based.

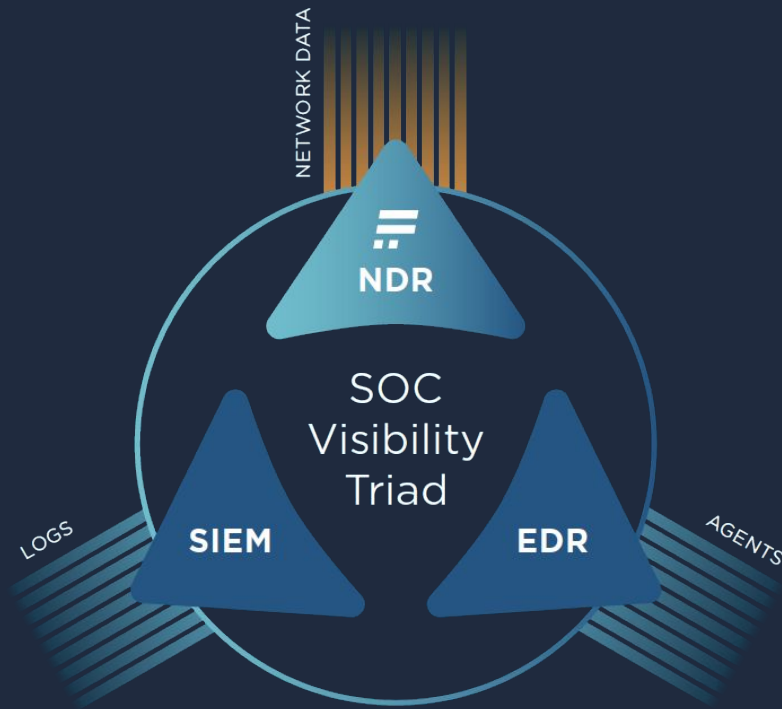
Provided evidence



Events, network telemetry, full packet capture, built-in packet analysis.

Security Visibility Triad

A network-centric approach to threat detection and response.



Questions

