

FLOWMON WEBINAR 24. 3. 2020

Encrypted Traffic Analysis for Security & Compliance

FM OS 10.03.02



Table of contents

1. Executive Summary	3
2. Encrypted Traffic Analysis (ETA) Dashboard	3
3. FMC Profiles	4
3.1. TLS Server version reporting Use Case	4
3.2. Detection of Malware by JA3 fingerprints Use Case	6
4. ETA Analyses	8
4.1. Public key length and algorithm analysis Use Case	8
4.2. Server Name Indication (SNI) Analysis Use Case	9
5. Certificate checkup notification Use Case	10
6. FMC Chapters	11
7. Conclusions	12

1. EXECUTIVE SUMMARY

Encrypted Traffic Analysis (ETA) is a method of malware detection and cryptographic assessment of secured network sessions, which does not rely on decryption.

New research from Flowmon and IDG Connect shows 99% of IT managers recognize encrypted network traffic as a source of security risks, but two-thirds of businesses fail to protect their assets from both internal and external threats misusing SSL/TLS.

TLS (a successor to SSL) handshake is a non-encrypted session through which client and server negotiates the encryption rules. Only after a secure channel is established, the traffic becomes encrypted. By reading the handshake and its specific parameters we can identify unusual behaviour. Download the Whitepaper here.

2. ENCRYPTED TRAFFIC ANALYSIS (ETA) DASHBOARD

Flowmon Dashboard provide us single pane of glass for Network and Security Operation (NetOps and SecOps) with customizable or preconfigured templates widgets (applied from Configuration Center -> Configuration Templates). It is possible to create multiple Dashboards which present different view on the network information (e.g. one dashboard for network operation, other for security or encrypted traffic analyses and many more). Responsive design allows to view dashboard on mobile phones and tablets.



FIGURE1: DASHBOARD USER INTERFACE

New widget		
Module		
 Flowmon Monitoring 	Center	Chang
Data to display		
Encrypted/Unencrypt	ted Traffic	Chang
Widget name		
Encrypted/Unencrypted Tra	ffic	
Data range		
Last day (generic time spa	•	
Last day (generic time spa	C	
Last day (generic time spa Widget Time series chart (Series Top-1 × 4 Top-8 × 4	9 ■ T09-2 X © T09-3 X © T09-4 X © T09-5 X © T09-6 X © T09-7 X T09-9 X © 109-10 X	•
Last day (generic time spa Widget Time series chart (Series Top-1 × Top-8 × Chart options	N C 1709-2 x ⊗1509-3 x ⊗1709+4 x ⊗1709+5 x ⊗1709+4 x ⊗1709+7 x 1709-5 x ⊗1509-10 x	*
Last day (generic time spa Widget Time series chart (Series Chart options Stacked chart ?	N Top-2 k ⊗ Top-3 k ⊗ Top-4 k ⊗ Top-5 k ⊗ Top-6 k ⊗ Top-7 k Top-9 k ⊗ Top-10 k	*
Lett day (generic time space Widget Time series chart (Series Chart options Stacked chart Axis Davent	■ T0p+2 x © T0p+3 x © T0p+6 x © T0p+5 x © T0p+6 x © T0p+7 x -T0p+6 x © T0p+10 x C Logarithmic	•
Left day (generic time space Widget Time series chart (Series Chart options Stacked chart ? Axis Left Table	N D Translik (Strastik (Strastik (Strastik (Strastik) (Strastik (Strastik)) C Leasting D	•
Last day (generic time spa Widget Time series chart (Series Chart options Stacked chart @ Axis @ Linear Table (Show colors @	N Tap+2 ≤ 0 10 + 3 × 0 10p+4 × 0 10p+5 × 0 10p+6 × 0 10p+7 × 10p+0 × 0 10 × Cognitive: ►	*
Lattay: generic time space Widget Time series chart (Series Chart options Stacked chart ? Table Table Show colors ? Show percents	N Top-2 k ⊕ Top-3 k ⊕ Top-4 k ⊕ Top-5 k ⊕ Top-6 k ⊕ Top-7 k Top-1 k ⊕ Top-10 k ○ Logurthmic	
Lattay (peerts the spa Widget The series durf Grees Staked durf Ads Show percents Show percents Columns	N Top-2 k © Top-3 k © Top-4 k © Top-5 k © Top-6 k © Top-7 k Top-9 k © Top-10 k C Loguithmic C	*

FIGURE 2: NEW DASHBOARD WIDGET SETUP

New Widget setup

- Selection of a suitable pre-prepared chapter from Flowmon Monitoring Center (FMC -> Reports -> Chapters)
- 2. Type of Chart (Pie or Linear/Logarithmic)
- 3. Selection of time interval for data conversion
- 4. Number of TOP Time series in the chart and their values
- 5. Possibility of linear or logarithmic condition and colour of table

3. FMC PROFILES

3.1 TLS SERVER VERSION REPORTING USE CASE

TLS Server Version Report provide information about used <u>TLS Protocol versions</u> in whole monitored traffic (recommended parent FMC Profile is All Sources) with visibility into potential unsecure and vulnerable cryptography mechanism. It allows to to show us lower TLS Protocol version than recommended TLS Protocol version for advanced security (e.g. TLS 1.0, TLS 1.1, TLS 1.2 or SSL versions).





Edit profile 'TLS server versions'		х
TLS server versions		
Parent profile	Group	
All Sources 🔹	No group	
Start date 2020-02-08 09:50	End	
Current time Maximal size 1.00 GB	Expires never	
Type ⊛ Real ◎ Shadow	Granularity 5 minutes 1 minute 30 seconds 	
Mass operations •	Disabled channel 📒 Enabled chann	el
NAME	CHANNEL OPTIONS POSITION ACTIO	N
🔲 🥚 TLS 1.3	^ <i>∕</i> i	i I
🔲 🛑 TLS 1.2	↑ / i	i I
🔲 🛑 TLS 1.1	^ / i	i
🔲 🛑 TLS 1.0	^ <i>∕</i> í	i I
	SAVE SAVE AS A NEW ITEM CA	NCEL

- I. Profile name
- 2. Parent profile of source data for new profile
- 3. Group definition like "ETA"
- 4. Start date can be recalculated with history data
- 5. Expiration for data collection
- "Real" type is with real data stored on disc and "Shadow" is about only data for graphing
- 7. Granularity for interval of collected data samples
- 8. Specification of unlimited count of channels

Edit channel 'TLS	1.3'				>			
Channel	Enabled Flow and chart data are not collected for disabled channel and all its sub-channels.							
Name	TLS 1.3	Position	Above the X-axis	•				
Color								
	tls-sver "TLS 1.3"							
Filter								
All channels Selected channels								
	127.128.0.0 (demo-flowsast-1, NetFlow-port3000) × ~							
Parent channels (5)	Parent channels (5) 127.0.0.1 (localhost, AWS VPC) ×							
127.128.0.0 (demo-flows.us-east-1, AWS VPC) ×								
10.0.0.22 (localhost) × localhost ×								
	+ Channel chart option	IS						
			- 1	SAVE	CLOSE			

- 1. Position above or under X-axis
- 2. Every one channel is defined by filter
- User can choose parent 's profile channels with concrete source data

3.2 DETECTION OF MALWARE BY JA3 FINGERPRINTS USE CASE

JA3 is a much more effective way to detect malicious activity over SSL than IP or domain-based IOCs. Since JA3 detects the client application, it does not matter if malware uses DGA (Domain Generation Algorithms), or different IPs for each C2 host, or even if the malware uses Twitter for C2, as JA3 can detect the malware itself based on how it communicates, rather than what it communicates to. This is a straightforward way how to use Flowmon to find possible threats in connection with detecting specific JA3 fingerprints. In this Use case we have been used JA3 database: https://sslbl.abuse.ch/ja3-fingerprints/

What is JA3 Fingerprint?

- Method describing encrypted communication between client and server
- Calculated during TLS handshake

How it works:

- 1. consists of headers from Client Hello message from TLS / SSL handshake
- 2. SSLVersion, Cipher, SSLExtension, EllipticCurve, EllipticCurvePointFormat respond 769,47-53-5-10-49161-49162-49171-49172-50-56-19-4,0-10-11,23-24-25,0
- 3. finally, MD5 hash is applied, which corresponds to the JA3 fingerprint de350869b8c85de67a350c8d186f11e6



FIGURE 5: CHART WITH TYPE OF MALICIOUS TRAFFIC BY JA3 FINGERPRINT

IMPORTANT NOTE

Bypassing proxy by camouflage of encrypted traffic:

- camouflage can be recognized by negotiated encryption, usually ciphers are proposed, which are generally recognized as compromised or already compromised
- communication to the Internet directed to compromised IP addresses, compromised HTTP hostname, SNI (name servers in the certificate), etc.
 Communication is detected by the BLACKLIST method in the ADS module.

6

dit profile 'Malware by JA3 fing	gerprints'	×			
Profile name	Description	-			
Malware by JA3 fingerprints	malicious NAD fingerprints identified by SSL Blacklist by ABUSE				
Parent profile	Group				
All Sources •	-No group- +	Edit channel W	dwind		5
Start date	End III Continuous profile	Channel	* Enabled		
Constitute			Disabled	Free and chart data are not collected for deal shared and all its sub-charmals.	ident
Maximal size	Expires	1.000	Admini	Persitive Allow the Party 1	
1.00.08	never	Caller	-		
Type	Granularity		Starlah Selecteration	COMPACTOR OF MILLION	
# Real	# 5 minutes		1941 Tonne (11994) 498	Gold tearpointee (14)	
Shadow	1 minute 30 seconds	riter			
Mass operations +	Disabled channel 🚦 Enabled channel	Al channels is	Selected channels		
	CHANNEL BOUTTON ACTION				
10 Hours	OPTIONS FOSTION ACTION	Parent character	AL CONTRACTOR AND		
🕕 😑 Enotet	÷ / I				
🗉 🔴 Ged	* 2.8				
E 🔵 Allfred	÷ / i		+ Channel chart of	ptions	
-		-			

FIGURE 6: FMC MALWARE BY JA3 FIGERPRINT PROFILE SETUP

IMPORTANT NOTE

In case of profile filter definition with JA3 fingerprints monitoring is not important how many fingerprints are used for the specific malware, it need to be used "OR" as separator between every tls-ja3 parameter.

C STATISTICS	LIST OF FLOWS			Edit output				× 58 •
				Name extended to				
imit to 20 ·				TLS Certificate				
ggregate	none selected	B Source Pol man	ai e [24]	H TLS issuer common name TLS certificate validity from TLS Public key algorithm	 TLS Subject cannot TLS Contribute valid TLS Public large large 	en name i Al Stal Subject organis Alty to ii Tal Signation olgan A	istise sales ithen	
Sort by start time.	of firms	E Destination Prof	17 * 34	TLS Client TLS Client version TLS Client version (0 TLS Client assailur (0 TLS Elliptic curves	# 113 Cafer rates 11 113 Extension type 11 118 Extension type	ii 1,5 Cheel restars	0 54	
Use selected channels	 Use all channels in the 	entended-samba /	· · · ·	TLS JA3 If TLS JAS ringeptist TLS Main				
utput extended-tis	- + a	estended-the		TLS Carlent type TLS betwee version	 Tut mechanic typ Tut tense random 	e II 1.5 telap See 12 II 1.5 telap See		
FILTER		emendeo TLS-centricanes		R YLS Server cipher ruite Output	11 Year of proto respect	anten P 1,5 server harte ()	M)	
FILTER 15-seer y filters +hone+		enerated TLS centrums		Corput				MAVE FAITER
PLTER Is user y filters «None» Q. PROCESS		ennebel ILI-centions		V Tuð Server opher suði Objut	i tut potropi	All Server and All Se	nel 	awer.
PLTER IN-SHEF IN SHORE IN SHOR	*	Rossing Charles		I TuStene opter une		eter * 1.4 sever sev 31 (1) (100) (100) (100) (100) (1) (100) (100) (100) (1) (100) (100) (100) (1) (100) (100) (100) (1) (100) (100) (100) (100) (1) (100)	ME 100	LAVE FATER CANCE. 00 -24 15:25:00
Pictor Is-see Pictor Is-see Pictor Pictor Pictor Istination Port Ist	* SCERTIFICATE VALIDITY TO 2016-01-25 12:00:50	READED TUS CENTRONS	BL CHIMA			All January and January a	ME 100 00 - 3020- BYTES 5.0 K	AAVE FASTER CANCE 00-04 15/2500 TLS SUBJECT ORGANISATI Fac
filter +bone= filter +bone= Q peocess Stination PORT [10] 442	• 5-0811FRCATE VALIDITY TO 2018-01-05 12:00:00 N/A	READED TUS CENTRONS 2	BL CHIMA Decision destroction destro		I 133 period segar Carl	All Jacob Hall (All	не ос. 3020- вутез 5.0 к 1.2 к	SAVE FASTER SAVE FASTER 00-24 152500 TLS SUBJECT ORGANISAT
PILTER Street r filters +NODE> Q. MODESE STINATION PORT TEL 445 445	• 2016-01-25 10:0050 1016-01-25 10:0050 NGA 2017-08-01 01:99-59	ROSENNI LUCIERLOPES Z	BLCHNOL Geoldenedigene defendigenedi		List of the segment of the segm	All January and January a	не отрана начи таки отрана вутава 5.0 к 1.2 к 4.2 к	ANY FRITER COMM. 33 - OK 15-2500 TLS SUBJECT ORGANISATI Fat
Ристон (13)-1947 15)-1947 19 19 19 19 19 19 19 19 19 19	• 2014-01-25 10:000 2014-05 10:000 NUA 2017-06-01 01:99-59 NUA	KON HELI CONTRACTORIA (CONTRACTORIA) KON HELI CONTRACTORIA (CONTRACTORIA)	BLORMON Geologia-color-action driata-accomp-color-action baaaa_accomp-color-action baaaa_accomp-color-action		Las 2 parts regard	All James and James a	не ос. 2000- вутез 5.0 к 1.2 к 4.2 к 2.2 к	ANY FRITER UNITE 33 - OK 15-2500 TLS SUBJECT ORGANISATI Fat

FIGURE 8:: "LIST OF FLOWS" TAB FOR A MORE DETAILED LOOK AT THE FLOW PARAMETERS, SELECTING THE APPROPRIATE "EXTENDED-TLS" OUTPUT

IMPORTANT NOTE

For relevant encrypted communication outputs where the TLS Handshake parameters are located, it is advisable to add one of the encrypted communication parameters, in our case "tls-sver", without a value, to the filter.

4. ETA ANALYSES

4.1 PUBLIC KEY LENGTH AND ALGORITHM ANALYSIS USE CASE

Weak short keys and outdated algorithms are a serious security risk. Insufficient key length makes it easier for an attacker to perform brute force decryption. Outdated algorithms suffer from vulnerabilities malicious actors can exploit to break in (think Heartbleed). We should always check the key length and algorithm as one because different algorithms require different key lengths, for example, elliptic curve cryptography algorithms (ECC) have shorter keys while having equivalent key strength as RSA (RFC 4492):



FIGURE 9: TIME INTERVAL SELECTION

Also thanks to the visibility of the key length parameter or its algorithm, we are able to identify possible risks in the network, associated with this and resulting greater vulnerability due to simpler encryption. Based on the parameter used, it is also possible to create a chapter for the calculated data in the widget in the Flowmon dashboard.

	ced analysis 2020-03-27	09:45 - 2020-03-27	12:30						2
🕻 STATI	STICS						р	revious results 2020-03	•27 14:25:52 •
op 10	Base the statistics on the	parameter TLS Public	key length Sor	t by flows		×			
Show s	econd chart for value "Other"								
Limit									
Use san	npling 🕕								
Use sel	ected channels 🔘 Use all channe	els in the profile							
FILTER									
Q PROC	SHOW IN TIME						All 20	Sources 20-03-27 09:45:00 - 2020-03	-27 12:30:00
							To	p 10 TLS Public key length sor	t by Flows
OLOR	START TIME - FIRST SEEN	DURATION	TLS PUBLIC KEY LENGTH	FLOWS	INPUT PACKETS	INPUT BYTES	PACKETS PER SECOND	BITS PER SECOND	BYTES PER PACKET
	2020-03-27 09:39:49.356	2 h, 50 m, 9.438 s	N/A	199.07 K (96.2%)	10.16 M (94.0%)	7.8 GB (95.0%)	994	6.6 M	
	2020-03-27 09:40:35.101			6.48 K (3.1%)	490 78 K (4 5%)	320.52 MB (3.8%)	48	265 A K	82
2		2 h, 48 m, 49.601 s	2048	0.4011 (0.1-0)	470.70 ((4.0-0))			200.4 K	68
2	2020-03-27 09:42:11.323	2 h, 48 m, 49.601 s 2 h, 47 m, 4.861 s	2048	1.29 K (0.6%)	145.87 K (1.4%)	94.21 MB (1.1%)	14	203.4 K	82 68 67
2 2 3 4	2020-03-27 09:42:11.323 2020-03-27 09:46:08.423	2 h, 48 m, 49.601 s 2 h, 47 m, 4.861 s 2 h, 41 m, 0.619 s	2048 256 1024	1.29 K (0.6%) 72 (0.0%)	145.87 K (1.4%)	94.21 MB (1.1%) 269.62 KB (0.0%)	14	78.8 K 228	82 68 67 25
	2020-03-27 09:42:11.323 2020-03-27 09:46:08.423 2020-03-27 09:55:51.978	2 h, 48 m, 49.601 s 2 h, 47 m, 4.861 s 2 h, 41 m, 0.619 s 2 h, 21 m, 20.895 s	2048 256 1024 4096	1.29 K (0.6%) 72 (0.0%) 27 (0.0%)	145.87 K (1.4%) 1.08 K (0.0%) 5.04 K (0.0%)	94.21 MB (1.1%) 269.62 KB (0.0%) 4.12 MB (0.0%)	14 0 0	200,4 K 78.8 K 228 4.1 K	82 68 67 25 85
2 3 4 5 Dther	2020-03-27 09:42:11.323 2020-03-27 09:46:08.423 2020-03-27 09:55:51.978 N/A	2 h, 48 m, 49.601 s 2 h, 47 m, 4.861 s 2 h, 41 m, 0.619 s 2 h, 21 m, 20.895 s N/A	2048 256 1024 4096 other	1.29 K (0.1%) 72 (0.0%) 27 (0.0%) 0 (0.0%)	145.87 K (1.4%) 1.08 K (0.0%) 5.04 K (0.0%) 0 (0.0%)	94.21 MB (1.1%) 269.62 KB (0.0%) 4.12 MB (0.0%) 0 B (0.0%)	14 0 0	2004 K 78.8 K 228 4.1 K	82 68 67 25 85

FIGURE 10: TLS PUBLIC KEYLENGHT ANALYSIS

8

ENCRYPTED TRAFFIC ANALYSIS FOR SECURITY & COMPLIANCE

Advanced analysis 20209327043 202093271230 Image: Statistic Control Contenter Control Control Control Control Control Control C
c STATESTICE LIST OF FLOWS 2020 03 27 14 35.06 Top 0 Base the statistics on the parameter T.S. Public key algorithm Sort by flows C Show second chart for value "Other"
Top 1 Base the statistics on the parameter TLS Public key signation Sort by flows Sort
Show second durit for value "Other" Use support to the second durit for value "Other" Use support to the second durit for value "Other" Use support to the second durit for value "Other" Use support to the second durit for value "Other" Note: Show in Time
 Linit Use satisfies ● Use satisfies ● Vie satisfie
Use sampling Use
Use selected channels Use selected channels Use all channels in the profile FILTER
FILTER All Sources All Sources Top 1013 Palls lay algorithm sort by flows port 43
Recess Show IN TIME All Second Second 27 (19450) - 2020 03-27 (1920) To port 443
COLOR START TIME - FIRST SEEN DURATION TLS PUBLIC KEY ALGORITHIM FLOWS INPUT PACKETS INPUT BYTES PACKETS PER SECOND BITS PER SECOND BYTES PER PACKETS
1 2020 03 27 0941:14.441 2 h, 48 m, 24.957 s NA 26.96 K (77.4%) 2.37 M (78.6%) 2.35 GB (85.2%) 224 2.0 M
2020-03-27 09:40:35.101 2 h. 48 m. 49:601 s rsaEncryption 6.58 K (18.9%) 496.44 K (16.5%) 324.8 MB (11.5%) 49 269.0 K
Image: Control of the contro
1 202003/27/074211322 2 h, 47m, 4861 s id-eePablicKey 1.28 k (3.7) 145.62 k (4.8) 9.114 MB (2.3) 1.4 78.8 k Other NA NA other 0 (0.0%) 0 (0.0%) 0 B (0.0%) 0 0

FIGURE 11: TLS PUBLIC ALGORITHM ANALYSIS

4.2 SERVER NAME INDICATION (SNI) ANALYSIS USE CASE

Similarly to ALPN, SNI is a TLS extension. It allows TLS-capable servers to host multiple services on the same IPs. Clients add this extension with the hostname of the website they want to connect to.

Q Advar	ISTICS ELIST OF FLOWS	7 09:45 - 2020-03	+27 12:30	utar			Pr	vevious results 2020-03	-27 14:18:41 •
 Show s Limit Use sal Use sel FILTER 	econd chart for value "Other" mpling 1 jected channels O Use all chan	nels in the profile	unit (int)						
Q PRO	eesa 🖍 show in time		(All 202 Re	Souces Souces 2003-27 09-45-00 - 2020-02 10 TLS server name (SHI) so	27 12:30:00 t by βγtes
COLOR	START TIME - FIRST SEEN	DURATION	TLS SERVER NAME	FLOWS	INPUT PACKETS	INPUT BYTES	PACKETS PER SECOND	BITS PER SECOND	BYTES PER PACKET
	2020-03-27 09:46:10.946	2 h, 28 m, 12.878 s	video-vie1-1.xx.fbcdn.net	183 (0.1%)	123.36 K (1.1%)	100.69 MB (1.2%)	13	95.0 K	855
2	2020-03-27 09:52:46.426	2 h, 32 m, 41.175 s	r1sn-2vq5-vngl.googlevideo.com	97 (0.0%)	89.59 K (0.8%)	82.81 MB (1.0%)	9	75.8 K	969
3	2020-03-27 09:46:07.731	2 h, 41 m, 33.112 s	scontent-vie1-1.xx.fbcdn.net	479 (0.2%)	77.46 K (0.7%)	50.66 MB (0.6%)	7	43.8 K	685
	2020-03-27 09:47:41.734	2 h, 40 m, 40.248 s	sci2-1.am.microsoft.com	70 (0.0%)	62.29 K (0.6%)	45.53 MB (0.5%)	6	39.6 K	766
5	2020-03-27 09:45:45.809	2 h, 40 m, 38.482 s	9638.482 fe2.update.microsoft.com	155 (0.1%)	48.07 K (0.4%)	42.89 MB (0.5%)	4	37.3 K	935
6	2020-03-27 09:47:41.733	2 h, 40 m, 40.246 s	sci1-1.am.microsoft.com	53 (0.0%)	52.15 K (0.5%)	38.2 MB (0.5%)	5	33.2 K	768
7	2020-03-27 12:09:13.828	5 m, 38.777 s	r2sn-2vq5-vngl.gvt1.com	2 (0.0%)	41.41 K (0.4%)	37.13 MB (0.4%)	122	919.4 K	940
	2020-03-27 09:57:38.568	2 h, 8 m, 13.183 s	oneclient.sfx.ms	13 (0.0%)	38.83 K (0.4%)	33.44 MB (0.4%)	5	36.5 K	903

FIGURE 12: TLS SERVER SNI ANALYSIS

IMPORTANT NOTE

In case of data volume analysis in this way, the TOP10 results of the largest data volumes transmitted in communication with individual TLS server name (SNI) results. Based on the parameter used it is also possible to create a chapter for the calculated data in the widget in Flowmon dashboard.

5. CERTIFICATE CHECKUP NOTIFICATION USE CASE

While checking for expired certificates is an obvious step, we might also want to check for soon-to-be-expired certificates to prepare in advance. Furthermore, monitoring certificates and their usage in development, testing and production environments is a way to protect against and identify leaking private keys and other sensitive information.

Flowmon allow us to setup notification that the SSL certificate has expired and needs to be renew. For the purposes of notification, it is possible to use several combined actions, such as notification on an e-mail, run a user script or send a syslog to SIEM System.

nabled		
	×	
lame	The only valid characters are a-z, A-Z, 0-9, -, + and	
	Web_Certificate_Expiratio	
rofile	All Sources •	
ilter	net 52.59.133.0/24 and t1:-vto < "now"	
hannels	® All	
	Only the selected	
Canditiana		
Conditions Conditions based on tota	al flow summary	
total flows	Absolute value	
Conditions based on indi	Ividual Top 1 statistics	
Trigger		
Each time	after 1 • x condition = true, and block the next trigger for 0 • cycles	
Actions		
R No action	_	
ACUONS	SAVE SAVE AS A NEW ITEM SAVE AND TEST SCRIPT	сл
Actions .	SAVE SAVE AS A NEW TEXT SCRIPT	CA
Actions	TAVE SAVE AS A NEW TEXE SAVE AND YEST SOBRY	CA
Actions R. No action	SAVE SAVE AS A NEW TED SAVE AND TEST SCHIPT	CA
Actions	ANT SAVE AS A NEW TRDE	CA
Actions Action	ANY ANA ANY ITEE SAVE AND YEST INDEED	CA
Actions Actions No action Send email	SAVE AS A NEW TICK	CA
Actions Actions No action Send email	SAVE SAVE AS A NEW ITEM SAVE AND TEST SOBRET	CA
Actions Actions No action Send email	Exve Exve as a new itter Exve as a new itter Recipient	CA
Actions Actions Actions No action Send email	Taxe Save As A NEW TOX Save As TEST SCREET Recipient:	CA
Actions Actions No action Send email	Ever Sove as a new riter Recipient Subject Alert triggered Use GPG •	CA

FIGURE 13: CERTIFICATE CHECKUP NOTIFICATION SETUP

- 1. Name of Alert
- 2. Parent profile like source of data
- 3. Additional filter as condition
- 4. Used channels from parent profile
- 5. Condition based on total flow sumary
- 6. How many times is alert trigered
- 7. Actions may by combined

Send a syslogSend SNMP trap

6. FMC CHAPTERS

In the REPORTS tab in the left panel of the FMC module, it is possible to click through to the CHAPTERS section, where chapters are defined as a source of pre-calculated data, not only for reports, but also for the widgets in Flowmon Dashboard itself. These chapters can be fully utilized also for the purpose of monitoring encrypted traffic.

	OVERVIEW > SEND RE	EPORT () REPORTS 🗮 CHAPTERS	
Luser kratky •			
+ NEW CHAPTER			
STATUS	NAME	TYPE	TOOLS
	FIGURE 12: TLS S	JERVER SNI ANALYSIS	
ALLOWED TLS Public key lenght		Ф ТОР	🖍 EDIT 📱 DELETE
ALLOWED TLS server name (SNI)		(В) ТОР	🖍 EDIT 📲 DELETE
ALLOWED TLS Signature algorithm		(в) тор	🖍 EDIT 📋 DELETE
ALLOWED TLS validity TO		(в) тор	🖍 EDIT 🚺 DELETE

E l'a de la composition						4.	6		×
Edit chapter			en	cz	Jþ	de	Tr	es	×
Name	TLS server name (SNI)								
Description	TLS server name (SNI)								
Profile	All Sources	•						_10	
	• All								
Channels	Only the selected								
Туре	Top chapter								
— Top chapter - setting	S								- 1
Тор	10 •								
Base the statistics on the parameter	TLS server name (SNI)								
Sort by	bytes 🔹								
Chapter columns	none	none						•	
	none	none						•	
	none •	byte	S					Ŧ	
Filter									-
Filter									
Placklist									
DIGUNIISU	<none></none>	+	NEW E	LAC	KLIST	ſ			
Recompute	do not recompute 🔹								

FIGURE 15: TLS SEVER NAME (SNI) CHAPTER SETUP

- 1. Name and Description of Chapter
- 2. Source Profile of traffic data
- 3. Channels selection in profile
- 4. Type of Chapter (Pie or Linear/ Logarithmic)
- 5. No. Of TOP values
- 6. Parameter statistics
- 7. Sort by value
- 8. Chapter columns description
- 9. Filter specification
- 10. Recomputing of data in time

FLOWMON

7. CONCLUSIONS

Scanning...

99% of IT professionals see encrypted traffic as a possible source of security threats. Don't let the encrypted traffic turn into security risk. Gain a scalable visibility of threats in encrypted traffic when preserving privacy and with no impediment to latency for both, Network and Cloud Operation (NetOps) and Security Operation (SecOps) with Flowmon Probes, Flowmon Collectors and Flowmon ADS.

www.flowmon.com