



How to aggregate your Nipper Audit Reports in Elasticsearch and Explore the Data in Kibana

গ্য TITANIA

titania.com

Nipper and Elastic Integration

Reducing your mean time to detect misconfigurations and vulnerabilities in firewalls, switches and routers, Titania Nipper accurately audits network devices, prioritizes risks and provides exact technical fixes to help remediate issues.

Nipper's accurate audit data – such as your detailed compliance posture against standards including DISA STIG, DHS CDM/NIST 800-53 and PCI – can now be injected into the Elastic Stack via JSON, where the combined solution provides greater scope to analyze and remediate large numbers of your machines on a daily basis.

The Kibana dashboard then gives you the power to examine your security posture from different angles, filtering by categories of error and drilling down to precise detail about devices/models impacted and how to mitigate risks.

This user guide shows you step-by-step how to aggregate your Nipper audit reports in Elasticsearch and use your Kibana dashboard to explore the data.

Published May 2022

© Titania Limited 2022, All Rights Reserved

This document is intended to provide advice and assistance for the installation and running of Nipper software. While Titania takes care to ensure that all the information included in this document is accurate and relevant, customers are advised to seek further assistance from our support staff if required.

No part of this documentation may be copied or otherwise duplicated on any medium without prior written consent of Titania Limited, publisher of this work.

The use of Nipper software is subject to the acceptance of the license agreement.

Titania Limited Security House Barbourne Road Worcester WR1 1RS

Telephone: (+44)1905 888 785 Technical Support: support@titania.com Licensing: enquiries@titania.com Nipper Support: https://www.titania.com/support/nipper-support

TITANIA

Table of Contents

Contents	3
Prerequisites for Aggregating Nipper Audit Reports in Elasticsearch	4
Step 1 Configuring Nipper to Emit JSON in the Correct Format	4
Step 2 Running an Audit	5
Step 3 Creating the Elastic Index	6
Step 4 Use Logstash to Inject Nipper Output into the Elasticsearch Index	7
Step 5 Creating a Kibana Index Pattern	8
Step 6 Exploring the Data	11
Conclusion and Further Help	12

Prerequisites for Aggregating Nipper Audit Reports in Elasticsearch

Before you begin, please ensure you have completed the prerequisite technical set up:

- Download the digital version of this guide from the support section of the Titania website for a link to scripts you will need to download (a zip file called Nipper_Elastic_Ingest),
- » Nipper (v 2.6.3 or above) is licensed and installed on your local Windows 10 machine,
- » WSL is configured and available to run Logstash,
- » Elastic and Kibana are installed and running on your local machine*, there is no security on the Elastic Index, and
- » Docker Desktop is installed on Windows 10 (a powershell script is provided in the Nipper_Elastic_ Ingest zip file to pull and run the containers).

* If Elastic and Kibana are installed remotely, the URLs provided in the digital version of this guide will need to be updated accordingly, and the Logstash conf script adjusted to connect to the instance. An example file 'ls_with_creds.conf' is provided in the Nipper_Elastic_Ingest zip file.

For further information on installing the Elastic stack, please refer to the Elastic website: elastic.co

Step 1

Configuring Nipper to Emit JSON in the Correct Format

Logstash expects JSON in NDJSON. This means that each JSON Object appears on a separate line in the file, and not encapsulated in an array.

In order to configure Nipper to emit the JSON in the correct format you need to:

- » Open Nipper and click 'Settings'
- » Click the 'Logging' icon and open the 'File' tab
- » Ensure that:
 - » 'Enable logging to File' is checked
 - » The file path to the output file is OK
 - » 'Compact JSON' is selected from the dropdown
 - » 'Stream output' is checked, and
 - » 'Select All' Logging Trigger Levels is checked
- » Finally, click 'OK' to confirm the settings.

New to Nipper?

You can download the Nipper Beginner's Guide from the Titania website: titania.com

- » If you need to install Nipper:
 - » Go to the 'Downloading Nipper' section of the Nipper Beginner's Guide
- » If you need to install your license:
 - » Go to the 'Downloading your license' section of the Nipper Beginner's Guide
- » To audit your devices and generate reports:
 - » Open Nipper and select 'New Report' on the Nipper homepage. Step-by-step guides to generating each report can also be found on the website: www.titania.com/support

General ✓ Enable logging to File Logging File path and name Format Format to use as output for file logs Compact JSON JSON Settings ✓ Stream output Compact JSON EOL Format Windows (CR LF) CEF Settings EOL Format Windows (CR LF) Levels File Logging Trigger Levels ✓ Select All V > Audit Fail > Check Fail > Check Pass > Generation > Report Summary > Generation > Report Summary ✓ System ✓ Error	General Event Log	File TCP U	DP Email		
Logging File path and name C:/example/nipper.json Format Format to use as output for file logs JSON Settings Stream output Stream output Compact JSON CGropact JSON EOL Format Windows (CR LF) CEF Settings EOL Format EOL Format Windows (CR LF) Levels File Logging Trigger Levels File Logging Trigger Levels Select All ✓ Select All Audit Fall > Audit Fall Audit Pass > Check Faall Select All > Check Fall Select All > Report Select All > Audit Fall Select All > Check Fall Select All > Check Ramual Select All > Generation Select All > Seport Select All Select All > Check Fall Select All > Check Fall Select All > Seport Select All Select All	General				
Logging File path and name C:/example/nipper.json Format Format to use as output for file logs JSON Settings Stream output Stream output Compact JSON CGropact JSON EOL Format Windows (CR LF) CEF Settings EOL Format EOL Format Windows (CR LF) Levels File Logging Trigger Levels File Logging Trigger Levels Select All ✓ Select All Audit Fall > Audit Fall Audit Pass > Check Faall Select All > Check Fall Select All > Report Select All > Audit Fall Select All > Check Fall Select All > Check Ramual Select All > Generation Select All > Seport Select All Select All > Check Fall Select All > Check Fall Select All > Seport Select All Select All	Enable logging to File				
Format F			oricon		
Format to use as output for file logs Compact JSON JSON Settings JSON Settings Stream output Windows (CR LF) CEF Settings Windows (CR LF) EOL Format Windows (CR LF) Levels Steam output File Logging Trigger Levels Steam output Select All P P Audit Fail Audit Fail > Check Fail Check Fail > Check Ranual Select all > Check Pass Select all > Report Summary Select all		c./example/nip	61.300		
SSON Settings Stream output Compact JSON EOL Format Windows (CR LF) CFF Settings EOL Format Windows (CR LF) Levels File Logging Trigger Levels Select All ▼ Report > Aduit Fail > Aduit Fail > Aduit Fail > Check Fais > Check Annual > Check Pass > Generation > Generation > Report Summary ▼ System	Format				
Stream output Compact JSON EOL Format Windows (CR LF) CEF Settings Windows (CR LF) EOL Format Windows (CR LF) Levels Image: Compact Comp	Format to use as output f	or file logs	Compact JSC	ON	
Compact JSON EOL Format Windows (CR LF) CEF Settings EOL Format Windows (CR LF) Levels File Logging Tigger Levels S select All	JSON Settings				
CEF Settings EOL Format Windows (CR LF) Levels Tile Logging Tigger Levels ✓ Select All ✓ Report > Audit Pasi > Check Fail > Check Manual > Check Manual > Check Pass > Generation > Report Summary ✓ System	Stream output				
CEF Settings EOL Format Windows (CR LF) Levels Tile Logging Tigger Levels ✓ Select All ✓ Report > Audit Fail > Audit Fail > Check Fail > Check Manual > Check Manual > Check Manual > Check Manual > Check Tais > C	Compact JSON EOL Form	at	Windows (CR	R LF)	
EOL Format Windows (CR LF) Levels File Logging Trigger Levels ✓ Select All > Audit Fail > Audit Fail > Audit Fail > Check Fail > Check Manual > Chec					
Levels File Logging Trigger Levels ✓ Select All ✓ Report > Audit Fail > Audit Fail > Check Fail > Check Manual > Check Pass > Generation > Report Summary ✓ System					
File Logging Tigger Levels Select All Report Audit Fail Audit Fail Audit Fail Check Fail Check Pass Generation Report Summary System	EOL Format		Windows (CR	R LF)	
✓ Select All ▼ Report > Audit Fail > Audit Pass > Check Fail > Check Manual > Check Pass > Generation > Report Summary ▼ System	Levels				
Report > Audit Fail > Audit Pass > Check Fail > Check Manual > Check Pass > Generation > Report Summary Y System	File Logging Trigger Level	ls			
Audit Fail Audit Pass Check Fail Check Manual Check Pass Generation Report Summary System	Select All				
Audit Pass Check Fail Check Manual Check Pass Generation Report Summary System					
 Check Fail Check Manual Check Pass Generation Report Summary System 					
Check Pass Generation Report Summary System					
Seneration Report Summary System					
 > Report Summary > System 					
✓ System		arv			
✓ Error	✓ System				
	Error				

W TITANIA

Step 2

Running an Audit

- » Now click the 'Reports' icon to choose the audit you wish to run
- » Follow the onscreen instructions to choose the network device configurations you wish to include in your reports scope
- » Click 'Finish'
- » The file will now appear in the specified directory.

If there are lots of devices being audited and/or lots of audit types being conducted, it can take time to write out the file after the audit is complete.

Listing the size of the file a few times until it stops growing in size ensures that the process is complete.

Please note Nipper will append to this file if further audits are performed, so you may wish to move/delete the file before performing a subsequent audit.

PS C:\exa	nple> ls				
Direct	tory: C:\example				
Mode	LastW	riteTime	Length	Name	
-a	31/01/2020	16:11	7345901	nipper.json	

The contents of nipper.json should look similar to the fragment below, which is shown as an example:

{"audit_type":"Security Audit","date_time":"Fri Jan 31 16:05:41
2020","device":{"collection_ip":"","filename":"3com5500
.txt","hostname":"5500-EI","manufacturer":"3COM","model":"5500 Series
Switch","operating_system":{"name":"SS4","version
":"5500-EI"}},"ease":{"description":"Dictionary-based password
guessing attacks have been widely documented on the Inte
rnet and published media, enabling an attacker with very little
knowledge or experience to perform the attack. There ar
e a numb

* Note there is no '[' opening bracket. Just a '{' opening bracket, and the JSON record is all on one line.

Step 3

Creating the Elastic Index

» Navigate to your Kibana dashboard: http://localhost:5601/app/kibana#/home?_g=()

	n about how usage data helps us manage and improve	our products and services, see our Privac	y statement. To stop collection, disable usag	e data nere.
	smiss			
6				
a				
8	Add Data to Kibana Use these solutions to quickly turn your di			
8	Use these solutions to quickly turn your a	ata into pre-built dasriboards and monitorin	g systems.	
8	_		-	
2				
	APM	Logging	Metrics	SIEM
3	APM automatically collects in- depth performance metrics and	Ingest logs from popular data sources and easily visualize in	Collect metrics from the operating system and services	Centralize security events for interactive investigation in
a l	errors from inside your	preconfigured dashboards.	running on your servers.	ready-to-go visualizations.
¢	applications.			
-	Add APM	Add log data	Add metric data	Add security events
÷				
۲				
	Add sample data		from log file	Use Elasticsearch data

- » Select the 'Dev Tools' icon from the left hand toolbar
- » Now configure the index and apply a mapping. The mapping extends the index length of some fields, and masks out those not needed.

Locate the .txt file script (shown right) in the Nipper_Elastic_Ingest zip file to copy and paste into the Console panel.

» Once the text has been pasted into the console, click anywhere inside the text, then click the 'Run' arrow in the top right hand corner.

This action creates an index called 'nipper' with the correct mappings to accept the data from the tool.

If the index already exists, then you will get an error in the right hand pane after clicking 'Run'.





W TITANIA

» If you wish to start afresh, issue a 'DELETE /nipper' on the Console pane, and then try again.

There is no need to replace the index creation text, just append it in the Console window, click on it, then click 'Run'. Once the index is deleted, you can return to the creation text, click that, and press 'Run' again.

You now have an index with the correct mapping to accept Titania data.

Step 4

Use Logstash to Inject Nipper Output into the **Elasticsearch Index**

The next step is to get the data into the index. An easy way to do this is using Logstash from the Elastic ELK stack. To do this, Logstash needs a config file.

- » Locate the .exe file named 'I.conf' (shown right) in the Nipper_Elastic_Ingest zip file.
- » Now invoke Logstash: cat nipper.json | logstash -f l.conf
- » The nipper.json data is now in Elastic.





Below it is invoked on a WSL (windows subsystem for Linux) Ubuntu instance. Note the output to the console issues some warnings, but completes successfully:

cat nipper.json | logstash -f l.conf --path.data . -l OpenJDK 64-Bit Server VM warning: Option UseConcMarkSweepGC was deprecated in version 9.0 and will likely be removed in a future release.

WARNING: An illegal reflective access operation has occurred

WARNING: Illegal reflective access by com.headius.backport9.modules.Modules (file:/usr/share/logstash/logstash-core/lib/jars/jruby-complete-9.2.8.0.jar) to field java.io.FileDescriptor.fd

WARNING: Please consider reporting this to the maintainers of com.headius.backport9.modules.Modules

WARNING: Use --illegal-access=warn to enable warnings of further illegal reflective access operations

WARNING: All illegal access operations will be denied in a future release

Thread.exclusive is deprecated, use Thread::Mutex

WARNING: Could not find logstash.yml which is typically located in \$LS_HOME/config or /etc/logstash. You can specify the path using -path.settings. Continuing using the defaults

Could not find log4j2 configuration at path /usr/share/logstash/config/log4j2.properties. Using default config which logs errors to the console

- [INFO] 2020-01-31 18:01:44.570 [main] writabledirectory Creating directory {:setting=>"path.queue", :path=>"./queue"}
- [INFO] 2020-01-31 18:01:44.593 [main] writabledirectory Creating directory {:setting=>"path.dead_letter_queue"; :path=>"./dead_letter_queue"}

- [WARN] 2020-01-31 18:01:45.367 [LogStash::Runner] multilocal Ignoring the 'pipelines.yml' file because modules or command line options are specified [INFO] 2020-01-31 18:01:45.386 [LogStash::Runner] runner Starting Logstash ("logstash.version"=>"7.5.2") [INFO] 2020-01-31 18:01:45.428 [LogStash::Runner] agent No persistent UUID file found. Generating new UUID {uuid=>"5b1127a5-1139-4949-aec4-c18a3e88fbfa", :path=>"./uuid"} [INFO] 2020-01-31 18:01:47.634 [Converge PipelineAction::Create<main>] Reflections Reflections took 66 ms to scan 1 urls, producing 20 keys and 40 values
- [INFO] 2020-01-31 18:01:49.890 [[main]-pipeline-manager] elasticsearch Elasticsearch pool URLs updated {:changes=>{:removed=>[], :added=>[http://localhost:9200/]}}

[WARN] 2020-01-31 18:01:50.199 [[main]-pipeline-manager] elasticsearch - Restored connection to ES instance {:url=>"http://localhost:9200/"}

[INFO] 2020-01-31 18:01:50.475 [[main]-pipeline-manager] elasticsearch - ES Output version determined {:es_version=>7]

[WARN] 2020-01-31 18:01:50.482 [[main]-pipeline-manager] elasticsearch - Detected a 6.x and above cluster: the 'type' event field won't be used to determine the document _type {:es_version=>7} [INFO] 2020-01-31 18:01:50.563 [[main]-pipeline-manager] elasticsearch - New Elasticsearch output {:class=>"LogStash::Outputs::Elasticsearch", :hosts=>["//localhost:9200"]}

[INFO] 2020-01-31 18:01:50.647 [Ruby-0-Thread-5: :1] elasticsearch - Using default mapping template

[WARN] 2020-01-31 18:01:50.714 [[main]-pipeline-manager] LazyDelegatingGauge - A gauge metric of an unknown type (org.jruby.specialized.RubyArrayOneObject) has been create for key: cluster_uuids. This may result in invalid serialization. It is recommended to log an issue to the responsible developer/development team

[INFO] 2020-01-31 18:01:50.726 [[main]-pipeline-manager] javapipeline - Starting pipeline [d=>*main", "pipeline.workers"=>8, "pipeline.batch.size"=>125, "pipeline.batch.delay"=>50, "pipeline. max_inflight"=>1000, "pipeline.sources"=>["/c/example/l.conf"], :thread=>*#<Thread:0x6dd7bd2c run>"}

[INFO] 2020-01-31 18:01:50.768 [Ruby-0-Thread-5::1] elasticsearch - Attempting to install template {:manage_template=>{"index_patterns"=>"logstash-*", "version"=>60001, "settings"=>{"index. refresh_interval"=>"5s", "number_of_shards"=>1}, "mappings"=>{"dynamic_templates"=>{{"message_field"=>{"path_match"=>"message", "match_mapping_type"=>"string", "mapping"=>{"type"=>"text", "norms"=>false}}}, {"string_fields"=>{"match_mapping_type"=>"string", "mapping"=>{"type"=>"text", "norms"=>false, "fields"=>{"type"=>"keyword"=>{"type"=>"keyword"=>{"type"=>"keyword"=>{"type"=>"keyword"=>{"type"=>"keyword"=>{"type"=>"keyword", "geore_above"=>256}}}}, "properties"=>{"@timestamp"=>{"type"=>"date"}, "@version"=>{"type"=>"keyword"}, "geore=>"text", "norms"=>false, "fields"=>{"type"=>"text", "norms"=>false, "fields"=>{"type"=>"keyword"=>{"type"=>"keyword", "geore_above"=>256}}}, "properties"=>{"@timestamp"=>{"type"=>"date"}, "@version"=>{"type"=>"keyword"}, "geore=>"text", "norms"=>false, "fields"=>{"type"=>"keyword"=>"type"=>"keyword", "geore_above"=>256}}}, "float", "longitude"=>{"type"=>"alf_float"})}}

[INFO] 2020-01-31 18:01:50.965 [[main]-pipeline-manager] javapipeline - Pipeline started {"pipeline.id"=>"main"}

- The stdin plugin is now waiting for input:
- [INFO] 2020-01-31 18:01:51.130 [Agent thread] agent Pipelines running {:count=>1, :running_pipelines=>[:main], :non_running_pipelines=>[]}
- [INFO] 2020-01-31 18:01:51.792 [Api Webserver] agent Successfully started Logstash API endpoint {:port=>9600}
- [INFO] 2020-01-31 18:01:57.911 [LogStash::Runner] runner Logstash shut down.

Step 5

Creating a Kibana Index Pattern

- » Firstly, click on the 'Settings' icon in the Kibana dashboard
- » And click on the 'Index Patterns' link



» Click on the blue 'Create Index Pattern' button



» Now type the name of the index you created into the index pattern box

You don't have to type the complete name - you can use wild cards (this helps if you want Kibana to look over multiple Elastic indexes) - but in this case, typing nipper* works.

It will tell you Kibana has matched with the Elastic index called nipper*.

- » Click the 'Next Step' button
- » Select date_time from the drop down box, and click the 'Create Index' pattern.

The date_time is the field you mapped to contain the date of the events in the Nipper JSON output.

You will now see that the index has been created.

I	Elasticsearch							
0	Index Management	nipper*						* 2 [
1	Index Lifecycle Policies Rollup Jobs	Time Filter field name: da	ate_time					
	Transforms	This page lists even	field in the nipper* index	and the field's	associated cor	e type as recorde	ed by Elasticsea	rch. To change a fiel
8	Remote Clusters		search Mapping API %				,	
1	Snapshot and Restore License Management	Fields (267)	Scripted fields (0)	Source filt	ers (0)			
	8.0 Upgrade Assistant							
1	-	Q Filter						All field types
3	Kibana	Name		Туре	Format	Searchable	Aggregatable	Excluded
2	Saved Objects	@timestamp		date		•	•	4
	Spaces Reporting	@version		string		•		6
	Advanced Settings	@version.keyword		string		•	•	
5		_id		string		•	•	6
2		_index		string		•	•	6
2		_score		number				6
•		_source		_source				
		_type		string		•	•	é
		audit_type		string		•		6
		audit_type.keyword		string		•	•	é
		Rows per page: 10 💊					< 1 2	3 4 5 27



» Next, click on the 'Discover' icon on the left toolbar.

If the data you are analysing wasn't created in the last 15 minutes, it is likely you will need to change the time window with the calendar item to see the data.

» Now you should see the data loaded into Elastic. In this case there are 3221 records.



4	D Discover	0
O	New Save Open Share In	Inspect
	🖺 🗸 Search	KQL 🛍 🗸 Last 1 year Show dates 🔿 Refres
ŝ	(e) - + Add filter nipper*	9 3221 hits
8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8	Q Search field names Image: Constraint of the state	Jan 31, 2019 @ 18.22-22.802 - Jan 31, 2020 @ 18.22-22.802 — Arto ~
	t @version t _Jd t _Jndax # _score t _Sype t audk_Sype	Distance Distance Jan 31, 2020 0 16111182.000 message_level[Critical Scomers: [Billering Gue 31, 2020 0 16101152.000 [Billering Gue 31], 2020 0 16
Ŷ	t audits	> Jan 31, 2020 @ 16:11:02.000 ressage_level. Critical comment: #timestamp: Jan 31, 2020 @ 18:01:05.050 title: Mules following beny All modit.type: Filtering Complexity date.time: Jan 31, 2020 @ 16:11:02.000 idi: mammal fails heat: THEMLEMICTOR for example.them.and them.and them.
	/ count	<pre>metric modulor(or) personalizerian(p) personalizerianene automatica(p)) device.operating system.new: XN edvice.operating/system.version: 17.3 device.newsfacturer: Natchbarn device.model: XN 5 Series device.hostname: XN 5.Series message.type: Compliance Test Fail</pre>

- » Load in the dashboard
- » And select the 'Settings' menu again

4	D Discover					٥	
9	New Save Open Share	Inspect					
•	🖺 🗸 🛛 Search		KQL 👼] ✓ Last 1 year	Show dates	C Refre	esh
	(=) + Add filter nipper*	0		3,221 hits			
	Q Search field names		Jan 31, 2019 @ 18:32:22.892 - J	Jan 31, 2020 @ 18:32:22.892 — Auto	~		
50 m 15	 Filter by type Selected fields φsource Available fields	3000 2500 1500 1000 500					
2	@ @timestamp @version Lid	500 0	2019-11-01 2019-12-01 2020-01-01				
5	t _index # _score t _type t audit_type	> Jan 31, 2020 €	audit.type: Filtering Complex host: TWUKLAPTOP79 device.co; device.operating_system.versi	ent: @timestasp: Jan 31, 2020 0 18:01 (ity date_time: Jan 31, 2020 0 16:11:02 Illection_ip: device_filename: device on: 4.1 device_manufacturer: Check Poi _IP60w_message_type: Compliance Test Fa	.000 id: menual: false .operating_system.name: CP nt device.model: CheckPoint	IP60W	11
2	t audits t audits t comment # count	> Jan 31, 2020 0	audit_type: Filtering Complex host: TNUKLAPTOP79 device.co; device.operating.system.name:	ent: @timestamp: Jan 31, 2020 0 18:01 ity date_time: Jan 31, 2020 0 16:11:02 llection_ip: device.filename: WatchGu XTM device.operating.system.version: evice.hostname: XTM_5_Series message_ty	.000 id: manual: false ard_XTM_5_Series.xml 11.7.3 device.manufacturer:		
	device.collection_ip device.filename	> Jan 31, 2020 0	audit_type: Filtering Complex	ent: @timestamp: Jan 31, 2020 @ 18:01 city date_time: Jan 31, 2020 @ 16:11:02 llection_ip: device.filename: device	.000 id: manual: false	ng Deny A	411

» Select the 'Saved Objects' link



- » Click the 'Import Objects' button
- » Now from the requester, import the nipper_kibana_dashboard.ndjson provided in the Nipper_Elastic_Ingest zip file.

This file contains the definitions of example visualisations, as well as a dashboard containing those visualisations.

	Management / Saved o	bjects	0
3	Elasticsearch		
0	Index Management Index Lifecycle Policies	Saved Objects	🗄 Export 2 objects 🔄 Import 😋 Refresh
1	Rollup Jobs Transforms	From here you can delete saved objects, such as saved searches, via their associated application, which is probably what you should	You can also edit the raw data of saved objects. Typically objects are only modified d use instead of this screen.
8	Remote Clusters	Q Search	Type ✓ 👘 Delete 🛛 Export ✓
1	Snapshot and Restore License Management		
	8.0 Upgrade Assistant	Type Title	Actions
		Advanced Settings (7.5.1)	000
	Kibana	☐ & nipper*	***
	Index Patterns Saved Objects Spaces	Rows per page: 20 🗸	
	Reporting		
	Advanced Settings		
>			

» Select the 'Dashboard' icon

Elasticsearch			
Index Management Index Lifecycle Policies Rollup Jobs Transforms	Saved Objects From here you can delete saved objects, such as saved searches. medified via their associated application, which is probably what y		C Refres
Remote Clusters Snapshot and Restore	Q Search	Type ✓ 🕆 Delete	
License Management 8.0 Upgrade Assistant	Type Title		Action
	Advanced Settings [7.5.1]		
Kibana Index Patterns	Advanced Settings [7.4.2]		
Saved Objects	B Nipper		
Spaces Reporting	☐ ♣ nipper*		
Advanced Settings	A nipper**		
	A keith*		
	_ ♣ apm-*		
	☐ Ⅲ /goto/224c24b08415cf1e5cd027635dd4fdb5		
	Audit Session List		
	🗌 🖄 Test Status		
	Chooser		

» And finally, click on the Nipper dashboard link.

📕 🖸 Da	shboards	
0		
ø	Dashboards	① Create dashboard
là:	Q Search	
3		
ŵ	Title Description	Actions
&	Nipper	0
69	Rows per page: 20 V	
2		
da		
5		
ି		
A		
4		
ŵ		
0		

Step 6 Exploring the Data

- » You will now be presented with a dashboard like this allowing you to click and filter on the results in the usual Kibana manner
- » Scroll down the dashboard to see heat maps and detailed audit findings and vulnerabilities

Here you can explore your security posture from different angles, filtering by categories of error and drilling down to precise detail about devices/models impacted and how to mitigate risks...





	Dashb	board / Editin	ig Nipper (ur	isaved)		0
Ð		Ne: Euden Catalyst Swi Firev Quidway Swi	itch - wall -	4-5 5-6 6-7		
9		Rou 200 Appliance (Ga CheckPoint IP6 Point VPN-1 Edge	uter – aia) – iOW –	•7-8		
îi	Check	Point VPN-TEage	00004000			
2			NSA-AUTR			
Ì			NSN			
2				·		-
9	Security Audit					ණ
3	Finding ID ≑ Tit	tle 🗘	Impact Rating 🌩	impact =	Count	
5	FLTR- Pao 020 Sou De	ter Rules Allow ckets From Any urce To Any estination And y Port	Critical	If network filtering rules are not configured to restrict access to network services from only those hosts that require the access then unauthorized access may be gained to those services covered in this issues finding. For a network edge device, this could lead to a remote attacker gaining access to network service. For an internal device this could lead a malicious user gaining unauthorized access to a service.	8	
Ĵ	FLTR- Pac 020 De	ter Rules Allow ckets To Any stination And y Port	Medium	If network filtering rules are not configured to restrict access to network services from only those hosts that require the access then unauthorized access may be gained to those services covered in this issues finding. For a network edge device, this could lead to a remote attacker gaining access to network service. For an internal device this could lead a malicious user gaining unauthorized access to a service.	5	
2 2	FLTR- Pao 020 Ne	ter Rules Allow ckets To etwork estinations	Information	al If network filtering rules are not configured to restrict access to network services from only those hosts that require the access then unauthorized access may be gained to those services covered in this issues finding. For a network edge device, this could lead to a remote attacker gaining access to network service. For an internal device this could lead a malicious user gaining unauthorized access to a service.	5	
3		ter Rules Allow ckets To	Medium	If network filtering rules are not configured to restrict access to network services from only those hosts that require the access then unauthorized access may be gained to those services covered in this issues finding. For a network edge device, this could lead to a remote attacker gaining	5	-
	STIG Detail Finding ID \$ Title		ntegory chec	k ⊜ Description ⊜ Fix ⊕	Count ≑	\$ 1
	V-3143 Dev	vices exist CA h standard		w the network devices configuration to determine if the vendor default Network devices not protected with strong Remove any word is active. If any vendor default passwords are used on the device, this is a password schemes provide the opportunity for vendor default	17	

Conclusion and Further Help

If you have followed this guide, you will see how quick and easy it is to aggregate your Nipper audit reports in Elasticsearch.

Now you can explore your data in Kibana, prioritize your risks and use Nipper's exact technical fixes to help remediate any vulnerabilities or issues on your network.

If you would like any help or advice about the steps or scripts included in this guide, simply contact our dedicated Support team on:

Tel: (+44)1905 888 785 Email: support@titania.com

Our solution advisors will be more than happy to help walk you through this or any other auditing processes with our Nipper software.

			Missi	ion Critical Net	twork			
				CATI				
Result	Scope	#	Title				Severity	Responsibi
FAIL	2	V-3196	An insecure version of Si	NMP is being us	sed.		CATI	IAO
FAIL	٥	V-3062	Passwords are viewable	V-30	85 F/	AIL.		
Result	Scope	#	Title	HTTP server is The network element must he administrative access disable	not disabled	Severity Rule ID	GATH SV-41467r2_rule	ā
FAIL	9	V-3085	HTTP server is not disat			STIDIO	NET0740	
FAIL	6	V-3966	More than one local acc	Findings	Туре		Sever	ity
FAIL	6	V-3969	Network element must of	router03 router29	Cisco Router Cisco Router		Missic	in Critical
FAIL	2	V-14671	NTP messages are not a	Quidway Office-Juniper-SRX 1000-61	Huawei Quidway Switch Juniper SRX Firewall 3COM 5500 Series SW		Missic	n Critical
FAIL	0	V-31285	BGP must authenticate	XTM_5_Series	WatchGuard XTM 5 Ser	ies XTM5'5		n Critical
				watch555 router318	WatchGuard XTM Cisco Router		Missie	in Critical in Critical
Result	Scope	#	Title	Remediation	ble using HTTP (port 80) for adr	ninistrative access		6
FAIL	0	V-3020	DNS servers must be det				CAT III	IAU

Example analytics shows the prioritization of remediation that can be achieved when audit data is combined with value chain data on the mission criticality of the device/ network.

About Nipper

Nipper accurately audits the security of firewalls, switches and routers to detect exploitable misconfigurations that pose risk to the network, prioritized by criticality. Applying Nipper's compliance lens to the findings also provides the evidence needed to assure compliance with RMFs including DISA RMF, NIST 800-53/171, STIG, CMMC and PCI. All findings are output as an easy-to-read report, or a JSON for integration with SIEM, GRC and other data visualization systems.

Nipper's risk remediation advice and exact technical fixes for misconfigurations also support and accelerate the process of becoming secure and compliant.

About Titania

Protecting over 25 million people globally, Titania software is trusted to secure the world's most critical networks against preventable attacks. Nipper intelligently automates configuration auditing to analyze misconfigurations and validate your network security against the latest risk management frameworks, assurance and compliance standards.

Stay secure and complaint with Nipper. Find out more.

titania.com/products/nipper/

titania.com