



Cloud monitoring
using
CHR and Big-Data

Summary

- About Us
- General background on CHR
- CHR Amazon EC2 installing
- CHR Use cases
- Cloud monitoring elements
- Reporting , Alerting and Trigger

>whoami

Shlomi Gutman

CTO of Voicenter (Israel)

VP of Cloud Products at QXIP (Amsterdam)





VOICENTER

Let's talk business

Voicenter is A leading **telecommunication technology company** providing top-tier business telephony since 2007

We are delivering a 'One-stop-shop' solution for business all around the world

 **Telecom Services**

 **PBX**

 **Call Center Solution**



QXIP - Voice Capture Engineering & Development

QXIP {QuickSIP} is an R&D Company specializing in Open-Source and Commercial Voice Technology Development.



What's CHR?

Cloud Hosted Router (CHR) is a RouterOS version intended for running as a virtual machine.

It supports the x86 64-bit architecture and can be used on most of the popular hypervisors such as VMWare, Hyper-V, VirtualBox and others.

CHR has full RouterOS features enabled by default but has a different licensing model than other RouterOS versions.



CHR Licensing License

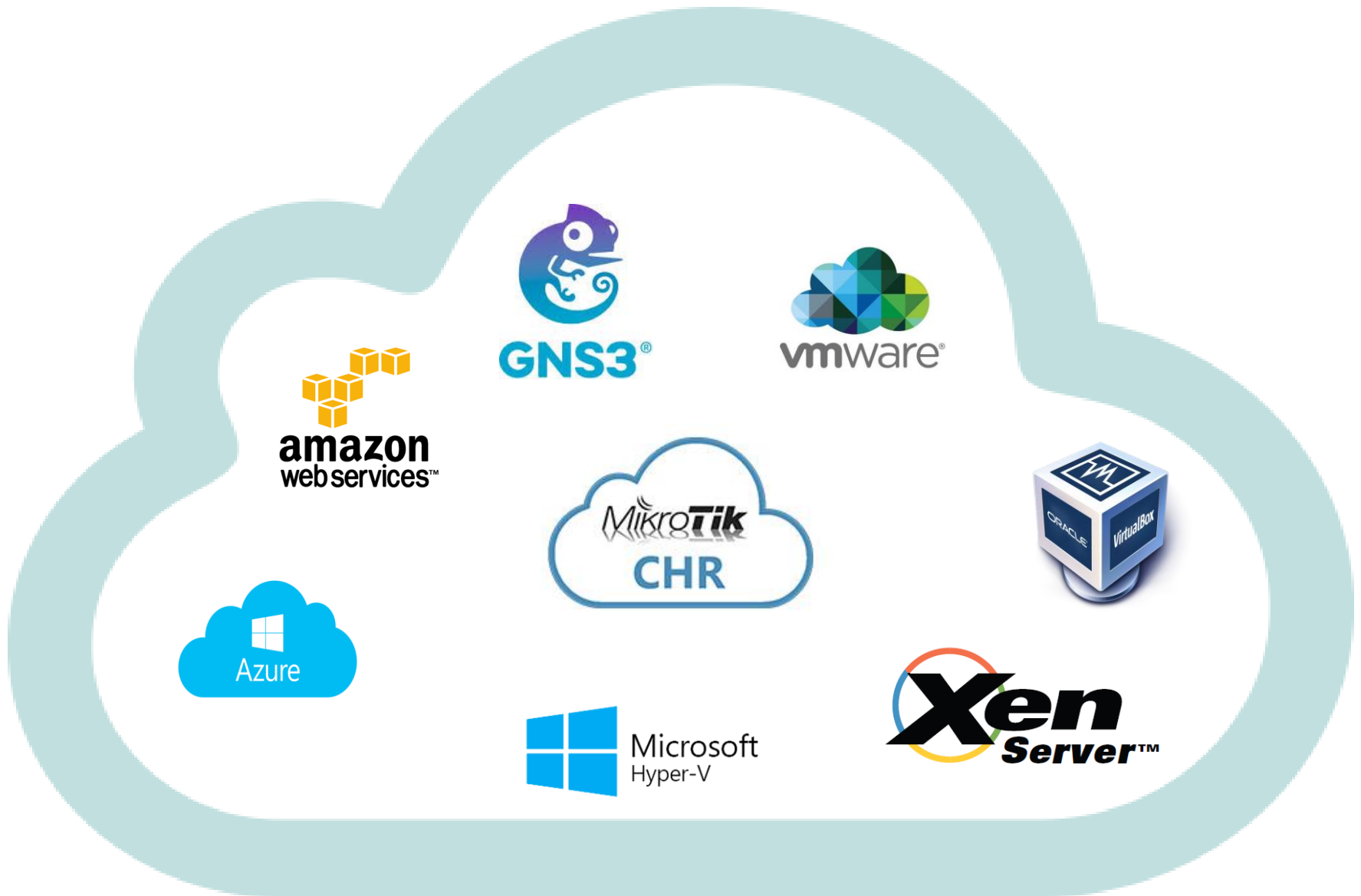
Perpetual is a lifetime license - buy once, use forever .

It is possible to transfer a perpetual license to another CHR instance.

License	Speed limit	Price
Free	1Mbit	FREE
P1	1Gbit	45\$
P10	10Gbit	95\$
P-Unlimited	Unlimited	250\$

If the CHR instance will not be able to access the account server to renew the license , it will behave as if the trial period has ran out and will not allow an upgrade of RouterOS to a newer version.

CHR hosting environment



Installing CHR on AWS – Step 1

The screenshot displays the AWS Management Console interface. At the top, there are navigation tabs for 'Services' and 'Resource Groups'. The left sidebar contains a navigation menu with categories like 'EC2 Dashboard', 'INSTANCES', 'IMAGES', 'ELASTIC BLOCK STORE', and 'NETWORK & SECURITY'. The main content area is titled 'Resources' and shows a summary of EC2 resources in the 'US West (N. California)' region: 0 Running Instances, 2 Elastic IPs, 0 Dedicated Hosts, 0 Snapshots, 0 Volumes, 0 Load Balancers, 3 Key Pairs, and 5 Security Groups. Below this, a blue box contains a promotional message for Amazon Lightsail. The 'Create Instance' section is visible, with the text 'To start using Amazon EC2 you will want to launch a virtual server, known as an Amazon EC2 instance.' and a blue 'Launch Instance' button circled in red. Below the button, a note states 'Your instances will launch in the US West (N. California) region'. At the bottom of the console, there are sections for 'Service Health' and 'Scheduled Events'. The footer includes 'Feedback', 'English', and a copyright notice: '© 2008 - 2017, Amazon Web Services, Inc. or its affiliates'.

Select CHR Image (AMI)- Step 2

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 1: Choose an Amazon Machine Image (AMI)

[Cancel and Exit](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

The screenshot displays the AWS console interface for selecting an AMI. On the left sidebar, the 'AWS Marketplace' filter is selected and circled in red with the number '1'. The search bar at the top contains the text 'mikrotik' and is also circled in red with the number '2'. The search results show a single product, 'Cloud Hosted Router' by MikroTik, which is also circled in red with the number '3'. The 'Select' button for this product is highlighted with a red circle and the number '3'. The product details include a 'Free tier eligible' badge, a star rating of (0), version 6.34.1, and a description: 'Use the CHR for protecting your cloud servers using RouterOS firewall which supports Layer7 filtering, dynamic address lists and more; for running your own VPN service or ...'. The 'More info' link is also visible.

Select Instance Tab – Step 3

Services Resource Groups

nitzan gutman N. California Support

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

Filter by: All instance types Current generation Show/Hide Columns

Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)
Note: The vendor recommends using a t2.micro instance (or larger) for the best experience with this product.

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
<input type="checkbox"/>	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.xlarge	4	16	EBS only	-	Moderate	Yes

Cancel Previous Review and Launch Next: Configure Instance Details

Setup your network – Step 4

The screenshot shows the AWS Management Console interface for configuring an EC2 instance. The navigation bar at the top includes 'Services', 'Resource Groups', and user information. The breadcrumb trail indicates the current step is '3. Configure Instance Details'. Below the breadcrumb, the title 'Step 3: Configure Instance Details' is followed by a descriptive paragraph. The configuration form includes several sections: 'Number of instances' (set to 1), 'Purchasing option' (with a checkbox for 'Request Spot instances'), 'Network' (set to 'vpc-... | VOICENTER'), 'Subnet' (set to 'subr... | VOICENTER | us-west-1c'), 'Auto-assign Public IP' (set to 'Enable'), 'IAM role' (set to 'None'), 'Shutdown behavior' (set to 'Stop'), 'Enable termination protection' (checkbox), 'Monitoring' (checkbox), and 'Tenancy' (set to 'Shared - Run a shared hardware instance'). At the bottom right, there are buttons for 'Cancel', 'Previous', 'Review and Launch', and 'Next: Add Storage'. A red oval is drawn around the 'Network', 'Subnet', and 'Auto-assign Public IP' sections.



Configure – Step 5

Services ▾ Resource Groups ▾ ⌵

nitzan gutman ▾ N. California ▾ Support ▾

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: Create a new security group
 Select an existing security group

Filter

Security	Name	Description
<input type="checkbox"/>	sg-ac915ccb	Cloud Hosted Router-6-34-1-AutogenByAWSMP- This security group was generated by AWS Marketplace and is based on recommended settings for Cloud Hos
<input type="checkbox"/>	sg-d1ed35b6	Cloud Hosted Router-6-34-1-AutogenByAWSMP-1This security group was generated by AWS Marketplace and is based on recommended settings for Cloud Hos
<input checked="" type="checkbox"/>	sg-e5f6bc81	default default VPC security group

Inbound rules for sg-e5f6bc81 (Selected security groups: sg-e5f6bc81)

Type ⁱ	Protocol ⁱ	Port Range ⁱ	Source ⁱ
All traffic	All	All	0.0.0.0/0
SSH	TCP	22	0.0.0.0/0

Cancel Previous **Review and Launch**

Installing CHR on AWS – Step 6



Launch Status



Your instances are now launching

The following instance launches have been initiated: [i-06cfd9dafee68cbb](#) [View launch log](#)



Get notified of estimated charges

Create [billing alerts](#) to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier).

Finally... Winbox ... IP... Connect ...

The screenshot displays the AWS Management Console interface. At the top, the navigation bar shows 'Services', 'Resource Groups', and user information 'nitzan gutman' in 'N. California'. The left sidebar contains navigation options like 'EC2 Dashboard', 'Events', 'Tags', 'Reports', 'Limits', 'INSTANCES', 'IMAGES', 'ELASTIC BLOCK STORE', and 'NETWORK & SECURITY'. The main content area shows a table of EC2 instances with one instance 'i-06cffd9dafee68cbb' of type 't2.micro' in the 'us-west-1c' zone, with a status of 'running'. Below the table, the details for this instance are shown, including 'Public IP: 54.183.162.115'. A 'WinBox v3.7 (Addresses)' window is overlaid on the console, with the 'Connect To:' field containing the IP address '54.183.162.115'. Red circles highlight the public IP in the console details and the IP address in the WinBox window.

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Check
	i-06cffd9dafee68cbb	t2.micro	us-west-1c	running	Initializin

Instance: i-06cffd9dafee68cbb Public IP: 54.183.162.115

Property	Value
Instance ID	i-06cffd9dafee68cbb
Instance state	running
Instance type	t2.micro
Elastic IPs	
Public DNS (IPv4)	-
IPv4 Public IP	54.183.162.115
IPv6 IPs	-
Private DNS	ip-192-168-30-176.us-west-1.compute.internal
Private IPs	192.168.30.176
Secondary private IPs	
VPC ID	vpc-43f5f5
Subnet ID	subnet-b197

WinBox v3.7 (Addresses)

Connect To: 54.183.162.115

Keep Password

Open In New Window

Buttons: Add/Set, Connect To RoMON, Connect

Change Password !!!

CHR - Use case Types

- Virtual Instance
 - ✓ Custom hardware
 - ✓ Management - Dude ,RADIUS
 - ✓ Labs setup



Virtualization – CHR vs x86

Why use the CHR instead of the traditional x86 VM?

- Optimized for Virtualization
 - 64 bit support
 - Fastpath support
 - Driver support
- Paravirtualized NIC –
 - Using the CHR allows us to use the a paravirtualized NIC which is capable of speeds beyond 10 Gbps.
 - The E1000 NIC used in the x86 VM is only capable of 1Gbps.
- Future proof – The CHR will continue to be developed

CHR - Use case Types

- **Cloud Connectivity**
 - ✓ VPN cloud - Road Warrior
 - ✓ Direct Connect alternative
 - ✓ Secure distributed cloud environment



CHR - Use case Types

- **Cloud monitoring**
 - ✓ Cyber Defense
 - ✓ Billing Logic on Steroids
 - ✓ Centralized Log Analyze



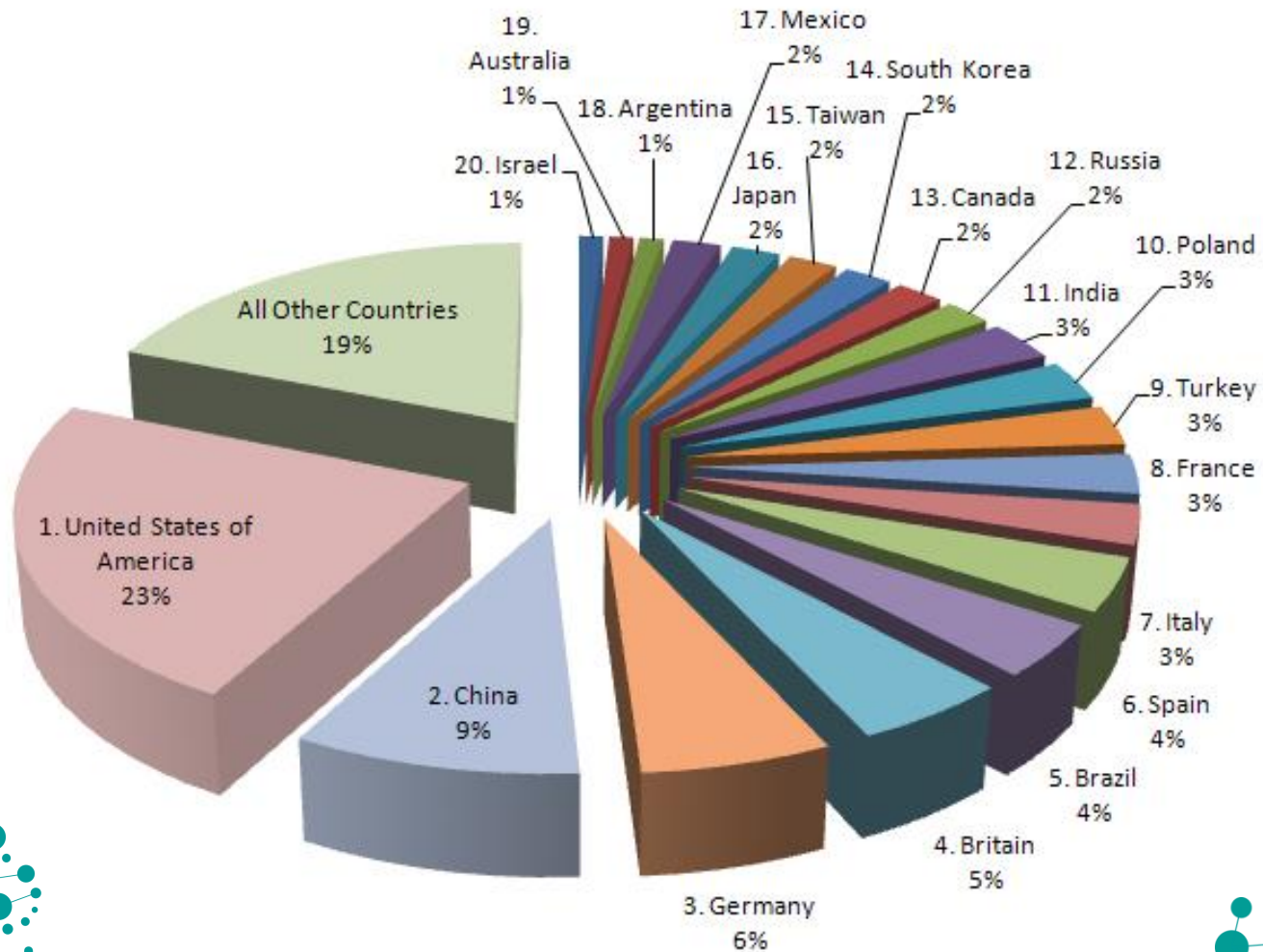
CYBERWAR

END OF
THE
WORLD

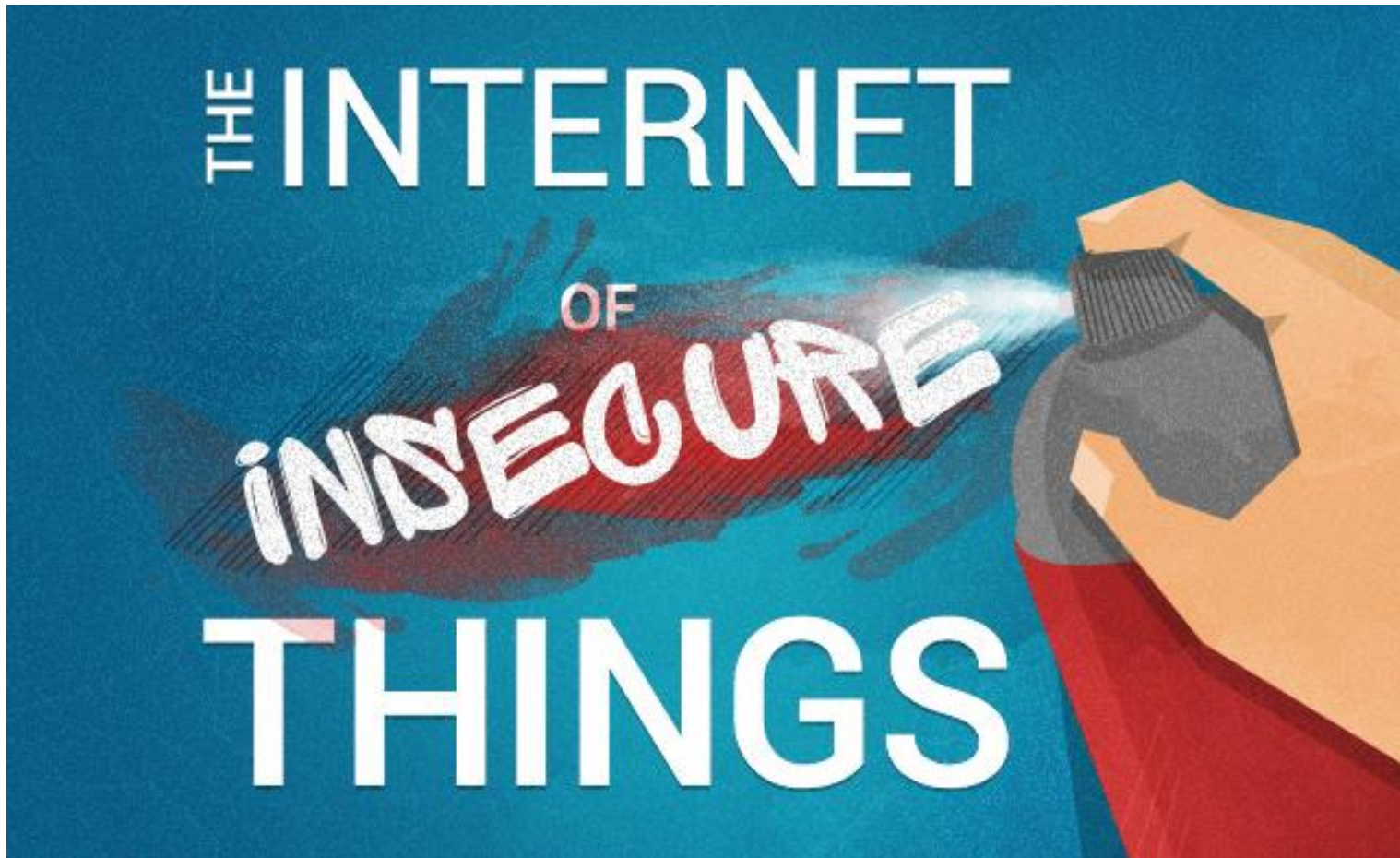
(AS WE KNOW IT)

THE UNIVERSITY OF ALABAMA

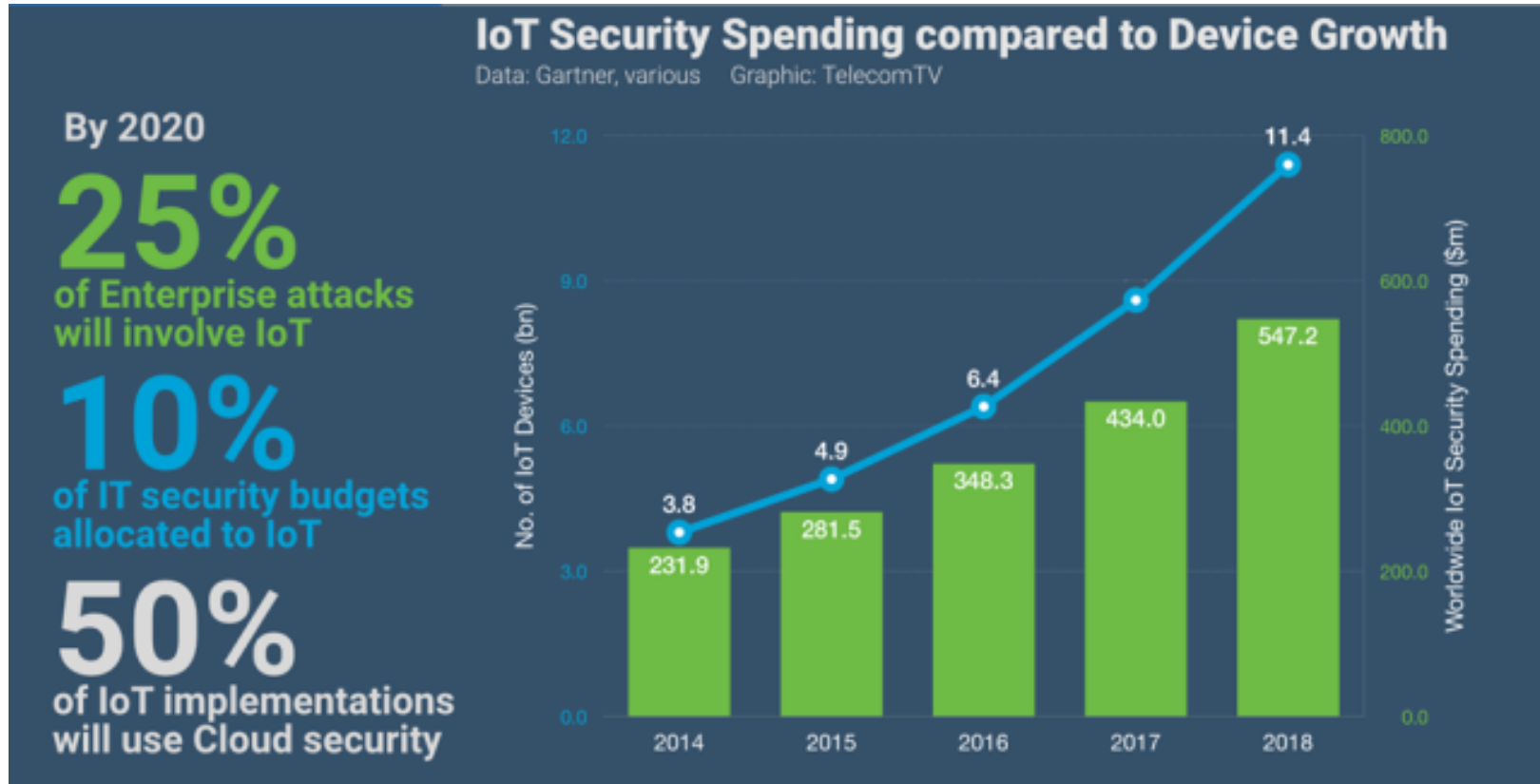
Cyber crime top 20 countries attracts



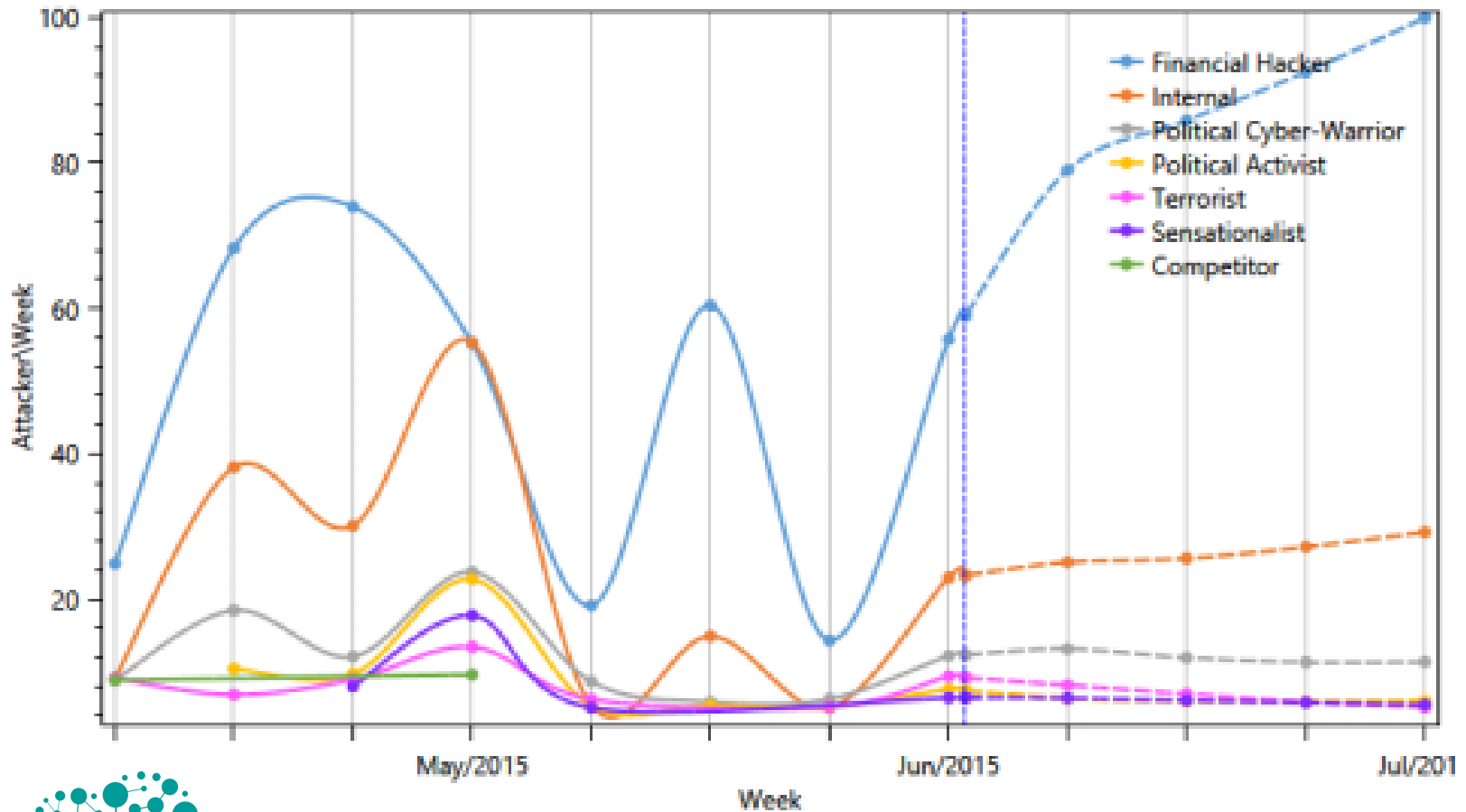
IOT – the missing S



General background on cyber attracts



Who is behind cyber crime ?





CALVIN DIDN'T REALISE THAT IN JUST 3 SECONDS HE'D
HAVE A 2ND CHANCE TO MAKE A 1ST IMPRESSION...



How to ship your data(Syslog)

The screenshot shows the Mikrotik WinBox interface with several windows open, illustrating the steps to configure Syslog logging:

- Step 1:** The **Logging** menu is selected in the left sidebar.
- Step 2:** The **Logging** window shows a table of logging rules:

Name	Type
MyPaStash	remote
* disk	disk
* echo	echo
* memory	memory
* remote	remote

Step 3: The **Log Action <MyPaStash>** window is shown with the following configuration:

- Name: MyPaStash
- Type: remote
- Remote Address: 66.66.66.66
- Remote Port: 514
- Src. Address: (empty)
- BSD Syslog
- Syslog Facility: 3 (daemon)

Step 4: The **Logging** window shows a table of logging rules with actions:

Topics	Prefix	Action
* critical		echo
* error		memory
* info		memory
* warning		memory
warning		MyPaStash

Step 5: The **Log Rule <warning>** window is shown with the following configuration:

- Topics: warning
- Prefix: (empty)
- Action: MyPaStash

How to ship your data (NetFlow)

The screenshot shows the Mikrotik WinBox interface with the following configuration steps highlighted:

- 1**: The 'Traffic Flow' menu item in the left sidebar.
- 2**: The 'Targets' button in the 'General' tab of the NetFlow configuration window.
- 3**: The '+' (Add) button in the 'Traffic Flow Targets' table.
- 4**: The 'OK' button in the 'Traffic Flow Target' dialog box.

Address	Port	Version
66.66.66.66	1234	9

```
/ip traffic-flow  
set cache-entries=4M enabled=yes  
interfaces=BRIDGE
```

```
/ip traffic-flow target  
add dst-address=66.66.66.66  
port=1234 version=5
```

Shipping Big Data Log

- **paStash** is a tool to manage spaghetti I/O with input, processors and output.
- modules for all seasons and protocols.



<https://github.com/sipcapture/paStash>

PaStash Config



```
input {
  udp {
    host => 0.0.0.0
    port => 514
    type => syslog
  }
}

filter {
  regex {
    regex => /^(S)/+/
    fields => [toto]
  }
}

output {
  elasticsearch {
    host => localhost
    port => 9200
  }
}
```

Input plugins

- [File](#)
- [Syslog](#)
- [ZeroMQ](#)
- [Redis](#)
- [HTTP](#)
- [Websocket](#)
- [TCP / TLS](#)
- [Google app engine](#)
- [AMQP](#)
- [SQS](#)
- [NetFlow](#)
- [Freeswitch ESL](#)
- [Asterisk AMI](#)

Filter plugins

- [Regex](#)
- [Grok](#)
- [Mutate Replace](#)
- [Grep](#)
- [Reverse DNS](#)
- [Compute field](#)
- [Compute hash](#)
- [Compute date field](#)
- [Split](#)
- [Rename](#)
- [Multiline](#)
- [Json fields](#)
- [Geoip](#)
- [Eval](#)
- [Bunyan](#)
- [HTTP Status Classifier](#)

Outputs

- [ZeroMQ](#)
- [ElasticSearch](#)
- [Statsd](#)
- [Gelf](#)
- [File](#)
- [HTTP Post](#)
- [Websocket](#)
- [Redis](#)
- [Logio](#)
- [TCP / TLS](#)
- [AMQP](#)
- [SQS](#)
- [HEP](#)

Parsing Mikrotik Netflow

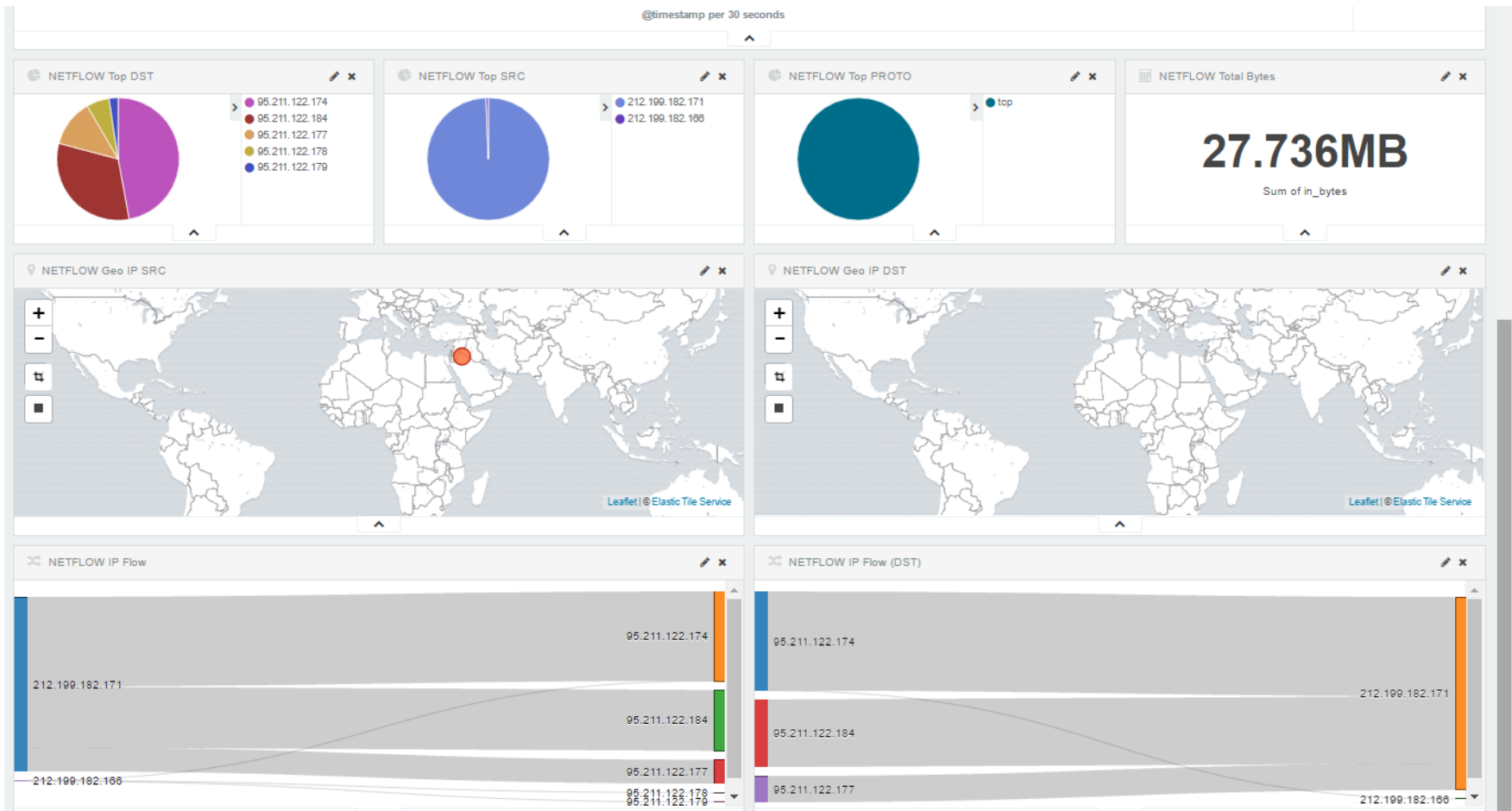
Doc: netflow-2017.03.31/netflow/AVsjaW0eN5kWO_T6cPTP

Table	JSON
⊙ @timestamp	March 31st 2017, 11:09:34.395
‡ @version	1
‡ _id	AVsjaW0eN5kWO_T6cPTP
‡ _index	netflow-2017.03.31
# _score	1
‡ _type	netflow
# dst_mask	0
⊙ first_switched	January 23rd 1970, 10:33:58.552
# fsId	256
# in_bits	640
# in_bytes	80
‡ in_dst_mac	000000000000
# in_pkts	2
# input_snmp	11
📄 ipv4_dst_addr	199.58.84.53
‡ ipv4_dst_addr_geo_city	Wilmington
‡ ipv4_dst_addr_geo_country	US

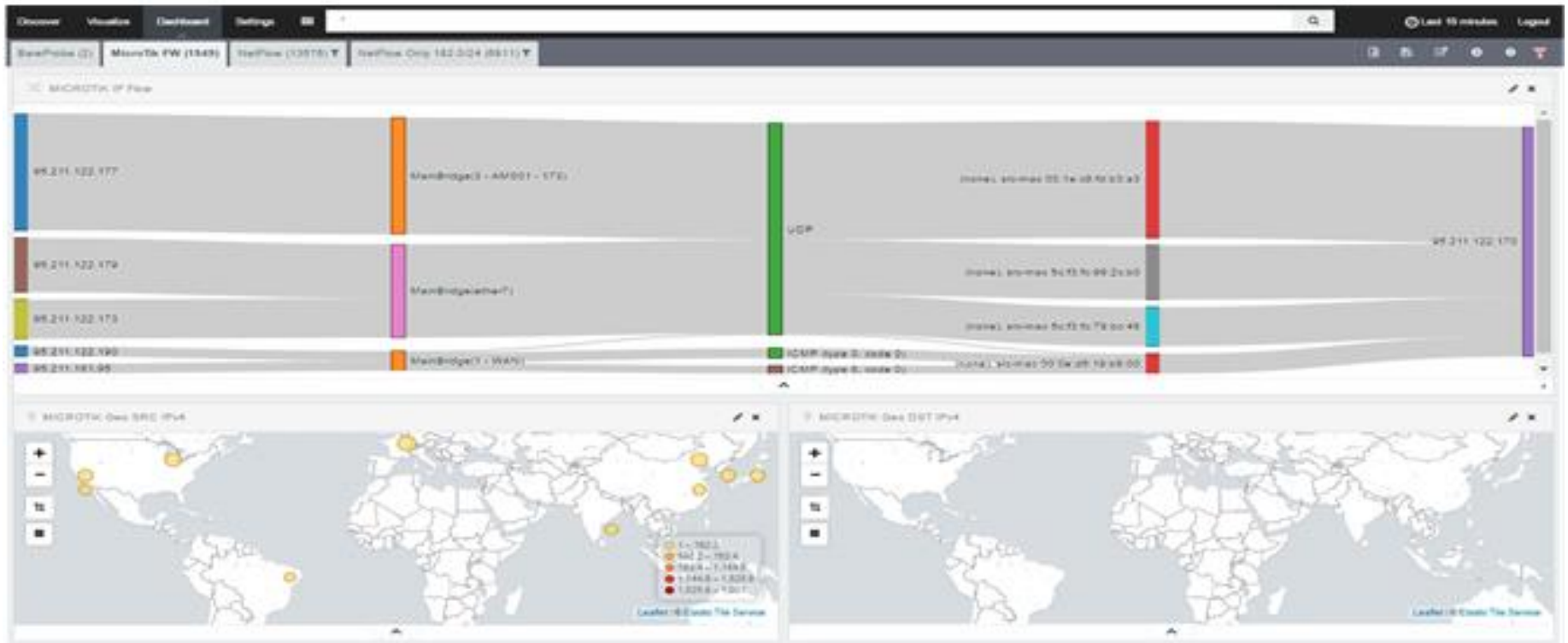
Parsing Mikrotik Log

Table	JSON
@timestamp	March 31st 2017, 11:12:22.635
@version	1
_id	AVsja_d1N5kWO_T6ccba
_index	mikrotik-2017.03.31
_score	1
_type	firewall
action	input
dstip	95.211.122.170
dstip_geo_country	NL
dstip_geo_lonlat	4.9, 52.3667
dstport	53
host	95.211.122.170
in	MairBridge(ether7)
len	66
logsource	info
message	firewall,info input: in:MairBridge(ether7) out:(none), src-mac 5c:f3:fc:79:bc:48, proto UDP, 95.211.122.173:48095->95.211.122.170:53, len 66
out	(none), src-mac 5c:f3:fc:79:bc:48
parsed	true
srcip	95.211.122.173
srcip_geo_country	NL
srcip_geo_lonlat	4.9, 52.3667
srcport	48,095

Mikrotik Netflow Dashboards



Mikrotik Logs Dashboards



Elasticsearch

Elasticsearch is a search engine based on Lucene. It provides a distributed, multitenant-capable full-text search engine with an HTTP web interface and schema-free JSON documents.



elastic

Siren alerting & reporting application

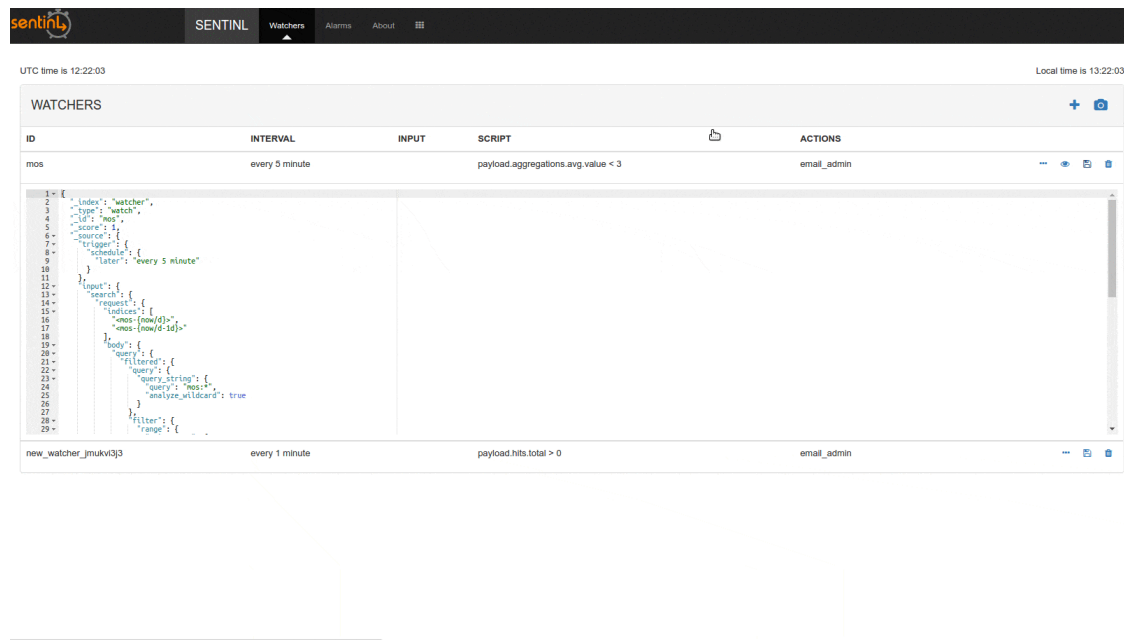
SENTINL extends Siren with Alerting and Reporting functionality to monitor, validate and inform users and administrators on data series changes using standard queries or join queries, programmable validators, transformers and messages to send out using a variety of configurable actions including sending action to the Mikrotik API as well as sending Emails, Slack Messages, API Webhooks, PDF Snapshots of Charts, creating new Documents and much more.



Siren Alerting & Reporting App

Siren

Enterprise provides many unique features and enables integrators to realize unique Business Intelligence creatures. With such power, automating workflows and being able to get notified with data detections quickly becomes a key requirement.



The screenshot displays the Siren Alerting & Reporting App interface. The top navigation bar includes the Siren logo, "SENTINL", and menu items for "Watchers", "Alarms", and "About". The main content area is titled "WATCHERS" and features a table with columns for ID, INTERVAL, INPUT, SCRIPT, and ACTIONS. Two watchers are listed: "mos" and "new_watcher_jmukvi3j3". The "mos" watcher is selected, and its configuration is shown in a code editor. The configuration includes a trigger set to "every 5 minute" and a script that performs a search on the "mos" index, filtering for "Mos" in the "message" field and analyzing the "urlcard" field. The script also includes a filter for "range".

ID	INTERVAL	INPUT	SCRIPT	ACTIONS
mos	every 5 minute	payload.aggregations.avg.value < 3		email_admin
new_watcher_jmukvi3j3	every 1 minute	payload.hits.total > 0		email_admin

```
1- {
2   "index": "watcher",
3   "type": "watch",
4   "if": "log",
5   "score": 5
6   "source": {
7     "trigger": {
8       "schedule": {
9         "later": "every 5 minute"
10      }
11    }
12  }
13  "input": {
14    "request": {
15      "indices": [
16        "mos-{now/d}",
17        "mos-{now/d-1d}"
18      ]
19    }
20    "body": {
21      "query": {
22        "filtered": {
23          "query_string": {
24            "query": "Mos*",
25            "analyze_urlcard": true
26          }
27        }
28      }
29    }
30  }
31  "filter": {
32    "range": {
```



Pushing your **data** out of the **box**



clusterz.io

Contact us today for a month free trial

info@clusterz.io

THANK YOU!

