

# BLOX FEST

Infoblox 



# Andrew St Jean

Solutions Developer –  
Empowered Networks



# Topics Covered

- NetMRI Overview
- Compliance Policies and Rules
- Change Scripts and Jobs
- Triggering Jobs using Compliance Rules
- Q&A

# NetMRI Overview – Common Pain Points

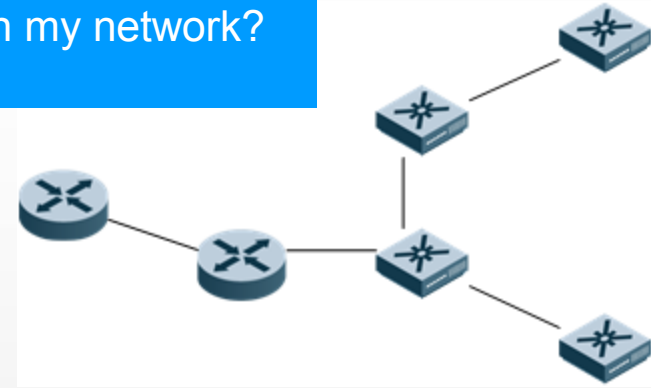
So many changes, so little time.

service timestamps debug uptime	✓
service timestamps log uptime	✓
no service password-encryption	✗
↓	
service timestamps debug uptime	✓
service timestamps log uptime	✓
service password-encryption	✓



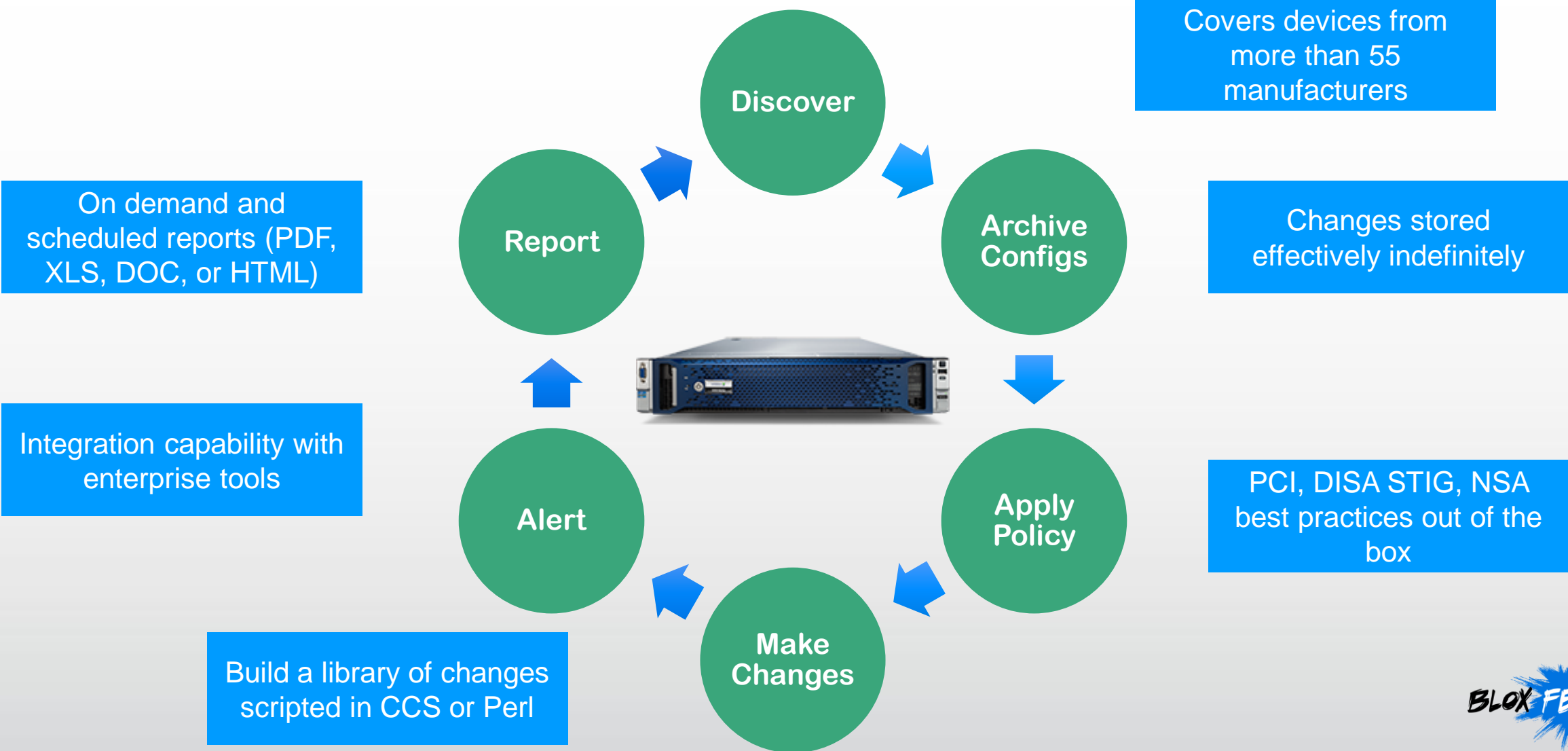
Are my devices configured the way they should be?

What's in my network?



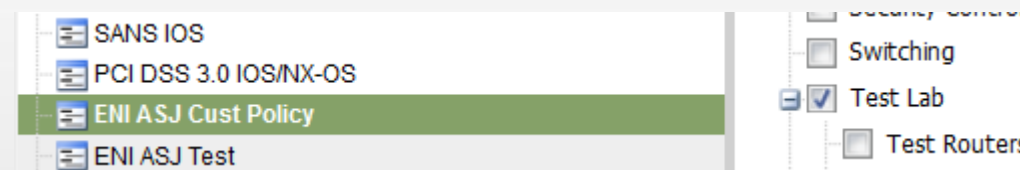
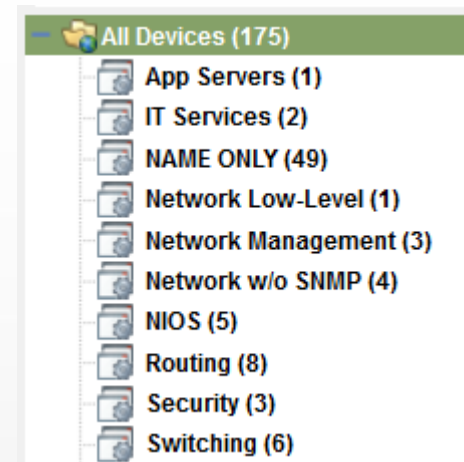
service timestamps debug uptime	✓
service timestamps log uptime	✓
no service password-encryption	✗

# NetMRI Overview



# NetMRI Overview – Device Groups

- Used to group and organize managed devices
- Used as targets for compliance policies and change scripts
- Are dynamic



```
$Assurance > 75 and $Type in ["Router","Switch-Router"]
```

# NetMRI Overview - Issues

- Tell you when there is a problem with a device
- Compliance policy violations can raise Issues
- Change scripts can raise Issues

Severity ▲	Last Seen	Title	# Affected	# New	# No Change	# Cleared	# Suppressed
Error	2016-03-08 10:11:36	<a href="#">VLAN Member Priority</a>	1	0	1	0	0
Error	2016-03-08 10:11:26	<a href="#">VLAN Member Minimum Priority</a>	1	0	1	0	0
Error	2016-03-08 10:11:11	<a href="#">Device Issue Limit Exceeded</a>	1	0	1	0	0
Error	2016-03-08 10:10:11	<a href="#">Access Port With PortFast Disabled</a>	14	0	14	0	0
Error	2016-03-08 10:10:11	<a href="#">Trunk Port With PortFast Enabled</a>	1	0	1	0	0
Error	2016-03-08 09:42:28	<a href="#">Policy Violation: ENI ASJ Cust Policy</a>	3	0	3	0	0
Error	2016-03-08 09:42:28	<a href="#">Policy Violation: ENI ASJ Test</a>	3	0	3	0	0
Error	2016-03-08 09:42:27	<a href="#">Policy Violation: ENI JP Cust Policy</a>	3	0	3	0	0
Warning	2016-03-08 10:47:27	<a href="#">Interface Not Stable</a>	3	0	3	0	0
Warning	2016-03-08 10:42:27	<a href="#">Unidirectional Traffic Flow</a>	1	0	1	0	0
Warning	2016-03-08 10:13:45	<a href="#">Device Fan Problem</a>	2	0	2	0	0

**Config Running Not Saved** In: All Devices (175)  
Showing details for All Devices group

**Component:** Configurations      **Correctness:** -0.5  
**Severity:** Info                      **Stability:** 0.0  
**Last Seen:** 2016-03-09 09:28:08

**Components Affected by Issue (Current)**

Search... Views Filters Display [Icons]

Device Name	Reboot Time	Changed Time	Saved Time	Time Difference	Last Seen
<a href="#">empasa-pic01</a>	2015-12-14 10:20:21	2016-02-26 10:27:03	2016-01-08 14:05:07	48d 20:21:56	2016-03-09 09:28:08





# Compliance Policies and Rules

- A way to ensure device configurations are what they should be
- Rules check configuration files
- Policies are collections of rules
- Policies are deployed against device groups

**Rule Logic Builder**

Enforce This Rule: if (1) then 2

#	Type	Note
1	Config File Match	Must Contain AT LEAST ONE of These Lines ^username
2	Config File Match	May Not Contain Any of These Lines ^username \S+( privilege \d+)?( nopassword)?\$

**Rules in this Policy**

Name	Severity
PCI 3.0 IOS/NX-OS Two Factor Authentication	error
PCI 3.0 IOS BOOTP Server disable	error
PCI 3.0 IOS CDP Service	info
PCI 3.0 NX-OS CDP Service	info
PCI 3.0 IOS Console Exec 15 Minute Timeout	error
PCI 3.0 NX-OS Console Exec 15 Minute Timeout	error
PCI 3.0 IOS Console Local or AAA Login	error
PCI 3.0 NX-OS Console Local or AAA Login	error

<input type="checkbox"/> DISA v8, r11 STIG Perime	<input type="checkbox"/> Optimizers
<input type="checkbox"/> DISA v8, r11 STIG Perime	<input type="checkbox"/> Ottawa Production Cisco Devices
<input type="checkbox"/> SANS IOS	<input type="checkbox"/> Pickering Production Cisco Devices
<input checked="" type="checkbox"/> PCI DSS 3.0 IOS/NX-OS	<input checked="" type="checkbox"/> Routing
<input type="checkbox"/> ENI ASJ Cust Policy	<input type="checkbox"/> Security





# Compliance Policies and Rules

## Rule types – Simple rules

- Most straightforward to write
- Use regular expression matching to ensure certain commands are present in a configuration file
- Can also ensure certain commands are absent

**Simple Rule:**

Config File Must Contain: AT LEAST ONE of These Lines

```
^ntp authentication-key \d+ md5 \S+
```

Config File May Not Contain: Any of These Lines

```
^ip http server
```

# Compliance Policies and Rules

## Rule types – Rule logic builder rules

- More complex but more versatile
- Combines multiple simple rules
- Can use conditional logic

**Rule Logic Builder**

Enforce This Rule: 1 or 2

#	Type	Note
1	Config File Match	Must Contain AT LEAST ONE of These Lines ^no ip bootp server
2	Config File Match	Must Contain AT LEAST ONE of These Lines ^ip dhcp bootp ignore

**Rule Logic Builder**

Enforce This Rule: if (1) then 2 or 3

#	Type	Note
1	Config File Match	May Not Contain Any of These Lines ^no ip domain(\s -)lookup
2	Config File Match	Must Contain AT LEAST ONE of These Lines ^ip domain(\s -)name .+
3	Config File Match	Must Contain AT LEAST ONE of These Lines ^ip domain(\s -)list .+

# Compliance Policies and Rules

## Rule Types – Raw XML Rules

- Most complex but can do things other rule types can't
- Can access List objects
- Can control message output in raised Issues

List Name: Logging Servers    Description: Syslog servers

<input type="checkbox"/>	Network View	Syslog Server
<input type="checkbox"/>	PIC	192.168.151.33
<input type="checkbox"/>	PIC	192.168.151.34
<input type="checkbox"/>	PIC	192.168.151.254
<input type="checkbox"/>	OTT	192.168.200.90
<input type="checkbox"/>	OTT	192.168.200.92

Message:

Extra NTP servers: 10.47.128.10    Missing NTP servers:

# Compliance Policies and Rules

## Customer use case

The Customer

Power company subject to NERC Critical Infrastructure Protection

The Requirement

Needed a way to demonstrate compliance with CIP requirements

The Solution

Wrote custom compliance rules using existing out of the box rules as starting point

The Result

Built-in compliance reports used to demonstrate compliance with configuration policies





# Change Scripts and Jobs

- Change scripts are used to push changes to network devices

Actions	Name ▲	Language	Run Level	Created By	Updated By	Updated On
⚙️	IOS Debug Mode Left Enabled	CCS	High	admin	admin	2016-02-09 12:07:14
⚙️	IOS Disable Unneeded Services	CCS	High	admin	admin	2016-02-09 12:07:19
⚙️	IOS DNS Configuration	CCS	High	admin	admin	2016-02-09 12:07:15
⚙️	IOS Enable Recommended Interface Settings	CCS	High	admin	admin	2016-02-09 12:07:17

- Running or scheduling a change script creates a job

Actions	Name	Level ▲	Approved By	Schedule	Status
⚙️	Reload Upgraded Routers	High	astjean	Once on March 10 at 02:00 AM	Scheduled

- Job results are viewable in NetMRI

Status	Job ID ▼	Name	Script	Start Time	End Time	Summary Count
✓ OK	20	<a href="#">Run Now [1 Get NIOS Networks]</a>	<a href="#">1 Get NIOS Networks</a>	2016-03-01 10:47:17	2016-03-01 10:49:43	Total: 1, Pending: 0, OK: 1, Error: 0, Other: 0

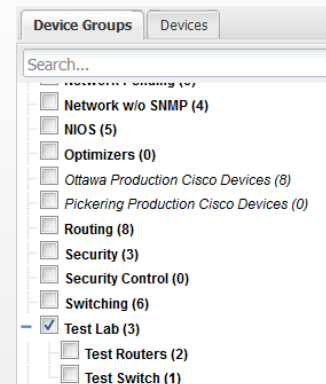


# Change Scripts and Jobs

## Change Script Capabilities

- Can raise Issues
- Can be applied to individual devices and device groups
- Can access List objects

Severity	Generated	Title	Component	# Raised	# Affected
Info	2016-03-16 14:19:33.0	<a href="#">1 SNMP ACL Update Succeeded</a>	Configurations	1	1



List Name: Logging Servers    Description: Syslog servers

<input type="checkbox"/>	Network View	Syslog Server
<input type="checkbox"/>	PIC	192.168.151.33
<input type="checkbox"/>	PIC	192.168.151.34
<input type="checkbox"/>	PIC	192.168.151.254
<input type="checkbox"/>	OTT	192.168.200.90
<input type="checkbox"/>	OTT	192.168.200.92

# Change Scripts and Jobs

## Customer use case

### The Customer

Retail company with thousands of stores

### The Requirement

After router firmware upgrade, wanted to check each device immediately after reload to ensure it was back on the network

### The Solution

Used a change script to reload device and ping until the device responded. Issues raised on success and failure.

### The Result

Change script run against sets of devices. Admins notified via email of job results.



# Triggering Jobs

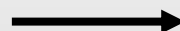
- Change scripts usually run immediately or scheduled by a person



```
2. Action: 'Set SNMP ACL'
13:21:55 Action-Commands
13:21:55 ✓ Command condition matches
13:21:55 $enable_changes eq "on" and $snmp_community ne ""
13:21:55 ✓ config terminal
13:21:56 ✓ snmp-server community brokenbells RO 40
13:21:56 ✓ end
13:21:57 ✓ copy running-config startup-config
```

- Change scripts can also be run automatically, triggered by policy rules

```
✘ Error
Message:
Line 68 matches expression 'snmp-server community .+? R[OW]$'.
```



```
2. Action: 'Set SNMP ACL'
13:21:55 Action-Commands
13:21:55 ✓ Command condition matches
13:21:55 $enable_changes eq "on" and $snmp_community ne ""
13:21:55 ✓ config terminal
13:21:56 ✓ snmp-server community brokenbells RO 40
13:21:56 ✓ end
13:21:57 ✓ copy running-config startup-config
```



# Triggering Jobs

Why use triggered jobs to push changes?

- Low priority problems that don't impact device functioning
- Misconfigurations that open security vulnerabilities



# Triggering Jobs

## Customer use case

The Customer

Oil and gas company subject to PCI audits

The Requirement

Needed to reduce time between the detection of a policy violation and remediation of the violation

The Solution

Use triggered jobs to automatically correct misconfigurations related to PCI standard

The Result

PCI violations are remediated automatically for relevant devices



# Questions?

