ROCHESTER
SECURITY SUMMIT

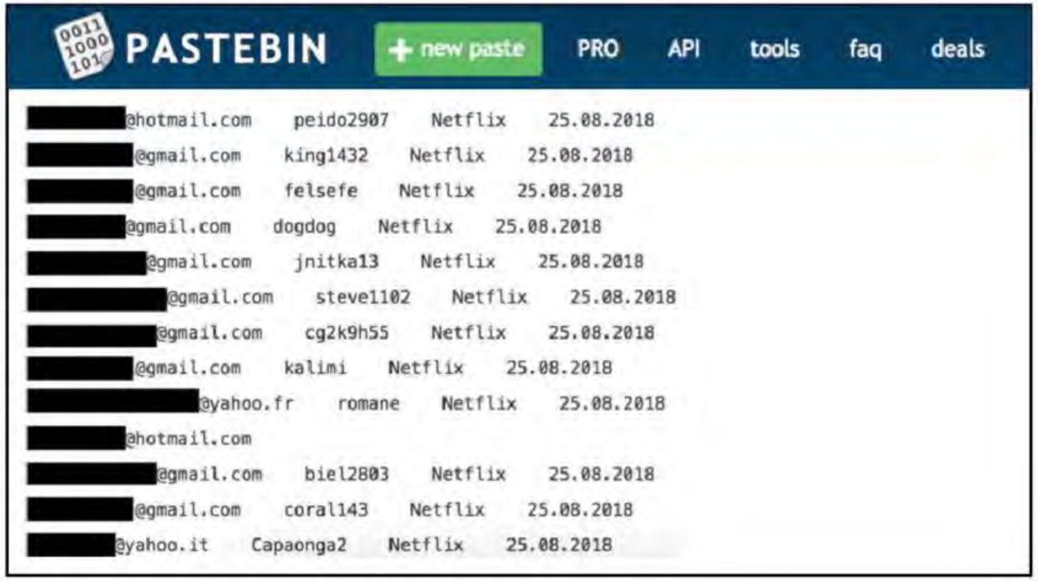
The journey of security automation

Peter Luo
Ph.D., Ex-Microsoft, co-founder@ Tonomy

Agenda

- Security Automation
- Node-RED High Level
- Demo
- Node-RED Deep Dive
  - Nodes
  - Workflow
  - Playbooks
  - Workflow management
- From automation to AI

Threat Monitoring



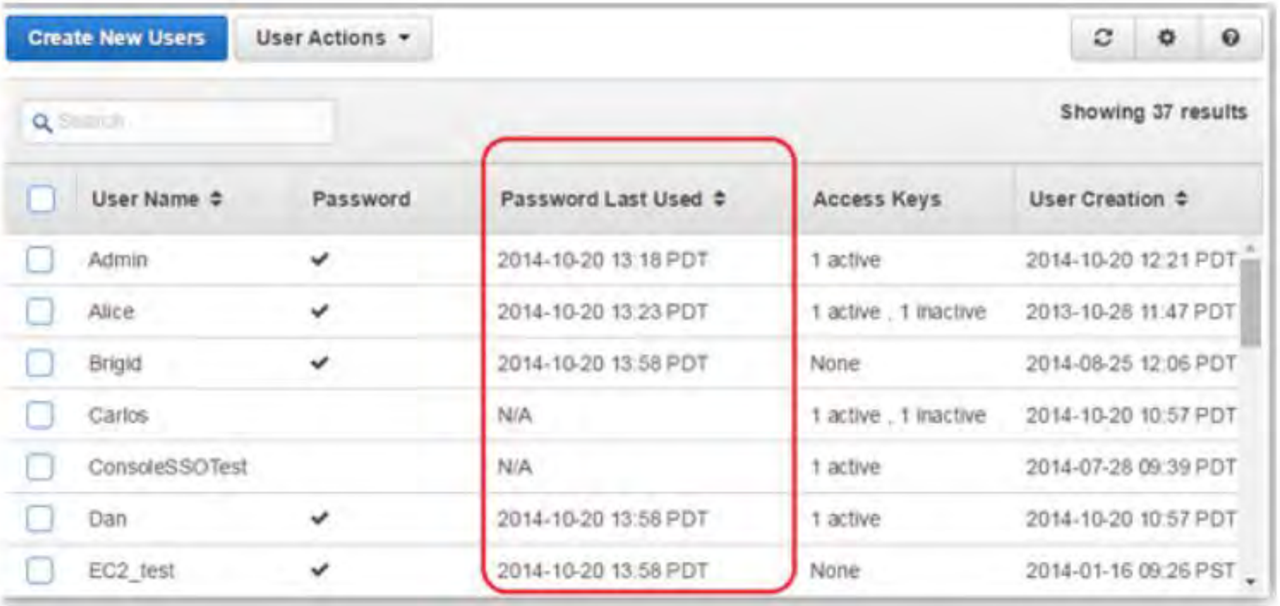
[redacted]@hotmail.com	peido2907	Netflix	25.08.2018
[redacted]@gmail.com	king1432	Netflix	25.08.2018
[redacted]@gmail.com	felsefe	Netflix	25.08.2018
[redacted]@gmail.com	dogdog	Netflix	25.08.2018
[redacted]@gmail.com	jnitka13	Netflix	25.08.2018
[redacted]@gmail.com	steve1102	Netflix	25.08.2018
[redacted]@gmail.com	cg2k9h55	Netflix	25.08.2018
[redacted]@gmail.com	kalimi	Netflix	25.08.2018
[redacted]@yahoo.fr	romane	Netflix	25.08.2018
[redacted]@hotmail.com			
[redacted]@gmail.com	biel2803	Netflix	25.08.2018
[redacted]@gmail.com	coral143	Netflix	25.08.2018
[redacted]@yahoo.it	Capaonga2	Netflix	25.08.2018

How do I know

Is my company’s data leaking here?

Leaking data exchanged online **almost every minute**

Auditing



Showing 37 results

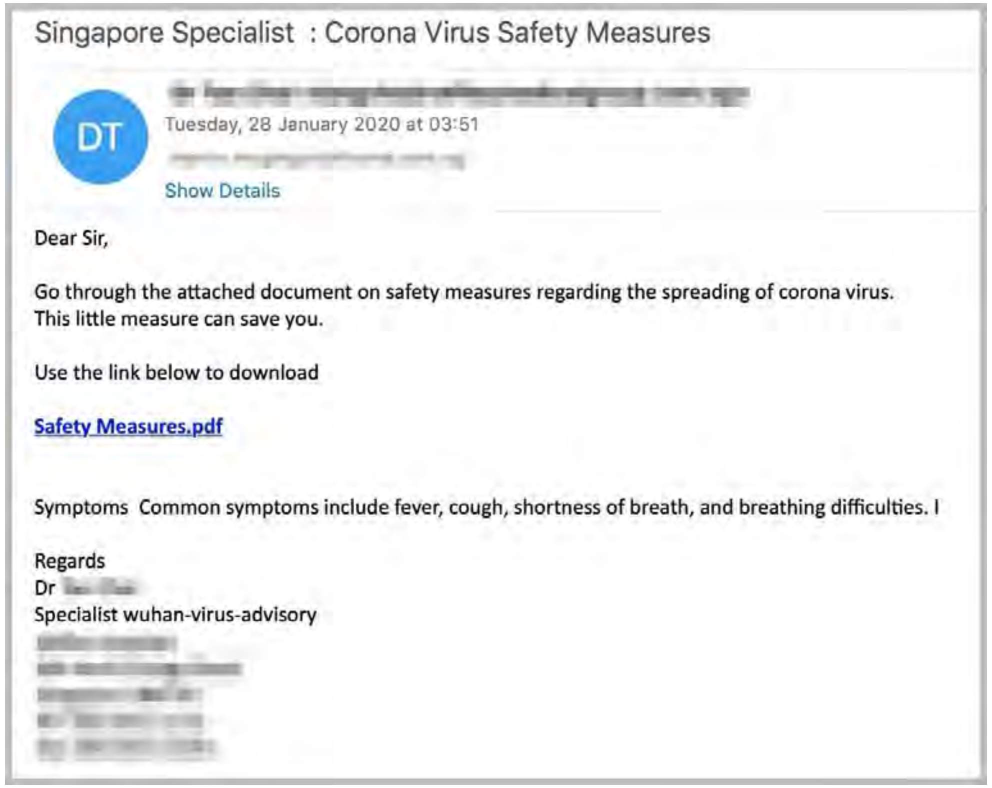
□	User Name ⇕	Password	Password Last Used ⇕	Access Keys	User Creation ⇕
□	Admin	✓	2014-10-20 13:18 PDT	1 active	2014-10-20 12:21 PDT
□	Alice	✓	2014-10-20 13:23 PDT	1 active , 1 inactive	2013-10-28 11:47 PDT
□	Brigid	✓	2014-10-20 13:58 PDT	None	2014-08-25 12:06 PDT
□	Carlos		N/A	1 active , 1 inactive	2014-10-20 10:57 PDT
□	ConsoleSSOTest		N/A	1 active	2014-07-28 09:39 PDT
□	Dan	✓	2014-10-20 13:58 PDT	1 active	2014-10-20 10:57 PDT
□	EC2_test	✓	2014-10-20 13:58 PDT	None	2014-01-16 09:26 PST

How do I ensure every user

- MFA enabled
- Password rotate every 3 months
- Decommissioned user is removed

More than **100s** users I am managing

Investigation



Singapore Specialist : Corona Virus Safety Measures

DT [redacted]

Tuesday, 28 January 2020 at 03:51

[redacted]

Show Details

Dear Sir,

Go through the attached document on safety measures regarding the spreading of corona virus.
This little measure can save you.

Use the link below to download

Safety Measures.pdf

Symptoms Common symptoms include fever, cough, shortness of breath, and breathing difficulties. I

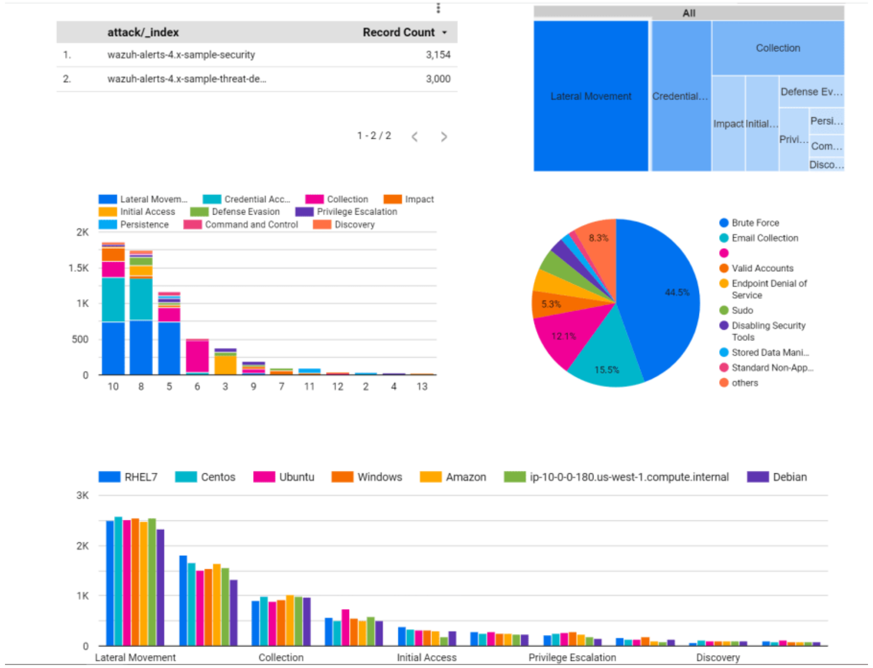
Regards
Dr [redacted]
Specialist wuhan-virus-advisory
[redacted]

Analyze reported phishing?

- Analyze Header
- Analyze URL
- Analyze Attachment
- Analyze Content
- Delete Email

3-5 reported emails/minute, 30 minutes per investigation

Reporting



	attack/_index	Record Count ▾
1.	wazuh-alerts-4.x-sample-security	3,154
2.	wazuh-alerts-4.x-sample-threat-de...	3,000

1 - 2 / 2 < >

Generate reports for different stakeholders for information from different places

- Vulnerability scanner
- End point
- Network
- SIEM
- Etc.

1-2 times every month, data from 5-10 tools needs to be consolidated

Security Control validation

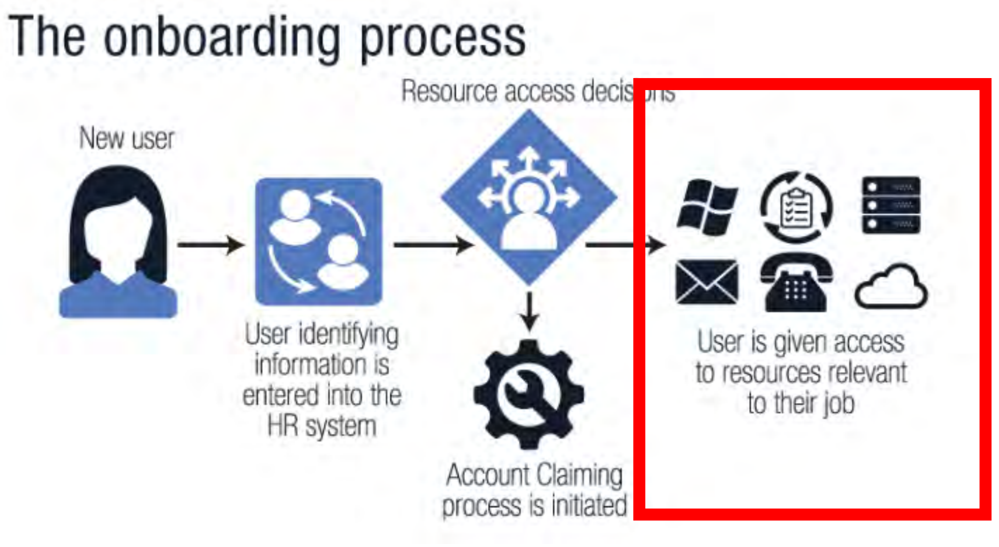
How do I make sure

- DLP is working
- Network detection is working
- Endpoint detection is working
- Etc.

Hackers work any time, need to validate
Continuously

> "Security control validation represents the discipline of ensuring that any controls in place are actually working as required."

Administrative Tasks


The onboarding process
Resource access decisions
New user
User identifying information is entered into the HR system
Account Claiming process is initiated
User is given access to resources relevant to their job

Why do I spend time on

- Adding new people to a list of software
- Remove them when they leave

Am I supposed to work on

- Discover risks
- Mitigate risks

Add users one by one, boring and yet risky

What if we can automate?

What is unique about Node-RED

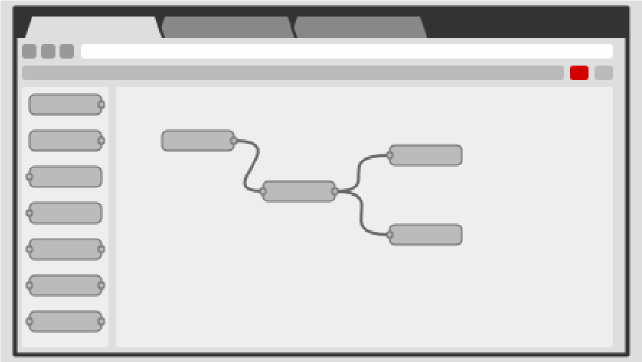
- Less Code or No-Code Platform

- Large community

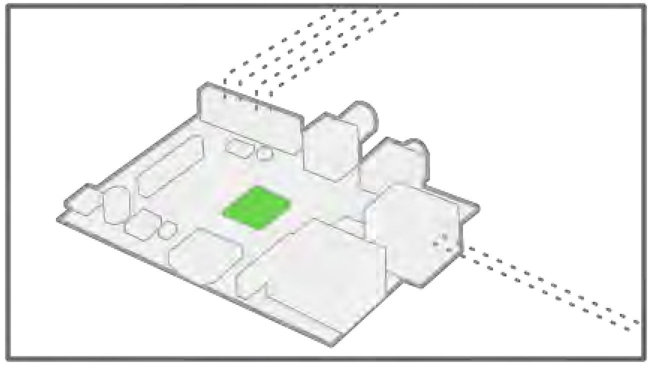
- **>3000** 3rd party integrations

DEMO TIME

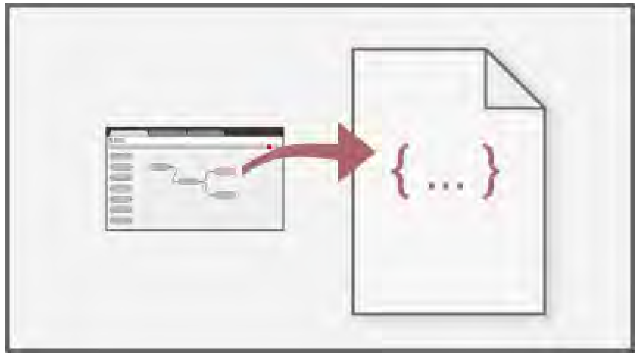
Node-RED high level



Browser-based flow editing

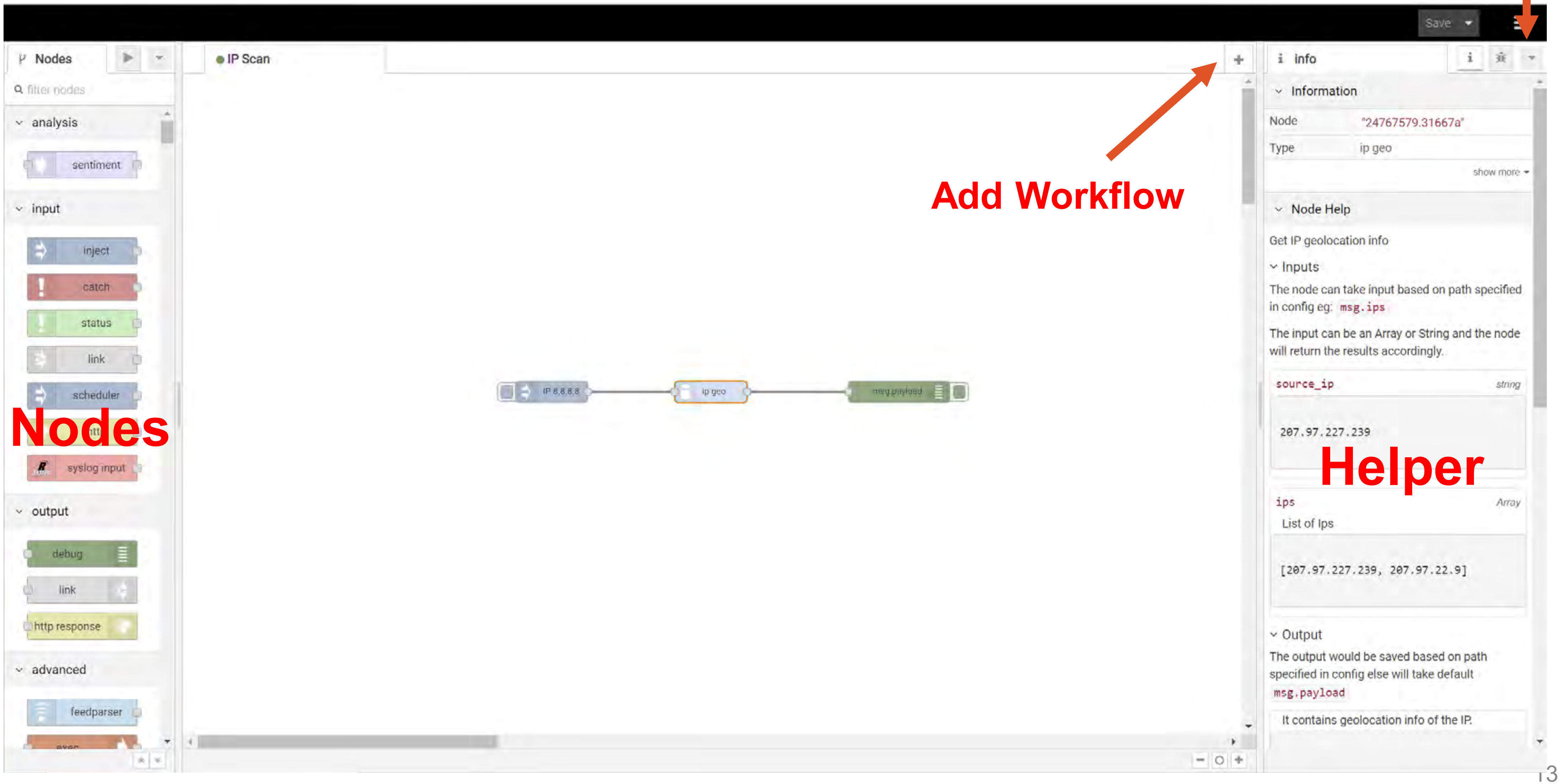


Built on Node.js



Easy Share

Quick View



Get IP geolocation info

Inputs

The node can take input based on path specified in config eg: `msg.ips`

The input can be an Array or String and the node will return the results accordingly.

`source_ip` *string*

```
207.97.227.239
```

`ips` *Array*

List of Ips

```
[207.97.227.239, 207.97.22.9]
```

Output

The output would be saved based on path specified in config else will take default `msg.payload`

It contains geolocation info of the IP.

Nodes

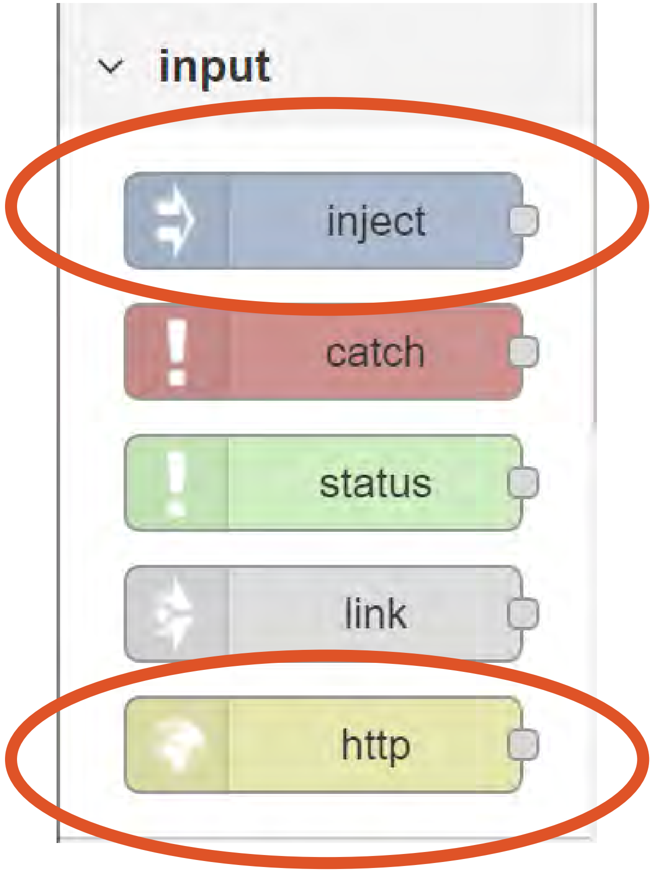
- Input Node

- Output Node

- Utility Function Node

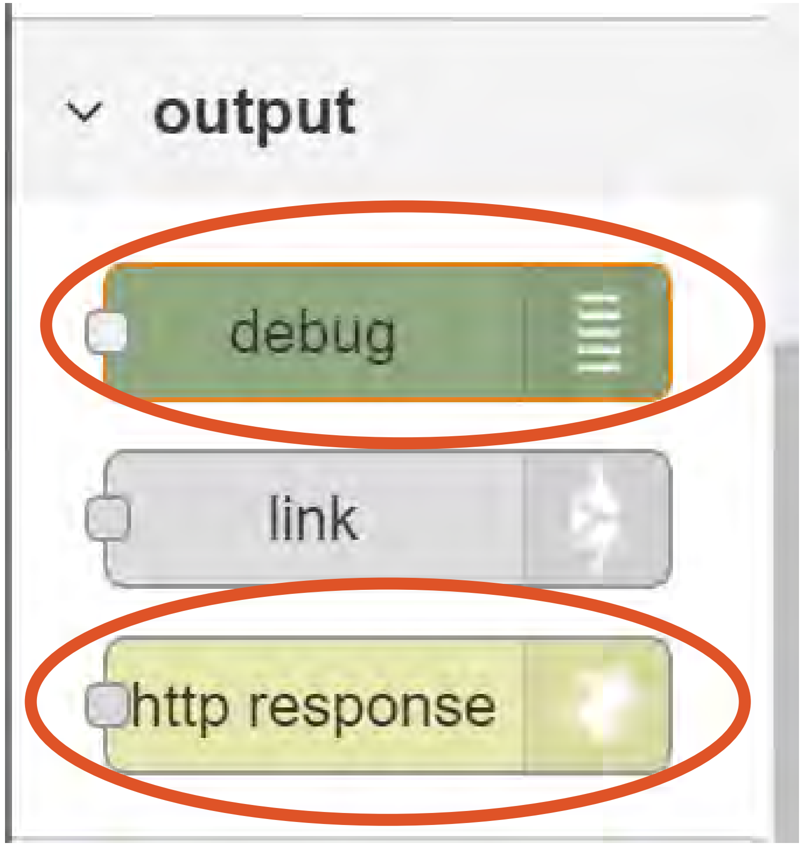
- Third Party Action Node

Input - Output Type

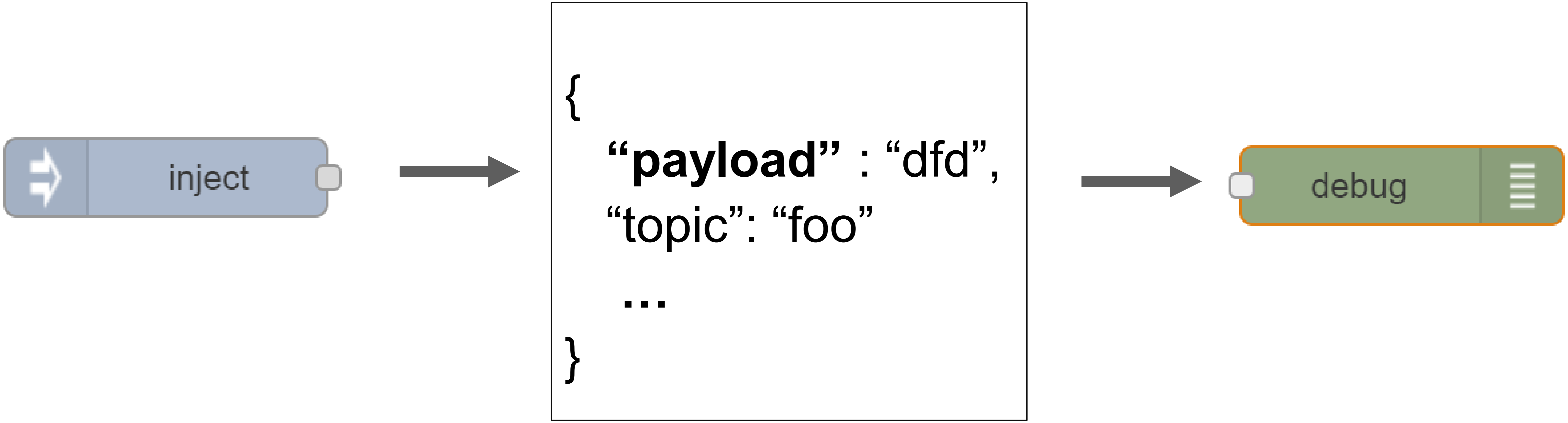


Two Mode:

- **Repetitive/Ad-hoc Task (Proactive)**
- **Rest API (Passive)**



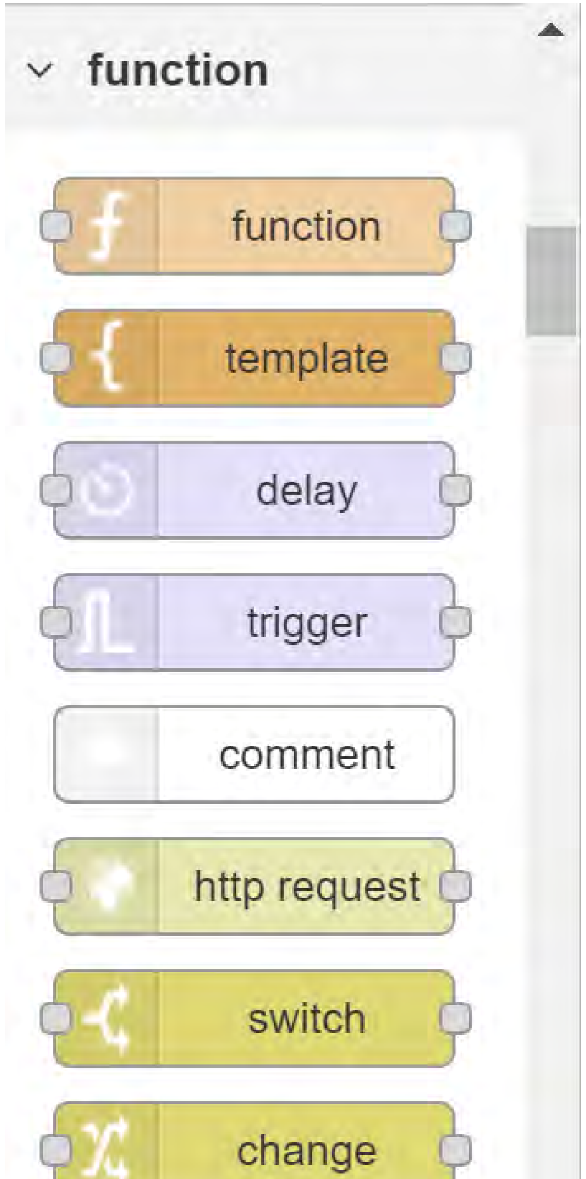
Message passed between nodes

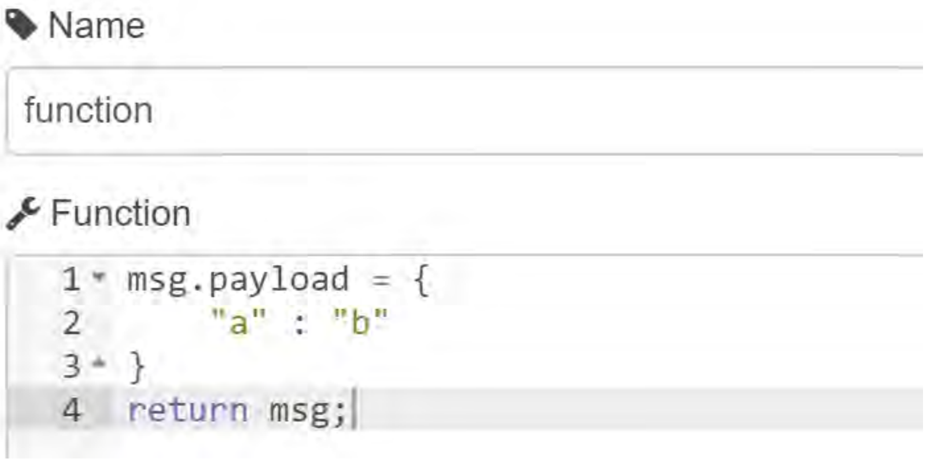


```
{
   “payload” : “dfd”,
   “topic”: “foo”
    ...
}
```

Data Object: msg

More Nodes – Flexible Function

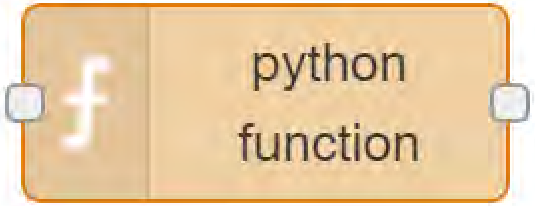


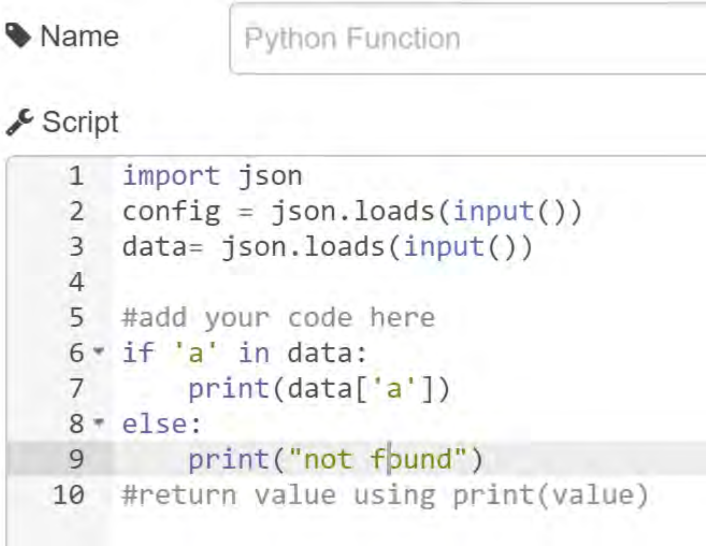

Name

function

Function

```
msg.payload = {
        "a" : "b"
}
return msg;
```




Name Python Function

Script

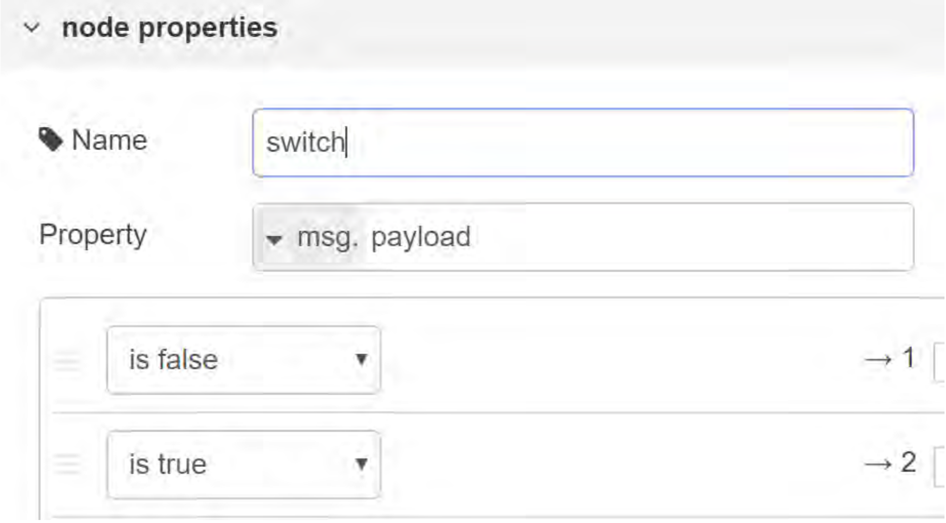
```
import json
config = json.loads(input())
data= json.loads(input())

#add your code here
if 'a' in data:
    print(data['a'])
else:
    print("not found")
#return value using print(value)
```

More Nodes – Logic Function

Splits a message into a sequence of messages.

Joins sequences of messages into a single message.



node properties

Name: switch

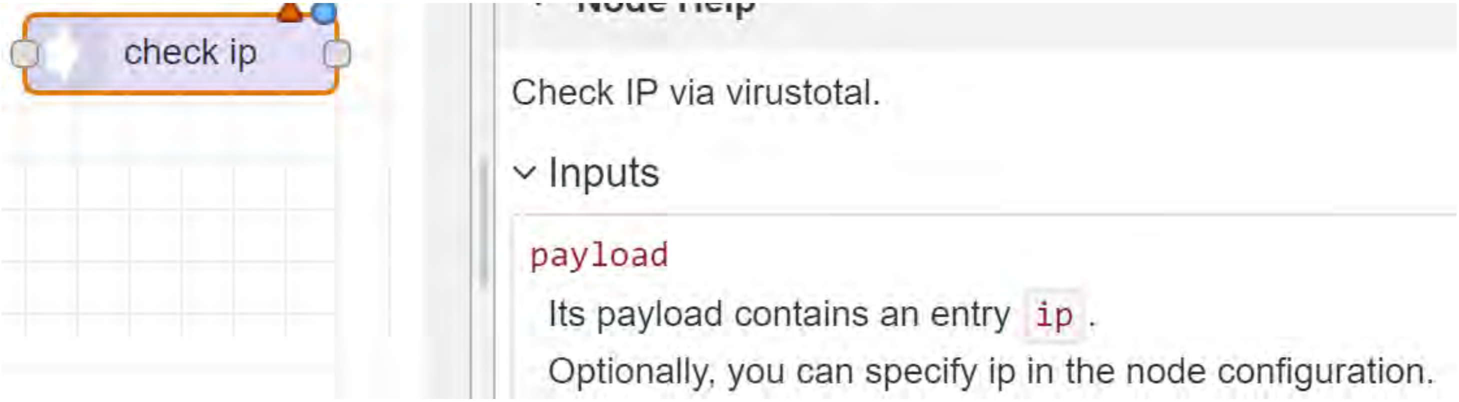
Property: msg. payload

is false → 1

is true → 2

More Nodes – Third Party Integrations

- Alexa Ranking
- Carbon Black
- Crowd Strike
- Have I Been Pwned
- JIRA
- NESSUS
- Rapid7 Nexpose
- Rapid7 Appspider
- Service Now
- Shodan
- ThreatCrowd
- Sumologic
- VirusTotal



Node Help

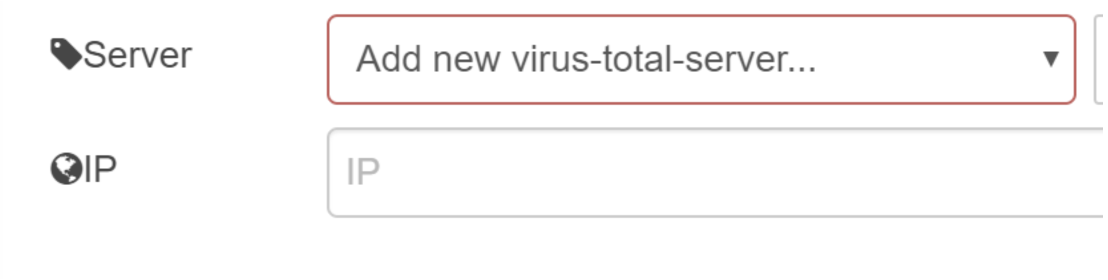
Check IP via virustotal.

Inputs

`payload`

Its payload contains an entry `ip` .

Optionally, you can specify ip in the node configuration.



Server: Add new virus-total-server... ▾

IP: IP

Workflow Management

- Playbooks

- Workflow sharing

More Demos

- IoC extractor
- Phishing Investigation
- Http request
- Report automation

Yes, automation is cool!

Monitoring
Pastebin.com
AdHocUrl

Incident Response
Send email
Enrich Ip
Block Ip

Compliance/Audit
Cloud User audit
Policy Validation

Security Control
DLP verification

Administration
Provision new employees
Dismiss employee

Report
PowerBI
Google Data Studio

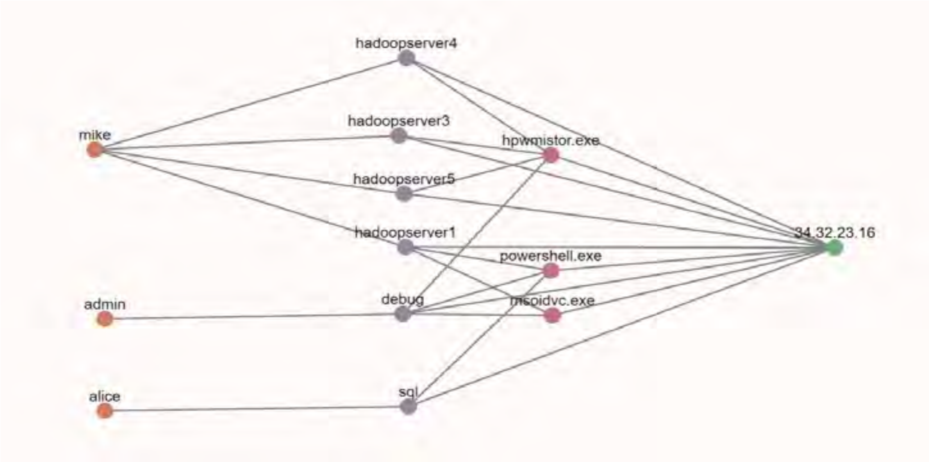
From ad-hoc automation to AI

How do I know if something is truly malicious?

1,000 alerts/day

- Analysis unmanageable
- 10 min/alert = 166 hours/day
- Risks go undetected

False positives easier to identify



300 false positives reduced to 1 story & auto-resolved in future, eliminating future FPs

- Visualizations ease analysis across 17 detection types
- Multiple users making connection to the same IP
- Automated recommendations reduce skills barrier: “Resolve as False Positive”

True positives aligned with MITRE ATT&CK stories

Reported Phishing
8:12:33 | PHISHING | bryan@gmail.com | receiver@phish.com | www.scam.com

Login From Medium Risk Region
13:12:33 | CLOUD | bryan | azure vm1 | 23.34.34.53

Abnormal Process Connection
13:13:33 | END POINT | bryan | azure vm1 | powershell.exe | 34.32.23.12

Beaconing Detected
18:12:33 | NETWORK | bryan | azure vm1 | 34.32.23.12 | every 5 mins

Data Exfiltration
23:12:33 | NETWORK | bryan | azure vm1 | 34.32.23.12

5 detections tell story of Bryan’s account phished, accessed & used for exfiltration

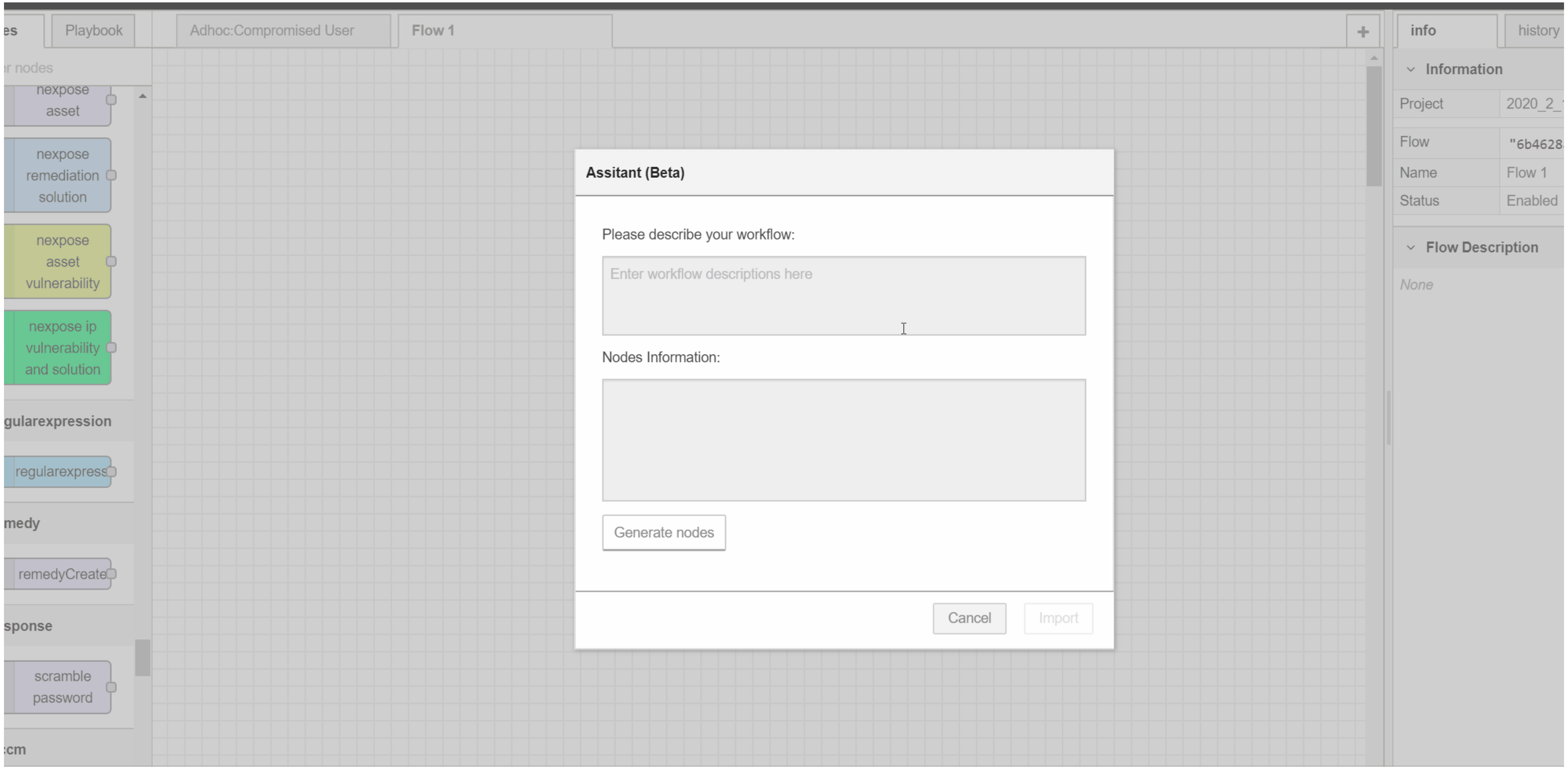
- Timelines speed alert’s story
- Automated recommendations: “Speak with Bryan, isolate & clean host, reset passwords”

Automation vs AI

Process-driven vs **Data-driven**

	Ingest	Enrich	Investigate	Respond	Optimize
	SIEM Email & cloud Network & endpoint Vulnerability	Dedupe alerts Extract artifacts Enrich context	Correlate Prioritize Root cause	Decide & manually respond	Tune alerts Create automation Tune automation
+ Automation		Automate enrichment		Automate preset responses	Drag & drop
+ AI		Automate deduplication Alert intelligence	Discover patterns Correlate alerts Prioritize Suggest root cause	Recommend decision Recommend action	NLP Suggest tuning

Create automation using AI



Assitant (Beta)

Please describe your workflow:

Enter workflow descriptions here

Nodes Information:

Generate nodes

Cancel

Import

Peter Luo

pchluo@dtonomy.com