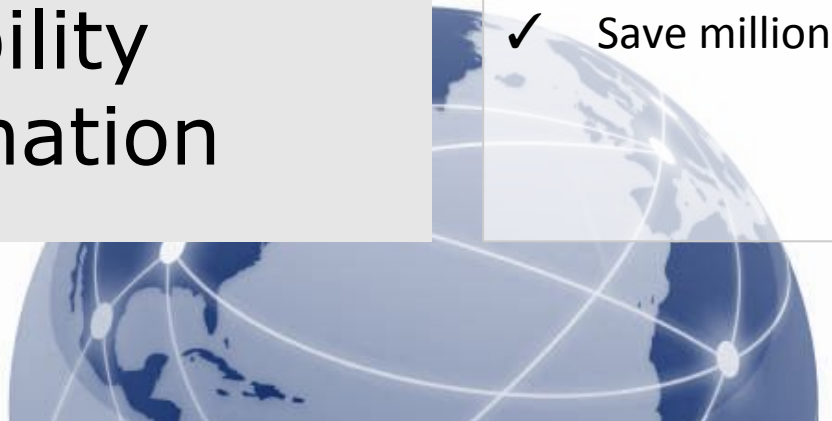
Automate Everything: The Future of Security Automation

Jim MacLeod, Technical Product Marketing

About Indeni

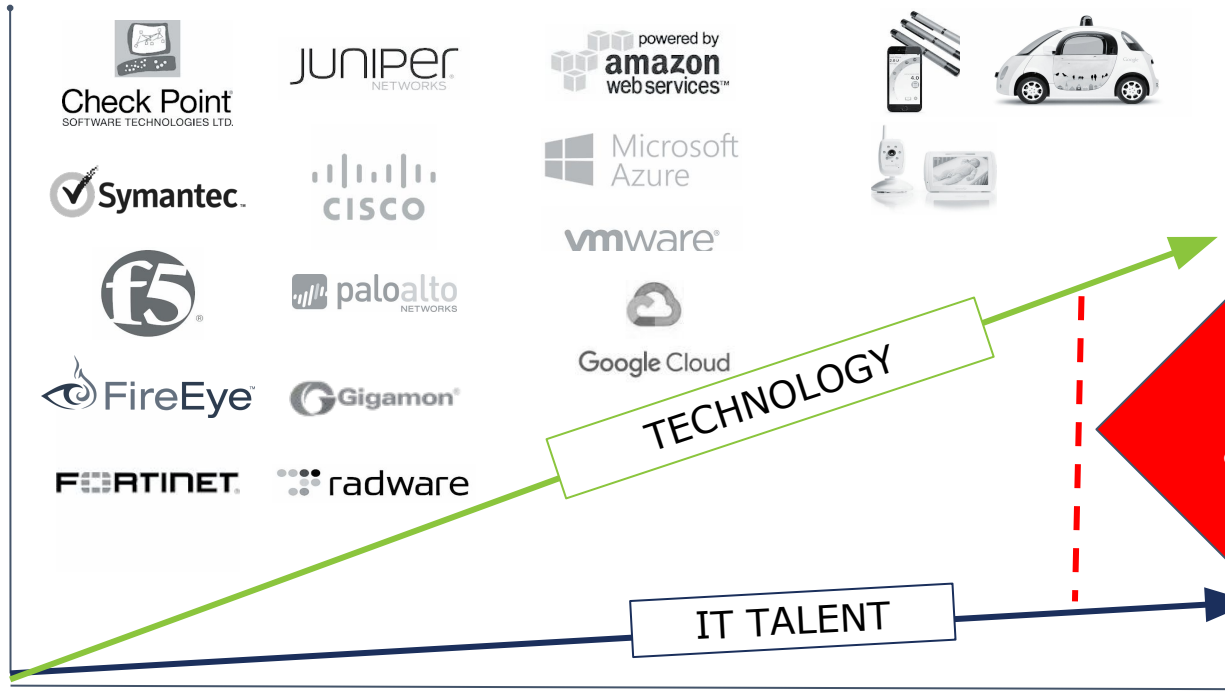
The leader in security infrastructure stability automation

- ✓ **Process 2.5 Billion metrics / day**
- ✓ Significantly reduce risk of outages
- ✓ Save millions of dollars in losses



indeni

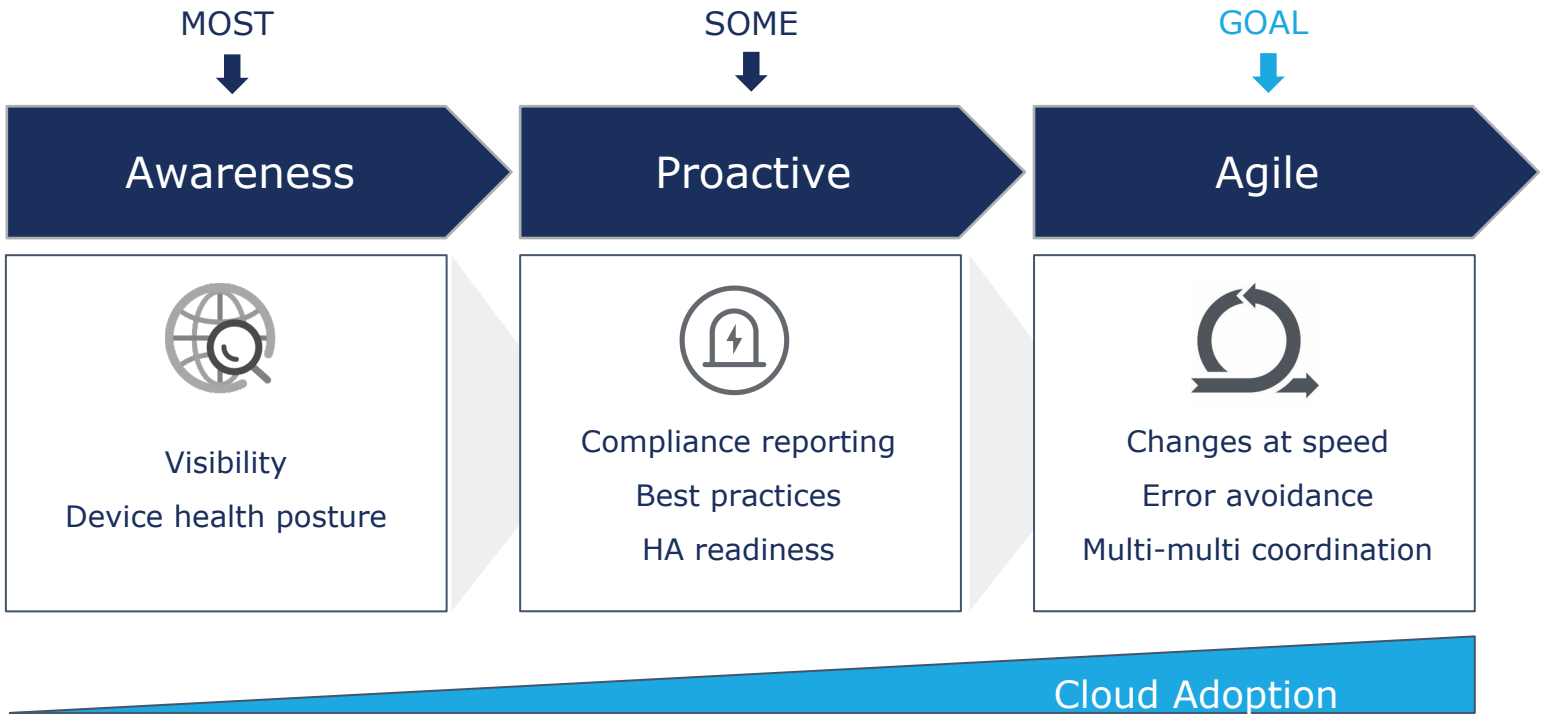
Technology Has Outpaced IT Skill Sets



- **100+** Security technologies
- **67%** Hybrid environments
- **58B** Connected ces by 2020

indeni

Q: How to Achieve Agile IT Operations



indeni

Historically-tested method: Automation!

indeni

So let’s build automation!

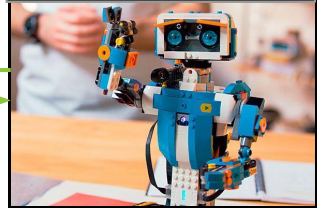
What IT Can Learn From LEGO

Auto binding bricks, 1949

Lego System, 1960

Town, Space, Castle, 1978

STEM Robotics, Today



Everything Works Together

Firewalls

paloalto NETWORKS

Web Proxies

Symantec. + BLUE COAT
Defining the Future of Cyber Security

Load Balancers

f5 radware A10 AVI Networks

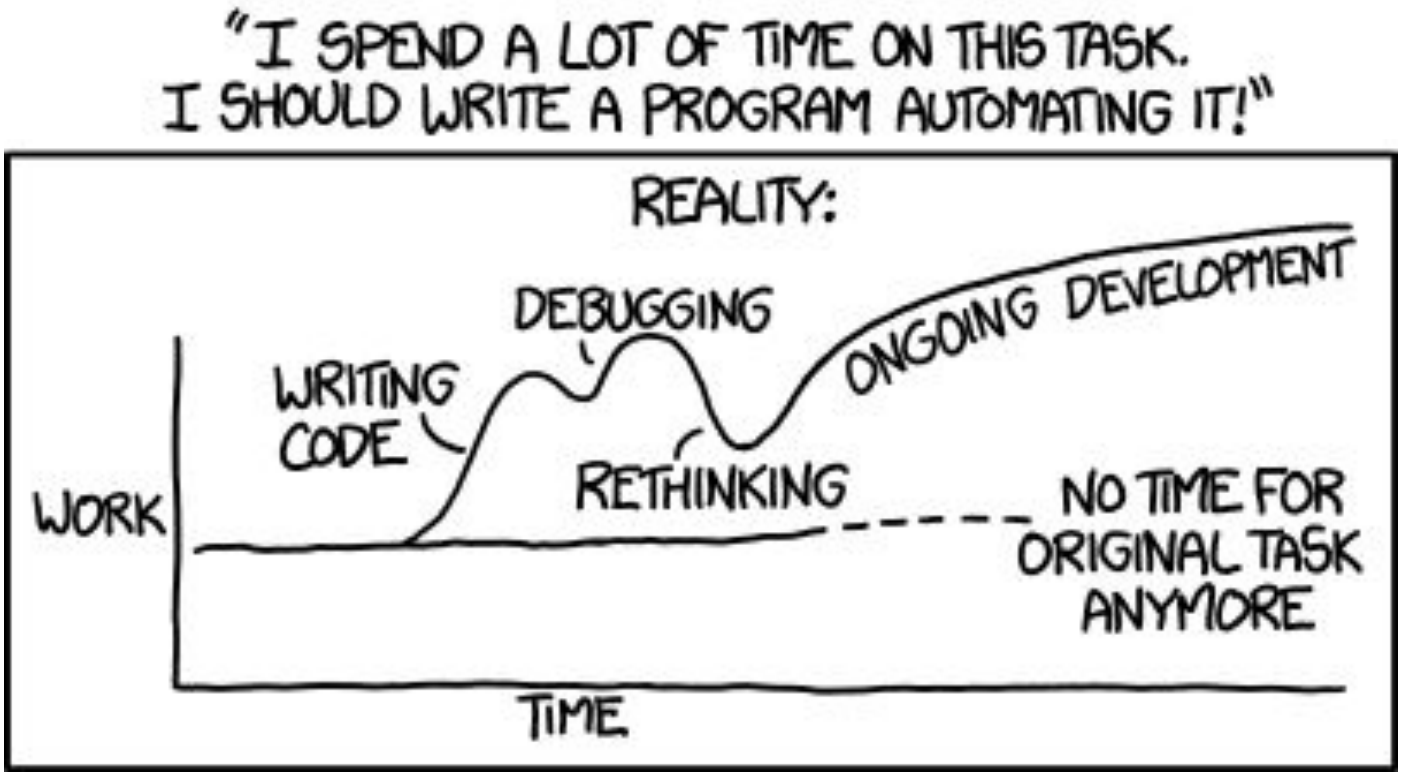
Other Security Devices

No System

indeni

What Happens When The Blocks Don't Fit Together?

Some bricks click easier than others...



indeni

5 Lessons Learned

From 10 years of developing networking and security automation scripts 😅

LESSON #1

CLI outputs will change

Improvements in command outputs can make your life more difficult

- in 9.0:

```
KiB Mem :  7152416 total,  576596 free,  3413104 used,  3162716 buff/cache
```

- in 8.1:

```
Mem:  9208696k total,  8900044k used,  308652k free,  256980k buffers
```

...ndeni-knowledge/parsers/src/panw/panos/show-system-resources/show-system-resources.parser.1.awk

```
#Cpu(s):  2.2%us,  3.5%sy,  0.5%ni, 93.6%id,  0.0%wa,  0.0%hi,  0.2%si,  0.0%st
/Cpu.*%id/ {
    idle = trim($5)
    sub(/%id,/, "", idle)

    cputags["cpu-id"] = "MP"
    cputags["cpu-is-avg"] = "false"
    cputags["resource-metric"] = "true"

    writeDoubleMetric("cpu-usage", cputags, "gauge", 100 - idle, "true", "CPU Usage", "percenta
}

#Mem:   4057012k total,  3540068k used,   516944k free,    89628k buffers
/^Mem/ {
    total_k = $2
    used_k = $4
    buffers_k = $8
    sub(/k/, "", total_k)
    sub(/k/, "", used_k)
    sub(/k/, "", buffers_k)
    used_k = used_k - buffers_k # In linux we shouldn't count "buffers" as used

    mem_tags["name"] = "PA firewall management plane"
    writeDoubleMetric("memory-free-kbytes", mem_tags, "gauge", total_k - used_k, "true", "Memory
    writeDoubleMetric("memory-total-kbytes", mem_tags, "gauge", total_k, "true", "Memory - Tota
}

# Update: memory-usage = (used - (buffers+cached))
# https://live.paloaltonetworks.com/t5/Management-Articles/SNMP-Poll-Reports-Different-Memory-Us
#Swap: 2007992k total,     4408k used,  2003584k free,  1293004k cached
/^Swap/ {
    cached_k = $8
    sub(/k/, "", cached_k)

    mem_tags["resource-metric"] = "true"
    writeDoubleMetric("memory-usage", mem_tags, "gauge", (used_k - cached_k)/total_k*100, "true
}
```

Before

```
#%Cpu(s):  6.4 us,  4.1 sy,  0.4 ni, 88.9 id,  0.0 wa,  0.0 hi,  0.1 si,  0.0 st
/^%Cpu.*id/ {
    idle = $8


    cputags["cpu-id"] = "MP"
    cputags["cpu-is-avg"] = "false"
    cputags["resource-metric"] = "true"

    writeDoubleMetric("cpu-usage", cputags, "gauge", 100 - idle, "true", "CPU Usage", "percenta
}

#KiB Mem :  7152416 total,   363372 free,  3990316 used,  2798728 buff/cache
/^KiB Mem/ {
    total_k = $4

    free_k = $6

    used_k = $8
    buffers_k = $10


    mem_tags["name"] = "PA firewall management plane"
    writeDoubleMetric("memory-free-kbytes", mem_tags, "gauge", free_k, "true", "Memory - Free",
    writeDoubleMetric("memory-total-kbytes", mem_tags, "gauge", total_k, "true", "Memory - Tota
}
END {




    mem_tags["resource-metric"] = "true"
    writeDoubleMetric("memory-usage", mem_tags, "gauge", used_k/total_k*100, "true", "Memory Us
}
```

After

indeni

Quick Notes on Errror-Resistant Code

1. Use “Input Validation”
   a. Screen-scraping is vulnerable to reading the wrong data
   b. Don’t rely on what you’ve read until you sanity-check it
      i. If you’re expecting a number, but you get a word instead…

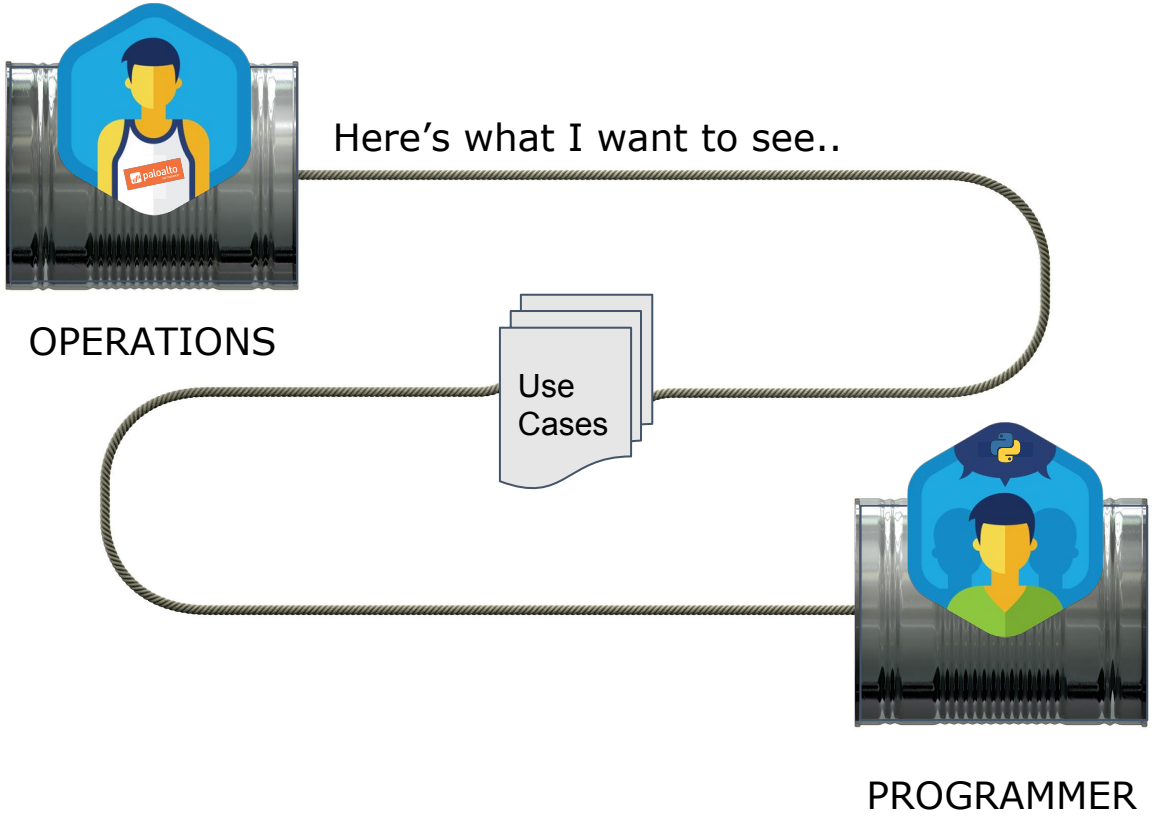
2. Try the “Try/Catch” pattern
   a. Aka “Error handling” or “Don’t just crash”
   b. Something unexpected happened?
      i. Expected exception: do the needful for this scenario
      ii. Unexpected exception: don’t have to stop everything else

indeni

LESSON #2

Don’t play telephone

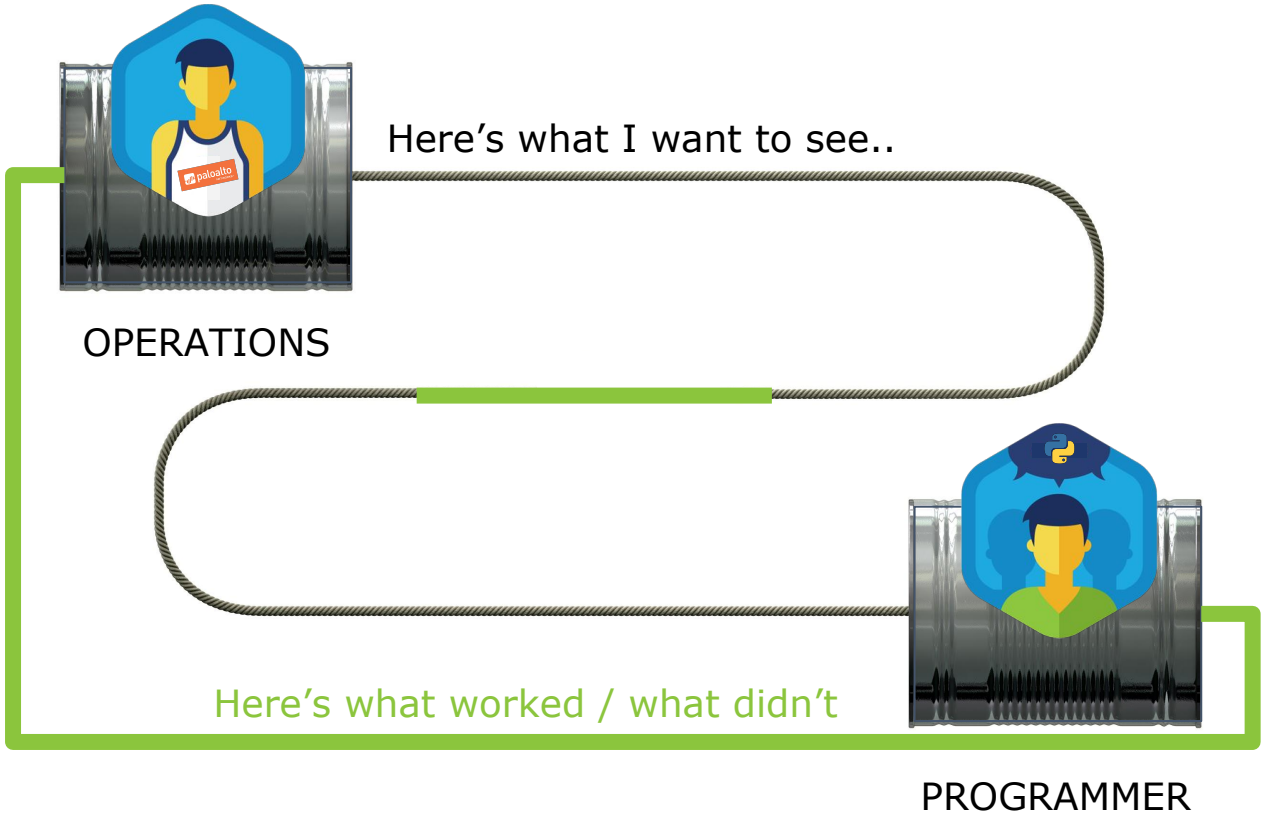
Take the specifications from the users to the software engineers…?



Business analysis with functional use cases:

- CLI command
- Sample output
- "It's very simple"
- Alignment problems
- Type Mismatches
- False positives
- Edge cases
- Data overwrites
- Boundary overruns

Avoid problems. Close the loop.



Create a continuous feedback loop:

- What worked
- What didn't
- How to improve
- Detect and tune false positives

indeni

Quick Note on SMEs & Programmers

Encourage them to interact frequently

It will slow down the initial process

BUT

It will create higher quality code faster

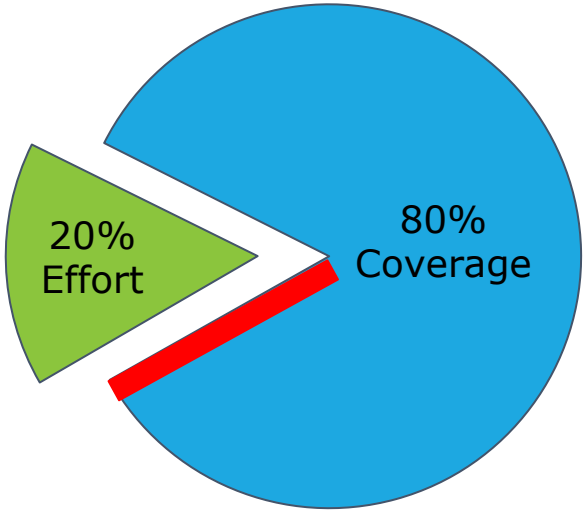
End result: more reliable automation

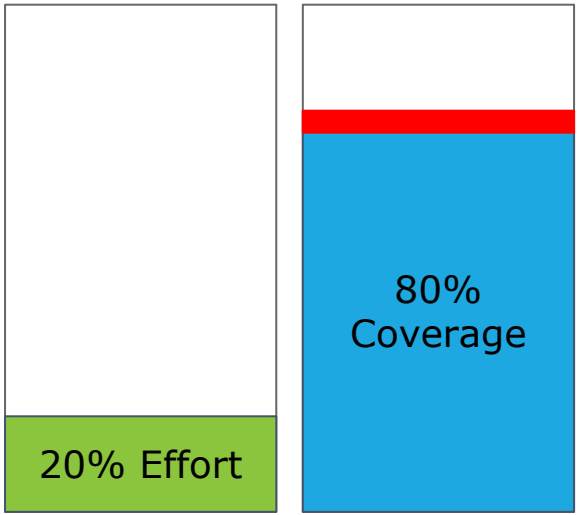
indeni

LESSON #3

Use the 80/20 rule

20% will cover 80% of issues





A small set of scripts can cover the vast majority of issues *

*But there's always that one..

indeni

Quick Note on Early Progress

1. Focus on the “happy path”
   a. Do the easy things first, exceptions are many

2. Bundle development of similar operations
   a. BUT make sure a failure won’t cascade
   b. Can a single bug kill all of your automation?

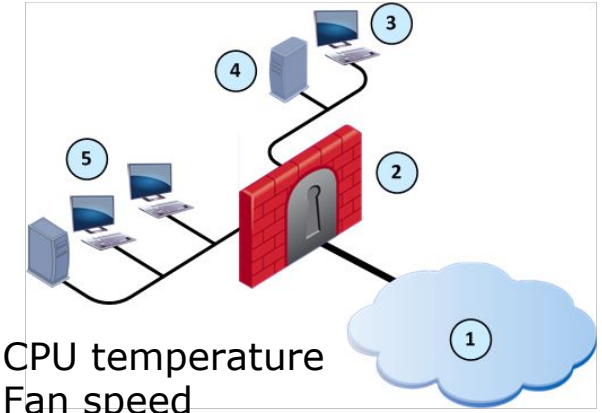
3. ~~Profit~~ Early success to validate concept

LESSON #4

Take all features into consideration

Example: Appliance vs Cloud

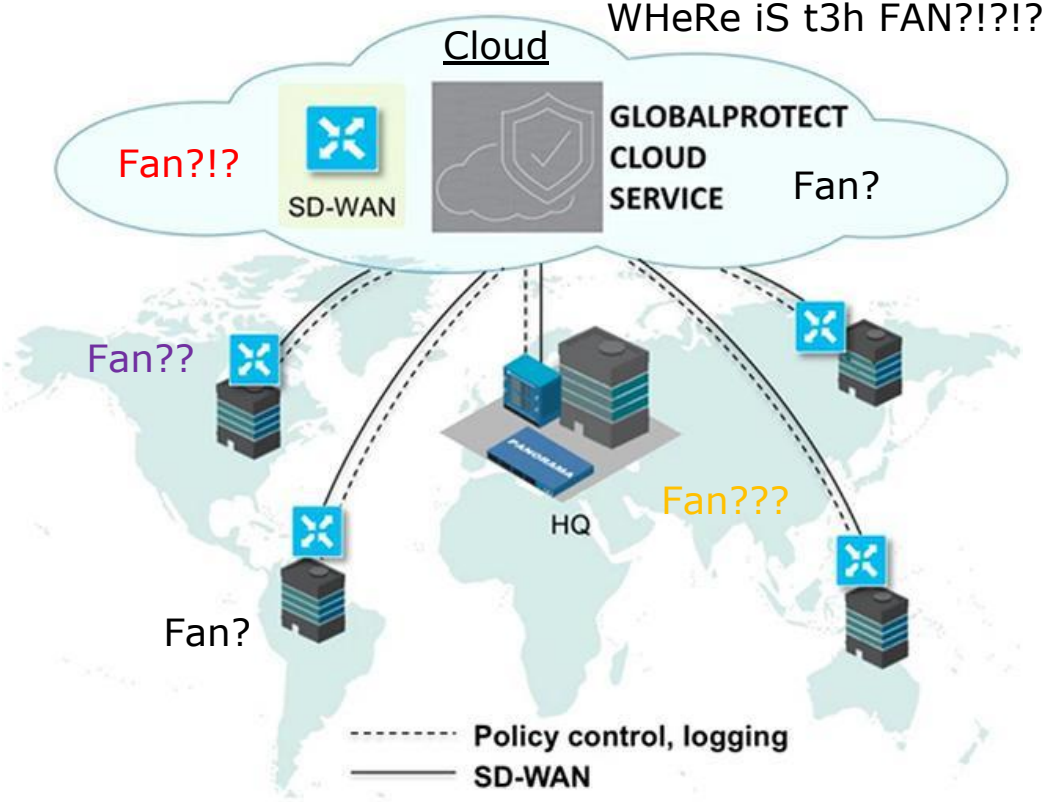
On Premises



- CPU temperature
- Fan speed

WHeRe iS t3h FAN?!?!?

Cloud



Quick Note on Future-Proofing

Think about where you're starting

Think about where you're growing

Make choices that won't **delay** your completion

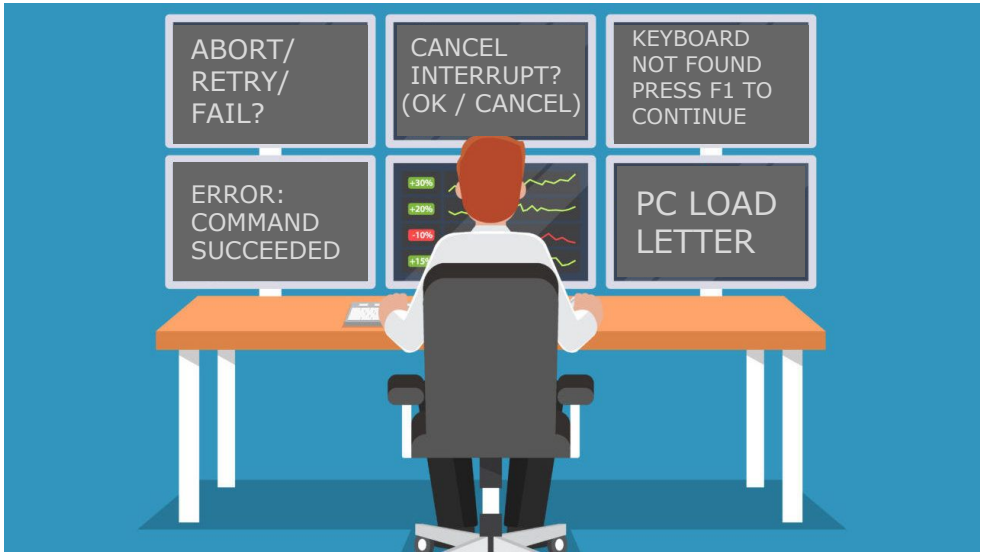
(unless they delay your start)

LESSON #5

Make it actionable

Don’t Let Automation Waste Your Time

What good is an alert if you can’t tell if you need to take action?



Does the output tell you:

- Should I care about this?
- What is the issue?
- **How do I solve?**

indeni

How to Automate Everything

CLI outputs will change

Don’t play telephone. Close the loop

Use the 80/20 rule

Consider all features - cloud and on premises

Make notifications actionable

indeni


Let’s Apply this to PAN-OS

CLI, XML/API, or ReST API?

CLI:
- Pro: Familiar command set for experienced admins
- Con: Must parse command output
- Tools: SSH, Expect, Awk

XML/API:
- Cons: XML, learning curve
- Pros: Machine-readable output, “easy” to map CLI->XML command
- Tools: curl, xpath

ReST API (JSON):
- Cons: Focus on rules/objects, learning curve
- Pros: Machine-readable output, API documentation, “shiny”
- Tools: curl, jq

Best Practices Audit

Tool to analyze NGFW, improve catch rate, reduce attack surface:

Pros

- Up-to-date analysis based on Tech Support (TS) .tgz file
- Clear rating of current security posture

Cons

- Requires manual export & upload of TS file
- Single best "next step" not always clear, your PAN SE can help

Conclusion

- Add BPA (and Expedition) as part of your periodic audit practice
- Great tool for automated analysis, but needs more automation

Expedition, BPA, and Indeni

	Expedition	BPA	Indeni
Form factor	Downloadable VM or installation script to deploy on Ubuntu VM	Web app	Downloadable VM
Intended use	Policy migration, optimization, and suggestions based on traffic logs	Periodic assessment to improve security coverage per NGFW	Operational validation of stability and compliance across all NGFWs
Paradigm	Manual upload to local VM or cloud	Manual upload to cloud	NGFWs connected to on-prem VM
Frequency	Periodic	On demand	Continually
Input	Legacy firewall policy and/or Palo Alto Networks configuration and logs	TS TGZ file, manual mapping of interfaces, zones	Username, password IP for NGFW, connects to XML-API and SSH
Output	Palo Alto Networks NGFW policy (xml/set) and Ansible scripts	Multi-page heatmap, report, and recommended settings per finding	Individual notifications of current issues per NGFW, plus fix for each
Next step	Evaluate policy for suitability in environment	Identify and prioritize, implement, and repeat	Fix issues, prioritized in order of severity rating
Main users	Security engineering / architecture	Security audit	Operations
Main benefits	Accelerated deployment of NGFW from migrated policy, enriched with best practices, iron-skillets, and policy suggestions to reduce attack surface	Assessment of security posture, improvement recommendations, and historical overview to track progress	Real time detection and how-to-fix for issues that could lead to outages, plus best practice enforcement

Global Counters

Lightweight method for debug & diagnostic

- Like ifconfig counters
  - Per-interface counters (drop, xmit, rcv, error, etc.)
  - Global counters are similarly specialized across many functions
- Easy to poll
  - Can be filtered
  - Can query delta since previous poll (e.g. 1/minute -> count/minute)
- Referenced by a variety of KB articles per-subject
  - Valuable for troubleshooting
  - Not technically “documented”, so changes might happen unannounced
- Logging can be enabled for certain counters:
  - https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIIkCAK

Debug

Generate more output at the CLI and/or logs

Pros	Cons	Conclusion
• Gain insight into current behavior • Allows temporary changes with (mostly) light impact	• Shows scary message when enabling • Can alter system behavior in subtle ways	• Use when needed, but only when needed • Slightly risky if used with automation

HA / Sync

- Not everything is sync'd
  - https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/high-availability/reference-ha-synchronization.html
- Example: Default Gateway
  - If secondary has different DG, that i/f might be in a different zone
  - After failover, packet path may not match (sync'd) security policy
  - https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cm1GCAS
- Other examples
  - Management config changes can cause HA sync failures:
    - https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClpuCAC
  - **NTP server**: log timestamp mismatch, bad if forwarded to Demisto etc
  - **SNMP**: leads to different visibility levels on HA peers
  - Licenses, support subscriptions, dynamic content...

Service connection monitoring

- Feature: deep analysis using updated information
  - Apps, anti-virus, threats, Wildfire, Cortex, Prisma, …?!?
- Common problem:
  - Download without applying
- Howto:
  - *show config running* -> search for ‘anti-virus’ and other key terms
- Example Command:
  - *show config running xpath devices/entry/deviceconfig/system/update-schedule/anti-virus/recurring/*/action*
- See also:
  - https://www.reddit.com/r/paloaltonetworks/comments/87pqxs/show_config_running_xpath/

SSL Decrypt

- Feature:
  - MITM SSL to allow payload malware inspection
- Common problem:
  - PAN-OS version doesn't support recent TLS
- Example KB article: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cle3CAC
- Command(s):
  - *show counter global name [...]*
    - proxy_ssl_no_resource
    - proxy_ssl_unsupported
    - proxy_ssl_unsupported_cipher
    - ssl_server_cipher_not_supported
    - ssl_sess_id_resume_drop
  - Each counter indicates a slightly different cause

Resources to Get Started

XML/API Getting Started

- Generating API Key:
  https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-panorama-api/get-started-with-the-pan-os-xml-api/get-your-api-key.html

- Using the CLI to generate XML API commands:
  https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-panorama-api/get-started-with-the-pan-os-xml-api/explore-the-api/use-the-cli-to-find-xml-api-syntax

- Setting RBAC restrictions for service accounts:
  https://indeni.com/docs/user-guide/part-2-getting-started/2-1-adding-user/pan/

Adding hardware monitoring

Once your monitoring is fully established:

CLI Commands to View Hardware Status:

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClW2CAK

Suggestions:

- Management plane CPU
- MAC table (in highly dynamic environments, e.g. public WiFi)

PowerShell wrapper: PowerAlto

Suite of Powershell utilities for Palo Alto XML/API

- Open source tool written by Brian Addicks
- HowTo: https://lockstepgroup.com/blog/scripting-with-palo-alto-networks/
- Docs: https://poweralto.com
- Source: https://github.com/brianaddicks/PowerAlto

Examples:

- Connecting with a PSCredential

```
> Get-PaDevice -DeviceAddress pa.example.com -Credential (Get-Credential)
```

- Connecting with an API key

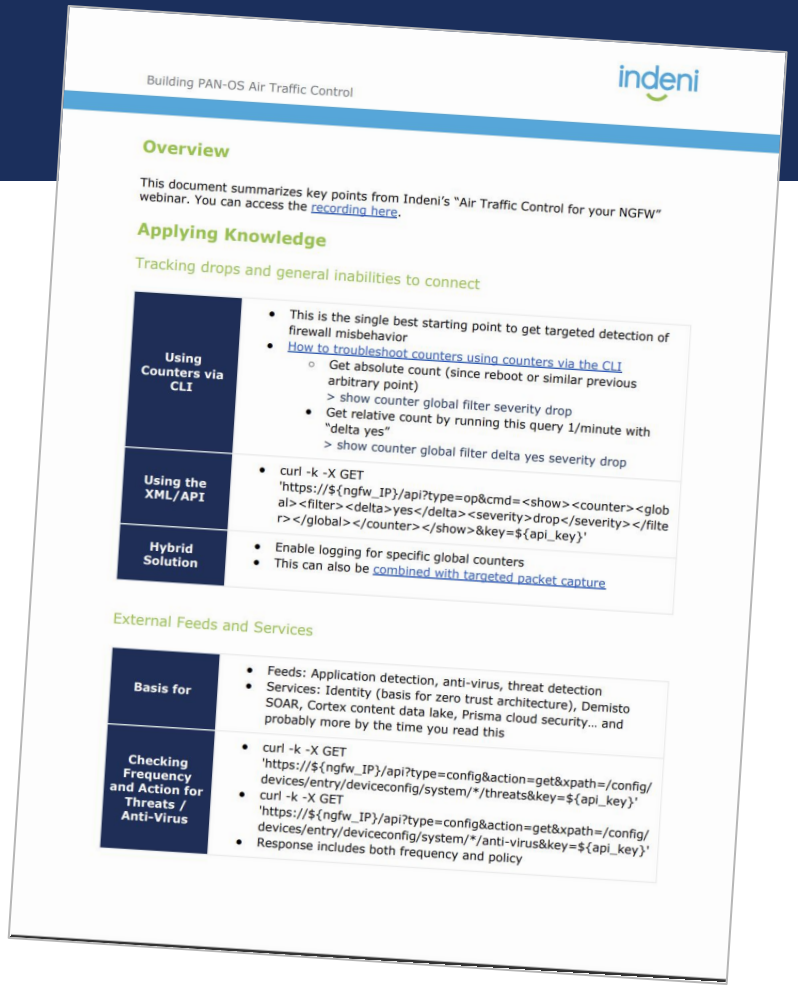
```
> Get-PaDevice -DeviceAddress pa.example.com -ApiKey 'mysupersecretapikey'
```

indeni + fuel
PALO ALTO NETWORKS USER GROUP

Key Resources

For you to leverage:

- **Indeni + Fuel On-Demand Webinar + Whitepaper:**
  "Air Traffic Control for NGFW"
- **Indeni Blog Post:**
  "Network & Security Automation: When the Lego Blocks Don't Fit"
- **Palo Alto Deployment Trends**
- **Indeni Automation Explorer**



Building PAN-OS Air Traffic Control

indeni

Overview

This document summarizes key points from Indeni's "Air Traffic Control for your NGFW" webinar. You can access the recording here.

Applying Knowledge

Tracking drops and general inabilities to connect

Using Counters via CLI	• This is the single best starting point to get targeted detection of firewall misbehavior
	• How to troubleshoot counters using counters via the CLI
	  ○ Get absolute count (since reboot or similar previous arbitrary point)
	  > show counter global filter severity drop
	  ○ Get relative count by running this query 1/minute with "delta yes"
	  > show counter global filter delta yes severity drop

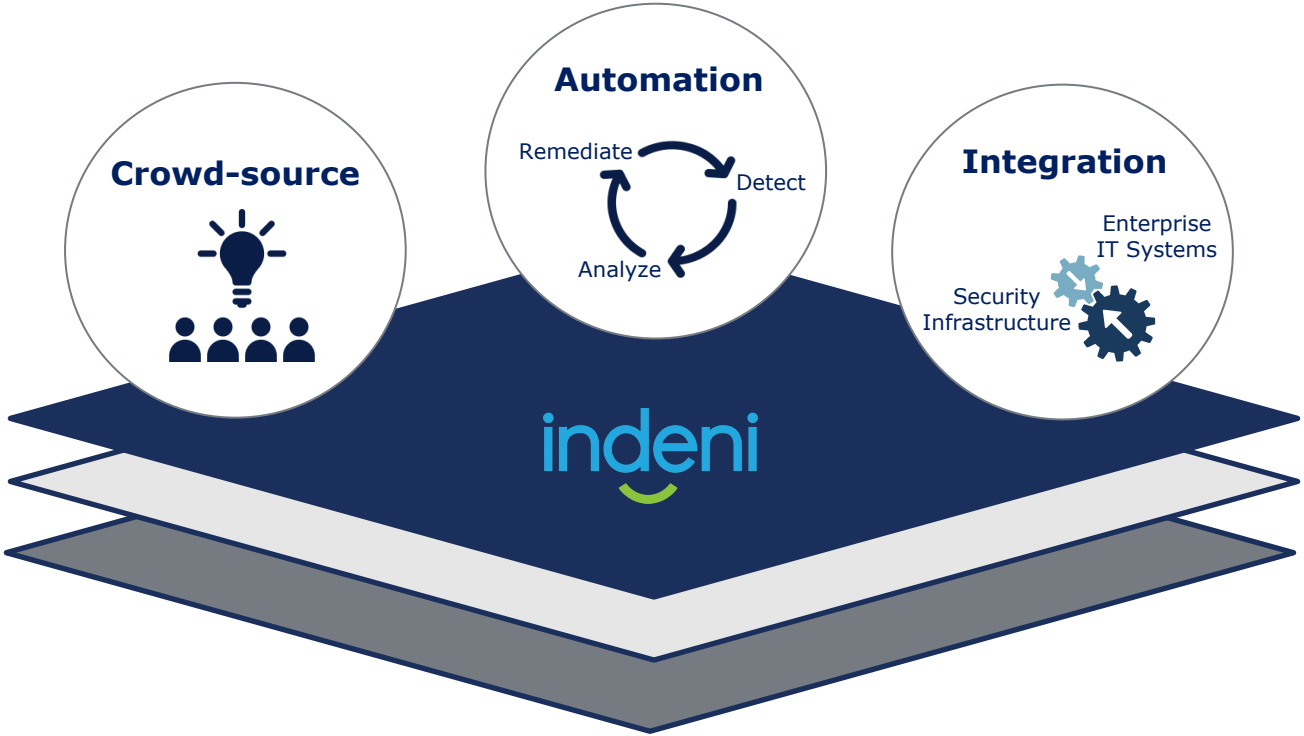
Using the XML/API	• curl -k -X GET 'https://${ngfw_IP}/api?type=op&cmd=<show><counter><global><filter><delta>yes</delta><severity>drop</severity></filter></global></counter></show>&key=${api_key}'
Hybrid Solution	• Enable logging for specific global counters • This can also be combined with targeted packet capture

External Feeds and Services

Basis for	• Feeds: Application detection, anti-virus, threat detection • Services: Identity (basis for zero trust architecture), Demisto SOAR, Cortex content data lake, Prisma cloud security… and probably more by the time you read this
Checking Frequency and Action for Threats / Anti-Virus	• curl -k -X GET 'https://${ngfw_IP}/api?type=config&action=get&xpath=/config/devices/entry/deviceconfig/system/*/threats&key=${api_key}' • curl -k -X GET 'https://${ngfw_IP}/api?type=config&action=get&xpath=/config/devices/entry/deviceconfig/system/*/anti-virus&key=${api_key}' • Response includes both frequency and policy

indeni

Indeni. Security Infrastructure Automation



indeni

Q&A

Jim MacLeod, Technical Product Marketing
jim.m@indeni.com | twitter: @shewfig