Security Orchestration @priceline.com

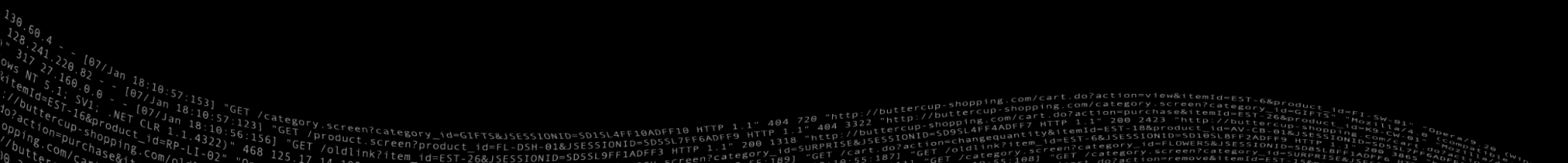
Tony Lin | Sr. Security Engineer

October 2018

- Priceline offers more ways to save and more deals than anyone else in travel. With multiple ways to save on hotel rooms, rental cars, airline tickets, vacation packages and cruises, Priceline is a one-stop-shop for travelers looking for great deals.
  - ~$10B Saved through its suite of travel reservation services.
  - 100M Reservations
  - Up to 60% discounts on published hotel, rental car and flight prices through proprietary Express Deals(R) and Name Your Own Price(R) services.

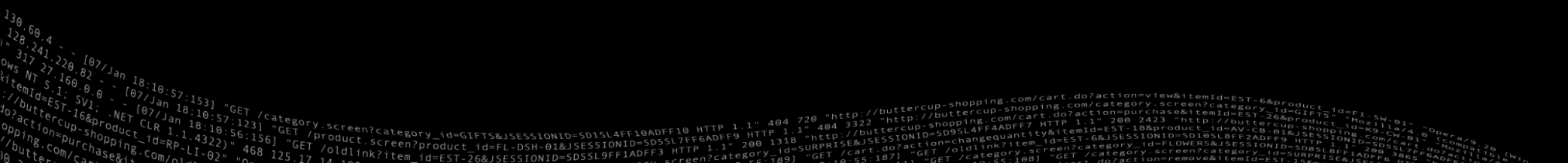
About Me…

- Splunk User for 4 years
  - Design, Deploy, Maintain
  - Core Splunk, Splunk Enterprise Security, Phantom
- Python noob
- 7 Years working in the INFOSEC



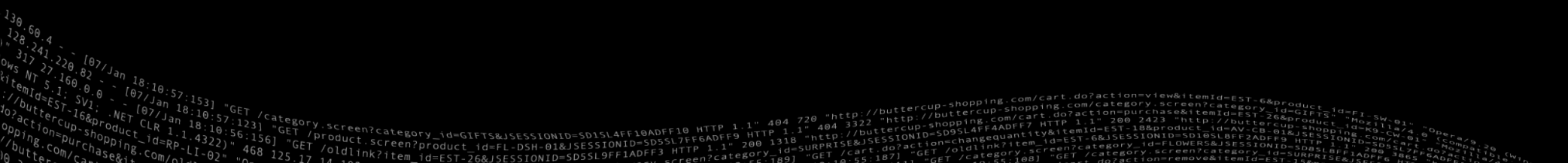
Splunk @ priceline

- ~ 6TB License
- ~12 Trillion events indexed daily
- ~ 20 Physical indexers in different geographic locations
- HTTP Event Collector + Universal Forwarder
- Collecting on-prem and cloud-based events



What's in this Talk

- Challenges for the INFOSEC team @priceline
- Why we selected phantom
- Our process of building security orchestration
- Demo
- Lessons learned
- Future plan



Challenges

Challenge 1

Limited Staff to Cover a Massive Scope

Offense

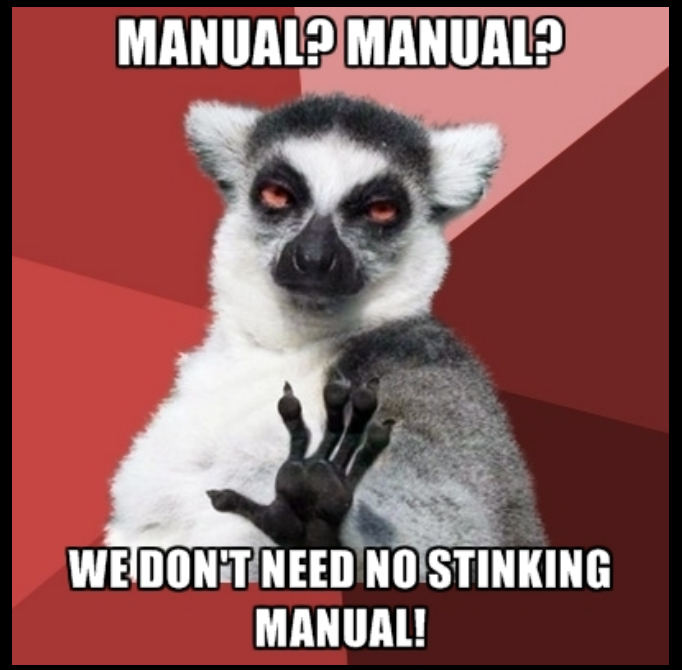
- Application and network security testing, automating when possible
- Employee social engineering and attack simulation
- Red team testing

Defense

- Network and system monitoring
- Incident response
- User Awareness
- DDOS prevention

Compliance

- Lead on PCI, partner requirements & Group program assessment
- Assist on SOX, GDPR readiness
- Strong partnership with Privacy



Challenge 2

Hybrid and Complex Security Technologies and Platforms











Challenge 3

Lack of Data Enrichment and Correlations

- Sanitize and analyze the data
- Link all the resources to a single incident
- Add actions to the response cycle
- Document the process

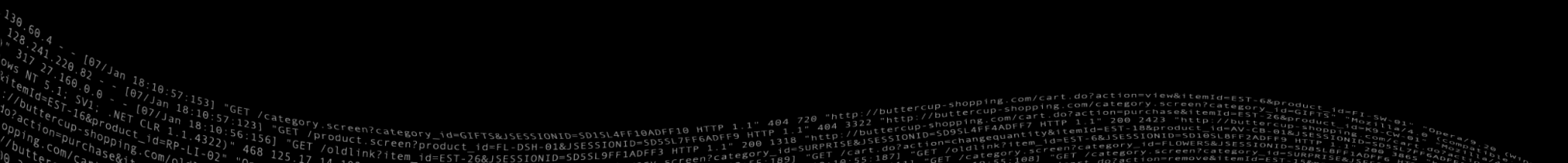
(thanks >)

3 Observations

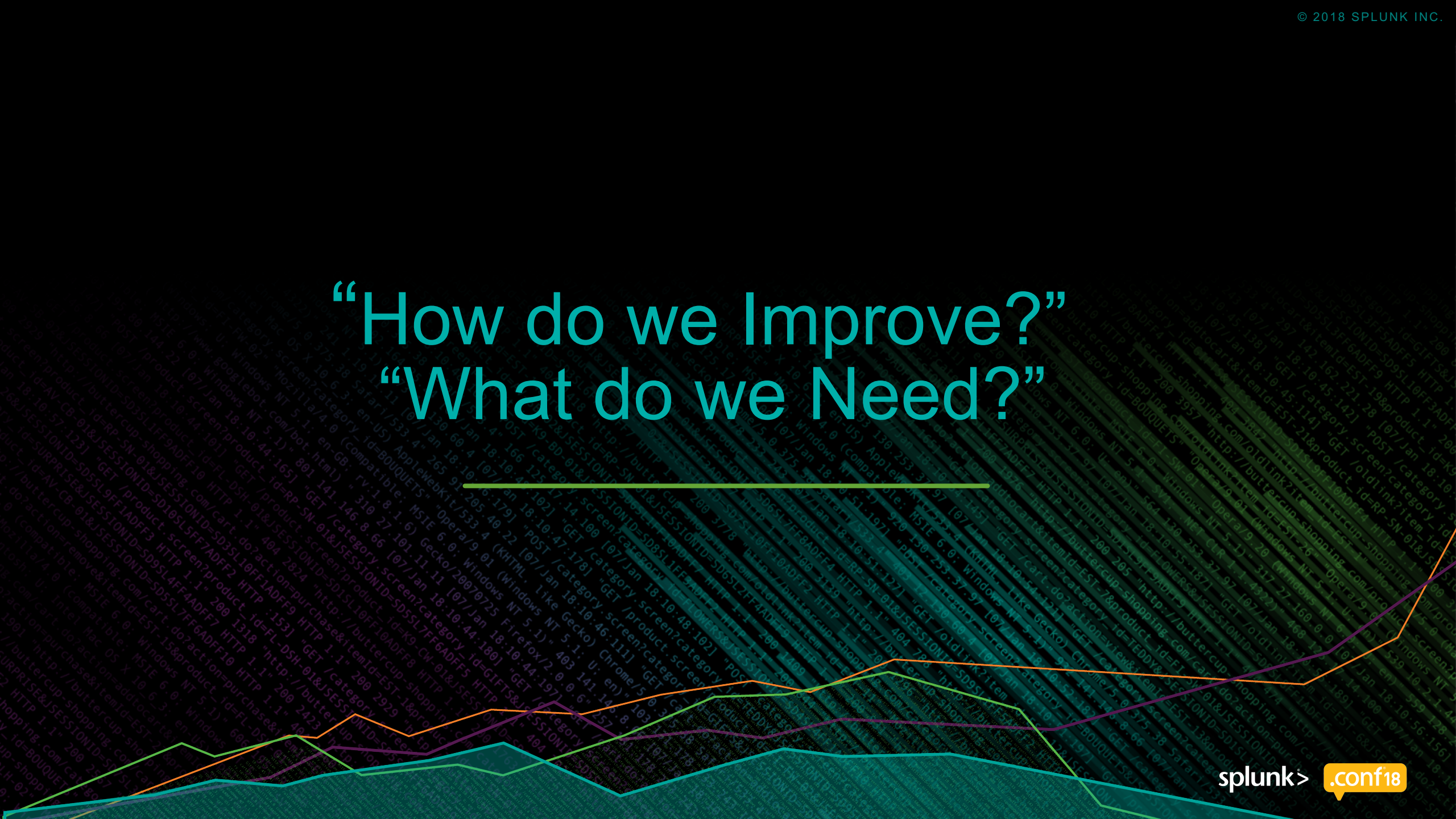
"Security and other Ops team spent most of the time working on tasks that are repetitive in security operations while all has limited staff"

"There's a gap of knowledge between security team and Ops team when executing actions for an incident"

"The results are hard to document into a single place for future references"

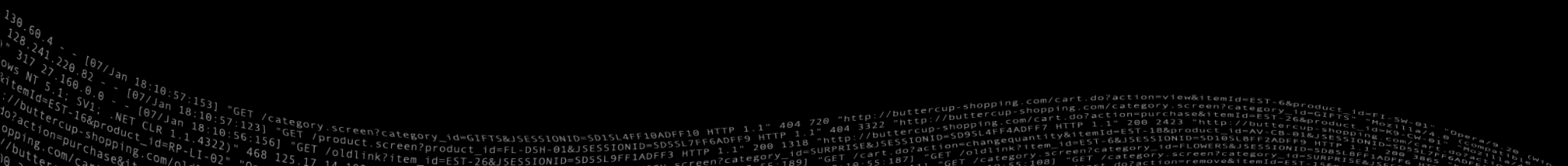


“How do we Improve?”
“What do we Need?”



Our Criteria

- Integrate different technologies into one platform for execution
- Low learning curve across different teams
- Interactive GUI for designing playbooks
- Flexibility to customize API-based apps
- Seamless integration with ticketing system
- Splunk friendly

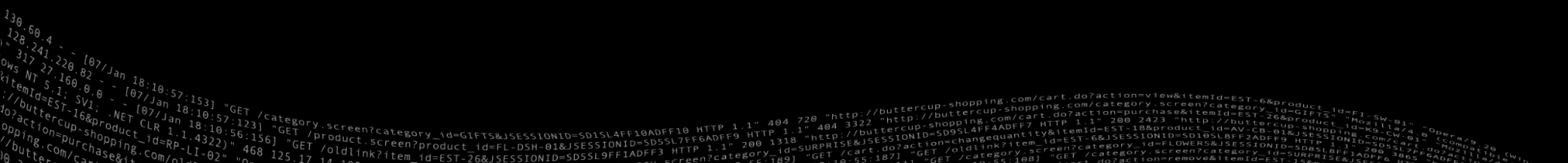


“Free people from doing repetitive and trivial tasks”

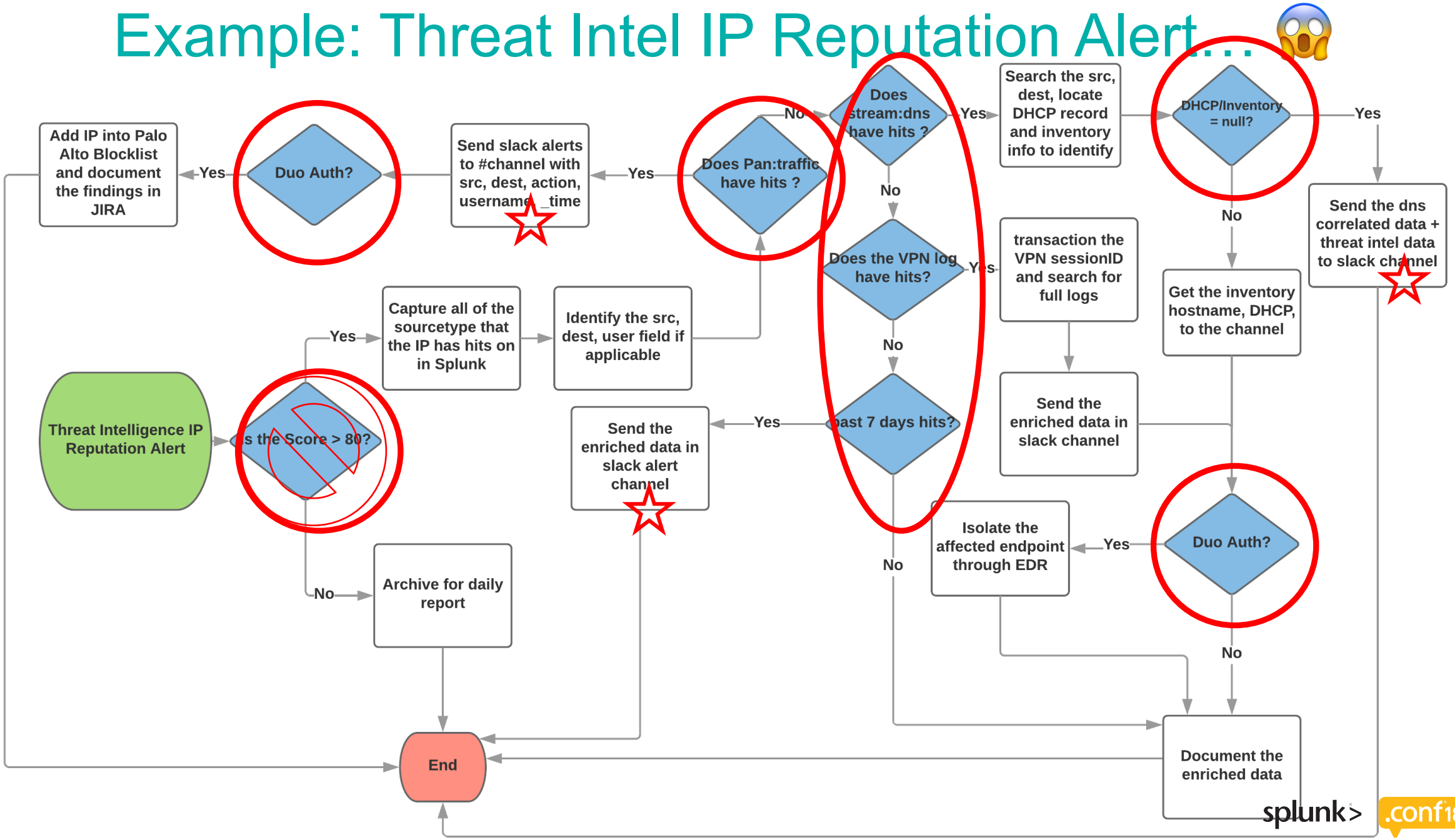
splunk> .conf18

Keep It Simple

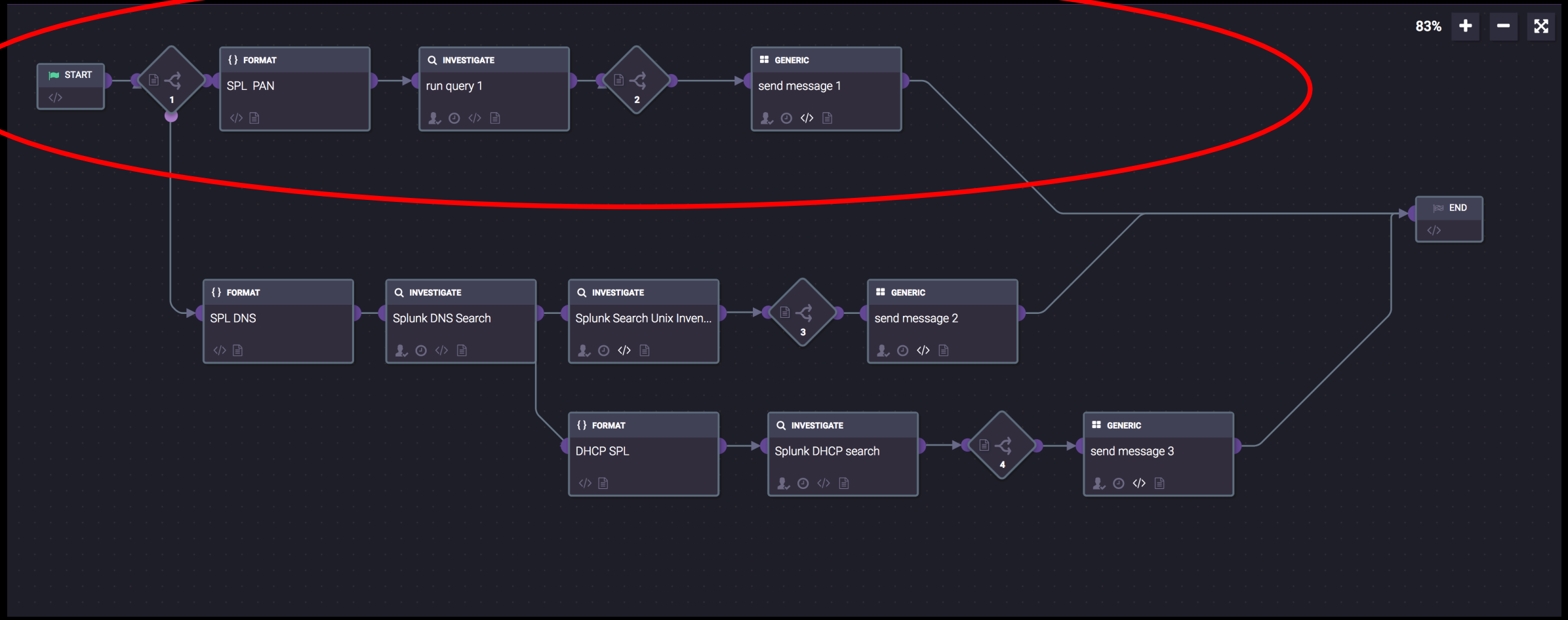
- What are the most time consuming tasks?
- How many of them are level 1/2 jobs?
- Are there more information we could have missed?



Example: Threat Intel IP Reputation Alert…



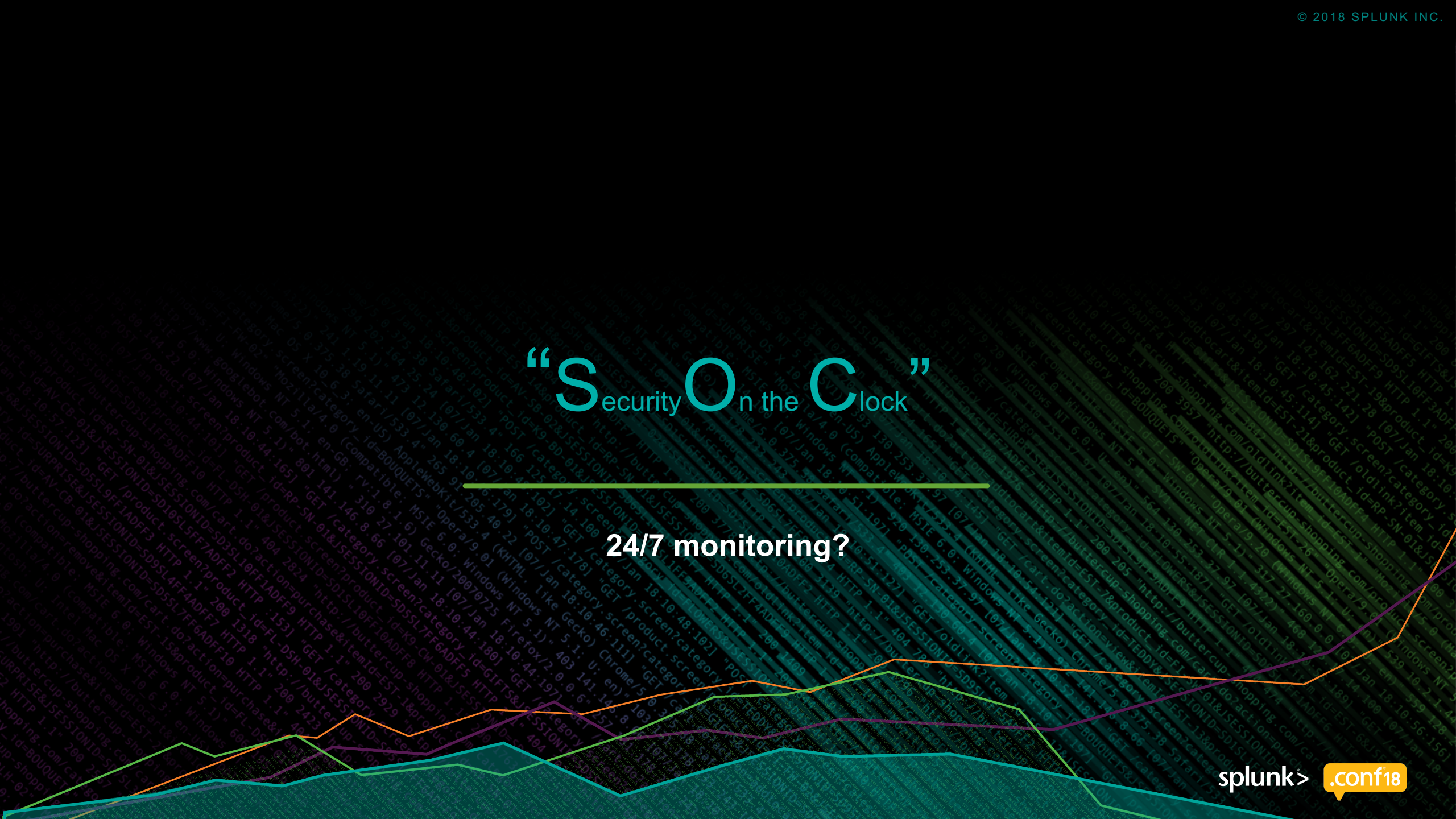
Do it in Phantom…



Use Case: Triage a Risky IP

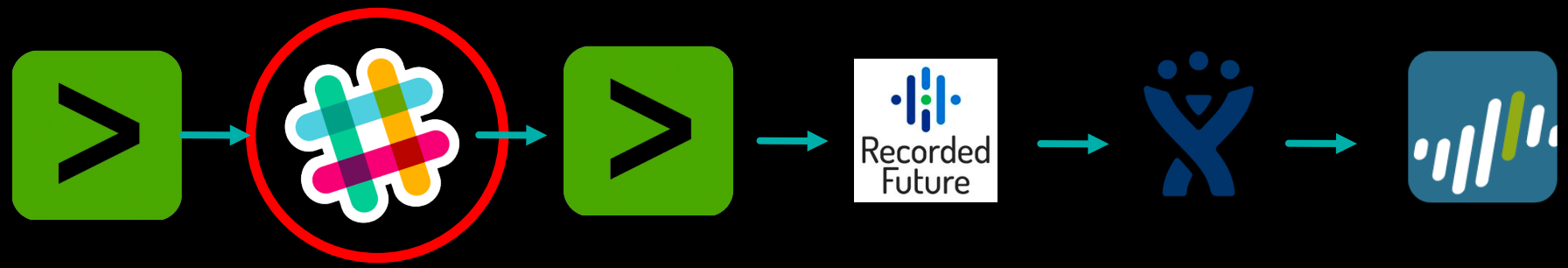
“Security On the Clock”

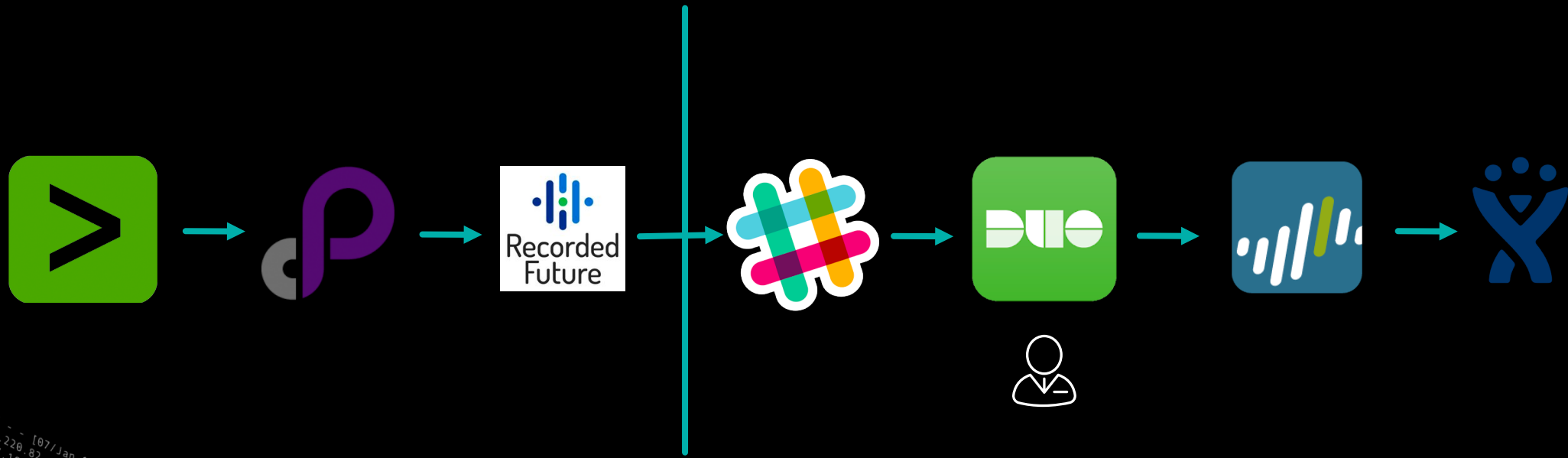
24/7 monitoring?

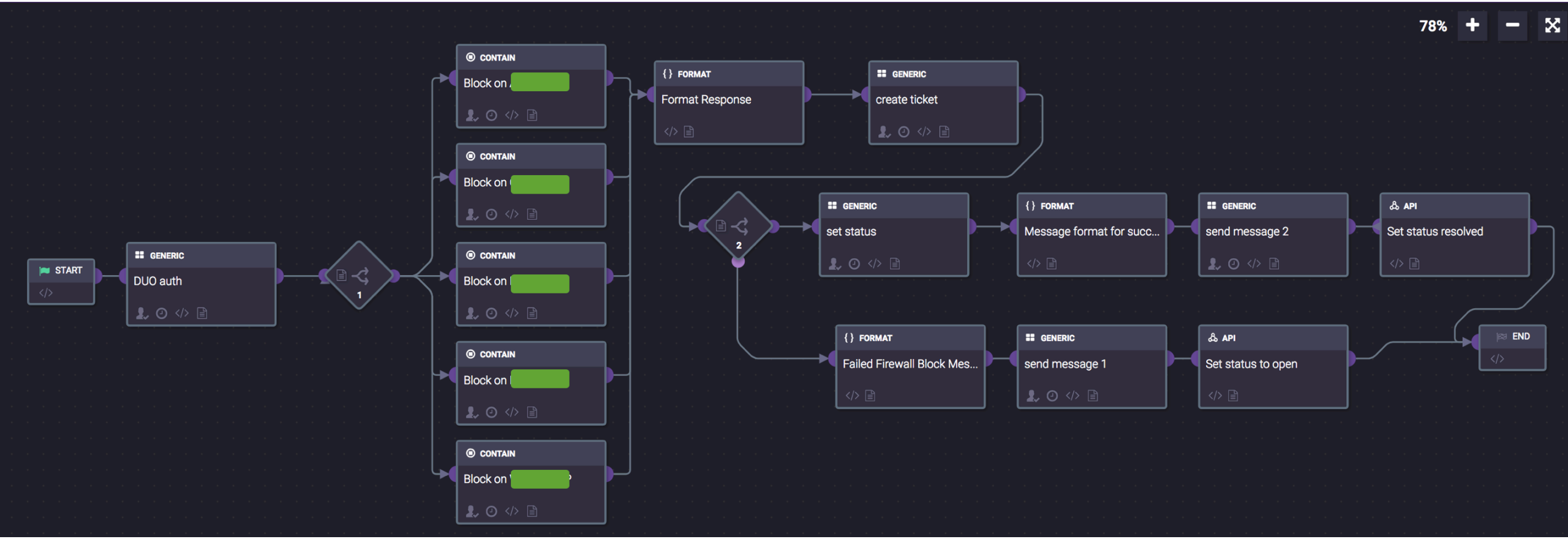


splunk> .conf18

Work Anywhere







DEMO

splunk> .conf18

Window Help

3 KB/s
13 KB/s

infosec-alerts

13 | Add a topic

Today

Show results in Splunk

Splunk Alert Today at 11:20 AM

Tony Lin 11:21 AM

@phantomautobot run_playbook --repo local "Block IP" 4921

phantomautobot APP 11:21 AM

Container URL: https://ash1-phantom-401.corp.priceline.com/mission/4921

```
Playbook: local/Block IP
Playbook run ID: 1565
Playbook queueing result: Playbook run successfully queued
```

Please check https://priceline.atlassian.net/browse/INFOSEC-40438 , some of the firewalls rules are not executed successfully.

```
Playbook: 273
Playbook run ID: 1565
Playbook run result: success
```

Jira Cloud APP 11:21 AM

INFOSEC-40438: Phantom Triggered IP Block Action

`Priority 3 (Medium)` priority `Request` in `Open` assigned to **Unassigned**

phantomautobot APP 11:37 AM

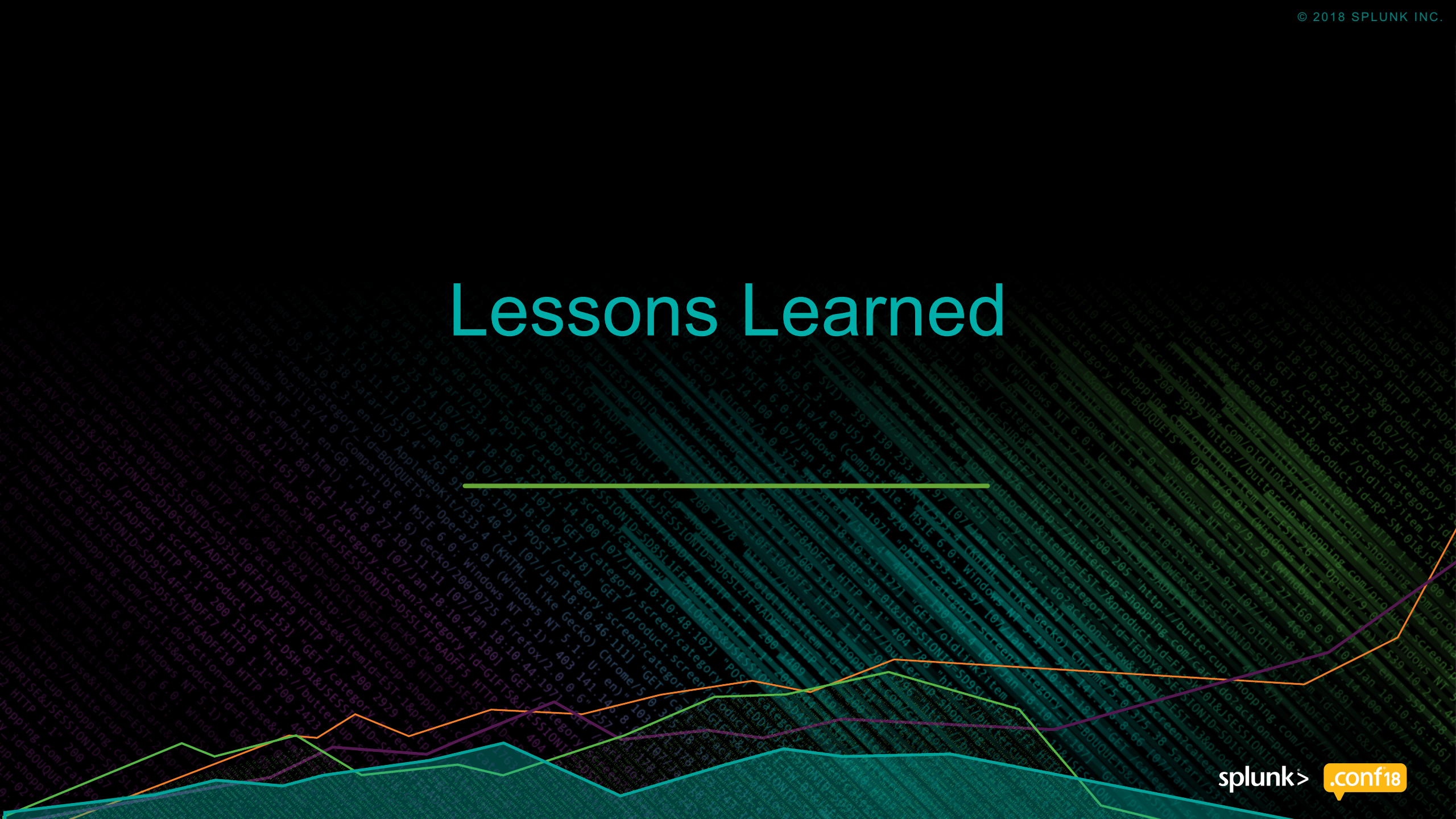
🔎 **Recorded Future High Risk IP Alert**

https://app.recordedfuture.com/live/sc/entity/ip:162.88.96.194

risk score: `75`
log source: `palo:traffic`
src_ip: `10.23.42.27`
src_zone: `LAN`
dest_ip: `162.88.96.194`
dest_zone: `INTERNET`
dest_port: `80`
event_count: `1`
firewall action : `allowed`
container_id: `5045`

Message infosec-alerts

Lessons Learned



- Be Careful about Calling 3rd-party API!
- Use Splunk as a Central Point for Event Search/Enrichment
- Dedup/Stats/Fields/Where + CEF fields Mapping + Labels
- Have Multiple Simple Playbooks >> Glue All Scenarios into 1 Playbook
- Enrichment v. Action, Pick Your Battle
- Use Customize Code on Action Block. Not on the Whole Playbook!
- Rename the Action Block
- Always Run in Mission Control First to Get the JSON
- Play with Containers
- Community Playbooks
- Ask @phantom/my.phantom.us

Future Plans

MITRE Enterprise ATT&CK™ Framework

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
Image File Execution Options Injection			Forced Authentication	Network Share Discovery	AppleScript		Man in the Browser	Exfiltration Over Physical Medium	Multi-hop Proxy
Plist Modification			Hooking	System Time Discovery	Third-party Software		Browser Extensions		Domain Fronting
Valid Accounts			Password Filter DLL	Peripheral Device Discovery	Windows Remote Management		Video Capture	Exfiltration Over Command and Control Channel	Data Encoding
DLL Search Order Hijacking			LLMNR/NBT-NS Poisoning	Account Discovery	SSH Hijacking	LSASS Driver	Audio Capture		Remote File Copy
AppCert DLLs		Process Doppelgänging	Securityd Memory	File and Directory Discovery	Distributed Component Object Model	Dynamic Data Exchange	Automated Collection	Scheduled Transfer	Multi-Stage Channels
Hooking		Mshta	Private Keys	System Information Discovery		Mshta	Clipboard Data	Data Encrypted	Web Service
Startup Items		Hidden Files and Directories	Keychain		Pass the Ticket	Local Job Scheduling	Email Collection	Automated Exfiltration	Standard Non-Application Layer Protocol
Launch Daemon		Launchctl	Input Prompt	Security Software Discovery	Replication Through Removable Media	Trap	Screen Capture	Exfiltration Over Other Network Medium	
Dylib Hijacking		Space after Filename	Bash History			Source	Data Staged		Communication Through Removable Media
Application Shimming		LC_MAIN Hijacking	Two-Factor Authentication Interception	System Network Connections Discovery	Windows Admin Shares	Launchctl	Input Capture	Exfiltration Over Alternative Protocol	
AppInit DLLs		HISTCONTROL			Remote Desktop Protocol	Space after Filename	Data from Network Shared Drive		Multilayer Encryption
Web Shell		Hidden Users	Account Manipulation	System Owner/User Discovery	Pass the Hash	Execution through Module Load		Data Transfer Size Limits	Standard Application Layer Protocol
Service Registry Permissions Weakness		Clear Command History	Replication Through Removable Media		Exploitation of Vulnerability		Data from Local System	Data Compressed	
Scheduled Task		Gatekeeper Bypass		System Network Configuration Discovery	Shared Webroot	Regsvcs/Regasm	Data from Removable Media		Commonly Used Port
New Service		Hidden Window	Input Capture		Logon Scripts	InstallUtil			Standard Cryptographic Protocol
File System Permissions Weakness		Deobfuscate/Decode Files or Information	Network Sniffing	Application Window Discovery	Remote Services	Regsvr32			
Path Interception			Credential Dumping		Application Deployment Software	Execution through API			Custom Cryptographic Protocol
Accessibility Features		Trusted Developer Utilities	Brute Force	Network Service Scanning		PowerShell			Data Obfuscation
Port Monitors		Regsvcs/Regasm	Credentials in Files	Query Registry	Remote File Copy	Rundll32			Custom Command and Control Protocol
Screensaver	Exploitation of Vulnerability			Remote System Discovery	Taint Shared Content	Scripting			
LSASS Driver	Extra Window Memory Injection			Permission Groups Discovery		Graphical User Interface			Connection Proxy
Browser Extensions	Access Token Manipulation			Process Discovery		Command-Line Interface			Uncommonly Used Port
Local Job Scheduling	Bypass User Account Control			System Service Discovery		Scheduled Task			Multiband Communication
Re-opened Applications	Process Injection					Windows Management Instrumentation			Fallback Channels
Rc.common	SID-History Injection	Component Object Model Hijacking				Trusted Developer Utilities			
Login Item	Sudo	InstallUtil				Service Execution			
LC_LOAD_DYLIB Addition	Setuid and Setgid	Regsvr32							
Launch Agent		Code Signing							
Hidden Files and Directories		Modify Registry							
.bash_profile and .bashrc		Component Firmware							
Trap		Redundant Access							
Launchctl		File Deletion							
Office Application Startup		Timestomp							
Create Account		NTFS Extended Attributes							
External Remote Services		Process Hollowing							
Authentication Package		Disabling Security Tools							
Netsh Helper DLL		Rundll32							
Component Object Model Hijacking		DLL Side-Loading							
Redundant Access		Indicator Removal on Host							
Security Support Provider		Indicator Removal from Tools							
Windows Management Instrumentation Event Subscription		Indicator Blocking							
		Software Packing							
Registry Run Keys / Start Folder		Masquerading							
Change Default File Association		Obfuscated Files or Information							
		Binary Padding							
Component Firmware		Install Root Certificate							
Bootkit		Network Share Connection Removal							
Hypervisor		Rootkit							
Logon Scripts		Scripting							
Modify Existing Service									

attack.mitre.org

Thank You

Don't forget to rate this session in the .conf18 mobile app

tony.lin@priceline.com