

Automation in modern Incident Detection & Response (IDR) process

Nazar Tymoshyk (UnderDefense)

Agenda

1. About me
2. WHAT is Automation and Orchestration and Incident Response
3. WHY we talk about this?
 - a. The problems of Modern Security Operations
 - i. People
 - ii. Speed
 - iii. False Positives and Use case addiction
 - b. The problems of Modern IR process
 - c. Money/ROI
4. Humans vs Machines
5. HOW
 - a. Automation
 - b. Playbooks
 - c. Threat Intelligence
 - d. Orchestration
 - e. Tools
6. ROI
7. Q&A



Key Takeaways

1. What to Measure in modern SOC
2. How Automation vs Orchestration works
3. How to improve Response efficiency
4. How to win more time to live

Personal Information

Name: Nazar Tymoshyk

Title: CEO of UnderDefense

In Security: from 2008

Father of 1 daughter, 1 company,
1 community

Email: nt@underdefense.com

Founder of OWASP Lviv

Building best Defensive cybersec company in Ukraine.

Talant - to find best talents and develop them

Addiction - Efficiency and Successful Ukraine





Everyone
wanted to be a
Pentest Ninja



TODAY

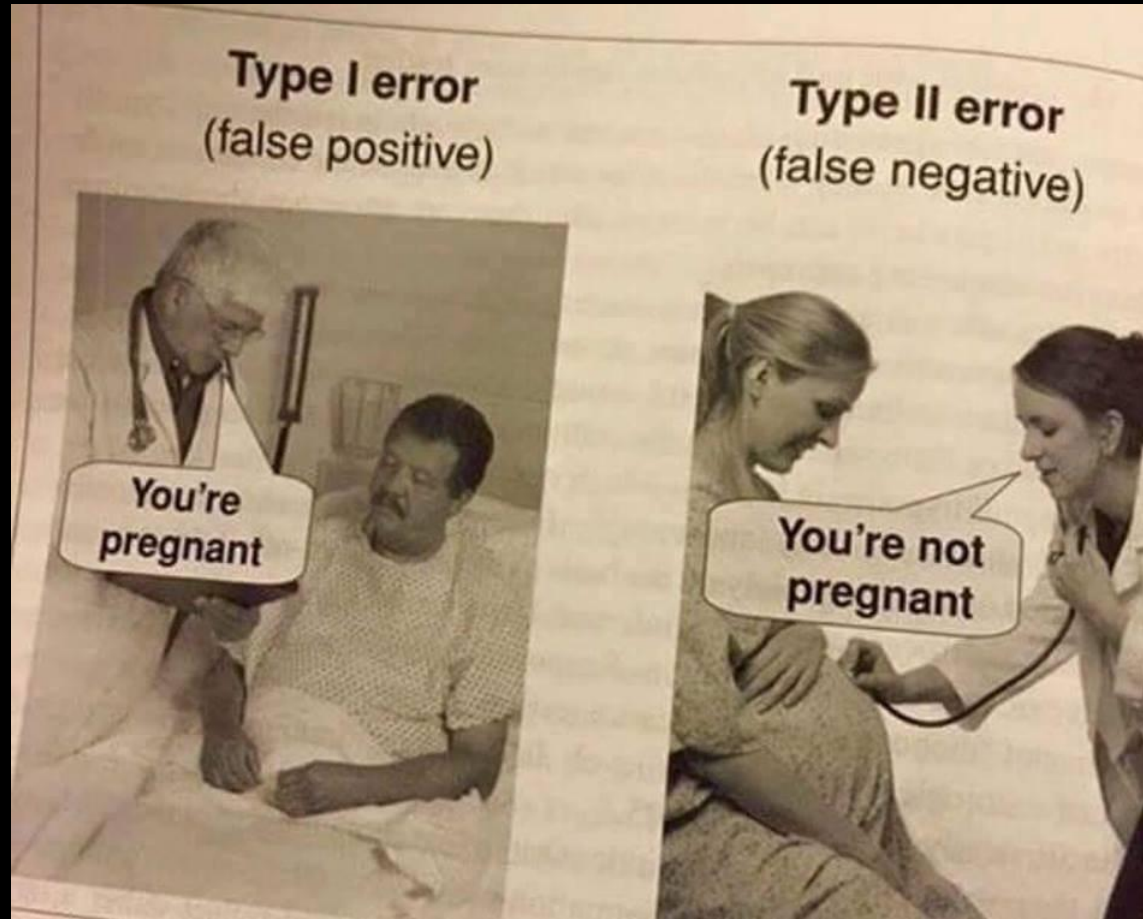
Many wants to
become a
Hunters and
build their
own SOC/SIEM

WHY we talk about THIS?

All SOC clients ask us: “Give me all data - I want to see **ALL data.**”

CREATE MORE USE CASES”

Use case addiction



More SOC alerts - is it good or bad?



SOC vs NOC

SOC CHALLENGES



80%

Not enough
time



79%

Not enough
people



71%

Responding to a
large number of
incidents



69%

Too many
false
positives



46%

Too many
alerts

\$\$\$

42%

Cost and
skills to
operate



53.2%

Rarely update
playbooks



41.8%

Don't measure
IR metrics

TYPICAL CHALLENGES

1. Hybrid and Complex Security Technologies and Platforms
2. Limited Staff to Cover a Massive Scope
3. COMPLIANCE + OFFENSE + DEFENSE

What should we do with alerts we failed to process because of flood?



Orchestration

How different technologies (both security-specific and non-security-specific) are integrated to work together

Automation

How to make machines do task-oriented "human work".

Utilizing Security Product APIs to connect and run repetitive tasks faster and avoid human mistakes.

Incident management & collaboration

End-to-end management of an
Incidents / Cases by people

MISSION CONTROL

collaboration





I'm alone.

Problems with People

- Can get Sick
- Tired/Bored
- Sometimes Lazy
- Need Motivation
- Not experienced
- Not systematic
- Have a lot of Needs
- Expensive
- SOMETIMES NOT WANT TO BE EFFICIENT



Machines

- ★ Fast
- ★ Analytically consistent
- ★ Not instinctive
- ★ Minimal bias
- ★ Require time for learning



Humans

- ★ Visual and instinctive
- ★ Quickly learn on new data acquiring new experience
- ★ Not efficient
- ★ A lot of biases
- ★ Slow
- ★ But Flexible
- ★ SMART
- ★ CREATIVE

SPEED



RcMeLo

Robotics & Mechatronics

TIME & COMMUNICATION

=

IMPACT & \$\$\$\$

If you play a chess with enemy - you
need to take decisions faster as they
are already in

Speed can reduce Cost = more
availability for **IMPROVEMENTS**

If you do your decisions faster =>
Theoretically you can go home faster

and even meet friends, drink more bear, pass OSCP, OSCE, prepare a
speech for **DefCon 0322 Lviv**

“Free people from doing repetitive
and trivial tasks”



WHERE TO START?

Measure

Time to Detect

Time to Investigate

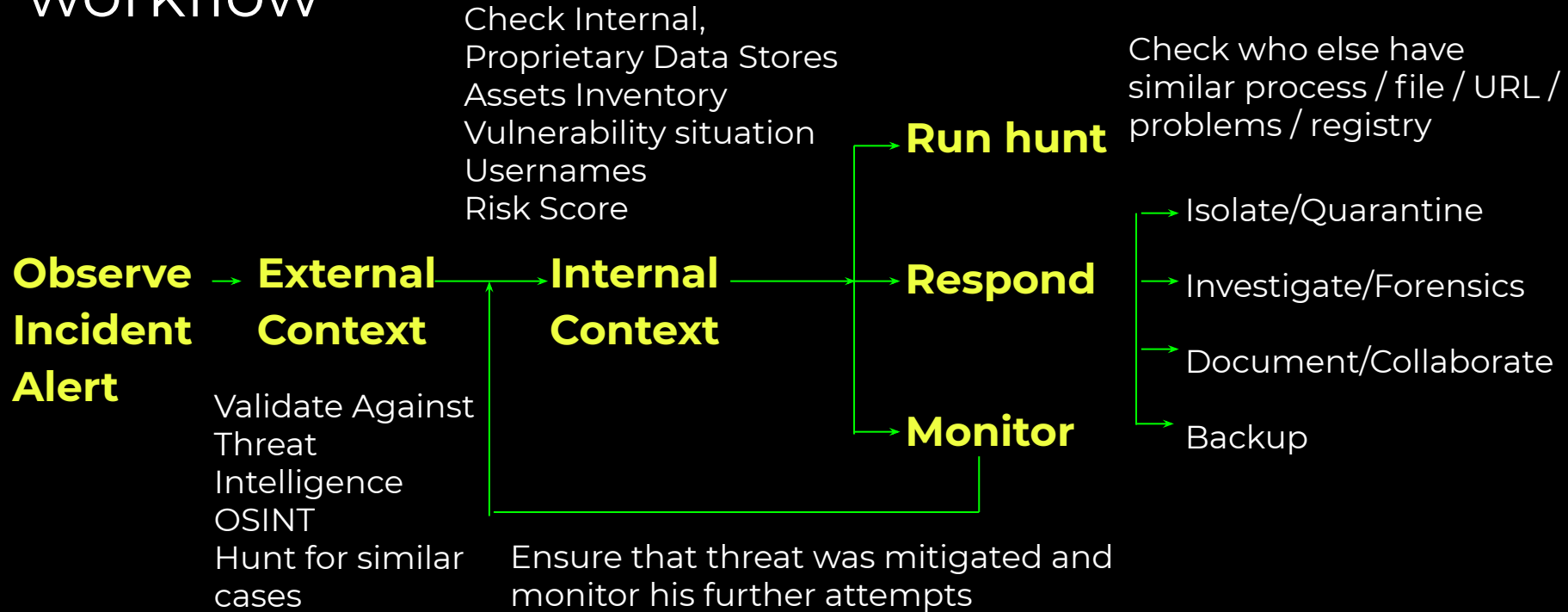
Time to Contain

Time to Respond

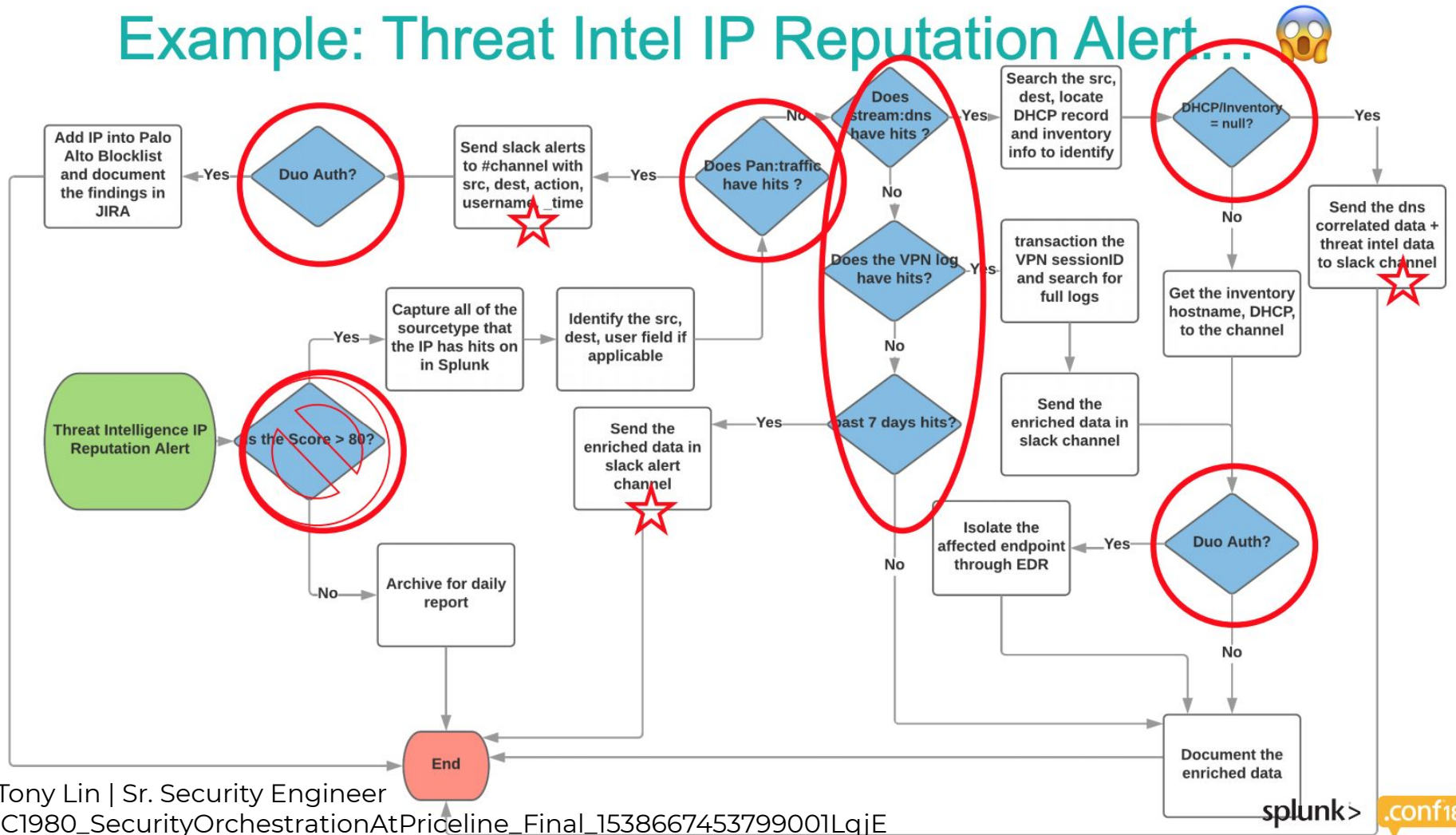
Time to Recover

Time to compile Lessons Learned and back it to the process

Incident Detection and Response (IDR) workflow



Example: Threat Intel IP Reputation Alert... 🤖





Splunk Alerts Bot May 3, 7:48 PM •

Possible XSS Attack

Query: ?msg=<script>alert(\"test\")</script>

Source: 192.168.109.111

Destination: 192.168.109.104

Site: 192.168.109.104



Reply



Splunk Alerts Bot May 3, 7:48 PM •

Possible XSS Attack

Query: ?msg=<script>alert(\"test\")</script>

Source: 192.168.109.111

Destination: 192.168.109.104

Site: 192.168.109.104

Follow



Reply



Splunk Alerts Bot May 3, 7:48 PM •

Possible XSS Attack

Query: ?msg=<script>alert(\"test\")</script>

Source: 192.168.109.111

Destination: 192.168.109.104



Jump to bottom

Automate Security Operations Workflow

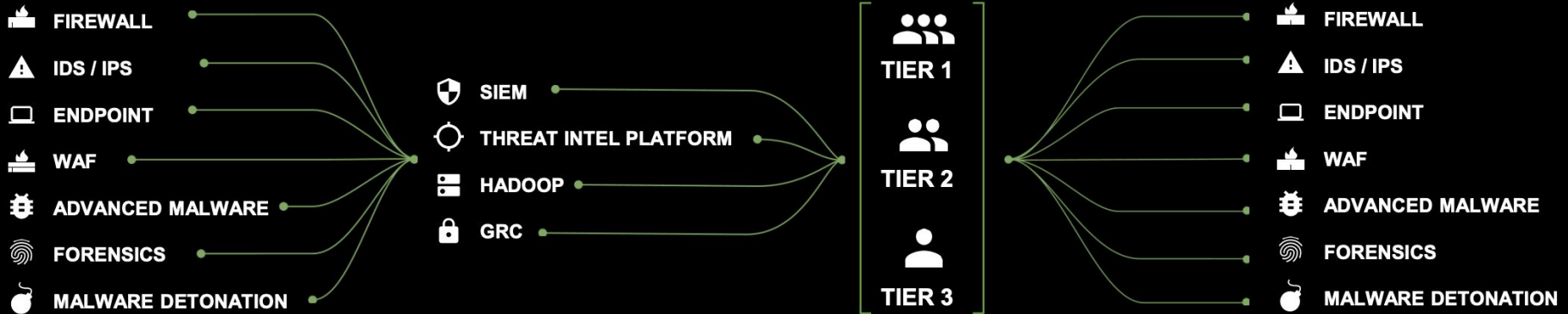
Collect data

Build Analytics

Take Decision

Act

(Orient / Sense-making)



AUTOMATED
(SOC)

MANUAL (IT/NOC)
(currently)

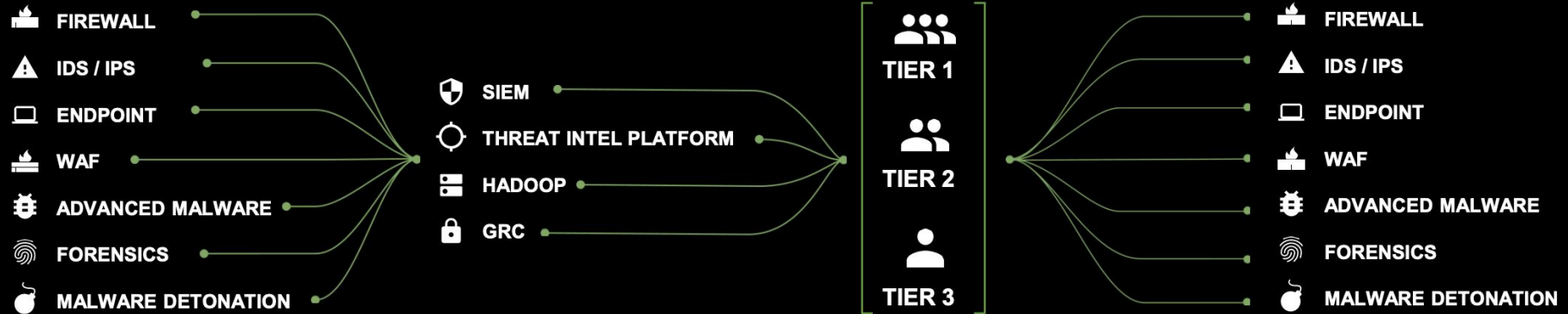
Automate Security Operations Workflow

Collect data

Analytics

Decision Making

Acting



AUTOMATED

**Automate, Enrich, add
context and reaction!**

SOC Analyst Daily Workflow Inputs and



	INGESTION OR ALERTING	EXTERNAL VALIDATION	INTERNAL HUNTING	MONITORING	RUN JOBS	NOTIFICATIONS
	Threat Intel SIEM events Phone calls	VirusTotal OpenDNS iSight	Logs Endpoint search	Firewall Rules IDS Signatures Endpoint Alerts Proxy Blocks	Malware Analysis Forensics	Ticketing Reports
Actions	Poll Push	Look Up	Hunt	Set Block/Quarantine	Analyze Get...	Send Receive
Artifacts	Events	Context	Artifacts	Artifacts	Artifacts	Measure

Tools

What tools we recommend?




DEMISTO
A PALO ALTO NETWORKS® COMPANY



Orchestration capabilities

Apps




amazon
web services™

AWS Publisher: Jarid Richardson and Joseph Sirak Version: 1.0.1 [Documentation](#)

Implements investigation and containment by integrating with the AWS API

► 10 supported actions




amazon
web services™

AWS Publisher: Booz Allen Hamilton Version: 1.0.0 [Documentation](#)

A Phantom integration that facilitates interaction with the AWS API.

▼ 18 supported actions

- **test connectivity** - Validate the asset configuration for connectivity using supplied configuration
- **blacklist ip** - Blacklist IP by adding a rule to every subnet NACL accessible by credentials
- **whitelist ip** - Whitelist IP by removing any block rules from NACLs
- **disable acct** - Disables an AWS IAM user account
- **enable acct** - Enables an AWS IAM user account
- **remove access** - Removes EC2 Access for a given IAM user
- **enable access** - Enable EC2 Access for a given IAM user
- **remove sg access** - Removes Security Group Access for a given IAM user
- **enable sg access** - Enable Security Group Access for a given IAM user
- **remove sg ingress** - Removes ingress rule from security group
- **lookup instance** - Return AWS EC2 instance information using IP address or Instance Id
- **create instance** - Creates an AWS instance from an image id
- **start instance** - Start EC2 instance
- **stop instance** - Stop EC2 instance
- **snapshot instance** - Snapshot AWS instance that has the given IP address
- **quarantine instance** - Quarantines AWS instance that has the given IP address
- **asg detach instance** - Detaches an instance from an auto-scaling group
- **invoke lambda** - Invoke an AWS Lambda function




amazon

AWS Athena Publisher: Phantom Version: 1.0.6 [Documentation](#)

This app supports investigative actions on AWS Athena

Orchestrations/Integrations




Cisco ASA Publisher: Phantom Version: 1.2.17 [Documentation](#)

This app supports containment actions like 'block ip' in addition to investigative actions like 'get config' and 'get version' on a Cisco ASA device.

▼ 7 supported actions


- **terminate session** - Terminates all VPN sessions of a user
- **list sessions** - List the current VPN sessions
- **unblock ip** - Unblock an IP
- **block ip** - Block an IP
- **get version** - Gets the software version information of the device.
- **get config** - Gets the current running config of the device.
- **test connectivity** - Validate the asset configuration for connectivity. This action runs a few commands on the device to check the connection and credentials.



Cisco Catalyst Publisher: Phantom Version: 1.2.13 [Documentation](#)

This app supports containment actions like 'set system vlan' in addition to investigative actions like 'get config' and 'get version' on a Cisco Catalyst switch.


▶ 4 supported actions



Cisco ESA Publisher: Phantom Version: 1.0.9 [Documentation](#)

This app supports **investigation** on the Cisco Email Security Appliance (ESA) device.

▶ 2 supported actions

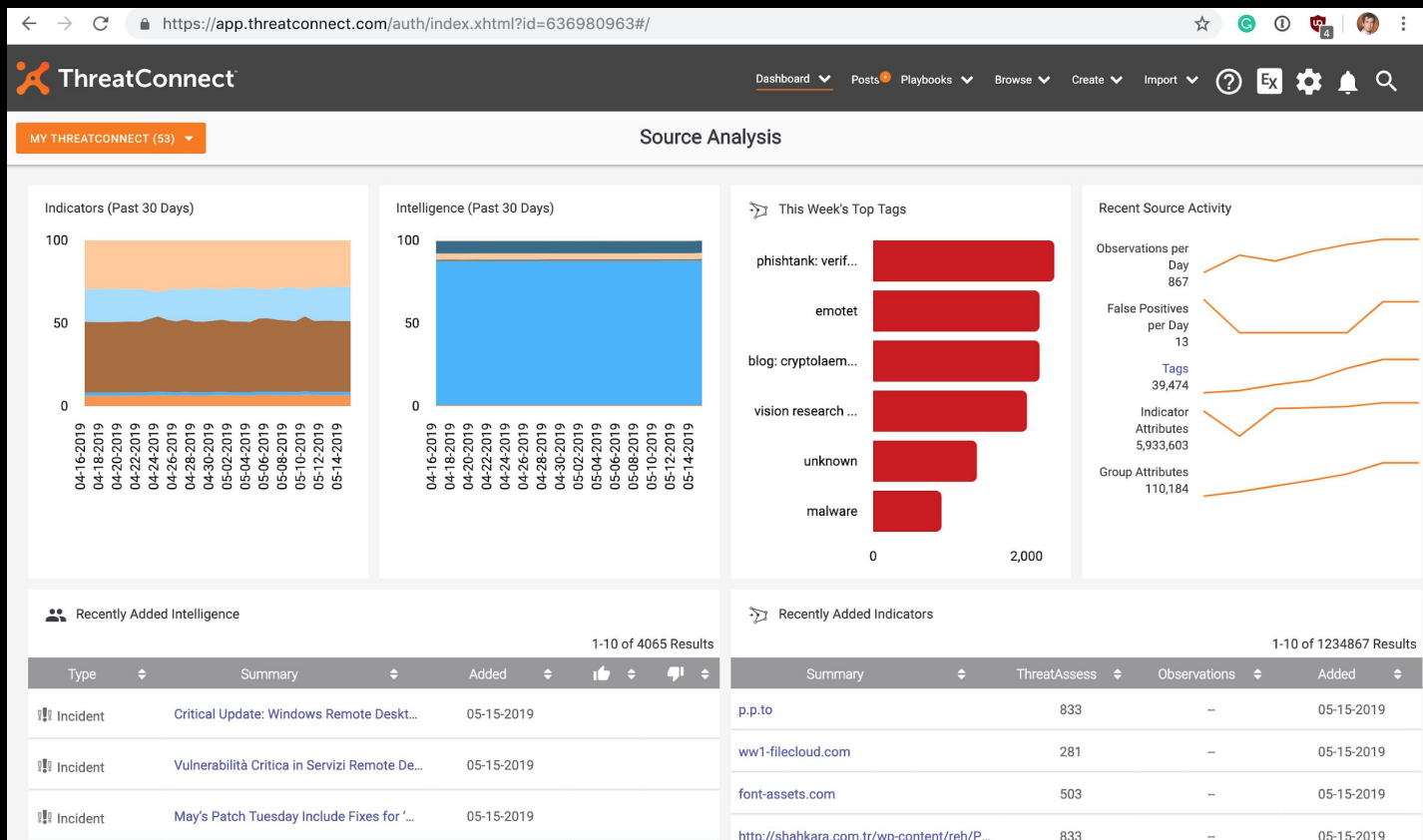


Cisco Firepower Publisher: World Wide Technology Version: 1.2.2 [Documentation](#)

This app interfaces with Cisco Firepower devices to add or remove IPs or networks to a Firepower Network Group Object, which is configured with an ACL.

▶ 4 supported actions

Threat Intelligence - ThreatConnect



Threat Intelligence - Anomali

← → ↺ https://ui.threatstream.com/threat-models

Threat Bulletins

10 1 - 10 of 5,527 items

Name	Last Updated	
cybereason: Excel4.0 Ma...	2019-05-15 14:36:12	
Bleeping Computer: Nor...	2019-05-15 14:32:26	
Bleeping Computer: Joke...	2019-05-15 14:32:13	
Recorded Future: Early Fi...	2019-05-15 14:31:57	
Naked Security by Sopho...	2019-05-15 14:30:53	

[See more in Threat Bulletins](#)

Actors

10 1 - 10 of 186 items

Name	Last Updated	
APT3 (Digital Shadows Id...	2019-05-07 17:44:15	
MuddyWater	2019-04-30 17:25:49	
APT28	2019-04-30 04:08:01	
OilRig	2019-04-26 16:44:09	
The Lamberts	2019-04-24 20:27:08	

[See more in Actors](#)

Campaigns

10 1 - 10 of 41 items

Name	Last Updated	
Bad Tidings Campaign	2019-03-20 03:00:00	
Tax Refund Phishing ca...	2019-02-21 01:44:50	
CISA, DHS Issue Emerge...	2019-01-28 23:08:25	
GRIZZLY STEPPE	2019-01-27 18:35:50	
Threat Group Steals Dat...	2019-01-07 21:11:01	

[See more in Campaigns](#)

TTP

10 1 - 10 of 1,129 items

Name	Last Updated	
Blue Boxing [CAPEC 5]	2019-03-16 14:55:21	
[MITRE ATT&CK] Winlogo...	2019-02-19 21:00:18	
[MITRE ATT&CK] XSL Scri...	2019-02-11 18:12:14	
[MITRE ATT&CK] Window...	2019-01-15 17:10:02	
[MITRE ATT&CK] Window...	2019-01-15 17:09:46	

[See more in TTP](#)

Incidents

10 1 - 10 of 118 items

Name	Last Updated	
Nordstrom Data Breach	2019-05-10 18:00:37	
Indian Local Search Com...	2019-04-18 19:51:08	
MageCart Attacks Ameri...	2019-03-25 20:02:36	
Verifications.io Data Bre...	2019-03-12 18:58:38	
Customers of TurboTax ...	2019-03-04 14:16:44	

[See more in Incidents](#)

Signatures

10 1 - 10 of 12,376 items

Name	Last Updated	
WannaCry Ransomware	2019-05-01 16:19:29	
Suspicious Rundll32 Acti...	2019-05-01 16:18:46	
Suspicious RASdial Activity	2019-05-01 16:18:38	
Multiple Failed Logins wi...	2019-05-01 16:18:31	
Netsh RDP Port Forwardi...	2019-05-01 16:18:21	

[See more in Signatures](#)

Vulnerabilities

Playbooks vs Instructions



Standard Operating Procedures (SOPs)

Instructions/Guidelines

Collaboration

Event Management

Case management

Reporting & Metrics

Automate investigation, data enrichments, Integrations,
Response

HIGH ▾

TLP:RED ▾

| Tenant: _default_ |

More ▾

Tasks Activity Guidance

Task List EDIT

▾ Detection

Current ☒

✓ Determine if an incident has occurred
assigned to Alex Cain



✓ Analyze precursors and indicators
assigned to Andrii Valchuk



Look for correlating information
assigned to no one

Perform research
assigned to no one

Confirmed incident

< Back to case

Analyze precursors and indicator

Assigned to Andrii Valchuk ▾

► DESCRIPTION

▾ NOTES (7)

🔍 Search notes

Confirmed Incident by Phantom Demo | Tue a

Yes

Closing Comments by Phantom Demo | Tue a

Tasks Activity Guidance

Recent Activity

Kevin Rexroat Yesterday at 1:44 pm
comment

promoted to case "Malicious URL Request Attempt" (id: 8272)

Andrii Valchuk a minute ago
changed owner on task "Determine if an incident has occurred" (id: 295) to Alex Cain

marked task "Determine if an incident has occurred" (id: 295) resolved

changed owner on task "Analyze precursors and indicators" (id: 296) to Andrii Valchuk

marked task "Analyze precursors and indicators" (id: 296) resolved

@apatel lets solve it together

automation In 25 minutes

▾ phishing_investigate_and_res...

▸ url reputation

▸ ip reputation

▸ geolocate ip

whois ip

phantom.act(): Failed to get asset to execute the action. Action execution shall fail

get screenshot

1 action failed for app Screenshot Machine

Comment



HOW

Keep It Simple

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

Activities

Automated

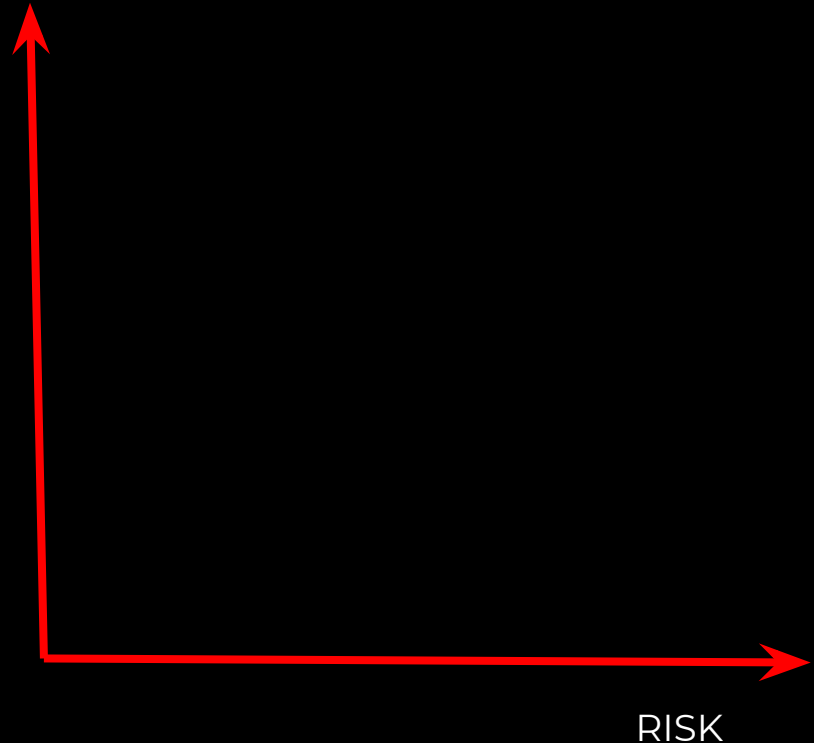
Select scripts run automatically. All decisions for triage, response and remediation are decided automatically

Semi-Automated

Select playbooks and actions run automatically. Analysts make triage, response and remediation decisions

Manual

Ownership -> Triage -> Analysis -> Disposition



Observe

POLL
PUSH INGEST
SET STATUS
SET SEVERITY
CREATE
ARTIFACTS
SAVE OBJECTS
SET TAGS

Orient

On Enrichments

FILE ANALYSIS
DOMAIN ANALYSIS
URL ANALYSIS
HOST ANALYSIS
IP ANALYSIS
LOGON ANALYSIS
RUN QUERY
GET EVENTS
Get customer info
Get system info
Get BU info
Run query Lookup info
Hunt file
URL Rep
Domain Rep
Get File
Check white/black lists

Act

(Manually/Automated)

DISABLE USER BLOCK
HASH BLOCK URL
BLOCK DOMAIN
BLOCK IP
QUARANTINE HOST
BLOCK PROCESS
DISABLE VPN

Notify

Collaborate

EMAIL SOC
EMAIL
LEADERSHIP
CHAT IT HELP
DESK EMAIL
ENGINEERING
PROMPT SOC
TASK SOC
Get Approval
Promote Case
Prompt Analyst
Change Severity
Change Sensitivity

Document

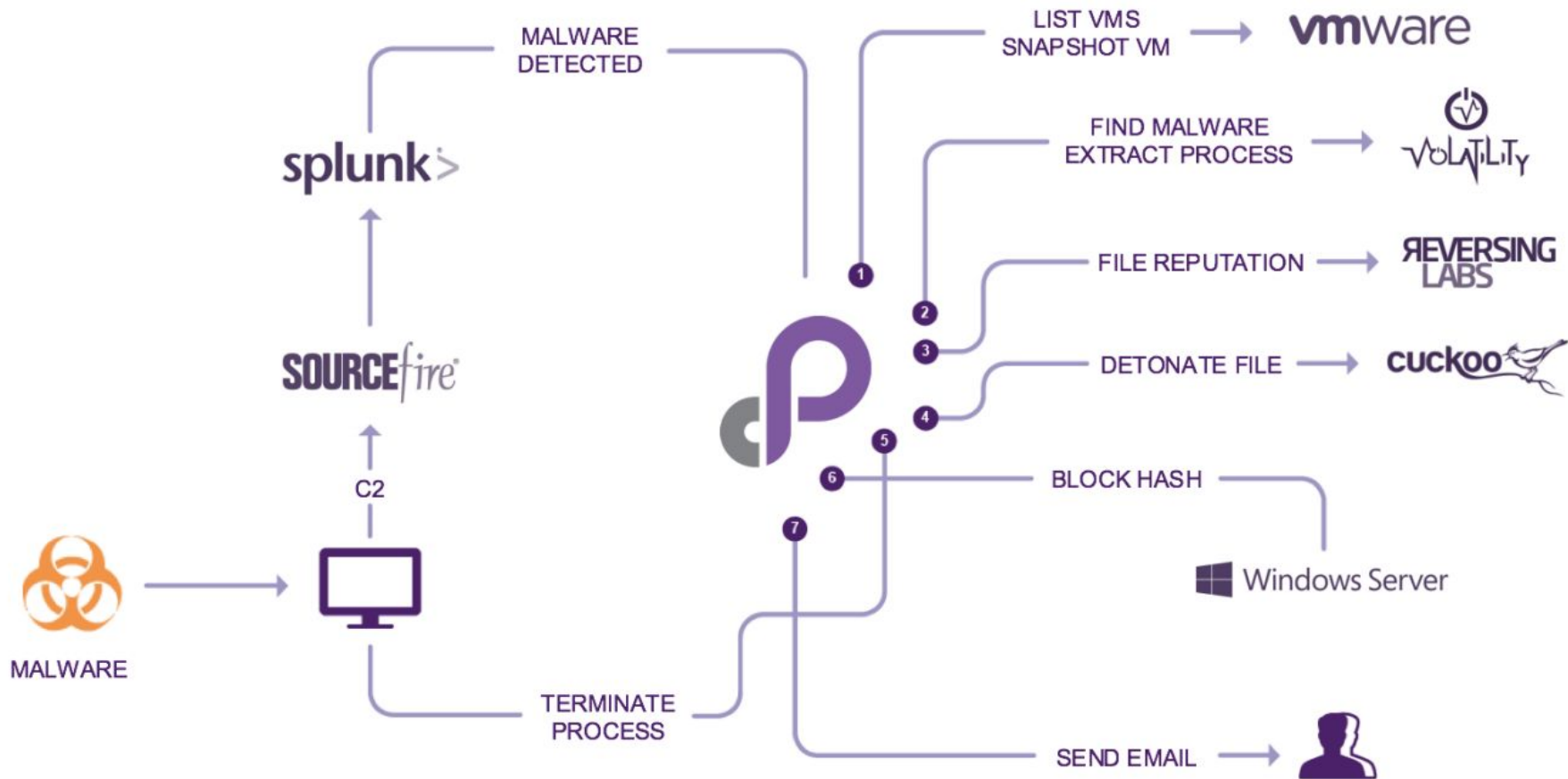
Knowledge base

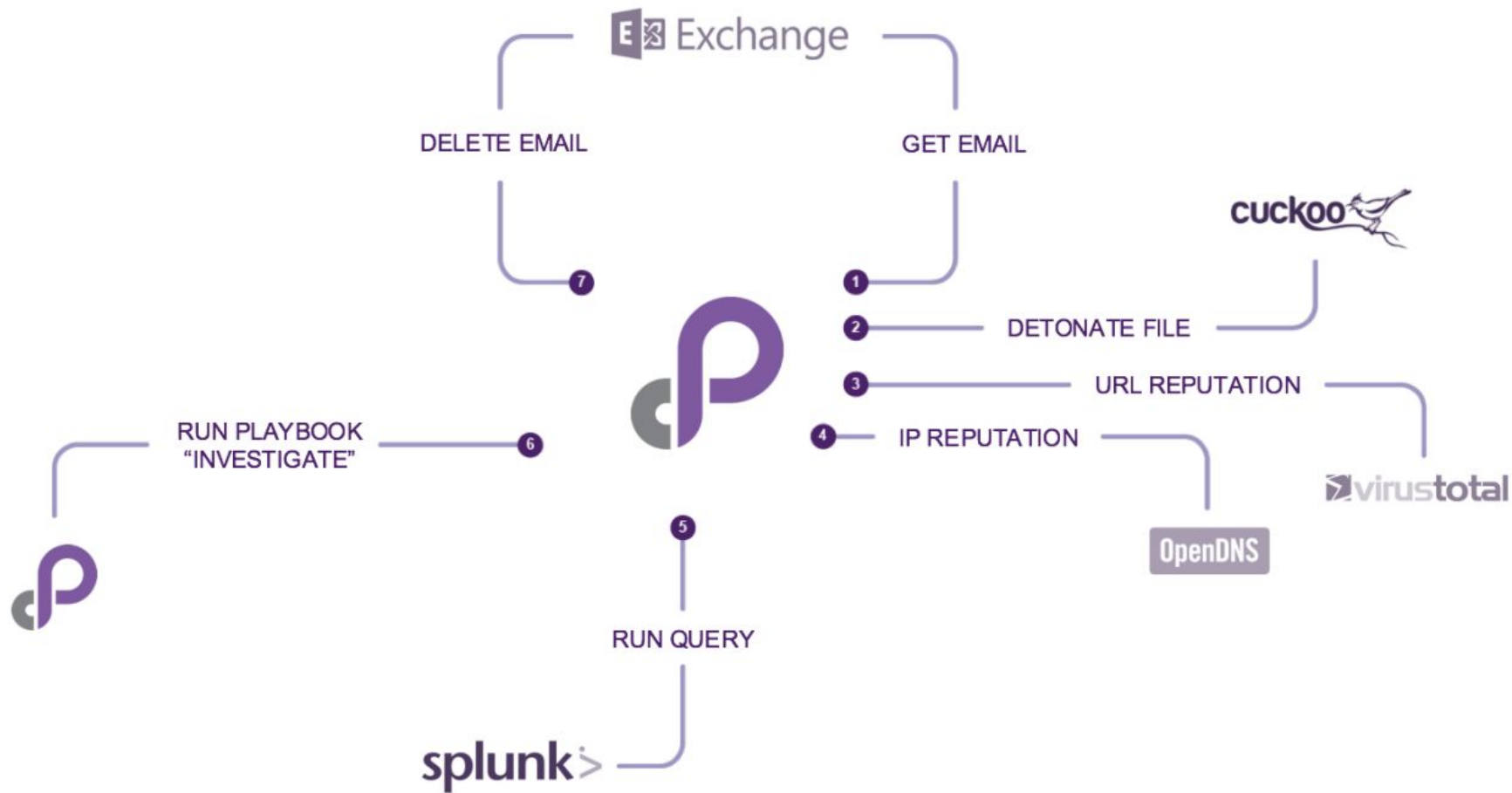
CREATE TICKET
UPDATE TICKET
CLOSE TICKET
TRANSFER TICKET
QUERY TICKETS
CREATE ARTIFACTS
CLOSE OBJECTS

Prioritize



Community Playbooks





< scan network

Advanced Settings

Configure Action by Asset by App

Filter by Type

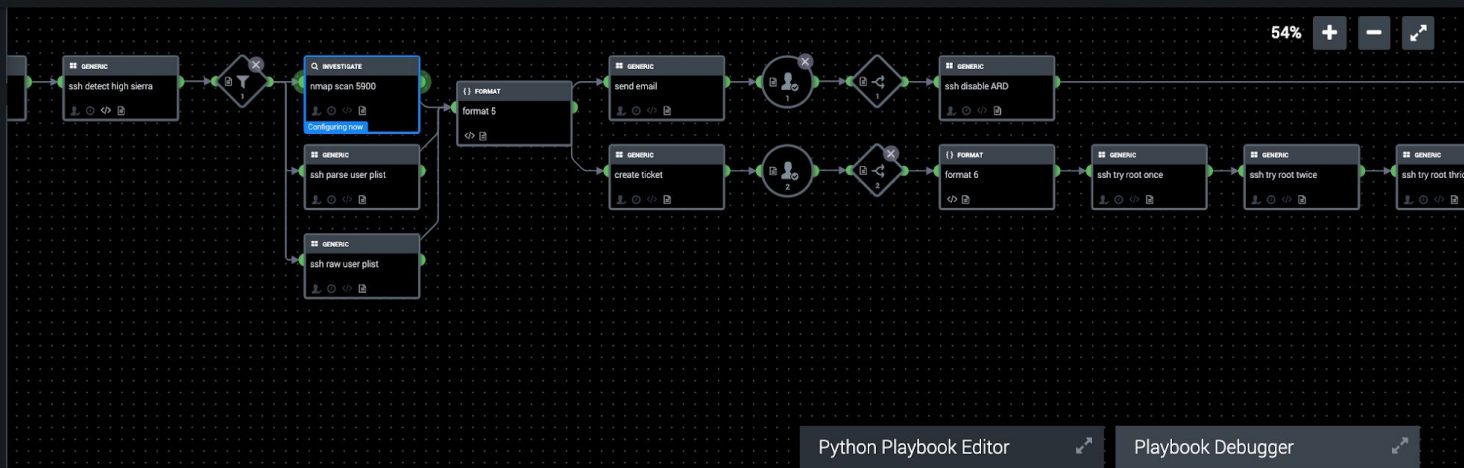
Available Assets (1)

Search assets

nmap

CONFIGURING

There are no assets configured that support this action.



Function nmap_scan_5900

```
91
92 #phantom.debug('Action: {0} {1}'.format(action['name'], ('SUCCEEDED' if success else 'FAILED')))
93
94 # collect data for 'nmap_scan_5900' call
95 filtered_results_data_1 = phantom.collect2(container=container, datapath=["filtered-data:filter_1:condition_1:ssh_detect_high_sierra:action_result.parameter.ip_hostname", "filtered-
data:filter_1:condition_1:ssh_detect_high_sierra:action_result.parameter.context.artifact_id"])
96
97 parameters = []
98
99 # build parameters list for 'nmap_scan_5900' call
100 for filtered_results_item_1 in filtered_results_data_1:
101     if filtered_results_item_1[0]:
102         parameters.append({
103             'portlist': 5900,
104             'script-args': "",
105             'udp_scan': "",
106             'ip_hostname': filtered_results_item_1[0],
107             'script': "",
108             # context (artifact id) is added to associate results with the artifact
109             'context': {'artifact_id': filtered_results_item_1[1]},
110         })
111
112 phantom.act("scan network", parameters=parameters, assets=['nmap'], callback=join_format_5, name="nmap_scan_5900")
113
114 return
```

splunk>phantom

macos_root_password_mitigate

< execute program

Advanced Settings

General Settings

Action Settings

Join Settings

Configure Action

by Asset by App

Filter by

Type

Available Assets (1)

Search assets

ssh_macos_administrator CONFIGURING

There are no assets configured that support this action.

General Settings

Custom Name

ssh disable ARD

Description (code comment)

Use the built-in perl script called "kickstart" to turn off all access to ARD, stopping the service listening on TCP 5900.

Notes (block tooltip)

Use the built-in perl script called "kickstart" to turn off all access to ARD, stopping the service listening on TCP 5900.

9 missing assets

Repo: community

PLAYBOOK SETTINGS

CANCEL

SAVE

54%

+

-

GENERIC

send email

1

1

GENERIC

create ticket

2

2

GENERIC

ssh disable ARD

CONFIGURING NOW

FORMAT

format 6

GENERIC

ssh try root once

GENERIC

ssh try root twice

GENERIC

ssh try root thrice

END

Python Playbook Editor

Playbook Debugger

ALERT

Test it before
Network is
DOWN



ML use cases

CASE 6: EXTRACTING DUPLICATE INCIDENTS

CASE 4: VISUALIZING RELATED INCIDENTS

CASE 3: COMMONLY USED SECURITY COMMANDS

CASE 2: SECURITY EXPERT SUGGESTIONS

CASE 1: INCIDENT OWNER RECOMMENDATIONS

Chatbots



SLA

Response Settings

The Default Event SLA is a positive numeric value, and is in minutes. The SLA is the amount of time that will be permitted to Approve an Action against an Asset needing Approvals before it is late and is escalated.

DEFAULT SETTINGS

High severity


minutes

Medium severity

minutes

Low severity

minutes

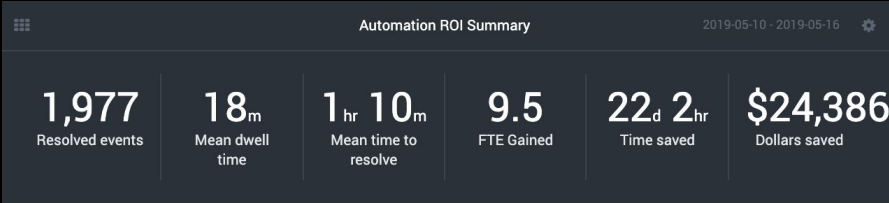
☒ Automatic self-approval 

When all of the SLA escalations have expired without being acted on, the Executive Approvers will receive an SLA breach notification.

Executive approvers (receive notices on SLA breaches)

▼

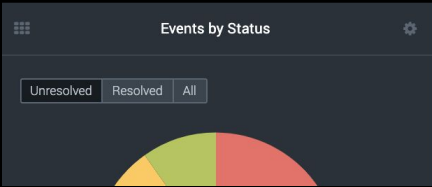
Estimated hours saved per month



Open

Name	SLA	SEVERITY
Malicious URL Request Attempt	+ 6%	HIGH
Malicious URL Request Attempt	+ 6%	HIGH
Malicious URL Request Attempt	+ 6%	HIGH
ASN Transaction	+ 4%	HIGH
ASN Transaction	+ 4%	HIGH
ASN Transaction	+ 4%	LOW
Malicious URL Request Attempt	+ 3%	MEDIUM
ASN Transaction	+ 3%	HIGH

< 1 2 3 4 5 ... 13 >



Top Playbooks and Actions

Top Playbooks Top Actions All Categories

Top Playbooks	Actions	Execute Time	Executed
phishing_investiga	10174	an hour	2004

ROI



THREE - HUHHA

Key Takeaways

1. Document your process and Measure where you're losing YOUR time
2. Be careful before applying it on Production, TEST-TEST-TEST
3. Make NOC/IT your FRIENDS though SOAR
4. More Automation - more TIME, less people, ability to learn
5. By implementing automation and orchestration aiming to:
 - > Focus analysts time on analysis
 - > Focus analysts time on finding threats
 - > Reduce risk through speed and consistency

And **remember** - Tools don't matter...

When you
have a ~~GUN~~

Brain





THANK YOU

Nazar Tymoshyk
CEO at UnderDefense

Contact: nt@underdefense.com



