

Scary Fast Intelligence-Based Hunting with Splunk>Phantom



EY Cybersecurity

October 2019 | Final Version



Haris Shawl

EY | Senior Manager & Threat Intel Guru



Robb Mayeski

EY | Senior Manager & Security
Automation Magician

Forward-Looking Statements



During the course of this presentation, we may make forward-looking statements regarding future events or plans of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results may differ materially. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only, and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionalities described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Turn Data Into Doing, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2019 Splunk Inc. All rights reserved.



How do you hunt in your environment?

The scary fast way

EY Cybersecurity

We're not just auditors and accountants...

Threat Detection & Response

- 24x7x365 threat monitoring
- Threat identification and alert triage
- Threat notification and escalation
- Containment, eradication and recovery recommendations
- Attack disruption of pre-approved activities
- Automated attack containment

Threat Intelligence

- Threat detection signatures (YARA, SNORT, etc.)
- Daily intelligence production
- Adversary infrastructure monitoring
- External commercial feeds
- External infrastructure analysis
- Honeypots & sink holing

Threat Hunting

- Analyst-driven (daily to weekly)
- Intelligence-triggered (daily to weekly)
- Anomaly-based (continuous)
- Scenario-based (monthly to quarterly)
- Mission-based (monthly to quarterly)

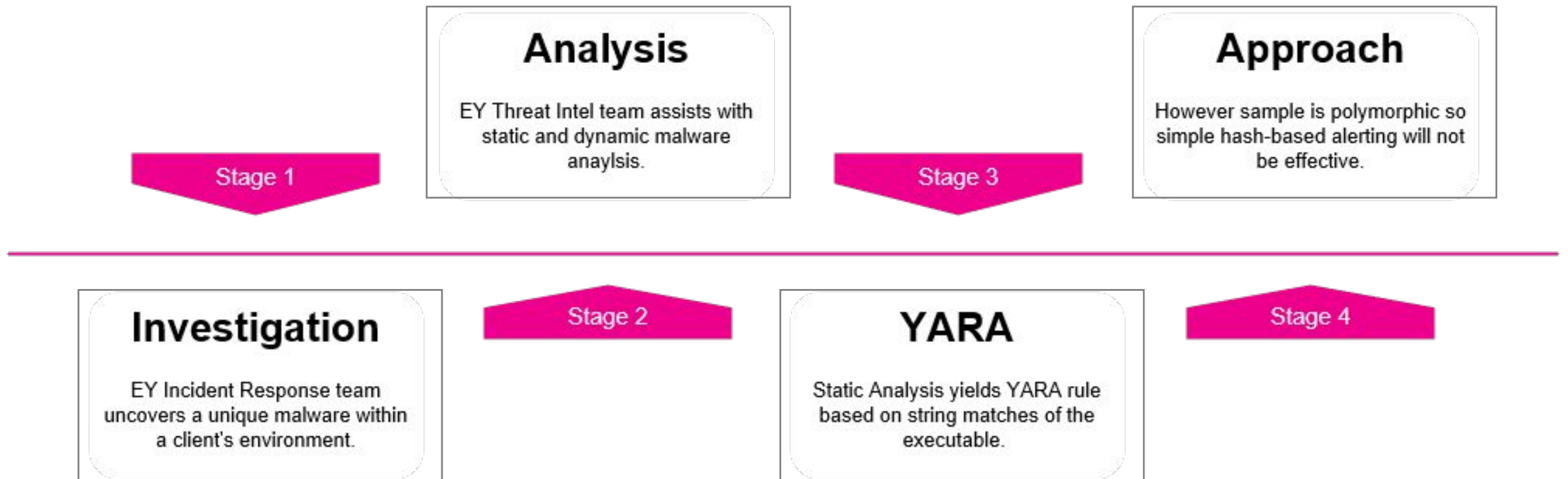
Incident Response

- Investigation management and coordination
- Malware analysis
- Eradication event planning and execution assistance
- Computer forensics
- Executive communications
- Global team

Setting the scene: External company Intrusion

© 2019 SPLUNK INC.

We caught some malware and wrote a signature



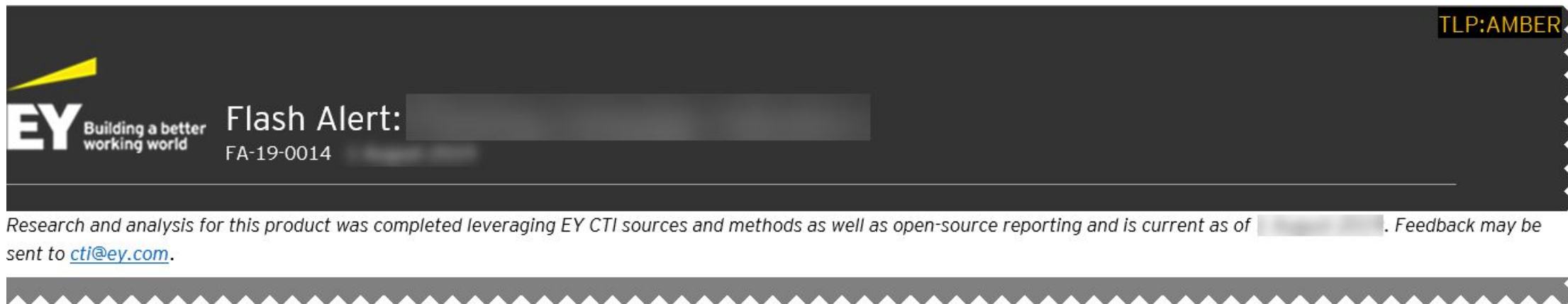
YARA: a set of rules that characterizes malware in an attempt to identify it consistently.

How do we utilize the new YARA signature to hunt easier for similar malware or infections?”

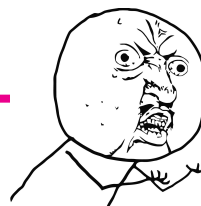
Automation. Powered by Splunk>Phantom

A Report goes out via Cyber Threat Intel

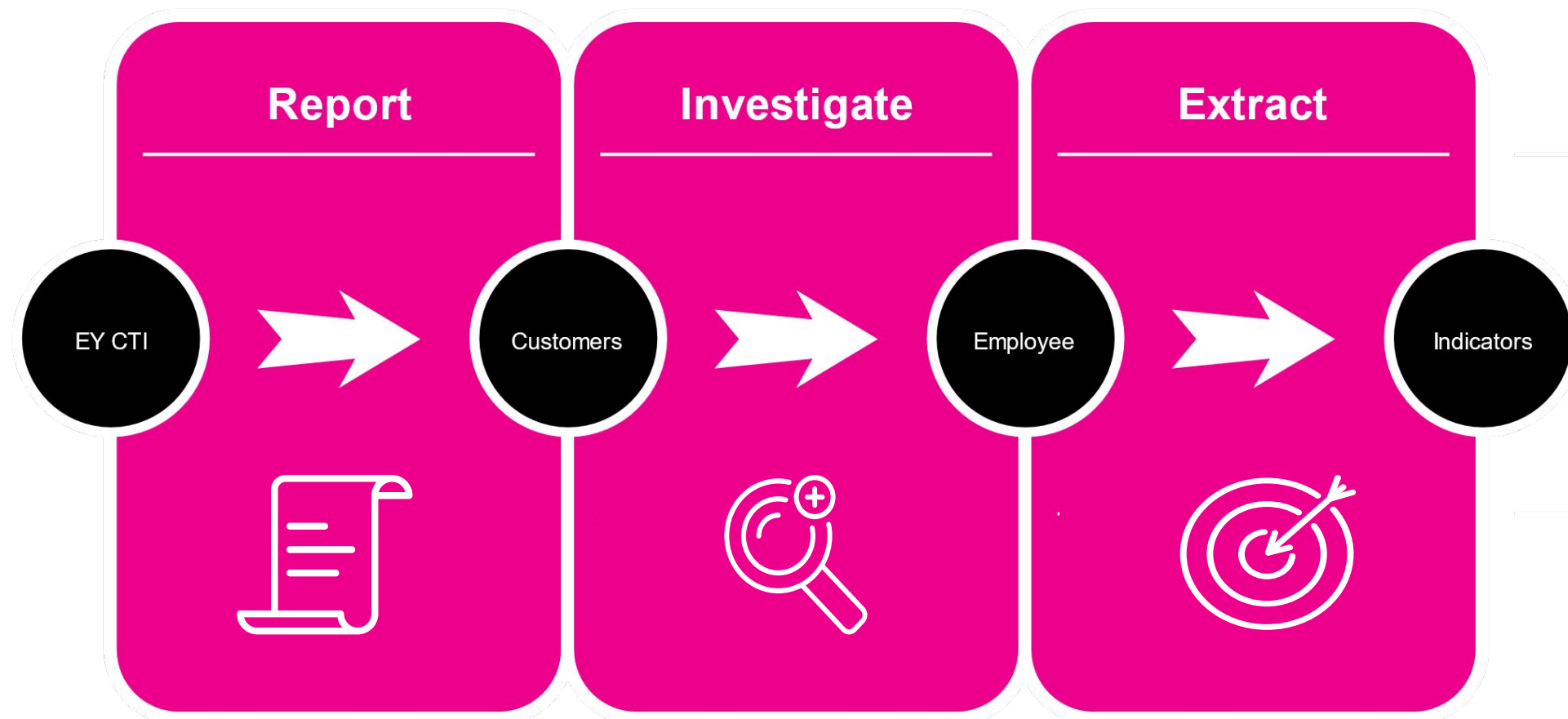
EY CTI writes a report of the newly found malware from the investigation, sends to threat intel customers



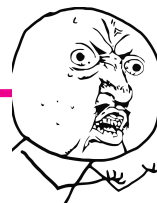
A person must manually extract the technical indicators to process them into their environment



A report goes out via Cyber Threat Intel

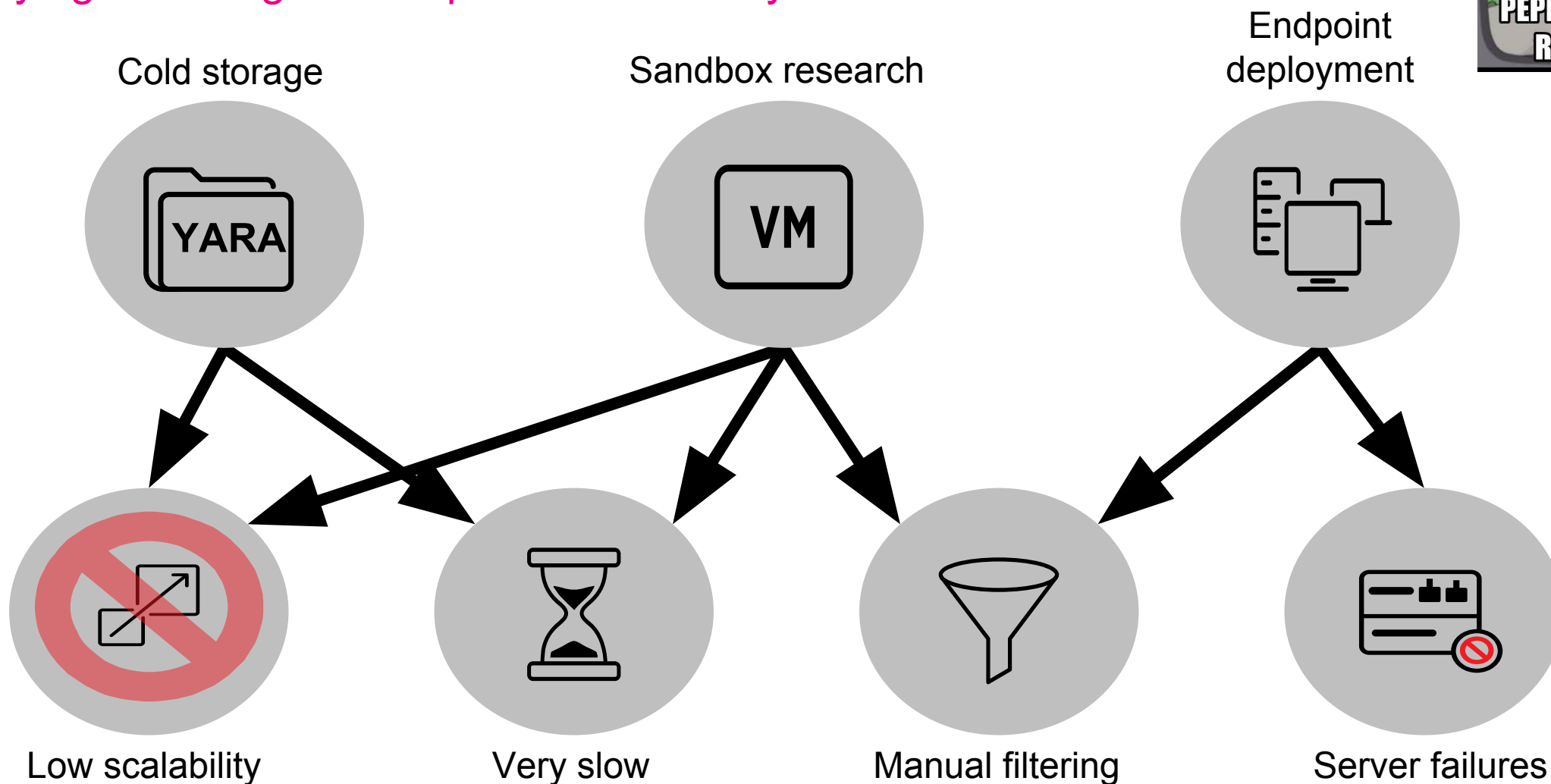


- ▶ A person must manually extract the technical indicators to process them into their environment



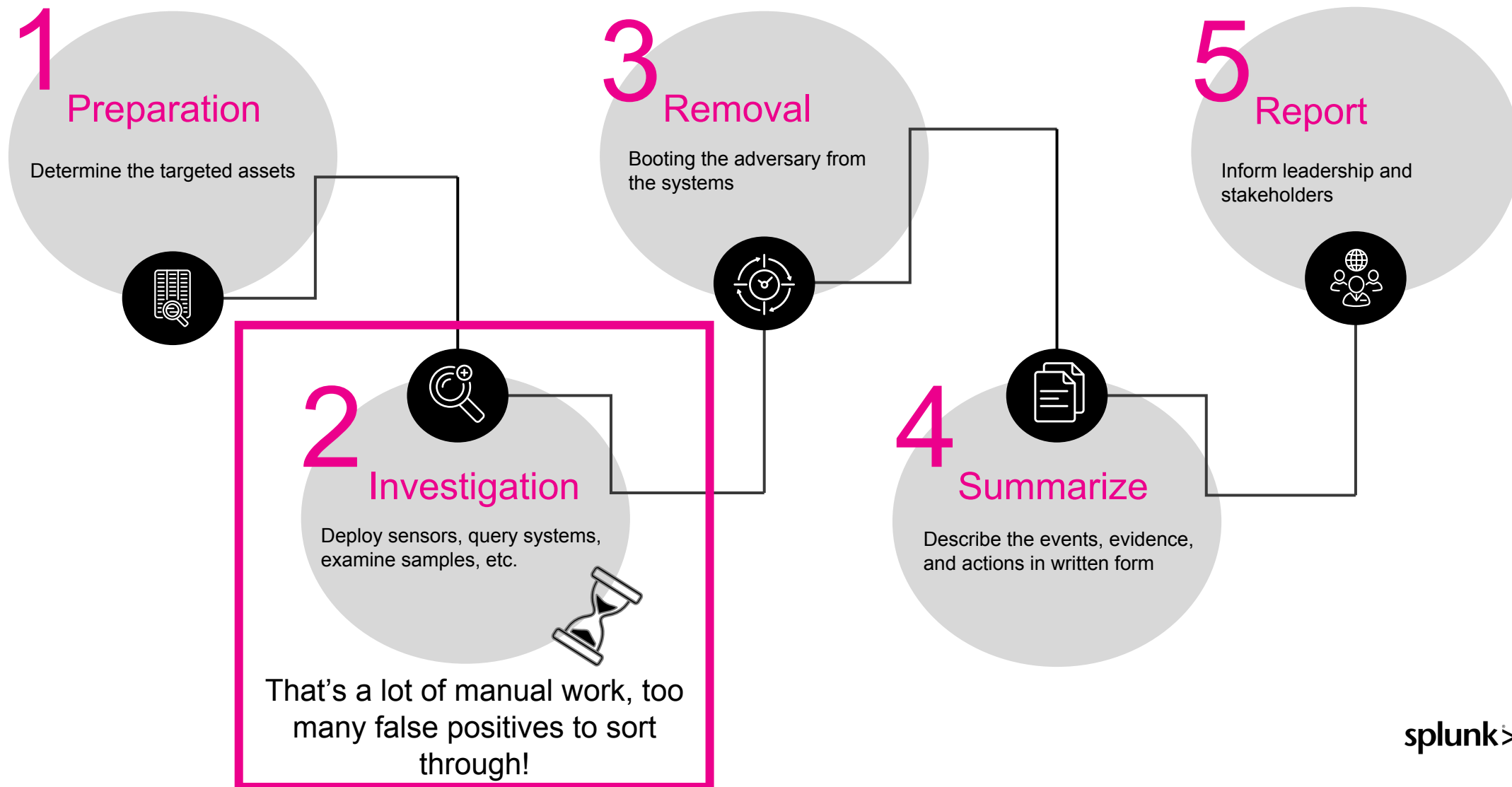
Ye Olde Days; Manual Hunting

Applying those signatures pre-Phantom days



What does a manual hunt look like?

Finding out what happened and what the extent is



“How do we hunt faster and
how do we take the info from
this incident to help others?”

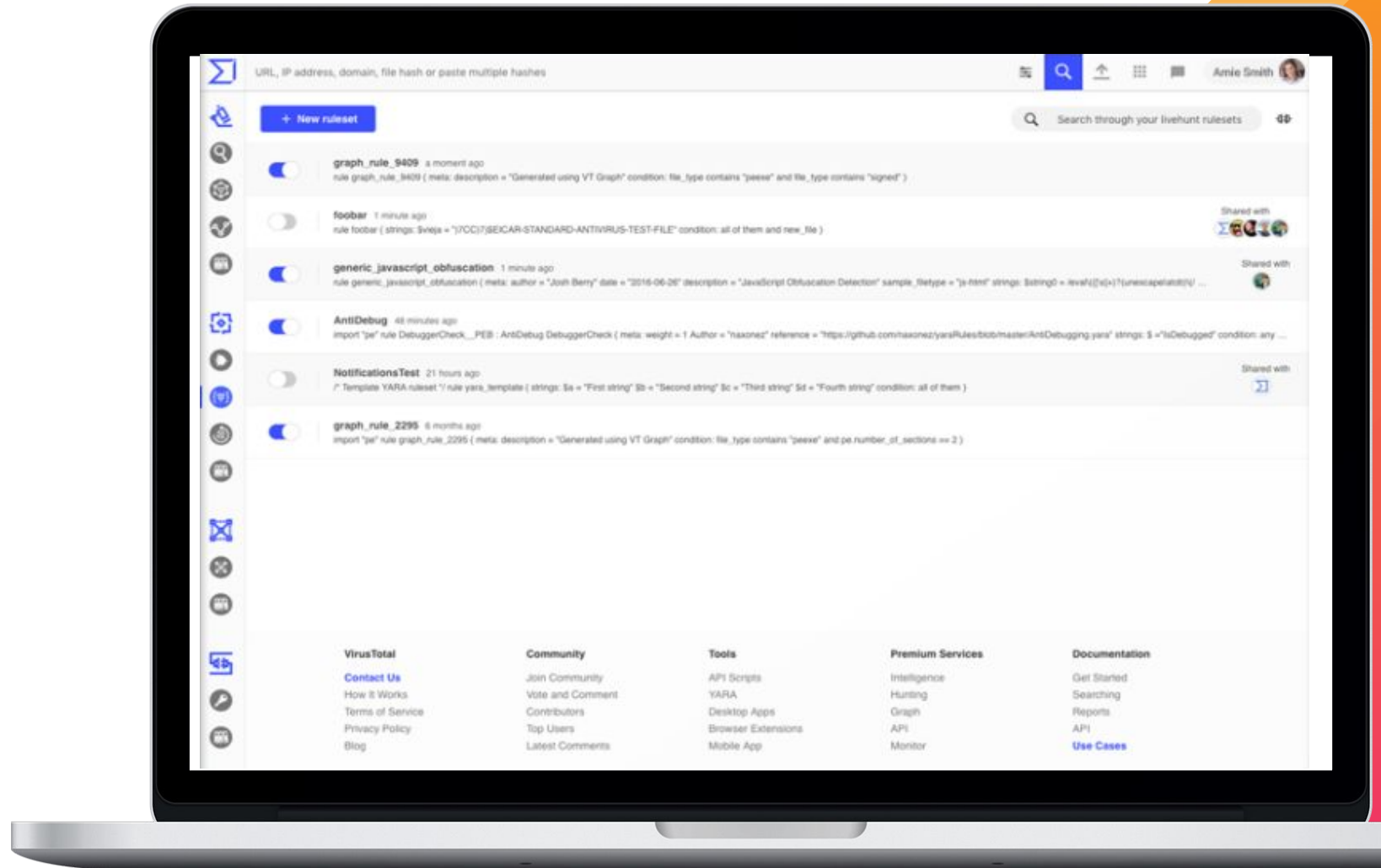
Automation. Powered by Splunk>Phantom

Playbook in Phantom

Hunt in your network,
at speed

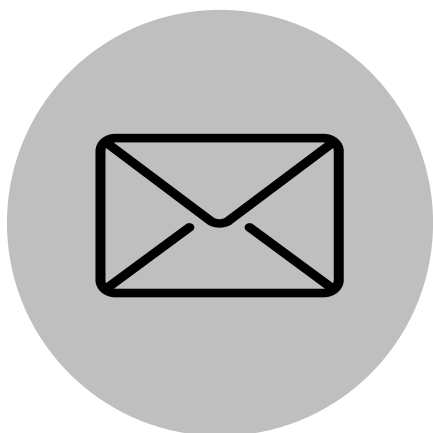
Modeled after VirusTotal
YARA Hunt concept where
with the premium
VirusTotal a hunt can be
run for malware variants in
external datasets
(VirusTotal).

With this hunt you can do it
internally and can gain
visibility into your network.

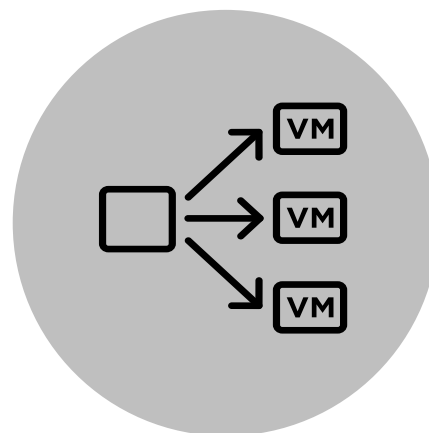


Playbook in Phantom

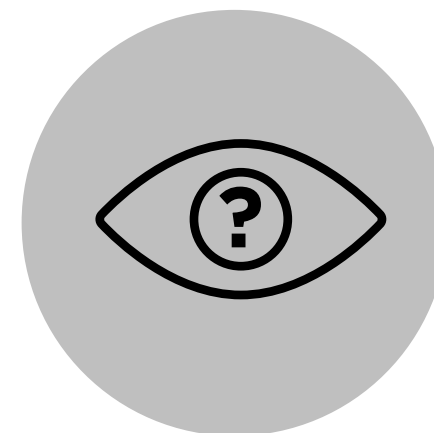
What does the hunt look like in Phantom?



Ingest CTI email and
parse the YARA rule



Push the YARA rule
to Tanium, Carbon
Black



Set to a YARA scan,
off peak hours, runs
over hours

If we found a match...



Playbook in Phantom

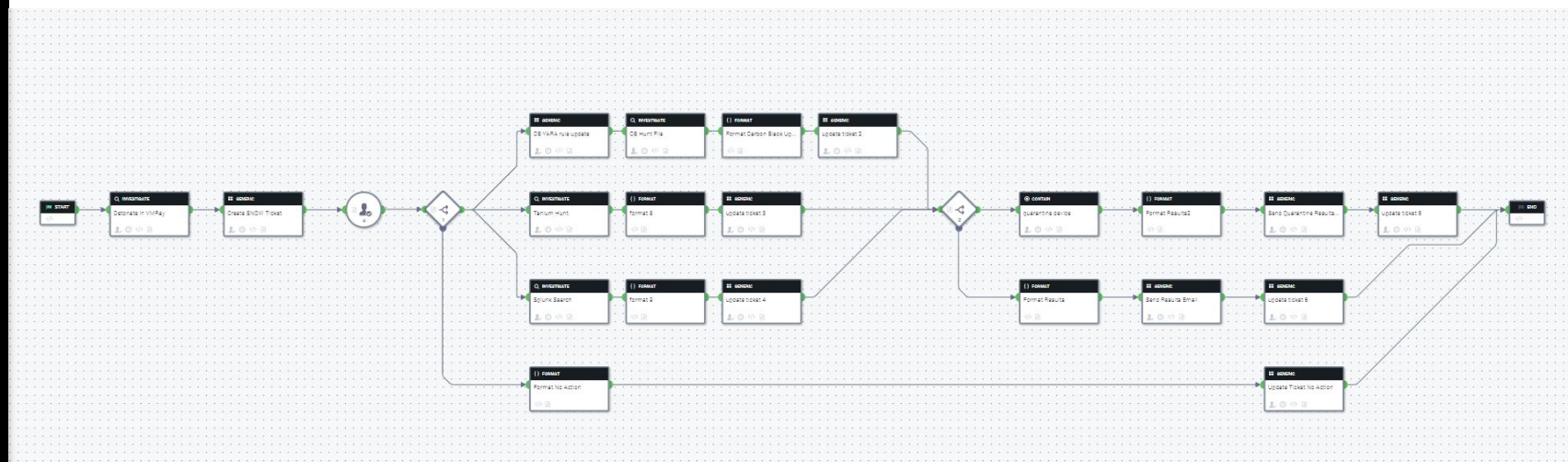
Now that we've found a match using Tanium, Carbon Black

Phantom Integrations Needed

What you need to make this work

- Endpoint Detection & Response (EDR) Tool (Carbon Black or Tanium)
- Malware Sandbox (VMRay)
- Splunk & Phantom
- Ticketing system (ServiceNow)
- Email ingestion (Exchange)



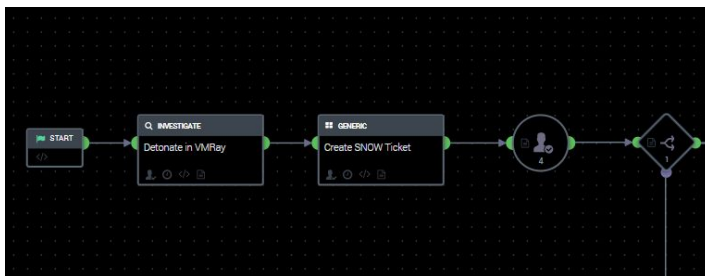


Breaking Down the Playbook

Visualizing how it all fits together

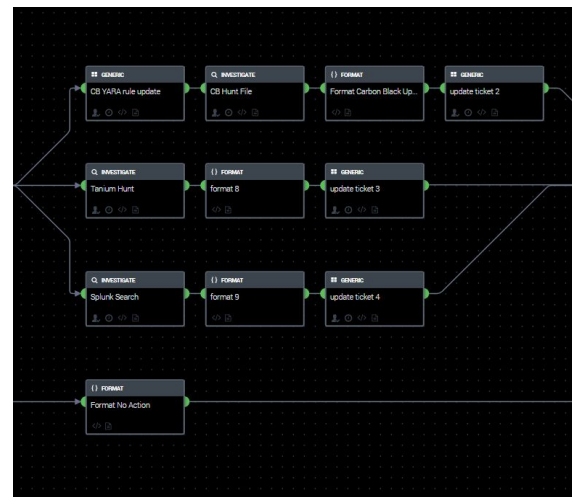
Response actions based on hunt

- Quarantine asset if deemed infected
- Notify response team on communication platforms



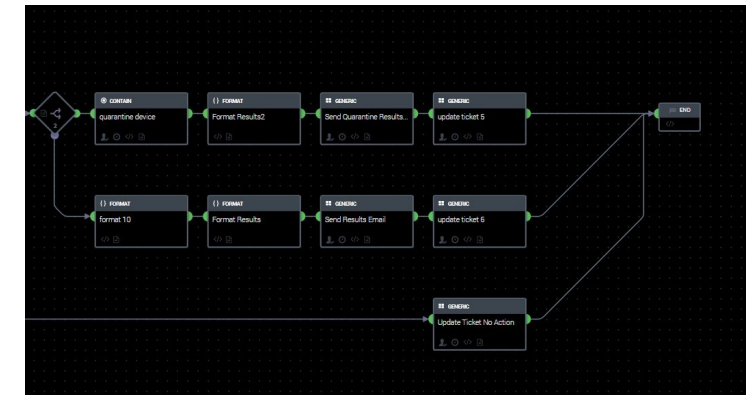
Hunt the network for signatures

- Update Yara rules
- Search for any rule or signature based hits across toolset



Triage after initial receipt of Yara and malware samples via email

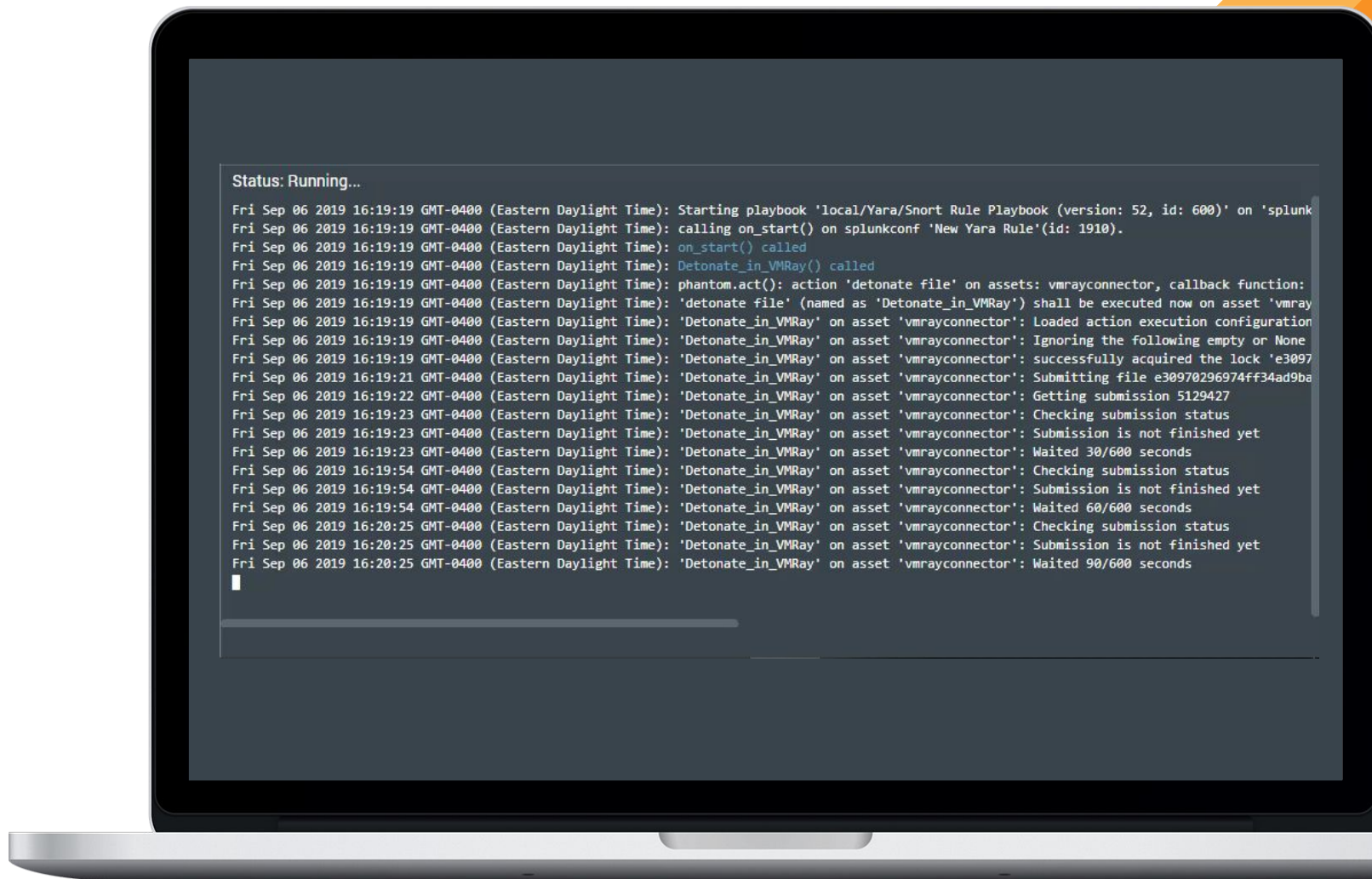
- Detonate sample to gain insights
- Present insights and ask analyst if hunt should continue



Actually automating the hunt



How the hunt actually executes in Phantom



The screenshot displays the Splunk Phantom Mission Control interface. At the top, the header includes the Splunk logo, a search bar, the text "MISSION CONTROL", a version indicator "version 4.1.94", and a notification bell icon.

Below the header, the main content area shows details for a specific event (ID: 1603). It includes a status bar with "MEDIUM" severity, "TLP:AMBER" classification, and an SLA status of "Exceeded by 3 days". The owner is listed as "Robb Mayeski".

A table of key metrics is displayed:

Source ID:	Activity Start:	Created:	Opened:	Playbooks Run:
[Redacted]	Thu at 4:53 pm	Thu at 4:53 pm	Not opened	20
Artifacts:	Activity End:	Updated:	Resolved:	Actions Run:
2	Ongoing	4 minutes ago	Not resolved	14

Buttons for "JSON", "AUDIT", "EXPORT", and "EDIT" are available.

The main interface is divided into several tabs: Activity, Guidance, Timeline (selected), HUD, Artifacts, Vault, Approvals, and Reports. The Timeline tab shows a horizontal timeline with a vertical red line indicating the current time. A list of recent activity is shown on the left, including "Yara/Snort Rule Playbook" and "detonate file". The timeline itself shows a sequence of actions: "update ticket", "Note Prompt", "prompt", "create ticket", "detonate file", and "Yara/Snort Rule Playbook".

At the bottom, there is a "Comment" field and a "MANAGE WIDGETS" button.

The image shows a laptop screen with four Splunk dashboards arranged in a 2x2 grid. Each dashboard has a sidebar on the left with search queries and a main content area with data tables.

VMRAY

Search query: `detonate file e30970296974ff34ad9bae...`

SUBMISSION ID	ANALYSIS ID	FINISHED	SEVERITY	URL
5139125	None	True	suspicious	https://cloud.vm
5139125	None	True	suspicious	https://cloud.vm
5139125	None	True	suspicious	https://cloud.vm
5139125	None	True	suspicious	https://cloud.vm

Carbon Black.

Search query: `hunt file 548f14dd160e4aae4041ed 462766292796E1D3454C3 902CD44142E7E8DBEF72`

MD5	ENDPOINTS	SIGNED	COMPANY NAME
462766292796E1D3454C3F050C580940	cdntdains01 5 cdntdair01 4 cdntdalc01 1 cdntdalfs01 6 cdntdalrt01 7 cdntdalms01 2 caas_demo_ep05 11 caas_demo_ep04 ...	Signed	Free Software Foundation

splunk>

Search query: `run query sourcetype="bit9_cbs_sam" index="yara_rule" "wicked"`

HOST	INDEX	LINECOUNT	SOURCE	SOURCETYPE	SPLUNK_SERVER
cdnxdalsp01	yara_rule	1	yaraRuleData.csv	csv	cdnxdalsp01
cdnxdalsp01	yara_rule	1	yaraRuleData.csv	csv	cdnxdalsp01
cdnxdalsp01	yara_rule	1	yaraRuleData.csv	csv	cdnxdalsp01
cdnxdalsp01	yara_rule	1	yaraRuleData.csv	csv	cdnxdalsp01

servicenow

Search query: `update ticket eb866869db333300827f90 6b53e461db333300827f90`
create ticket

NUMBER	SHORT DESCRIPTION	DESCRIPTION
INC0010012	New File Detonation	A New File Has Been Detonated, Prompting User for further action.

TANIMUM.

Search query: `run query tanmgt01.taniumpoc.caast Get Index Query File Details`

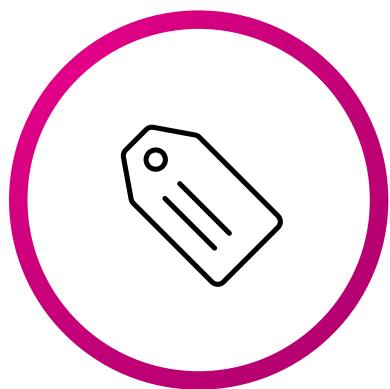
Is Parsed	Timeout Seconds
True	60

Run Query Results

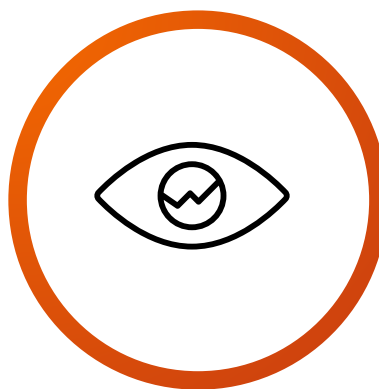
MD5 HASH	SHA1 HASH	SHA256 HASH
712356bf79a10f4c45cc0a1772bbeaf6	6faefa9e7ad2f9eb2d1cd9c129d6345d2424	
712356bf79a10f4c45cc0a1772bbeaf6	6faefa9e7ad2f9eb2d1cd9c129d6345d2424	
712356bf79a10f4c45cc0a1772bbeaf6	6faefa9e7ad2f9eb2d1cd9c129d6345d2424	

What comes next?

New logic in Splunk ES for alerting and detection



Case Management
ticketing tracking



New logic in Splunk
ES for alerting and
detecting



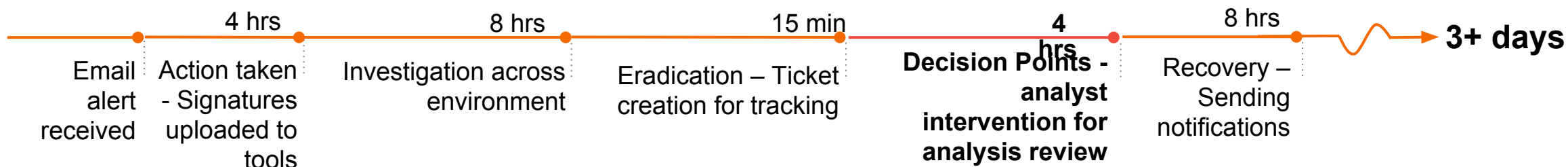
Specific tasks for the
IR team to gather
artifacts



What makes the Hunt “Scary Fast”

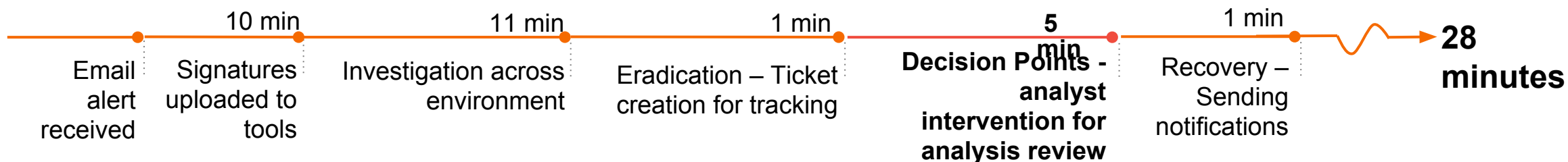
Phantom saves the day, at speed

Manual... it's “scary slow!”



Without SOAR this process can, in some instances, take 3+ days depending on variables such as staff, environment complexity, and risk tolerance just to name a few.

What makes it “scary fast?”



28 minutes with SOAR
versus over a day
without.

Key Takeaways

Orchestration for the win

1. Because, “Phantom”
 - Better reporting (combining results from an endpoint and network sensor)
 - More robust (plugging into all the tools with one click instead of forgetting one or two)
 - Faster time (from YARA/SNORT rule creation to execution in an environment and results would take days/weeks or not even be attempted)
2. Analysts did these YARA hunts in VTI in the past, now we can do it within a customer’s security data lake!

DEMO

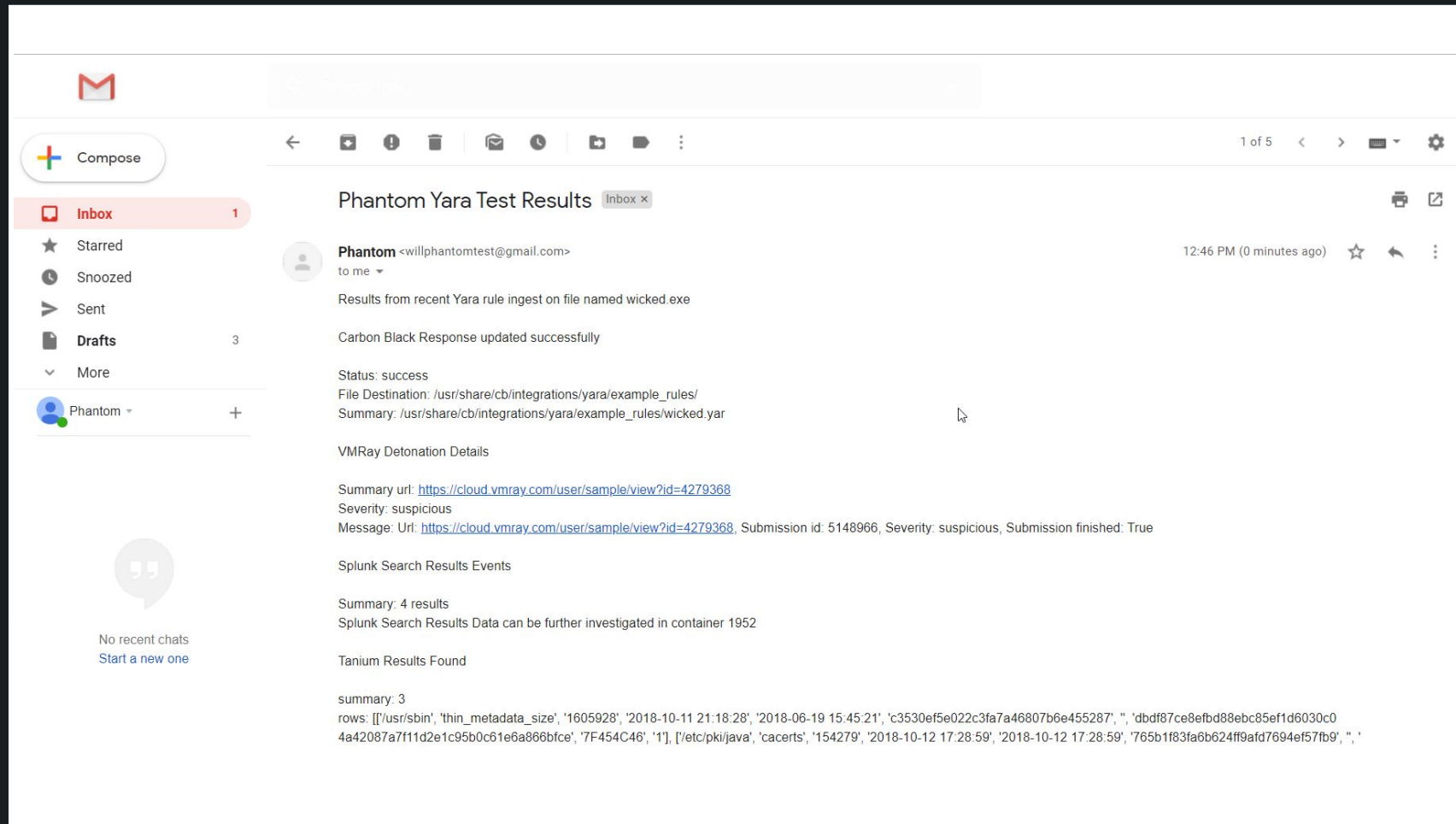
The screenshot shows a Gmail inbox with the 'Primary' tab selected. The inbox is empty, displaying the message: "Your Primary tab is empty. Personal messages and messages that don't appear here. To add or remove tabs click [inbox settings](#)."

On the left sidebar, the 'Compose' button is visible, along with folders: 'Inbox', 'Starred', 'Snoozed', 'Sent', 'Drafts' (4), and 'More'. A contact named 'Phantom' is listed at the bottom of the sidebar.

At the bottom of the sidebar, there is a section for 'No recent chats' with a link to 'Start a new one'.

At the bottom of the main content area, it shows '0 GB (0%) of 15 GB used' and a 'Manage' link.

Overlaid on the right side of the screen is a 'New Yara Rule from Malware Sample' dialog box. The dialog has a title bar with standard window controls. It contains two input fields: the first is labeled 'Phantom' and the second is labeled 'New Yara Rule from Malware Sample'. Below these fields is a large text area. At the bottom of the dialog, there are two file attachments: 'wicked.yar (1K)' and 'wicked.exe (70K)', each with a close button (x). Below the attachments is a 'Send (Ctrl-Enter)' button. At the very bottom of the dialog is a 'Send' button with a dropdown arrow. To the right of the 'Send' button are icons for text formatting (bold, italic, underline, link, image, video, link, currency) and a trash icon.





Q&A

Haris Shawl | Threat Intel Guru
Robb Mayeski | Security Automation Magician

EY Team Credit

Development and Hunt Team at EY



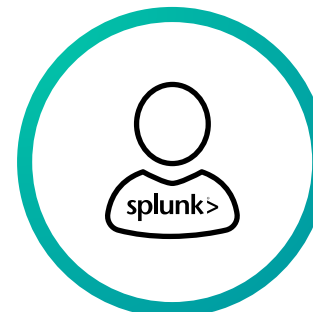
Himanshu Anand



Mike Palitto



Ruchir Arya



Chris Jones



Will Burger



Thank

You



Go to the .conf19 mobile app to

RATE THIS SESSION

