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

splunk> .conf19

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.

How do you hunt in your environment?

The scary fast way

splunk> .conf19

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

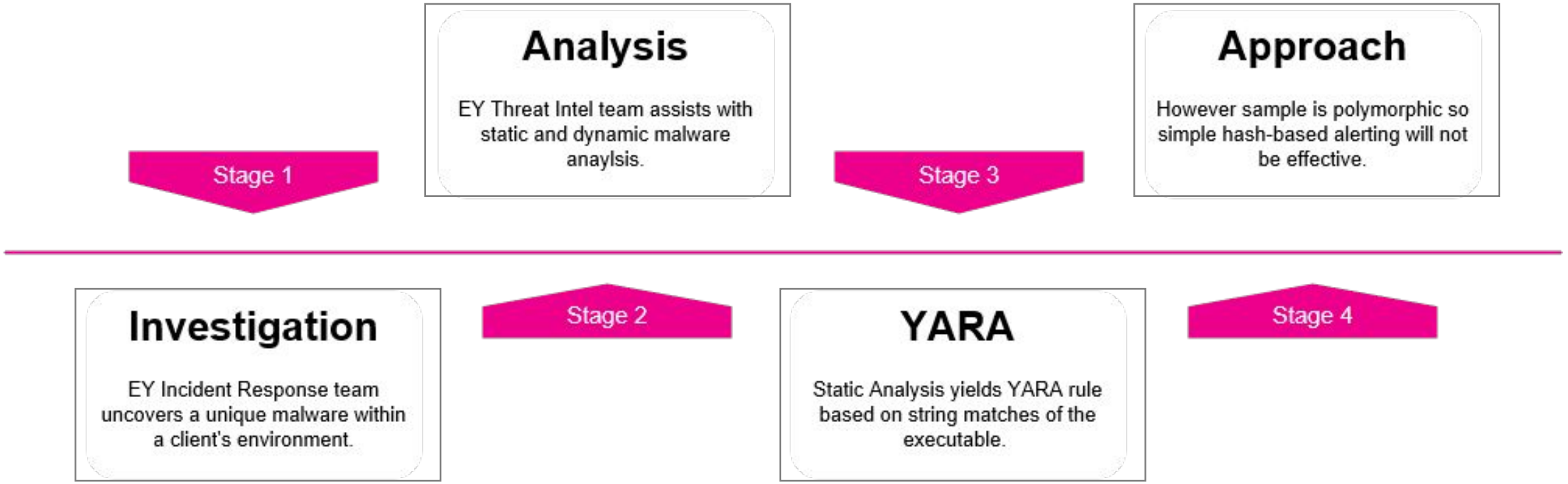
- Analyst-driven (daily to weekly)
- Intelligence-triggered (daily to weekly)
- Anomaly-based (continuous)
- Scenario-based (monthly to quarterly)
- Mission-based (monthly to quarterly)

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

We caught some malware and wrote a signature



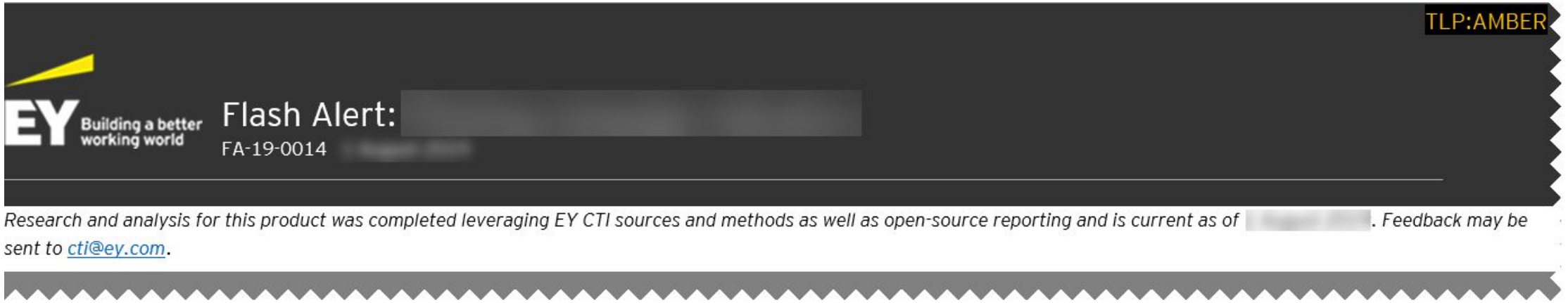
YARA: a set of rules that characterizes malware in an attempt to identify it consistently.

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


TLP:AMBER

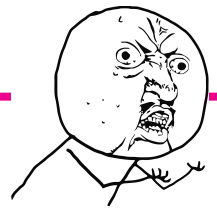
EY Building a better working world

Flash Alert: [redacted]

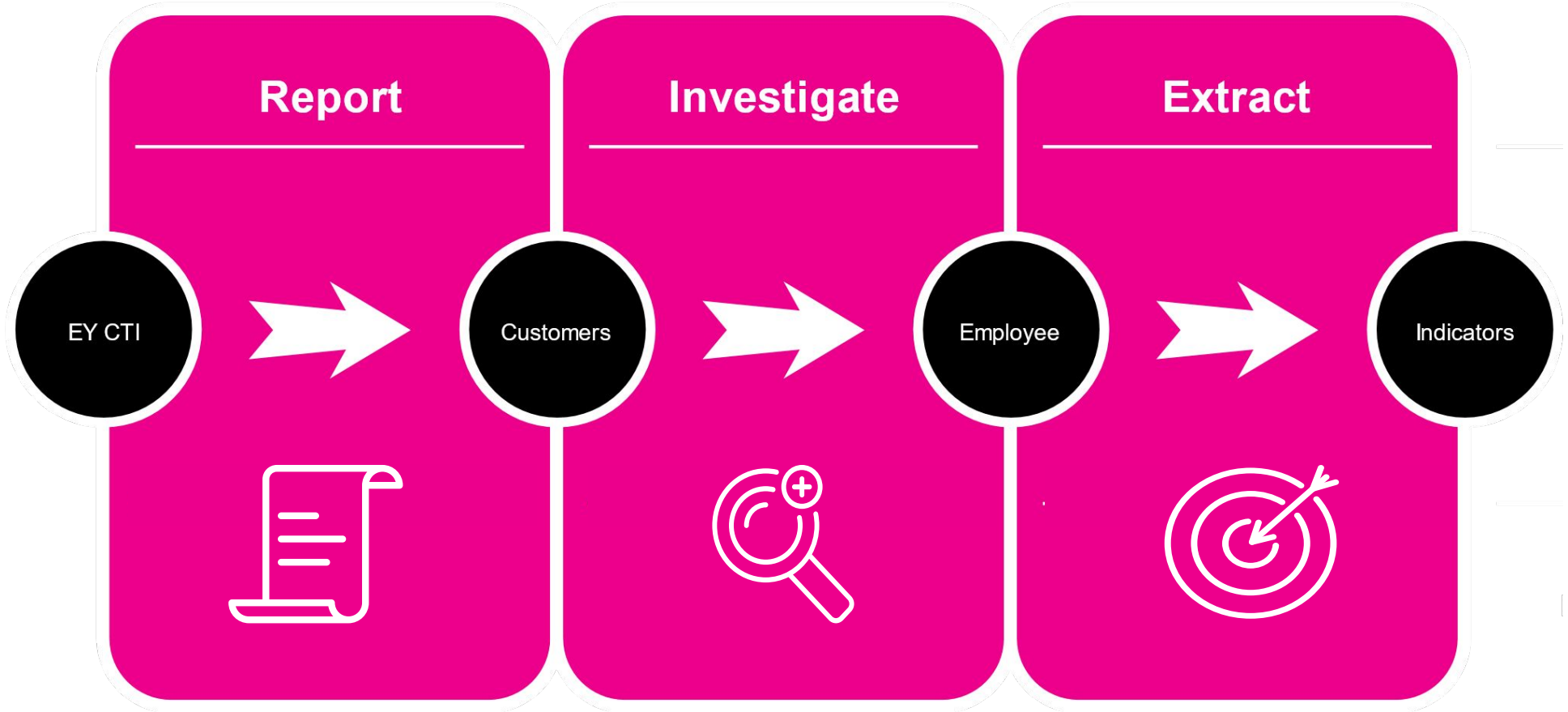
FA-19-0014 [redacted]

Research and analysis for this product was completed leveraging EY CTI sources and methods as well as open-source reporting and is current as of [redacted]. Feedback may be sent to cti@ey.com.

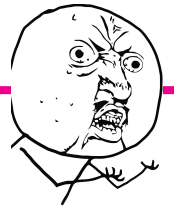
A person must manually extract the technical indicators to process them into their environment



A report goes out via Cyber Threat Intel

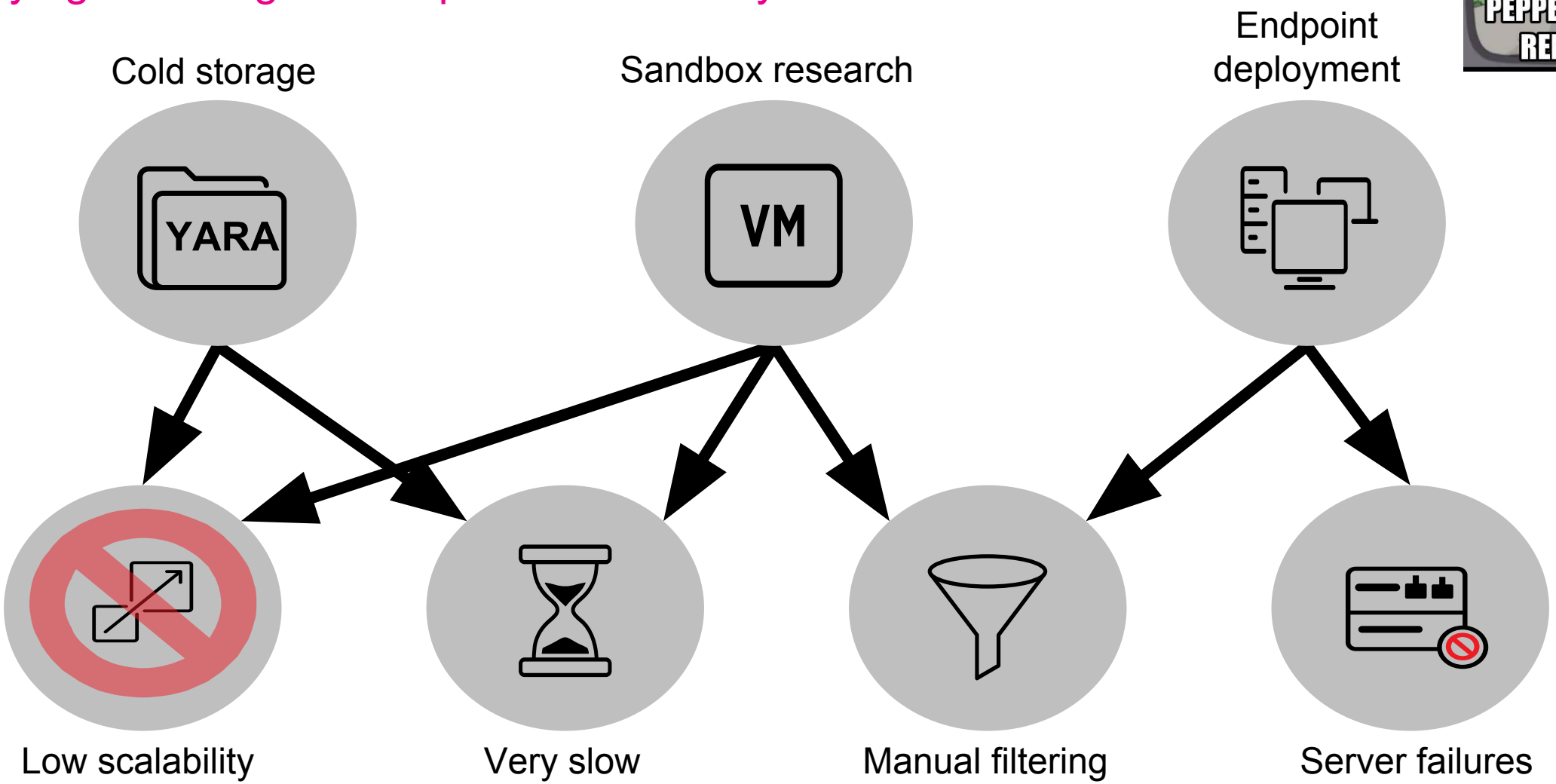


- A person must manually extract the technical indicators to process them into their environment



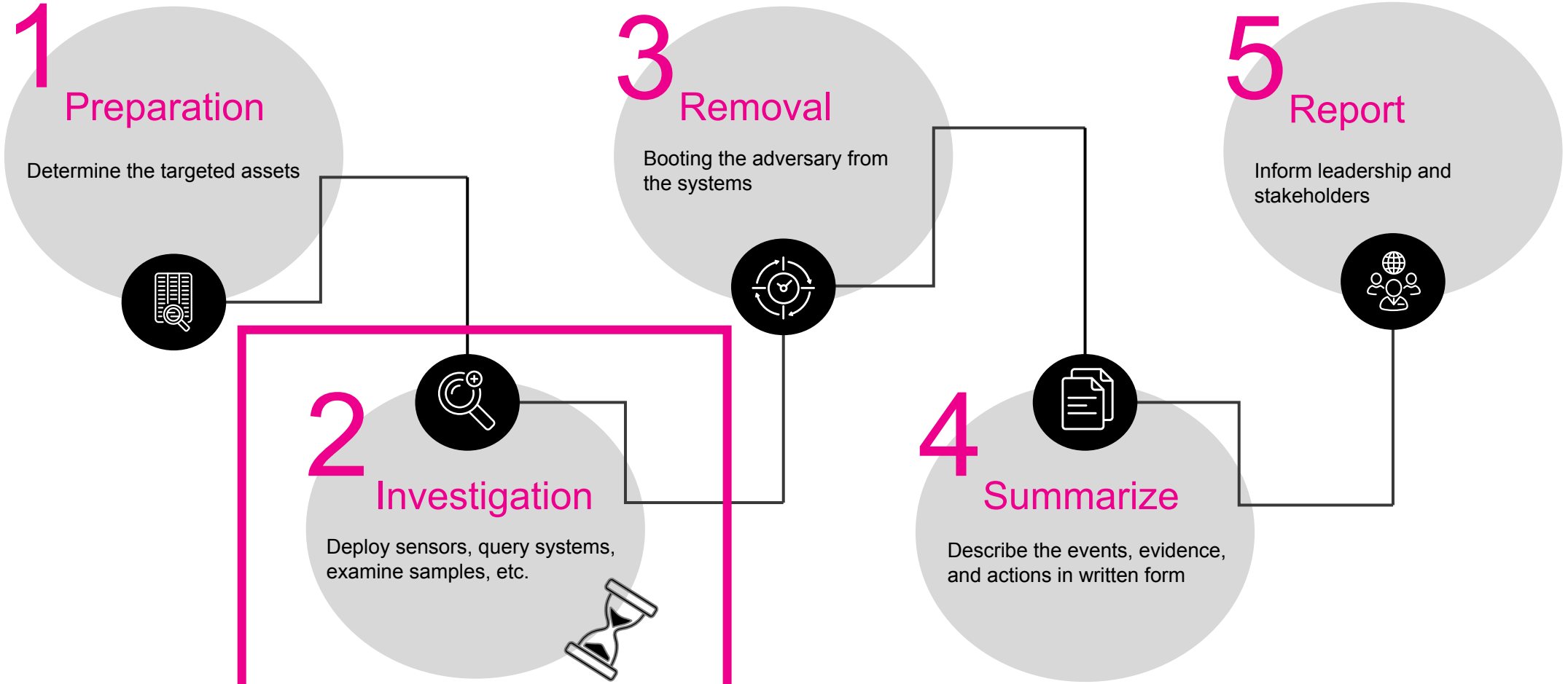
Ye Olde Days; Manual Hunting

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?"

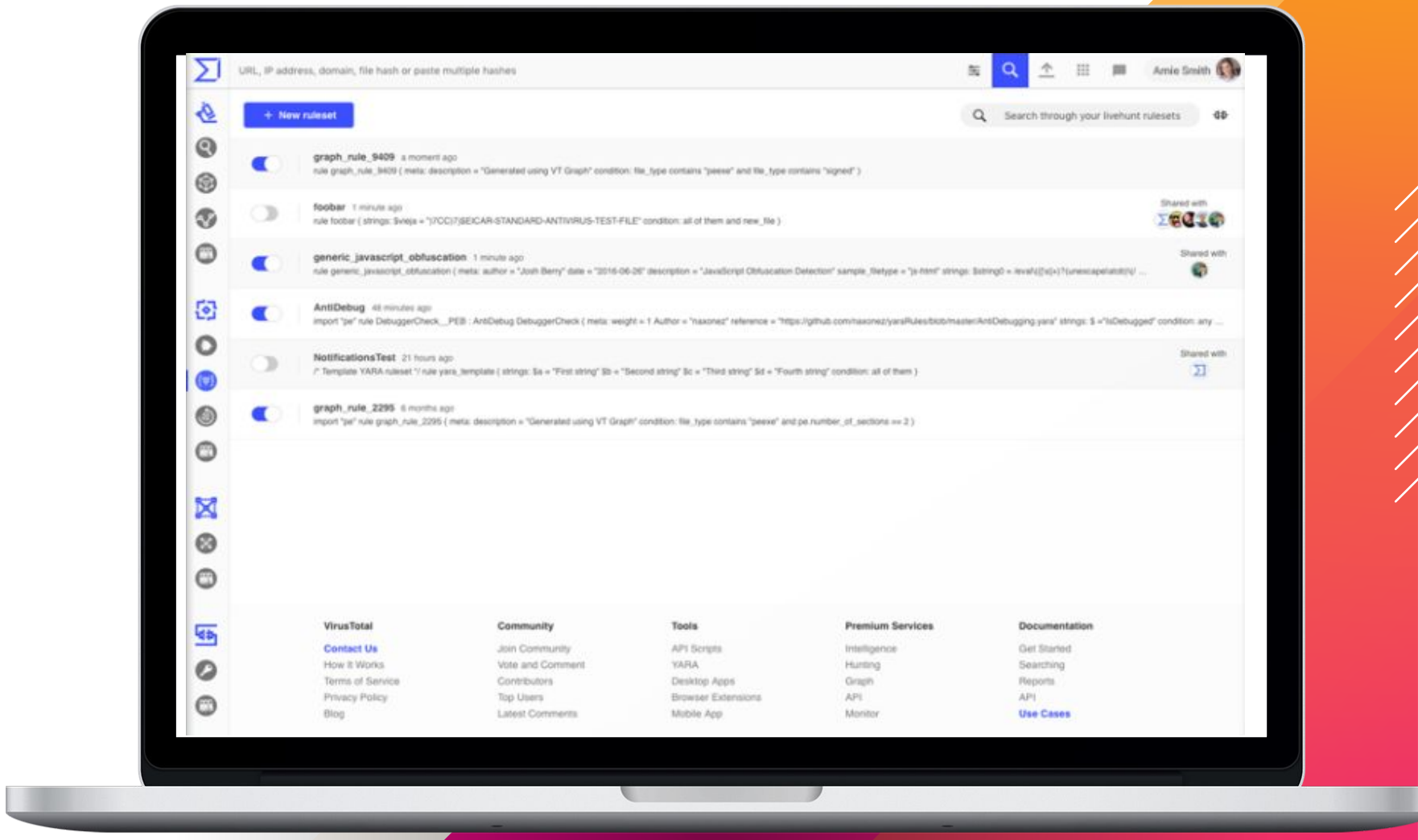
Automation. Powered by Splunk>Phantom

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).

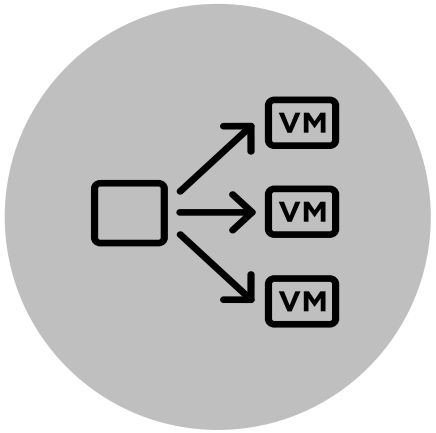
With this hunt you can do it internally and can gain visibility into your network.



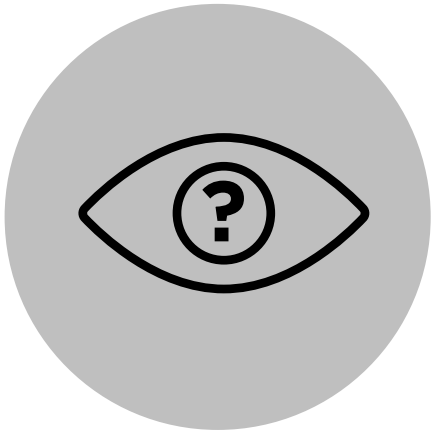
Playbook in Phantom

What does the hunt look like in Phantom?

Ingest CTI email and parse the YARA rule

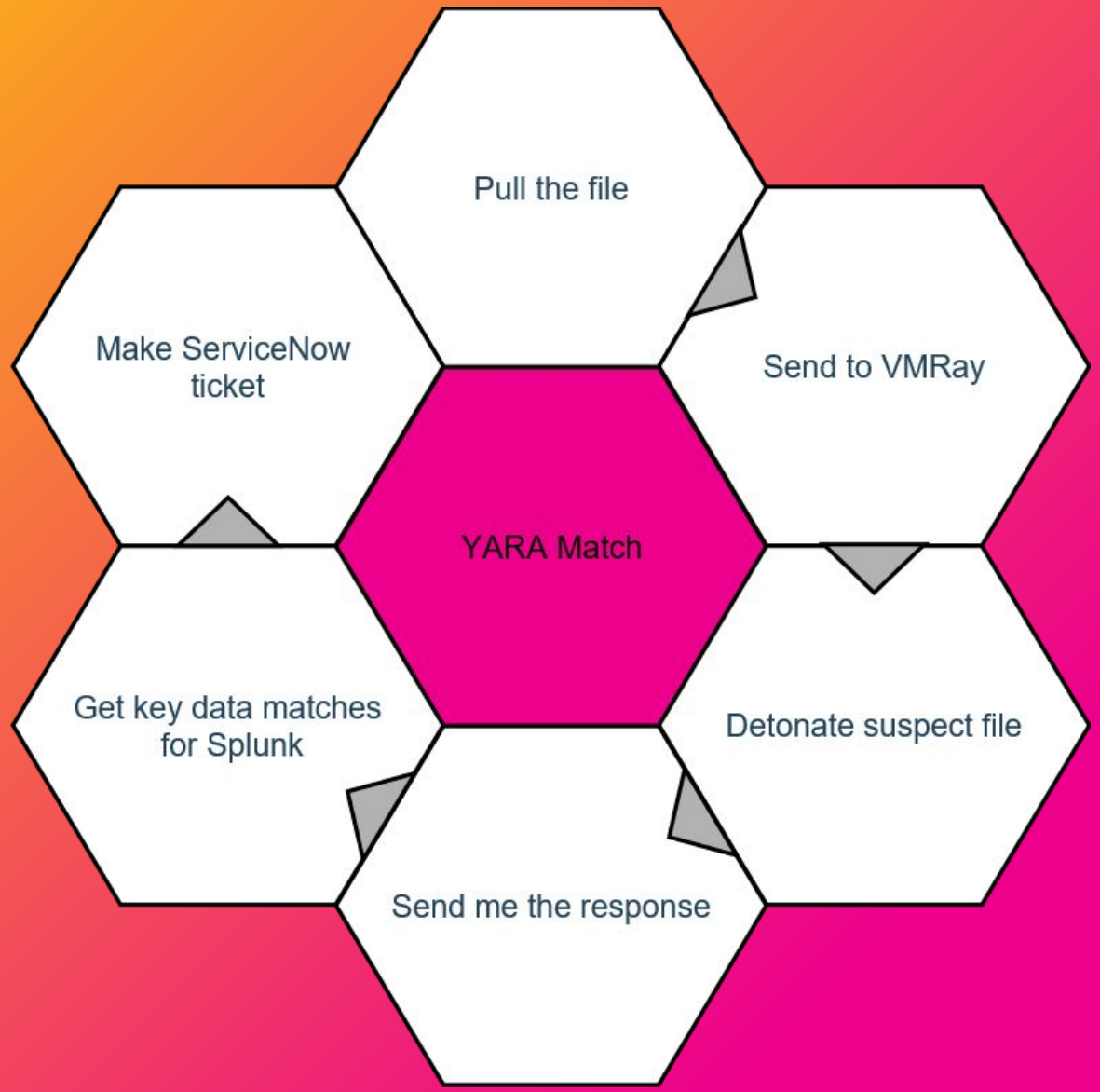


Push the YARA rule to Tanium, Carbon Black



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

If we found a match…



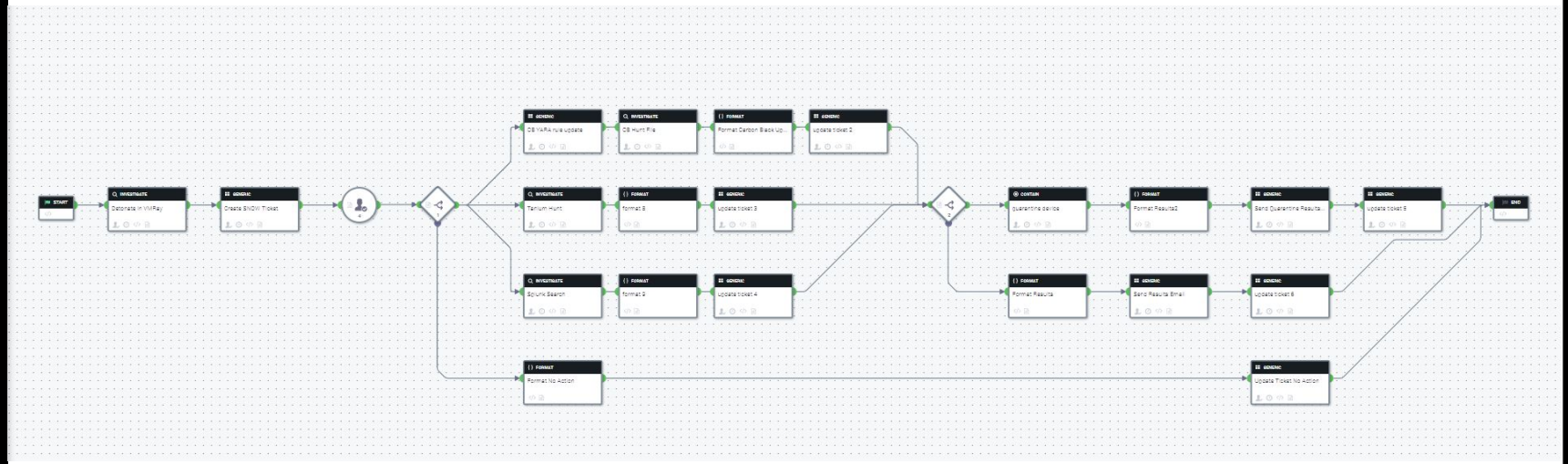
Playbook in Phantom

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)

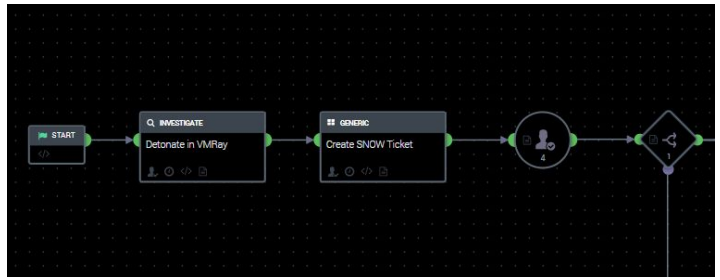


Breaking Down the Playbook

Visualizing how it all fits together

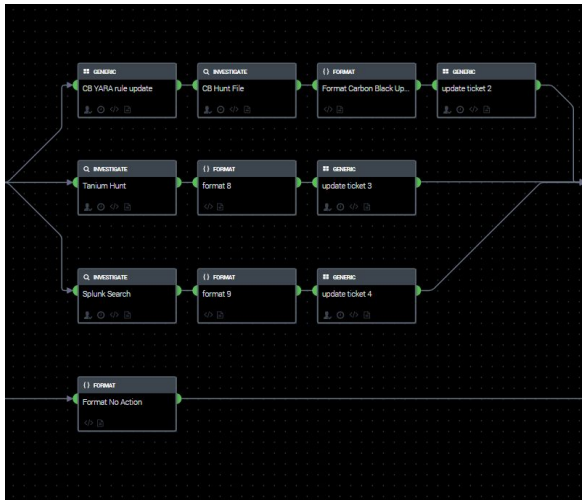
Response actions based on hunt

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



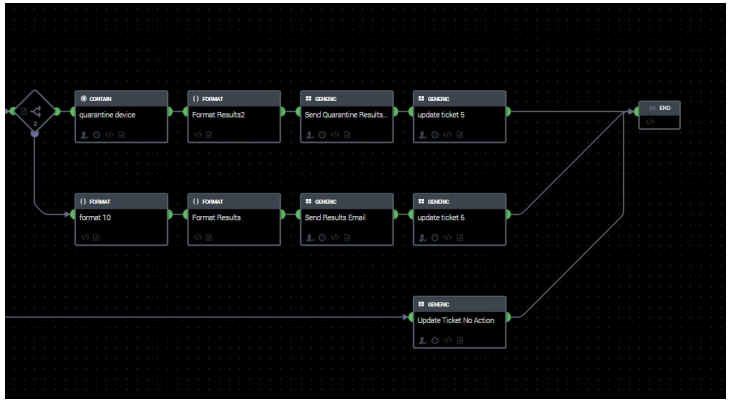
Hunt the network for signatures

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



Triage after initial receipt of Yara and malware samples via email

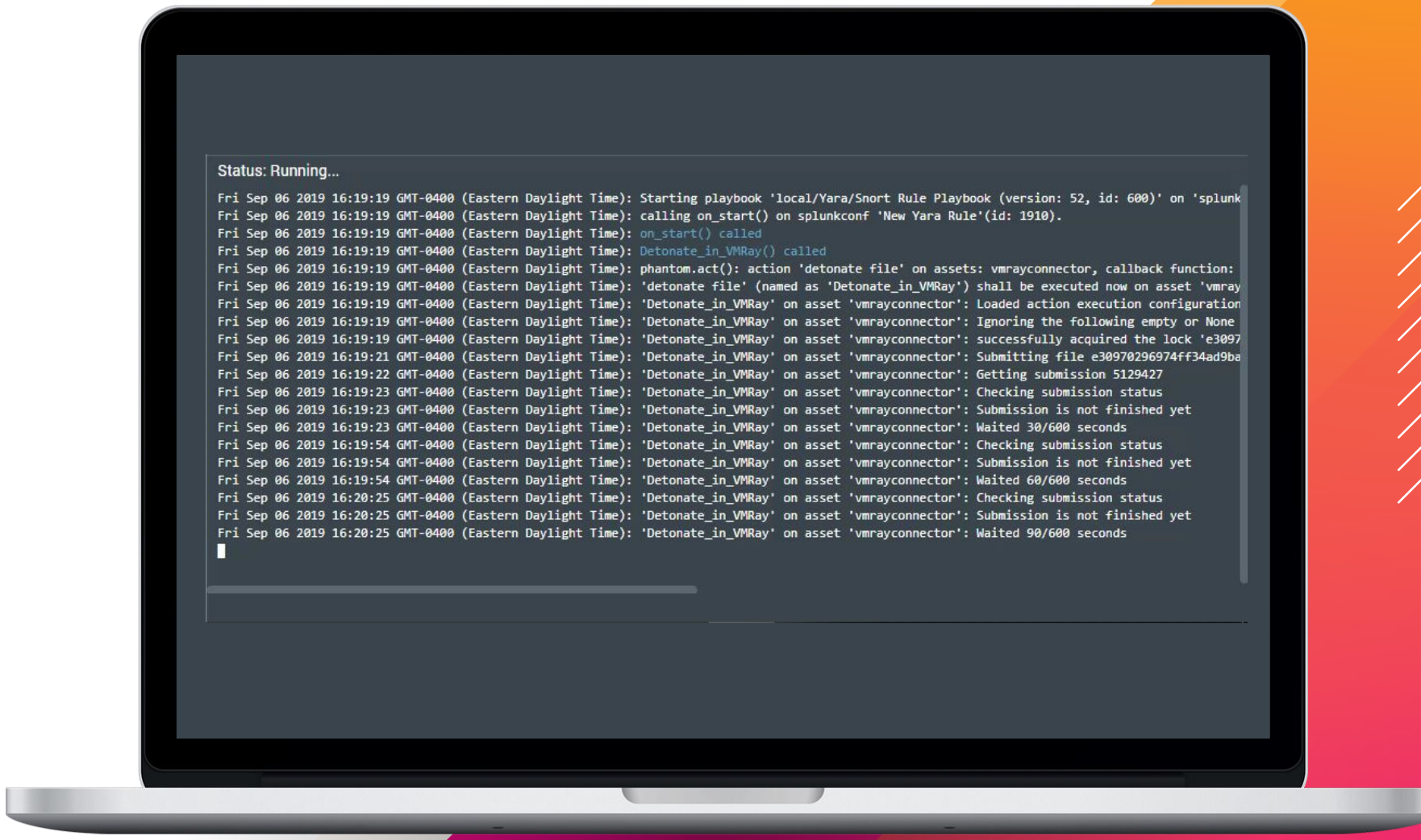
- Detonate sample to gain insights
- Present insights and ask analyst if hunt should continue

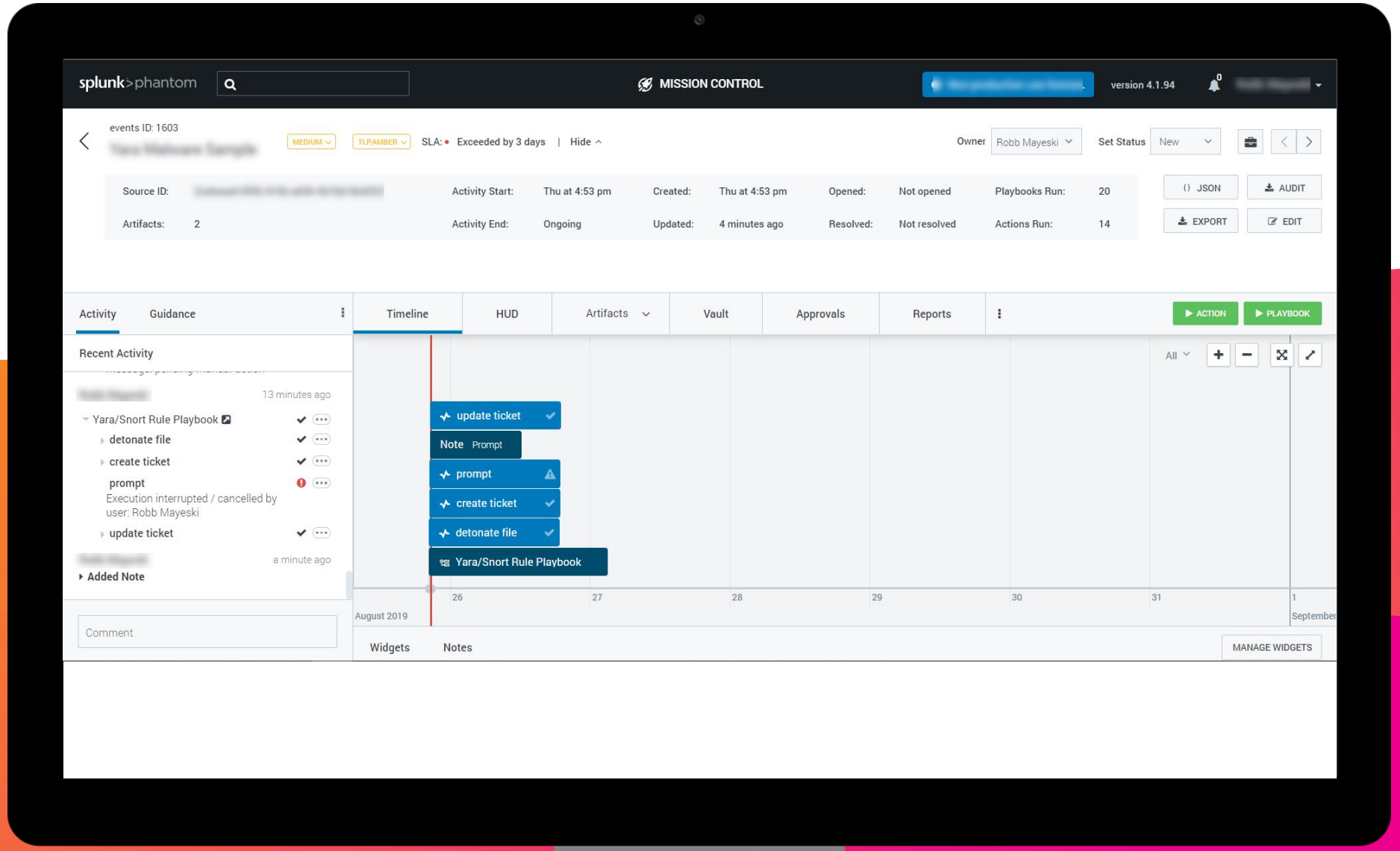


splunk> .conf19

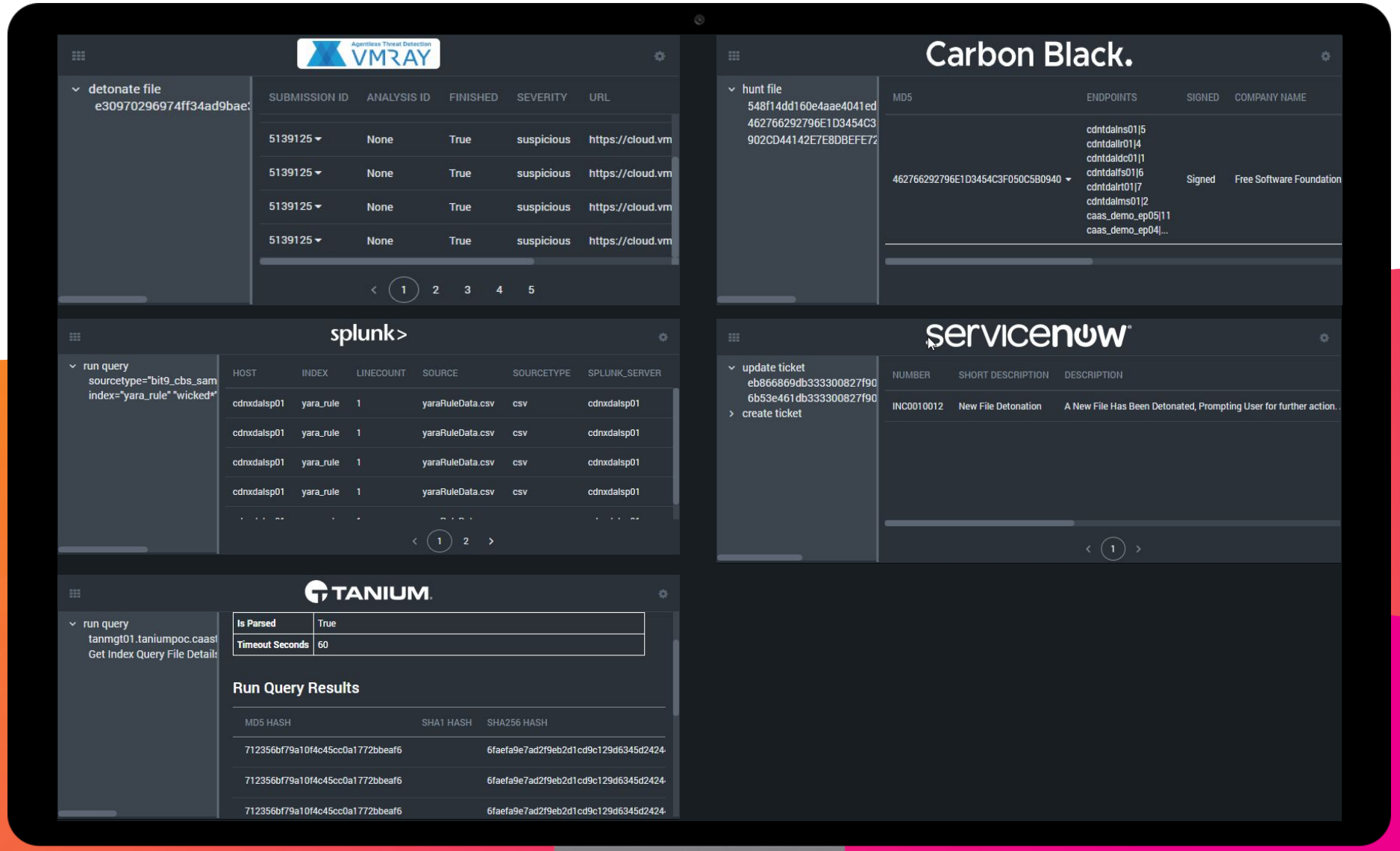
Actually automating the hunt

How the hunt actually executes in Phantom





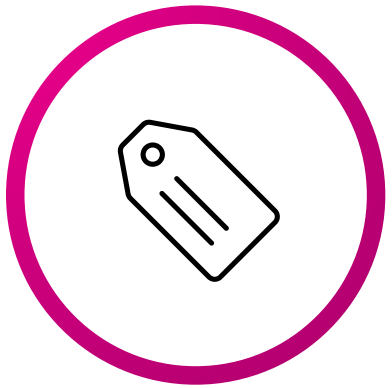
splunk> .conf19



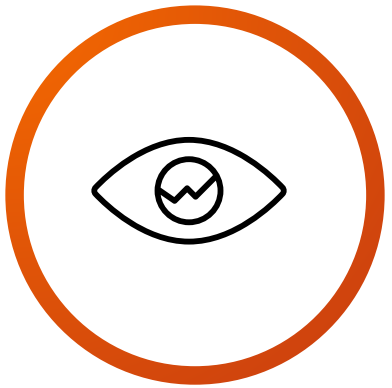
splunk> .conf19

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

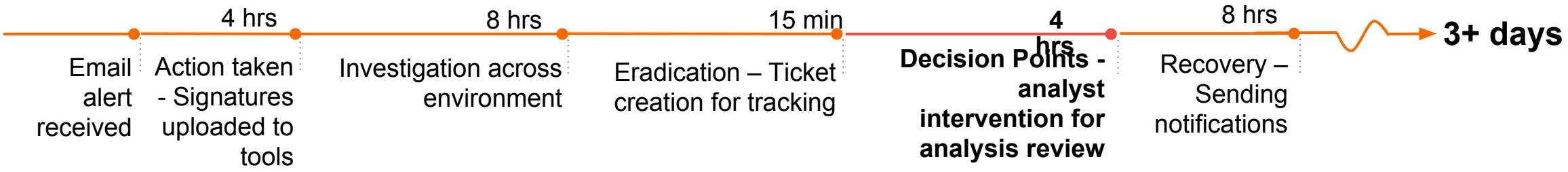
Specific tasks for the IR team to gather artifacts

What makes the Hunt "Scary Fast"

Phantom saves the day, at speed

splunk> .conf19

Manual... it's “scary slow!”



Exchange

TANIUM.

splunk>

servicenow

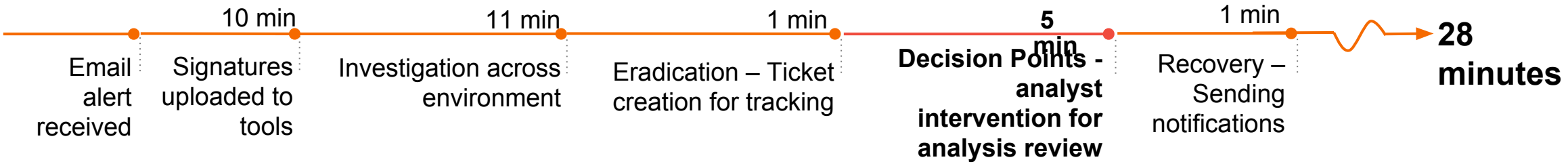
Agentless Threat Detection VMRAY

Carbon Black.

Phantom

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?”



Exchange

TANIUM.

splunk>

servicenow

Agentless Threat Detection VMRAY

Carbon Black.

Phantom

28 minutes with SOAR versus over a day without.

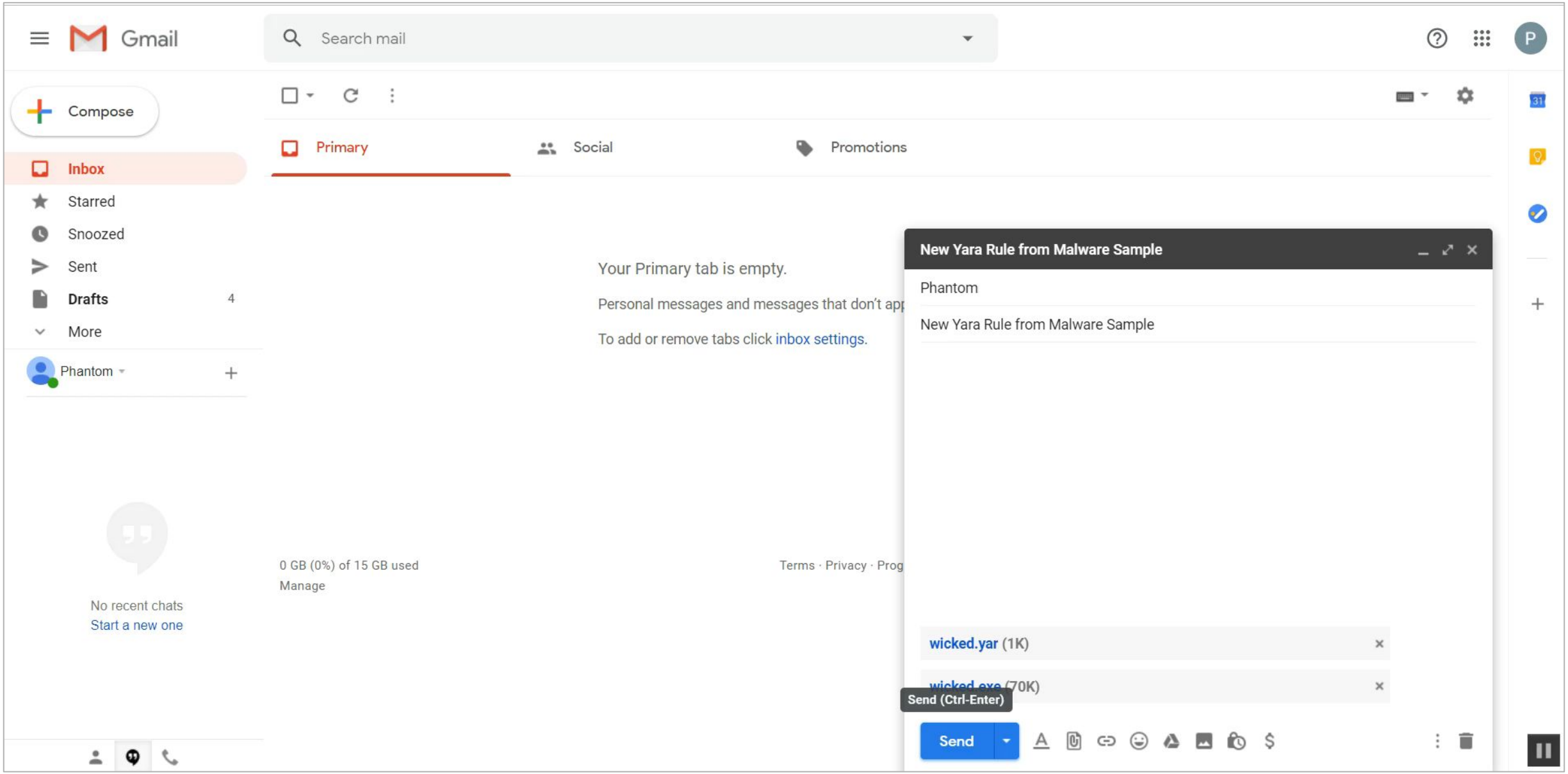
Key Takeaways

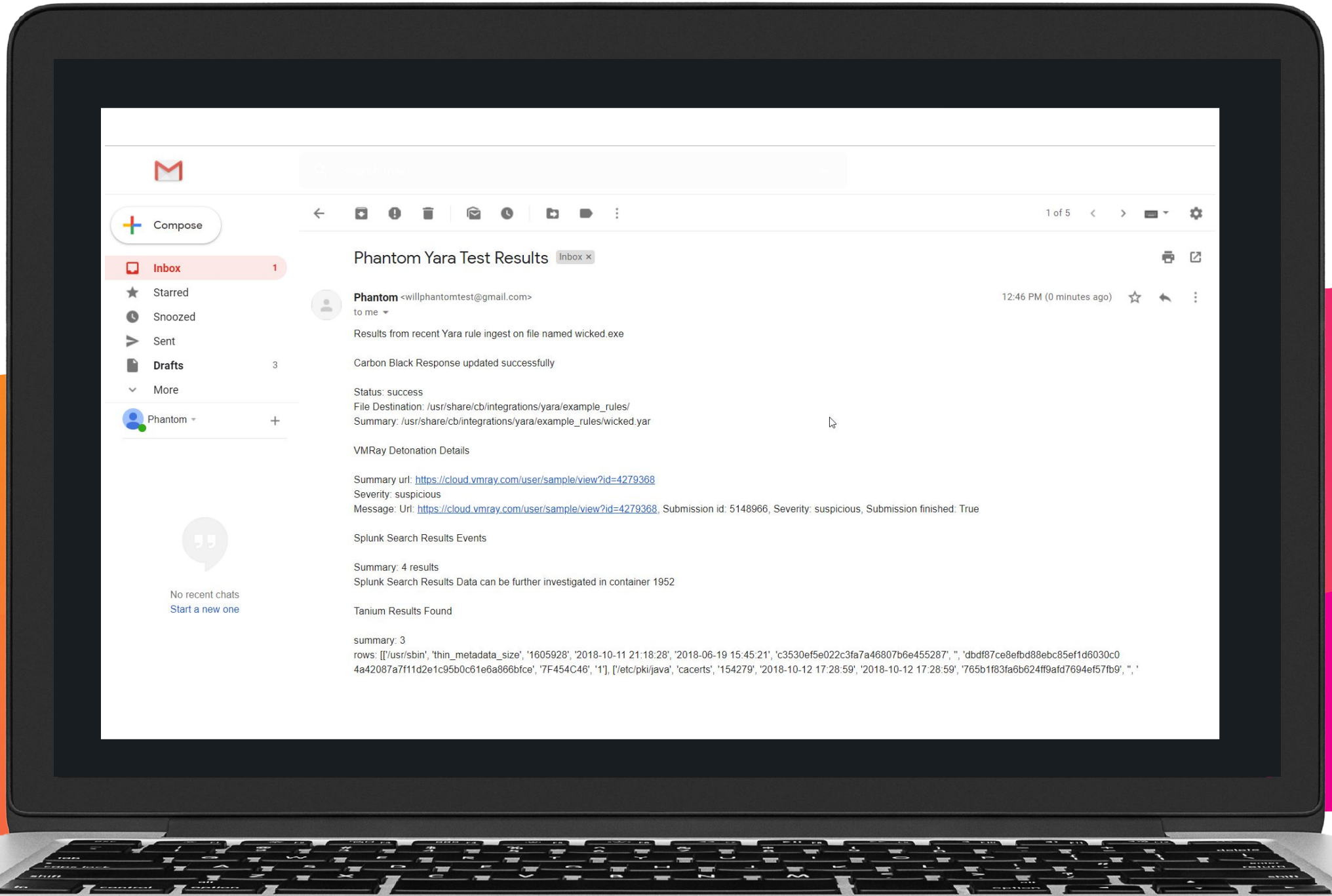
Orchestration for the win

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





Q&A

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

splunk> .conf19

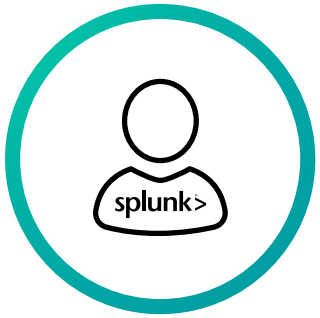
EY Team Credit

Development and Hunt Team at EY

Himanshu Anand

Mike Palitto

Ruchir Arya



Chris Jones

Will Burger

.conf19

splunk>

Thank You !

Go to the .conf19 mobile app to

RATE THIS SESSION