

From 30 Minutes To 40 Seconds: Applying Adaptive Response To Automate Human Event Triage With Splunk ES & Phantom

Oliver Friedrichs
CEO & Founder, Phantom

John Stoner
Security Strategist, Splunk

.conf2016

splunk >

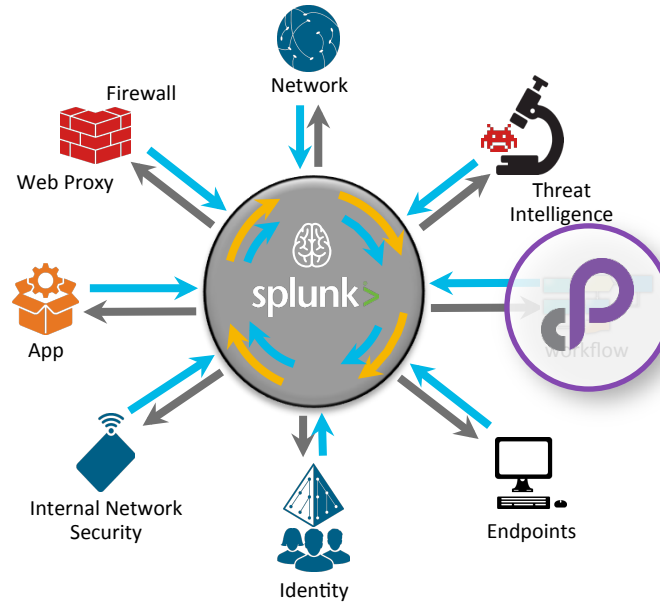
Disclaimer

During the course of this presentation, we may make forward looking statements regarding future events or the expected performance 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 could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC. 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, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make. 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 functionality described or to include any such feature or functionality in a future release.

Session Agenda

- Review of Adaptive Response
- Splunk/Phantom Key Concepts
- Demos: Splunk ES/Phantom
- Customer Case Studies

Adaptive Response Framework



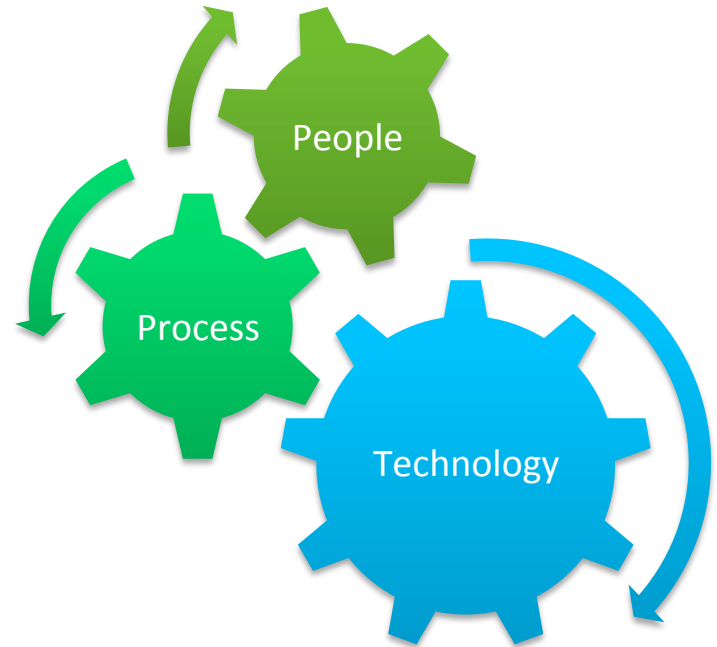
Why Security Orchestration Matters

- Market leading MSSP
- Home grown correlation engine - Our version of a SIEM
- Hundreds of customers
- Scalable process
- Custom tools for the analyst to make a decision
 - IP history across organization and business sector
 - Threat Intelligence Portal for global threat landscape reference
 - Ticketing system
 - Call tree to notify on alerts
 - Device uptime/outages for engineering
- Some events could be auto-commented and handled
 - Which events?
 - How would they be handled?
- But does one size fit all?

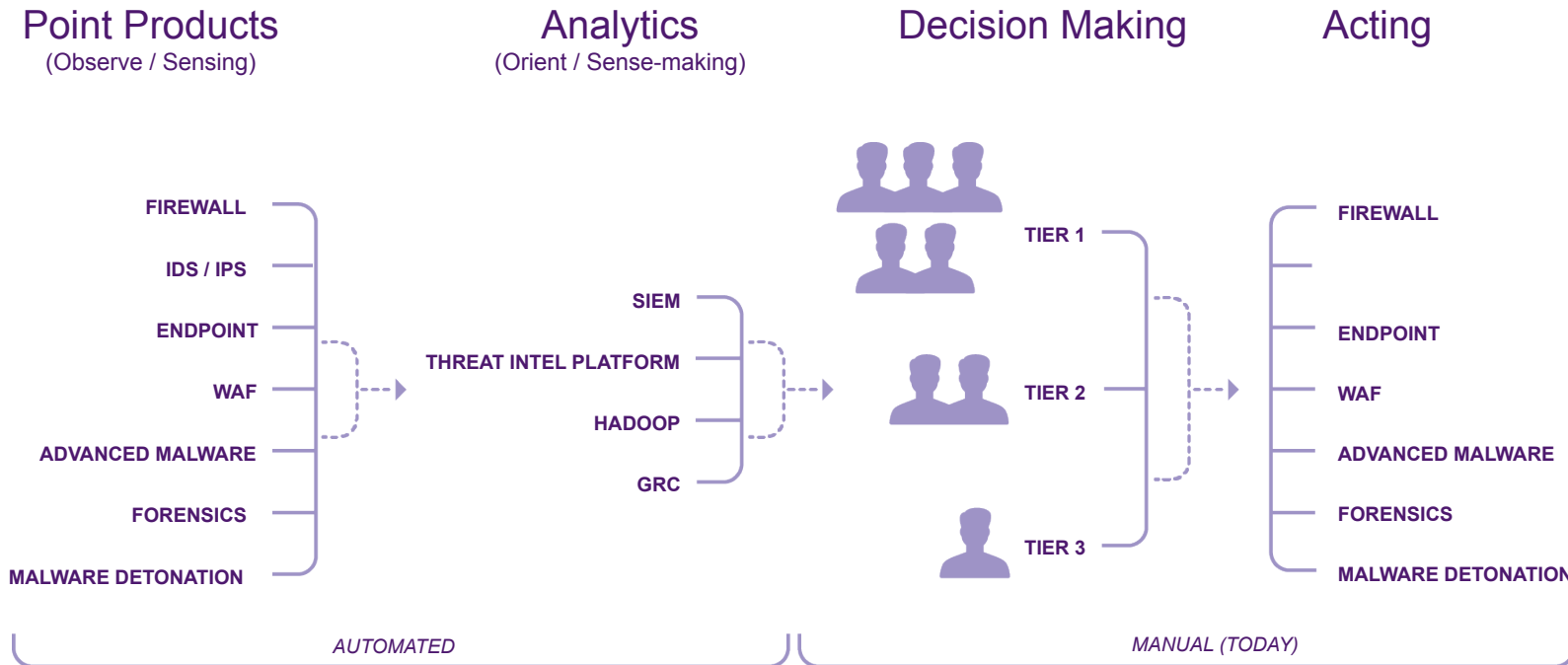


Fast Forward 10 Years Or So....

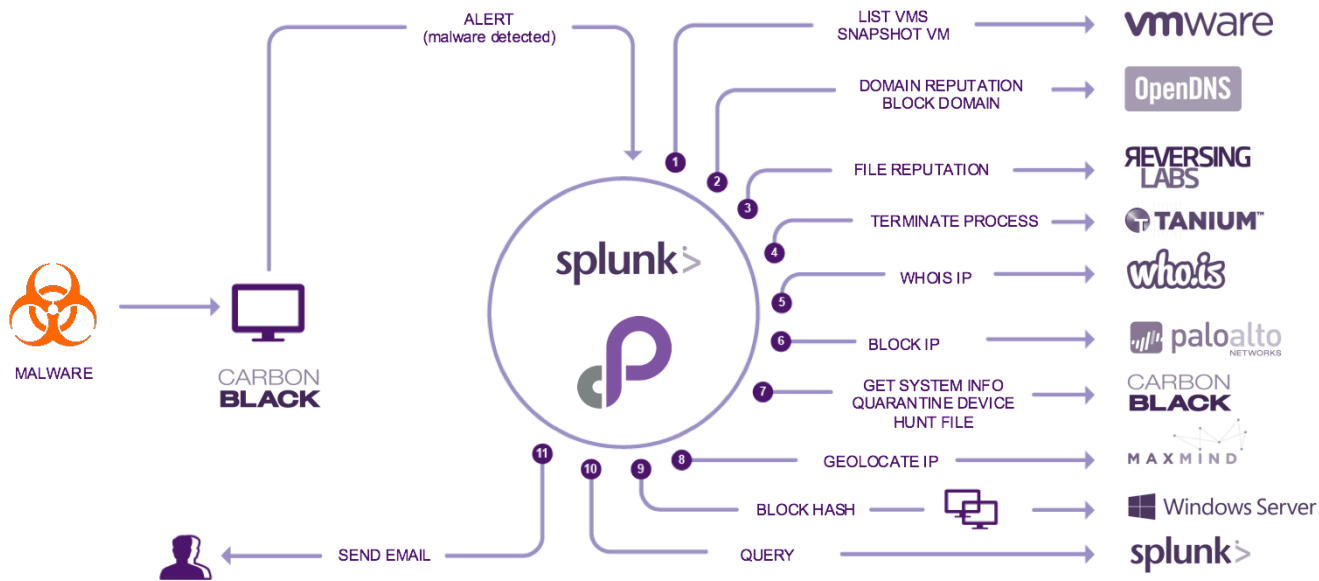
- Continual, pervasive attacks
- Not dealing with a single attack where the firewall and the IDS see the attack and dutifully return an alert
- Attacks can occur from anywhere and can be asynchronous
- Need to detect and contain is critical until eradication and remediation can take place
- Limited pool of security talent
- Limitless attack surface
- Time to detect is too long
- Costs continue to increase
- Security product sprawl
- How do we handle large amounts of attacks in a scalable, repeatable manner?



Automating Security Operations



Phantom & Adaptive Response Initiative



Incident Review – Analyst Queue

splunk App: Enterprise Security John Stoner Messages Settings Activity Help Find

Security Posture Incident Review My Investigations Advanced Threat Security Domains Audit Search Configure Enterprise Security

Incident Review

Urgency

- CRITICAL 0
- HIGH 4
- MEDIUM 39
- LOW 0
- INFO 0

Status **Name**

Owner **Search**

Security Domain **Time**

Tag

✓ 43 events (8/14/16 3:00:00.000 PM to 8/15/16 3:16:32.000 PM) Job ▾ || Smart Mode ▾

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect 1 hour per column

Edit Selected | Edit All 43 Matching Events | Add Selected to Investigation ◀ prev 1 2 3 next ▶

<input type="checkbox"/>	Time	Security Domain	Title	Urgency	Status	Action	Owner	Actions
> <input type="checkbox"/>	8/15/16 6:47:22.000 AM	Endpoint	Host With Old Infection Or Potential Re-infection (unknown On 10.11.36.36)	High	New		unassigned	▾
> <input type="checkbox"/>	8/15/16 6:02:50.000 AM	Endpoint	High Or Critical Priority Host With Malware Detected	High	New		unassigned	▾
> <input type="checkbox"/>	8/15/16 2:47:18.000 AM	Endpoint	Host With A Recurring Malware Infection (unknown On 10.11.36.36)	High	New		unassigned	▾
> <input type="checkbox"/>	8/14/16 9:55:29.000 PM	Endpoint	Host Sending Excessive Email (10.11.36.36)	High	New		unassigned	▾
> <input type="checkbox"/>	8/15/16 2:17:20.000 PM	Network	DNS Logs - Unusal Outbound Activity	Medium	New		unassigned	▾
> <input type="checkbox"/>	8/15/16 2:02:39.000 PM	Network	DNS Logs - Unusal Outbound Activity	Medium	New		unassigned	▾
> <input type="checkbox"/>	8/15/16 1:47:25.000 PM	Network	DNS Logs - Unusal Outbound Activity	Medium	New		unassigned	▾
> <input type="checkbox"/>	8/15/16 12:02:47.000 PM	Network	DNS Logs - Unusal Outbound Activity	Medium	New		unassigned	▾
> <input type="checkbox"/>	8/15/16 10:02:41.000 AM	Network	DNS Logs - Unusal Outbound Activity	Medium	New		unassigned	▾
> <input type="checkbox"/>	8/15/16 8:01:33.000 AM	Network	DNS Logs - Unusal Outbound Activity	Medium	New		unassigned	▾
> <input type="checkbox"/>	8/15/16 8:01:33.000 AM	Network	DNS Logs - Unusal Outbound Activity	Medium	New		unassigned	▾
> <input type="checkbox"/>	8/15/16 7:32:24.000 AM	Network	DNS Logs - Unusal Outbound Activity	Medium	New		unassigned	▾
> <input type="checkbox"/>	8/15/16 7:17:28.000 AM	Network	DNS Logs - Unusal Outbound Activity	Medium	New		unassigned	▾

Chris Moreno : Malware Infection 🔍 📄 ⌚

Notable Events and Field Actions

Edit Selected | Edit All 43 Matching Events | Add Selected to Investigation ◀ prev 1 2 3 next ▶

i	Time	Security Domain	Title	Urgency	Status	Action	Owner	Actions
>	8/15/16 6:47:22.000 AM	Endpoint	Host With Old Infection Or Potential Re-infection (unknown On 10.11.36.36)	High	New		unassigned	▼
>	8/15/16 6:02:50.000 AM	Endpoint	High Or Critical Priority Host With Malware Detected	High	New		unassigned	▼
>	8/15/16 2:47:18.000 AM	Endpoint	Host With A Recurring Malware Infection (unknown On 10.11.36.36)	High	New		unassigned	▼
✓	8/14/16 9:55:29.000 PM	Endpoint	Host Sending Excessive Email (10.11.36.36)	High	New		unassigned	▼

Description:
The device 10.11.36.36 was detected making 10 SMTP connections to 10 destinations.

Additional Fields

Value
Source: 10.11.36.36 8820
Source Business Unit: americas
Source City: Washington D.C.
Source Country: USA
Source Expected: false
Source Latitude: 38.959405
Source Longitude: -77.04
Source PCI Domain: untrust
Source Requires Antivirus: false
Source Should Time Synchronize: true
Source Should Update: true

Event Details:

event_id	142F7578-8E84-4A8E-A1B4-1B54FACDC06B@@notable
event_hash	02f3a478dbb0353ca5434f954496a1f7
eventtype	modnotable_results
	notable

Action

- Google 10.11.36.36
- Intrusion Search (as destination)
- Intrusion Search (as source)
- Notable Event Search
- Malware Search
- Nbtstat 10.11.36.36
- Nslookup 10.11.36.36
- Ping 10.11.36.36
- Stream Capture
- Traffic Search (as destination)

Correlation Search:
[Endpoint - Host Sending Excessive Email - Rule](#)

History:
[View all review activity for this Notable Event](#)

Contributing Events:
[View email-related traffic for source 10.11.36.36 for this event](#)

Notable Event Actions

Edit Selected | Edit All 43 Matching Events | Add Selected to Investigation

« prev 1 2 3 next »

<input type="checkbox"/>	Time	Security Domain	Title	Urgency	Status	Action	Owner	Actions
> <input type="checkbox"/>	8/15/16 6:47:22.000 AM	Endpoint	Host With Old Infection Or Potential Re-infection (unknown On 10.11.36.36)	High	New		unassigned	▼
> <input type="checkbox"/>	8/15/16 6:02:50.000 AM	Endpoint	High Or Critical Priority Host With Malware Detected	High	New		unassigned	▼
> <input type="checkbox"/>	8/15/16 2:47:18.000 AM	Endpoint	Host With A Recurring Malware Infection (unknown On 10.11.36.36)	High	New		unassigned	▼
▼ <input type="checkbox"/>	8/14/16 9:55:29.000 PM	Endpoint	Host Sending Excessive Email (10.11.36.36)	High	New		unassigned	▼

Description:
The device 10.11.36.36 was detected making 10 SMTP connections to 10 destinations.

Additional Fields	Value	Action
Source	10.11.36.36 8820	▼
Source Business Unit	americas	▼
Source City	Washington D.C.	▼
Source Country	USA	▼
Source Expected	false	▼
Source Latitude	38.959405	▼
Source Longitude	-77.04	▼
Source PCI Domain	untrust	▼
Source Requires Antivirus	false	▼
Source Should Time Synchronize	true	▼
Source Should Update	true	▼

Event Details:

event_id	142F7578-8E84-4A8E-A1B4-1B54FACDC06B@@@notable@@@02f3a478dbb0353ca5434f954496a1f7	▼
event_hash	02f3a478dbb0353ca5434f954496a1f7	▼
eventtype	modnotable_results	▼
notable		▼

Correlation Search:
[Endpoint - Host Sending Excessive Email - Rule](#)

History:
[View all review activity for this Notable Event](#)

Contributing Events:
[View email-related traffic for source 10.11.36.36 for this event](#)

- Add Event to Investigation
- Create notable event
- Build Event Type
- Extract Fields
- Share Notable Event
- Suppress Notable Events
- View ModAction Invocations
- View ModAction Results
- Show Source

Event Actions At Search

The screenshot shows the Splunk Enterprise Security interface. At the top, the navigation bar includes 'App: Enterprise Security', user 'John Stoner', and various menu items like 'Messages', 'Settings', 'Activity', 'Help', and 'Find'. Below this is a search bar with the query: ``datamodel("Intrusion_Detection","IDS_Attacks") | search (IDS_Attacks.dest="10.11.36.36" OR IDS_Attacks.src="10.11.36.36")`. The search results show 6 events. A visualization of these events is shown as a timeline with green bars. Below the timeline, a table of event actions is displayed.

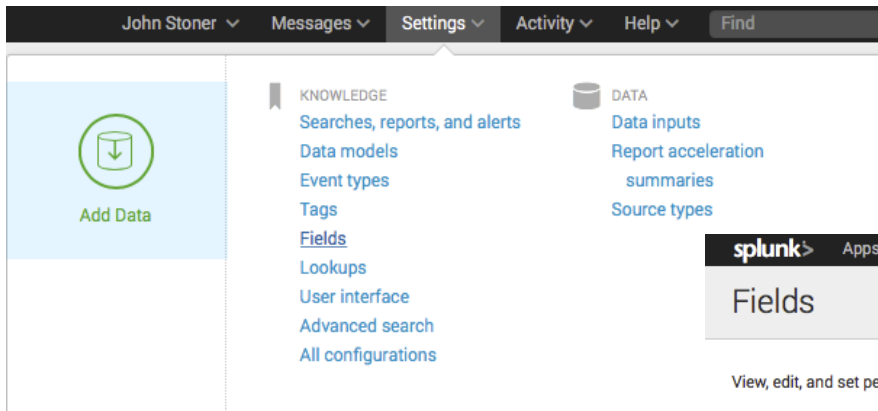
Event Actions	Value	Actions
Add Event to Investigation	127.0.0.1	▼
Create notable event	sample:juniper_idp_vuln_events	▼
Build Event Type	juniper:idp	▼
Extract Fields	unknown	▼
Show Source	Predefined	▼
<input type="checkbox"/> IDS_Attacks.dest	10.11.36.36	▼
<input type="checkbox"/> IDS_Attacks.dest_bunit	americas	▼
<input type="checkbox"/> IDS_Attacks.dest_priority	high	▼
<input type="checkbox"/> IDS_Attacks.dvc	192.168.1.130	▼
<input type="checkbox"/> IDS_Attacks.dvc_bunit	americas	▼
<input type="checkbox"/> IDS_Attacks.dvc_category	iso27002	▼
<input type="checkbox"/> IDS_Attacks.dvc_priority	high	▼
<input type="checkbox"/> IDS_Attacks.ids_type	network	▼

Field Actions At Search

The screenshot shows the Splunk Enterprise Security interface. At the top, there's a navigation bar with 'App: Enterprise Security' and user 'John Stoner'. Below that, a 'New Search' bar contains the query: `'datamodel("Intrusion_Detection", "IDS_Attractions")' | search (IDS_Attractions.dest="10.11.36.36" OR IDS_Attractions.src="10.11.36.36")`. The search results show 6 events. A timeline visualization is visible above a table of events. The table has columns for 'Time' and 'Event'. One event is expanded, showing a detailed view of an intrusion detection event. A context menu is open over the 'IDS_Attractions.dest' field, which has the value '10.11.36.36'. The menu includes options like 'Edit Tags', 'Access Search (as destination)', 'Access Search (as source)', 'Asset Center', 'Asset Investigator', 'Domain Dossier', 'Map 10.11.36.36', 'Google 10.11.36.36', 'Intrusion Search (as destination)', and 'Intrusion Search (as source)'. The table below the event details shows various fields and their values, such as 'host' (127.0.0.1), 'source' (sample.juniper_idp_vuln_events), and 'IDS_Attractions.dest' (10.11.36.36).

Type	Field	Value
Selected	host	127.0.0.1
	source	sample.juniper_idp_vuln_events
	sourcetype	juniperidp
Event	IDS_Attractions.action	unknown
	IDS_Attractions.category	Predefined
	IDS_Attractions.dest	10.11.36.36
	IDS_Attractions.dest_bunit	americas
	IDS_Attractions.dest_priority	high
	IDS_Attractions.dvc	192.168.1.130
	IDS_Attractions.dvc_bunit	americas
	IDS_Attractions.dvc_category	iso27002
	IDS_Attractions.dvc_priority	high
	IDS_Attractions.ids_type	network

Workflow Actions



splunk> Apps ▾

Fields

View, edit, and set permissions on field extractions. Define event workflow actions and field aliases. Rename sourcetypes.

Type

Field aliases
Edit or add one or more aliases to field names

Calculated fields
Edit or add one or more calculated fields

Field extractions
View and edit all field extractions. Add new field extractions and update permissions.

Field transformations
Edit or add transformations for field extractions that use a transform.

Sourcetype renaming
Rename a source type. Multiple source types can share the same name.

Workflow actions
Edit or add workflow actions

Google

Fields » Workflow actions » Google

You do not have permissions to edit this configuration.

Google 10.11.36.36

Intrusion Search (as destination)

Intrusion Search (as source)

Notable Event Search

Malware Search

Nbtstat 10.11.36.36

Nslookup 10.11.36.36

Ping 10.11.36.36

Stream Capture

Traffic Search (as destination)

Label *

Enter the label that appears for this action. Optionally, incorporate a field's value by enclosing the field name in dollar signs, e.g. 'Search for ticket number : \$ticketnum\$'.

Apply only to the following fields

Specify a comma-separated list of fields that must be present in an event for the workflow action to apply to it. When fields are specified, the workflow action only appears in the field menus for those fields; otherwise it appears in all field menus.

Apply only to the following event types

Specify a comma-separated list of event types that an event must be associated with for the workflow action to apply to it.

Show action in

Action type *

Link configuration

URI *

Enter the location to link to. Optionally, specify fields by enclosing the field name in dollar signs, e.g. `http://www.google.com/search?q=$host$`.

Open link in

Link method

ids_search_dest_as_dest

[Fields](#) » [Workflow actions](#) » ids_search_dest_as_dest**You do not have permissions to edit this configuration.**

Google 10.11.36.36

Intrusion Search (as destination)

Intrusion Search (as source)

Notable Event Search

Malware Search

Nbtstat 10.11.36.36

Nslookup 10.11.36.36

Ping 10.11.36.36

Stream Capture

Traffic Search (as destination)

Label *

Enter the label that appears for this action. Optionally, incorporate a field's value by enclosing the field name in dollar signs, e.g. 'Search for ticket number : \$ticketnum\$'.

Apply only to the following fields

Specify a comma-separated list of fields that must be present in an event for the workflow action to apply to it. When fields are specified, the workflow action only appears in the field menus for those fields; otherwise it appears in all field menus.

Apply only to the following event types

Specify a comma-separated list of event types that an event must be associated with for the workflow action to apply to it.

Show action in

Action type *

Link configuration

URI *

Enter the location to link to. Optionally, specify fields by enclosing the field name in dollar signs, e.g. [http://www.google.com/search?q=\\$host\\$](http://www.google.com/search?q=$host$).

Open link in

Link method

nslookup_dest

Fields » Workflow actions » nslookup_dest

You do not have permissions to edit this configuration.

Google 10.11.36.36

Intrusion Search (as destination)

Intrusion Search (as source)

Notable Event Search

Malware Search

Nbtstat 10.11.36.36

Nslookup 10.11.36.36

Ping 10.11.36.36

Stream Capture

Traffic Search (as destination)

Label *

Enter the label that appears for this action. Optionally, incorporate a field's value by enclosing the field name in dollar signs, e.g. 'Search for ticket number : \$ticketnum\$'.

Apply only to the following fields

Specify a comma-separated list of fields that must be present in an event for the workflow action to apply to it. When fields are specified, the workflow action only appears in the field menus for those fields; otherwise it appears in all field menus.

Apply only to the following event types

Specify a comma-separated list of event types that an event must be associated with for the workflow action to apply to it.

Show action in

Action type *

Link configuration

URI *

Enter the location to link to. Optionally, specify fields by enclosing the field name in dollar signs, e.g. `http://www.google.com/search?q=$host$`.

Open link in

Link method

stream_dest

Fields » Workflow actions » stream_dest

You do not have permissions to edit this configuration.

Label *

Enter the label that appears for this action. Optionally, incorporate a field's value by enclosing the field name in dollar signs, e.g. 'Search for ticket number : \$ticketnum\$'.

Apply only to the following fields

Specify a comma-separated list of fields that must be present in an event for the workflow action to apply to it. When fields are specified, the workflow action only appears in the field menus for those fields; otherwise it appears in all field menus.

Apply only to the following event types

Specify a comma-separated list of event types that an event must be associated with for the workflow action to apply to it.

Show action in

Action type *

Link configuration

URI *

Enter the location to link to. Optionally, specify fields by enclosing the field name in dollar signs, e.g. `http://www.google.com/search?q=$host$`.

Open link in

Link method

Google 10.11.36.36

Intrusion Search (as destination)

Intrusion Search (as source)

Notable Event Search

Malware Search

Nbtstat 10.11.36.36

Nslookup 10.11.36.36

Ping 10.11.36.36

Stream Capture

Traffic Search (as destination)

Correlation Search Actions

Correlation Search

Search Name*

Application Context

Description

Describes what kind of issues this search is intended to detect

Search*

```
| datamodel "Authentication" "Failed_Authentication" search | stats values(Authentication.tag) as "tag",dc(Authentication.user) as "user_count",dc(Authentication.dest) as "dest_count",count by "Authentication.app","Authentication.src" | rename "Authentication.app" as "app","Authentication.src" as "src" | where 'count'>=6 | eval tag=mvjoin(tag,"|") | rename "tag" as "orig_tag"
```

[Edit search in guided mode](#)

[Edit search manually](#)

Actions

Include in RSS feed

Send email

Run a script

File name of the shell script to run

Splunk runs the script from \$SPLUNK_HOME/bin/scripts/

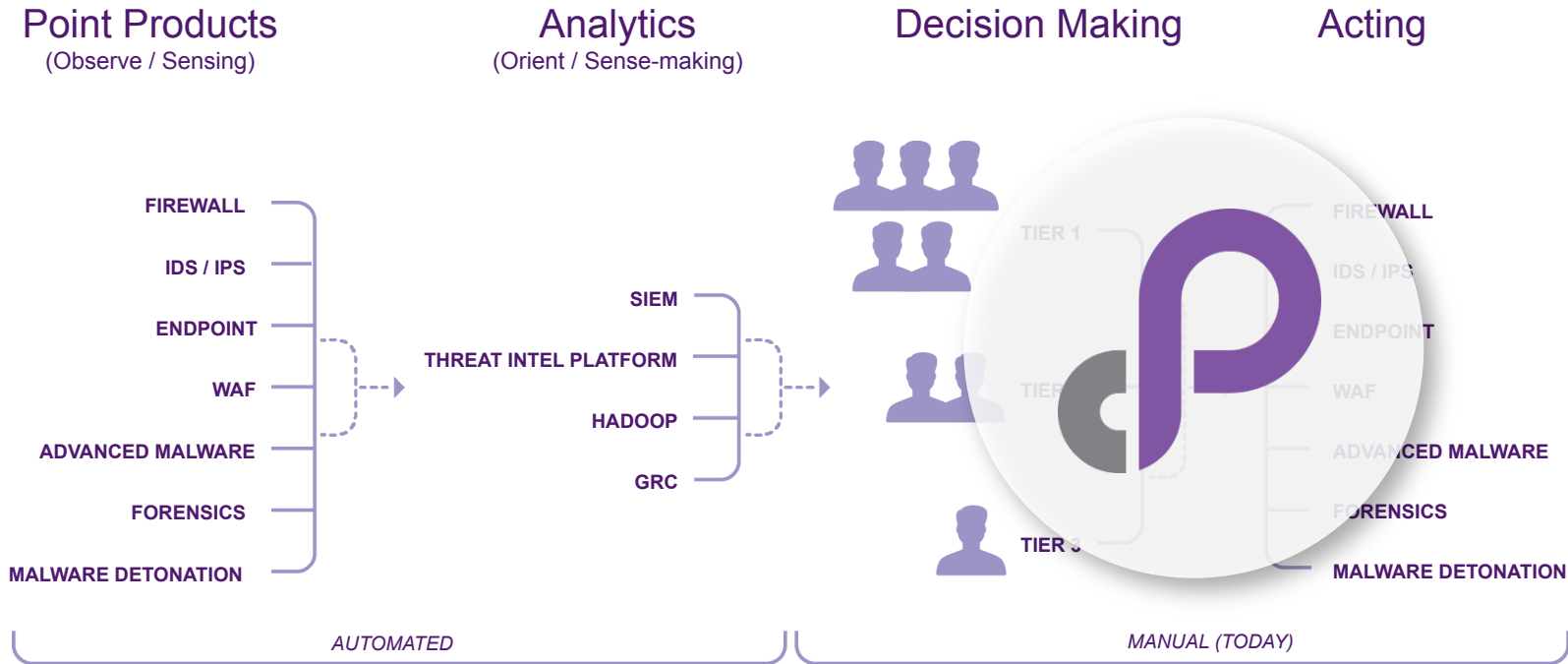
Start Stream capture

OK I Think I Found An Issue, What Should I Do?

- Validate Against Threat Intelligence
- Review Historical Data for the Host
- Check Internal, Proprietary Data Stores
- Look at Past Tickets
- Check Management Consoles for Additional Deep Packet Analysis
- Start a Backup
- Quarantine a System



Automating Security Operations

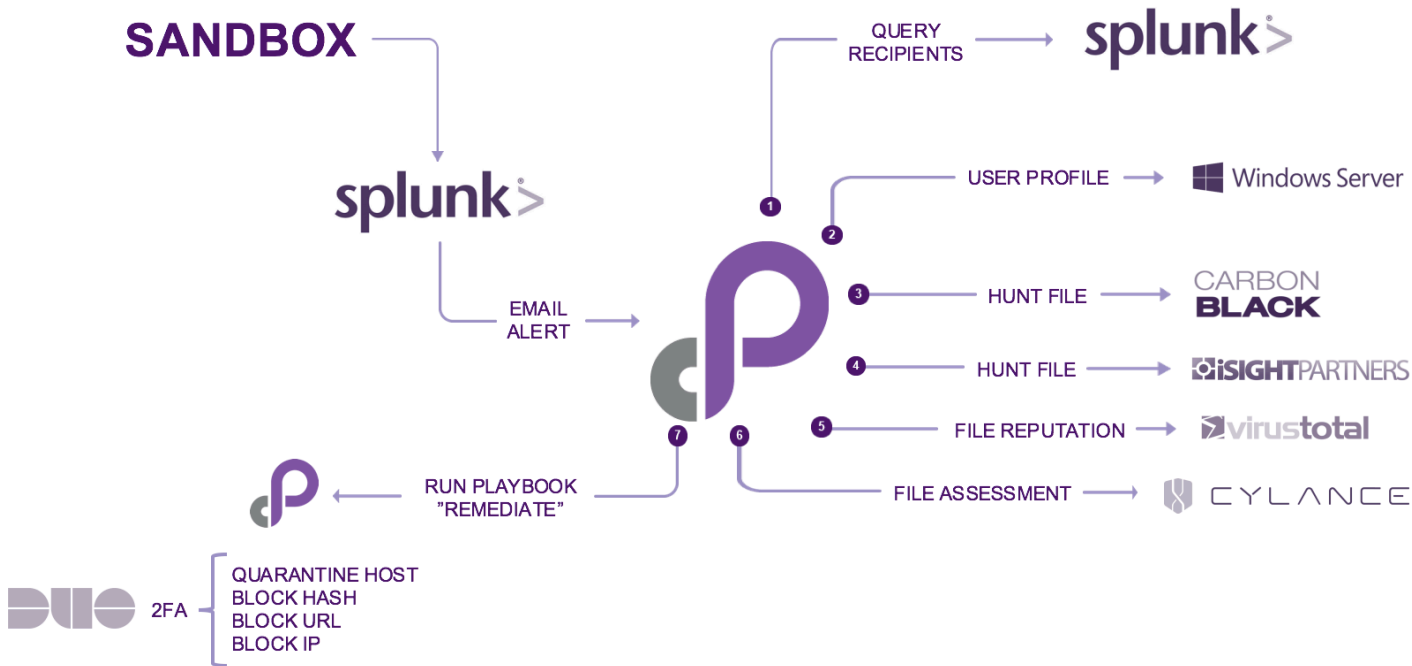


DEMO: Splunk ES/Phantom Integration

.conf2016

splunk >

Case Study: Automated Malware Analysis & Remediation



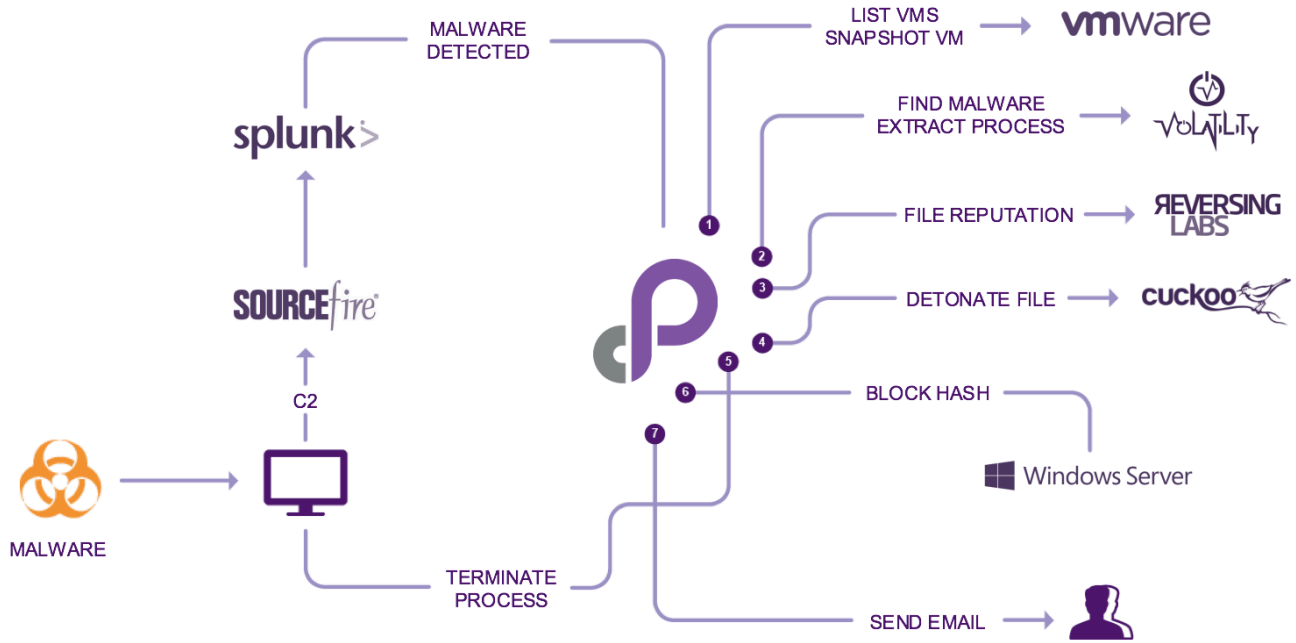
DEMO: Phantom Platform & Community



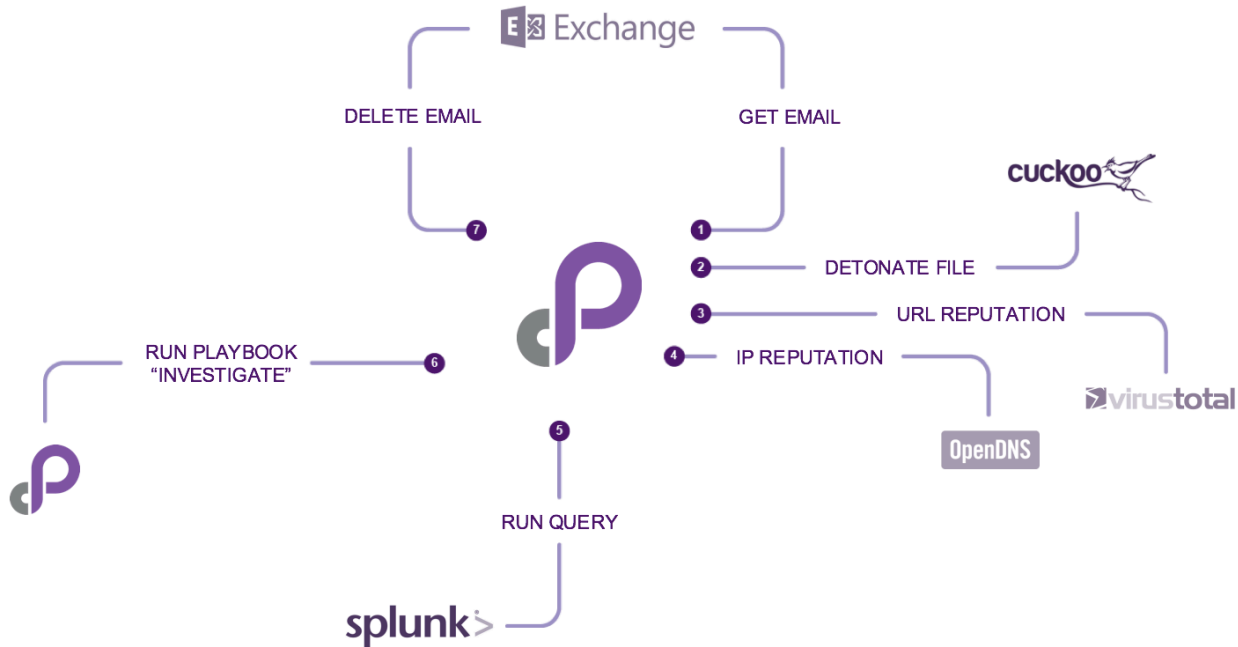
.conf2016

splunk >

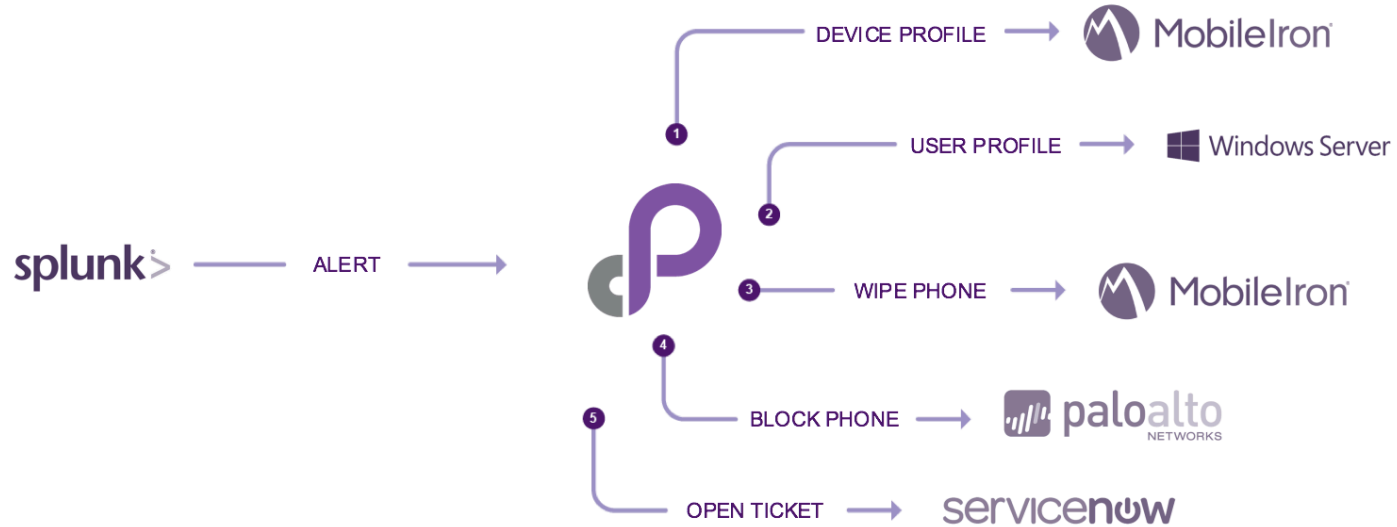
Case Study: Investigate And Contain



Case Study: Phishing Investigation



Case Study: Unauthorized IP



Session Recap

- Reviewed Adaptive Response
- Outlined Key Concepts for Splunk / Phantom
- Demoed Splunk ES / Phantom
- Shared Customer Case Studies
- What next?
 - Get the Free Community Edition @ www.phantom.us/join



blog.phantom.us



[Phantom-community](#)



twitter.com/tryphantom

THANK YOU

.conf2016