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>

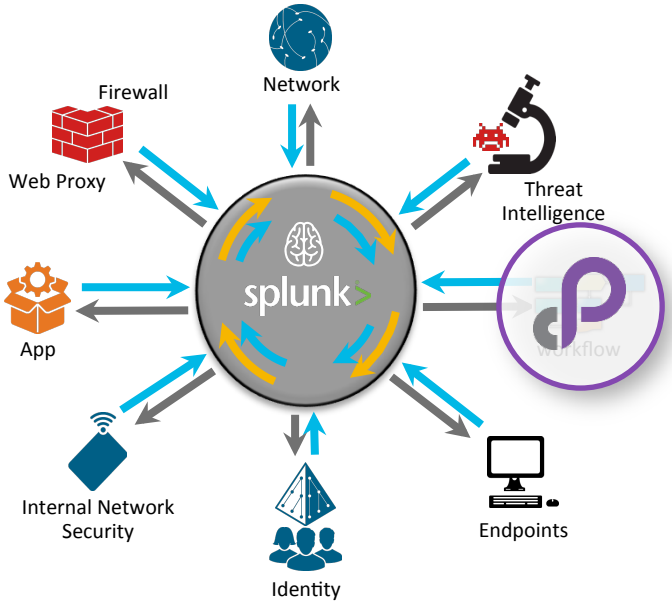
Disclaimer

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

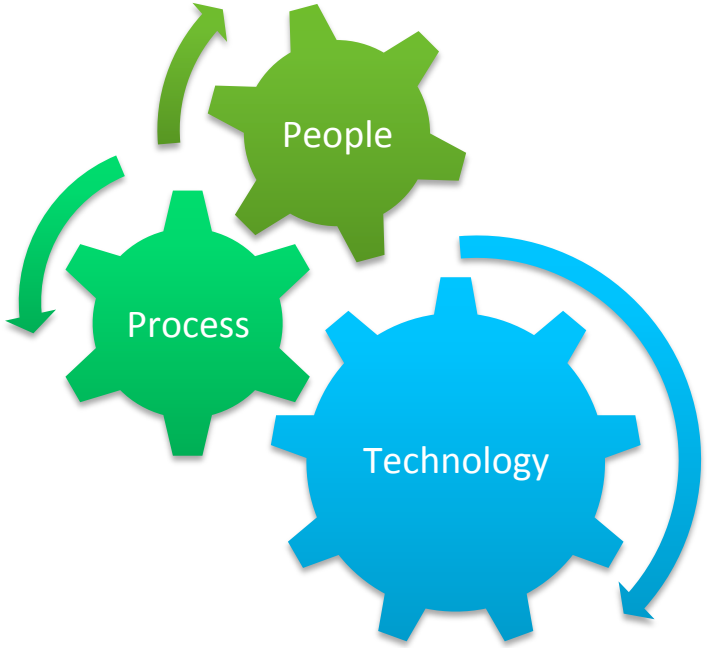


Why Security Orchestration Matters

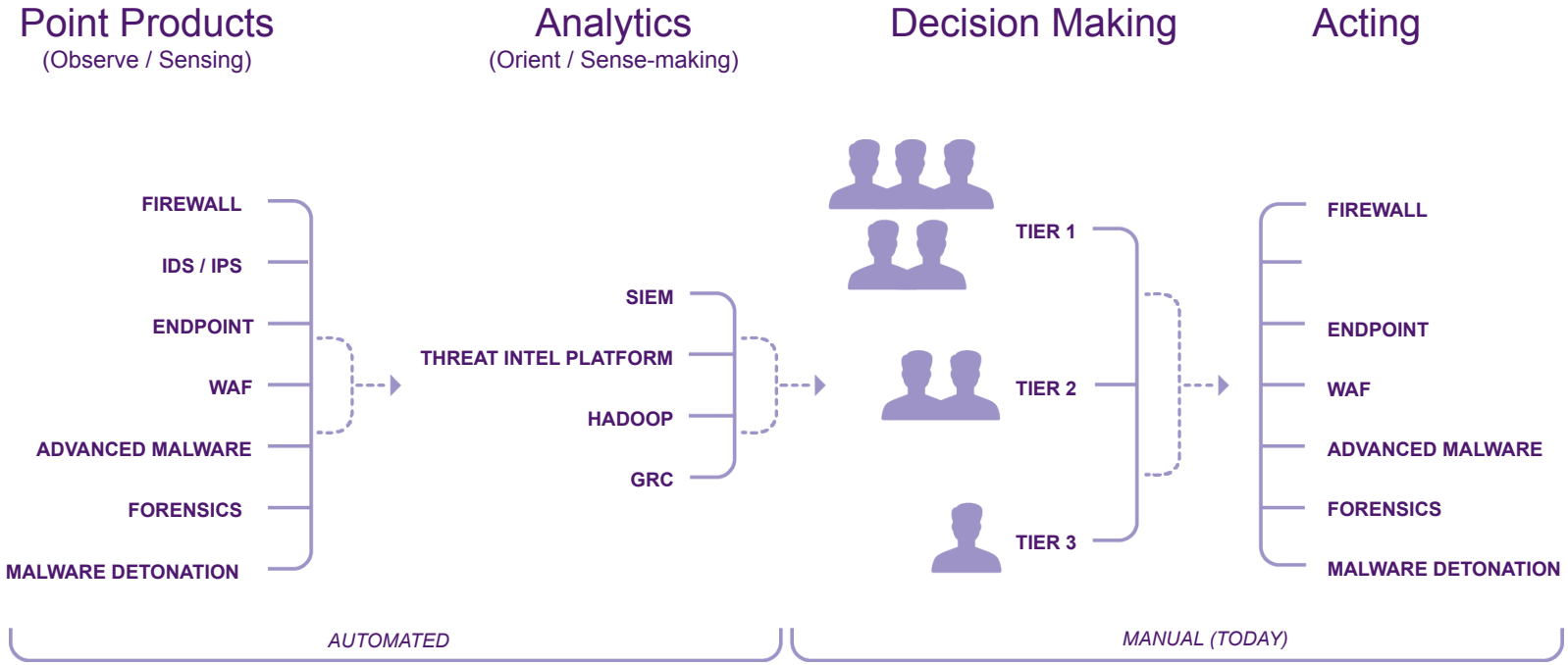
- Market leading MSSP
- Home grown correlation engine - Our version of a SIEM
- Hundreds of customers
- Scalable process
- Custom tools for the analyst to make a decision
  - IP history across organization and business sector
  - Threat Intelligence Portal for global threat landscape reference
  - Ticketing 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....

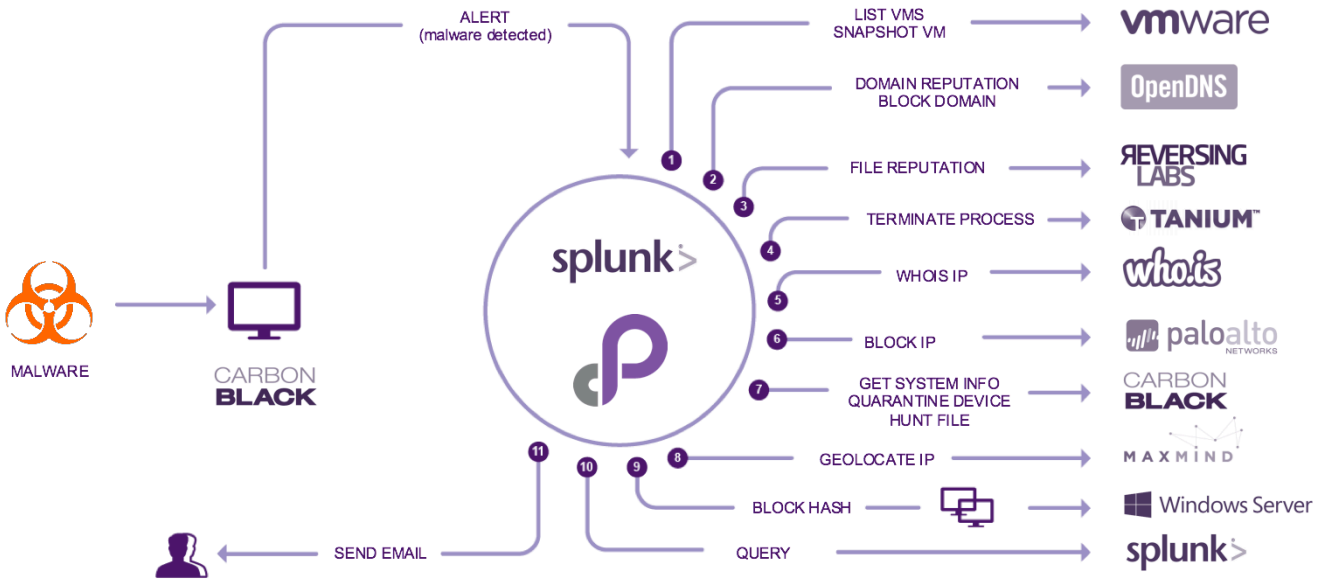
- Continual, pervasive attacks
- Not dealing with a single attack where the firewall and the IDS see the attack and dutifully return an alert
- Attacks can occur from anywhere and can be asynchronous
- Need to detect and contain is critical until eradication and remediation can take place
- Limited pool 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?



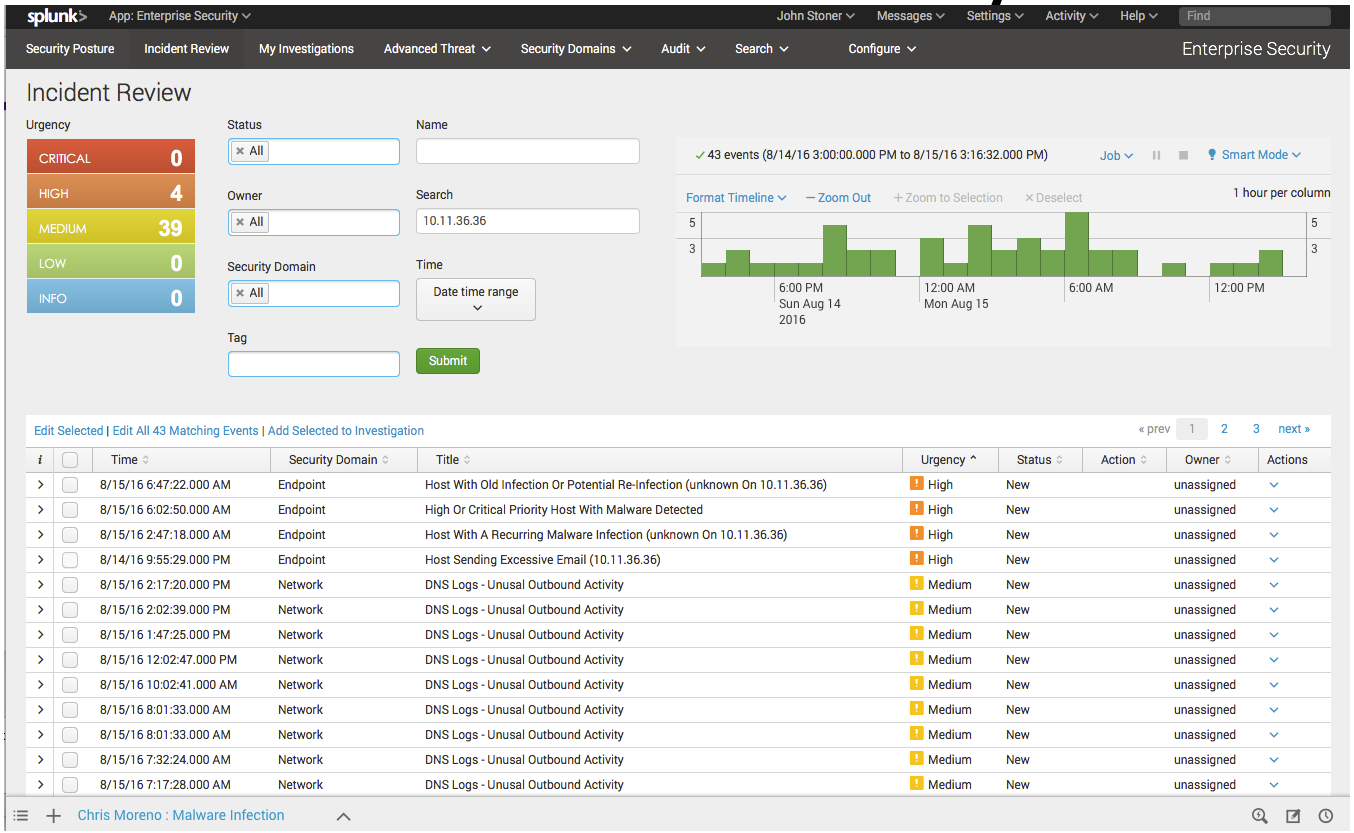
Automating Security Operations



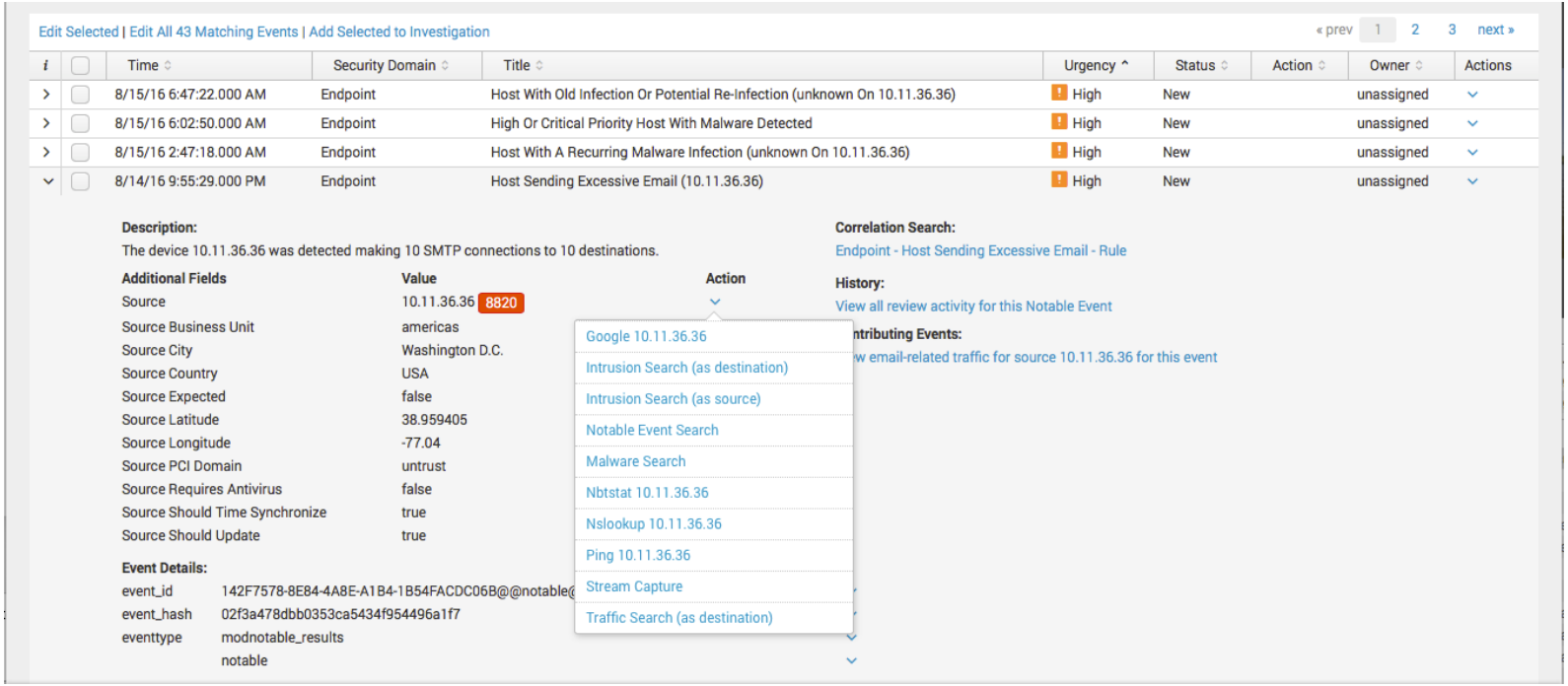
Phantom & Adaptive Response Initiative



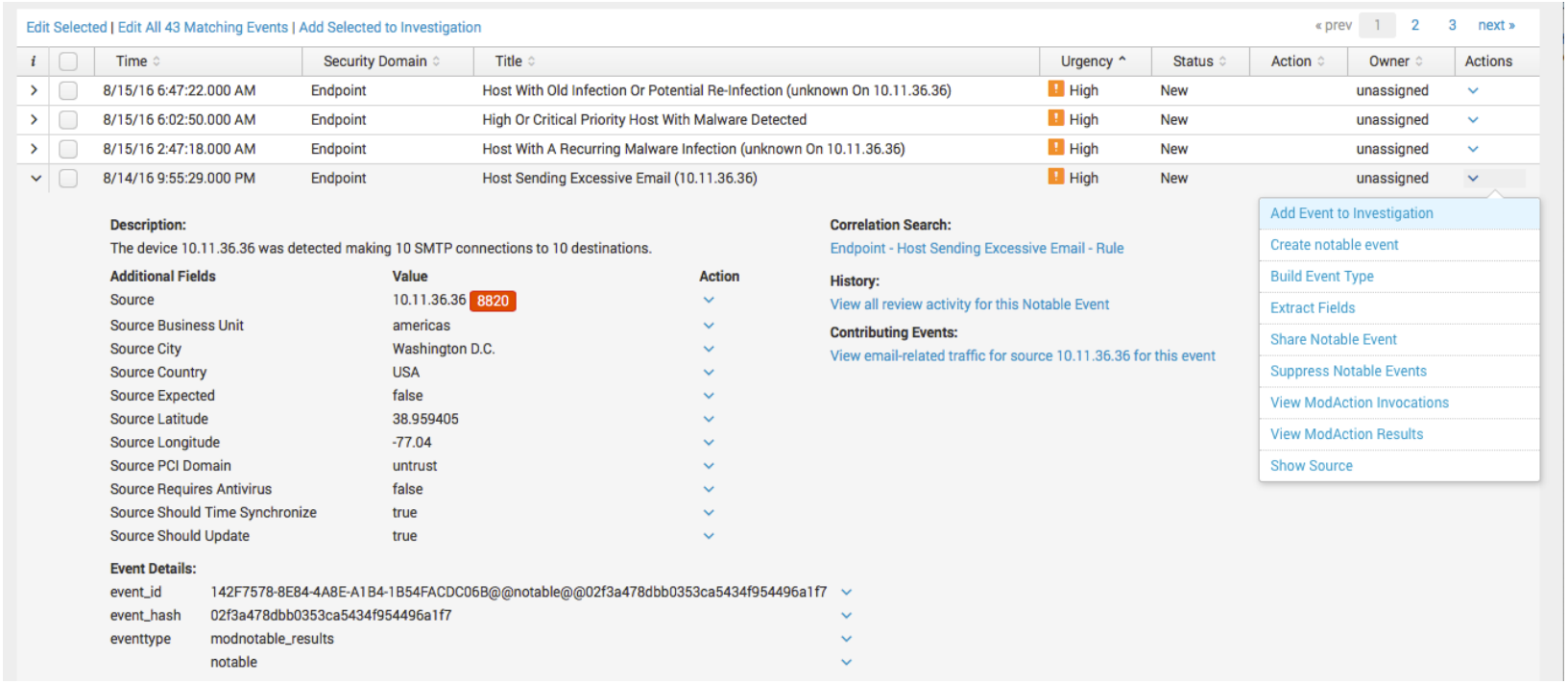
Incident Review – Analyst Queue



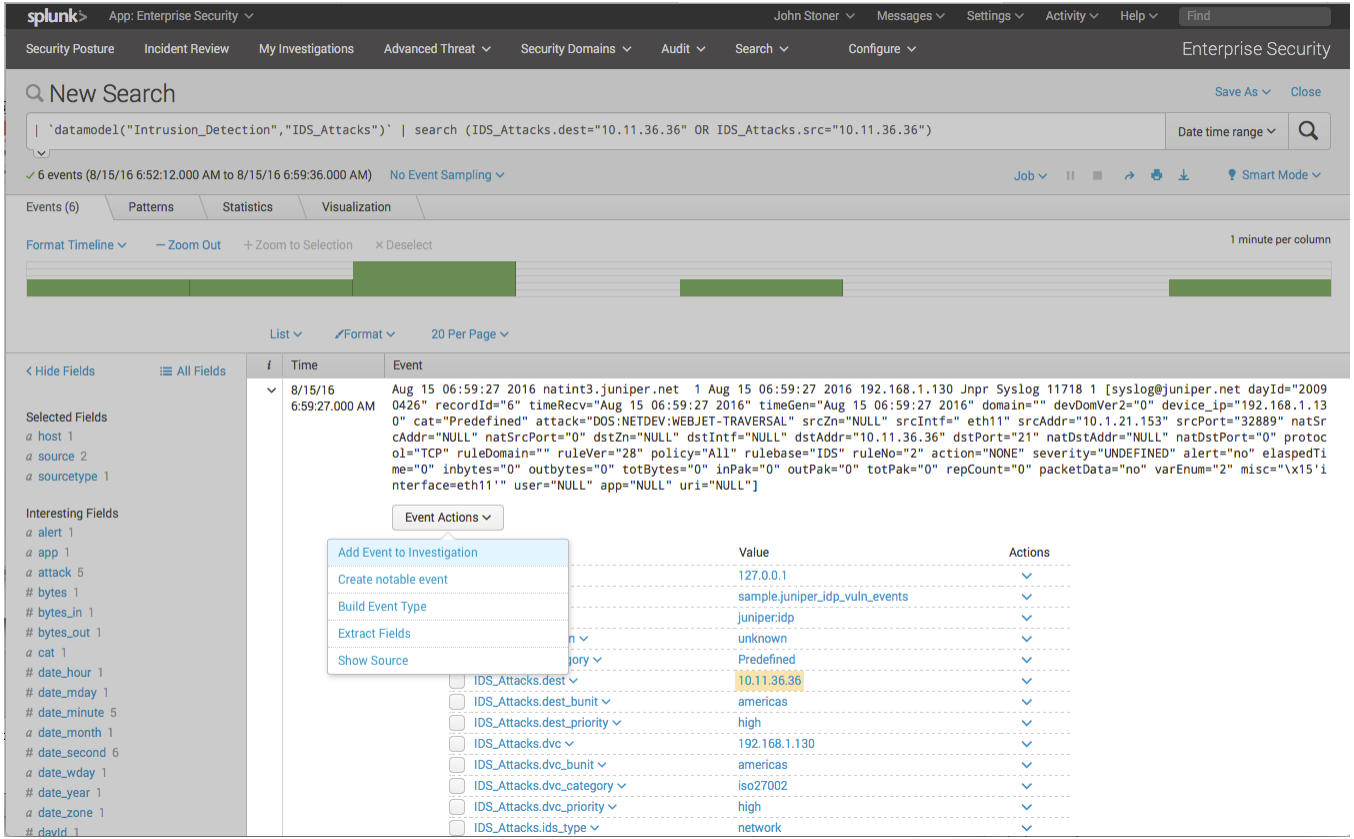
Notable Events and Field Actions



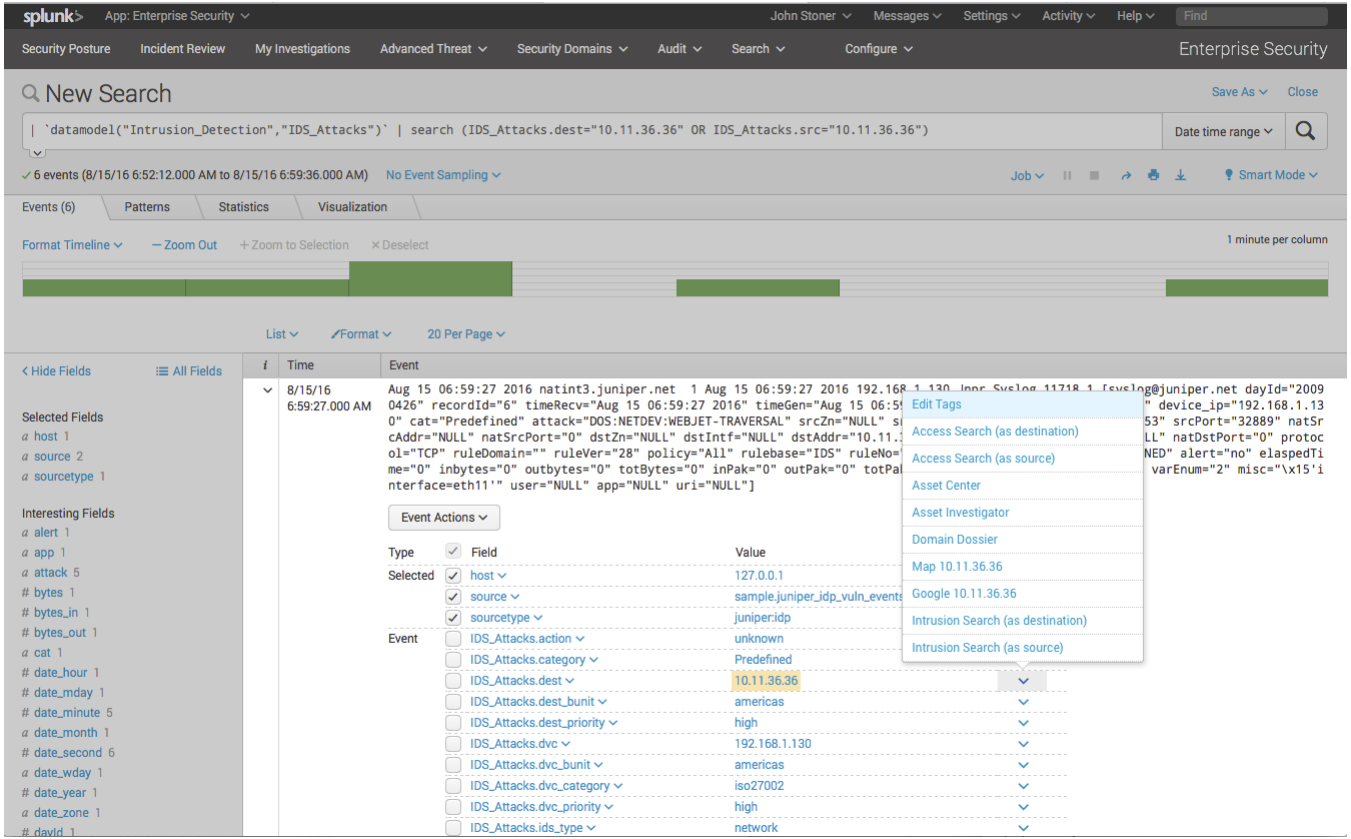
Notable Event Actions



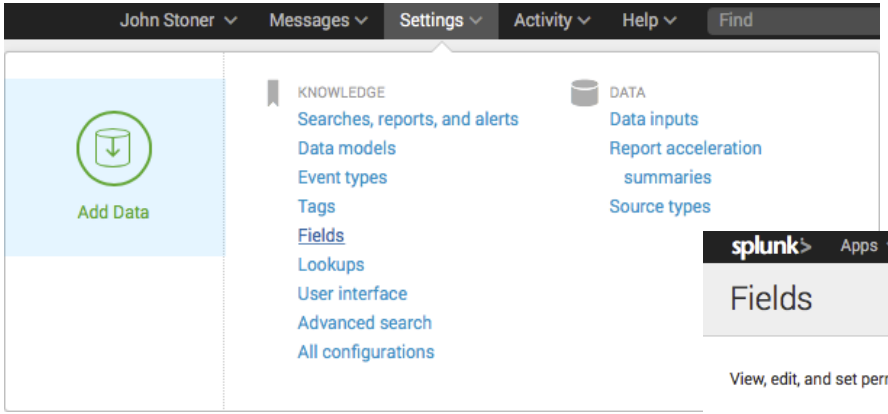
Event Actions At Search

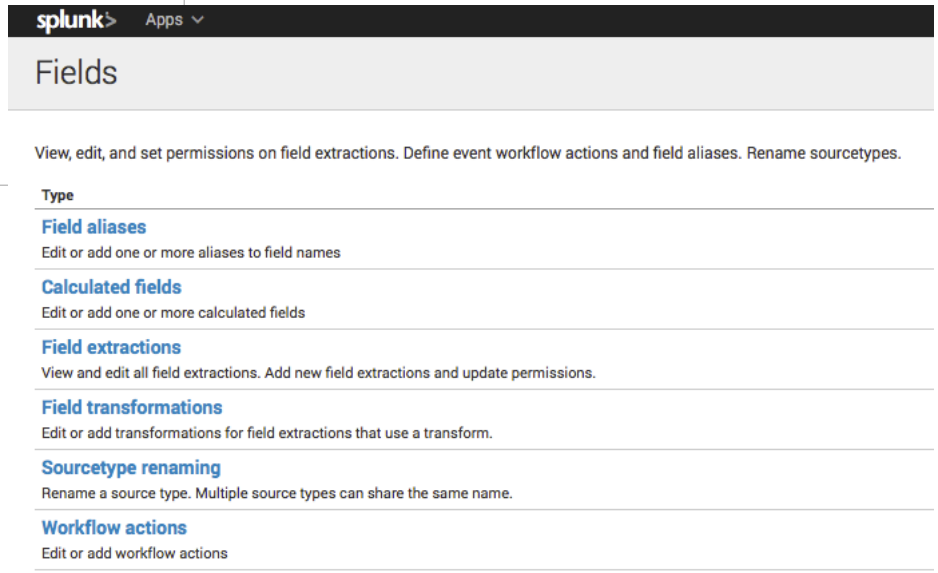


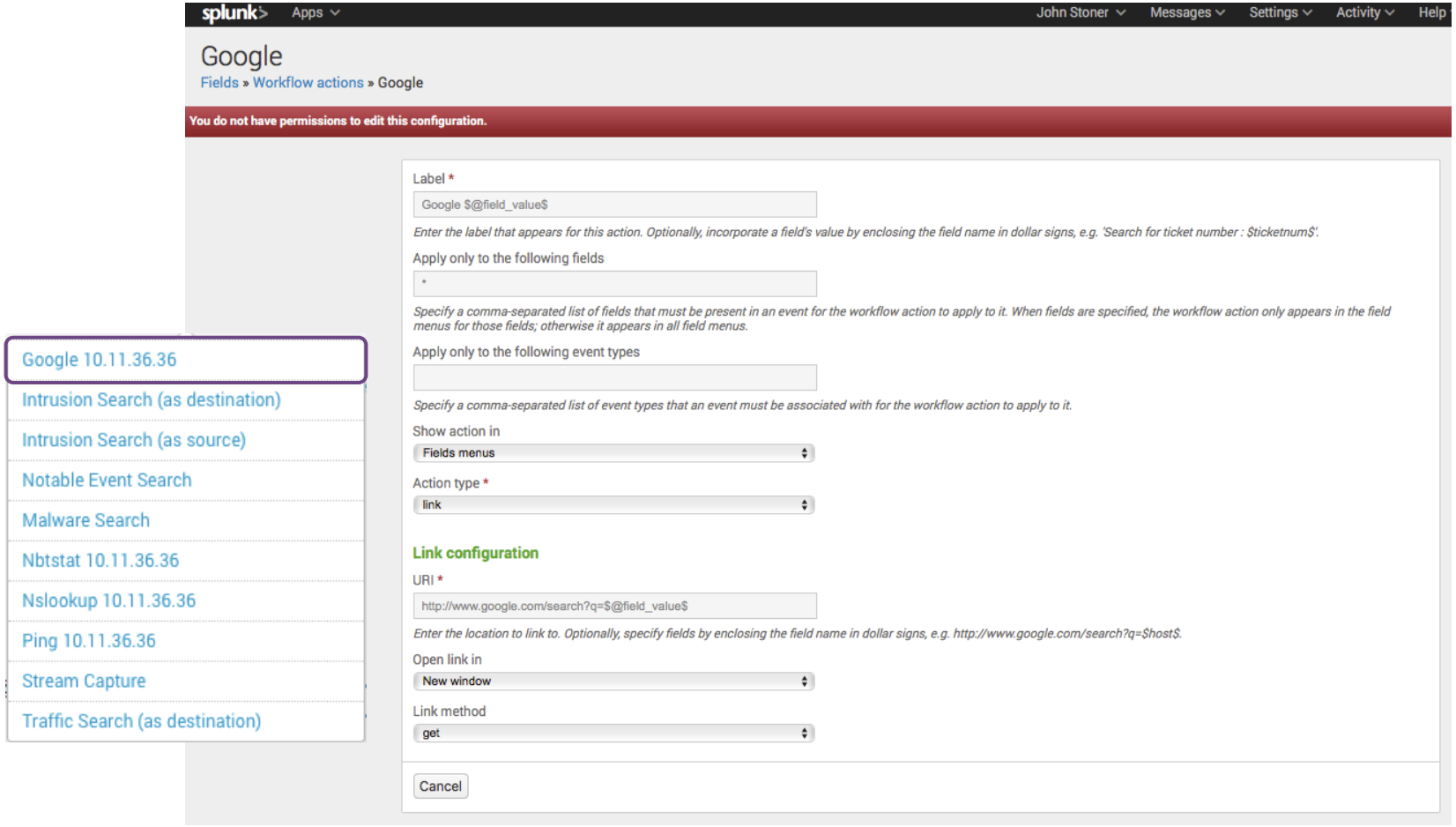
Field Actions At Search

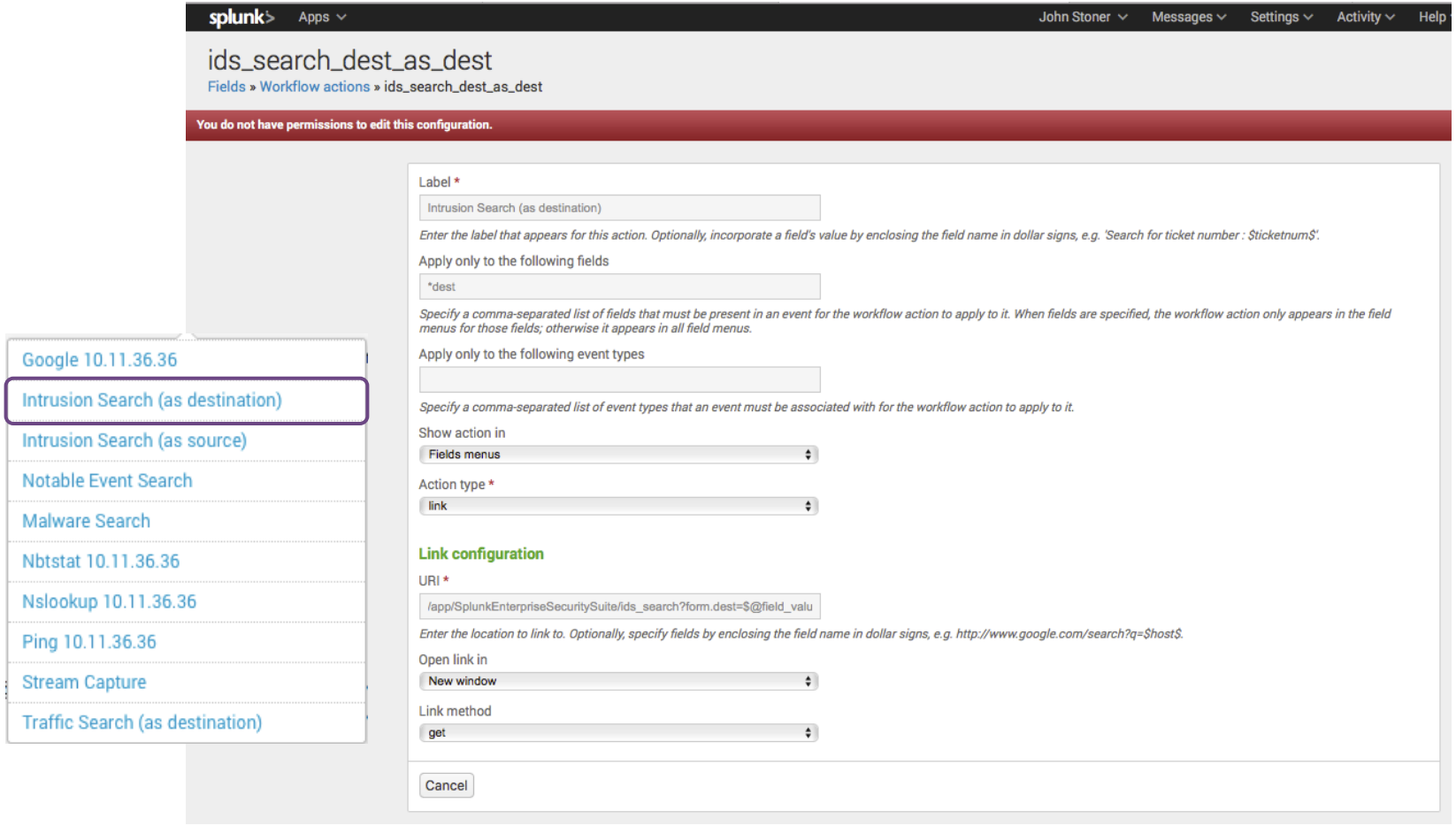


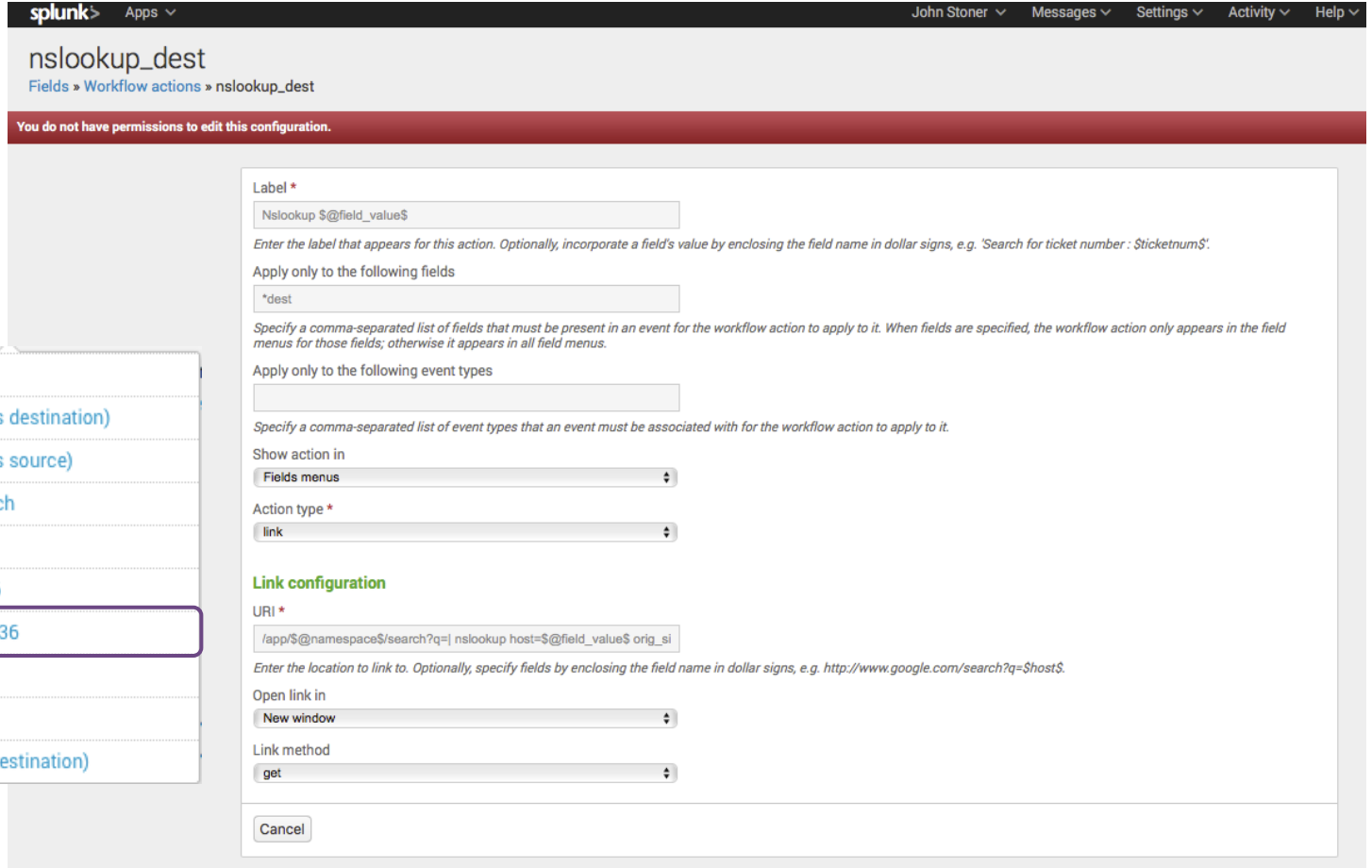
Workflow Actions

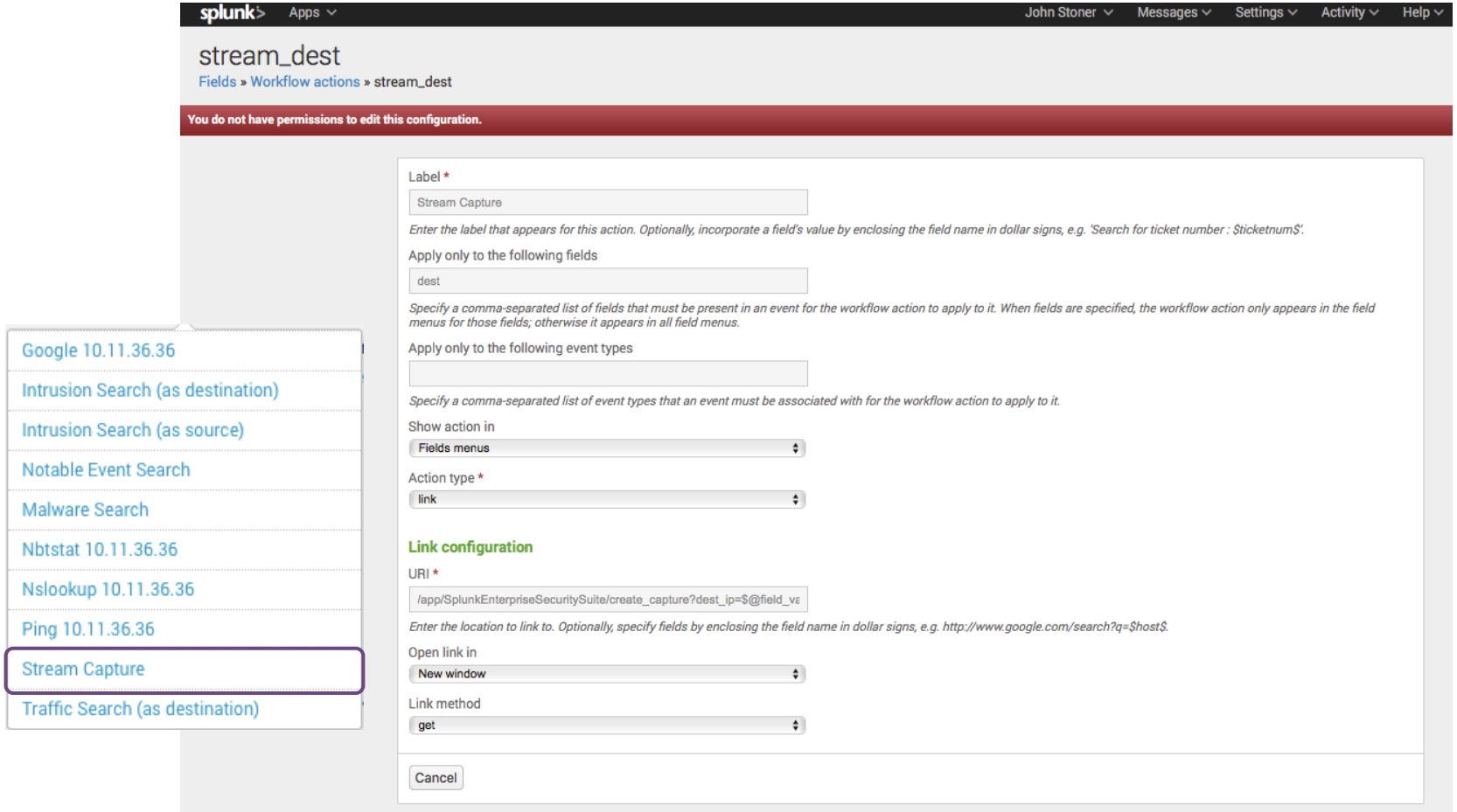




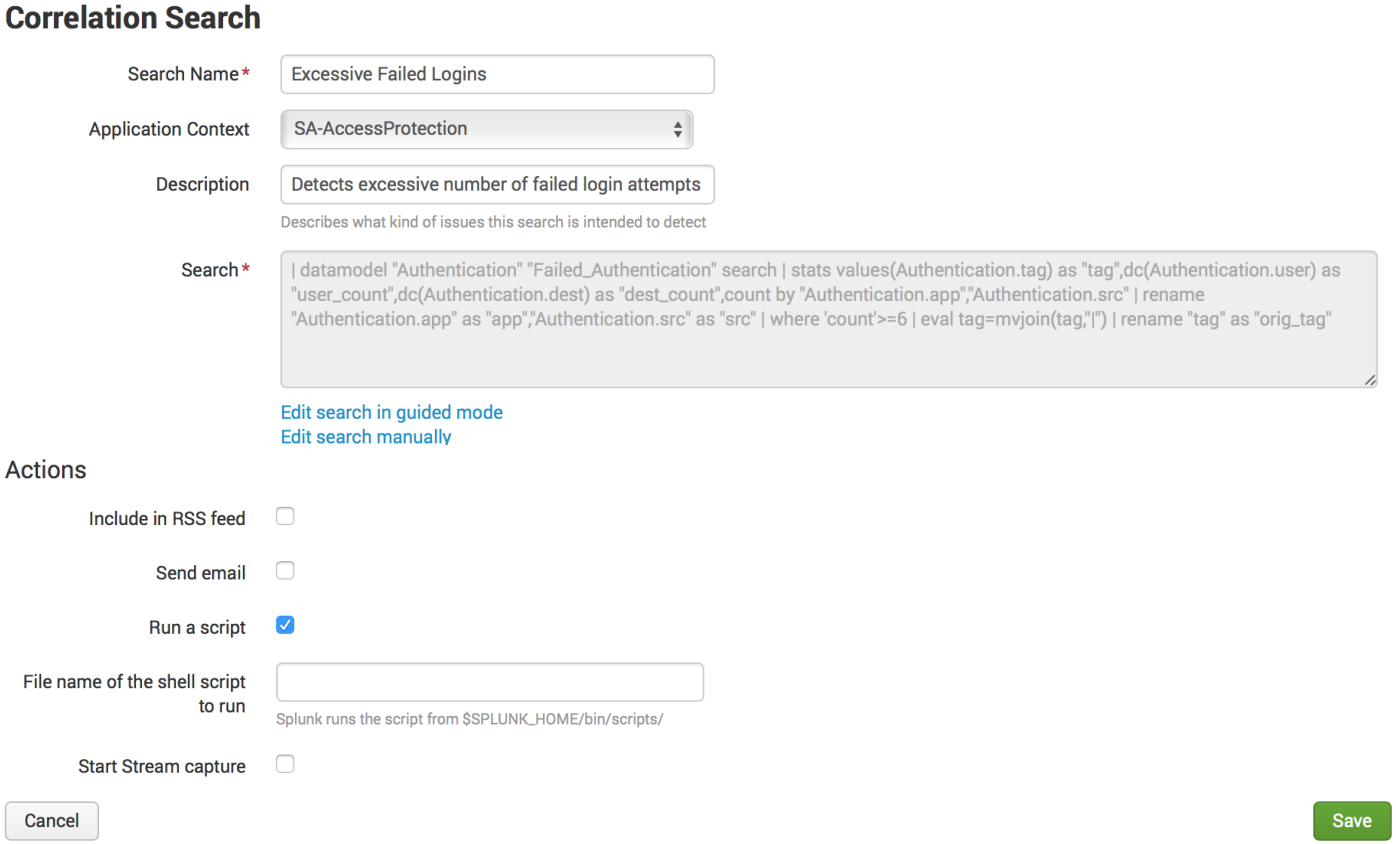

splunk> Apps
John Stoner
Messages
Settings
Activity
Help
Google
Fields » Workflow actions » Google
You do not have permissions to edit this configuration.
Label *
Google $@field_value$
Enter the label that appears for this action. Optionally, incorporate a field's value by enclosing the field name in 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
Fields menus
Action type *
link
Link configuration
URI *
http://www.google.com/search?q=$@field_value$
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
New window
Link method
get
Cancel
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)


splunk> Apps
John Stoner
Messages
Settings
Activity
Help
ids_search_dest_as_dest
Fields » Workflow actions » ids_search_dest_as_dest
You do not have permissions to edit this configuration.
Label *
Intrusion Search (as destination)
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
*dest
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
Fields menus
Action type *
link
Link configuration
URI *
/app/SplunkEnterpriseSecuritySuite/ids_search?form.dest=$@field_valu
Enter the location to link to. Optionally, specify fields by enclosing the field name in dollar signs, e.g. http://www.google.com/search?q=$host$.
Open link in
New window
Link method
get
Cancel
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)


splunk> Apps
John Stoner
Messages
Settings
Activity
Help
nslookup_dest
Fields » Workflow actions » nslookup_dest
You do not have permissions to edit this configuration.
Label *
Nslookup $@field_value$
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
*dest
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
Fields menus
Action type *
link
Link configuration
URI *
/app/$@namespace$/search?q=| nslookup host=$@field_value$ orig_si
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
New window
Link method
get
Cancel
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)


splunk> Apps
John Stoner
Messages
Settings
Activity
Help
stream_dest
Fields » Workflow actions » stream_dest
You do not have permissions to edit this configuration.
Label *
Stream Capture
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
dest
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
Fields menus
Action type *
link
Link configuration
URI *
/app/SplunkEnterpriseSecuritySuite/create_capture?dest_ip=$@field_va
Enter the location to link to. Optionally, specify fields by enclosing the field name in dollar signs, e.g. http://www.google.com/search?q=$host$.
Open link in
New window
Link method
get
Cancel
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)

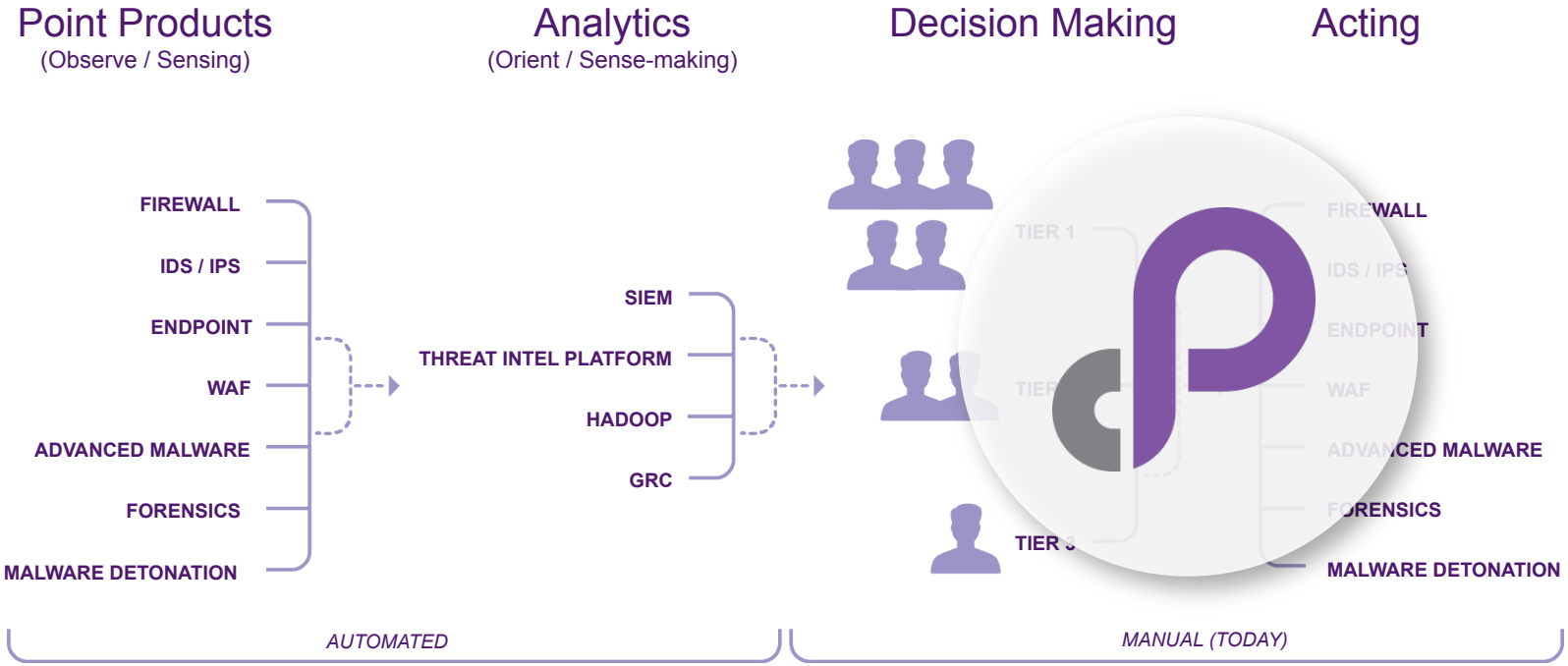
Correlation Search Actions



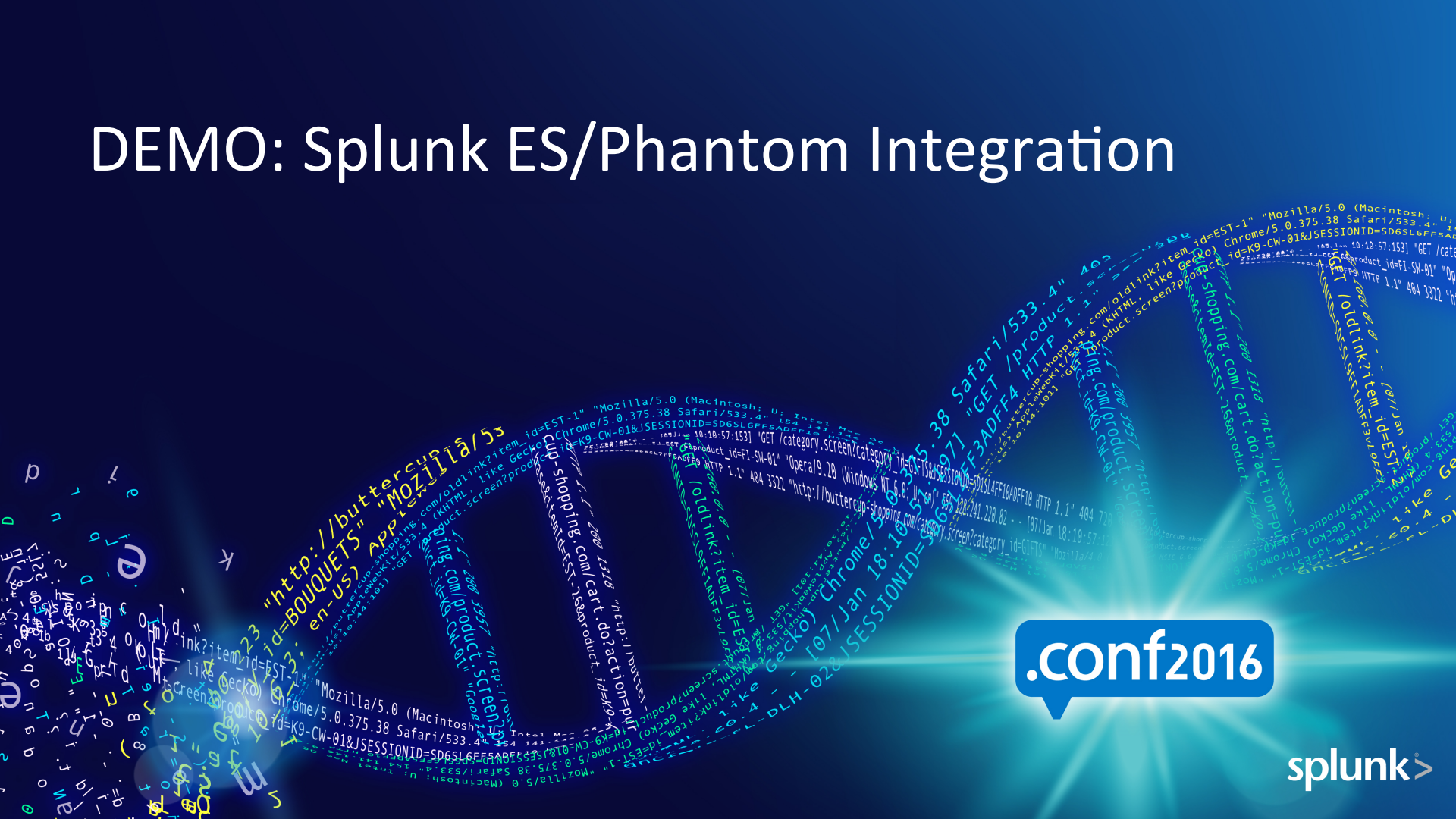
OK I Think I Found An Issue, What Should I Do?

- 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

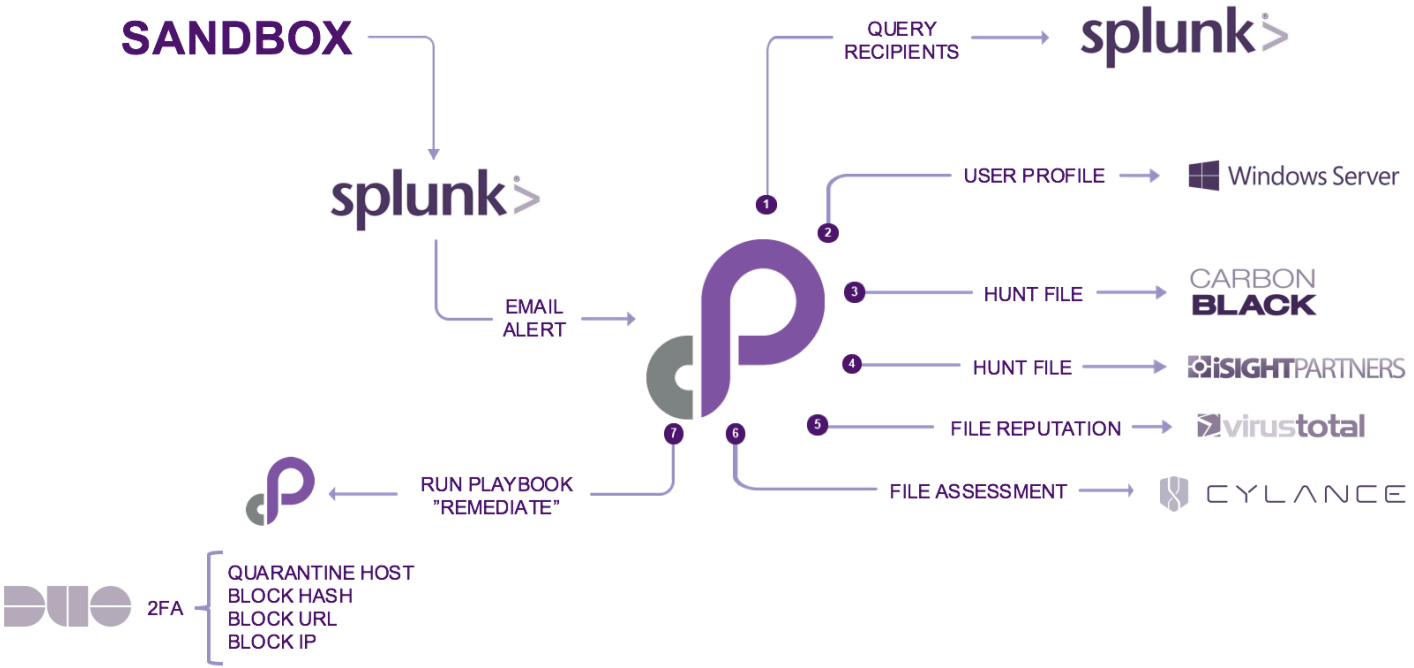
Automating Security Operations



DEMO: Splunk ES/Phantom Integration

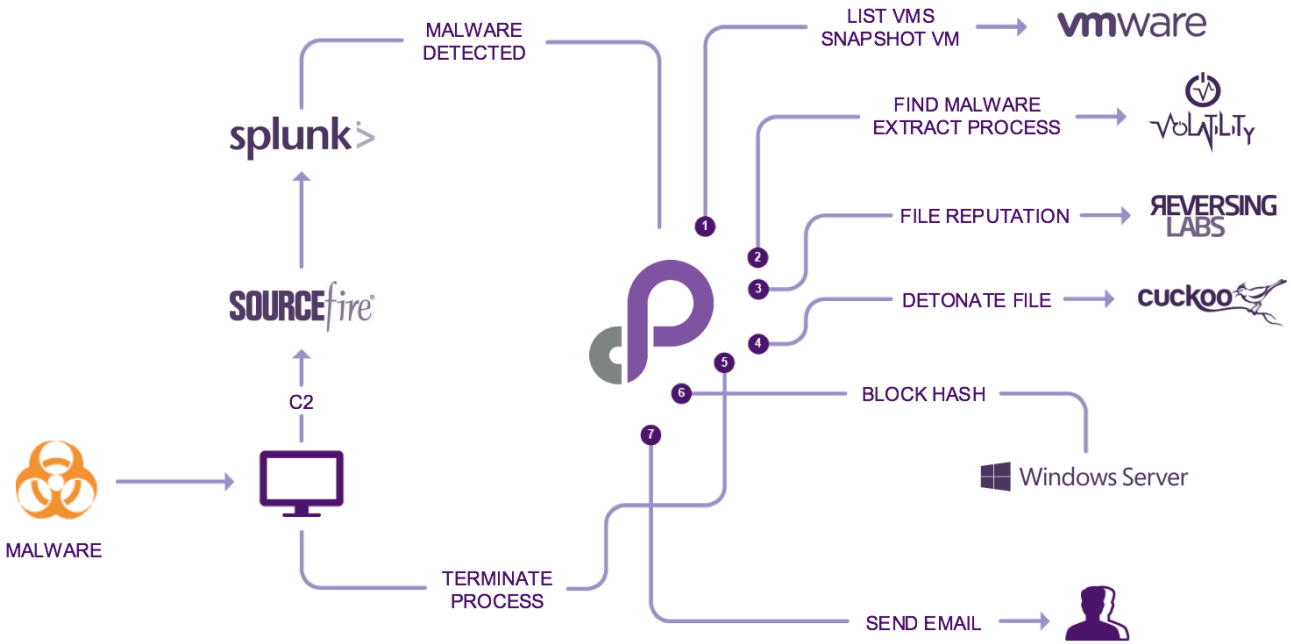


Case Study: Automated Malware Analysis & Remediation

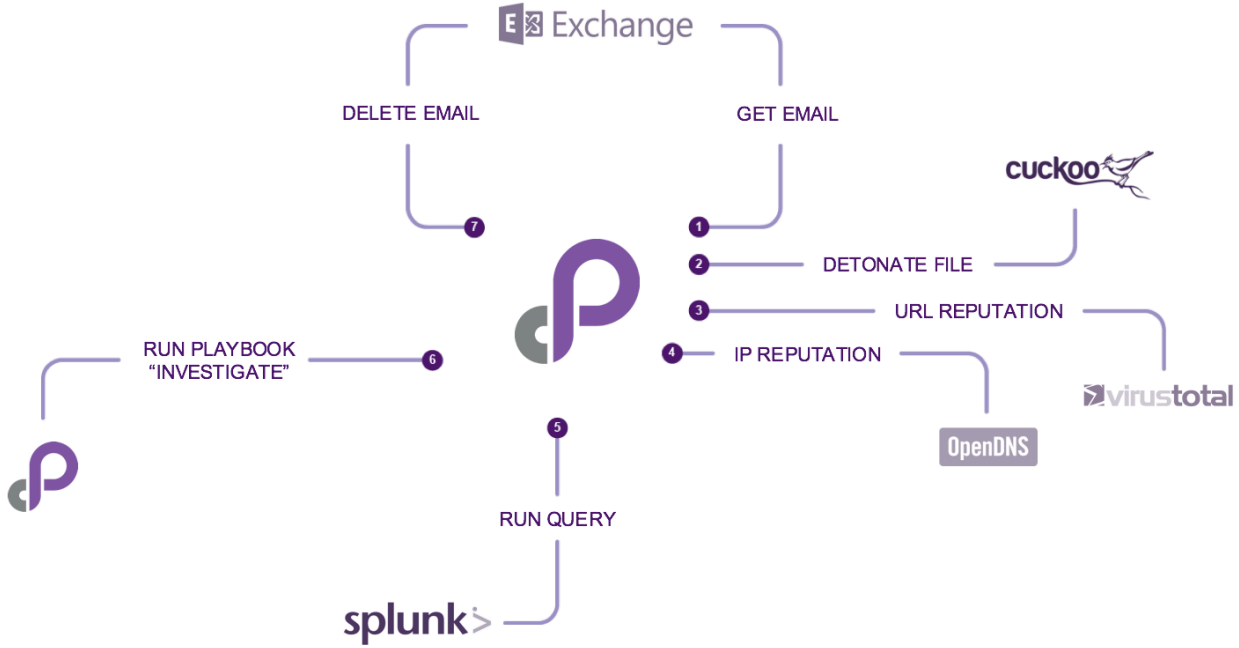


DEMO: Phantom Platform & Community

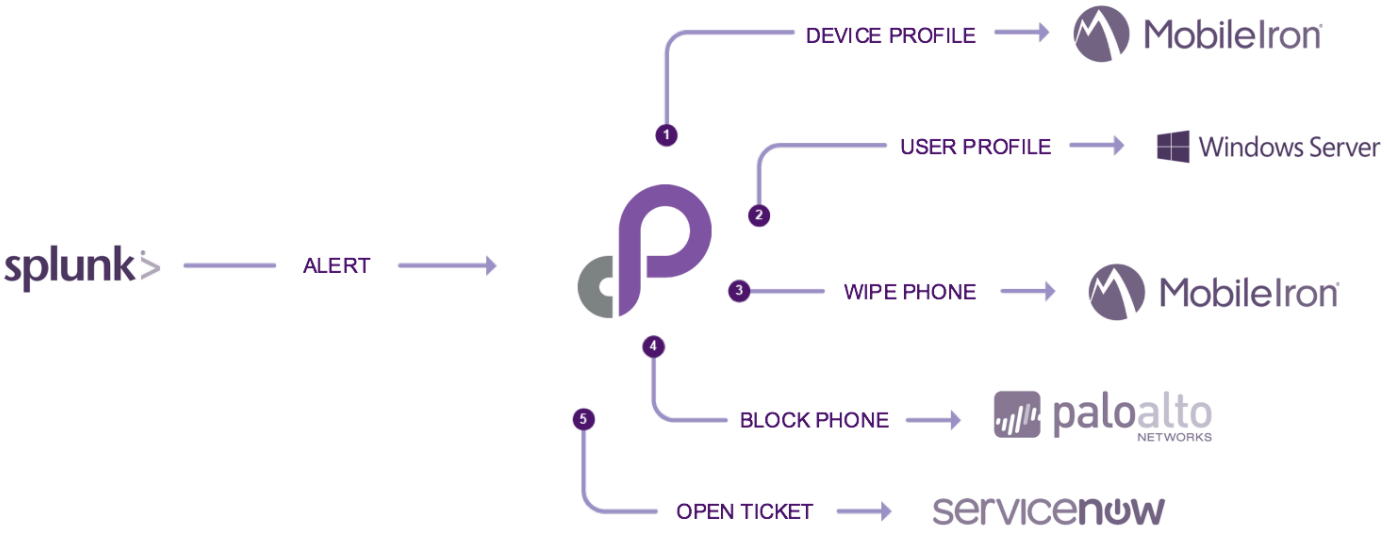
Case Study: Investigate And Contain



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

splunk>