

# The Security Looking Glass: Operationalizing Cloud Enterprise Security – An Adaptive Response Approach

Peter Hefley

Manager, Information Security

Republic Services Inc.

Nate Smalley

Solutions Engineer, 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.

# Who Is This Nate Smalley Guy



- IT Operations Technologist (Reformed Security Guy)
- Former Technical Director of Security & Monitoring Tools Team – Apollo Group (University of Phoenix)
- Currently Splunk Staff Sales Engineer supporting Republic Services

# Peter Hefley



- Hands-on experience with nuclear weapons, satellite communications, and cryptography
- Monitored and maintained physical security of an area twice the size of New Hampshire
- Built and managed a Cisco centric MSSP NOC/SOC for the financial industry
- Consultant, penetration tester, architect, and technical assessor for Fortune 500
- Manager of Information Security at RSI



# Security's Biggest Problem

PEOPLE

# Security's Biggest Problem

Qualified People

# Our Solution!

**SNAKE-OIL LINIMENT**

**RELIEVES INSTANTANEOUSLY**

**AND CURES HEADACHE, NEURALGIA, TOOTHACHE, EARACHE, BACKACHE, SWELLINGS, SPRAINS, SORE CHEST, SWELLING of the THROAT, CONTRACTED CORDS and MUSCLES, STIFF JOINTS, WRENCHES, DISLOCATIONS, CUTS and BRUISES.**

**It Quickly takes out the Soreness and Inflammation from Corns, Bunions, Insect and Reptile Bites.**

The best External Preparation for **BYCICLISTS** and **ATHLETES**. It makes the Muscles supple and Relaxes the Cords. Loosens the Joints and gives a feeling of Freshness and Vigor to the whole System.

**SNAKE-OIL LINIMENT CURES ALL ACHES AND PAINS.**

If you are suffering from Rheumatism, **ALWAYS** take **LA-CAS-KA** internally for the Blood and **use SNAKE-OIL LINIMENT** externally. When used together we **GUARANTEE A CURE** in every instance or **MONEY REFUNDED**.

---

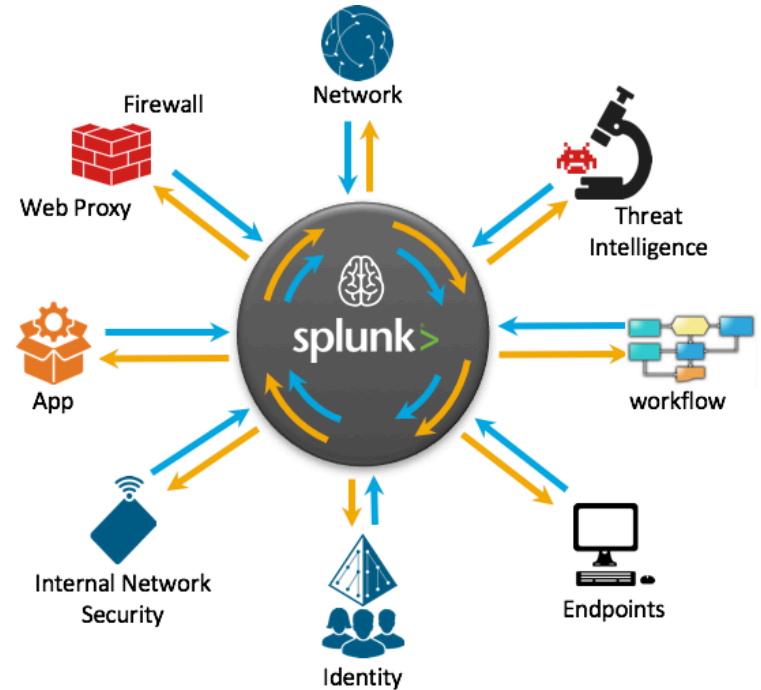
**If You Are Afflicted With DEAFNESS**

Get Our Specially Prepared

**PURE Rattlesnake Oil**

# Agenda

- What Is Adaptive Response?
- How Does This Fit Into The Kill Chain?
- What We Did To Address The Risks?
- Why Did We Do It?
- How You Can Do It, Too!

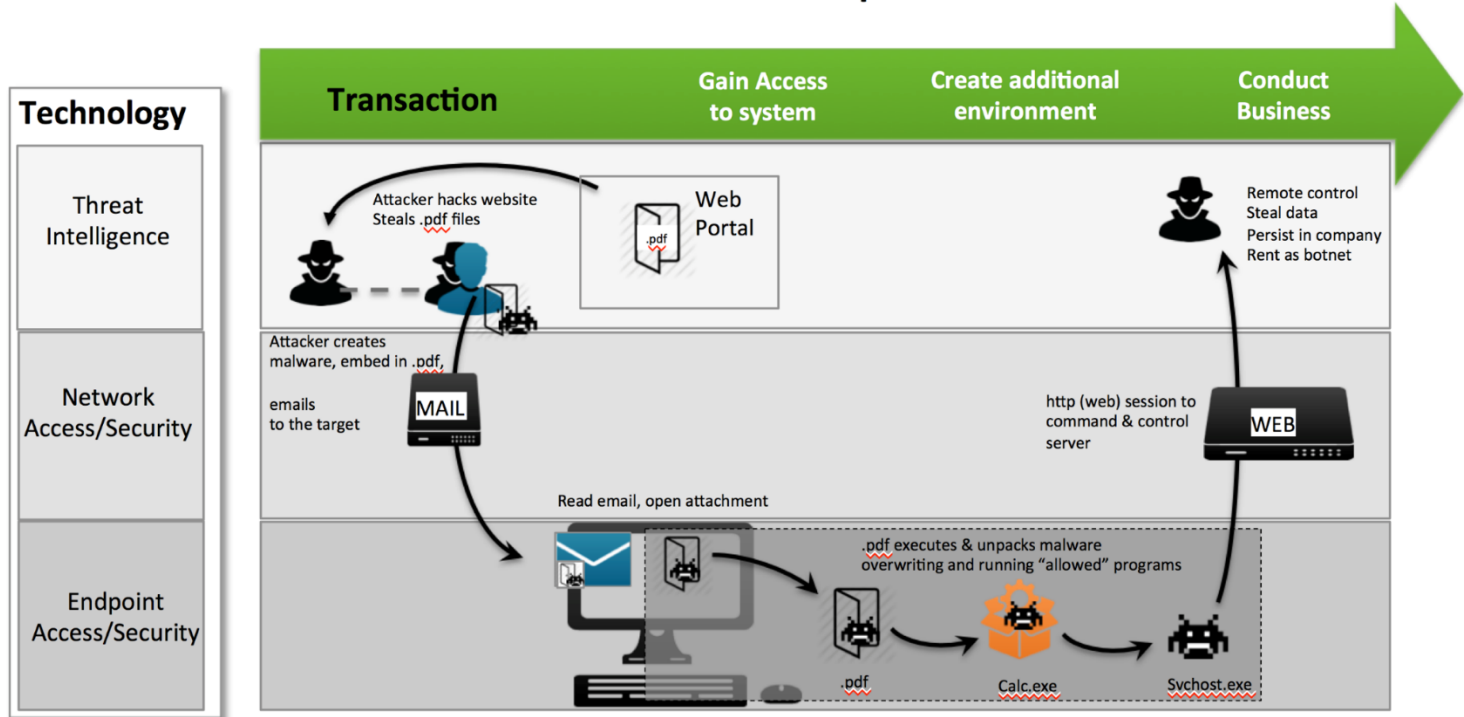


# Adaptive Response – Market Validation

Carbon Black, CyberArk, Fortinet, Palo Alto Networks, Phantom, Splunk, Tanium, ThreatConnect, and Ziften Demonstrated Splunk Adaptive Response at RSA Conference 2016

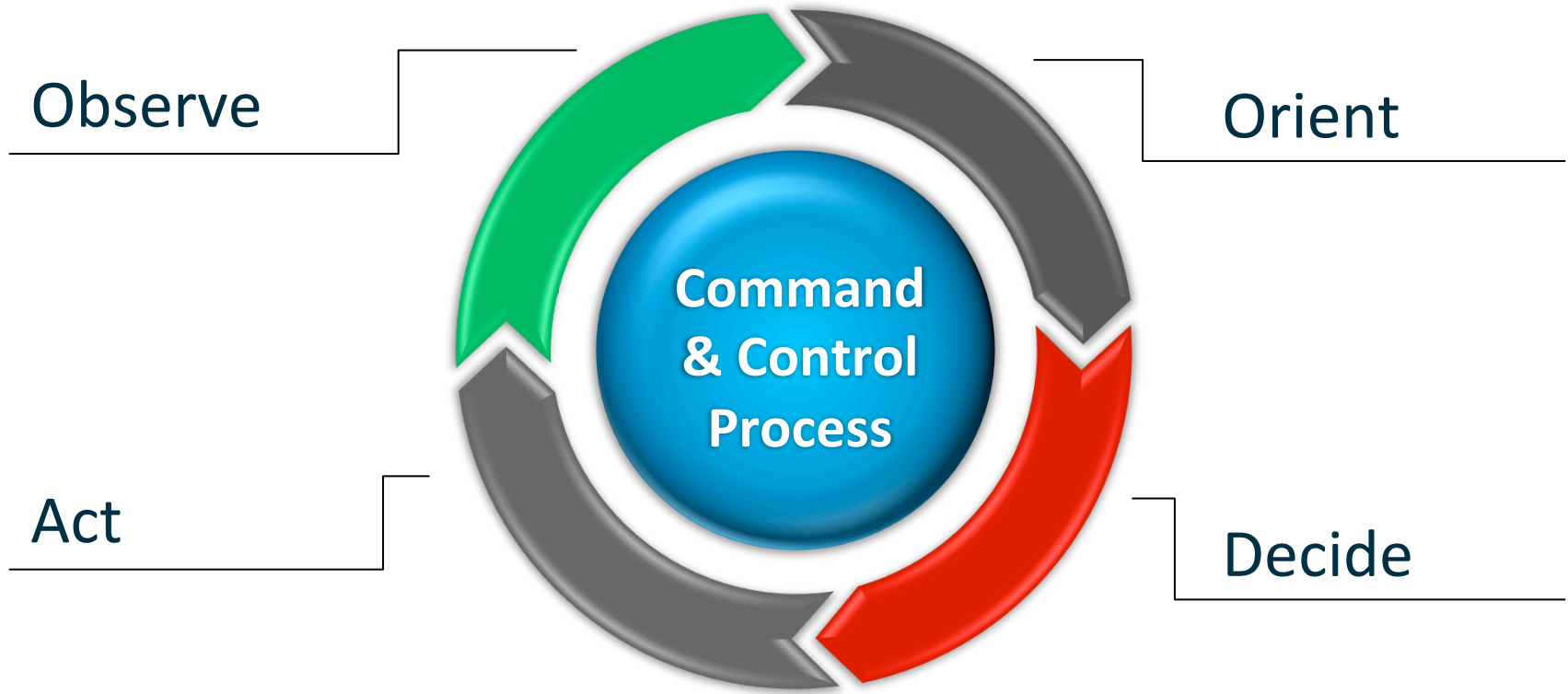
# Kill Chain Example

Modern Attacks are Multi-step Transactions

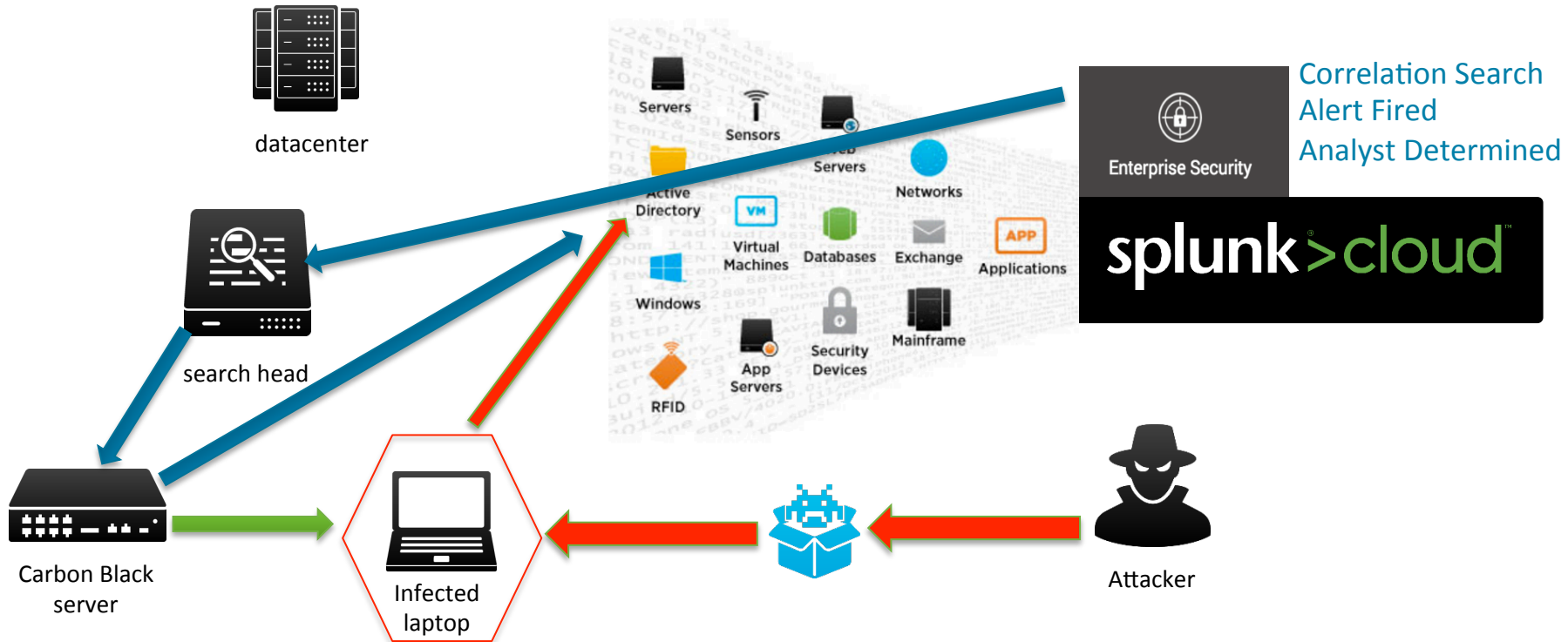




# Decision Loop



# The Flow “It Is Bidirectional”



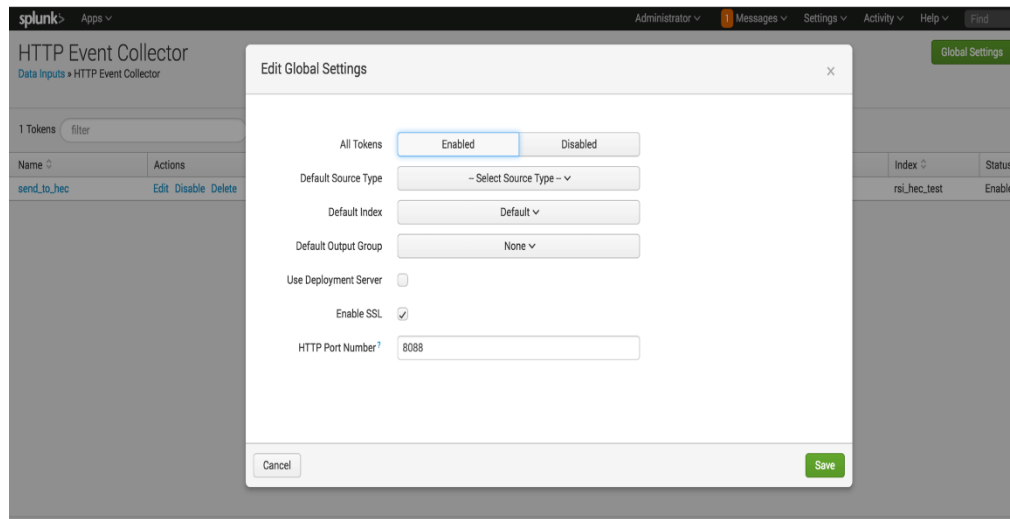
# What Did We Do?

1. Using the extentionable nature of Splunk, specifically HEC (HTTP Event Collector) and the Splunk alert actions capability
2. Created a capability for Analysts to invoke actions specifically around:
  1. Carbon Black – Host Based Firewalling
  2. Symantec – Deep Scanning
3. Empower Security Analysts to decide how and when to execute actions along the kill chain path through a click of a button in Splunk Enterprise Security
4. Validate Security Analyst actions had the desired effects
5. Reduce the risk for the organization and provide end to end tracking of a new capability within RSI Splunk Enterprise Security

# The Work - HTTP Event Collector

## Configure HEC REST point in Environment

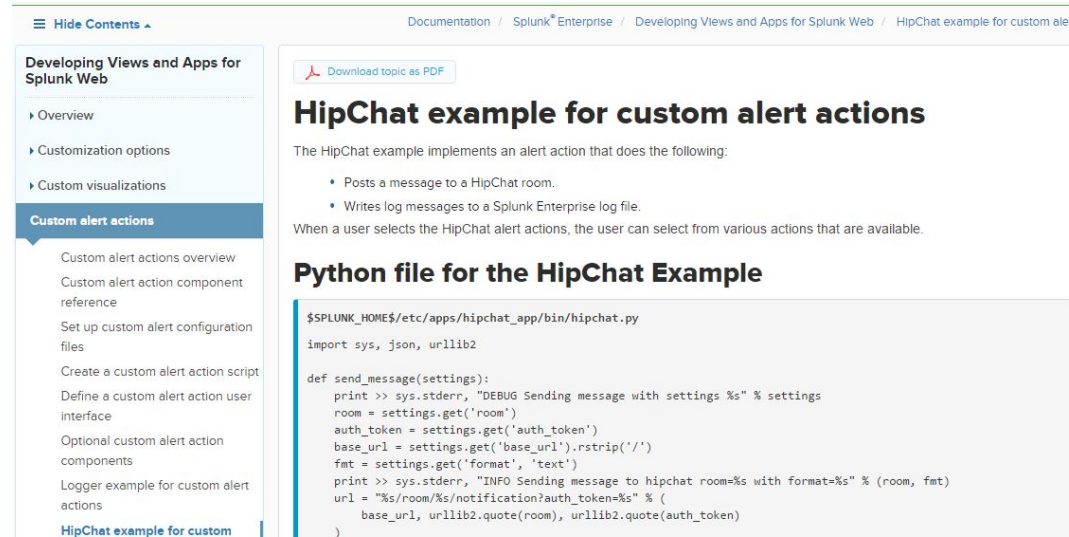
- Create a HEC Input
- Enable Global Settings
  - SSL Is a plus
- Note the Token (you'll use it later)



# The Work - Create An Alert Action

## The Magic of Creating your own

- Start with a template
- Splunk has a HipChat example that is AWESOME!
- <https://docs.splunk.com/Documentation/Splunk/6.4.2/AdvancedDev/ModAlertsAdvancedExample>



The screenshot shows a Splunk documentation page titled "HipChat example for custom alert actions". The page is part of the "Developing Views and Apps for Splunk Web" section. A sidebar on the left lists navigation options: Overview, Customization options, Custom visualizations, and Custom alert actions (which is currently selected). The main content area includes a "Download topic as PDF" button, the title "HipChat example for custom alert actions", and a description: "The HipChat example implements an alert action that does the following: Posts a message to a HipChat room. Writes log messages to a Splunk Enterprise log file." Below this, it states "When a user selects the HipChat alert actions, the user can select from various actions that are available." The section "Python file for the HipChat Example" contains a code block for the file `hipchat.py` located at `$$SPLUNK_HOME$/etc/apps/hipchat_app/bin/hipchat.py`. The code imports `sys`, `json`, and `urllib2`, and defines a `send_message` function that logs and posts a message to HipChat.

```
$$SPLUNK_HOME$/etc/apps/hipchat_app/bin/hipchat.py
import sys, json, urllib2

def send_message(settings):
    print >> sys.stderr, "DEBUG Sending message with settings %s" % settings
    room = settings.get('room')
    auth_token = settings.get('auth_token')
    base_url = settings.get('base_url').rstrip('/')
    fmt = settings.get('format', 'text')
    print >> sys.stderr, "INFO Sending message to hipchat room=%s with format=%s" % (room, fmt)
    url = "%s/room/%s/notification?auth_token=%s" % (
        base_url, urllib2.quote(room), urllib2.quote(auth_token)
    )
```

# The Work - Create An Alert Action

## Carbon Black Rest API Call

```
#!/usr/bin/env python
import sys
import requests
import json
# Reference: https://developer.carbonblack.com/reference/enterprise-response/5.1/rest-api/
#           https://developer.carbonblack.com/reference/enterprise-response/authentication/
#           http://docs.splunk.com/Documentation/Splunk/6.4.1/AdvancedDev/ModAlertsAdvancedExample

# Settings stanza
ssl_verify=False
headers = {'X-Auth-Token':token}

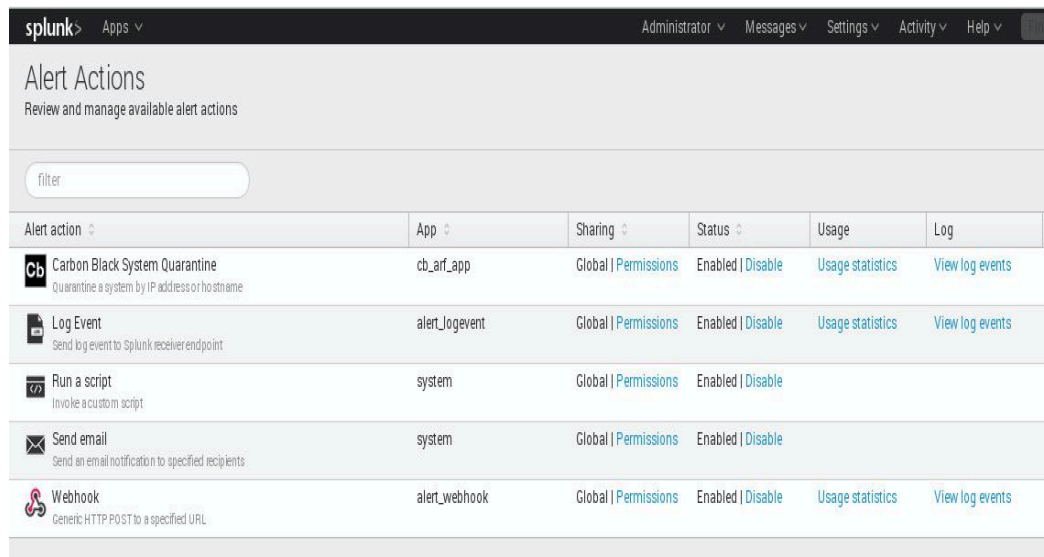
def enable_network_isolation(sensor_id):
    cb_session = requests.session()
    url = "%s/api/v1/sensor/%s" % (server, sensor_id)
    headers = {'X-Auth-Token':token}
    sensor_response = cb_session.get(url, headers=headers, verify=False)
    data = sensor_response.json()
    data["network_isolation_enabled"]=True
    r = cb_session.put(url, headers=headers, verify=False, data=json.dumps(data), timeout=120)
    r.raise_for_status()
    # Note that a 204 response indicates that everything is okay
    return r.status_code == 204
```








# The Work – Install The Alert Action

## Install the alert action on to Splunk HEC receiver

- Build it in an App
- Need THREE parts
  - Python Script (in <app>/bin/
  - Alert\_actions.conf (in <app>/default/)
  - App.conf (in <app>/default/)
  - Optional png File to make it pretty
    - Located <app>/appserver/static/

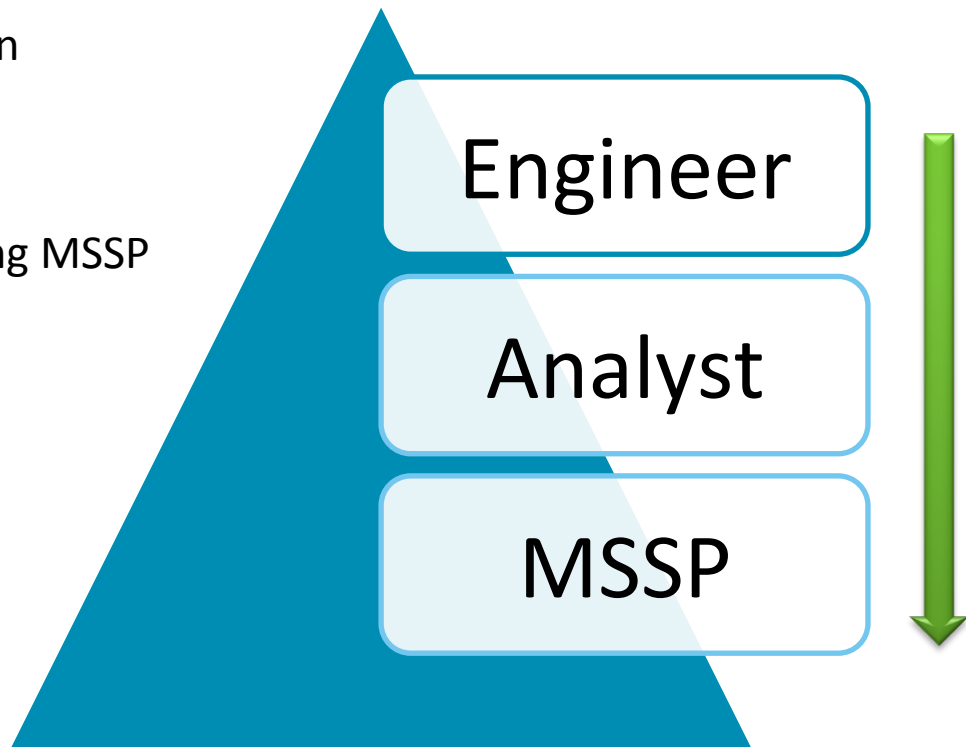


The screenshot shows the Splunk web interface for managing alert actions. The page title is "Alert Actions" with the subtitle "Review and manage available alert actions". There is a search filter box. Below is a table listing several alert actions with their respective app names, sharing settings, status, usage statistics, and log links.

Alert action	App	Sharing	Status	Usage	Log
 Carbon Black System Quarantine Quarantine a system by IP address or hostname	cb_arf_app	Global   <a href="#">Permissions</a>	Enabled   <a href="#">Disable</a>	<a href="#">Usage statistics</a>	<a href="#">View log events</a>
 Log Event Send log event to Splunk receiver endpoint	alert_logevent	Global   <a href="#">Permissions</a>	Enabled   <a href="#">Disable</a>	<a href="#">Usage statistics</a>	<a href="#">View log events</a>
 Run a script Invoke a custom script	system	Global   <a href="#">Permissions</a>	Enabled   <a href="#">Disable</a>		
 Send email Send an email notification to specified recipients	system	Global   <a href="#">Permissions</a>	Enabled   <a href="#">Disable</a>		
 Webhook Generic HTTP POST to a specified URL	alert_webhook	Global   <a href="#">Permissions</a>	Enabled   <a href="#">Disable</a>	<a href="#">Usage statistics</a>	<a href="#">View log events</a>

# Why Did We Do It

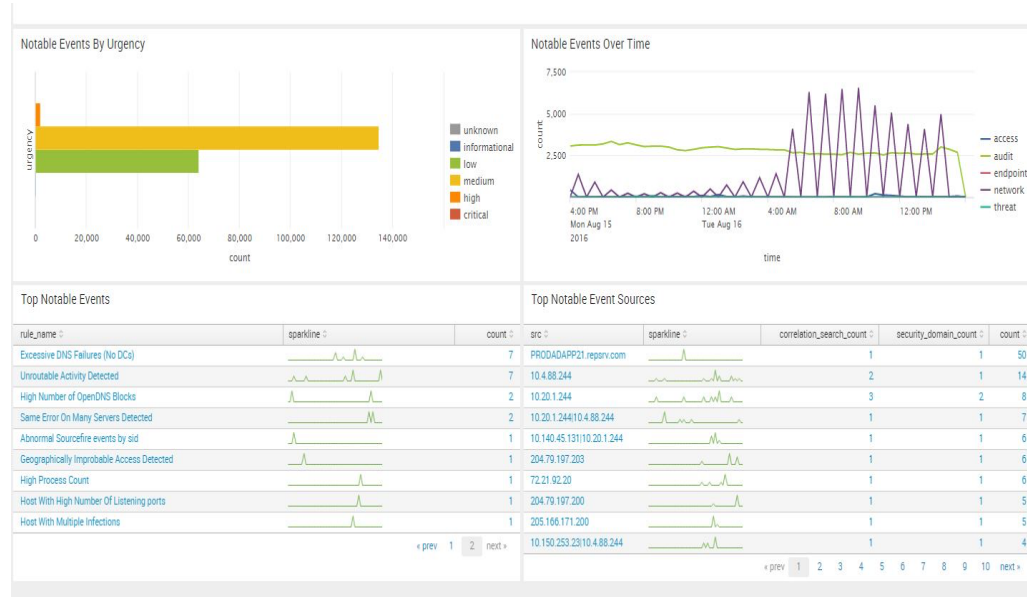
- Reduce the time to interrupt the kill chain
- Drive towards automation and security orchestration
- Empower security analysts and supporting MSSP
- BECAUSE IT WAS COOL TO DO



# MSSP / Security Analyst Work Flow

## Splunk Enterprise Security – Notable Security Events

- Analysts will see these in the Notable Events Overview Dashboard



# MSSP / Security Analyst Work Flow

## Splunk Enterprise Security – Notable Security Events

- Analysts will Click on Notable Events like:
  - Host with Multiple Infections
  - Using the Action for Host the Analyst now has “Quarantine CB Sensor at: \$Host\$”

The screenshot displays the Splunk Enterprise Security interface. At the top, there are filters for severity levels: MEDIUM (0), LOW (0), and INFO (0). Below these are search filters for Security Domain (set to 'All'), a date time range, and a Tag field. A 'Submit' button is visible. The main content area shows a table of events. The selected event is titled 'Host With Multiple Infections (PC05EJW)' and is categorized as 'High' urgency and 'Closed' status. The event details include a description: 'The device PC05EJW was detected with multiple (2) infections.' and a list of 'Additional Fields' with their values. An 'Action' menu is open, showing options like 'Edit Tags', 'Access Search (as destination)', 'Access Search (as source)', 'Asset Center', 'Asset Investigator', 'Search Carbonblack Events', 'Quarantine CB sensor at: PC05EJW', 'Domain Dossier', 'Map PC05EJW', and 'Google PC05EJW'. The 'Quarantine CB sensor at: PC05EJW' option is highlighted. The interface also shows a 'Correlation Search' section and a 'History' section.

# MSSP / Security Analyst Work Flow

## Splunk Enterprise Security – Notable Security Events

- Analysts will receive Confirmation
- Validation of the Entity
- History of Incident Details

The screenshot displays the Splunk Enterprise Security interface. The top navigation bar includes 'splunk>', 'App: Enterprise Security', 'Messages', 'Settings', 'Activity', and a search bar. Below the navigation, there are tabs for 'Security Posture', 'Incident Review', 'My Investigations', 'Advanced Threat', 'Security Domains', 'Audit', 'Search', and 'Configure'. The main content area is titled 'Carbon Black Isolation Details' and shows the host 'PC05E9JW' and event ID 'BSA90FB4-D1C9-42DE-B7D0-178C319'. A dropdown menu is set to 'Last 24 hours'. The 'Entity Being Isolated' section prominently displays 'PC05E9JW'. Below this, the 'Incident Details' section contains a table with the following data:

_time	rule_id	reviewer	urgency	status	owner	comment
2016-08-16 09:04:47.850	BSA90FB4-D1C9-42DE-B7D0-178C319F62C2@notable@48e8793959373d76b5efedc0fd96fb6	mmartin	informational	Closed	mmartin	SEP cleaned the files. No further action required.
2016-08-16 16:02:37.324	BSA90FB4-D1C9-42DE-B7D0-178C319F62C2@notable@48e8793959373d76b5efedc0fd96fb6	phelley@republicservices.com	high	Closed	mmartin	

# How You Can Do It, Too!

1. Identify your technology that can be leveraged similarly (e.g., MacAfee IPS/FW, Symantec FW, Carbon Black - because we have the Bytes for you, or others).
2. Download the app we have created using Splunk HEC and follow the instructions to leverage it yourself.
3. Share your story.
  1. Splunk blogs, YouTube or anywhere else someone can learn about your experience
  2. Leverage hosted events - User groups, SplunkLive, .Conf etc.



# What's Next?

Taking the Same Approach with Other technologies



# THANK YOU

.conf2016

