Burning Down the Haystack

Tim Frazier
Senior Security Engineer
tfrazier@splunk.com
Professional History

- EE, Army Comms + Cisco Networking background
- Transitioned to InfoSec after breaking things and seeing how important it is to build them right
- Worked in Security Operations in DoD and Electricity Sector industries
- Engineered, installed, configured, managed SOC toolsets and infrastructure
- Built Python Scripts to automate repetitive security operations/administration tasks – integrated with the APIs for Vuln Mgmt, Intelligent Taps, and IP Mgmt Tools
- Currently focused on helping organizations automate their processes
- CISSP and GICSP certified (If you care…)
The Haystack
So what do we do?

1. We could hire more people:

Good luck with that.
So what do we do?

2. More/better tools?

Detection is an ongoing arms race, but signal to noise ratio is usually a problem.
So what do we do?

3. Better Process(es)

Of course we need this, but it’s not quite enough.

Every org has their own process that has to be a bit different – kind of like opinions.
It’s time for something… “New”?

Automation - It’s been around for some time, just hasn’t been leveraged in Sec Ops as much as it should.

Security Automation & Orchestration:
- The glue between the myriad of tools
- The machine speed process driver
What is “Security Automation & Orchestration”?  

Definitions:  
**Security Automation**  
- *Machine-based execution* of one or more security actions.

**Security Orchestration**  
- *Machine-based coordination* of security actions *across a complex infrastructure*.

What SA&O is NOT:  
- Replacement for Human Analysts  
- Silver Bullet / Unicorn  
- MOAR blinky lights
Not a replacement for human analysts, you say?

David Autor:

**Will automation take away all our jobs?**

[TEDxCambridge](https://www.ted.com/talks/david_autor_why_are_there_still_so_many_jobs) • 18:37 • Filmed Sep 2016

- 18 subtitle languages 📚
- View interactive transcript 🎯
Automating More of Security Operations

Point Products (Observe / Sensing)
- FIREWALL
- IDS / IPS
- ENDPOINT
- WAF
- ADVANCED MALWARE
- FORENSICS
- MALWARE DETONATION

Analytics (Orient / Sense-making)
- SIEM
- THREAT INTEL PLATFORM
- HADOOP
- GRC

Decision Making
- TIER 1
- TIER 2
- TIER 3

Acting
- FIREWALL
- IDS / IPS
- ENDPOINT
- WAF
- ADVANCED MALWARE
- FORENSICS
- MALWARE DETONATION

AUTOMATED
MANUAL (TODAY)
Best Practices – field tested

• How do we Burn down the haystack!?!?
  • Start with the end goal in mind – Stop spear phishing? Remediate malware?
  • Identify the scenarios - Where do you spend the bulk of your time?
  • Then, what steps are taken
    – follow the white rabbit!

• To the White Board!
Best Practices – Field tested

• Once identified → Document and diagram
  • Be sure the steps and decisions at each point match what you have laid out
  • As your walking through the whiteboard, determine the time spent for the analyst on each step
  • How many times is this scenario carried out on average per day?
Best Practices – Field tested

- The results? Playbooks! (workflows of actions)
Getting Started

Ingredients List:

• 1-2 - Repetitive processes to automate (peeled)
• 1 (or 20) Cans - Security Tools with APIs + API docs!
• 2 Cups - Scripting Knowledge – Python, “requests” module, data management, web service

• (Optional) Automation & Orchestration platform (Free community editions available)
  • Rapidly accelerates time to value
  • Reduces required scripting knowledge
  • Provides the required low-level plumbing to facilitate Security Automation & Orchestration (SA&O)
Success Stories!

Great examples of Security Automation & Orchestration to follow…
Success Story: MSSP Security Event Triage

Automating common triage actions
Leveraged common actions + custom code

Series of 3 Playbooks
- Finding/correlating tickets OR create ticket
- Running SIEM Query & Reputation actions
- Updating ticket (w/ csv of query results)
- Save 3-5 minutes per event (x100s per day)

```python
def update_ticket_1(action=None, success=None, container=None, datapath=None):
    phantom.debug("Data of interest: \n")
    phantom.debug("Finding ticket \n")
    phantom.debug("Container: \n")
    tmpFilename = "/vault/tmp/data_for_Offense " + container["source_data_identifier"] + ".json"
    with open(tmpFilename, 'w') as tmpFile:
        for data_item in data_of_interest:
            if data_item[0] or data_item[1]:
                tmpFile.write(json.dumps(data_item))
        tmpFile.close()
    file_added_to_vault = phantom.Vault.add_attachment(tmpFilename, container_id=container["id"])
    phantom.debug("File added to vault: ")
    phantom.debug(file_added_to_vault)
    handle_file_added_to_vault["vault_id"]
    parameters = []
    ticket_id = ""
    for data_item in data_of_interest:
        if data_item[1]:
            ticket_id = data_item[2]
    # build parameters list for 'update_ticket_1' call
    ...
Success Story: Software Co. Phishing Email Triage

Ingested Email and performed reputation actions on artifacts

Based on results of reputation actions:
• Got mobile approval through use of ”Duo”
• After approval, implemented countermeasures
  • Blocking hashes using FireAMP
  • Blocking Domains using OpenDNS
Send an email to internal address
• Monitor mailbox and performs blocking actions on domains (minus whitelist)
• Sends email to appropriate parties and resolves event
Success Story: Financial Co. Hash Hunting

Started with Hashes
- Hunted using an endpoint platform with limited containment API
- Performed chained investigative actions for further detail
- Used direct communication to endpoint to delete the file from the endpoint
Success Story: Retail Co. Phishing Email Analysis

- Monitored mailbox was also receiving results from PhishMe Triage
- URL mangling resulted in inaccurate parsing of emails
- Used custom code to extract URLs and Domains
- Kicked off custom playbook
- Automated escalation and notification process

- 100-500 emails/day
- 8-40 hours/day savings
Success Story: Retail Co. Alert Suppression

- Received numerous duplicate / similar alerts – didn’t want to disable at SIEM
- First checked for same / similar named events in connected database
- Set thresholds for number of events in certain time period
- Promoted to a case after threshold and appended following events

```python
def Check_exist existing_container s(action=None, success=None, container=None, results=None, handle=None, filtered=None):
    phantom.debug('Check_exis ting_container s() called')

    name_value = container.get('name', None).split(' at ')
    compare_date = datetime.strptime(name_value[1].split('.')[0], '%Y-%m-%dT%H:%M:%S')
    phantom.debug(compare_date)

    url = 'https://127.0.0.1/rest/container?filter_name__icontains={0}'"&page size=0'.format(name_value[0])
    phantom.debug(url)

    r = requests.get(url, verify=False)
    phantom.debug(r.text)

    filtered_containers = []

    resp_json = r.json()
    for each in resp_json["data"]:
        each_date = datetime.strptime(each["name"] .split(' at ')[1].split('.')[0], '%Y-%m-%dT%H:%M:%S')
        phantom.debug(each_date)
        if each_date > (compare_date - timedelta(hours=24)):
            filtered_containers.append(each)
            phantom.debug(each["id"])  
            phantom.debug(each["container_type"])
            if each["container type"] == "case" and each["status"] == "closed":
                phantom.merge(case=each["id"], container_id=container["id"])
                phantom.close(container)
```
Success Story: Large Bank Alert Suppression

• Wanted to fire an alert once if conditions met, then suppress for 24 hours
• Queried SIEM once a minute to check for conditions
  • If conditions met, add the username/email to a custom list for 24 hours.
  • Playbook checked the list for existing matches before firing alert to achieve suppression
Success Story: Large Bank Malware Repo

- Wanted to check intel file hashes against their 2 AV engines through VT
- If their AV didn’t detect, they would download file and send to AV vendor for adding
  - This playbook also incorporated action caching to prevent license overuse
  - 7 day threshold, reputation checks, request VT rescan
Success Story: Public School System Alert Triage

- Received numerous alert types via email into a central mailbox
- Parsed key words in the subject to appropriately tag alerts
  - Used object oriented playbook writing to nest follow on playbooks for proper response
- Handled variety of alerts in a methodical, documented, detailed fashion
Success Story: Public School System Alerts

- Alerts into email box handled from end-to-end
- Through series of playbooks, majority of various alerts received into centralized mailbox are automatically addressed and closed
Success Story: Healthcare Co. #1 Phishing Investigations

- Started with emails in abuse box – filtered out several preconditions
- Checked a whitelist, detonated URLs and files, updated events and notified if above thresholds
Success Story: Healthcare Co. #2 Phishing Investigations

- Started with emails in abuse box – checked to ensure email was attached
- Performed reputation actions, SIEM queries, then escalated and responded as necessary
Success Story: Logistics Company Email Purge

- Constantly suffered Phishing attacks and needed to purge emails from O365
- Leveraged WinRM, Powershell and O365 Sec & Compliance center to kick off purge
  - Started either from email detection tool alerts or on demand
Success Story: Insurance Co. Registry Key Investigations

- SIEM alerts for registry run key added
- Initiate file acquisition, get file, detonate in sandbox, get report and then update SIEM event
Success Story: Insurance Co. Threat Activity

- SIEM alerts for activity matching an IOC – IP address, domain, etc.
- Kick off SIEM queries, detonate matching URLs from proxy logs
- Update events and escalated if sandbox report thresholds exceeded
Key Takeaways

• SAO saves you time – reduces noisy hay by triaging and closing automatically

• SAO makes your job less boring – less cut & paste and 16 browser tabs open at once

• SAO reduces risk to your organization by freeing you up to focus on what matters

• Think about:
  • “What is the process that I need to automate?”
  • Really drill down into the details

• Next Steps:
  • Scripting with APIs
Connect

Tim Frazier
Senior Security Engineer
tfrazier@splunk.com
@timfrazier1

Register, and download the Phantom platform for free!
https://www.phantom.us