Automating Malware Sandbox Analysis With Splunk

The accelerated Incident Response

Nick Crofts | Senior Security SME
Shafqat Mehmood – Manager Information Security Operations

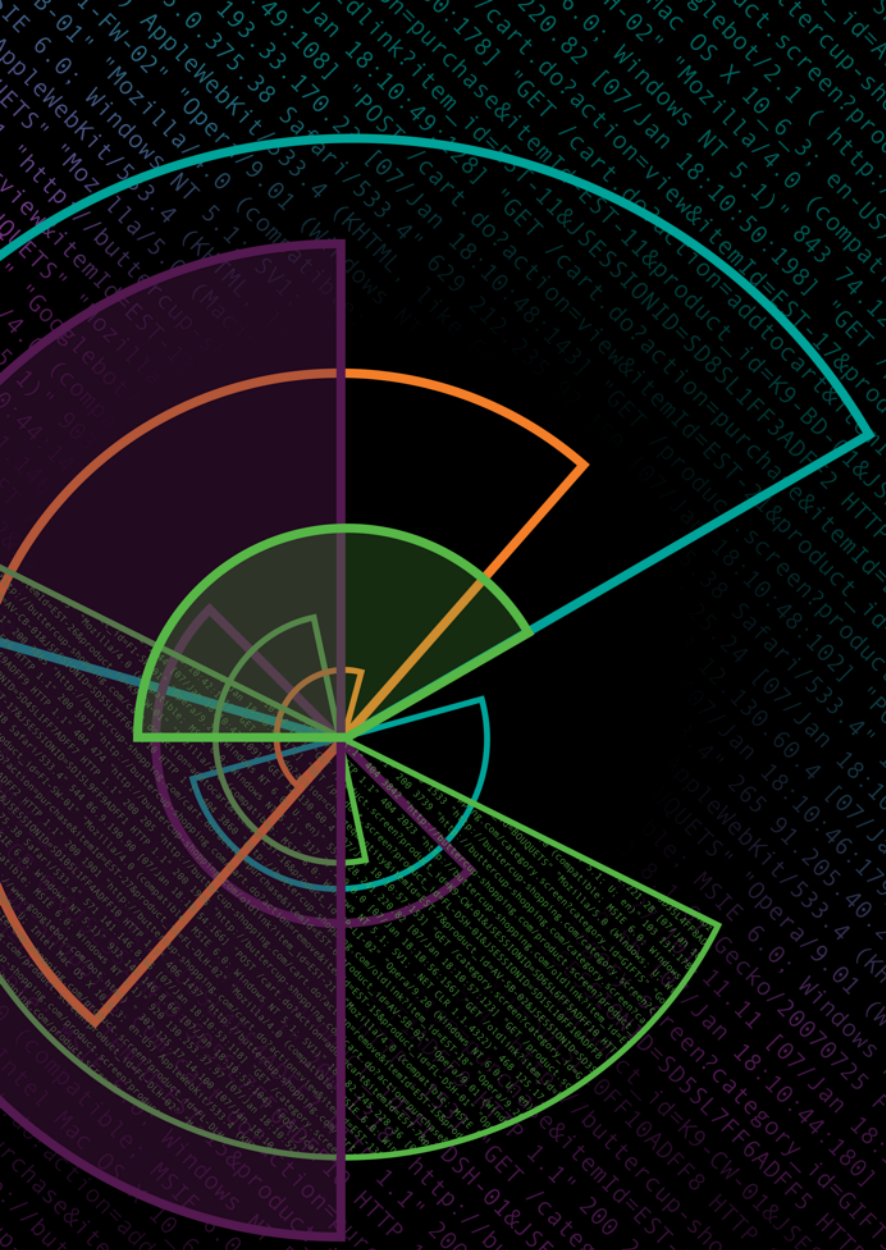
October 2018 | Version 2.0

Forward-Looking Statements

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 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.

splunk> .conf18



Who Are We?

Nick and Shaf

splunk> .conf18

Who is Nick?

Senior Security SME @Splunk (Melbourne Australia)

- Education
  - BS in Business Systems – Monash University
  - CISSP, CCNA, MCP
- Background
  - Sales Engineer last 4 years, Splunk & RSA
  - Security Engineer 10 years, SOC @ small MSSP
- Hobbies
  - Snowboarding
  - Long distance Running
  - Keeping fit
  - DLT / Blockchain / Cryptocurrencies

Who is Shaf?

Manager Information Security Operations @ KPMG (Australia)

- Education
  - PhD-(in progress) Artificial Intelligence
  - Advance Computer Security Certificate (Stanford University)
  - Over 25 professional certifications
- Background
  - Manager SOC last 3 years, KPMG
  - Security Operations Specialist 10 years, SOC @ Big 4's
  - Malware researcher
- Hobbies
  - Aeromodelling / Blockchain / Crypto currencies
  - Cycling
  - AI Research

Agenda

Going Cuckoo with Malware Analysis

- Problem
- Before Splunk & Cuckoo / After Splunk & Cuckoo
- Cuckoo Sandbox
- Splunk Stream
  - Stream 7.1, File Extraction
- Phantom Orchestration
- Use Cases
  - Using Stream
  - Symantec Endpoint Protection
- Demo
- Questions

Problem

Lack of open source malware analysis

No in-house threat intelligence

Inefficient incident response

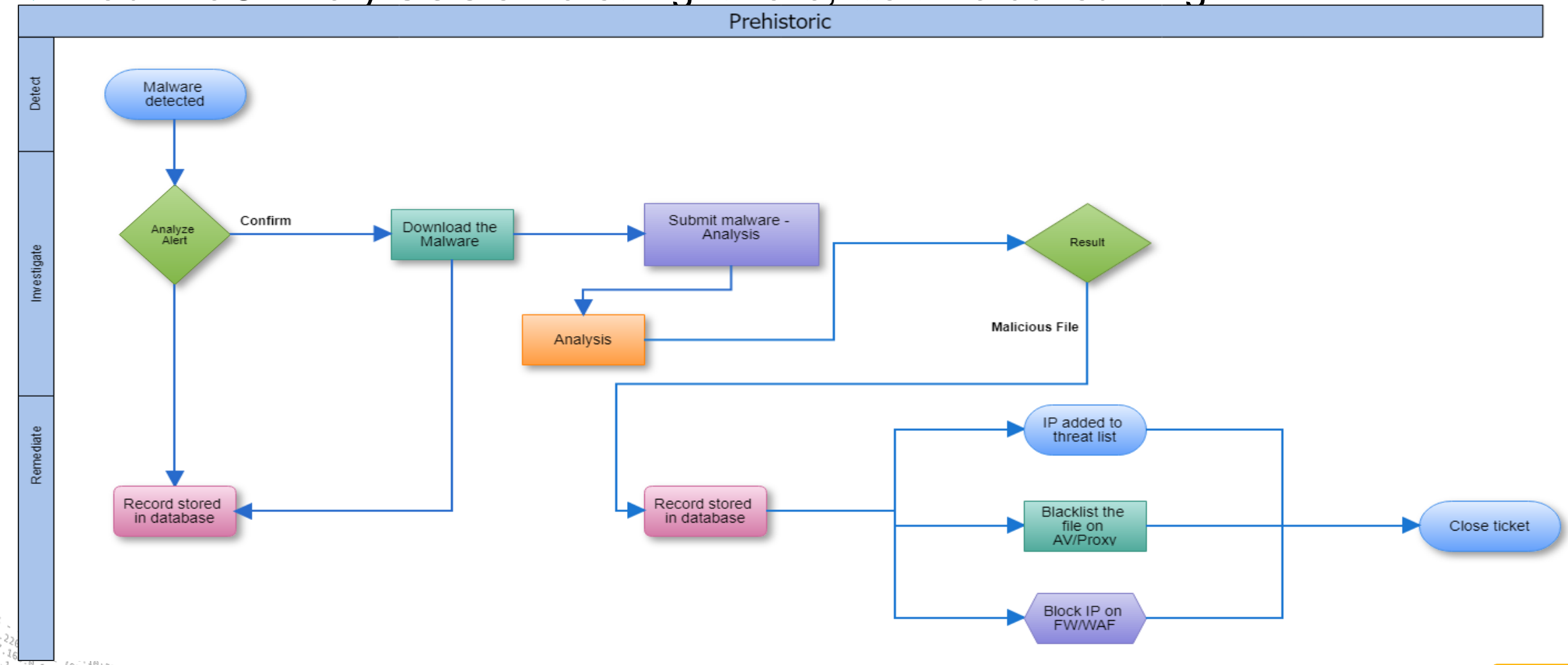
Problem

- Open Source malware analysis
  - Lack off in house malware analysis capability
  - Skill deficiency
  - Management support - $$
  - Company privacy policies
- In-House Threat Intelligence
  - Inefficient threat management
  - Time consuming – manual threat feed/IOC enrichment
  - Ongoing staff education and engagement
- -Incident Response
  - People, process, technology and information.
  - Preparedness, response and follow up activities.
- Current State
  - Manual process of collecting
  - submitting and analyzing suspicious file samples.
- Ideal end state
  - Automated: using stream, cuckoo and Splunk.

Before Splunk-Cuckoo

Incident Flow

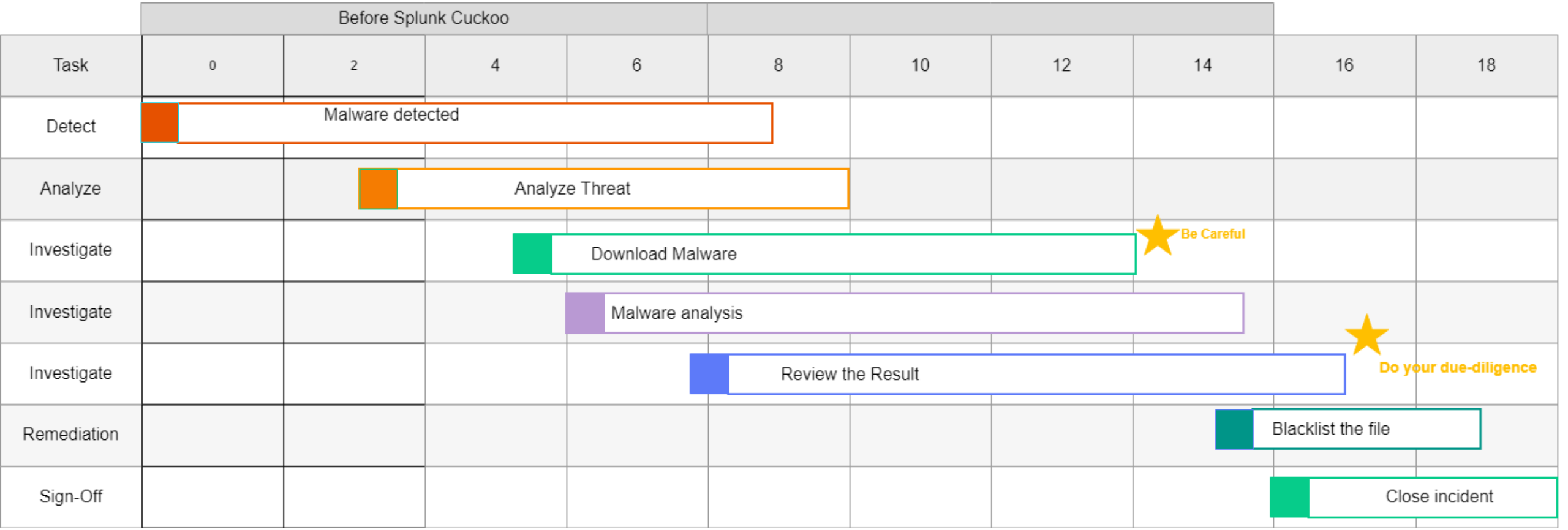
- Bad File☹ Every SOC's worst nightmare, it's time consuming!



Before Splunk Cuckoo

Time Line: Ave Response**18 hours**

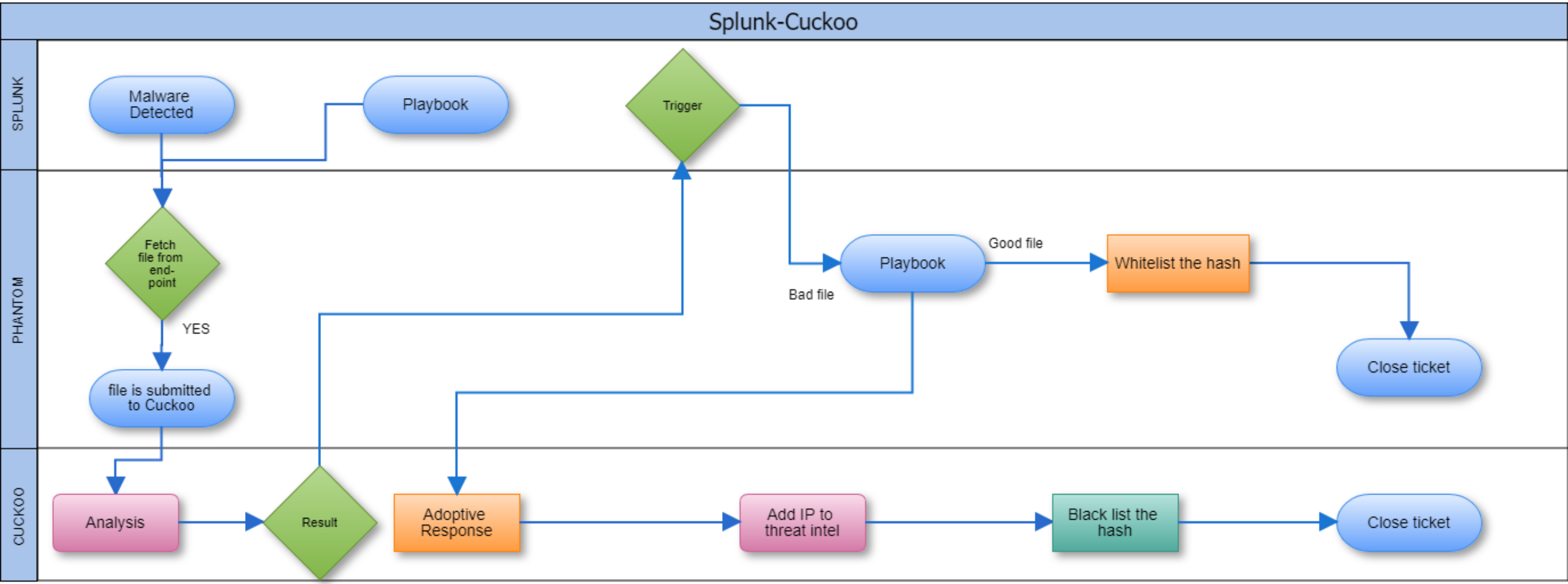
- Use case 1: Bad File. Every SOC's worst nightmare, it's time consuming!



After Splunk-Cuckoo

What's the response time?

- Welcome to Cuckoo Land



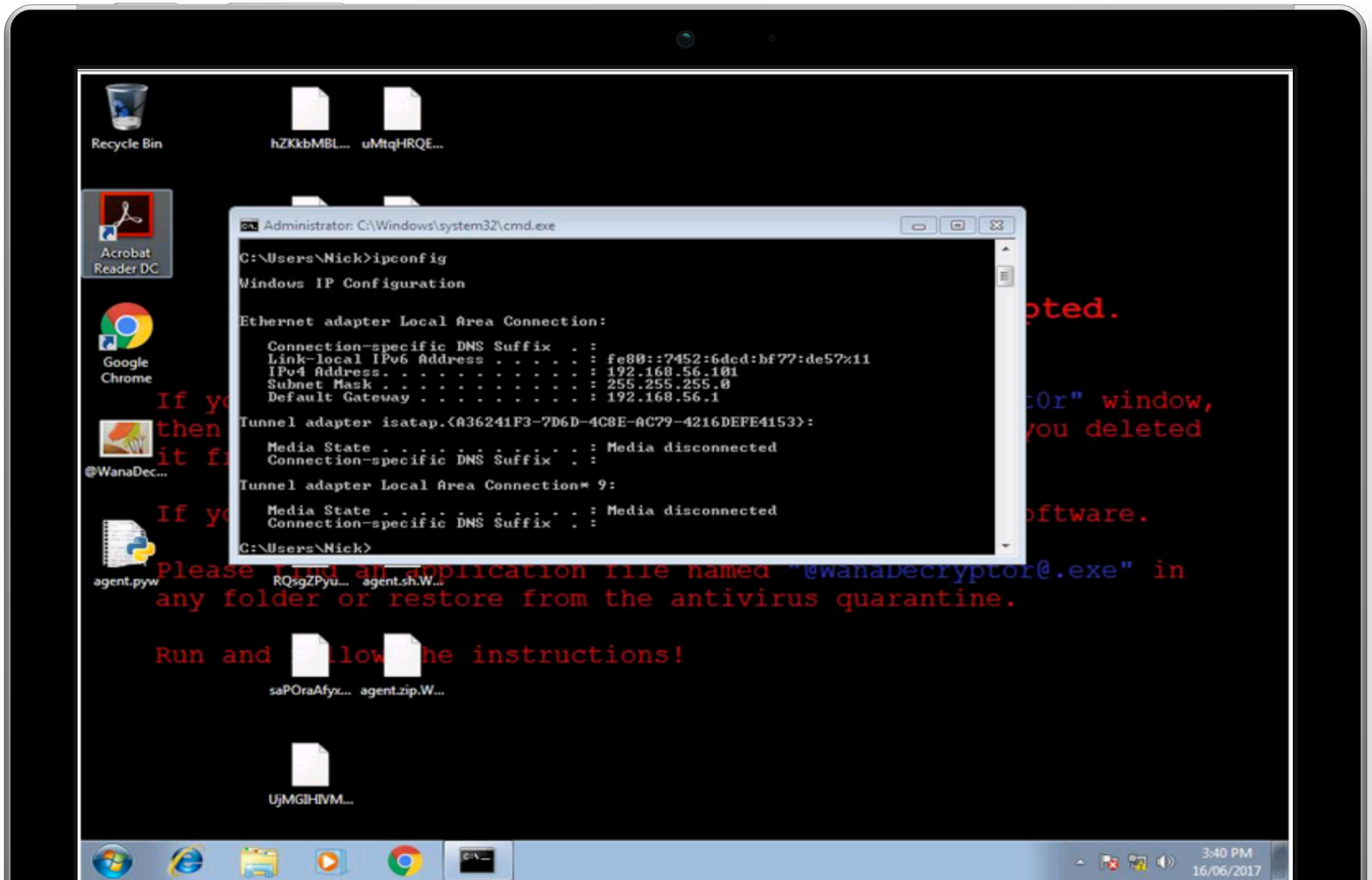
Components of Solution

Going Cuckoo with Malware Analysis

- Cuckoo
- Splunk Stream
- Phantom

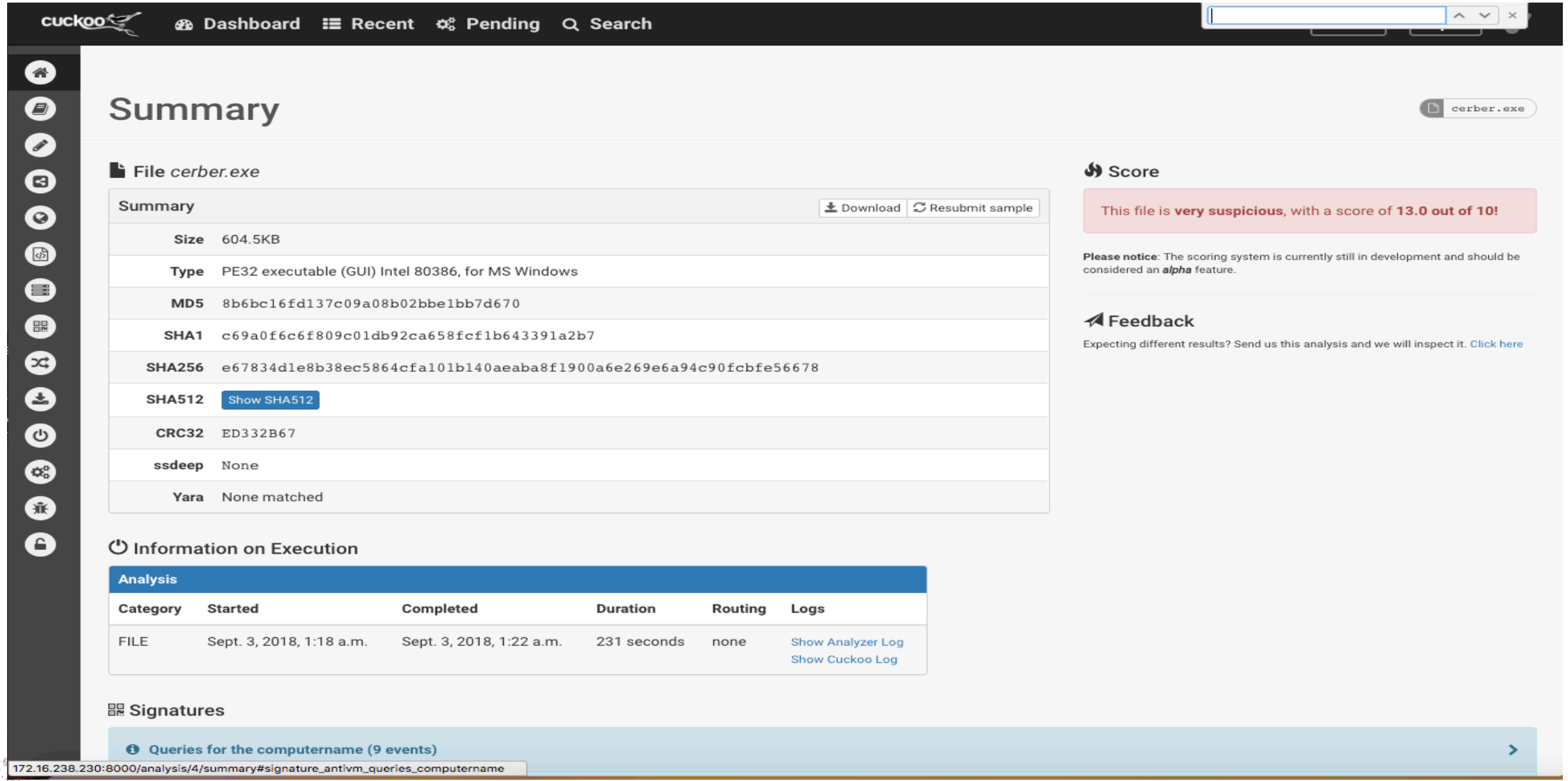
Cuckoo?

Cuckoo is an open source automated malware analysis system



- It can record the following results
  - Take memory dumps of malware processes
  - Network traffic traces
  - Take screenshots during execution
  - Track files created, deleted, downloaded or encrypted

splunk> .conf2017



splunk> .conf18

splunk> .conf18

Cuckoo – Let's Configure

Some tips for setting up Cuckoo

- Centos Desktop Server with Cuckoo installed
  - Virtualbox needs for guests. Latest versions do not like AWS so easier to test on a physical machine.
- Windows 7 and Windows 10 Guests
- Splunk and Cuckoo on same box originally
  - Both use Port 8000!
- Use isolated networks for testing!
- Malware samples downloaded from malware zoo to test. Careful, real malware here!
  - https://github.com/ytisf/theZoo
- One of the best guides for setting up cuckoo. Covers Masquerading guests, packages needed, virtualbox config and tcpdump permissions
  - https://blog.nviso.be/2018/04/12/painless-cuckoo-sandbox-installation/

Splunk Stream

splunk> .conf18

Deploy, Collect & Monitor Data with Stream

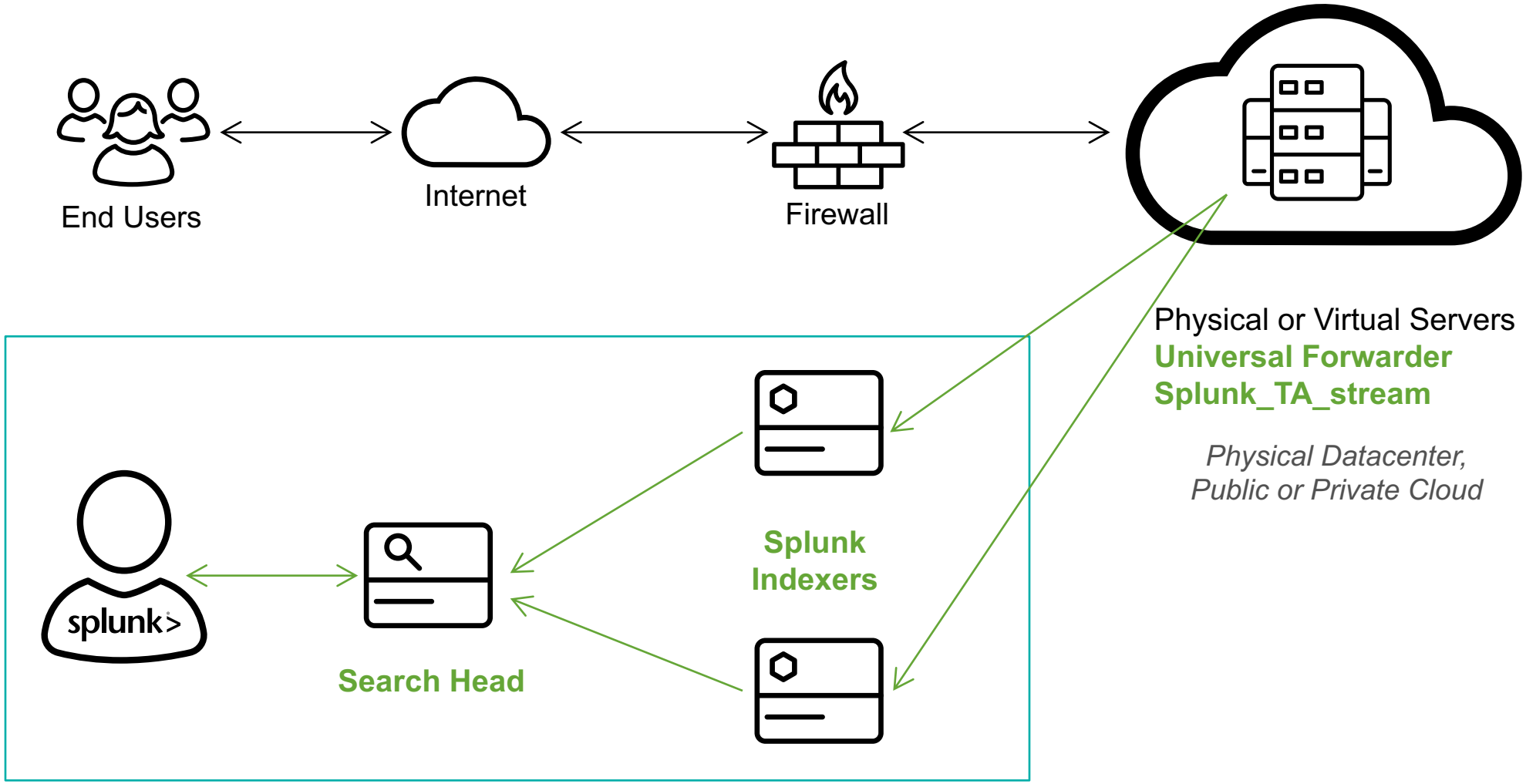
STM

Stream has two deployment architectures and two collection methodologies

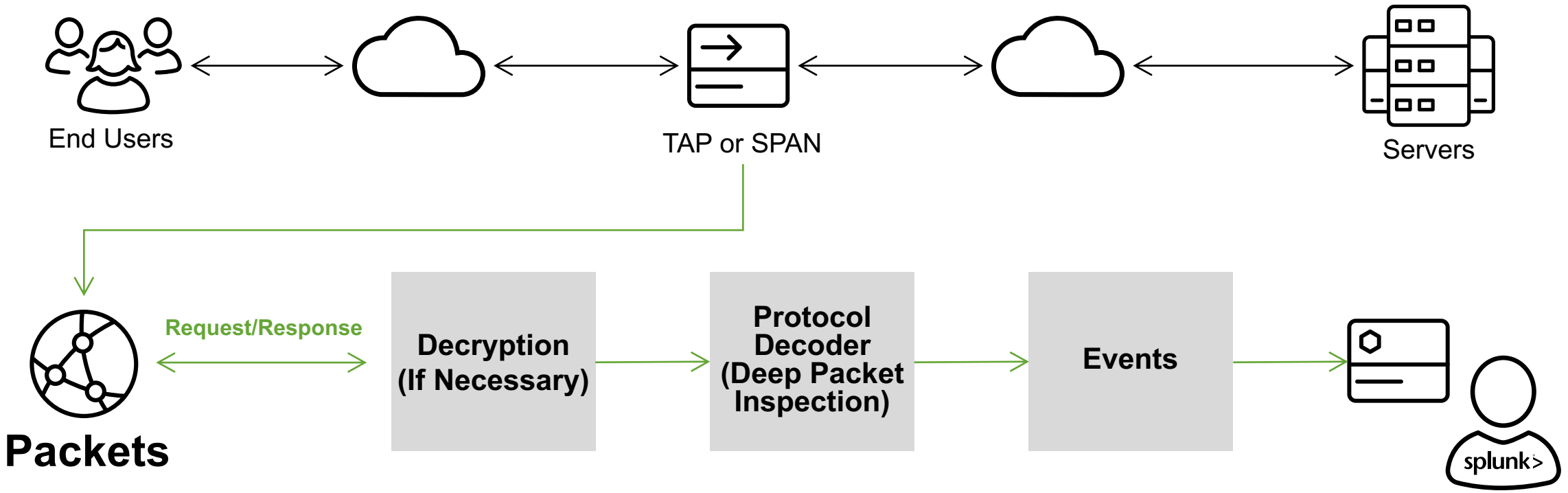
- **Deployment: (Production)**
  - Out-of-band (stub) with tap or SPAN port
  - In-line directly on monitored host
- **Collection: (Lab)**
  - Technical Add-On (TA) with Splunk Universal Forwarder (UF)
  - Independent Stream Forwarder using HTTP Event Collector (HEC)

- **New Content Extraction Types (7.0)**
  - MD5 Hash: Automatic Hashing for files over HTTP and SMTP
- **Targeted Packet Capture**
  - Supports capture of full network packets
- **File Extraction for metadata Streams**
  - Extract Content files from network
  - SMTP and HTTP protocols
  - Download files for analysis

Deployment: Run on Servers (Lab Method)



Wire Data Collection/Metadata Generation



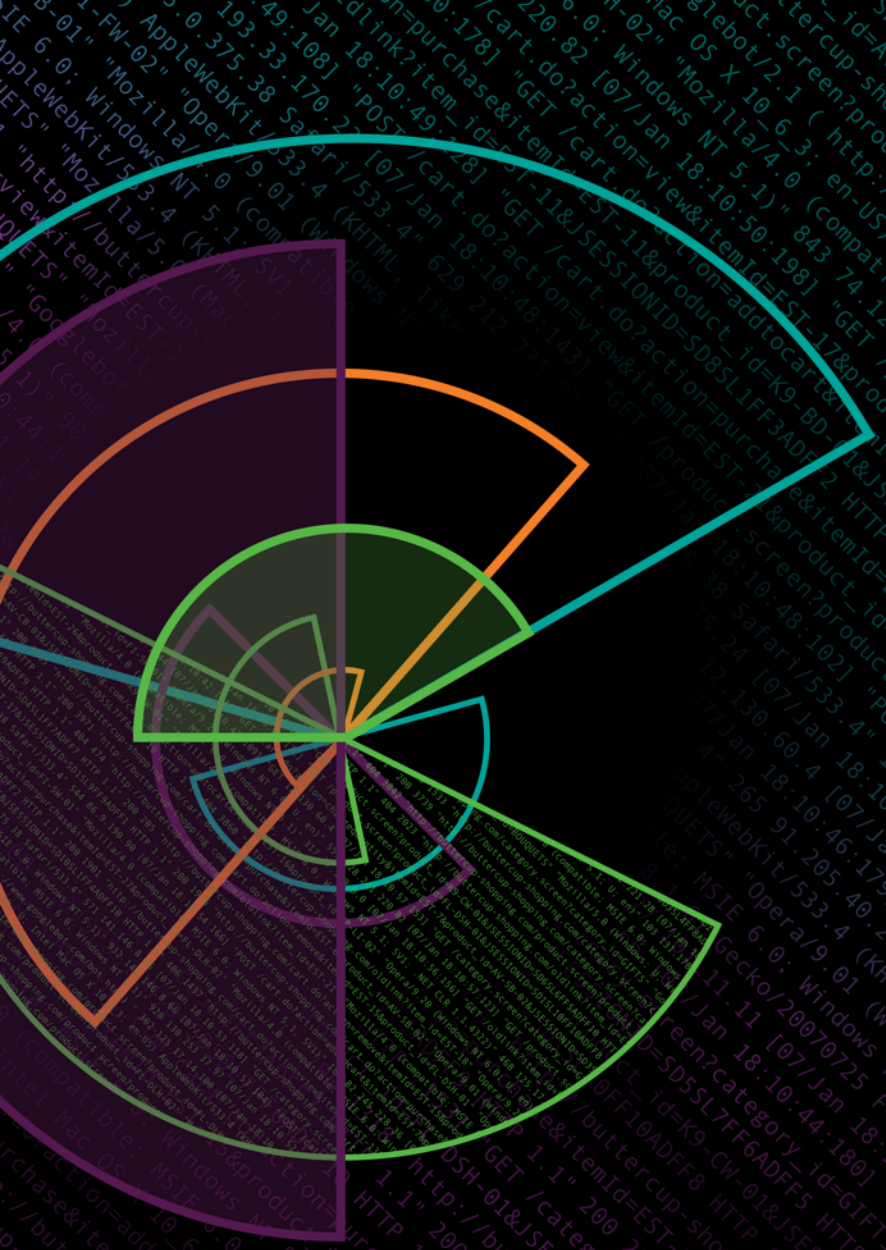
File Extraction - Stream

- Extracts Payloads from Network Traffic
- HTTP, HTTPS (With decryption) and SMTP
- Files are saved locally or to an NFS File share
- File name is a bit odd, but easy enough to find using Splunk Search

```
index=main "extracted_file{}"=* "extracted_file{}"=eb574b236133e60c989c6f472f07827b
| rename "extracted_file{}" as file_name
| rex field=flow_id "(?<first>..)(?<second>..)(?<rest>.*)"
| eval file_path= "/opt/splunk/packets/".capture_bucket_date."/".first."/".second."/".rest."/".file_name
```

file_path	first	second	rest	flow_id	file_name
/opt/splunk/packets/20180722/04/d7/61bd-4b65-42ad-b715-b63487858d27/eb574b236133e60c989c6f472f07827b	04	d7	61bd-4b65-42ad-b715-b63487858d27	04d761bd-4b65-42ad-b715-b63487858d27	eb574b236133e60c989c6f472f07827b

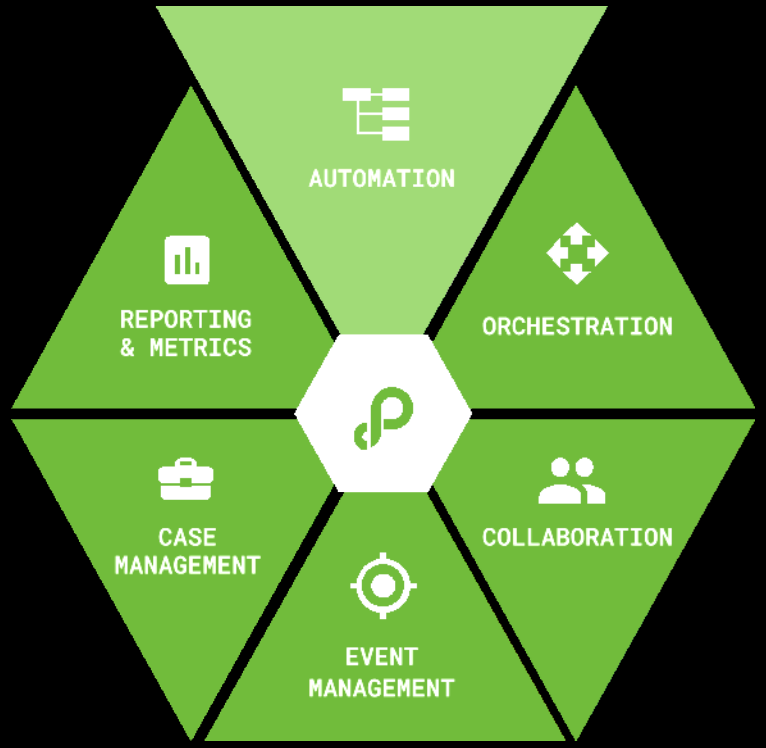
splunk> .conf18



Phantom

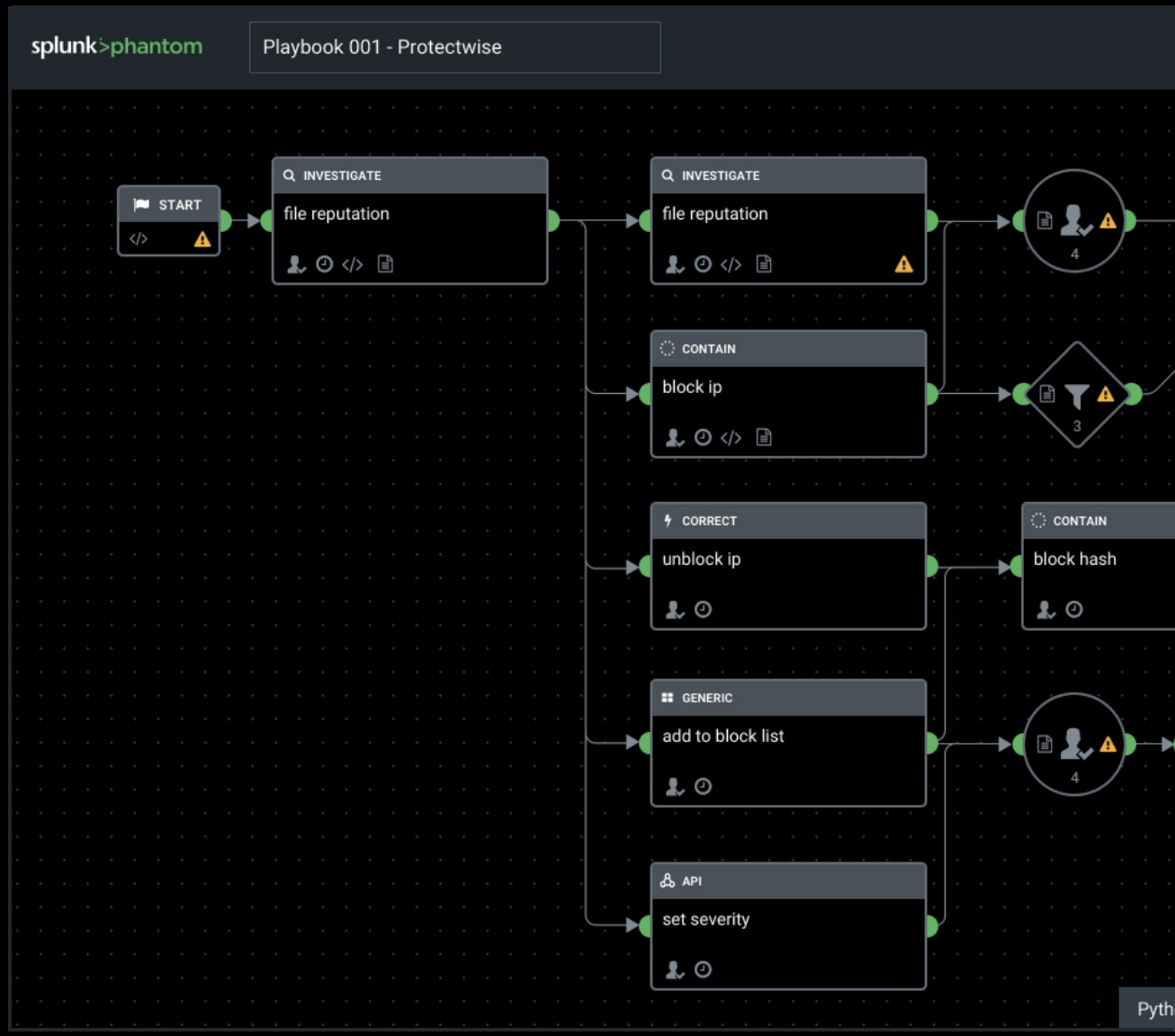
How it saved us time

splunk> .conf18

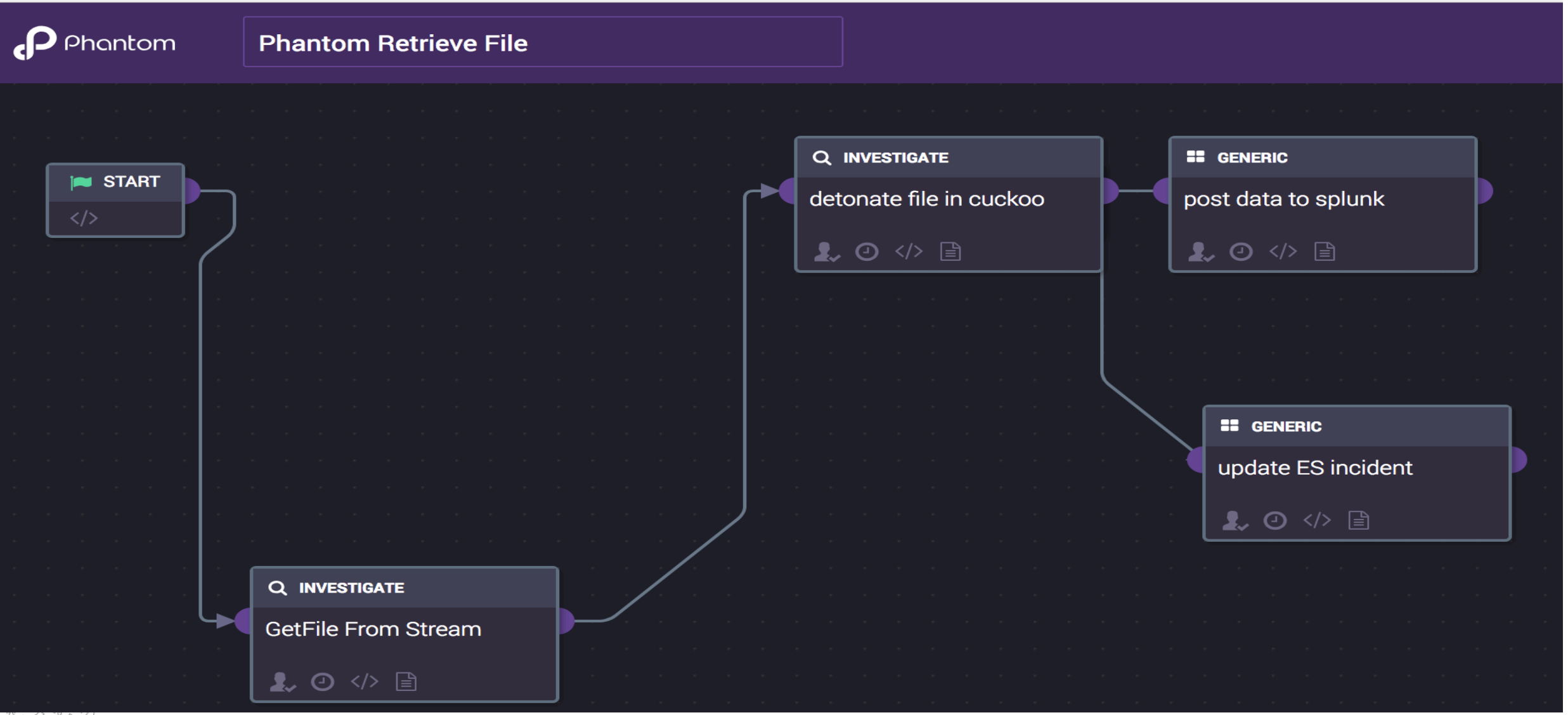


Automation

- Automate repetitive tasks to force multiply team efforts.
- Execute automated actions in seconds versus hours.
- Pre-fetch intelligence to support decision making.

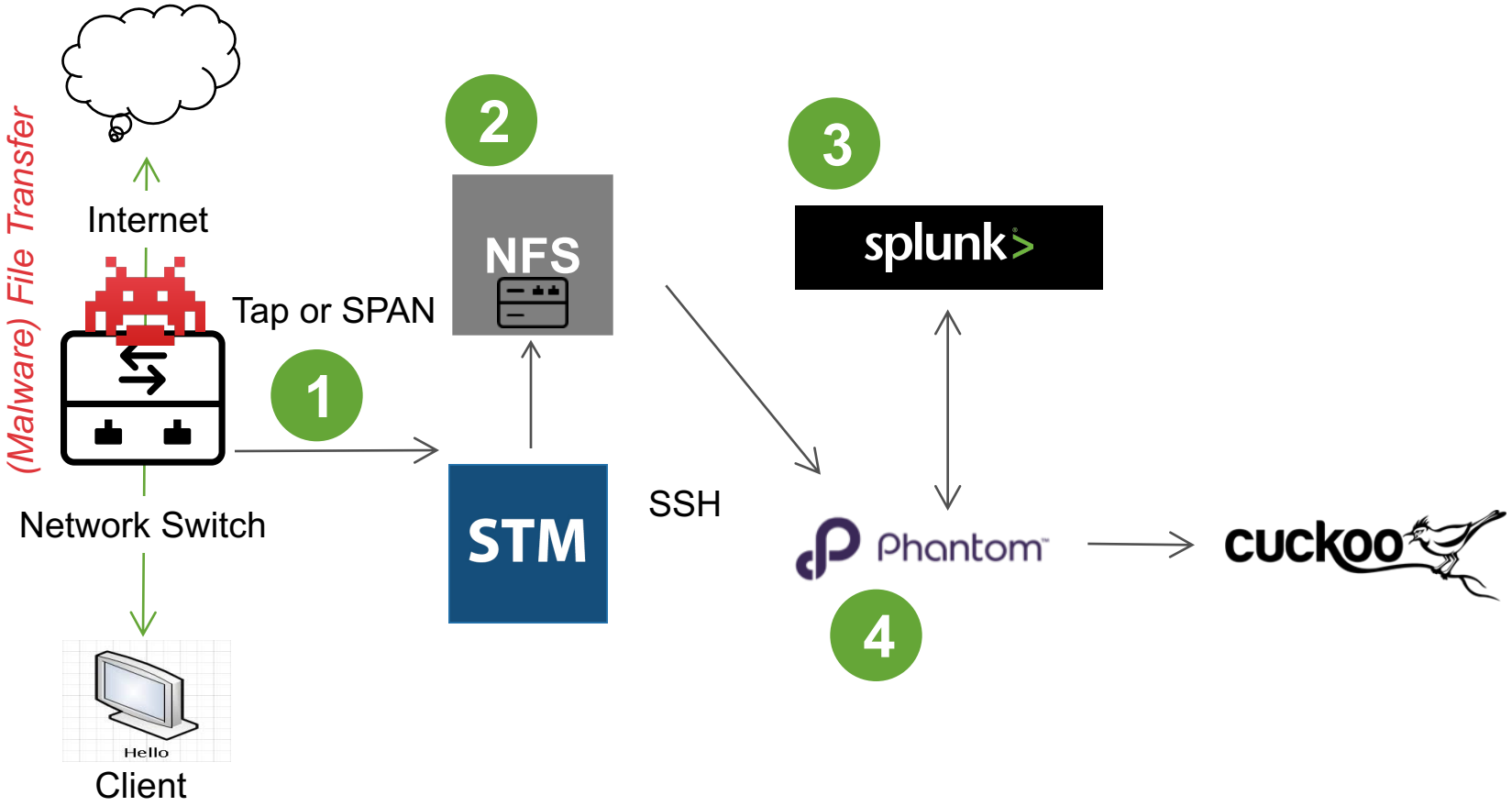


Phantom Playbook



Solution Overview

Splunk Stream - Cuckoo Malware Sandbox

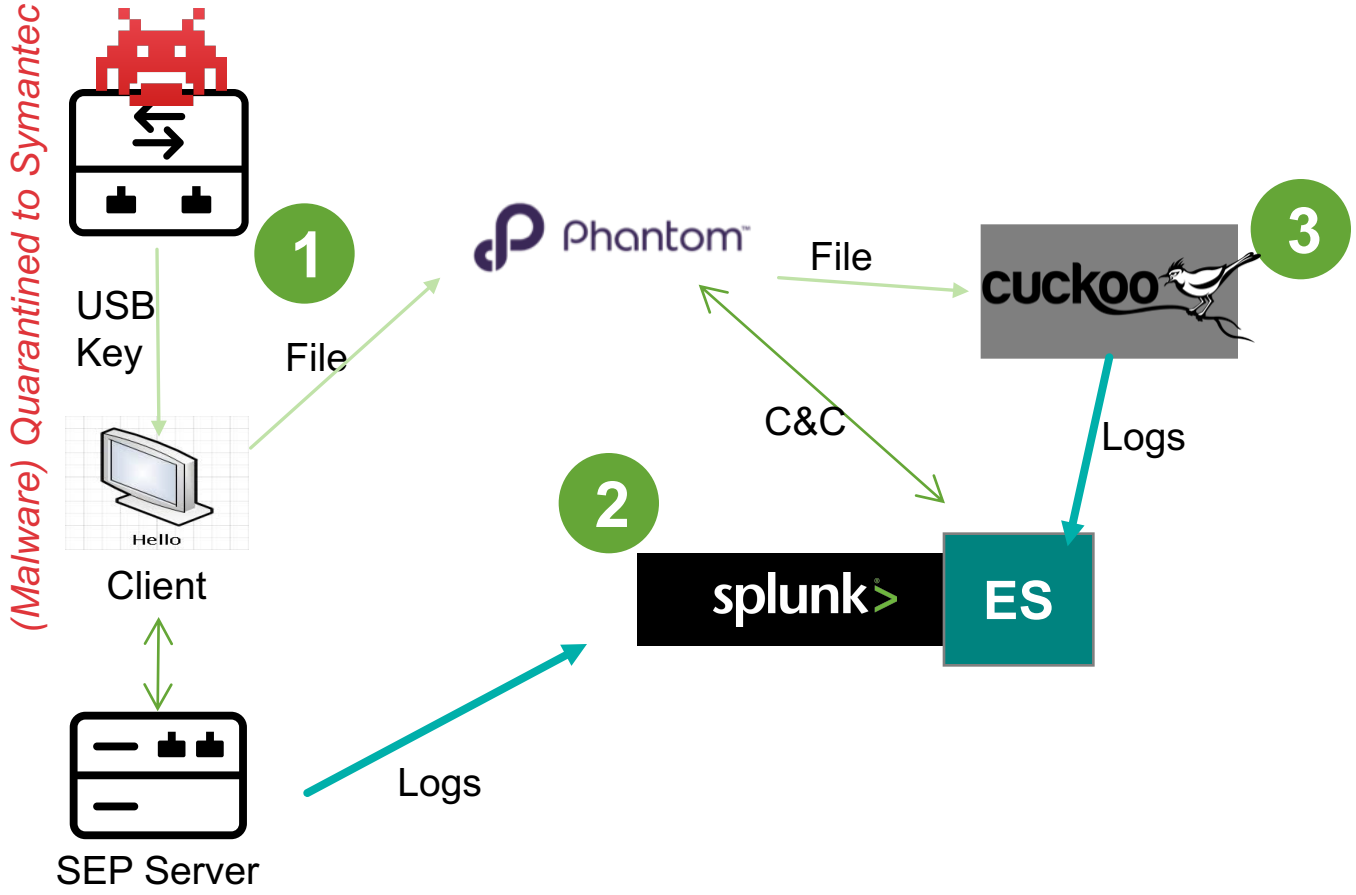


Use Case 1

- Suspicious file comes in over the network, via SMTP or HTTP
- Splunk stream decrypts any HTTPS, using proxy cert.
- All potentially malicious file types are sent to NFS share. We filter out some here using stream
- Splunk Correlation search filters the files further and sends selected ones to Cuckoo using Phantom
- Cuckoo automatically logs to Splunk using XML and success failure to ticket.
  - Dashboards in Splunk show Analysis results
  - Phantom can take further action if high result.

1. HTTPor SMTP Traffic between Client and Server directed towards Stream
2. Stream saves extracted payloads to NFS share.
3. ES Correlation Search triggers on certain files and initiates phantom playbook
4. Phantom Analysis the sample and Splunk reports on the file, file is automatically deleted if malicious

Symantec – Cuckoo Malware Sandbox



Use Case 2

- Suspicious file enters network via USB.
- Symantec will detect a suspicious file with inconclusive results
- Symantec quarantines file in quarantine
- Correlation rule creates incident in Splunk for detecting an unknown suspicious file which initiates phantom playbook to talk to cuckoo
- Cuckoo results fed back to Splunk / ES

1. Symantec detects suspicious file from USB and places in quarantine
2. Splunk correlation rule creates incident and initiates Phantom Playbook, which detonates the file with cuckoo
3. Results of file detonation go to both Splunk and Phantom
4. Incident created in ES if malicious. Higher fidelity alert than before

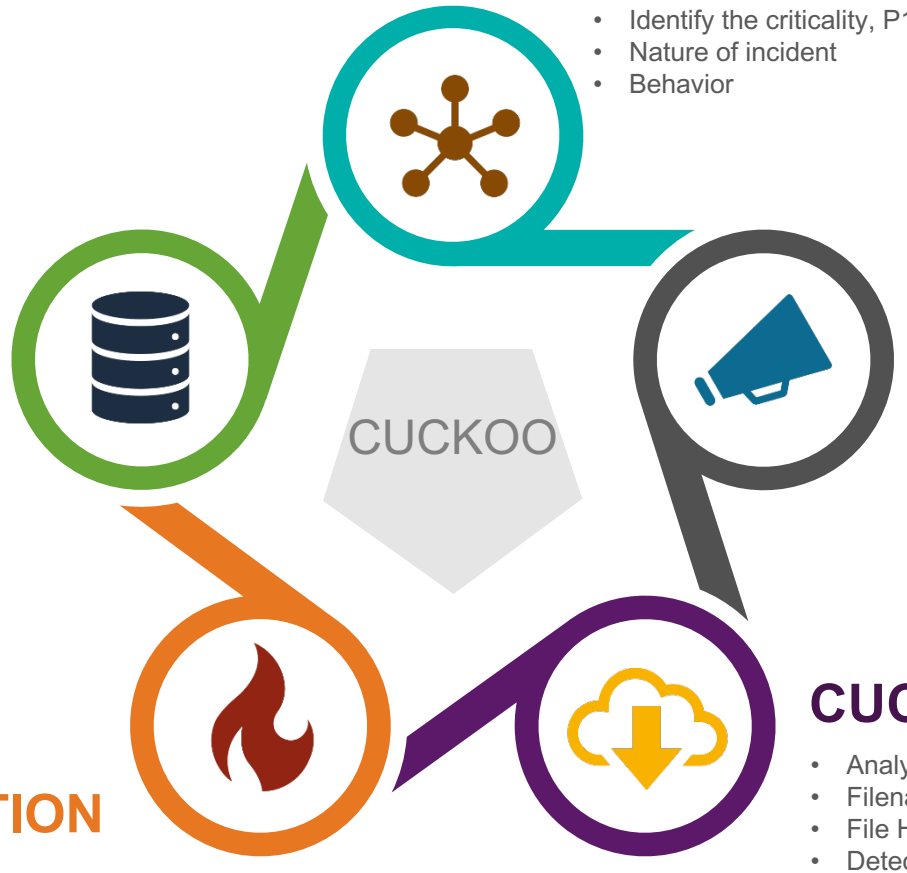
splunk> .conf18

Files with Inconclusive Analysis by Symantec

file_name	vendor_action	absolute_path
bugdojo+setup+1.13.0.exe	Quarantined	\\AU-LR90QFLA7\C$\ProgramData\Symantec\Symantec Endpoint Protection\14.0.3892.11013105\SRTSP\Quarantine\bugdojo+setup+1.13.0.exe
pip.exe	Quarantined	\\AU-LPC0RCTGL\C$\ProgramData\Symantec\Symantec Endpoint Protection\14.0.3892.11013105\SRTSP\Quarantine\pip.exe
FW Emailing All Clear Receipt $7254 17 DOC.msg	Quarantined	\\AU-LPC0Q43FU\C$\ProgramData\Symantec\Symantec Endpoint Protection\14.0.3892.11013105\SRTSP\Quarantine\FW Emailing All Clear Receipt $7254 17 DOC.msg
FW Purchase Order 37087-POR.msg	Quarantined	\\AU-LPC0Q43FU\C$\ProgramData\Symantec\Symantec Endpoint Protection\14.0.3892.11013105\SRTSP\Quarantine\FW Purchase Order 37087-POR.msg
4bfa1da0-16038df9	Quarantined	\\AU-LR90Q8M3M\C$\ProgramData\Symantec\Symantec Endpoint Protection\14.0.3892.11013105\SRTSP\Quarantine\4bfa1da0-16038df9
5413535b-54ff3f15	Quarantined	\\AU-LR90Q8M3M\C$\ProgramData\Symantec\Symantec Endpoint Protection\14.0.3892.11013105\SRTSP\Quarantine\5413535b-54ff3f15
spam-tickets.zip	Quarantined	\\AU-LPC0P0A7X\C$\ProgramData\Symantec\Symantec Endpoint Protection\14.0.3892.11013105\SRTSP\Quarantine\spam-tickets.zip
Famicom.Disk.System.7z	Quarantined	\\AU-LPC0TCBVF\C$\ProgramData\Symantec\Symantec Endpoint Protection\14.0.3892.11013105\SRTSP\Quarantine\Famicom.Disk.System.7z
via64.exe	Quarantined	\\AU-LPC0TDALS\C$\ProgramData\Symantec\Symantec Endpoint Protection\14.0.3892.11013105\SRTSP\Quarantine\via64.exe
Invoice from DATANET the Private Cloud Solutions Company.msg	Quarantined	\\AU10087727\C$\ProgramData\Symantec\Symantec Endpoint Protection\14.0.3892.11013105\SRTSP\Quarantine\Invoice from DATANET the Private Cloud Solutions Company.msg
truclientsupportabilitytool.exe	Quarantined	\\AU-LPC0F19GR\C$\ProgramData\Symantec\Symantec Endpoint Protection\14.0.3892.11013105\SRTSP\Quarantine\truclientsupportabilitytool.exe
e learning demo_2018.exe	Quarantined	\\AU-LPC0P0A2K\C$\ProgramData\Symantec\Symantec Endpoint Protection\14.0.3892.11013105\SRTSP\Quarantine\e learning demo_2018.exe
ildownloadwizard.exe	Quarantined	\\AU-LPC0SX6QT\C$\ProgramData\Symantec\Symantec Endpoint Protection\14.0.3892.11013105\SRTSP\Quarantine\ildownloadwizard.exe
nl custom toolbar - new brand (no update function).exe	Quarantined	\\AU-LR90Q9LY1\C$\ProgramData\Symantec\Symantec Endpoint Protection\14.0.3892.11013105\SRTSP\Quarantine\nl custom toolbar - new brand (no update function).exe
f_00678d	Quarantined	\\AU-LPC0SX58B\C$\ProgramData\Symantec\Symantec Endpoint Protection\14.0.3892.11013105\SRTSP\Quarantine\f_00678d
redemption.dll	Quarantined	\\AU-LR90QG074\C$\ProgramData\Symantec\Symantec Endpoint Protection\14.0.3892.11013105\SRTSP\Quarantine\redemption.dll

ile_name	vendor_action	absolute_path
ugdojo+setup+1.13.0.exe	Left alone	\\AU-LR90QFL9S\C$\ProgramData\Symantec\Symantec Endpoint Protection\14.0.3892.11013105\SRTSP\Quarantine\bugdojo+setup+1.13.0.exe
lbeaver-ce-5.1.4-x86_64-setup.exe	Left alone	\\AU-LPC0TDB7G\C$\ProgramData\Symantec\Symantec Endpoint Protection\14.0.3892.11013105\SRTSP\Quarantine\dbeaver-ce-5.1.4-x86_64-setup.exe
/yLocker v2.0.0.7.exe	Left alone	\\AU-LPC0TDBYY\C$\ProgramData\Symantec\Symantec Endpoint Protection\14.0.3892.11013105\SRTSP\Quarantine\MyLocker v2.0.0.7.exe
:loveretl-designer-win32-x86_64.exe	Left alone	\\AU-LPC0TDB7G\C$\ProgramData\Symantec\Symantec Endpoint Protection\14.0.3892.11013105\SRTSP\Quarantine\cloveretl-designer-win32-x86_64.exe
psc-11.4.006-install.exe	Left alone	\\AU-LPF163X5P\C$\ProgramData\Symantec\Symantec Endpoint Protection\14.0.3892.11013105\SRTSP\Quarantine\gpsc-11.4.006-install.exe

Solution Overview



IDENTIFY

- Identify the criticality, P1, P2, P3?
- Nature of incident
- Behavior

DATA ENRICHMENT

Record the MD5,IOC's and add them to local threat feed.

INCIDENT

Assess the likelihood and the nature of incident: Malware, Ransomware etc.
Impact to the eco-system

CUCKOO

- Analyze the files on Cuckoo
- Filename
- File Hash
- Detection score: 1- 10
- Integration with Virus Total for AV engines
- IP's, Hostname's and URL's

ORCHESTRATION

- Phantom to kick in the process based on cuckoo's analysis
- Whitelist
- Blacklist

Cuckoo Reporting

Cuckoo – Splunk Configuration

- Cuckoo creates xml files
- We installed splunk forwarder to monitor directory
  - Looking for report.xml
- Parser script to extract
  1. File Name
  2. File Hash
  3. File Score on Scale of 1 (clean) to 10 (Bad).
  4. Detected by AVs on Virus-Total
  5. List of IPs it connects.

Cuckoo Result in Splunk

_time	name	score	sha256	dest_ip
7/31/18 10:48:00.000 PM	gpsc-11.4.006-install.exe	7.2	987ac5506a5488a1193686f66cb45d3288c2258c510004edb2f361b67bb245jks	52.173.193.170
7/31/18 9:48:00.000 PM	cloveretl-designer-win32-x86_64.exe	6.2	5256ac5506a5488a1193686f66cb7ad3288c2258c510004edb2f361b452625	52.173.193.169
7/31/18 3:48:00.000 AM	MyLocker v2.0.0.7.exe	5.2	517ac5506a5485541193686f66cb57ad3288c2258c510004edb2f361b67452645	52.173.193.168
7/31/18 2:48:00.000 AM	dbeaver-ce-5.1.4-x86_64-setup.exe.exe	2.2	517ac5506a5488a1193686f66cb57ad3288c22582580004edb2f36hid74526er3	52.173.193.167 52.173.193.167
7/31/18 1:48:00.000 AM	bugdojo+setup+1.13.0.exe	6.9	517ac5506a5488a1193686f66cb57ad3288c2258c510004edb2f361b674526cc	52.173.193.166

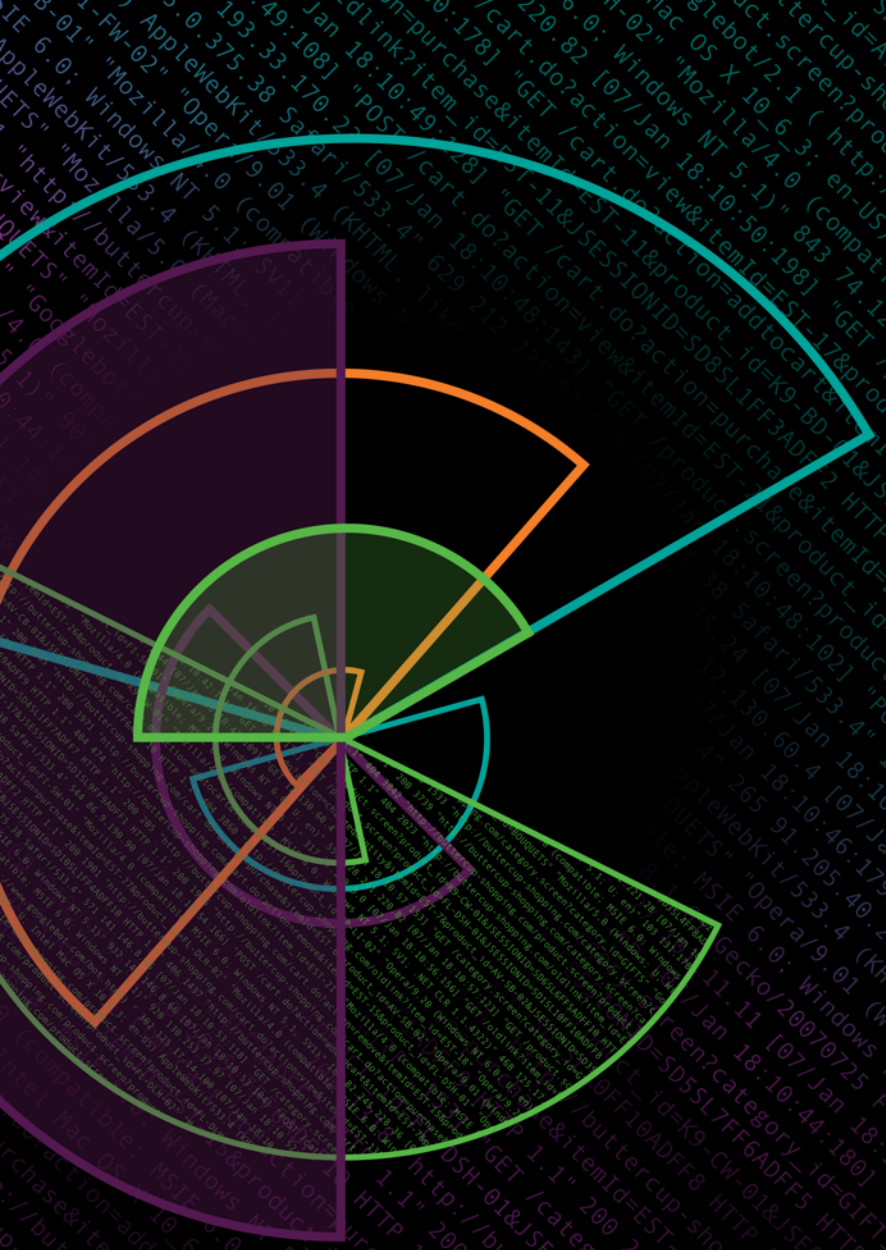
Challenges

Challenges

- Setting up Cuckoo sandbox securely
- HTTPS decryption
- File permissions on Splunk stream NFS share.
  - Splunk Stream, TCP Dump & Phantom
- Networking for guest machine can be tricky. Most issues reported to cuckoo and virtual machine network related. There's plenty of documentation
- Filtering Stream sessions affectively
  - Only PDF, Binaries and specific files cuckoo can accept
  - Max size 10mb
  - Threat feeds
  - NIST MD5 list
  - Phantom to filter further before sending to cuckoo
  - Roll the NFS directory after 3 days

Lessons Learnt

- Cuckoo is a jester (tricky)
  - Lots of settings you can get wrong
  - In lab its easy, but permissions need to be correct in prod so you don't get owned
- Cuckoo automation scripts help but don't get you the whole way
- XML is not consistent when sending to Splunk for reporting, need to modify first.
- SSL encrypted traffic proved difficult but easy with right tools
  - Decryption Certificate needed for stream.
  - Stream encrypts this in its store
  - Tap fabric would make life easy
- Phantom makes life even easier



Q&A

Nick Crofts | Senior Security SME

Shafqat Mehmood | SOC Manager

splunk> .conf18

Thank You

Don't forget to rate this session in the .conf18 mobile app