Hacking your SOEL

SOC Automation and Orchestration

Rob Gresham | Security Solutions Architect

October 2018

Forward-Looking Statements

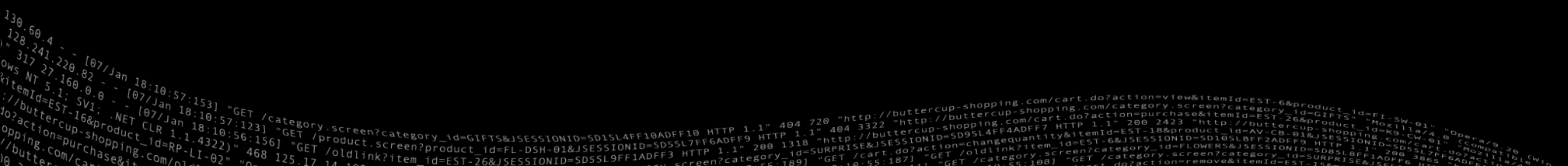
During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results 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

Agenda

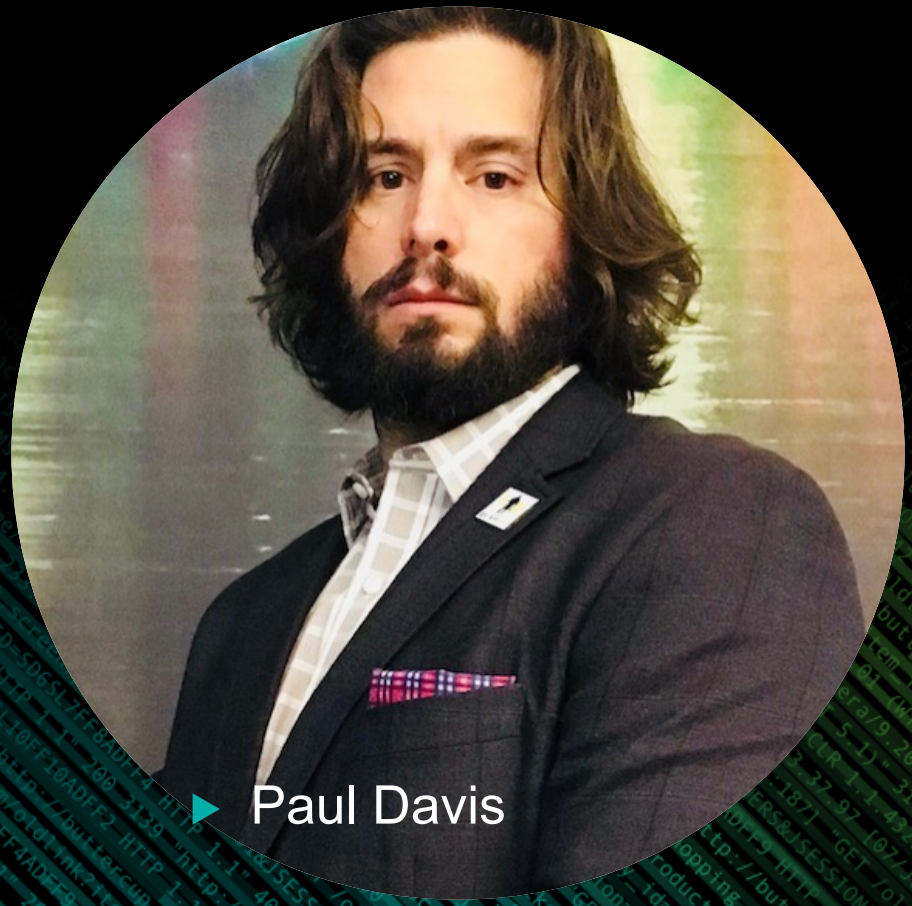
- SOAR History and the Future
- What is SOEL
- SOAR Loser?
- Hacking your SOEL
- Q&A



Our Speakers

ROB GRESHAM

Security Solutions Architect

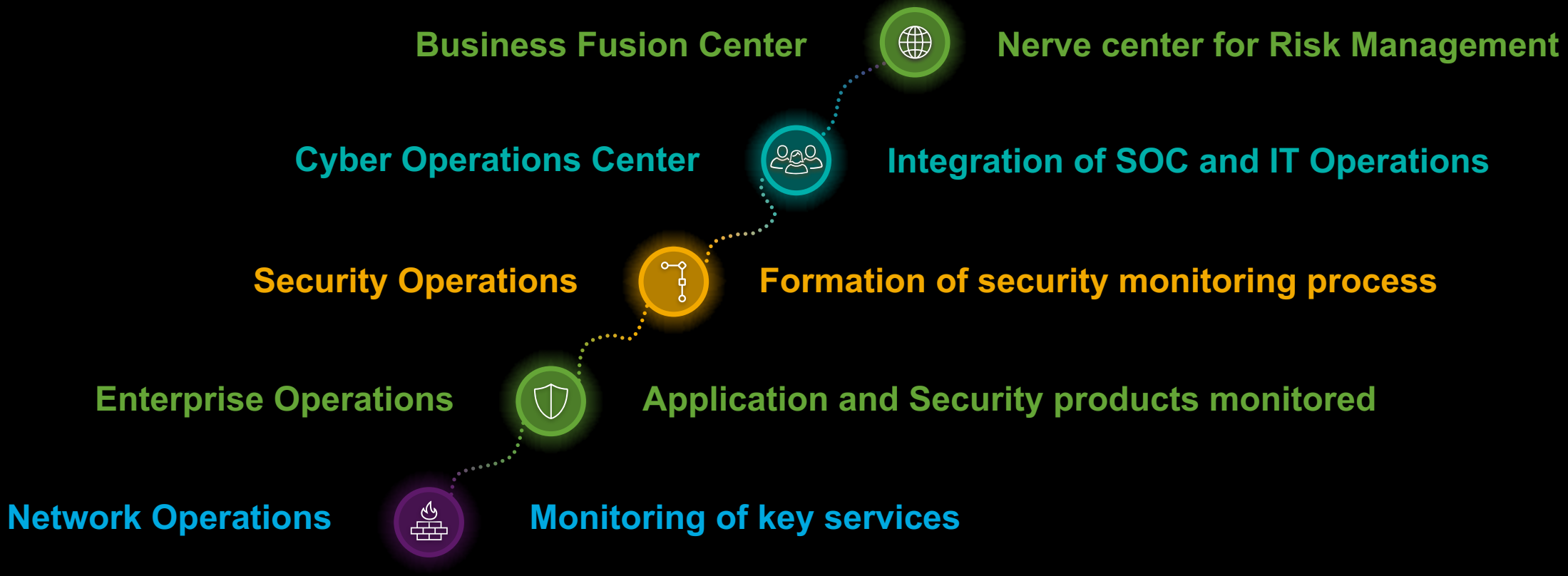


- Paul Davis
- Hacker of your SOEL

Key Takeaways

1. Understand SOEL and SOAR
2. Understand SOEL impacts and difference to SOAR development
3. How to use SOEL to ensure your SOAR is effective

Back to the Future of Security Operations



Security Operations Problems

Resources

Resource ***shortage of 1 million*** security professionals

Products

Endless assembly line of point products

Alerts

Escalating volume of ***security alerts***

Static

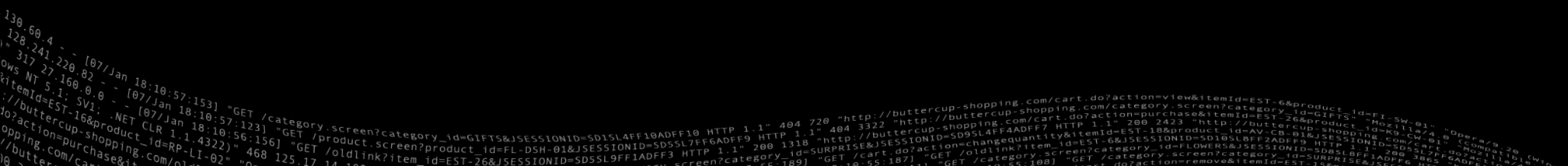
Static independent controls with ***no orchestration***

Speed

Speed of detection, triage, & response time ***must improve***

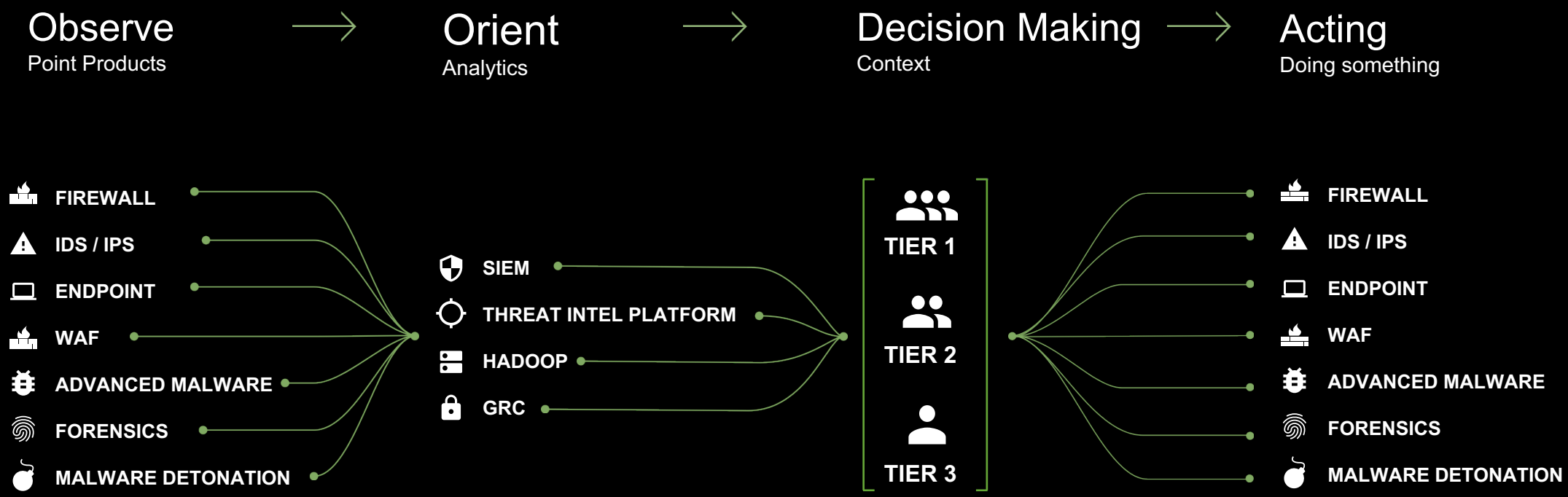
Costs

Costs ***continue to increase***



splunk> .conf18

6 Million Dollar SOC…



What is SOEL?

Security Operations Event Lifecycle

Security Operations Events Lifecycle

Every SOC process has them

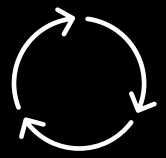
Traditional Security Operation Actions

INGESTION OR ALERTING

EXTERNAL VALIDATION

INTERNAL HUNTING

MONITORING



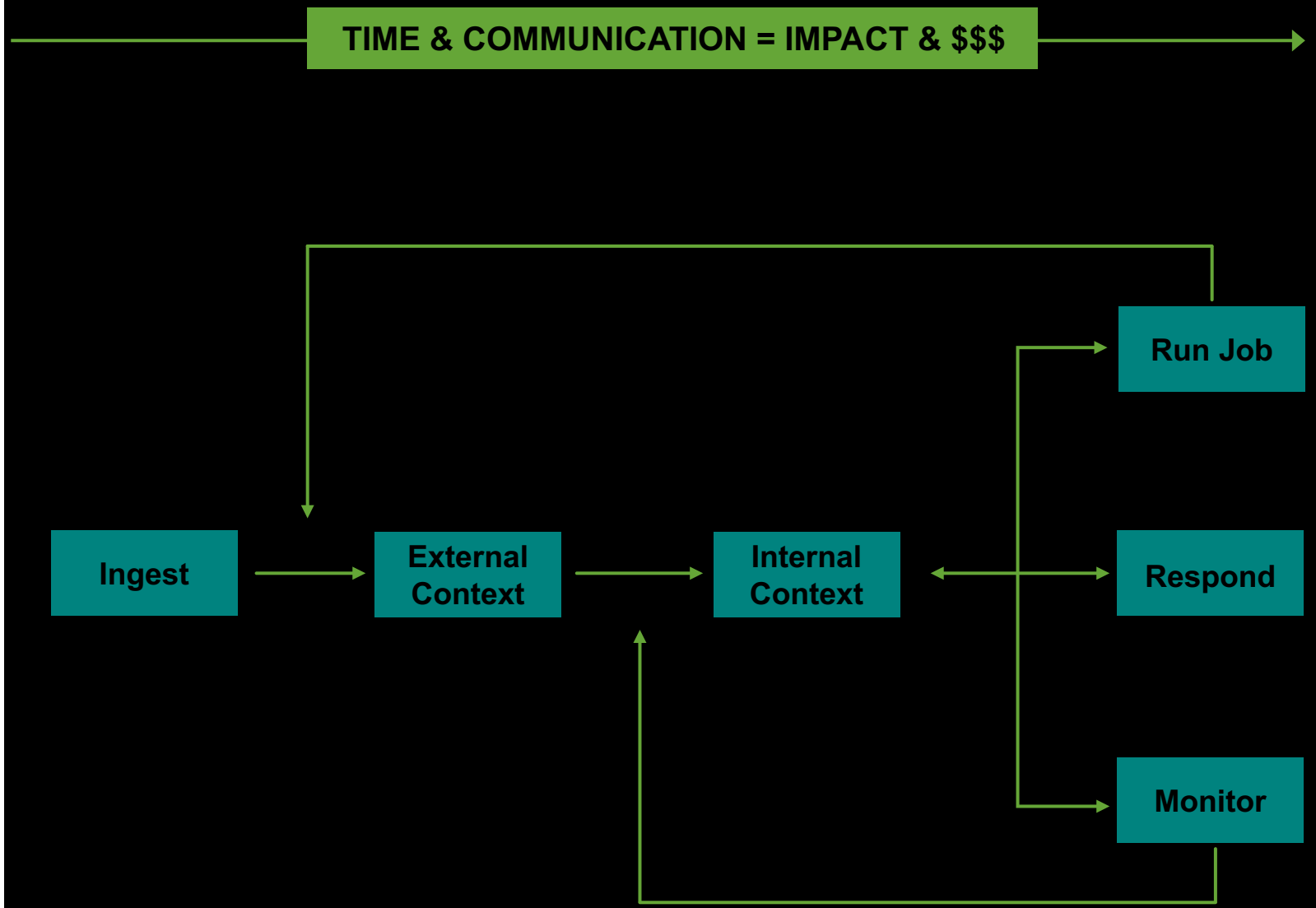
CHANGE

RUN JOBS

NOTIFICATIONS

Manage Impact with Response

The SOC's #1 Purpose








	INGESTION OR ALERTING	EXTERNAL VALIDATION	INTERNAL HUNTING	CHANGE / MONITORING	RUN JOBS	NOTIFICATIONS
	Threat Intel SIEM events Phone calls	VirusTotal OpenDNS iSight	Logs Endpoint search	Firewall Rules IDS Signatures Endpoint Alerts Proxy Blocks	Malware Analysis Forensics	Ticketing Reports
Actions	Poll Push	Look Up	Hunt	Set Block/Quarantine	Analyze Get…	Send Receive
Artifacts	Events	Context	Artifacts	Artifacts	Artifacts	Measure

Are You a SOAR Loser?

What is SOAR and why I am I missing out?

It's only for the big companies with lots of well documented responses…

splunk> .conf18

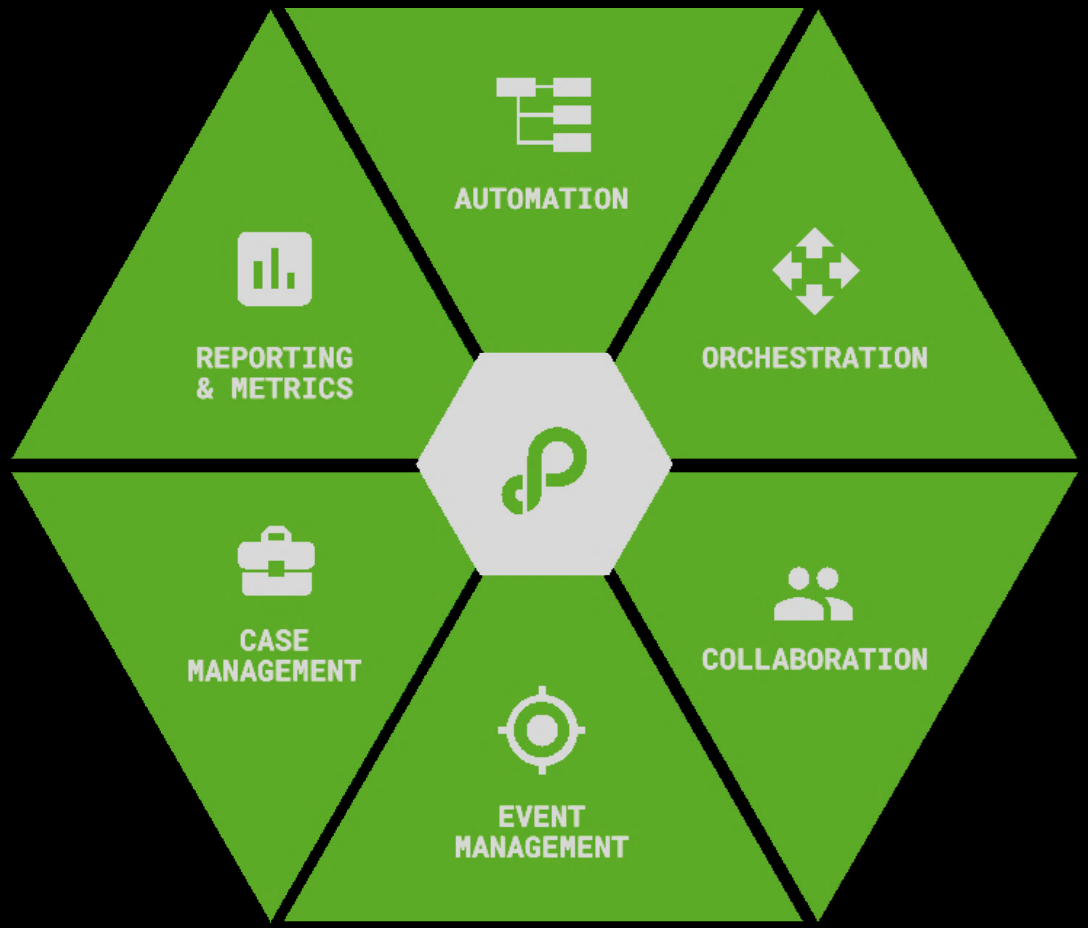
Don’t be a SOAR Loser!

Example of a industry-leading SOAR platform

SOAR = Security Orchestration, Automation, and Response

- ***Security Orchestration*** is *making music*
- ***Security Automation*** is a *bread maker*
- ***Security Response*** is the life blood of the SOC to *reduce Risk Impact*
- ***Hack your SOEL to get your SOAR on!***

Are You the Next Beethoven?



Conduct your team, processes and tools **together**

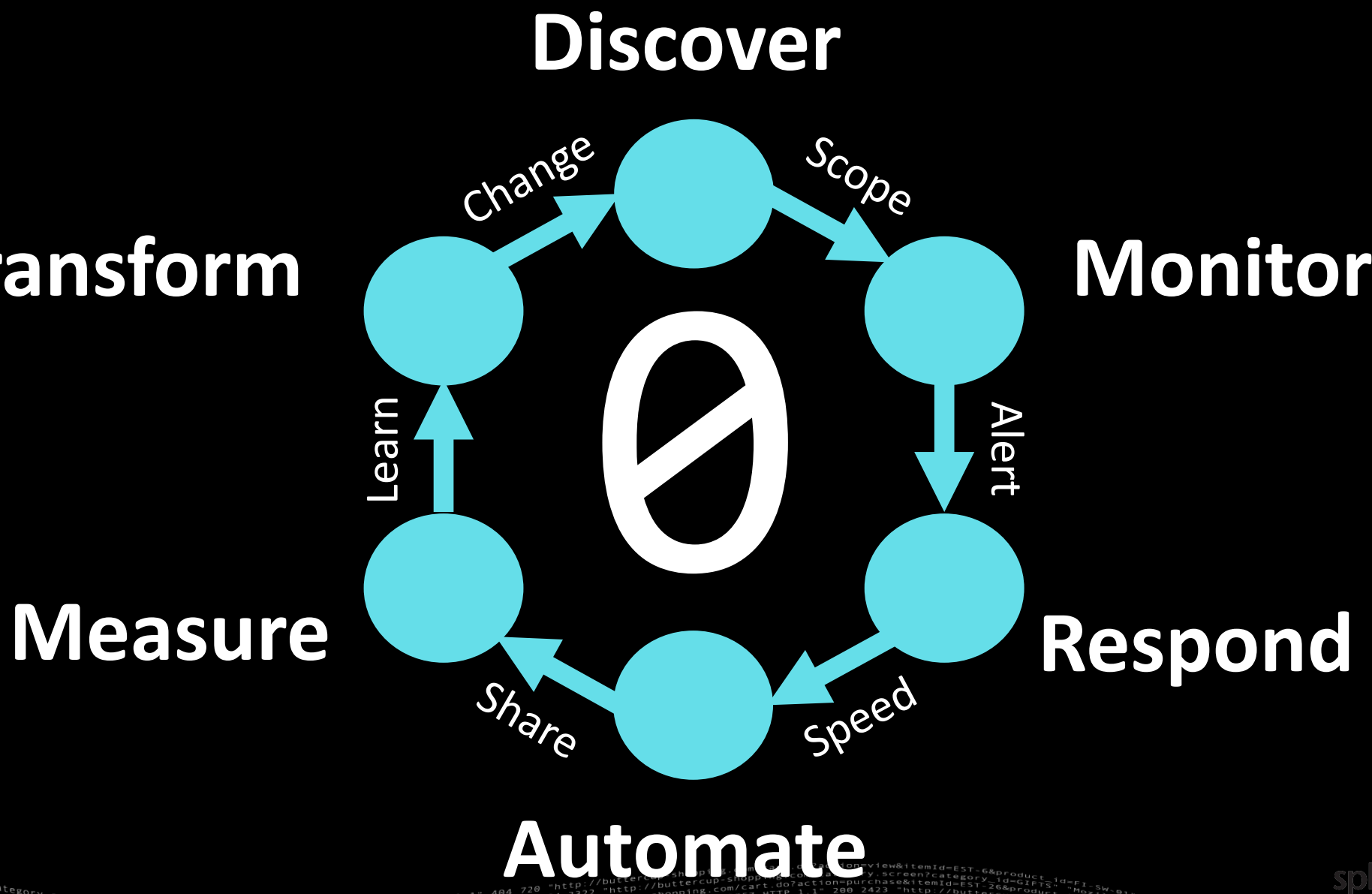
- Work smarter by automating repetitive tasks and focus on more mission-critical tasks
- Respond faster and reduce dwell times with automated integration, investigation, and response
- Strengthen defenses by integrating existing security infrastructure

Hacking your SOEL

Discovering your SOEL to help modernize your SOC

splunk> .conf18

How to Hack your SOEL



Use Case and Playbook Processing

MACHINE

Use cases engineered are usually **analytically consistent** and not instinctive

Generally **significantly faster** and effective when the analysis focused on logical decision with minimal bias

HUMAN

Visual and instinctive involving a level of experience and process learning

Generally, **not efficient** however highly effective, but prone to cognitive bias

Playbook Methodology

Develop compact playbooks that quickly perform common independent functions

EXAMPLE UTILITY PLAYBOOKS

- Ingest alert
- Create ticket
- Collect evidence
- Notify IR team
- Investigate evidence
- Scope event
- Contain asset
- Create ticket

INTERACTION

Owner, Actioner, Supporter, Consulted, Involved/Informed (OASCI) between teams, technology, or events

INPUT

Source(s) Event, Process, Information expected

ACTION

The transformation, duties, actions to be performed by a person, tool, analysis or correlation to a function

ARTIFACTS

The expected output of actions performed by the process or function

Use Case Overview

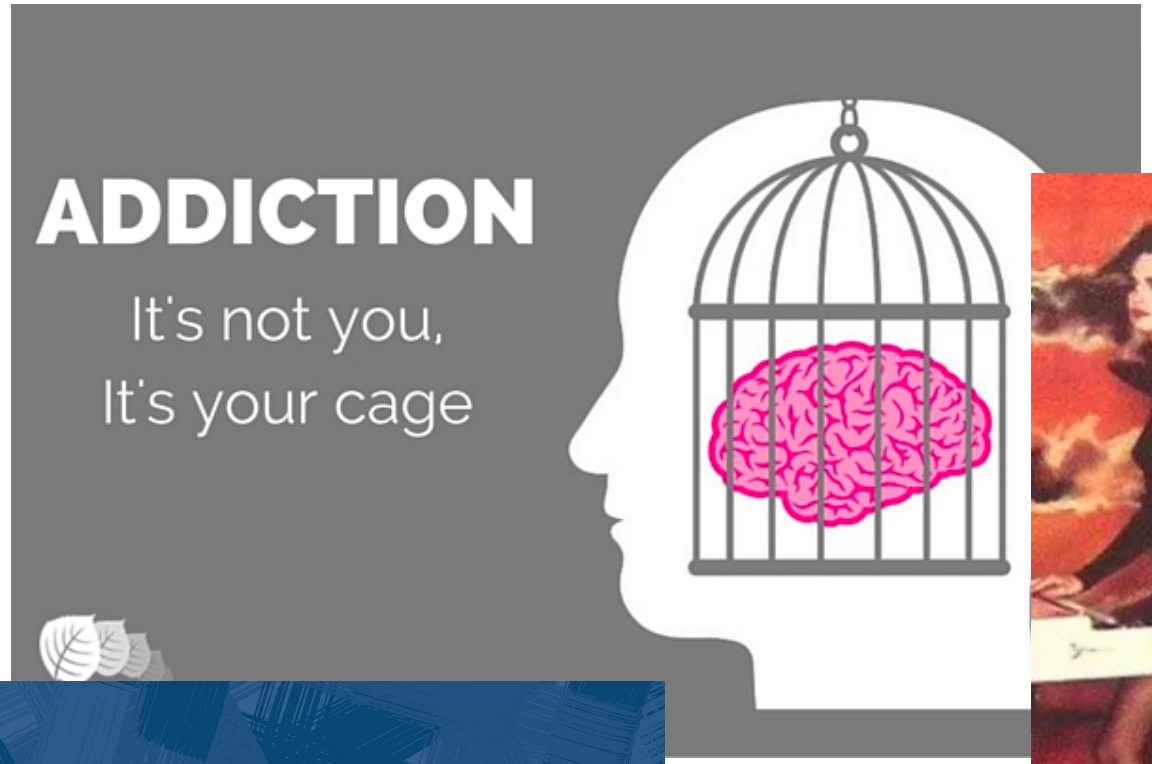
Security Analyst Use Cases			
Privileged user monitoring	Botnet Detection	Fraud detection in E-Payment	Unauthorized Service Monitoring
Identify Patient-Zero	Vulnerability Management Posture	Fraud detection Online Banking	Update Monitoring
Detecting Zero Day Attacks	Threat Intelligence Correlation	Fraud detection in proper service usage	Website defacement
Detect and Stop Data Exfiltration	User Account Sharing	Defense in depth investigations	Spam to external
Phishing Attacks	Incident Investigation across team's	Give team's the visibility they need	
SQL Injections	Dynamic Risk and Pattern Management	Monitoring of expired user accounts	

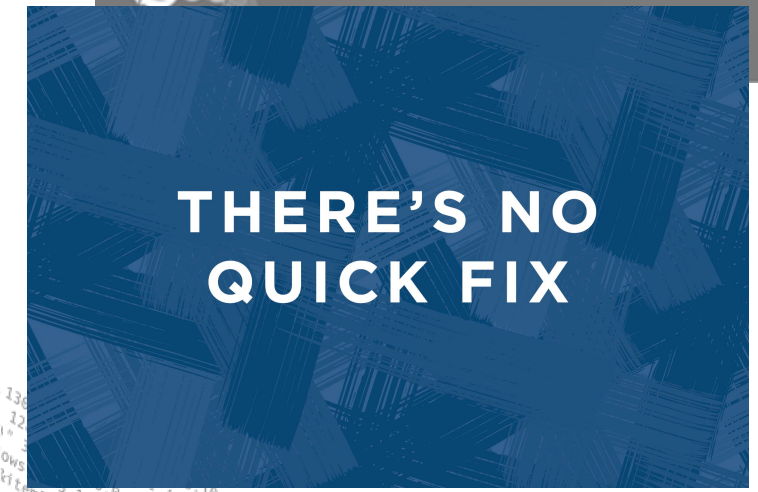
Hunter Use Cases			
On Demand APT Scanning	SSL certificate analytics	User Agent String analytics	

CISO Use Cases			
In the news!	Information Driven Security	Compliance reporting	Centralized Situational Awareness

splunk> .conf18

Use Case Addiction





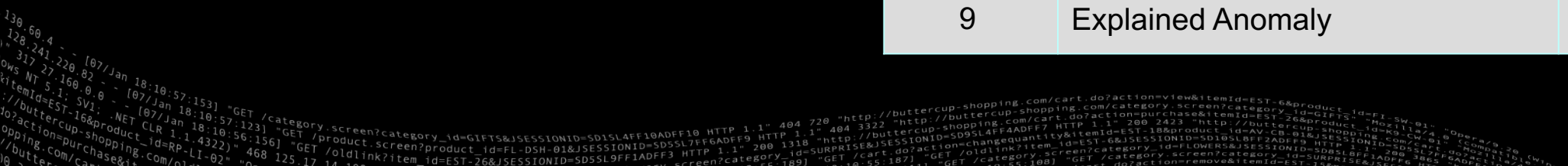
Don't be addicted to use cases, be addicted process adoption

Attack Vectors verses Incident Categories

Attack Vectors

- Network
- Host
- Unknown
- Attrition
- Web
- Email
- External
- Spoofing
- Improper Usage
- Theft/Lost
- Other

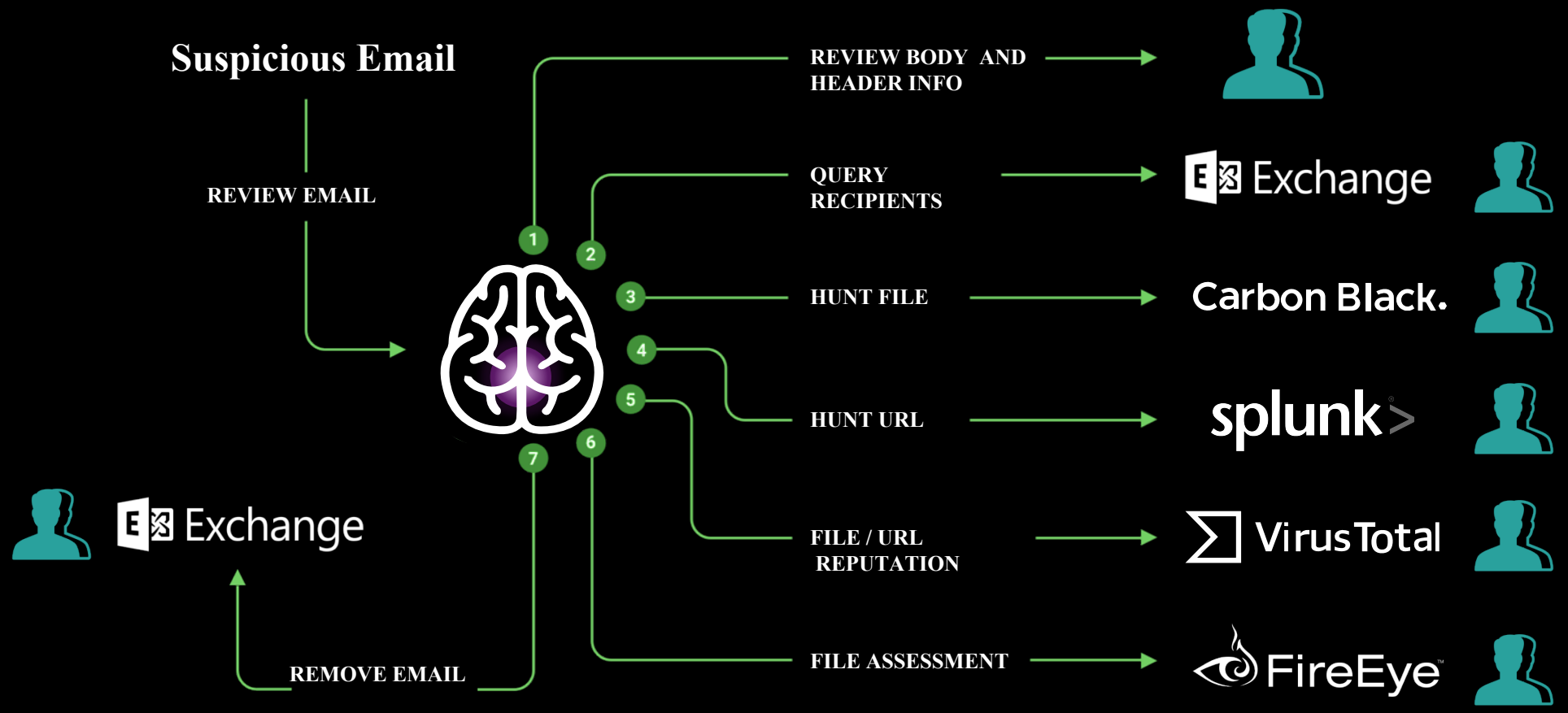
CATEGORY	DESCRIPTION	EVENT TYPE
0	Training and Exercises	Event/Incident
1	Root Level Intrusion	Incident
2	User Level Intrusion	Incident
3	Unsuccessful Activity Attempt	Event
4	Denial of Service	Incident
5	Non-Compliance Activity	Event/Incident
6	Reconnaissance	Event/Incident
7	Malicious Logic	Incident
8	Investigating	Event
9	Explained Anomaly	Event



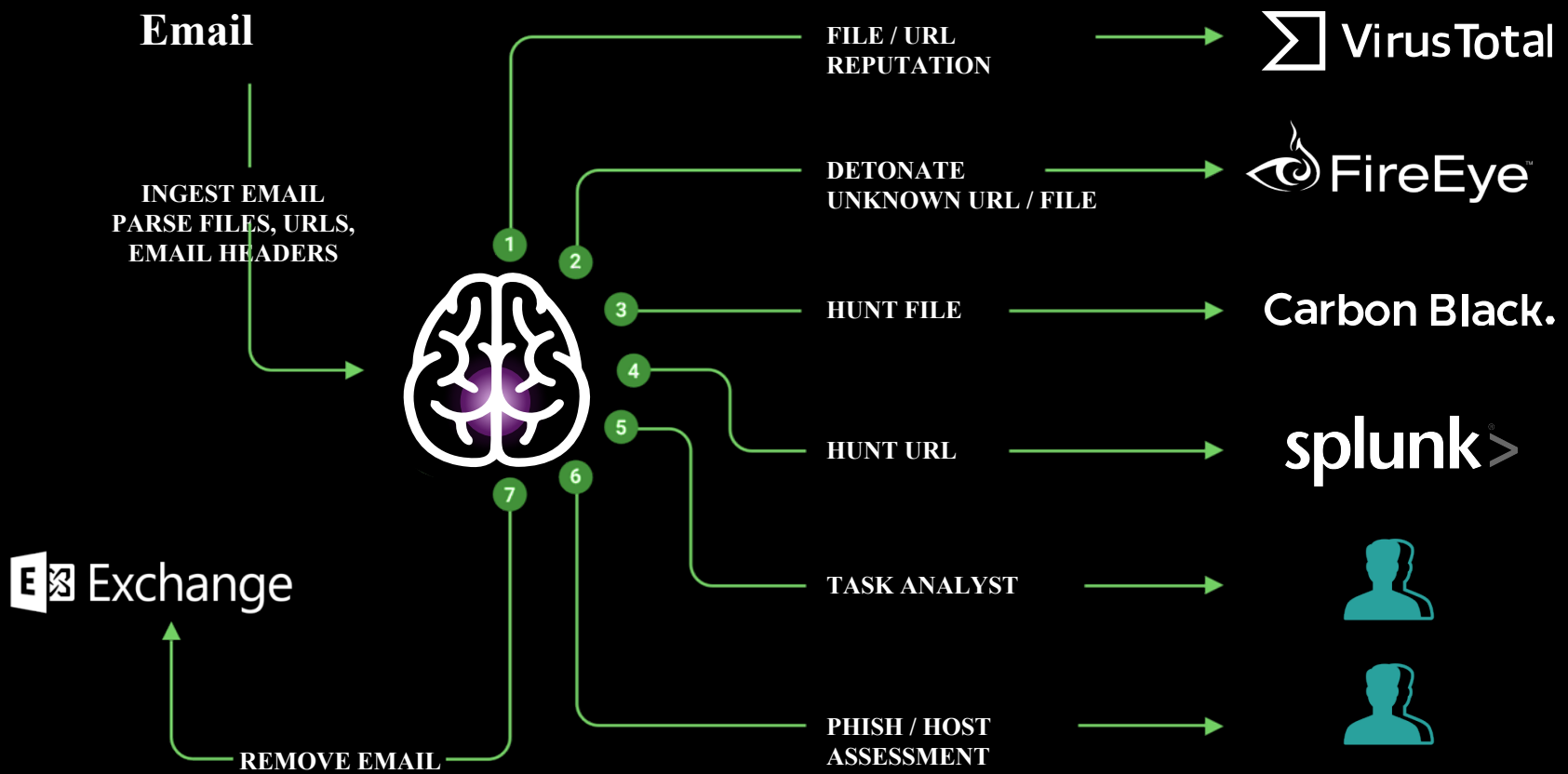
(Re)Defining Incident Response Playbooks

CATEGORY	DESCRIPTION	EVENT TYPE	INCIDENT RESPONSE PLANS
9	Training and Exercises	Event/Incident	
8	Root Level Intrusion	Incident	Host (Breach?)
7	User Level Intrusion	Incident	Host, Unknown, Account
6	Unsuccessful Activity Attempt	Event	
5	Denial of Service	Incident	Network, Spoofing, Attrition
4	Non-Compliance Activity	Event/Incident	Theft/Loss, Improper Usage, Account
3	Reconnaissance	Event/Incident	Network (Internal)
2	Malicious Logic	Incident	Host, Email, Web, External
1	Investigating	Event	
0	Explained Anomaly	Event	

Hacking your SOEL



Hacking your SOEL



INGEST	INVESTIGATE	CONTAIN	NOTIFY	DOCUMENT
POLL	FILE ANALYSIS	DISABLE USER	EMAIL SOC	CREATE TICKET
PUSH	DOMAIN ANALYSIS	BLOCK HASH	EMAIL	UPDATE TICKET
INGEST	URL ANALYSIS	BLOCK URL	LEADERSHIP	CLOSE TICKET
SET STATUS	HOST ANALYSIS	BLOCK DOMAIN	CHAT IT HELP	TRANSFER TICKET
SET SEVERITY	IP ANALYSIS	BLOCK IP	DESK	QUERY TICKETS
CREATE ARTIFACTS	LOGON ANALYSIS	QUARANTINE	EMAIL	CREATE ARTIFACTS
SAVE OBJECTS	RUN QUERY	HOST	ENGINEERING	CLOSE OBJECTS
SET TAGS	GET EVENTS	BLOCK PROCESS	PROMPT SOC	
		DISABLE VPN	TASK SOC	

”Customer Success is our commitment and your content”

splunk> .conf18

A Tale of Two Companies

Value Proposition

Same Use Case Different Results

Company 1

Seven months of development and they have 9 playbooks.

20 Events a day automated

Company 2

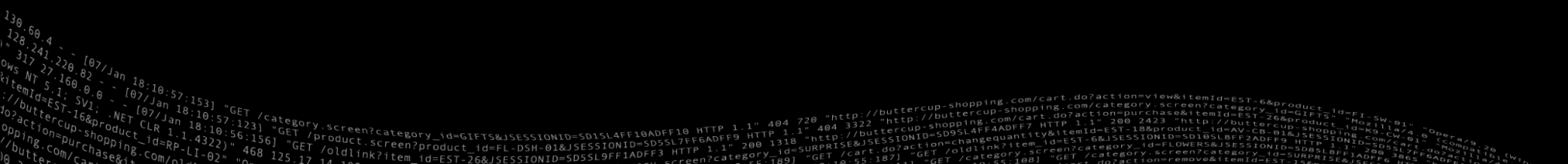
Four weeks of development and we have 9 playbooks.

Over 200 Events a day automated

File Analysis Playbook

Process hacking – which one is first?

- INPUT: *Receive a hash and/or file*
- INTERACTIONS:
- ARTIFACTS:
  - P1:
  - P2:
  - P3:
- ACTIONS:



splunk> .conf18

File Analysis Playbook

Define the Artifacts for **Decide** and **Act!**

- INPUT: Receive a hash and/or file
- INTERACTIONS:
- ARTIFACTS:
  - P1: Analyze, Prompt, Block Known malware (Block now)
  - P2: Analyze, Sandbox, (De)Escalate (Prompt, Review)
  - P3: Cache Results, Display Report (Required Manual Analysis)
- ACTIONS:

File Analysis Playbook

Build a utility playbook for file analysis

- INPUT: Receive a hash and/or file
- ACTIONS:
- INTERACTIONS:

VirusTotal, ThreatConnect, CarbonBlack, Falcon Sandbox, Analyst, SMTP, CB Response, Palo Alto, Zscaler, ThreatCrowd

- ARTIFACTS:
  - P1: Analyze, Prompt, Block Known malware
  - P2: Analyze, Sandbox, (De)Escalate
  - P3: Cache Results, Display Report, Manual Analysis

File Analysis Playbook

Build a utility playbook for file analysis

- INPUT: Receive a hash and/or file

- INTERACTIONS:

VirusTotal, ThreatConnect, CarbonBlack, Falcon Sandbox, Analyst, SMTP, CB Response, Palo Alto, Zscaler, ThreatCrowd

- ARTIFACTS:
  - P1: Analyze, Prompt, Block Known malware
  - P2: Analyze, Sandbox, (De)Escalate
  - P3: Cache Results, Display Report, Manual Analysis

- ACTIONS:

Block file
File Rep w/ rate limit
Block IP
Block Domain
Block URL
URL Rep
Domain Rep
Get File
Detonate File
Prompt Analyst
Change Severity
Change Sensitivity
Send Email
Quarantine Host

splunk> .conf18

File Analysis Playbook

Build a utility playbook for file analysis

- INPUT: Receive a hash and/or file

- INTERACTIONS:

VirusTotal, ThreatConnect, CarbonBlack, Falcon Sandbox, Analyst, SMTP, CB Response, Palo Alto, Zscaler, ThreatCrowd

- ARTIFACTS:
  - P1: Analyze, Prompt, Block Known malware
  - P2: Analyze, Sandbox, (De)Escalate
  - P3: Cache Results, Display Report, Manual Analysis

- ACTIONS:

Block file
File Rep w/ rate limit
Block IP
Block Domain
Block URL
URL Rep
Domain Rep
Get File
Detonate File
Prompt Analyst
Change Severity
Change Sensitivity
Send Email
Quarantine Host

Get Approval
Hunt file
Hunt URL
Promote Case
Cache Hash
Store File
Analyze File
Task Forensics
Block Process
Get customer info
Get system info
Check white/black lists
Get BU info
Run query
Lookup info (Threat Intel)

splunk> .conf18

File Analysis Playbook

Build a utility playbook for file analysis

- INPUT: Receive a hash and/or file

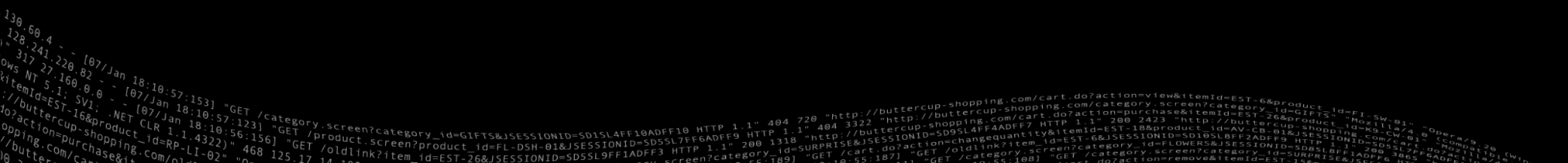
- INTERACTIONS:

VirusTotal, ThreatConnect, CarbonBlack, Falcon Sandbox, Analyst, SMTP, CB Response, Palo Alto, Zscaler, ThreatCrowd

- ARTIFACTS:
  - P1: Analyze, Prompt, Block Known malware
  - P2: Analyze, Sandbox, (De)Escalate
  - P3: Cache Results, Display Report, Manual Analysis

- ACTIONS:

Block file
File Rep w/ rate limit
Block IP
Block Domain
Block URL
URL Rep
Domain Rep
Get File
Detonate File
Prompt Analyst
Change Severity
Change Sensitivity
Send Email
Quarantine Host
Get Approval
Hunt file
Hunt URL
Promote Case
Cache Hash
Store File
Analyze File
Task Forensics
Block Process
Get customer info
Get system info
Check white/black lists
Get BU info
Run query
Lookup info (Threat Intel)



splunk> .conf18

File Analysis Playbook

Build a utility playbook for file analysis

- INPUT: Receive a hash and/or file
- INTERACTIONS:

VirusTotal, ThreatConnect, CarbonBlack, Falcon Sandbox, Analyst, SMTP, CB Response, Palo Alto, Zscaler, ThreatCrowd

- ARTIFACTS:
  - P1: Analyze, Prompt, Block Known malware
  - P2: Analyze, Sandbox, (De)Escalate
  - P3: Cache Results, Display Report, Manual Analysis

1 Ingest
2 Investigate
3 Contain
4 Notify
5 Record
6 Utility

- ACTIONS:

3 Block file
2 File Rep w/ rate limit
3 Block IP
3 Block Domain
3 Block URL
2 URL Rep
2 Domain Rep
1 Get File
2 Detonate File
4 Prompt Analyst
1 Change Severity
1 Change Sensitivity
4 Send Email
3 Quarantine Host
5 Create ticket

4 Get Approval
2 Hunt file
2 Hunt URL
2 Promote Case
2 Cache Hash
1 Store File
2 Analyze File
2 Task Forensics
3 Block Process
1 Get customer info
1 Get system info
2 Check white/black lists
1 Get BU info
1 Run query
2 Lookup info (Threat Intel)

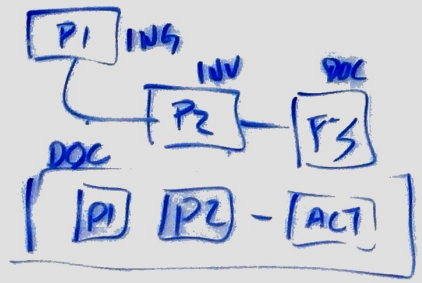
splunk> .conf18

Whiteboard Exercise

The faster hack and don't you just love "Office Lens"?

INPUT:
FILE HASH & POSSIBLE FILE
USERNAME / HOSTNAME

INTERACTION:
PAN, FALCON, VTI, THREATCROWD, SMTP, ANALYST
CB RESPONSE



1 INGEST
2 INVESTIGATE
3 CONTAIN
4 NOTIFY
5 DOC / UTIL

ACTIONS:
3 BLOCK FILE
2 FIL- DEP-RATELIMIT
3 BLOCK IP/HOSTNAME
2 DETONATE FILE
2 GET FILE
4 PROMPT ANALYST
4 CHANGE SEVERITY

4/5 SEND E MAIL
3 QUARANTINE HOST
2 HUNT FILE
4 PROMOTE CASE
4/5 CACHE HASH/RESULTS
2 CHECK LIST
2 VT RATE LIMIT - OVER/
4 TASK FORENSICS
2/3 -VAULT
4/5 -PIN HUD
1/2 RUN QUERY
1/2 1 DAY - USED

ARTIFACTS:
P1: ANALYZE, PROMPT & BLOCK MAL. HASH HOST
P2: ANALYZE, SANDBOX, ESCALATE / DE-ESCALATE
P3: CACHE RESULTS, DISPLAY REPORT, MANUAL ANALYSIS

Key Takeaways

Can you afford not to SOAR with your SOEL?

1. Understand SOEL and SOAR
2. Understand SOEL impacts and difference to SOAR
3. How to use SOEL to ensure your SOAR is effective

Q&A

Rob Gresham | SOEL Hacker

Paul Davis | Director of Success Chaos

Thank You

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