Don’t be a SIEMingly SOAR Loser…

@SOCologize

Rob Gresham

October 8, 2019

Abstract

What's in it for me?

Why Security Orchestration Automation and Response?

To integrate or to not?

ROI, the mystery to SOAR metrics

Case management, Service Catalogs or Digital workflows, Oh My?

How do I start to get my SOC to SOAR?

What do you use for best practices, or what is everyone else using?

A barrier of excellence was the reported absence of skilled staff at 58%

2019 SANS SOC Survey

Absence of SOAR

Absence of Effective Automation & Orchestration was 50%

Tools not integrated at 43%

Lack of Management Support at 37%

Lack of processes or playbooks at 37%

servicenow

SWIMLANE

CYBERSPONSE
ADAPTIVE SECURITY

DFLABS
CYBER INCIDENTS UNDER CONTROL

Microsoft

HEXADITE

splunk>phantom

Siemplify

resilient
an IBM Company

RAPID7

paloalto NETWORKS

DEMISTO
A PALO ALTO NETWORKS® COMPANY

IOMAND

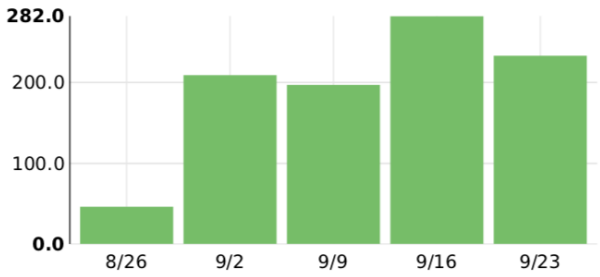
ATAR Labs, Ayehu, Cyberbit, CyberSponse, D3 Security, Demisto, DFLabs, EclecticIQ, IBM, Splunk, Rapid7, Resolve, ServiceNow, Siemplify, Swimlane, Syncurity, ThreatConnect, and ThreatQuotient.

Courtesy of Gartner Market Guides: https://www.gartner.com/en/research/methodologies/market-guide

ALL DATA SOURCES

1K

Incoming Events



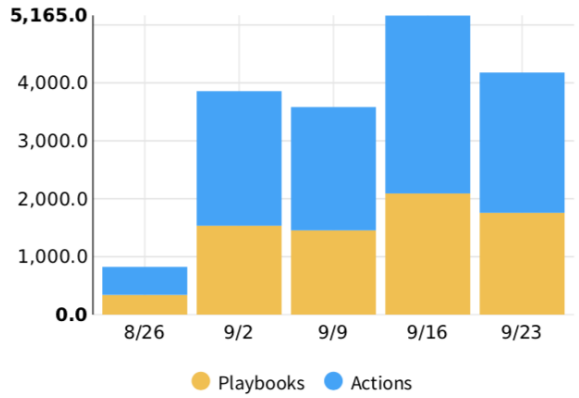
EXECUTED PLAYBOOKS & ACTIONS

7.6K

Playbooks Run

11.1K

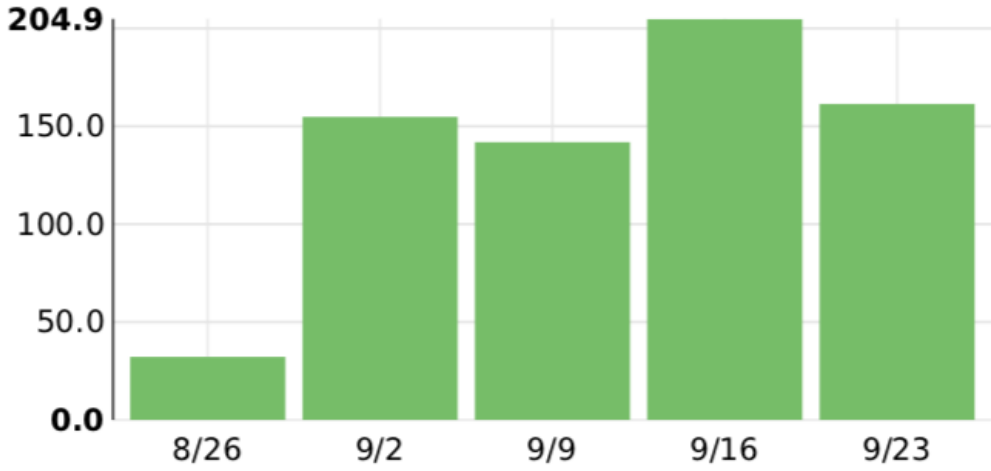
Actions Run



ROI

737.2

Hours Saved



11.1K

Dollars Saved

1

FTE Gained

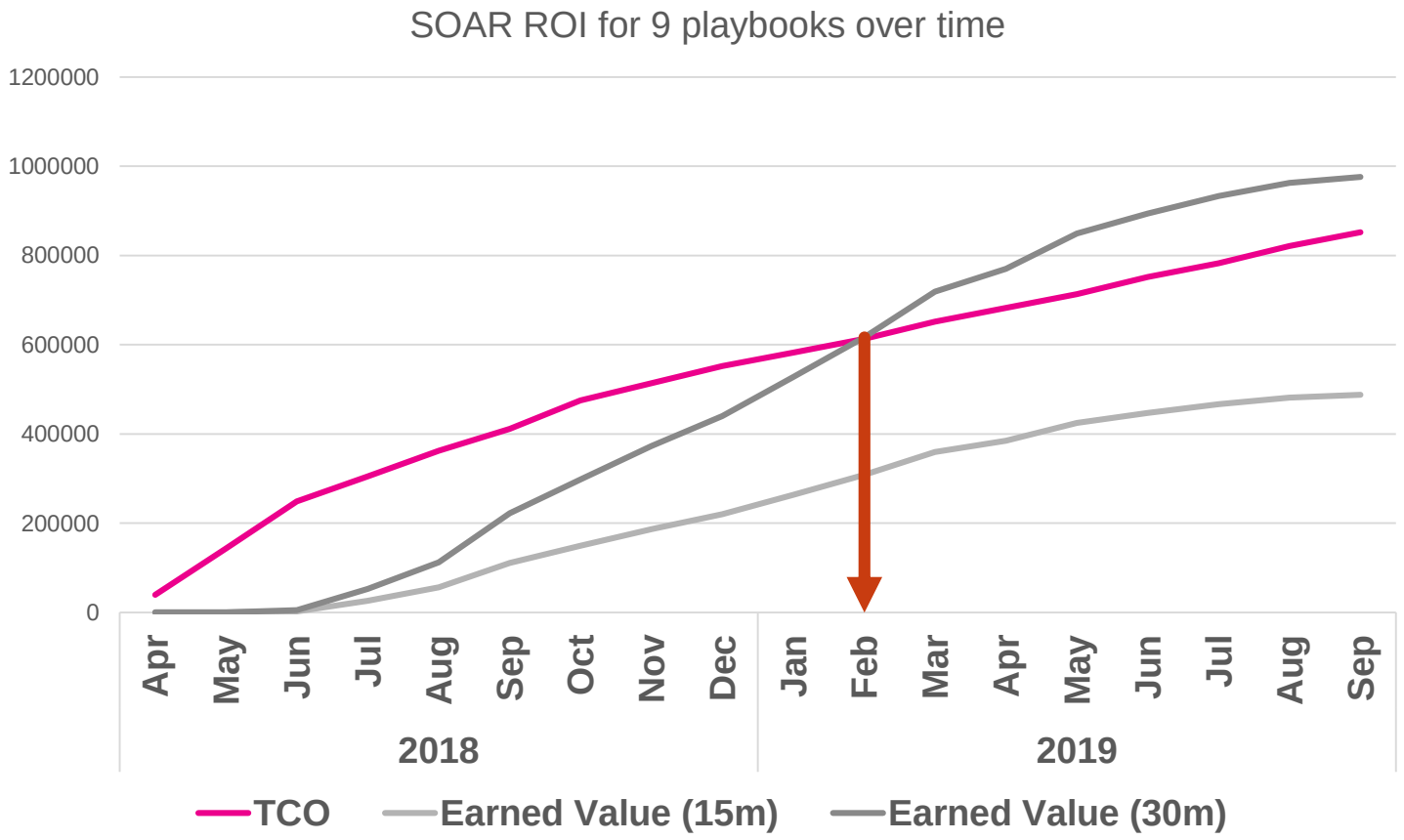
https://digitalguardian.com/blog/cyber-security-salary-guide-what-does-todays-cyber-security-workforce-make

Cyber Security Salary Guide:

What Does Today's Cyber Security Workforce Make?

Calculating SOAR ROI

Do you know when your investment breaks even?



Investment breaks even in 8 months with only 9 playbooks.

This customer had ~556 events a day

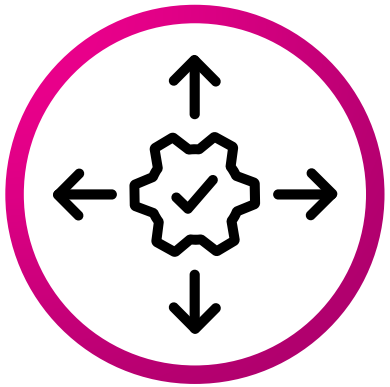
Average customer builds approximately 15-40 playbooks

$ 612,964.12

Meh-trics anyone?

SOAR ROI done right…

Mean Build Time



20 Days

4 Integrations and 9 Playbooks

Mean Time to Production

3 Months

9 Playbooks
585 Events a day

Technology / Human Cost

$851,725 to date

$7701 Support, License, Maintenance

ROI Value

Break even on Feb 23, 2019 at

$612,964.12

Integrations

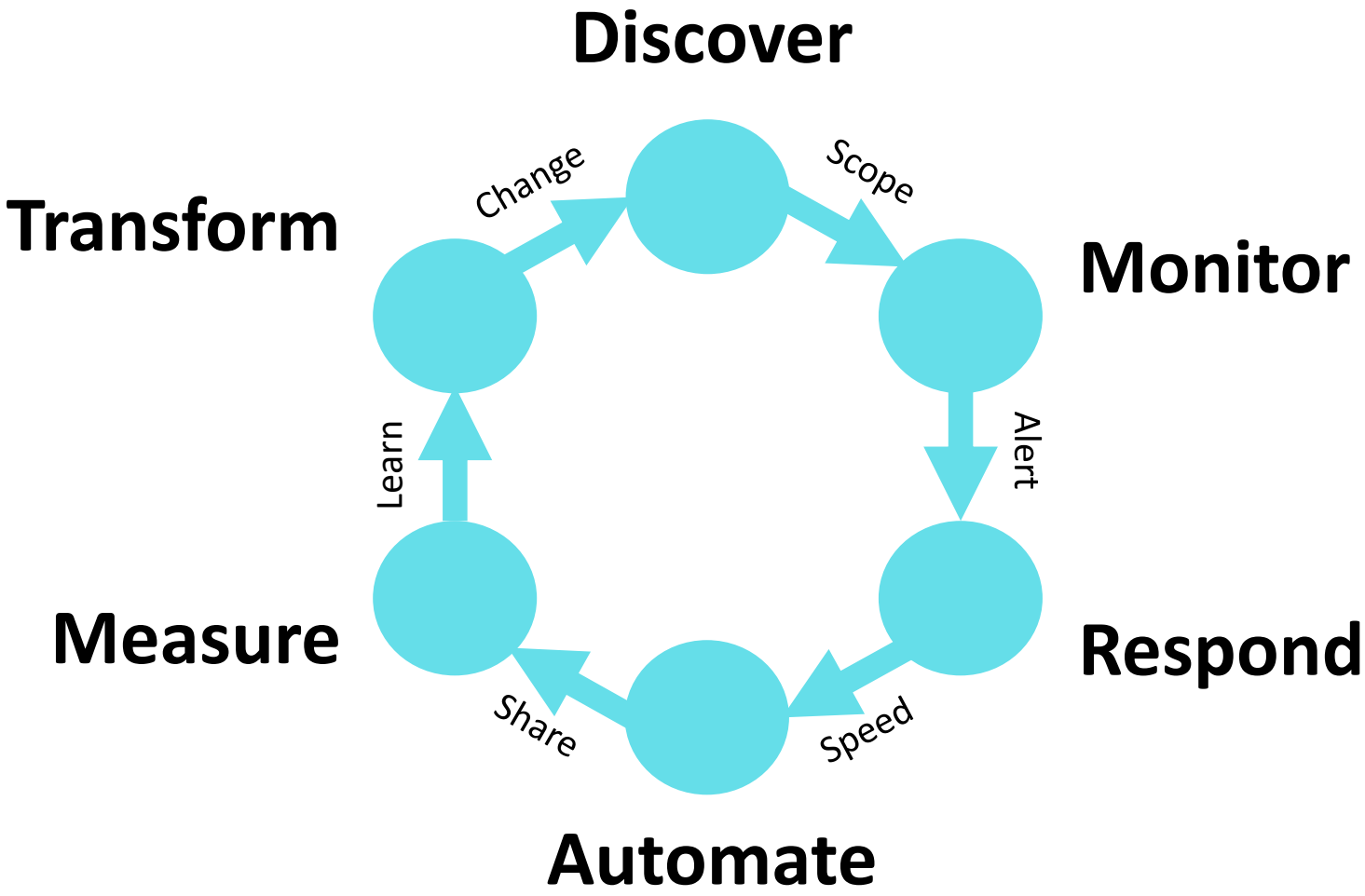
Which integration is best for our team?

Case Management Processing

Headless Operation

Operations Fractal

People, Process and Technology



KEEP
CALM
AND
RESPOND

closing time you don't have to go home but you can't stay here

Meh-trics

Just the basics, Start Macro move to Micro

Mean Time to Detect

Measure:

Time to Alert Analyst (New Event/Alert)

Mean Time To Respond

Measure:

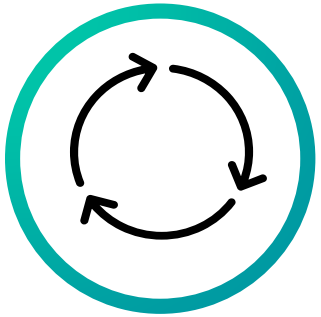
Time for Analyst to Pickup (New to Open Status)

Mean Time To Contain

Measure:

Time for Analyst to Contain (Time to Task Contain)

Mean Time To Recovery



Measure:

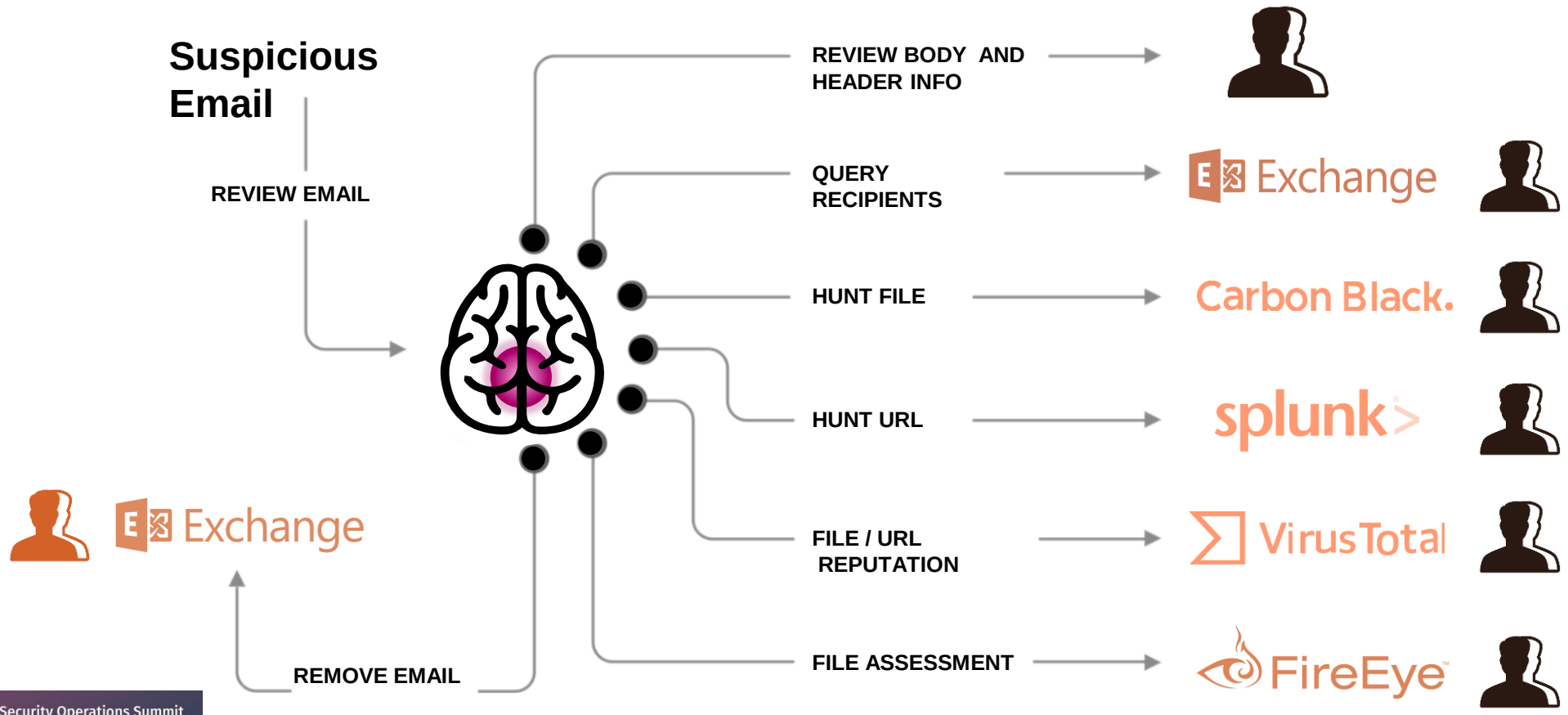
Re-image validation

Mean Time To Close

Measure:

Closing Dispositions

Hacking your SOEL



https://www.youtube.com/watch?v=_mnxZ1iSUGg

WHAT IS SOEL?

Security Operations Events Lifecycle

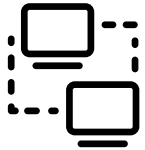
Traditional Security Operation Actions

INGESTION OR ALERTING

EXTERNAL VALIDATION

INTERNAL HUNTING

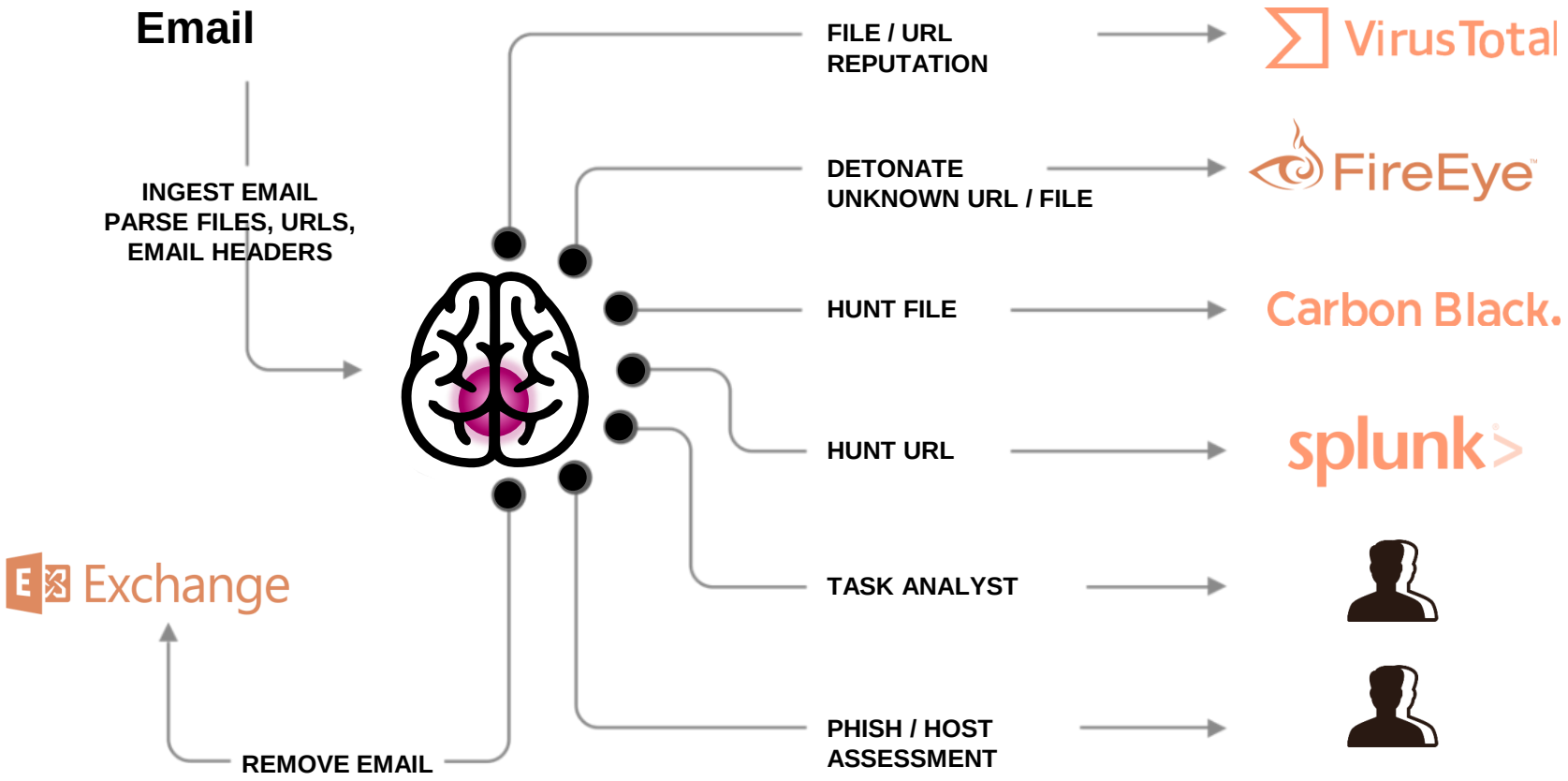
CHANGE / MONITORING



RUN JOBS

NOTIFICATIONS

Hacking your SOEL



Playbook Methodology

Compact playbooks that quickly perform common independent functions

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

Phishing Use Case Analysis

Build a utility playbooks to complete the process

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)

Phishing Use Case Analysis

1 Prepare
2 Investigate
3 Contain
4 Eradicate
5 Recovery
6 Lessons Learn

Build a utility playbooks to complete the process

INPUT: Receive and email with a url or file

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

ARTIFACTS:

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

ACTIONS:

- 3 Block file
- 2 File Rep
- 3 Block IP
- 3 Block Domain
- 3 Block URL
- 2 URL Rep
- 2 Domain Rep
- 2 Detonate File
- 2 Prompt Analyst
- 2 Change Severity
- 1 Change Sensitivity
- 5 Send Email
- 3 Quarantine Host
- 4 Create Ticket (re-image)
- 6 5 2 Add Note/Comment
- 4 Get Approval
- 2 Hunt file
- 2 Hunt URL
- 2 Promote Case
- 2 Analyze File
- 4 Task Forensics
- 3 Block Process
- 1 Get customer info
- 1 Get system info
- 4 Check white/black lists
- 4 Create Ticket (delete email)
- 1 Get BU info
- 2 Run query (other emails)
- 2 Lookup info (Threat Intel)

Summary answers

Automation should be metrics driven

SOAR should be helping drive your successful business metrics

Look to solutions integrate between solutions & integrate your processes

Your ROI should calculate the business value and

Case management (human augmentation) and integrated digital workflows for the whole

Get started on the simple task – Death by a thousand cuts

Use methodologies that work for your team, we use the Operations fractal, SOEL and I2A2

Next Steps

Is your organization up to it?

Train

Automate

Integrate

Process

Observe

Support

Table 4. Challenges to Full Integration and Utilization of a Centralized SOC Service Model Year-over-Year

	2019		2018	
Lack of skilled staff	57.7%	157	61.9%	148
Lack of automation and orchestration	49.6%	135	52.7%	126
Too many tools that are not integrated	43.0%	117	47.7%	114
Lack of management support	37.1%	101	37.2%	89
Lack of processes or playbooks	36.8%	100	42.7%	102
Lack of enterprisewide visibility	36.0%	98	41.8%	100
Too many alerts that we can't look into (lack of correlation between alerts)	32.0%	87	33.9%	81
Silo mentality between security, IR and operations	30.2%	82	30.1%	72
Lack of context related to what we are seeing	25.4%	69	18.8%	45
High staffing requirements	25.0%	68	27.2%	65
Regulatory or legal requirements	9.2%	25	12.6%	30
Other	4.8%	13	8.8%	21
Answered		**272**		**239**

Thank You