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%
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:
1K Incoming Events

7.6K Playbooks Run  11.1K Actions Run

737.2 Hours Saved

11.1K Dollars Saved  1 FTE Gained
Cyber Security Salary Guide:

What Does Today’s Cyber Security Workforce Make?

<table>
<thead>
<tr>
<th>Job</th>
<th>Average Salary</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Security Specialist</td>
<td>$52.54 per hour</td>
<td>United States</td>
</tr>
<tr>
<td>Information Security Analyst</td>
<td>$40.79 per hour</td>
<td></td>
</tr>
<tr>
<td>Security Engineer</td>
<td>$38.93 per hour</td>
<td></td>
</tr>
<tr>
<td>Security Analyst</td>
<td>$40.87 per hour</td>
<td></td>
</tr>
<tr>
<td>Intelligence Analyst</td>
<td>$24.54 per hour</td>
<td></td>
</tr>
<tr>
<td>Security Specialist</td>
<td>$14.83 per hour</td>
<td></td>
</tr>
<tr>
<td>Network Security Engineer</td>
<td>$51.80 per hour</td>
<td></td>
</tr>
</tbody>
</table>

Cyber Security Salaries in the United States
Salary estimated from 344,665 employees, users, and past and present job advertisements on Indeed in the past 12 months. Last updated: September 5, 2017

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
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
KEEP CALM AND RESPOND

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

BEAR FART
IF A BEAR FART'S IN THE WOODS
DOES IT SMELL?
MAYBE IT SMELLS LIKE THIS!

RECOVERY
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

Just the basics, Start Macro move to Micro
Hacking your SOEL

Suspicious Email
- REVIEW EMAIL
- REVIEW BODY AND HEADER INFO
- QUERY Recipients
- HUNT FILE
- HUNT URL
- FILE / URL REPUTATION
- FILE ASSESSMENT
- REMOVE EMAIL

Exchange
Carbon Black
Splunk
VirusTotal
FireEye

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

Email

- INGEST EMAIL
- PARSE FILES, URLs, EMAIL HEADERS

FILE / URL REPUTATION

- DETONATE UNKNOWN URL / FILE

- HUNT FILE

- HUNT URL

- TASK ANALYST

PHISH / HOST ASSESSMENT

- REMOVE EMAIL

Exchange

VirusTotal

FireEye

Carbon Black.

splunk
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

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

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

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

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:
- Block file (3)
- File Rep (2)
- Block IP (3)
- Block Domain (3)
- Block URL (3)
- URL Rep (2)
- Domain Rep (2)
- Detonate File (2)
- Prompt Analyst (2)
- Change Severity (1)
- Change Sensitivity (2)
- Send Email (5)
- Quarantine Host (3)
- Create Ticket (re-image) (4)
- Add Note/Comment (2)

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

GET APPROVAL
- Hunt file (4)
- Hunt URL (2)
- Promote Case (2)
- Analyze File (2)
- Task Forensics (4)
- Block Process (3)
- Get customer info (1)
- Get system info (1)
- Check white/black lists (4)
- Create Ticket (delete email) (4)
- Get BU info (1)
- Run query (other emails) (2)
- Lookup info (Threat Intel) (2)
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?

| Table 4. Challenges to Full Integration and Utilization of a Centralized SOC Service Model Year-over-Year |
|-------------------------------------------------|-----------------|----------------|
| **Train**                                       | **2019**        | **2018**       |
| Lack of skilled staff                           | 57.7%           | 61.9%          |
| Lack of automation and orchestration            | 49.6%           | 52.7%          |
| Too many tools that are not integrated          | 43.0%           | 47.7%          |
| Lack of management support                      | 37.1%           | 37.2%          |
| Lack of processes or playbooks                   | 36.8%           | 42.7%          |
| Lack of enterprisewide visibility               | 36.0%           | 41.8%          |
| Too many alerts that we can’t look into (lack of correlation between alerts) | 32.0%           | 33.9%          |
| Silo mentality between security, IR and operations | 30.2%           | 30.1%          |
| Lack of context related to what we are seeing   | 25.4%           | 18.8%          |
| High staffing requirements                      | 25.0%           | 27.2%          |
| Regulatory or legal requirements                | 9.2%            | 12.6%          |
| Other                                           | 4.8%            | 8.8%           |
| **Answered**                                    | **272**         | **239**        |
Thank You