Co-bot Uprising: Smart Automation for Blue Teams

Mark Orlando
March 2020
Who Am I?

Mark Orlando
19 years in cyber operations
Managed services, consulting, strategy, automation
SANS Instructor
Founder & CEO, Bionic
The Automation Imperative

You.

Very Important Security Data
“Heavy investments in technology have delivered disappointing results [in boosting performance] – largely because companies tend to use technology to mechanize old ways of doing business...speeding up those processes cannot address their fundamental performance deficiencies.”

- Michael Hammer, Harvard Business Review
Not All Automation is Equal

• Automation = improvement
• Don’t improve something to death
• Some improvements reduce risk
• Others increase quality
• Others reduce variance without adding value

How do I avoid over-engineering?
Let’s just go, go, go!

- “Micro-automation” doesn’t require a five step process (and is a very good idea)
- Larger initiatives, advent of AI/ML require more deliberate analysis and planning
Five Step Approach

1. Identify the Opportunity
2. Deconstruct the Task
3. Consider Return on Innovation Investment
4. Evaluate Automation Type
5. Evaluate Automation Impact

Desired result: **Measurable, Deliberate Improvement**
Step One: Identify the Opportunity

LOOK AT ALL THE PEOPLE

I DON'T WANT TO TALK TO
Step Two: Deconstruct the Task

**STEP 1**

1. Repetitive vs. Variable
   Does the task change depending on...

**STEP 2**

2. Independent vs. Interactive
   Does the task require dynamic user input?

**STEP 3**

3. Verbal vs. Electronic
   Does the task involve a conversation or can...
Step Three: Return on Improved Performance (ROIP)

(Think of this as a diminishing returns scale)

1. Negative Value
   Getting to minimally acceptable performance

2. Constant Value
   Getting consistent results that make little difference in strategic value

3. Incremental Value
   Each improvement has strategic value

4. Exponential Value
   Enabling rare or creative performance

- Ex: Detecting unknown / sophisticated attacks
- Ex: Better visibility or intelligence
- Ex: Automated reporting
- Ex: Ticket QA

SANS Blue Team Summit 2020
Step Four: Evaluate Automation Type

1. Robotic process automation (RPA)
2. Cognitive automation
3. Collaborative/social robotics
Step Five: Impact

- Substitute for something a human does
- Augment what a human does
- Create new/value-added work not being done today, or previously impossible without automation
Case Study 1: Add Event Context

IF YOU COULD JUST...

QUERY SIEM, IDENTITY, ENDPOINT, HISTORICAL DATA, LOG STORE AND SHIFT LOGS FOR...EVERY ALERT...THAT'D BE GREAT
## Deconstruct the Task

<table>
<thead>
<tr>
<th>Subtasks</th>
<th>Intent</th>
<th>Benefit</th>
<th>Dependency</th>
<th>Task Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Device identity</td>
<td>Device state and ownership</td>
<td>Improve detection</td>
<td>Asset inventory</td>
<td>Repetitive/Independent/Electronic</td>
</tr>
<tr>
<td>2. User identity</td>
<td>User role and likely intent</td>
<td>Improve detection</td>
<td>User/authentication data</td>
<td>Repetitive/Independent/Electronic</td>
</tr>
<tr>
<td>3. Incident history</td>
<td>Historical context</td>
<td>Improve detection</td>
<td>Case management system</td>
<td>Repetitive/Independent/Electronic</td>
</tr>
<tr>
<td>4. Threat data</td>
<td>IOCs or known TTPs</td>
<td>Improve detection</td>
<td>TIP/CMS or other central intel repo</td>
<td>Repetitive/Independent/Electronic</td>
</tr>
<tr>
<td>5. Forensic data</td>
<td>Increased fidelity</td>
<td>Improve detection</td>
<td>Endpoint detection and response platform and/or host scripts</td>
<td>Repetitive/Independent/Electronic (????)</td>
</tr>
<tr>
<td>6. User input</td>
<td>Likely intent</td>
<td>Reduce time to resolve</td>
<td>Automated user prompt and response</td>
<td>Variable/Interactive/Verbal</td>
</tr>
</tbody>
</table>
Return on Improved Performance

• Somewhere between constant and incremental value
• Every bit of context gets us closer to our goal
• The right context could be a game changer!
Example Alert

Name: Potential Malware Download – Blocked
Alert Source: Splunk
Alert Date: 2019-09-25 23:28:56
Status: Open

Severity: Low
Source IP: 10.10.4.251
Destination IP: 144.91.69.195
Alert ID: 2019-094435628
Alert Date: 2019-09-25 23:28:56

Mitigated by Controls?: Yes

Domain: 144.91.69.195
Alert Data Source: Bluecoat | Suspicious

Resolved IPs Past 30 Days
144.91.69.195

Resolved Domains Past 30 Days
N/A

Malicious IOCs: 3
OSINT Files: 2

Related Alerts: 4
Related Incidents: 1
Related Events: 5

Affected Device Type: Laptop | Dell | Win 10 x64 | 1809
Last Vulnerability Scan: 2019-09-15 | 5 Vulnerabilities Found

Device Owner: VIP | John Davis
Username: jdavis

Historical Context
Determine Device Owner
Gather Related Log and Host Data
Threat Applicable?

Example Alert
SANS Blue Team Summit 2020
Automation Type & Impact

Type
- RPA: Replaces tasks a human would do manually

Time*
- Implemented in SOAR, **20 minutes** on average
- **11 minutes** per case in data collection alone

Value
- Reduces time to identify/respond
- Reduces analysis fatigue

*SANS Blue Team Summit 2020

*YMMV!
Case Study 2: Threat Monitoring via Social Media

- Threats that impact our org or industry
-Leaks/dox
- New instrumentation, projects, & detections
## Deconstruct the Task

<table>
<thead>
<tr>
<th>Subtasks</th>
<th>Intent</th>
<th>Benefit</th>
<th>Dependency</th>
<th>Task Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Identify useful sources</td>
<td>Pull high quality, actionable information</td>
<td>Inputs to hunting and analysis, IR process</td>
<td>Data sources identified</td>
<td>Variable/Interactive</td>
</tr>
<tr>
<td>2. Collect data</td>
<td>Get information out of native platform into tools</td>
<td>Interoperate with our tools, reduce reliance on external sources</td>
<td>Task 1 + API access</td>
<td>Repetitive/Independent/Electronic</td>
</tr>
<tr>
<td>3. Filter noise</td>
<td>Reduce false positives</td>
<td>Minimize wasted cycles and rabbit holes</td>
<td>Task 2 + Known baseline, filtering terms/logic</td>
<td>Variable/dynamic/electronic</td>
</tr>
<tr>
<td>4. Process and store</td>
<td>Annotate and normalize</td>
<td>Data is available to our tools and actionable</td>
<td>Task 2 + TIP, CMS, other platforms where data can be enriched</td>
<td>Repetitive/Independent/Electronic</td>
</tr>
</tbody>
</table>
Return on Improved Performance

- Constant value – consistent, higher quality results
- Once we dial it in, relatively little additional improvements we can make that make an impact
## Indicators from Twitter via Python Script

<table>
<thead>
<tr>
<th>Fang use [.][d] hxxp</th>
<th>331</th>
</tr>
</thead>
<tbody>
<tr>
<td>c2:</td>
<td>70</td>
</tr>
<tr>
<td>ioc:</td>
<td>250</td>
</tr>
<tr>
<td>URLs included</td>
<td>374</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Top 10 Handles</th>
<th>Top 10 Linked FQDNs</th>
</tr>
</thead>
<tbody>
<tr>
<td>399 scumbots</td>
<td>251 pastebin.com</td>
</tr>
<tr>
<td>267 romonlyht</td>
<td>237 app.any.run</td>
</tr>
<tr>
<td>202 noladefense</td>
<td>191 urlscan.io</td>
</tr>
<tr>
<td>200 dgafeedalerts</td>
<td>127 virustotal.com</td>
</tr>
<tr>
<td>197 phishstats</td>
<td>116 cc.uec.ac.jp</td>
</tr>
<tr>
<td>129 kesagatame0</td>
<td>55 phishtank.com</td>
</tr>
<tr>
<td>127 crypt phishing</td>
<td>36 pulsedive.com</td>
</tr>
<tr>
<td>120 botysrt</td>
<td>10 app.threatconnect.com</td>
</tr>
<tr>
<td>103 pennysoc</td>
<td>7 github.com</td>
</tr>
<tr>
<td>96 ipnigh</td>
<td>7 beta.virusbay.io</td>
</tr>
</tbody>
</table>

| Top 10 Hashtags Used    | |
|-------------------------||
| 33 #infosec             | |
| 30 #cybersecurity       | |
| 14 #malware             | |
| 9 #threathunting        | |
| 9 #malwareanalysis      | |
| 9 #banker               | |
| 8 #rat                  | |
| 8 #emotet               | |
| 6 #loki bot             | |
| 5 #ursnif               | |
| 5 #agent tesla          | |
| 4 #threatintel          | |
| 3 #gootkit              | |
| 2 #spelevoek            | |
| 2 #nanocore             | |
| 2 #maldoc               | |
| 2 #keylogger            | |
| 2 #jasper loader        | |
| 1 #vidar                | |
Automation Type & Impact

Type
• RPA: Augments tasks a human would do manually

Situational Awareness
• Tough to quantify, but could probably look at increases in true positives

Value
• Additional intelligence
• Timely/actionable information
Where Would You Focus?

Alert context
Incremental value (each improvement has strategic value to our operations)
Quantifiable time savings in a repetitive, daily activity

Social media monitoring
Constant value (each improvement has some tactical value to our operations)
Additional data input, more visibility
Risks & Opportunities

- Staff re-training
- Configuration management
- Lack of analyst involvement
- Lack of sufficient gates/controls
- Supportability
Take-Aways

1. Automation is a process or a capability
2. Process helps us avoid rabbit holes with little or no return on our investment
3. Priorities are important: not all improvements provide equal value
4. Take an automation initiative (or proposed initiative) and try to quantify return on automation investment
Reinventing Jobs:
A 4-Step Approach for Applying
Automation to Work
by Ravin Jesuthasan and John Boudreau
Thank You!

@markaorlando
mark@bioniccyber.com