Biting into the Jawbreaker: Pushing the Boundaries of Threat Hunting Automation (#hamm)

Alex Pinto - Chief Data Scientist – Niddel
@alexpsec
@NiddelCorp
Agenda

• Who am I?
• Why does this talk exist?
• The Automation Barrier
• The Context Barrier
• The Experience Barrier
• The Creativity Barrier

• Hunting Automation Maturity Model
Who am I?

- Brazilian Immigrant
- Security Data Scientist
- Capybara Enthusiast
- Co-Founder at Niddel (@NiddelCorp)
- Founder of MLSec Project (@MLSecProject)
- What is **MLSec Project**? - Community of like-minded infosec professionals working to improve data science and machine learning application in security.
- What is **Niddel**? – Niddel is a security vendor that provides a SaaS-based Autonomous Threat Hunting System
Why does this talk exist?

Like any good story, it all started with a discussion on the Internet.
The Simple Truths of Threat Hunting
“Threat Hunting Jawbreaker”

Threat Hunting requires the focus to be on the people

Your job focuses on human adversaries but you may not encounter adversaries

You need the open-mindedness of a new person but hunting is not for new folks

Product vendors will pitch hunting but it’s not about the product

You need to rely on automation but you can’t fully automate hunting

Slide shamelessly lifted from one of @RobertMLee’s presentations. Accept no imitations.
David Bianco to the Rescue!

Why not describe hunting automation as a maturity model?

HMM0 Initial
- Relies primarily on automated alerting
- Little or no routine data collection

HMM1 Minimal
- Incorporates threat intelligence indicator searches
- Moderate or high level of routine data collections

HMM2 Procedural
- Follows data analysis procedures created by others
- High or very high level of routine data collection

HMM3 Innovative
- Creates new data analysis procedures
- High or very high level of routine data collection

HMM4 Leading
- Automates the majority of successful data analysis procedures
- High or very high level of routine data collection

[This is my first presentation without citing the PoP in 3 years]
“Data is not information, information is not knowledge, knowledge is not understanding, understanding is not wisdom.”

- Cliff Stoll
The Automation Barrier
Breaking the Automation Barrier

First Order (Indicator Matching)

- When 9 of 10 of you think of automation, you think of this.
- File hashes, YARA Rules, IP addresses, domain names
- Lowest possible bar for a vendor to claim they automate threat hunting
- Batch analysis / "Retro-hunting"
Choosing Indicators – RIG EK

Active actor registering domains - NOT Domain Shadowing

Email a.miroshichenko@yandex.ru is associated with ~234 domains ➩ Yay! Let’s go block this!!
Choosing Indicators – RIG EK

```
> bb_rig_ns <- bb_rig[order(bb_rig$num.hits, decreasing = TRUE)][bucket.type == "whois.registrant.email"][1:10]
> bb_rig_ns

<table>
<thead>
<tr>
<th>bucket.type</th>
<th>bucket.value</th>
<th>entity.category</th>
<th>num.hits</th>
</tr>
</thead>
<tbody>
<tr>
<td>whois.registrant.email</td>
<td><a href="mailto:stivemalone@gmail.com">stivemalone@gmail.com</a></td>
<td>rig</td>
<td>1353</td>
</tr>
<tr>
<td>whois.registrant.email</td>
<td><a href="mailto:stivie.malone@gmail.com">stivie.malone@gmail.com</a></td>
<td>rig</td>
<td>734</td>
</tr>
<tr>
<td>whois.registrant.email</td>
<td><a href="mailto:sizilsanksi@yahoo.com">sizilsanksi@yahoo.com</a></td>
<td>rig</td>
<td>62</td>
</tr>
<tr>
<td>whois.registrant.email</td>
<td><a href="mailto:steelehendershot@gmail.com">steelehendershot@gmail.com</a></td>
<td>rig</td>
<td>38</td>
</tr>
<tr>
<td>whois.registrant.email</td>
<td><a href="mailto:me@robcross.me">me@robcross.me</a></td>
<td>rig</td>
<td>33</td>
</tr>
<tr>
<td>whois.registrant.email</td>
<td><a href="mailto:ilan6741042@gmail.com">ilan6741042@gmail.com</a></td>
<td>rig</td>
<td>22</td>
</tr>
<tr>
<td>whois.registrant.email</td>
<td><a href="mailto:a.miroshichenko@yandex.ru">a.miroshichenko@yandex.ru</a></td>
<td>rig</td>
<td>15</td>
</tr>
<tr>
<td>whois.registrant.email</td>
<td><a href="mailto:bluestonewebdesigns@gmail.com">bluestonewebdesigns@gmail.com</a></td>
<td>rig</td>
<td>14</td>
</tr>
<tr>
<td>whois.registrant.email</td>
<td><a href="mailto:roger@ticktockholdings.com">roger@ticktockholdings.com</a></td>
<td>rig</td>
<td>14</td>
</tr>
<tr>
<td>whois.registrant.email</td>
<td><a href="mailto:spiros@wsigodigital.com">spiros@wsigodigital.com</a></td>
<td>rig</td>
<td>11</td>
</tr>
</tbody>
</table>
```

```
> bb_asn_rig_ip <- bb_rig_ip[order(bb_rig_ip$num.hits, decreasing = TRUE)][bucket.type == "asnumber"][1:10]
> bb_asn_rig_ip

<table>
<thead>
<tr>
<th>bucket.type</th>
<th>bucket.value</th>
<th>entity.category</th>
<th>num.hits</th>
</tr>
</thead>
<tbody>
<tr>
<td>asnumber</td>
<td>16276</td>
<td>rig</td>
<td>1669</td>
</tr>
<tr>
<td>asnumber</td>
<td>14576</td>
<td>rig</td>
<td>513</td>
</tr>
<tr>
<td>asnumber</td>
<td>48096</td>
<td>rig</td>
<td>103</td>
</tr>
<tr>
<td>asnumber</td>
<td>48347</td>
<td>rig</td>
<td>91</td>
</tr>
<tr>
<td>asnumber</td>
<td>35415</td>
<td>rig</td>
<td>86</td>
</tr>
<tr>
<td>asnumber</td>
<td>394279</td>
<td>rig</td>
<td>58</td>
</tr>
<tr>
<td>asnumber</td>
<td>60117</td>
<td>rig</td>
<td>28</td>
</tr>
<tr>
<td>asnumber</td>
<td>21100</td>
<td>rig</td>
<td>21</td>
</tr>
<tr>
<td>asnumber</td>
<td>19318</td>
<td>rig</td>
<td>20</td>
</tr>
<tr>
<td>asnumber</td>
<td>46606</td>
<td>rig</td>
<td>13</td>
</tr>
</tbody>
</table>
```

- **AS16276 – OVH SAS 😎 (maybe block?)**
- **AS14576 – Hosting Solution Ltd** (actually king-servers.com)
- **AS48096 – ITGRAD (any Russian offices?)**
Choosing Indicators – Context Matters

Can’t block this one, lol
Or this one either
Would not touch this one

Without context that ".com" and ".org" are usually ok, automation fails
The Context Barrier
Breaking the Context Barrier

- Using internal and external enrichments to improve decision making
- Internal:
  - Statistical analysis internal data (a.k.a all of the UEBA stuff, PCR, "stacking")
  - Knowledge from internal incidents
- External:
  - Pivoting / Visual Aids
  - Statistical analysis from enrichment data (pDNS / WHOIS)
Let’s build aggregation metrics for ”good places” and ”bad places” in traffic

We propose a ratio that compares the cardinality of the node connectedness:

- $B_{pp}$ – count of ”bad entities” connected to a specific pivoting point
- $G_{pp}$ – count of ”good entities” connected to a specific pivoting point

$$MR_{pp} = \frac{B_{pp}}{G_{pp} + B_{pp}}$$
Example - Maliciousness Ratio

- Looking at the base rate:
  - ASN Base Rate 0.6%
  - Country Base Rate 0.58%
  - TLD Base Rate 1.9%

- Telemetry from an pool of Niddel customers:
  - AS48096 – ITGRAD 87.5% => 145.9x more likely
  - Country RU 5.2% => 8.96x more likely
  - .org TLD 2.9% => 1.52x more likely
Challenges with the Approach

• How can we best define the cutting scores on all those potential maliciousness ratings?
• How to combine and weight the multivariate composition of these pivoting points?
• Solution is unique per company, including understanding telemetry patterns, risk appetite for FPs / FNs and decision points on when to block and when to alert on something.
The Experience Barrier
Breaking the Experience Barrier

- Combining all the signals from the hunting investigation and making a "call":
  - Does being registered in REG-RU and hosted in OVH enough for a conviction?
  - This shady thing is registered in MarkMonitor. Viral legit campaign?
- This "gut feeling" comes from years and years of knowledge and experience of handling alerts and incidents IRL.
Supervised Machine Learning!!

VS

THQUIRREL!
A More Involved Example (1)
A More Involved Example (2)

Build the campaign based on the relationships - they all share the same support infrastructure on the IP Address and Name Servers.
The Lee-Bianco Barrier
(a.k.a. The Creativity Barrier)
Now what?

- As threats evolve, new types of signals may be necessary for a conviction.

- If the system does not have access to the data that it requires, it cannot evaluate it for decision making.

- Some examples of recent "new" threats - Domain fronting, IDN phishing

- This is no different from "Writing a new Runbook" for your team
But what about Deep Learning?

- Convolutional Neural Networks are very good at looking at unstructured data and “figuring out” what the features should be.

- Great success for image and voice recognition:
  - Needs a lot of samples
  - Trivial to classify by a human

- Neither of these is the case for security – run away from DL vendors
Introducing HAMM
Hunting Automation Maturity Model (#HAMM)
1. Vast majority of “automating hunting” plays - a signature match. Incomplete strategy, both prone to a lot of false positives in badly vetted lists and a lot of false negatives because the lists will naturally be incomplete.

2. In this level, a system is evaluating individual hunting pivoting points registered or first visited. Identify all the entries that are related to the high maliciousness pivoting points, and even determine what they are related to based on the connections to known malicious samples.

3. Multivariate decision making by prioritizing which ones are the most relevant for detection under specific circumstances. Third Order systems can decide on the fly which variables from First and Second Order are the most relevant for an environment.
Hunting Automation Maturity Model (#HAMM)

- IOC Matching
- Signatures
- Anti-virus

- Security / Hunting Analytics
- Stats methods
- (Some) UEBA – maybe?

- Supervised machine learning with previous signals

- Rob [M|T] Lee
- David Bianco
- Probably not you
Hunting Automation Maturity Model (#HAMM)

[LAME]  [Predictive Incident Response?]  [Proactive Incident Response?]  [MAGIC]

[Threat Farming?]
"Computers are useless. They can only give you answers." – Pablo Picasso