Evolving the Hunt

David J. Bianco
Hunt Strategist
@DavidJBianco

Cat Self
Lead Threat Hunter
@CoolestCatiKnow
About Us

Enterprise detection & response specialist
Threat Hunting researcher

Threat Hunter
Former Red Team Engineer
Well-rounded Nerd (slightly biased)
It All Started When…

“I’d like you to take our Threat Hunting program to the next level.”
And Then the Meetings Started!

Strategic

Leadership
Team Leaders

Tactical

Operations
Round Tables
Our “Next Level” Opportunities

Program Focus

Operational Consistency

Hunt Topic Strategy
The Hunting Focus Had Drifted

Identifying Incidents & Gaps → Skills Development & Transfer
So We Refocused on Automation

MINIMAL
- Incorporates threat intelligence indicator searches
- Moderate or high level of routine data collection

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

LEVEL 3
- Creates new data analysis procedures
- High or very high level of routine data collection

LEVEL 4
- Automates the majority of successful data analysis procedures
- High or very high level of routine data collection

Graphic: Sqrrl
10lbs of Hunting in a 5 Day Bag

Day 1
- Data Collection
- Participant Prep
- Format Data

Day 2-4
- Format Data
- Hunt
- Submit findings

Day 5
- Findings Follow up
So We Got Help With the Bags

<table>
<thead>
<tr>
<th>Hunt Team Members</th>
<th>Week</th>
<th>Week</th>
<th>Week</th>
<th>Week</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hunter 1</td>
<td>Hunt</td>
<td>Hunt</td>
<td>Hunt</td>
<td>Hunt</td>
</tr>
<tr>
<td>Hunter 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hunter 3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Scheduling Wasn’t Working
We Start by Prioritizing Topics

We look at each topic through three lenses:

• Usage by tracked threat actors
• Risk by Impact & Likelihood
• Strength of Existing Detection
Then We Handcraft Our Brew

Sprint Theme

Priority Score

Special Requests

Sprint
In the End, it Looks Like...

Collect Hunt Ideas

Sprint Topic Selection

CTI & Detection Contribution

Set Sprint Themes

Hunt Team Grooming
Takeaways

Strategy

Preparation & Documentation

Full-Time Threat Hunters
Evolving the Hunt

David J. Bianco  
Hunt Strategist  
@DavidJBJianco

Cat Self  
Lead Threat Hunter  
@coolestcatiknow