Hunting is Sacred
It’s our right, but we never do it for sport

Ashraf M. Abdalhalim
Sr. Consultant, Incident Response & Forensics
#ThreatHuntingSummit
“Hunting is sacred, little brother. It’s our right, but we never do it for sport.”

— Bagheera

Mowgli: Legend of the Jungle

https://images.dawn.com/news/1181218

https://www.imdb.com/title/tt2388771/mediaviewer/rm2913091584
Ashraf M. Abdalhalim (TANGO)

@AshAbdalhalim

Incident Response, Sr. Consultant

FIREEYE™, MEA
Mandiant Consulting

- From SD based on SA
- Played different roles in IT & INFOSEC
- Last 5+ years, focused on:
  - Incident Response
  - Threat Hunting
  - Tactical Threat Intel
  - Reverse Engineering
Agenda

- The problem
- Case studies
- Guiding principles
- The solution
- Conclusion
The Problem
Mind the SEAMS
Hunting

In The Jungle
- Hunt = Search + Kill
- Integrated and synchronized
- Predators do both instinctively and seamlessly

In Cyber Security
- Hunt = Search
- Response = Kill
- Defenders have to do both seamlessly too

https://en.wikipedia.org/wiki/Predation
The fraternal twins

<table>
<thead>
<tr>
<th>HUNT</th>
<th>RESPONSE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Young</td>
<td>Older</td>
</tr>
<tr>
<td>Proactive</td>
<td>Reactive</td>
</tr>
<tr>
<td>Iterative</td>
<td>Trigger-based</td>
</tr>
<tr>
<td>Scope to lead</td>
<td>Lead to scope</td>
</tr>
<tr>
<td>Intra-departmental</td>
<td>Inter-departmental</td>
</tr>
<tr>
<td>Resourcing</td>
<td></td>
</tr>
</tbody>
</table>

Actually triplets...

<table>
<thead>
<tr>
<th>Hunting</th>
<th>Investigation</th>
<th>Remediation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Response</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

©2019 FireEye
Industry’s done great work to improve the Hunt and Response, sort of separately.

Do we mind the seams?

This talk addresses the seams:

- What can go wrong?
- How to stitch the seams between Hunt and Response?
  - Integrate and synchronize

[ wikibutton wikilink wikisite=en.wikipedia.org wikitext=Hunter-killer_team wikiversion=latest ]

---

Hunter-Killer team

---
Case Studies
Real cases from frontlines
Case #1

1. First finding kicked off the response

4. Subsequent hunt missions identified **new** actor(s)

2. Scope was identified and passed to Remediation

5. Scope: **different** compromised territories

3. Remediation included costly enterprise-wide countermeasures

6. High cost, tired team, and **patchy** countermeasures
Case #2

1. A finding kicked off the response

2. Scope was passed to Remediation

3. Remediation was delayed for either technical or business reasons

4. Adversary had **not** been tracked

5. By the time of the remediation, the adversary had already shifted
Case #3

1. Remediation was done with gaps, cheers, and celebrations!

2. No post-remediation assessment and monitoring

3. Gaps were not identified, removal of adversary was not confirmed
Case #4

1. Adversary’s TTPs and new hunting ideas/data were identified!

2. Obtained Intel was not leveraged

3. No follow up Targeted hunt missions
The Solution

Let’s KILL it...
“Defense is permeated with more or less pronounced elements of the offensive. In the same way, the attack is not a homogeneous whole: it is perpetually combined with defense”  Clausewitz, On War

- "Active defense: employment of limited offensive actions and counterattacks to deny a contested area or position to the enemy"  U.S. DoD Dictionary
Two as one
one + one = one

Sqrrl’s Hunting Cycle
Create Hypotheses
Inform Analytics
Uncover Patterns
Investigate

SANS Incident Response Process
Preparation
Identification
Containment
Recovery
Eradication
Lesson Learned

Hunt
Investigate
Remediate
Kill Chain (F2T2EA)

- The industry adopted the **defensive** use of the Kill Chain
- Military model to **plan** and **execute** targeting
- “**Targeting**: the process of **selecting** and **prioritizing targets** and matching the appropriate **response** to them”  
  U.S. DoD JP3-60
- “**Target**: is an entity (**person, place, or thing**) that’s considered for possible engagement to **neutralize** the function it performs for the adversary”  
  U.S. DoD JP3-60

- **Persona**: compromised account
- **Place**: compromised system
- **Thing**: utility, tool, or malware

**F2T2EA**
- Find
- Fix
- Track
- Target
- Engage
- Assess
"While steps are listed in order to ease explanation, several steps are accomplished simultaneously and overlapped"
Emerging target is discovered and characterized for further prosecution

The Hunt mission:

- Threat situational awareness
  - Adversarial TTPs (ATT&CK)
- Environment situational awareness
  - Anomalous behavior

Leads (emerging targets):

- Adversary’s capability/infrastructure
- Compromised account/system
- Location of the adversary is **determined**
- The lead is **investigated** and the intrusion is **scoped**
  - List of the compromised systems/accounts
  - Initial compromise
  - Access and persistence mechanism
  - List of utilities/tools/malware
- **Fix step stitches the seam between Hunt & Investigation**
  - Leads from the Hunt are exploited to the max
  - Intel obtained informs the subsequent hunts
    - New ideas and data sources for hunting
Find  Fix  Track  Target  Engage  Assess
- Adversary’s activities and movements are monitored
- Focused sensors
  - Endpoint
  - Network
- Track step feeds into:
  - Fix: new territories to be investigated
  - Target: to update the remediation plan
- “If Track continuity is lost, Fix step will likely have to be repeated and possibility the Find step” *US DoD JP3-60*
Matching appropriate response to the targets

Capabilities, needed to engage the targets, are selected and tested:

- Network-level blocking
- Password resetting
- Systems rebuilding/cleaning
- Timing of the engagement

Target should be kicked off as early as possible

Track stitches the seam between Investigation and Remediation

Plan is always fresh and updated based on the inputs from Track
Find
Fix
Track
Target
Engage
Assess
- Actions are **taken** against the targets
- Remediation actions are **executed** and **verified**.
  - Blocking adversary’s infrastructure
  - Rebuilding/cleaning system
  - Resetting accounts
- Preferably off the adversary’s operational hours
- Follow up sweeps are executed to confirm the desired effect
- Findings are communicated back to Fix, Track, Target or Engage steps
- Assess stitches the seams between Remediate and Hunt/Investigation
Closing Thoughts

- Despite the *symbiosis* between Hunt and Response, the *seams* exist and can lead to *failure*.

- Operational perspective, that *integrates* and *synchronizes* the Hunt and Response tasks, is crucial for *success*.

- Neither *offense* nor *defense* is a homogenous whole.

- Hunt and Response together are the manifestation of *offense* in *defense*.

- Hunt + Response => *Targeting* of adversary’s presence (*targets*) in your environment.

- *Kill Chain* can be used to model, integrate, and synchronize Hunt and Response.
Thanks! @AshAbdalhalim