Plan for an Evaluation of Government Cyber Threat Hunting Processes

William Maxam, wmaxam@purdue.edu and James Davis, Advisor davisjam@purdue.edu

Cyber intrusions cost organizations, on average, $13 million[1] and remain undetected for longer than 200 days[2]. Cyber intrusions impact:
- Governments
- Private corporations
- Critical infrastructure

Average # of days to identify a data breach[2]

Cyber Threat Hunting (TH) is a focused search to identify concealed network intruders. The early detection of adversaries translates to significant cost savings:

Dwell Time Reduction vs. Reduction in Business Impact[3]

Most organizations that perform threat hunting operate without a well-defined process[5]:

Organizations that follow a Threat Hunting Methodology[5]

Research Target

A better understanding of current cyber threat hunt processes may allow for:
- Faster integration of new members
- More efficient use of team members
- More automation of threat detection

Our Proposed Methodology:

Interview members (both experienced and inexperienced) from 2 premier Government TH organizations: one military and one civilian.

Analyze interview data, examining the TH team as a system with a focus on the process they use.

Document processes used by successful teams so that they can be studied further or implemented by teams lacking a process.

Recommend actionable changes for less effective processes which could be implemented by government or non-government teams.

Current Progress:

2 pilot studies have been conducted with more interviews being scheduled for April and May.

[1]: Accenture's 2019 The Cost Of Cybercrime report
[2]: IBM Security's 2020 Cost of a Data Breach Report
[3]: Aberdeen's 2017 Quantifying The Value Of Time In Cyber-threat Detection And Response
[4]: The Industrial Age of Hacking by Nosco et al. USENIX Security Symposium 2020
[5]:SANS 2017 The Hunter Strikes Back Report
[6]:SANS 2018 Threat Hunting Survey Results