Poster: Attendee Survey of an Educational Threat Hunting Exercise

Mahnoor Jameel, Adam Bates
University of Illinois at Urbana - Champaign
{mjameel2, batesa}@illinois.edu

I. Introduction

Cyber attacks have been increasing throughout the last decade, which makes it important to train analysts to effectively 'threat hunt'. Threat hunting involves detecting, investigating, and responding to security threats within an organization's IT infrastructure. Analysts' ability to quickly respond to threats is directly proportional to the monetary loss of an organization [1].

Despite the growing need for threat hunting, there has been little research on how to effectively train analysts on learn these skills. Outside of hands-on industry experience, educational opportunities to learn about threat hunting are limited. In this work, we partner with the facilitators of a major education-based threat hunting workshop that hosts events at universities throughout the United States. This workshop provides trainings on exemplar security tools then challenges attendees to investigate a series of multi-faceted attack scenarios designed to simulate real-world threat actors. These attack scenarios are divided into smaller subtasks that serve as Capture-the-Flag challenges. Attendees complete with one another in small teams to to complete the challenges the fastest.

To address this gap in research, our study aims to investigate the circumstances that lead to successful threat hunting. Specifically, we conducted a survey of participants who had attended the educational workshop. By analyzing the survey results, we hope to identify the factors that contribute to effective threat hunting. This information can then be used to develop more effective training programs and best practices for organizations looking to improve their threat hunting capabilities. Ultimately, this research can help organizations better protect themselves against the increasing threat of cyber attacks.

II. Educational Threat Hunting CTF

We partnered with industry practitioners to administer a survey at a popular on-going threat hunting educational workshop that took place at six different locations across the United States between October 2022 and April 2023. The workshop spans two days and includes demonstrations and tool tutorials on various security tools, including EDR, NIDs, and log search tools like Security Onion and Ghidra. The participants are walked through examples of challenge where the tools are used. The latter days of the workshop involved participants solving challenges with unique attack chains designed to simulate real-world scenarios, with the option to form teams or participate alone. Their performance and interations with the server is tracked throughout the event and stored.

TABLE I: Participant Demographics

Gender		
Male	N = 70	76.0%
Female	N = 18	19.6%
Prefer not to disclose	N = 4	4.4%
Age Groups		
18-20	N = 32	34.8%
21-24	N = 45	48.9%
25-29	N = 4	4.3%
30-34	N = 5	5.4%
35-39	N = 3	3.3%
45-49	N = 1	1.1%
60-64	N = 2	2.2%
Education Level		
HighSchool	N = 1	1.1%
Undergraduate	N = 79	85.9%
Gradaute	N = 9	13.1%

On the second day, participants have until noon to complete the challenges, after which they presented their solutions during a debrief session, which also serves as a break in the programming. At the start of this session, the facilitators advertised our online survey through an announcement and powerpoint slide, inviting all attendees to participate while making it clear that the survey was separate from the workshop and not mandatory. Attendees that participated in the survey were given a $15 Amazon e-giftcard in exchange for their participation.

III. Methodology

To gain comprehensive feedback from participants, our survey was structured into different sections. The first category focused on general demographics and prior exposure to security concepts. We wanted to know if participants had any relevant experience before attending the workshop, as this could influence their performance in the competition.

The later sections of the survey focused on the tools that the participants used during the event and the Capture-the-flag challenges they solved. We asked participants to explain how they solved certain challenges and what difficulties they faced. This feedback was valuable in understanding the effectiveness of the tools and identifying areas where additional support may be necessary to improve performance in future workshops.

In addition to our survey, the facilitators of the workshop shared data from the CTFd [2] server with us after the event.

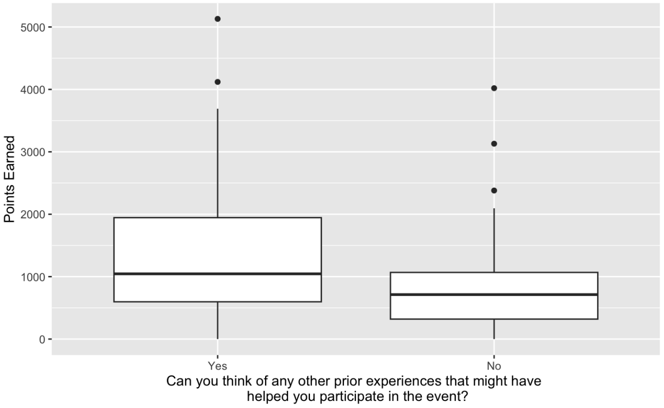

Fig. 1: Box and whisker plots comparing participants prior experience with security to the number of points they earned in the competition.

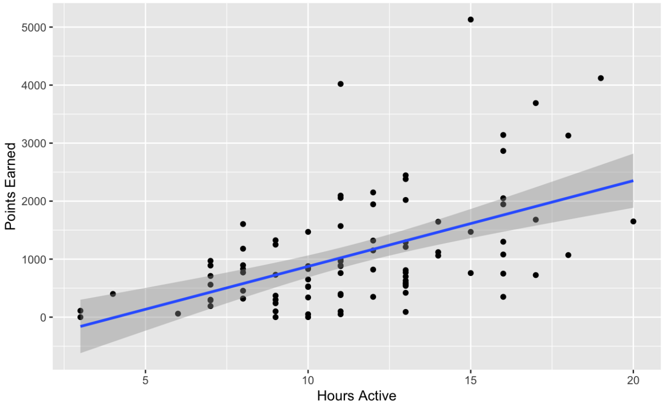

Fig. 2: Plot of Hours active on the server with the Total Points Earned

The data tracks the performance of all the attendees and provides insights into how they approached the challenges and their success rates. By combining our survey data with this information, we can gain valuable insights about which factors influence performance in threat hunting workshops. This information can be used to improve future workshops and training programs to better equip analysts with the skills and knowledge needed to effectively detect, investigate, and respond to security threats.

IV. Preliminary Results

Our survey has been distributed in six locations of the education threat hunting event, with more locations to come in the future. In total we have 91 participants. Table I summarizes our participant demographics. Below, we provide some data characterization from our preliminary analysis.

A. *Effects of Prior Exposure to Security Concepts*

We begin by comparing participants responses on the demographics questions to their points earned as recorded on the CTFd server. Figure 1 reports box and whisker plots for whether participants had participated in security extracurriculars . While prior exposure led to a small median increase in points earned, the upper two quartiles of performers with prior exposure earned many more points as compared to their counterparts without prior exposure. Although security clubs and undergraduate CTF competitions tend to focus more on offensive security than defense and investigation, it appears that these experiences may provide transferrable knowledge that aids in threat hunting tasks. Our final analysis will include a multidimensional regression modeling to determine the individual contributions of prior exposure as compared to other competing predictors.

B. *Alternate Predictors of Performance*

As an alternative to prior exposure to security concepts, we also wish to explore whether experience-agnostic factors contributed to individual participant success in the competition. One such factor is the number of hours spent solving challenges – workshop attendees were given the option to continue to work through the night between the first and second days of the event, leading to considerably variability between participants in the total number of hours worked. To investigate this, we extracted the “active hours” for each user from the CTFd server, where we considered a participant to have been active in that hour if they had interacted with the server in any way. This estimate of hours works thus may be an under-approximation if participants were working independently without staying active on the CTFd server.

Figure 2 reports the points earned per participant relative to their hours active. We observe a clear trend between hours worked and points earned, as confirmed by a simple linear regression (β=144, $p < 0.01$). This result is encouraging, as it may suggest that success in learning threat hunting skills is primarily a function of time spent. Participants with prior exposure to extracurriculars may been more successful simply because they are used to competing in CTF-style events and were prepared to work into the evening in order to succeed. Our final analysis will tease apart the individual contributions of these predictors of success.

V. Conclusion

Overall, our study suggests that both time and experience are important factors in improving performance in threat hunting exercises. By understanding and utilizing these factors, analysts can be trained more effectively, and organizations can better prepare for and prevent cyber attacks.

References

[1] 2019. How Many Alerts is Too Many to Handle? https://www2.fireeye.com/StopTheNoise-IDC-Numbers-Game-Special-Report.html.

[2] CTFd Server. https://ctfd.io/