Everybody's Got ML, Tell Me What Else You Have: Practitioners' Perception of ML-Based Security Tools and Explanations (Supplementary Materials)

Jaron Mink*, Hadjer Benkraouda*, Limin Yang*,
Arridhana Ciptadi†, Ali Ahmadzadeh‡, Daniel Votipka||, Gang Wang*
*University of Illinois at Urbana-Champaign †Truera ‡Blue Hexagon ||Tufts University
{jaronmm2, hadjerb2, liminy2}@illinois.edu, arridhana@gmail.com, ali@bluehexagon.ai, dvotipka@cs.tufts.edu, gangw@illinois.edu

1. Tasks Performed by Participants

	Technical Task	Count
Threat Detection	Intrusion Detection	7
	Alert Analysis	4
	Threat Hunting	3
Threat Mitigation	Reverse Engineering	8
	Incident Response	3
	Host-based Forensics	3
	Threat Research	1
Security Assessment	Vulnerability Assessment	8
	Compliance Audits	1
Tool Management	Integrate Multiple Tools	6
	Maintain Model/Service	4
	Manage IT Policies	3
Tool Production	Tool Design/Development	12
	Data Collection	4
	Data Curation	1

TABLE 1: **Tasks Performed by Participants** — We report the different technical tasks undertaken by the participants with/for the classification tools.

2. Screening Questions

Before we invite participants to an interview, we first ask them to fill the a set of screening questions presented here to determine eligibility (see Section 3 of the main paper for details).

2.1. Experience and Background

Q1 What is your job title?
[open text response]

Q2 Please briefly describe your job responsibilities and tasks. (two sentences is enough)
[open text response]

Q3 Which of the follow best categorizes your cybersecurity knowledge?
- Offensive Security (Red Team)
- Both (Purple Team) / General Security
- Defensive Security (Blue Team)
- Neither
- Other (please specify) [open text response]

Q4 Which of the following best describes your current employment status?
- Employed full-time
- Employed part-time
- Defensive Security (Blue Team)
- Neither
- Other (please specify) [open text response]

Q5 How many years of working experience do you have in cybersecurity?
[open text response]

Q6 What best describes the primary industry of your organization?
- IT and technology
- Financial services
- Public sector (government, education, etc.)
- Business and professional services
- Health, pharmaceuticals, and biotech
- Telecommunications
- Manufacturing and production
- Retail
- Energy, oil/gas, and utilities
- Travel and transportation
- Construction and property
- Other (please specify) [open text response]

2.2. Demographics

Q7 What is your gender?
- Female
- Male
- Non-binary
- Prefer to not disclose
- Prefer to self-describe [open text response]

Q8 What is the highest degree or level of school you have completed (If you're currently enrolled in school, please indicate the highest degree you have received.)
- 10th grade or less (e.g. some American high school credit, German Realschule, British GCSE)
- Secondary school (e.g. American high school, German Gymnasium, Spanish or French Baccalaureate, British A-Levels)

- Trade, technical or vocational training
- Some college/university study without earning a degree
- Associate degree (A.A., A.S., etc.)
- Bachelor's degree (B.A., B.S., B.Eng., etc.)
- Master's degree (M.A., M.S., M.Eng., MBA, etc.)
- Professional degree (JD, MD, etc.)
- Other doctoral degrees (Ph.D., Ed.D., etc.)
- Prefer to not disclose
- Other (please specify) [open text response]

Q9 Which race/ethnicity do you identify with? *Please check all that apply.*

- White or of European descent
- South Asian
- Hispanic or Latino/a/x
- Middle Eastern
- East Asian
- Black or of African descent
- Southeast Asian
- Indigenous (such as Native American, Pacific Islander, or Indigenous Australian)
- Prefer to not disclose
- Prefer to self-describe (please specify) [open text response]

Q10 What is your age? (in years)
[open text response]

Q11 What country do you currently reside in?

- [List of all Countries]

Q12 Are you physically located in an European Economic Area (EEA)?

- Yes
- No

Q13 Please provide your email so we can contact you and send you an amazon gift card for your participation. (Both corporate and personal emails are fine)
Your email will never be used to associate you with your responses. Your email will be permanently separated from your responses once you have been compensated.
[open text response]

3. Interview Guide & Questions

To maintain consistency between interviews, the interviewer followed the interview guide presented here to ensure responsible procedures for conducting qualitative interviews. This interview guide was adapted from the one presented in Rader et. al [1].

3.1. Before Attendee Enters

Room Owner:

- Make sure the host gives every other researcher co-host ability.
- Make the researcher who is recording to the cloud host (ask for co-host after you give it away!).
- Record to two different places (locally, to cloud), for example https://obsproject.com/ or quicktime on mac).

Everyone:

- Turn on Cameras, test mics.
- Open interview-specific script.

3.2. When Attendee Enters

Introduction:

- Greeting, introduce yourself and the group, thank them for coming e.g.: Good afternoon! Thank you for coming and participating in our interview study. I am _____ and I'm joined by my research colleagues _____.

Overview:

- **Describe study, procedure, expected time e.g.:** We're going to be asking you some questions today about your experiences working in the security field. We expect this interview will take around an hour to complete.
- **Reassure them to give honest answers, we aren't judging or testing:** We're trying to gather your honest thoughts and views on this subject so we'd like to assure you that we aren't trying to test your knowledge or judge your opinion. We may ask you questions on subjects you aren't knowledgeable on, it's perfectly alright to say you are unsure or you don't know.
  You may reassure them that not doing everything perfectly is normal, e.g., "you may not always have time to..."

Consent:

- **Reference the consent form, remind them of confidentiality and opt-out e.g.:** When taking our survey you signed a consent form, I just wanted to emphasize that what you say to us during the interview will be kept confidential, and you can stop participating at any time, just let us know. If you feel uncomfortable answering any question, we can skip them with no penalty.

Questions before beginning:

- **Ask for questions about the procedure:** Before we start recording and begin the interview, would you like to ask us any questions?

Recording:

- State that you will now turn on the recording, **then do so**, tell them it is now running & re-ask for consent if needed (local / state laws).
- Verify that the host is also recording to cloud, and assigned backup is also recording.
- State the participants ID/qualtrics code/..., as well as date and time and interviewer names, to make matching easy later on.

Interview:

- Ask the interview questions, remember not to prime, listen carefully, and follow up where appropriate.
- Maybe cross out questions that you don't have to ask.

Questions: Background

Q1 Can you tell us a bit about your job? What are your current duties and what do you do on a day-to-day basis?

Q2 In performing your job, is there anyone you interact with? What do these interactions typically look like?

Questions: Usage of Classification Tools

[Read Aloud] We're going to be asking you a series of questions around "Classification tools". You can consider this any tool that makes a decision or helps you decide if some event, or piece of data, such as a file or network packet, is "Benign" or "Malicious". This could take the form of a set of matching rules, heuristics, or a machine learning model, among others. Before we continue, do you have any questions?

Q3 What classification tools do you use to assist you? What information is provided?

[Optional] Could you explain in your own words how these classification decisions are made?

Q4 Can you give an example of how you might utilize the results of the tool?

Q5 Do you ever adapt the tools for your environment/use cases? **[If yes]** How and Why?

Q6 What were some factors taken into consideration when deciding to use this tool compared to others?

[Optional] Do you ever evaluate whether a tool is effective? If so, could you explain how that evaluation is done?

Q7 Do you have any concerns that the tool may provide incorrect responses?

Questions: Perception of ML Models

Q8 Have you heard about any tools that use ML?

Q9 [If ML tool previously mentioned] You mentioned using a machine learning-based tool, could you tell me a bit more about that tool? [If ML tool NOT previously mentioned] Do you utilize any machine learning-based tools? What are they?

Q10 [if an ML tool is used] Could you name some reasons why you utilize a machine learning model-based tool? [if an ML tool is NOT used] Could you name some of the reasons why you don't utilize a machine learning-based tool?

Q11 [if an ML tool is used] Although you do use them, do you see any negatives related to using a machine learning-based tool? [if an ML tool is NOT used] Although you don't use them, do you see any benefits related to using a machine learning-based tool?

Q12 Has machine learning exceeded or fallen short of any expectations?

Questions: Machine Learning Explanations

[Read Aloud] Suppose you were using your regular tool to perform [your task]. Assume that you run the tool to evaluate, and it unexpectedly reports the analyzed [object/file/behavior/event] as malicious.

Q13 What do you currently do when one of these tools tells you a classification decision you weren't expecting?

[Optional] What kind of information could help you feel confident in deciding your next actions? Suppose you were in the same scenario, but instead of your normal tool, you now used a machine learning-based model as your tool.

Q14 Would this change what you do after your tool tells you a classification decision you weren't expecting?

[Optional] In this new scenario, what kind of information could help you feel confident in deciding your next actions?

[Read Aloud] We're now going to present some ideas for additional information that may help you in circumstances like these.

Q15 If the model presented to you a history of how the [file/object/event/etc] arrived at its destination, would you find that helpful?

Q16 Similarly, if the model highlighted the history that has influenced the model decision the most, would you find it helpful?

Q17 If you know the confidence of the model's prediction for a specific instance, would that make any difference in your reaction? I also posted it in the chat to help you keep track of it.

Q18 Do you think it would be helpful to get examples of similar [object/file/behavior/event]? If so, what would a similar example look like for you? How would you use this information?

Q19 Would the set of top measurements/features that are driving the prediction be useful?

Q20 Given all the points that were brought up (enumerate all options in chat), which one of the above added information would you find more useful?

[Shared in Chat]

- (Highlighted) Object History: A (highlighted) history of the object and its important interactions that led to its classification.
- Prediction Confidence: A number from 0-100 describing the confidence of the classification.
- Similar Examples: A set of objects that had similar features and their resulting classification.
- Highlighted Features: A set of highlighted features that were most important in determining the object's classification.

Q21 How would you use this additional information, what changes? Why would this be helpful in performing your job? e.g., Confidence, effectiveness, cut time, provide justification, catches mistakes

Q22 If you could add any piece of information, what would ideally add to the classifiers result to best help you? How would this be helpful? **[If yes]** What would it look like?

Q23 If you had access to these additional pieces of information, would this change affect your opinion of using a machine learning system?

Q24 If you had access to these additional pieces of information, would this change how machine learning is used in your company?

Q25 Would you have any additional worries in using or having an explanation method? **[If not mentioned]** Do you think a false explanation could mislead you?

Q26 These are some of the proposed techniques for machine learning explanations. Have you heard of these or any similar techniques before? **[If yes]** From where?

Q27 Would you expect any kind of standard for these explanations to help communicate with other stakeholders? **[If yes]** What might you expect this to look like?

3.3. After the Interview

- Turn off the recording, state that you did so.
- Remind them of the procedure for compensation.
- Ask if the participant still wants to say anything or ask any questions.
- Thank them for their time and participation again, wish them a nice day.
- Sometimes people want to learn about results; note their contact details and remember to send them a draft of the paper.
- Possibly debrief.

References

[1] E. Rader, S. Hautea, and A. Munasinghe, ""i have a narrow thought process": Constraints on explanations connecting inferences and self-perceptions," in *Proc. of SOUPS*, 2020.