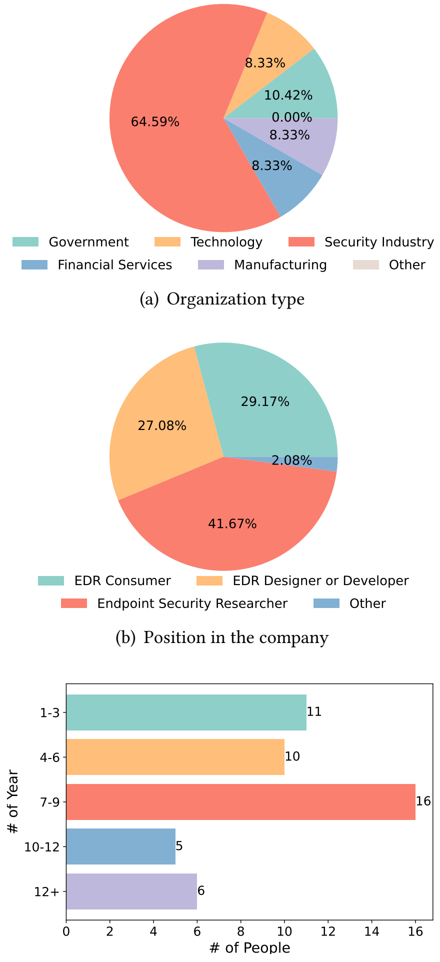

(a) Organization type

(b) Position in the company

(c) APT combating experiences

Figure 5: Participants of our online questionnaire

A BACKGROUND OF QUESTIONNAIRE PARTICIPANTS

Figure 5 shows the type of organizations, position in company, APT combating experiences of participants in our questionnaire study.

B ONLINE QUESTIONNAIRE

Our team has been working on provenance-based endpoint detection and response tools (P-EDR) for Advanced Persistent Threats (APT) detection for many years. We are currently working on a 10-minutes questionnaire for understanding the industry’s expectations about P-EDR systems. The finding may inspire us to design better P-EDR systems. This work was approved by our institution and we strictly follow our institution’s research data management policy. Your personal privacy information will be carefully processed and your thoughts will be accurately reflected in our study. Thanks for your participation!

(1) What is your job type?
- EDR Consumer
- EDR Designer or Developer
- Endpoint Security Researcher
- Others

(2) How many years of experience do you have in your role?
- 1 - 3
- 4 - 6
- 7 - 9
- 10 - 12
- 12+

(3) How would you rate your level of expertise in endpoint security monitoring?
- Very low
- Low
- Medium
- High
- Very high

(4) What is the type of organization you work in?
- Government
- Technology
- Security Industry
- Financial Services
- Manufacturing
- Others

(5) How many endpoints need to be protected in the SOC you work in?
- 0 - 1000 hosts
- 1001 - 10,000 hosts
- 10,001 - 100,000 hosts
- 100,001 - 1,000,000 hosts
- more than 1,000,000 host
- I don’t know

(6) What is the minimum amount of memory required on the machine where your EDR server is installed and running?
- 8 - 16GB
- 17 - 32GB
- 33 - 64GB
- 65 - 128GB
- more than 128GB
- I don’t know

(7) What is the average maximum amount of the host RAM memory that the EDR local agent runtime can occupy?
- < 100MB/host
- < 150MB/host
- < 200MB/host
- < 250MB/host
- more than 250MB/host
- I don’t know

(8) What is the average maximum percentage of the host CPU that the edr local agent runtime can occupy?
- 1 - 3%
- 4 - 5%
- 6 - 8%
- 9 - 10%
- more than 10%
- I don’t know

(9) How many security analysts are responsible for the above hosts?

- 1
- 2
- 3 - 4
- 5 - 10
- more than 10
- I don't know

(10) How many EDR alarms can a security analyst investigate on average per day (calculated on an eight-hour work schedule)?

- < 100 alarms/day/person
- < 150 alarms/day/person
- < 200 alarms/day/person
- < 250 alarms/day/person
- more than 250 alarms/day/person
- I don't know

(11) For graph-based APT detection device, how many nodes does the detected graph need to be controlled within?

- < 30 nodes
- < 50 nodes
- < 70 nodes
- < 100 nodes
- more than 100 nodes
- I don't know