Cybersecurity Usage in the Wild: A look at Deployment Challenges in Intrusion Detection and Alert Handling

Wyatt Sweat
Virginia Tech
Blacksburg, Virginia, USA
wyattsweat@vt.edu

Danfeng (Daphne) Yao
Virginia Tech
Blacksburg, Virginia, USA
danfeng@vt.edu

ABSTRACT

We examine the challenges cybersecurity practitioners face during their daily activities, employing a survey and semi-directed interview for data gathering. Practitioners report on the frequency and level of threats as well as other factors like burnout. These factors are observed to vary with organization size and field (e.g. Medical, E-commerce).

CCS CONCEPTS

• **Security and privacy → Usability in security and privacy**.

KEYWORDS

intrusion detection, human-computer interaction, cybersecurity

ACM Reference Format:
Wyatt Sweat and Danfeng (Daphne) Yao. 2023. Cybersecurity Usage in the Wild: A look at Deployment Challenges in Intrusion Detection and Alert Handling. In *WRIT '23: 8th Workshop on Research for Insider Threats, December 04, 2023, Austin, TX*. ACM, New York, NY, USA, 9 pages. https://doi.org/XXXXXXX.XXXXXXX

1 INTRODUCTION

This study covered the day-to-day operations and potential areas for improvement of cybersecurity practices. It is important to understand the implementation of policies with cybersecurity practitioners in the field. This practice can both illustrate the gap between the researched best practices and the current implementation as well as inform research goals going forward. We collected data from cybersecurity practitioners in different industries by distributing a survey and performing semi-structured follow-up interviews with a subset of the respondents.

There are several cases that motivate our work. The industry can significantly lag behind the research as illustrated in health care [5], local government offices [4], and others. Malicious actors may initiate actions to expand the attack surface due to the changing times such as enforced telecommuting during the COVID-19 pandemic [10]. How sensitive data is handled across multiple locations can likewise increase the attack surface. This change may be caused by the relationship between an organization and their customers. For example, hospitals may share very sensitive data between themselves where a single weak link could allow for exfiltration of patient data [5]. A hosting provider would need to work together with the cybersecurity practitioners of its client organizations to ensure data stability.

We seek to answer 4 sets of research questions with this work:

RQ1: What is the relationship between the frequencies between manual detection, false positives, and the delay between the start of an attack and detection?

RQ2: What are the common points where a cybersecurity practitioner is experiencing difficulty? What sort of system implementation could be conceived to increase the practitioner's efficiency?

RQ3: Are there currently tasks that are separate that could be integrated and streamlined to build a more holistic approach in dealing with malicious actors?

RQ4: What threats are major concerns for cybersecurity practitioners? How common are these attacks observed? Is there any relation between organizational size or sector (e.g. Medical, E-commerce, etc) and their priorities and encountered threats?

We conducted a two part investigation of cybersecurity practitioners. The first is a survey that quantifies the experiences of practitioners within their organization. The second part is conducting interviews over Zoom to gather qualitative data.

Our key contributions include:

- Interviewed participants reporting how the relations between organizations can guide cybersecurity policies. For example, a cloud service provider will need to have a policy that can accommodate the client's cybersecurity policy within it. An Intrusion Detection System (IDS) should be able to operate seamlessly within this nested security setup.
- The capabilities of cybersecurity resources varied wildly between our interview participants. Larger organizations had their own "red teams", seeking different vectors to attack and locate vulnerabilities in their organization that can be resolved. Smaller organizations lack their own specialized teams. They may have a skeleton crew who manages more than just cybersecurity or even hire outside contractors to manage their IDS. While some tools benefit both sizes of organization, research can be specialized for an organization's resources to better serve their needs.
- We queried interviewees on the effect of the COVID-19 pandemic on their organization from a cybersecurity perspective. Machines were often shifted from company owned and maintained property to employee owned leading to difficulties in managing updates. IDS that heavily weighted connection

WRIT '23, December 04, 2023, Austin, TX

ACM ISBN 978-1-4503-XXXX-X/18/06.
https://doi.org/XXXXXXX.XXXXXXX

location saw a decrease in precision due to the near instant shift to telecommuting across an organization. While the lockdowns are over in most parts of the United States, it does illustrate the effects of a major shift in how organizations operate which is valuable to consider for future events.
- Our study identifies the common high concerns and threats encountered for cybersecurity practitioners. We consider this both for specific organizational types (e.g. Medical) and the size of the organization.

2 RELATED WORK

A prior study [10] examined the cybersecurity challenges from telecommuting through interviewing participants over video conferencing. The target participants used computers regularly and had recently telecommuted for 3 weeks or longer prior to the study. Their work focused on the side of the telecommuter and the implications of their experience instead of the cybersecurity practitioner. This work was conducted during the pandemic looking at the strain of organizations that lacked a comprehensive telecommuting policy. Also of concern were what technologies and procedures were in place in relation to cybersecurity (e.g., VPNs). Finally, it examined the issues the end users experienced in day-to-day operation.

The work of [4] examined the current cybersecurity policies in various municipalities in the United States. The researchers surveyed cybersecurity practitioners in various local government offices of cities with populations greater than 10,000. The questions focused on the adoption of policies meant to secure data in a "Yes/No/Don't know" format. Their work showed a significant gap in the logging of connections, encryption, and access control. This quantitative study did not include a follow-up interview that would examine any nuances that could change the importance of the data. For example, one city might rely on data entry to a machine and not on the network that would change the attack surface.

In [5], the researchers interviewed cybersecurity practitioners in hospitals. The paper mentions the difficulties specific to hospitals in the sheer variety and number of medical Internet of Things (IoT) devices connecting to the network, adding to the overall complexity. Hospitals that work within the same network increase the attack surface dramatically and could have different levels of adoption of cybersecurity practices. A model in the paper illustrated areas that would be best for a cybersecurity practitioner to focus on in decreasing the overall vulnerability.

The work of [13] examined how rules are generated within Security Operation Centers (SOC). They interviewed 17 professionals over 9 organizations. Four of the nine organizations used custom internal rulesets with no use of pre-existing paid or community rulesets. One third of the organizations used a combination of custom internal and external (community or paid) rulesets to generate their alerts. The most important factors found for a rule were how well a rule could cover multiple variations of a threat type, the total number of alerts generated, and the false positive rate. False negative rate was not rated highly, with only 18 % of participants rating it as important. Responses focused on reducing the overall workload of the analysts, even at the sacrifice of overall coverage.

In [8], the researchers interviewed Chief Information Security Officers (CISOs) on how their interactions with directors affected the handling of cybersecurity threats and policy within their organization. Their work provides evidence that the directors have a strong reliance on the knowledge provided by the CISOs. This even extended to the point where some CISOs were believed to obfuscate results without being detected. Our work builds on this implicit trust and knowledge gap in the importance of communication between cybersecurity personnel and management for accomplishing their work.

3 BACKGROUND AND METHODOLOGY

An Intrusion Detection System (IDS) monitors an organization's computer resources for an intrusion. This system can manage a single computer or a network and includes other devices such as Internet of Things (IoT). An intrusion is any malicious activity that can hurt the underlying system, whether from external means or internal ones [6]. An employee intentionally transferring sensitive data to an unauthorized external IP address is an example of an internal intrusion, also known as an Insider Threat. An example of an external attack would be someone from outside the organization's network exploiting a zero-day vulnerability to gain unauthorized access to a machine.

Signature-based systems are primarily designed to defend against known threats [6]. Their detection schemata search for particular patterns when examining the system. A pattern of behavior may be defined as discrete rules or thresholds to flag malicious behavior. Signature-based detection systems often miss novel threats outside of what it has been designed to detect. Supervised learning models may be trained on labeled data to spot these malicious actions.

Anomaly-based detection schemata examine the incoming data looking for outliers. These outliers suggest a potentially malicious behavior that is then flagged as a potential threat. As this method is looking for unusual behavior, it does not require a training set of malicious behavior or an overarching policy to function. An anomaly-based detection system may flag unusual benign behavior as malicious.

Regardless of the type of detection methodology employed, the IDS is meant to reduce the workload of a cybersecurity practitioner. False Positives (FP) must be examined and dismissed by the practitioner. An excessive amount of FPs will decrease the efficiency of analysis work. False Negatives (FN) are attacks undetected by the system and would require manual detection methods. If the entire attack goes unobserved, then the system will be vulnerable to the malicious attacker's whims. The delay between an attack and its detection can determine the level of damage to the system. An Advanced Persistent Threats (APT) attack could span over several months with a focus on remaining stealthy. Others may reach their goal within a few hours such as a Distributed Denial of Service (DDos) attack. We seek to track all of these metrics in our study.

In our investigation of current day-to-day experience and pain points of cybersecurity practitioners, we conducted an investigation divided into two parts. The first was an online survey hosted with QuestionPro software. The second was a series of interviews conducted over Zoom. Both parts were approved by our university's IRB board. Our analysis was performed using Python 3.8.10 and the Statsmodels package. Graphs were created with Matplotlib and Seaborn packages for Python.

3.1 Survey Design

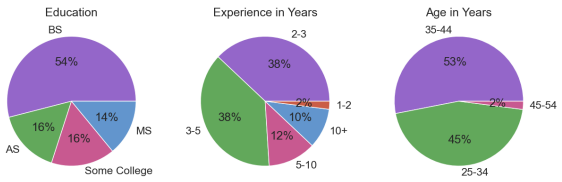

Figure 1: Demographics of the participants

Our target demographic is cybersecurity practitioners who have worked in the field for at least a year and are 18 years or older. The survey was created to take an average of 5 minutes to complete. We chose this over our original longer survey that received few participants. As portions of the data gathered could have a negative impact on the individuals or their respective organizations, we did not collect any personally identifying information for the survey. Survey participants tended to be between 35-44 years old (53%), have 2-5 years of experience (76%), have a Bachelor's degree (54%), and reside in the US (90%). For a full breakdown please see Figure 1.

We recruited 129 participants total. To ensure the data quality, our survey featured an image of a hyperlink that contained an improper top level domain and did not use a secure sockets layer (SSL). We asked if this was a phishing attempt or a legitimate link and their reasoning for their selection. This question aimed to filter out participants who lack basic cybersecurity knowledge. The short answer portion prevents an uneducated guess from being correct. After filtering the participants on survey completion and their answer to the above, we were left with 50 participants. Our main channel for recruitment was Reddit's r/cybersecurity (95%). Secondary sources were Commonwealth Cyber Initiative (CCI) advertisement (1%), and recommendations from interviewees (4%). Participants were offered $10 in compensation for their time.

3.2 Interview Design

Our target demographic was the same as the survey except for selecting cybersecurity practitioners who had worked in the field for at least 3 years. This interview was meant to take 30 minutes to complete and was conducted using Zoom. We did not collect any personally identifying information for the interview, as portions of the data gathered could have a negative impact on the individuals or their respective companies. In the case of them accidentally volunteering that identifying information mid-interview, we redacted it from our transcripts.

We recruited 10 participants total. The interview recruitment was an opt-in process with explanations that the discussion would be recorded and that they could quit at any time. The pool of interviewees was pulled from the same as the survey participants. Participants were offered $50 in compensation for their time.

A template was followed for the interview with additional questions asked if it seemed relevant to the study. For example, a participant might state their company did not worry about insider threats and later in the interview recount a textbook case of company secrets being leaked due to an insider. The nuance can be lost when participants are expected to follow a very structured Q&A. Likewise, what we assume are their concerns does not necessarily match up 1 to 1 with their actual concerns as shown in our results section.

4 SURVEY RESULTS

In this section, we present and discuss the results from our online survey.

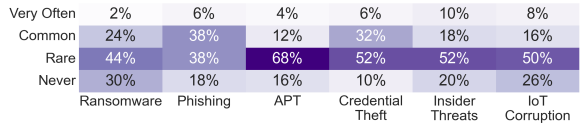

Figure 2: Observed frequency of threats encountered

4.1 The Frequency of Threats by Type

We queried participants on how often they encountered various types of threats as shown in Figure 2. This question was posed in reference to **RQ4**. We divided our categories into "Never", "Rare", "Common", and "Very Often". Survey participants were able to select one for each type of threat and could select the same frequency for different threat types if desired. Participants reported phishing and credential theft as seen commonly or more frequently 44% and 38% of the time, respectively.

For cybersecurity practitioners working within the medical field, IoT corruption and insider threats were reported as seen commonly or more often 50% of the time. IoT corruption is a glaring problem for hospitals who have a large amount of medical devices with little security [5].

A reported 27% of practitioners working in E-commerce reported insider threats as being encountered 'Very Often'. This threat type was more frequent than any other type. Several of the examples of threats given by E-commerce interviewees fell into this category as mentioned in Section 5.6.

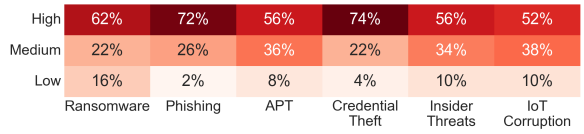

Figure 3: Level of concern of threats by type

4.2 Level of Concern of Threats by Type

In reference to **RQ4**, participants were asked to rate their concern over various attack types as seen in Figure 3. We divided our categories into "Highly Concerned/Priority", "Medium Concern/Priority", and "Low Concern/Priority". Participants were able to select one for each type of threat and could select the same level of concern for different threat types. Phishing and credential theft were the most commonly reported high concerns at 72% and 74% respectively. Phishing and credential management were commonly mentioned as major points of concern in our interviews in Sections

5.5 and 5.8 and the most commonly encountered threat type as shown in Figure 2.

Practitioners working within E-commerce rated insider threats as a high concern 73% of the time, beating out the other types. Participants of organizations with 100 or less total employees reported insider threats as a high concern 82% of the time, second only to credential theft at 86%. This could clash with common sense, where a smaller organization may expect a higher degree of loyalty from employees due to being more close-knit.

In Section 4.1, IoT corruption was reported as a common occurrence for cybersecurity practitioners in the medical field. Despite that result IoT Corruption was seen as only a medium priority half the time.

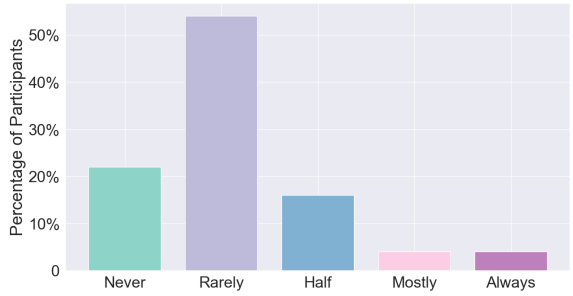

Figure 4: Percentage of participants reporting the frequency of false positives in their detection model's alerts

4.3 The Frequency of False Positives

We queried survey participants on the frequency they encountered false positives from the alerts generated by their IDS as shown in Figure 4. We divided the answers into a 5 part selection of "Never", "Once in a while", "About half the time", "Most of the time", and "Always". The most common answer was "About half the time" at around 40%. Over 59% of the respondents experienced false positives as often or more than true positives.

About 24% of respondents reported rates outside of our expectations, experiencing false positives half the time or more frequently. For example, the works of [7] and [1] report a precision of 83-93% and 87%-100% respectively. We speculate that the day-to-day operations of an organization over the course of several years will differ from a simulation or a small subset of the process. As discussed further in Section 5.3, multiple organizations with different cultures and processes may collaborate on a project. This interaction can create outliers that would lead to false positives. Expanding evaluations to include production datasets over extended time frames should give results more in line with actual applications.

For the anomaly-based approach, most (82%) reported false positives seen rarely or never. For participants using both methodologies, 77% reported seeing them rarely or less often but there were 15% less reports of false positives seen over half the time than an anomaly-only methodology. In reference to **RQ2**, a subset of cybersecurity practitioners could benefit from decreasing false positive frequency but the majority are within the expected performance. As mentioned above, more representative datasets might aid in lowering FPR.

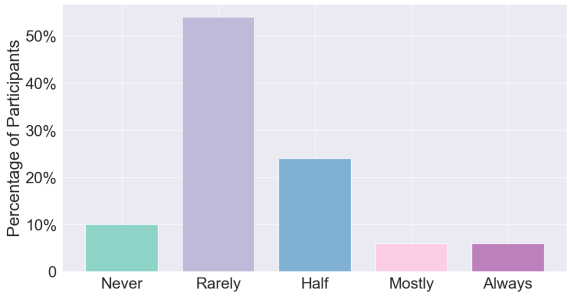

Figure 5: Percentage of participants reporting the frequency where manual detection was required in detecting an attack

4.4 Manual Detection Rate

Survey participants were questioned on the frequency they needed to manually examine their system to find a malicious event as seen in Figure 5. The answers were divided into a 5 part selection of "Never", "Once in a while", "About half the time", "Most of the time", and "Always". The most common response was "Rarely" at 54%.

Manual detection could be prompted by a proactive or reactive approach. An example of a proactive action mentioned in our interview process would be a "red team" bringing an issue to the cybersecurity practitioner before it was exploited. An example of a reactive action would be a customer or peer complaining of an issue and then the practitioner searching for the related malicious events. For smaller organizations, manually detecting false negatives can cost valuable human resources they may lack. Conversely, waiting to react to issues can erode customer trust with the organization. Balancing the reduction of false negatives with positives should be an important goal for IDS systems. This is discussed further in Section 5.1 during our interviews.

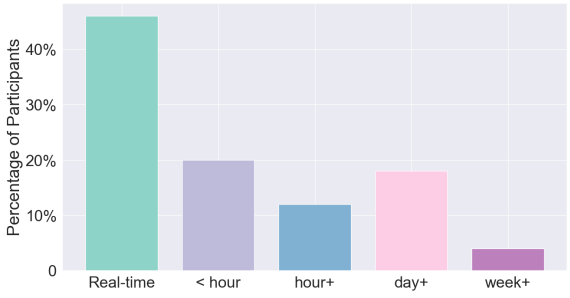

Figure 6: Percentage of participants reporting the delay between initial attack and a generated alert

4.5 Average Report Time

Survey participants were queried on the average delay between a threat being present and their IDS generating an alert. Figure 6 illustrates the delay between the initial attack and when it was discovered. We divided our sections into "Real-time", "< hour", "hour+", "day+", "week+", and "month+". More accurate timing was not used as we were asking participants as opposed to running tests directly on their system. The most common answer was "real-time" at about

Table 1: Participant distribution by organization sector and number of employees

Sector(% Total)	10-100	100-1000	1000+
Financial(20%)	10%	10%	0%
Governmental(10%)	6%	4%	0%
E-commerce(22%)	8%	12%	2%
Technology(30%)	12%	8%	10%
Medical(12%)	4%	6%	2%
Other(6%)	4%	2%	0%

46%. Of the intrusions or other malicious activity detected, most (78%) were found within a day. The remaining 22% of threats still took a day or more to discover.

In reference to **RQ1**, the delay time on an IDS is an important metric to consider along with precision and recall. For example, detecting an APT attack once the data has been exfiltrated is far worse than detecting it at the initial compromise. As discussed in our interview process in Section 5.4, many organizations do not have sufficient detection capabilities for the initial attack. Evaluating datasets by replaying them in real-time and recording the elapsed time before detection is an important metric that should be added in researching the effectiveness of a proposed solution.

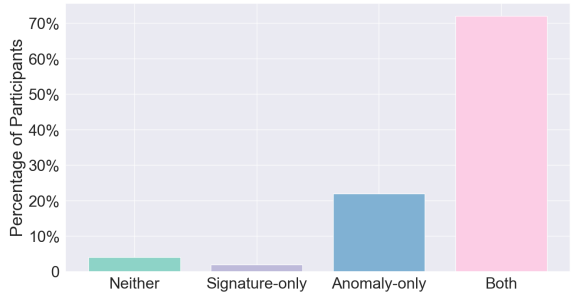

Figure 7: Percentage of participants whose organization used the listed model types

4.6 Detection Model Type Usage

As shown in Figure 7, regardless of organizational sector, the majority of respondents worked with solutions that leveraged both signature-based and anomaly-based solutions to detect threats. This does not mean that every dataset would be analyzed by a hybrid approach between the two, but that a variety of techniques are employed within their IDS.

Survey participants were questioned on their use of signature-based methods for threat detection. About 74% of participants stated that they used signature-based solutions in their work, with 2% responding that it was their sole method, as shown in Figure 7.

We sought to understand how often these rules were updated. Both the extremes of 'Never' and 'Daily' had a 28% chance with 'Weekly' and 'Monthly' at 21% as shown in Figure 8.

Survey participants reported on whether they employed anomaly-based detection methods or not. Around 94% of practitioners used

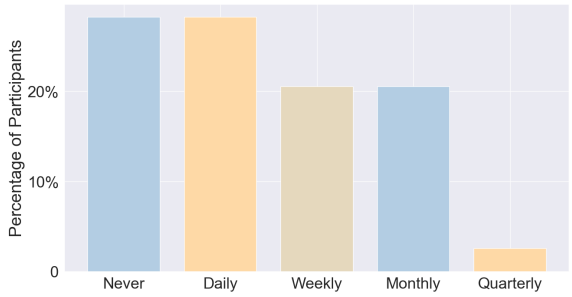

Figure 8: Percentage of participants reporting how often the rules were updated for signature-based detection methods

anomaly-based detection in their work, with 22% responding that it was their sole method as shown in Figure 7.

We wanted to understand if these were models that required retraining. About 72% stated that their models are regularly retrained while the remainder (approximately 28%) stated they were not.

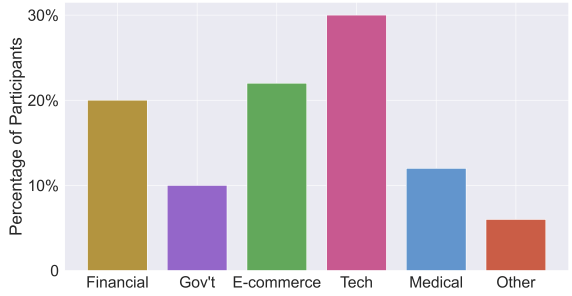

Figure 9: Demographics of the survey participants by organizational sector

4.7 Organization Demographics

Survey participants reported what sector their organization belonged to as seen in Figure 9. Participants were provided with a choice of "Financial", "Governmental", "E-commerce", "Technology", "Medical", and "Other". The Technology sector held the most respondents at about 30% with the E-commerce sector coming in second at about 22%. The largest group of participants (44%) worked for organizations with 100 or less employees, 42% worked for organizations between 100 and 1000 employees, and the remainder (14%) worked for larger organizations. Table 1 breaks down the distribution between organization sector and employee population.

The interviewees employed at smaller organizations either performed general IT tasks in addition to their cybersecurity role or were part of a cybersecurity consulting team working for multiple companies. This is explored further in Section 5.4.

4.8 Implications

- The highest concern for participants were dealing with phishing (72%) and credential theft (74%) as seen in Figure 3. These are the threats encountered commonly or more frequently 44% and 38%, respectively as seen in Figure 2.

- Within Medical organizations, IoT corruption and insider threats were seen commonly or more often 50% of the time. Despite that, IoT Corruption was only rated as a medium concern half the time which could put patients at significant risk.
- Smaller organizations rated insider threats as being an especially high concern (82%). This may break common sense, where the loyalty of employees might be assumed to be higher in smaller organizations.
- The majority of respondents (72%) employed both Signature and Anomaly-based IDS solutions in their organizations.

5 INTERVIEW RESULTS

In this section, we present and discuss the results of our 10 interviews performed over Zoom. The size of the organization participants were employed in varied from less than one hundred to over a million. For each issue reported by participants we discuss possible research directions and challenges.

5.1 The Need for Reducing Manual Forensic Workload

Some participants spoke on a single threat being the sign of a larger attack. They would need to look for further instances of that threat from other employees or machines. For example, there is an insider threat detected and forensic analysis shows it exfiltrated data to a particular internet address or service. The cybersecurity practitioner would want to know if any other employees interacted with that address that were not initially reported. Performing this task manually would be a needless time sink. If the results of the forensic analysis used the same model such as a provenance graph [3] then features from the forensic analysis could be transferred to the next round of detection. Events previously under the threshold could then throw alerts. The efficiency of the cybersecurity practitioner's time would be maximized.

After a successful malicious threat has been detected, the cybersecurity practitioner may prioritize recall over false positive rate (FPR) for related threats. Adopting a human-in-the-loop [16] model would allow the practitioner to adapt to the changing circumstances in response to malicious actors. This has been examined within IDS before for single cybersecurity tasks [12]. Research towards a human-in-the-loop system could bridge the gap between related tasks. For example, the cybersecurity practitioner may narrow down the attack to a certain signature, set of API calls, etc. Cross-referencing the expert's results against the model's could uncover undetected threats that were low confidence false negatives before. This process would be an example of a task that could be streamlined as mentioned in **RQ3**.

An additional technical challenge is how to update the machine learning model to reflect newly discovered threat cases without having to retrain the ML models from scratch. This is particularly challenging for anomaly detection models that are often originally trained on benign samples.

5.2 Software-as-a-Service handling nested security policies

Some participants report the need for client organizations to have their own security policies that work within cloud provider platform's policies. These different levels of security policies form a nested structure. However, the current security practice enforced by the cloud platform often is unable to handle the nested client-level rules with an automated system.

> "*There might be a security team who really knows how to [redacted] but they're bottlenecked in your company. So you say "well okay, I'm going to let you create your own rules, your own permissions but I'm going to put a policy that establishes guard rails that you can't do anything outside of what this boundary policy says.*"

As an example, the European Union enforces the General Data Protection Regulation (GDPR) for data protection and privacy. Works such as [9] use Natural Language Processing (NLP) to map the GDPR ruleset onto compliance management. There is only a single set of rules for this setup. With multiple sets of rules from different sources, the solution would require multiple layers that must operate without conflicts. Implementing this solution from the provider's side would be a white box problem as all the rules would need to be known. From the client's side, the provider's ruleset might not be fully explained to the client creating a black or gray box scenario.

5.3 The need for understanding the semantics of applications when designing detection solutions

Participants brought up several points that suggested a demand for better cybersecurity analysis methods for data sharing between organizations. Interviewees specifically mentioned APIs as being common vulnerabilities. This may be exacerbated as a high throughput can be a requirement for the communication channel in business-to-business level communication. The research performed by [2] of an attack specific query language and [15] partitioning a graph of the interactions within the monitored traffic. Both offer possibilities for handling a large volume of data. Adding a real-time limitation creates another hurdle to consider. Brute force attacks become easier for the attacker if the connection allows for millions of attempts in a short time span as one interviewee recalled:

> "*... and they were like, "you have this API that will tell us if credentials are valid or not" and I'm like "yeah, okay, so?"... [and they said] "and I burned through 72 million of these in an hour" and I'm like "oh, okay, you have my attention*"

Network packets for communication would be different depending upon the task the legitimate user or attacker is attempting. While a business might transmit millions of API calls, the type of call such as initial credential verification should not be happening at anywhere near the same rate or to the near total exclusion of other API calls. A finer level of granularity would be able to detect this phenomena.

Tools meant for other purposes can also give indications of malicious activity. In one instance, an interviewee spoke of how bad

actors were stealthily piggybacking off their service to build a competing business with all costs incurred by the organization itself. It was the organization's tracking of payment declines normally used in determining if the service is unexpectedly down or disconnected that allowed them to discover the events and take action. E-commerce and similar organizations have a stronger correlation of their operations to their websites and associated stack. An expansion of the data monitoring in pathways consistent with the operation of online activities can lead analysts to locate otherwise stealthy attacks.

5.4 Burnout is an ever present problem, especially in smaller organizations

For US-based participants with smaller cybersecurity teams, analysis may be one of the many tasks managed by a single employee which can cause an accumulation of stress. A third of those interviewed had either recently quit and moved to a different organization in the past month or had handed in their notice to quit. As one interviewee put it:

> "*I feel from a security point of view because we manage so many domains that everything from policy to incident response to technical decisions, design, architecture... you find yourself wearing too many hats, spread thin, you read these articles about CISOs being stressed out or quitting after a year... this is the reason why, you get pulled in every direction...*"

The larger organizations that we interviewed had dedicated red teams to find security vulnerabilities and report them before an attacker could make use of them. The earlier quote in Section 5.3 about the 72 million credentials in an hour is an example of a red team finding a flaw that led to a new monitoring policy being setup before the vulnerability was exploited.

This creates a difference in the needs depending upon the capabilities of an organization. Interview participants reported that within organizations with a limited cybersecurity presence, analysts were left to write their own queries instead of using other software.

Smaller organizations may also turn to outside organizations to aid in their cybersecurity needs. Two of our interviewees worked for cybersecurity-focused companies that were hired by organizations that lacked the capacity for an in-house cybersecurity team. While this can alleviate the lack of human resources, outsider aid can expand the attack surface with a greater risk of insider threats or compromised communications.

5.5 The complexity of credential confirmation is increasing

The complexity of the task of credential confirmation is increasing. The COVID-19 pandemic added a complicating factor. Location became a less valuable feature than before as an employee or customer might be connecting from a different location due to lockdown.

> "*there was a pandemic, are you going to restrict people from where they can connect from, you can't... we were seeing that in our [redacted] logs, our connection logs, we were seeing out of state, or rather out of country connections and it became more of a norm.*"

This credential confirmation issue is not only specific to the pandemic as shifts in organizational processes will change the data present for analysis. Examples would include a department being moved overseas, positions being shifted from in-house to contract, or job functions being consolidated to a subset of employees.

5.6 Insider Threats

Responses on the importance of insider threat detection were varied. Some interviewees were unconcerned about the potential of an insider threat while others had rigorous controls and policies in place. One of the latter felt that tools designed to detect insider threats could also locate unauthorized accidental activities partaken by employees as expressed below:

> "*The defenses against insider threats in a large production environment are the same as the defenses you have against people making mistakes and solving reliability issues.*"

Another interview participant expanded upon common mistakes that can lead to data loss:

> "*Somebody's got a webpage, and they thought that the access to it closed off... and they mis-configured it and it turns out it's open to the world. Somebody sends a spreadsheet with SSNs and credit numbers and I mistype your name, and it goes to a completely random email address.*"

An IDS that handles insider threats through anomaly detection should be capable of detecting these situations as they are outliers. It should generate an alert either upon the initial loss of privacy or upon the use of incorrect email when the unintended recipient decides to exfiltrate the data to an unauthorized location.

As a prime example of an insider threat, an interviewee came across employees being bribed by an outside source to report on user data. They expressed an interest in the tool's ability not only to identify the direct instances of insider threats but also any links with the particular outside source during forensic analysis.

5.7 Advanced Persistent Threats

Those that we interviewed did not view APTs as a high priority in their day-to-day operations. However, several expressed finding traces of APT attacks after the fact. One interviewee stated that apathy due to overwork could result in a negative impact of detecting APT attacks:

> "*Data was leaving the finance team and going to [redacted] and it was APT related. And that, was never detected... they're taking small chunks at a time... you could ignore it easily and say eh that's nothing, but it is something, it's big. You've already been hit with an infection that's allowed for that command and control communication, it's a very dangerous thing.*"

When APT attacks were specifically discussed with the interview participants, the lack of time and resources were the common reasons given for less focus devoted to those attacks. In light of the overwork expressed by participants and considering **RQ2**, a system

design that requires minimal intervention from the user would be preferred for less common threat types. This would not only be expressed by a lower false positive rate as discussed in Section 4.3, but also how understandable the output is to quickly analyze the alert.

5.8 Phishing attacks

Phishing was reported as the most common threat encountered and had the second highest level of concern as shown in Figure 2 and Figure 3 respectively. Half of the interview participants expressed encountering an abundance of phishing attacks, as one put it:

> "*...phishing still tends to be the number one vector... every now and then somebody at [redacted] falls for a scam like that... that's probably our biggest pain point...*"

Interviewees expressed that their main source for phishing attack mitigation was awareness training. This was an admittedly flawed approach as pointed out by one interviewee:

> "*You could provide as much training as you want to... but there is always that risk that someone is going to click on that link or that attachment.*"

5.9 Intra-department Communication

Participants raised the point that successfully dealing with a threat does not stop at detection. It often requires action from other departments that may be slow to act out of ignorance. This inaction can be exacerbated if the outstanding focus and culture of the company downplays a threat.

> "*I'm still challenged with this to some degree. I have to update technical people, I have to update business people, then I have to update the board and sometimes finding that balance between layman terms and technical terms it can be challenging, especially if you have a technical background. It comes as part of the job.*"

> "*The hard point for the company I was with was that it was early in [redacted] days, infosec was very much more concerned with discontinuity and internal IT rather than operating the system as a whole and there being an external actor.*"

Being able to display the forensic analysis of an attack can aid in the swift resolution of the threat. Provenance graphs have been used in analysis of attacks such as APTs [3], IDS [14], and others. While these solutions prune the trees to be human-readable, their output is meant for cybersecurity-literate individuals. Providing additional output that can display the threat to the layman would display the depth and breadth of the threat. This knowledge could aid in mobilizing other departments to cooperate quickly.

5.10 Data privacy concerns when transferring log data for IDS analysis

Having a 24/7 human component to IDS may require teams in multiple locations or outside consultants. This can involve the transfer of large amounts of data as one participant mentioned:

> "*...standing up a 24/7 security operation center, we've contracted with [redacted] to provide that after hours type of approach. So, we're just going over the details of shipping them [the logs]... we collect a lot of logs a day, a couple hundred gig a day, and so shipping the more critical ones to them...*"

This process creates a potential vulnerability if the data is intercepted either in transit or at the new location. Information about the network or the individual host systems could be gleaned from the data and provide attackers with valuable data that could be used to mount attacks on the system. One method of hiding sensitive data would be differential privacy. Running anomaly detection on this modified data has been shown to yield a 10% loss of the overall "utility" of the data [11]. Further work examining the effect this would have on anomaly-based IDS performance would be warranted.

6 SUMMARY OF RESULTS AND LIMITATIONS

We summarize our major findings below:

- In reference to **RQ4**, phishing and credential theft saw the highest levels of concern (Figure 3) and frequency (Figure 2) observed. Insider threats were reported as more frequent for those in the E-commerce and medical sectors. Insider threats were also the highest reported concern for participants in the E-commerce sector and the second highest for those in organizations with 100 or less employees. The medical sector saw IoT corruption commonly or more often 50% of the time. Despite that frequency, it was reported as only a medium priority for half of the respondents.
- Models tailored specifically to detect APT and insider threats were not employed by those we interviewed. However, several of the interviewees mentioned uncovering both of the aforementioned attacks at least once over their career. The survey results also had 84% and 80% encountering APTs and insider threats at least once, as seen in Figure 2. Interest was expressed in models that could handle overlapping issues. One example given was software that could detect insider threats could also catch human error and reliability issues for human directed processes.
- The frequency that manual detection was required half the time or more was 34%, as shown in Figures 5. In reference to **RQ2**, this appears to be an area where improvement of the models used would be of major benefit to cybersecurity practitioners.
- The delay between the attack and an alert is also an area of potential improvement. A portion (24%) of participants reported requiring a day or longer to detect a threat. This delay increases the time attackers have to exfiltrate the data or otherwise harm the organization.
- In reference to **RQ3**, related tasks that have a similar conceptual model can be streamlined to reduce the practitioner's workload. For example, threat detection and forensic analysis can both be modeled using a provenance graph and a truncated version displayed to the user. A solution that allows the user to perform related actions can create a more seamless experience. This in turn can reduce the amount of manual work performed searching for related threats and increase efficiency.
- The relative importance of recall and FPR may shift depending upon the state of an attack. In day-to-day activities, a

minimal FPR may be more important than a recall approaching 1. After a successful malicious threat has been identified, the priority of recall would rise. The type of employee and their placement within the organization and their location may affect the weight of certain features. Giving the cybersecurity practitioner limited control over these factors would aid in handling malicious threats.
- Cybersecurity design should consider the requirements of all participating organizations. A provider may offer hosting services to a client organization or the two organizations may operate at parity. This system should not create conflicts or loopholes that could be exploited by a malicious actor.

The potential pool of interview participants was restricted due to the English-only language usage. This limited the available interviewees and could obfuscate issues in other regions or cultures. Respondents would go into limited detail on some sensitive subjects and were not pressed due to ethical concerns. This created a loss of granularity when discussing some specific instances.

Our survey was kept brief to avoid interest waning or refusal to participate due to the time taken. Our initial survey contained 38 questions that would take around 30 minutes to complete. These questions delved into how well an IDS performed in detecting specific types of threats like APT, Insider Threats, etc. It also examined the usability of the tools and systems in place and their related workflows. This seemed too long as we only received 4 responses. We decided to shorten our survey and expand the interview to collect qualitative data on a subset of those questions. Finally, the answers of participants can only be based on their perception.

7 CONCLUSION

We examined the challenges cybersecurity practitioners face during their day-to-day activities through employing a survey and semi-directed interview for gathering qualitative and quantitative results. Phishing and credential theft were reported to be the most common and worrisome attacks experienced. Certain business sectors broke from this trend, such as participants in E-commerce reporting more insider threats and placing them as a high priority at the highest rate. Frequency and concern was not always proportional, such as practitioners in the Medical field reporting a high frequency of IoT corruption, but placing it at a lower priority than other threats.

Interviewees conveyed several major concerns. US based employees spoke strongly of being stretched thin, where any time saved is valuable. The IDS they employed only answered part of their questions. An alert for an attack doesn't always relay the breadth of the attack itself, leaving the practitioner to manually search for that information. The knowledge they gain from their investigation ideally should feed back into the IDS, generating additional alerts from the remaining false negatives. Interviewees discussed the increasing complexity of the organizational landscape as well. More businesses are integrating their digital processes, employees are not working in a controlled environment as often with the rise of telecommuting, and the company culture is lagging behind the technological progress in effectively managing risk.

Our study addressed the importance of understanding the challenges cybersecurity practitioners face in the field. Developing techniques to overcome the current pain points can increase the applicability of new research directions going forward.

ACKNOWLEDGMENT

This work has been supported by the Virginia Commonwealth Cyber Initiative (CCI) and the Office of Naval Research under Grant N00014-22-1-2057.

REFERENCES

[1] Bibek Bhattarai and Howie Huang. 2022. SteinerLog: prize collecting the audit logs for threat hunting on enterprise network. In *Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security*. 97–108.
[2] Peng Gao, Xusheng Xiao, Zhichun Li, Fengyuan Xu, Sanjeev R Kulkarni, and Prateek Mittal. 2018. {AIQL}: Enabling efficient attack investigation from system monitoring data. In *2018 {USENIX} Annual Technical Conference ({USENIX}{ATC} 18)*. 113–126.
[3] Xueyuan Han, Thomas Pasquier, Adam Bates, James Mickens, and Margo Seltzer. 2020. Unicorn: Runtime provenance-based detector for advanced persistent threats. *arXiv preprint arXiv:2001.01525* (2020).
[4] William Hatcher, Wesley L Meares, and John Heslen. 2020. The cybersecurity of municipalities in the United States: An exploratory survey of policies and practices. *Journal of Cyber Policy* 5, 2 (2020), 302–325.
[5] Mohammad S Jalali and Jessica P Kaiser. 2018. Cybersecurity in hospitals: a systematic, organizational perspective. *Journal of medical Internet research* 20, 5 (2018), e10059.
[6] Ansam Khraisat, Iqbal Gondal, Peter Vamplew, and Joarder Kamruzzaman. 2019. Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity* 2, 1 (2019), 1–22.
[7] Aechan Kim, Mohyun Park, and Dong Hoon Lee. 2020. AI-IDS: Application of deep learning to real-time Web intrusion detection. *IEEE Access* 8 (2020), 70245–70261.
[8] Michelle Lowry, Anthony Vance, and Marshall D Vance. 2021. Inexpert supervision: Field evidence on boards' oversight of cybersecurity. *Available at SSRN 4002794* (2021).
[9] Minh-Phuong Nguyen, Thi-Thu-Trang Nguyen, Vu Tran, Ha-Thanh Nguyen, Le-Minh Nguyen, and Ken Satoh. 2022. Learning to Map the GDPR to Logic Representation on DAPRECO-KB. In *Intelligent Information and Database Systems: 14th Asian Conference, ACIIDS 2022, Ho Chi Minh City, Vietnam, November 28–30, 2022, Proceedings, Part I*. Springer, 442–454.
[10] Borke Obada-Obieh, Yue Huang, and Konstantin Beznosov. 2021. Challenges and Threats of Mass Telecommuting: A Qualitative Study of Workers. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. 675–694.
[11] Norrathep Rattanavipanon, Donlapark Ponnoprat, Hideya Ochiai, Kuljaree Tantayakul, Touchai Angchuan, and Sinchai Kamolphiwong. 2021. Releasing ARP data with differential privacy guarantees for LAN anomaly detection. In *2021 18th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON)*. IEEE, 404–408.
[12] Rohani Rohan, Suree Funilkul, Debajyoti Pal, and Himanshu Thapliyal. 2021. Humans in the loop: Cybersecurity aspects in the consumer IoT context. *IEEE Consumer Electronics Magazine* 11, 4 (2021), 78–84.
[13] Mathew Vermeer, Natalia Kadenko, Michel van Eeten, Carlos Gañán, and Simon Parkin. 2023. Alert Alchemy: SOC Workflows and Decisions in the Management of NIDS Rules. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*. 2770–2784.
[14] Yulai Xie, Dan Feng, Yuchong Hu, Yan Li, Staunton Sample, and Darrell Long. 2020. Pagoda: A Hybrid Approach to Enable Efficient Real-Time Provenance Based Intrusion Detection in Big Data Environments. *IEEE Transactions on Dependable and Secure Computing* 17, 6 (2020), 1283–1296. https://doi.org/10.1109/TDSC.2018.2867595
[15] Zhiqiang Xu, Pengcheng Fang, Changlin Liu, Xusheng Xiao, Yu Wen, and Dan Meng. 2022. Depcomm: Graph summarization on system audit logs for attack investigation. In *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, 540–557.
[16] Fabio Massimo Zanzotto. 2019. Human-in-the-loop artificial intelligence. *Journal of Artificial Intelligence Research* 64 (2019), 243–252.