Work-From-Home and COVID-19: Trajectories of Endpoint Security Management in a Security Operations Center

Kailani R. Jones[1], Dalton A. Brucker-Hahn[1], Bradley Fidler[2§], and Alexandru G. Bardas[1]
[1] *University of Kansas (I2S - HASSC),* [2] *Independent Researcher*
kailanij@ku.edu, daltonhahn@ku.edu, brfid@icloud.com, alexbardas@ku.edu

Abstract

The COVID-19 surge of "Work From Home" (WFH) Internet use incentivized many organizations to strengthen their endpoint security monitoring capabilities. This trend has significant implications for how Security Operations Centers (SOCs) manage these end devices on their enterprise networks: in their organizational roles, regulatory environment, and required skills. By intersecting historical analysis (starting in the 1970s) and ethnography (analyzed 352 field notes across 1,000+ hours in a SOC over 34 months) whilst complementing with quantitative interviews (covering 7 other SOCs), we uncover causal forces that have pushed network management toward endpoints. We further highlight the negative impacts on end user privacy and analyst burnout. As such, we assert that SOCs should consider preparing for a continual, long-term shift from managing the network perimeter and the associated devices to commanding the actual user endpoints while facing potential privacy challenges and more burnout.

1 Introduction

COVID-19 has caused shifts in patterns of Internet use, with some tied to the surge in "work from home" (WFH) users [11]. Survey data suggests that at least 41.8% of Americans participated in WFH [47], and it is apparent that WFH will become an integral part of larger organizations in the future [53]. Security Operations Centers [109, 113], shorthanded SOCs, tend to play a central role in enabling this endeavour. SOCs are deployed by organizations in industry, government, and academia to manage their networks, defend against cyber threats, and maintain regulatory compliance [109, 113].

Our study analyzes through ethnographic and historical methods the causal forces that incentivize and intensify endpoint security monitoring by SOCs, particularly in the context of a prolonged and en masse COVID-19 WFH phenomenon. We see endpoint security management as the *monitoring and defense of client devices that possess authorized access to enterprise networks and resources*. These endpoints are Internet-connected devices of any kind, supplied by the organization or the individual, and are frequently used for a mix of professional and personal activities [1, 86].

While the practice of endpoint security management is not completely new, and the proliferation of heterogeneous devices has been ongoing, we anticipate that SOCs will increasingly be expected to perform these same functions with a far more differentiated (by device characteristic) and distributed (by location) network perimeter. SOCs now bear the burden of managing a network whose boundaries are regional, national, or even global based upon user locality [101]. As we later elaborate, our study can serve as a warning to how SOCs will, or have already been tasked with controlling/commanding endpoints. Yet these responsibilities may require additional organizational, technical, or training support. Understanding these new responsibilities as they relate to long-term endpoint monitoring trends, will be an important consideration for future SOCs, their staff, and their organizations.

Modern endpoint security management replaces old systems with new technologies *and* new social policies, giving SOC staff highly granular control over both individual end-devices (e.g., patch levels, firewall rules, installed applications) and end-users (e.g., login frequency, location, file downloads) [73, 114]. This control, in turn, contributes to the brittle state of endpoint security management. This brittleness can be attributed to an increase in vulnerability to unforeseen interaction effects than previous sociotechnical systems of security management [106–108]. Together, they increase the degree to which SOC staff regulate professional *and* personal Internet use (media consumption and sociality more generally).

We employ a multi-year ethnographic analysis of a U.S. SOC before and during COVID-19. Based on our *initial* ethnographic observations of events, we engage in a historical study to trace endpoint security management backward in time — is COVID-19's push towards WFH potentially another catalyst of SOCs assuming endpoint security management? The historical analysis evidence reveals how COVID-19 WFH is the latest manifestation of a broader, half-century trajectory in which manual security and monitoring tasks are increasingly

[§] Part of this work was performed while at Stevens Institute of Technology supplemented and replaced by more technological solutions. To be sure, labor-saving automation is a core or even defining activity of (broadly) computer science; however, our study does more than point out instances of labor-saving automation. Instead, we trace contemporary security practice backward in time, extending their historical trend lines by identifying the antecedent labor-intensive practices that they replaced. In turn, we analyze our ethnographic observations based upon the outcomes of our historical study.

The move toward more powerful endpoint security monitoring and data handling is not obvious. By intersecting history (starting in the 1970s) with ethnography (analyzed 352 field notes and performed two rounds of semi-structured interviews across 1,000+ hours in a SOC over 34 months) and complementing both with a quantitative analysis (covering 7 other SOCs), we show a shift in importance for endpoint security monitoring. Our ethnographic work reveals how WFH-incentivized endpoint monitoring is an outcome of characteristics (detailed below) that are shared by many SOCs. Specifically, our SOC's shared internal organizational and technical architecture, as well as the Internet environment in which it operates. Our study received IRB approval from our institutions and we also employed additional measures to protect our participants as detailed in Section 3.4.

Through our analysis, we argue that COVID-19's WFH shift will prove to be central to the evolution of SOCs, as well as, to the Internet at large. Further, it will raise a host of institutional and procedural questions to the community not only upon how the SOCs must address the increasing user autonomy, but do so under increased pressure in an already vulnerable environment contending with burnout-related challenges [63]. This will require corollary shifts in SOC objectives and in how SOC staff are evaluated. Empirically and analytically, our main contributions are as follows:

- A novel historical analysis covering the SOC's relationship with endpoint security management resulting in the current trajectories for SOC endpoint security management;
- An ethnographic study of a U.S. SOC's adaptation to the abrupt changes brought on by COVID-19 complemented by a permanent change to the enterprise network perimeter;
- Identification of an increasing tension between SOC security practices, SOC employees, and end-user autonomy potentially leading to increased burnout in an already vulnerable environment;
- An extensive validation effort that includes quantitative interviews conducted with seven other SOCs (from the government sector, industry, and academia).

2 Background and Related Work

Endpoint security management can be viewed as the process to monitor and defend client (a.k.a endpoint) devices that possess authorized access to enterprise networks and resources. Such client devices can be, but are not limited to, laptops, smartphones, tablets, Internet-Of-Things devices, and even small-scale managed networking devices such as switches. These endpoints are Internet-connected devices of any kind, supplied by the organization or the individual, and are frequently used for a mix of professional and personal activities [1, 86]. Typical functions within endpoint security management include endpoint inventory, adjusting system configurations, restricting access through content filtering, and more [18]. To protect not only these endpoints but also the organization's resources, Security Operation Centers tend to oversee endpoint security management [31].

Security Operations Centers (SOCs) are central components of modern enterprise networks. Organizations in industry, government, and academia deploy SOCs to manage their networks, defend against cyber threats, and maintain regulatory compliance [109, 113]. SOCs are organized in various ways ranging from a flat structure to hierarchical tiers of analysts, specialists, and managers [106, 107]. The structure and scope of the performed activities are mostly determined by the organization's size, services offered to its users, or its domain of activity. Albeit, all SOCs still perform certain core functions: incident management, monitoring and detecting threats, security administration, architecture and engineering, and long-term planning [7, 31, 106, 118]. Just as each enterprise network includes unique aspects in its configuration and layout, so too are SOC tasks [106] and the maturity-level of a SOC [117]. Even the names that fall under the broad SOC umbrella may be different across organizations e.g., Computer Security Incident Response Team (CSIRT) [29, 107], Network Operations Center (NOC) [106], Network and Security Operations Center (NSOC) [108], Cybersecurity Operations Center (CSOC) [48], Security and Compliance Center [106], Managed Security Service Provider (MSSP) [10], etc.

Prior bodies of work studied SOCs by conducting surveys [31, 101, 103, 118], interviewing analysts [7, 9, 69] or performing participant observation [106–109]. These works uncovered various technical problems SOCs face such as prioritizing high numbers of opaque alerts, lack of logging, and assigning levels of severity to alerts [9, 31, 103]. Furthermore, other works identified sociotechnical issues such as analyst burnout [106], breakdowns between analysts and managers [69], and the contradictions between tools, analysts, and processes [108]. Our work contributes to this body of research by presenting a historical analysis on the trajectory of endpoint management, while also highlighting additional layers of sociotechnical complexity within a SOC.

More recently, a few surveys measured COVID-19 and WFH impacts on SOCs. SIEMplify conducted a survey focused primarily on COVID-19's impact [101]. This survey covered 393 SOC employees and asked about the effects upon the security posture (26% of respondents reported a worse security posture), the number of alerts (42% reported increased alerts), and the incoming phishing emails (57% reported a rise). Additionally, they find that investigating suspicious activities, collaborating, and communicating has become more challenging in this environment. Another survey, covering 150 security and technology leaders, focused upon COVID-19's WFH phenomena [16]. The majority of the respondents believe that their current infrastructure supports WFH, and that their security posture can handle the risks. Some respondents reported a high volume of attacks and adopted new services in lieu of COVID-19 [16]. Lastly, a survey conducted by Cybersecurity Insiders across 287 cybersecurity professionals, found the majority of respondents still work from home. Many are worried about securing network access, personal devices, and installed applications which pose data leakage risks, while some respondents are concerned with (1) users' exposure to malware and phishing and (2) unmanaged endpoints [21, 22].

It is apparent that SOCs are complex structures with varying names, operations, and challenges. It is also plausible that technically analyzing a plethora of SOCs may not completely capture COVID-19's impact. In our work, we proceed with a multi-layered approach. We leverage historical analysis methods to uncover long-term trends and study a SOC with anthropological approaches to help support our historical findings. We further generalize our findings by conducting surveys with seven other SOCs representing various sectors (academic, government, and industry).

3 Methodology, Data, and Participants

This study leverages historical and ethnographic methodologies to investigate a SOC's role in endpoint management within the context of WFH. Studying individual SOCs is the main route to detailed information about their operations and staff, but if used as the sole analysis, it does not permit us to extrapolate larger trends. To provide an explanation of the changes we now see underway, we require methods that can both (1) elucidate the causal mechanisms behind SOC operations (i.e., a bottom-up analysis), and (2) explain how those operations fit into the larger domain of SOCs and their trajectory (i.e., a top-down analysis). Moreover, to confirm that our observations in the context of COVID-19 are not specific to only one SOC, we quantitatively interviewed seven other SOCs. Figure 1 illustrates the high-level procedures and methods taken to conduct this study.

3.1 Historical Analysis

Our historical analysis aims to understand, within larger-scale change, the trajectory of endpoint control in present-day SOCs during the WFH phenomenon triggered by COVID-19. To the best of our knowledge, we are the first paper to perform a historical analysis of endpoint security control through SOCs.

Our historical approach, a qualitative research method, can be understood as *applied* [55], in that it is designed to *understand specific phenomena*. Although we elaborate upon this method below, we outline the approach in Algorithm 1.

```
Input: Evidence Repositories with keyword list
Result: Endpoint management trajectories
initialization;
Add "endpoint management" to the keyword list;
while keywords have not been searched do
    extract a keyword from the list;
    search the evidence sources with the keyword;
    if document context matches the keyword, is the
      first instance within our repository sources, and is
      relevant to SOCs and endpoint management, then
        extract relevant events and record the included
          fundamentally new technologies by usage;
        extract contextual keywords from the events;
        filter contextual keywords by leveraging
          NGRAMs to understand their
          pertinence/long-term scalability;
        if contextual keywords are pertinent and we
          have not encountered its root-cause within
          endpoint management then
            add the contextual keywords;
        end
    end
    remove the keyword from the list;
end
compile the list of technologies, group them into
  periods by usage and root-cause;
```

Algorithm 1: Overview of the historical analysis methodology. We start searching for keywords with the evidence sources listed in Section 3.1. As we locate pertinent documents, we extract common contextual keywords and repeat the searches until no keywords remain. We finish by identifying periods of endpoint security management based upon technological usage.

Evidence Sources: Our evidence draws on primary sources: documentary and born-digital data, with clear provenance linking it to the event in question, and subject to minimal editing or commentary. Inasmuch as possible, we avoid less reliable sources of evidence, such as firsthand accounts and other forms of after-the-fact recollections. Our searched repositories include Request For Comments (RFC) documents [27], ACM and IEEE digital libraries [5, 59], Defense Technical Information Center (specifically the defense agency newsletters) [36], UCLA University Archives Special Collections [116], reference manuals that focus on the historical usage of tools [38], history-focused and formally published books (e.g., [2, 20, 24]), Charles Babbage Institute collection [84], National Archives [81], and, more broadly, other professional societies' publication archives (often mediated by Google Scholar). These sources are typically located in either contemporary publication databases (e.g., the ACM Digital Library), or historical repositories (e.g., the Computer

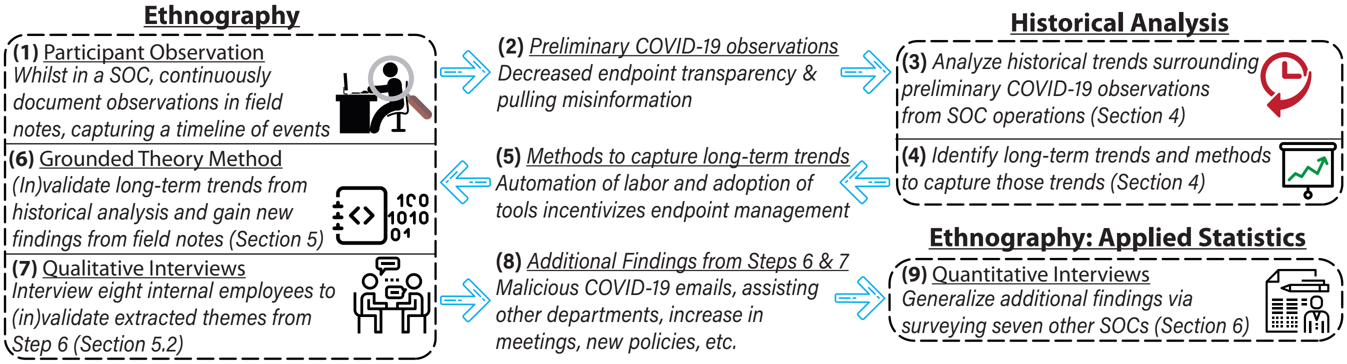
Ethnography
(1) Participant Observation
Whilst in a SOC, continuously document observations in field notes, capturing a timeline of events
(6) Grounded Theory Method
(In)validate long-term trends from historical analysis and gain new findings from field notes (Section 5)
1C0
1010
01
(7) Qualitative Interviews
Interview eight internal employees to (in)validate extracted themes from Step 6 (Section 5.2)
(2) Preliminary COVID-19 observations
Decreased endpoint transparency & pulling misinformation
(5) Methods to capture long-term trends
Automation of labor and adoption of tools incentivizes endpoint management
(8) Additional Findings from Steps 6 & 7
Malicious COVID-19 emails, assisting other departments, increase in meetings, new policies, etc.
Historical Analysis
(3) Analyze historical trends surrounding preliminary COVID-19 observations from SOC operations (Section 4)
(4) Identify long-term trends and methods to capture those trends (Section 4)
Ethnography: Applied Statistics
(9) Quantitative Interviews
Generalize additional findings via surveying seven other SOCs (Section 6)

Figure 1: Synthesis of Ethnography and Historical Analysis – Historical analysis is used to identify long-term trends and methods to capture those trends in the current day. Our ethnography provides the high-level issues but also acts as a validating resource towards the trends identified through historical analysis. To confirm and generalize our findings, qualitative interviews with the SOC employees were conducted whilst pairing a quantitative interview (survey) with seven other SOCs.

History Museum [30]), which provide certainty as to a piece of evidence's providence. As shown in Algorithm 1, we begin the historical analysis with these listed sources.

Keywords and Filtering: This line of historical inquiry includes better-known phenomena and events, such as, the emergence of the Security Operations Center. We focus on historical trends in the monitoring and management of networked, local host machines, or endpoints by first searching for the phrase "endpoint management" and working backwards in time from the first account of "endpoint management" to the first known instance of securing endpoints. Next, we explain these trends by revealing their origins in (1) broad functional requirements that arise from a combination of the network and host architectures, and (2) the scale, kinds, and geographic distribution of use. In other words, we look for fundamental changes to endpoints that would negatively impact endpoint security management during that era. After analyzing the resulting documents, we continue to extract common phrases used under the context contained within multiple selected texts (e.g., "NOC", "SOC", "content handling", "acceptable use policies"). As our terminology expanded, our inquiry led us to phenomena that, while uncontroversial, fall outside of the usual scope of Internet history. Such phenomena include the basic security practices of 1970s and 1980s campus and office computer labs, such as "keycard locks" and "antivirus software". We select accounts which were professionally refereed, and which appear (retrospectively against the historical record) to reflect standard or increasingly standard practices. The list of keywords and the corresponding resources is available in Appendix A.1 – Table 5.

As we broaden our scope more towards present-day whilst adding peripheral context, the amount of relevant work drastically accumulates. For these cases, we also pair Google NGRAM [49] with Google Scholar samplings to understand long withstanding terminology frequencies paired and how they were used in publications during those periods. Through this, we are able to observe major changes in the technologies, techniques, and terminology specific to endpoint security management. This technique enables us to uncover historical activities that would not appear when, for example, searching for "cybersecurity" in 1980s publications.

Generating Periodizations: Occurring after we finish filtering texts, collecting key words, and utilizing Google NGRAM, our historical analysis enables us to identify and describe six main periods of endpoint management. We do not suggest that the basic characteristics of these periods were uniform, but instead, that these characteristics describe general trends throughout history. Our date ranges are approximate, and denote a "season" of endpoint management. We limit our focus to unclassified Arpanet/Internet-connected endpoints on enterprise networks: this excludes non-Arpanet/Internet endpoints and private access through Internet Service Providers (for reasons explained below). Our history presents a subset of the Internet's far larger historical evolution. Our goal is to explain the adaptation of the historical lineage with causal links to present-day endpoint technologies, rather than a complete global history of networking and paths not taken. We note here that the identified trends are not always as visible from individual experience, and thus, there are many current-day solutions that we do not mention as their origin fall inside our defined periods but outside of the evolution of SOC endpoint security management. *We date technologies to the period of their widespread use, and not to their invention.*

3.2 Ethnography and Fieldwork

A major limitation of finding patterns in history is correlation in time, but only in time. In short, we have no empirical account of the actual dynamics: the changes in SOC techniques and technologies that one would expect to see in response to one of the theorized external forces. To help solidify our initial SOC observations (indicators of endpoint management) and findings from our historical analysis, we leveraged three ethnographic research methods: (1) participant observation field notes combined with Grounded Theory Method, (2) semi-structured interviews, and (3) surveys.

Participant Observation: Field notes were collected through participant observation [64, 106, 107] by embedding an observer into a SOC. These insights allow us to better understand the pressures and challenges faced by a real-world SOC.

For 34 months (June 10, 2019 to May 16, 2022), one fieldworker was embedded within our observed SOC to collect field notes. A graduate student with a background in computer science worked alongside SOC analysts to help improve operations whilst recording observations and gaining an in-depth understanding about the environment. Embedded 7.80 ± 2.06 hours a week for a total of 1,000+ hours, our fieldworker recorded their observations based on over 500 employee discussions. Aside from meetings, the fieldworker also analyzed the ticketing systems, tools and solution deployments, and documentation. Although some of the communication occurred through e-mail and Microsoft Teams [78] prior to WFH, the WFH transition increased this type of digital communication and video conference calls.

Grounded Theory Method: We used Grounded Theory Method (GTM) to analyze the 352 collected field notes (additional details of which can be found in Appendix A.2). GTM allows us to create theories using interviews and/or participant observation field notes. This approach has been leveraged in previous works to uncover user perceptions' around privacy [3] and cryptocurrency [72] as well as modelling analyst burnout [106]. Thus, GTM allows us to uncover and extract meaningful themes of SOCs in the context of COVID-19. Prior to COVID-19, we focused on analyzing cybersecurity metrics. Our focus of SOCs, with respect to COVID-19, redirects our analysis to attempt to answer the following open-ended questions: (1) what happens to a real-world security environment during a crisis and (2) how do tools, services, and analysts "react" to the unexpected circumstances?

With our defined research questions, we iteratively analyzed field notes by following GTM's three steps: open coding, axial coding, and selective coding [104]. The first iteration, open coding, involves parsing the field notes to identify insights and uncover potential phenomena by labelling observations known as codes throughout the documents. After identifying our codes, we performed axial coding which consists of combining the previous codes from open coding into larger themes. Based on these larger themes, we leveraged selective coding to understand the reasoning behind each of these categories. Specifically, why these themes are the main concerns. The codebook is included in Appendix (Table 7).

Semi-structured Interviews: To validate, or invalidate, themes extracted by GTM, we conducted two rounds of live 30-minute, semi-structured interviews with eight internal SOC employees for a total of 12 interviews (as seen in Table 1). Between interview rounds, one employee transitioned to another department and three employees reduced their workload to participate in the second round of interviews. Questions were forwarded to each employee a few days prior to the interview, so participants would feel more comfortable. When sending the questions and upon beginning the interview, participants were notified that (1) these are semi-structured interviews, thus we may ask other questions about the topic at-hand, and (2) they could opt out or add to questions as desired.

Whilst our fieldworker was embedded, they personally noted an impact on work, productivity, and communication. Based on these observations, questions were tailored to elucidate these phenomena. A focus upon analysts' perceptions of the changed environment was taken for the first round of interviews. Thus we asked about their respective roles and how they felt if those roles had or had not altered. During the second round, we wanted to uncover analysts' perceptions surrounding our derived themes and to better understand the context surrounding more *technically* based themes. The fieldworker analyzed the interview notes via coding until thematic saturation was reached [57]. More information on the interview process is located in Appendix A.3.

Surveys: We leverage historical analysis to understand long-term trends in SOCs, but a generalization of the findings from our ethnography is necessary. From July 26 to Aug 5, 2021, we conducted quantitative interviews with seven SOCs. In this research, a survey is a type of quantitative interview [60]

These quantitative surveys consisted of close-ended questions allowing us to (1) follow our previous findings and (2) reduce the amount of required effort from the respondents. Whilst crafting this survey, we followed the Brief, Relevant, Unambiguous, Specific and Objective method (BRUSO) [60] to decrease required respondent effort. For close-ended questions, we provided many answers, but we also included an additional category in the case a respondent did not feel like the provided answers were sufficient. We standardize the answers provided in the demographics section by following previous work [31]. Lastly, to prevent "item-order" effect (i.e., ordering of questions alter responses), we alter the ordering of available selections on multiple choice questions.

Because we cannot determine the population sampling size, we chose a non-probability sample method: convenience sampling [60]. Since we choose participants in close proximity willing to partake in this research, we may introduce a slight sampling bias; however, we pose that we are not attempting to uncover new trends from this survey, rather, we aim to validate our findings from the ethnography. We conducted the survey and relied upon descriptive statistics for analysis. Our survey questions are located in Appendix A.3.

3.3 Participants

With ethnographic methods, we analyzed one SOC through participant observation and semi-structured interviews while pairing the experience of seven other SOCs via quantitative interviews (a.k.a., surveys). These perspectives help us identify how our findings extend across SOC domains.

ID	Job Title	Round 1	Round 2
P1	IT Security Specialist	Yes	No*
P2	IT Security Specialist	Yes	Yes
P3	IT Compliance Manager	Yes	Yes
P4	Chief Information Security Officer	Yes	Yes
P5	IT Security Specialist	Yes	Yes
P6	IT Coordinator	No*	Yes
P7	IT Analyst	No*	Yes
P8	IT Analyst	No*	Yes

Table 1: Demographics of the internal participants (semi-structured interviews). * Due to work demands, some participants could not participate in both interview rounds.

Participation Observation Demographics: The SOC under study (via participant observation and *semi-structured* interviews) oversees all major security operations for the entire organization with more than 30,000 users (both customers and employees). In a hierarchical structure, the SOC includes three layer 2 (L2) analysts who oversee incident management, alert remediation, and security engineering. The two L3 and L4 managers' responsibilities focus more on planning future infrastructure to increase the organization's security posture; however, they also assist with L2 activities as needed. L1 analysts are located in general IT help desk, and they are not directly included in our study. L1 analysts have limited formal security training, and their cybersecurity functions include well-documented processes: password resets, unlocking disabled accounts, and assigning encryption certificates. Although the SOC manages the majority of security-related events, it is fairly small (see Table 1) with a low-medium maturity rate per SOC-CMM [117].

Survey Demographics: Since our findings cover the impacts on SOCs rather than individual employees, we reached out to Chief Information Security Officers and similar positions to answer on the behalf of their respective SOC. Seven final participants and their demographics are located in Table 2. Overall, the majority of the respondents oversee security operations in the education and government sectors, and users tend to be more localized than our respondents from industry (one can be classified as an MSSP, and the other oversaw an already distributed workforce). We asked about performed functions such as "Security monitoring and detection"(n=7), incident response (n=6), alert and incident remediation (n=6), data protection and monitoring (n=5), SOC architecture and engineering (n=5), threat research (n=5), compliance support (n=4), digital forensics (n=3), security road map and planning (n=2), and penetration testing (n=1).

We postulate that the variety of our participants help generalize our ethnographic findings via their diversity within differing sectors, activities, policies (5 SOCs have privacy polices), user base, and payment methods (contractors versus employees). Our participants oversee multi-layered SOCs ranging from Forbes 500 companies, to academic institutions with 30,000+ users, and even SOCs protecting states.

Job Title	Tenure	Sector
Chief Information Security Officer	6	Education
Chief Information Security Officer	4	Education
Chief Information Security Officer	2	Government
Vice President Security Operations	7	Industry
Director of Information Security	9	Industry
Information Security Officer	5	Education
Director of Information Security	3	Education

Table 2: Demographics of quantitative interview participants (survey). The participants represent seven different SOCs.

3.4 Ethical Considerations

Our study was approved by our institutions' Human Subjects Departments (Institutional Review Board, IRB). To preserve anonymity, we encoded the analysts' names, and we do not apply extensive demographics to each encoded name. With a smaller SOC, pairing detailed demographic data and encodings would allow direct identification of the actual employee. Upon capturing field notes, we protected analysts by not recording their real name or any personally-identifiable information. Lastly, we stored notes and the survey results where only the participating researchers were provided access. Besides verbally informing the participants about our practices, we also provided them with our IRB-approved protocol document. For the survey, due to the generally sensitive technical nature of the discussed topics, we provided written disclaimers about questions being optional, and committed to aggregating and anonymizing results.

4 The Evolution of Endpoint Management

The findings from our historical analysis are summarized below (additional information is available in Appendix A.1). Detailed in Section 3.1, our goal is to understand the historical trajectory of endpoint control based on causal links to present-day SOCs (not a complete global history).

The Early Operational Arpanet (1972-1979): The Arpanet network layer consisted of a network of packet-switching Interface Message Processors which implemented a distributed routing algorithm and error correction [76]. Outside of a small number of secured networks for classified work [112], network security was largely based around endpoint's regulated physical spaces [37, 38]. Overall the DARPA-led ecosystem of researchers and contractors exercised multiple forms of endpoint control. Basically, each site required access control measures—physical or software-based—to ensure only authorized users and, crucially, authorized use. While there were no technical or organizational mechanisms for content handling as defined today, content was nonetheless *managed* by regulating use of the systems and the identity of the users [34, 35, 42].

The ARPA Internet (1980-1986): Between 1976-83, Arpanet transitioned to becoming the official core routing area of the new Internet [96]. The Defense Communications Agency (DCA, now DISA, which took over many operational duties from DARPA in 1975) [2] further prohibited (1) unauthorized LANs at official ARPA Internet sites, and (2) unauthorized dial-in access by a new generation of "computer freaks" equipped with their own modems and PCs [56]. The DCA further developed its requirements for organizational management of endpoints and added centralized access control to the dial-in points [44]. Meanwhile, PCs began replacing terminal rooms and computer service centers [24].

All of these changes differentiated the network edge beyond a smaller number of highly managed and physically controlled machines. To account for the fragmentation, DARPA directed the implementation of the Domain Name System resulting in a new set of regulations and organizational requirements [105]: local security policies to prohibit misuse and to ensure proper technical configuration [89, 90]. The local computing facilities connected to this network, however, remained largely the same. Excluding sites with strict information security (e.g. government classification), computer labs and centers enforced "acceptable use" through both organizational and technical means [2, 82].

The NSFNET Before Privatization (1986-1990): The National Science Foundation Network (NSFNET) backbone began connecting regional networks, which linked campus networks with the ARPA Internet [2]. The trend toward network edge fragmentation, already underway, intensified with (1) the rapid proliferation of attaching networks [15, 98], (2) private vendors offering heterogeneous networking protocols and products [83], and (3) the large-scale replacement of mainframes with PCs [24]. Network management quickly became "the most pressing issue in data communications" [26]. The endpoint control requirements for the NSFNET's networks mimicked those on the Arpanet. Visible in the Acceptable Use Policies (AUPs), it permitted authorized users and use, contained no expectation of privacy, and network operators could remove misbehaving entities from the network [2, 82].

New networking tools expanded the central monitoring of host behavior [2, 82] and helped lab administrators maintain the same level of control over endpoints as previously exercised over the mainframes. Anti-virus and disk management software (e.g., flashing/formatting hard drive and reinstalling software), became a widespread commercial product during this period, monitored system files and processes, and routinely brought end systems back to their proper configuration [33, 99]. Due to this, the beginnings of distrust to hardware began [99]. Organizations created formal information security policies to control these computers [45].

Connected, Private Enterprise Networks (1991-1999): During the mid-1990s changes in Internet technologies and use drove new changes in endpoint control. At the highest levels, the privatization of the NSFNET (and thus the civilian Internet) backbone began [85]. By 1993, bottom-up Internet growth expanded Internetwork connections dramatically outside of the control typically exercised by the U.S. Government over the 1980s Internet [28, 41]. Border Gateway Protocol (BGP) helped shield global routing from these new, institutionally distant networks [17, 28, 71, 92]. The 1993 "Eternal September" cultural phenomenon attests to longtime users' widespread perception that "netiquette" could no longer be enforced on new users through social mechanisms [68].

After a wave of automation [25, 94] and the rise of ticketing systems in the late 1980s [58, 61, 65], securing end systems in organizations was highly institutionalized. Organizations introduced physical access control and logging (e.g. CCTV) [14, 62]. LAN servers were in use to increase the resolution of control beyond re-imaging systems on reboot and cleaning out viruses and worms [14], and on the social end, organizations created centrally managed contact-points for reporting online abuse [12, 13]. AUPs proliferated in order to help regulate endpoint use [50].

Diversifying the Enterprise Network Edge (2000-2019): The 2000s and 2010s brought a new and dramatic wave of network differentiation. Laptops, which came into widespread use in the 1990s, were increasingly integrated with enterprise networks as technologies like IPsec [46, 111] and the Peer-to-Peer Tunnelling Protocol [88, 100] enabled better security for remote use. Although network encryption was introduced in 1970s, we see the phrase "endpoint encryption" termed during this time [37, 51]. Smartphones and tablets furthered this trend whilst also increasing mobility [121]. The Google NGRAM results for "Work From Home" increase gradually during the post-war US (1945 - 1970s), with significant growth in the 1980s, and spike dramatically in 1998-99 [52]. Externally, the Internet spread to include individual, institutional, and nation-state adversaries, not only with attacks on networks and end devices, but also on users (i.e., social engineering) [23].

This period is one of integration and further automation of NOC/SOCs, and the second half of this period sees their increasing ability to monitor and manage end devices. Middleware such as firewalls—and their increasing integration into other tools—responded to the growing threats outside the enterprise network [8]. Cloud computing permitted new forms of network architecture, management, and flexibility (e.g. Software Defined Networking), as well as easier handling of content intended for end devices (e.g. email, web links) [54, 70]. Heavy office desktop machines and labs full of secured personal computers gave way to ubiquitous laptops and smartphones [121]. This phenomena introduced "bring you own devices" (BYOD) along with the challenges to secure an even more distributed environment [79].

Captured later in our ethnography, on the eve of COVID-19's global spread, vendors offered—and organizations implemented—an increasingly wide range of endpoint control systems. Although we located evidence of technological distrust during the 80s, the Zero Trust Framework, formerly published in 2020, furthers this perception of distrust [95].

The Patterns of Endpoint Management to COVID-19: Based on our historical analysis, we draw the following conclusions for our ethnographic investigation. In the Arpanet-

Internet networking lineage, centrally coordinated management of endpoint systems was a typical feature of (what we now call) enterprise-scale network management. Thus, we suggest that *any present-day expansion of largely technical endpoint control mechanisms reflects one period in a longer series of changes that predate COVID-19*.

Endpoint management is carried out through a mix of organizational and technological means. These organizational means are simply the structured (or programmed) human activity necessary to operate complex technical systems (e.g., in-person lab monitoring and ticketing systems). In the historical scholarship, these organizational means are less prominent, because we suggest that they are not classified as important innovations or technological accomplishments – many of these organizational mechanisms predate even the Arpanet [91].

We interpret this history to suggest that the organizationally instituted endpoint management techniques *worked*, in part because they managed simpler systems with fewer threats. When organizational techniques became too labor-intensive or lost effectiveness due to the changing contexts, administrators turned to technological solutions, and thus to a drive to automate. Through Internet history, endpoint management underwent a process of automation, whereby manual tasks were partially replaced with combinations of digital computation and (likely fewer, and perhaps different) manual tasks.

As the endpoints moved beyond the domain of local organizational control–either in new distributed forms throughout an organization, or completely outside the organization itself–the effectiveness of organizational management techniques for endpoint systems *must have* declined dramatically. This decline, in turn, triggered technological solutions, or replacements, for these formerly manual tasks (i.e., automation). Given resource constraints in the contexts under study, we assume that investments from the enterprise network's management, who oversees operation and security, were made out of necessity. We argue that the widespread nature of the changes documented here further rules out highly localized, cultural, or irrational causes in general–and instead points to shared organizational and technological solutions to challenges posed by the changing technical and use environment.

5 Ethnographic Analysis of a SOC in the U.S.

In this section, we discuss our discoveries from studying a hierarchical-structured U.S. SOC securing over 30,000 users. A major limitation of finding patterns in history is correlation in time, but only in time. Through ethnographic approaches, our main goal is to provide empirical evidence of a SOC changing in light of COVID-19's WFH, namely by how analysts redirect their efforts during this change (e.g., labor-automation via tools, manually intensive tasks).

As indicated by our historical analysis, if we locate organizational means and forms of automation specific to endpoint security management, COVID-19 may potentially indicate another period of increased endpoint security management. Similar to the phenomena of BYOD, this period may introduce additional challenges for SOCs [79]. In short, specific themes of the ethnographic study determined by the historical review include our ethnographic emphasis on the SOC 'tooling up' with automation techniques in order to deal with endpoint challenges (as detailed below), and that history showed us that there was always a social and a technical dimension.

5.1 Participant Observation Findings

Before and throughout the COVID-19 transition, our embedded fieldworker operated alongside analysts to develop in-depth knowledge about the environment. Known as participant observation, the following subsection outlines our findings strictly from this methodology.

Our fieldworker observed and noted the SOC's dependence on the firewall, vulnerability scanner agents, and locally-installed anti-virus on endpoints to protect the majority of users. Our embedded fieldworker experienced, first-hand, the shifting priorities within the SOC as a response to COVID-19's WFH phenomena. Based on these evolving priorities, shown in Figure 2, we identified one trend that, we believe, will alter the long-term methods SOC employees use to secure their environment - endpoint management. Furthermore, we also experienced the unintended consequences of this trend such as privacy implications and analyst burnout.

Preparation - The Beginning (Early-Mid March 2020): During the beginning of the COVID-19 pandemic, we witnessed the majority of users and their work devices moving off the physical campus rendering a number of processes ineffective such as devices not present behind the firewall, external traffic not detected by the intrusion detection system (IDS), and the VPN at maximum capacity.

In this SOC, the analysts maintain the VPN, thus they scrambled to increase the VPN capacity and ensure not only could end users securely connect to and access on-premise resources, but the SOC also needed to protect endpoints from external threats when accessing the World Wide Web.

Aside from increasing the VPN capacity, communication changed, *"[Virtual] communication went through the roof"* (P1). Talking to other employees is no longer a casual conversation which P5 expressed, *"Hallway conversations don't exist anymore, so we have to be more direct."* In other words, these 5-minutes cubicle conversations turned into 60-minutes virtual meetings. The entire SOC echoed this sentiment where the increase impedes them from performing their daily operations. Mainly stemming from other departments wanting security-conscientious personnel to ensure best-security practices, (P4) indicated that some meetings were irrelevant to security. Along with adjusting the VPN and the increase in meetings, other departments had extra tasks to ensure the organization could still operate with the altered physical location. Unfortunately, these other departments also oversaw security-related operations (specifically the L1 IT help desk), and the

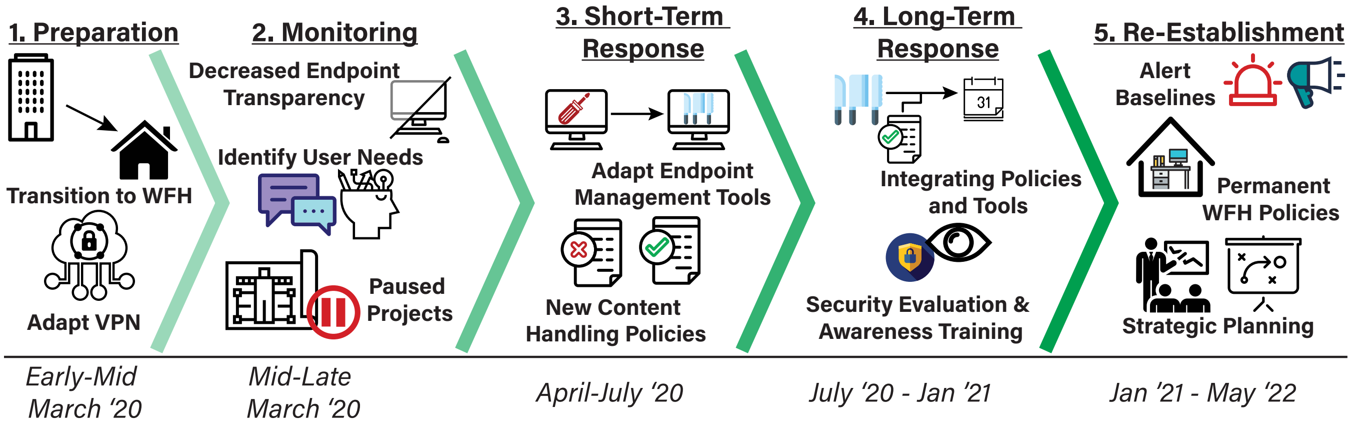

Figure 2: Observed SOC's Response to COVID-19 – Prior to WFH, the SOC's team met to discuss the possibility of remote work. Upon the organization temporarily pausing operations and the follow of users returning, the SOC worked towards not only identifying changes needed to support the new environment but also considering the change in current security controls.

SOC was forced to temporarily oversee these security-related operations in addition to the SOC's current tasks.

To summarize, the SOC balanced increasing the cybersecurity tools' capacity and overseeing additional security tasks whilst the organization demanded more of their time.

Monitoring (Mid-Late March 2020): To ensure the organization can still operate, both users and employees who did not have an organization-owned device were offered one, thus the number of deployed endpoints increased. However, the analysts quickly highlighted the dangers of this such as documenting the device inventory going home with end users. Notably, P5 expressed their concerns regarding device inventory, *"I'm concerned about endpoint monitoring and endpoint patching. I want to know what was taken off-campus and if everyone told the correct personnel to keep track of inventory."* This concern's motivation comes from (1) how the physical network location is an important indicator for threat detection, and (2) if new security-related technology needs to be installed on these endpoints, the SOC needs to determine which endpoints currently do or do not have that protection.

"It doesn't do any good to provide security on campus when there isn't anyone there anymore." (P2) Aside from the increased endpoints, yet a lack of device inventory, the analysts were also concerned with the decreased transparency of their endpoints' actions. Within our SOC, there was a heavy reliance upon the firewall and network access points for network transparency. However, all of these devices shifted from leveraging the campus' physical access points protected by firewalls to leveraging home or public networks. In other words, the origin of network traffic moved from mainly inbound to outbound, meaning they were no longer covered by the organization's firewall. Although a virtual private network (VPN) will route traffic behind the firewall, not all users installed, or use the SOC-controlled VPN. As P4 pointed out, *"we just don't have visibility on what endpoints are doing"* which P2, P3, and P5 all agreed.

With an increase in external endpoints (i.e., devices not leveraging the organization's network) but a decrease in security coverage (i.e., firewall doesn't apply to non-VPN traffic), the responsibility of the SOC to protect devices was strained. This was particularly evident when another similarly structured organization was targeted by ransomware. As P5 fearfully expressed, *"the news out of [organization's] ransomware attack is dire."* and P2 shared this concerned sentiment. This ransomware exploits unpatched vulnerabilities, targets user accounts and performs spear-phishing attacks. Securing these vectors requires endpoint patching and monitoring incoming emails [110]. This attack was particularly motivating for the SOC not only because of the attack's success as P5 shows, *"... 1) It seems likely it's Netwalker, which is the same ransomware that hit [an organization]. 2) They actually paid"*, but in addition, it highlights the lack of endpoint management in which the SOC is no exception: *"We also need to assume that personal devices are a serious threat here since we cannot enforce any kind of controls over them with our current toolset. I believe [vendor] has tools we can push out via the VPN client which would help but is not a perfect solution since not everyone is using the VPN."* (P5). In other words, personal devices located on the end user's personal network pose a large problem to work computers.

On top of the issues directly facing the SOC, the organization imposed changes upon all the departments that contradicted with the SOC's needs. During WFH, a few projects could impact end users such as moving email inboxes into the cloud, automatically installing client-side software for increased security, or deploying self-phishing exercises. Attempting to continue these efforts posed a risk of disrupting the organization's end users, thus these projects were temporarily suspended. This means that all of IT temporarily paused projects to allow users to adjust to WFH which conflicted with the SOC's attempt to re-establish better security tools in hopes to increase transparency.

Suspicious Emails Reported by Users	Counts	Percentage
Legitimate Emails	1,964	8.6%
Malicious - Non COVID-19	19,819	87.5%
Malicious - COVID-19	880	3.9%
Total	22,647	100%

Table 3: Statistics of COVID-19's impact on incoming, unblocked emails from January 1, 2020 to February 1, 2022.

All in all, during March, the SOC increased the VPN capacity, attended more meetings, oversaw security functions from tier 1 (a.k.a., L1), handled the uncertainty around asset inventory, witnessed the gap of protection across endpoints, and scrambled to identify how to defend against ransomware.

Short-Term Response (April-July 2020): Another priority, labor-wise, was an increased effort on monitoring and managing malicious emails. In particular, the organization experienced an influx of malicious emails taking advantage of the pandemic which coincides with SIEMplify's survey [101]. Because these emails contained terminology/text specific to COVID-19, the SOC released public communication reports which (P5) helped develop, *"are there any other COVID-19 emails you could forward to me? I'm working up a memo"*. These experiences paired with public articles highlighting recent COVID-19 scams (i.e., one manager requested a correlation between a public dataset and the organization's email dataset), increased the priority of monitoring incoming emails and resulted in a new script to calculate the distribution of emails specific to COVID-19. Attackers also filed fraudulent unemployment claims that affected organization's employees who would forward those emails to the SOC. These two events increased the SOC's pressure on monitoring emails.

The SOC employs two main techniques when stopping these types of attacks (blocking malicious URLs and pulling emails from inboxes). Thus, we wanted to better quantify the impact on COVID-19 related emails. We numerically analyzed malicious COVID-19 emails *reported* directly to the SOC between January 1, 2020 to February 1, 2022 as seen in Table 3. Out of the 22,647 reported emails during this duration, 19,819 emails were malicious with 880 of those malicious emails mentioning COVID-19 within the content.

Protecting users from email is not the SOC's only motivation. The SOC also wanted to proactively protect the endpoints' applications. Additional controls are required to increase endpoint protection, but the SOC's pre-WFH security solutions were no longer sufficient. To address this shortcoming, the SOC focused on re-tuning applications such as Zoom [123]. The SOC required adjustments to Zoom across all users such as pushing out updates and mandating security settings for all users, *"FYI the Zoom changes went through last night. Password required on all Zoom meetings after the change (this can't be shut off) and caller ID masking is enabled for dial in users"* (P5). For a clearer understanding, we calculated the number of times an article covering Zoom vulnerabilities was shared amongst the team. Between March 15th and December 31st of 2020, the SOC shared 220 URLs containing various security information with 14 of these URLs discussing the latest Zoom vulnerabilities.

Aside from reconfiguring applications, the SOC focused on their current cybersecurity toolset and adjusted technical settings particularly within the anti-virus application: increasing password complexity requirements (i.e., credential protection), preventing certain applications from executing through the preexisting anti-virus, and privilege escalation prevention. Not only are these controls similar to endpoint protection, but they also protect against data loss stemming from the user, which in turn protects the organization from compromised user accounts [77, 102, 115, 119]. To further prevent data loss, the SOC restricted certain types of device applications as deemed suspicious by the software (e.g., patch level, device behavior etc). These findings are similar to Cybersecurity Insider's survey where respondents were concerned about unmanaged endpoints leaking data [21].

Partially unrelated to COVID-19 but still occurring during the phenomena, establishing these short-term solutions were met with additional challenges: slow vendors. When attempting to establish other services to re-instantiate the security posture, vendors were slow upon providing financial quotes, and the SOC encountered issues implementing proof-of-concepts within the organization. Furthermore, a last-minute change caused the SOC to implement an entirely new encryption certificate setup during the midst of WFH.

Long-Term Response (July 2020-January 2021): Whilst accounting for the organization's pause on projects, the SOC adjusted security settings to better reflect the new phenomena. However, these adjustments reflect a short-term solution and do not account for the lack of transparency or control over endpoints. During this study, the SOC also tested other tools with more robust monitoring behavior and easier integration with current tools (i.e., blocking DNS requests through an additional service rather than the firewall). This behavior coincides with a small percentage of analysts surveyed by CSO [16]. They also consider cloud-based instances instead of on-premise installed applications due to the change in location and the concerns related to remotely installing client-side applications (i.e., agentless installation). Unfortunately, to add to the responsibilities of an arguably already overloaded SOC, newer alert detection services introduce additional challenges such as the increase of alerts as P4 and P5 highlight, *"how do we deal with the backlog of alerts?"*

The SOC wanted to further secure the organization's resources from compromised endpoints. With devices and users needing external access into the organization's data center, the need for data protection rose which P5 desired, *"If there are ways to monitor for massive data [exfiltration] at the border, I'm all ears,"* and P4 mirrored, *"Daily checks of botnet activity... Periodic check of SaaS platforms... In regards to potential data exfiltration."* Thus, we witnessed a special case of endpoint management: content handling. We define SOC content handling as actions taken to prevent users from accessing the organizations' resources based upon the content's semantic meaning. In this case, the SOC is looking at the semantic-meaning of data passed through the network.

Conditional access is another technique used to protect the organization by restricting endpoints. In this work, we define conditional access as the action to restrict endpoint's access to specified resources typically based upon semantic information. The SOC attended training webinars and tested in-place applications that could potentially limit user's access to software applications and data. In order to implement conditional access, analysts determine high-risk features and prevent certain devices with those identified features from obtaining important resources. For example, one discussion revolved around preventing devices running end-of-life Windows 7 from accessing cloud-based storage.

Even though these changes are motivated with good intentions (e.g., protect the organization from threat actors), we noted a decrease in end-user's right to privacy. User devices are not restricted to organizational use and in fact, can be used for personal matters. With these new tools, the SOC analysts could now leverage more of the individual user's activity as these tools correlate directly to the user rather than aggregated network traffic during pre-WFH. For example, our SOC primarily monitored endpoints' traffic within the network perimeter. Under the regular operating procedure, devices were isolated or blocked from the enterprise network when suspicious network traffic to and/or from those devices was detected. Once a device was blocked, its user/users and the corresponding network administrator were identified and then notified. *Only then*, depending on the type of compromise and the involved user account(s), the SOC accessed the device and analyzed information directly on that endpoint.

With no or very limited network traffic to serve as a warrant for identifying malicious behavior during WFH, the SOC had to compensate for the lack of visibility by relying on a continuous access to endpoint devices that monitor very detailed and in-depth system behavior, system contents, and user activity (similar to a constant search without a warrant/preliminary indicator). The SOC analysts noted this challenge, *"User behavior [analytics] is a political issue ... the current language is 'we only monitor devices' yet it's typically a 1-to-1 ratio"*(P2), and communicated that they want to address expectations to user privacy. We are not aware of endpoint data being misused in our SOC; however, this presents the possibility of COVID-19's WFH phenomena acting as another catalyst towards decreasing end user anonymity.

Re-Establishment (March 2021-May 2022): During these challenges, we noticed actions towards returning to the office. In March 2021, a few managers began partially working from their on-campus offices (witnessed by our embedded observer during conference calls). When the mask mandate was lifted, the SOC's organization announced new WFH policies, and the managers requested help to develop a work schedule that supports at least one analyst physically present at the office and the rest working from home. As the SOC slowly transitions back into the office, there are noticeable changes still present in the wake of COVID-19. In particular, new anti-virus and DNS monitoring systems were integrated into everyday alert handling tasks. Although these two solutions intend to increase transparency by monitoring the local device no matter its location, we are beginning to see the consequences of quickly rolling out tools under stress (tools do not deliver features suited for day-to-day operations, failed tool integrations were not removed from devices thus increasing the attack surface through unmaintained endpoint agents). Furthermore, new policies regarding data handling, data confidentiality, and data usage ethics have been issued at an organization-wide level. We also see that the majority of meetings are still conducted online over Zoom or Microsoft Teams. In addition, many of the projects initially paused have resumed, but many deadlines have been delayed as a consequence.

Lastly, we saw a reduced budget greatly affect not only the organization, but also the employees within this SOC. These budget cuts, initially occurring at the height of WFH, resulted in a reduced salary across all SOC employees, restrictions upon onboarding new security tools to protect against current cybersecurity trends, and a drop in training opportunities (where the latter was very prevalent in this environment pre-WFH). To the best of our knowledge, these continue to this day. Compounding these arguably stressful events, the SOC also experienced (1) incidents over vacation days thus eliminating the potential for relaxation, (2) the nationwide vulnerability, Log4J [6], quickly following the reductions of vacations, and (3) potential cyber threats from the Russia and Ukraine war [39]. With an overwhelming amount of stressors placed on the SOC employees, we witnessed burnout amongst employees and high turnover in a short time period.

5.2 Semi-Structured Interview Summaries

To help validate our findings from participant observation, we conducted two rounds of semi-structured interviews amongst our SOC employees from participant observation.

Whilst our fieldworker was embedded, they personally noted an initial impact on work, communication, and productivity. As the SOC's initial WFH demands decreased, we conducted the first round during the long-term response period (Oct 2021), and focused on verifying these initial impacts.

Although we interviewed 12 participants, only 5 participants were present for the first round as described in Section 3. For the first interview, not all participants agreed on each question. This was most times a consequence of employment position or duration within the SOC. However, all participants felt that their work altered in some way: increase (n=2), decrease (n=1), work changed (n=2). For the participant noting a decrease, they viewed physical visitations as a sign of progress, *"People are not dropping by the office to*

Sector	#	Endpoint Access	Privacy Policy	Changed WFH Model	Endpoint Transparency	Impacted Projects	Monitors Emails
Education	4	True (4)	True (3)	True (2)	Down (2), Up (1)*, Same (1)**	True (4)	True (4)
Government	1	False (1)	False (1)	True (1)	Same (1)**	True (1)	True (1)
Industry	2	True (2)	True (2)	True (1)	Same (2)	True (1)	True (1)
Total	7	True (6)	True (5)	True (4)	Same (4)** Down (2), Up (1)*,	True (6)	True (6)

Table 4: Descriptive Statistics of Surveyed SOCs (Section 6). It appears that the biggest determination towards decreased endpoint transparency lied within SOCs who have a mostly local, centralized workforce. *Reported new devices were provided in lieu of WFH leading to better transparency. **Began with poor transparency which continued during COVID-19's WFH.

talk about things"(P3). A similar theme appeared when we asked other participants about communication, *"... I won't get a good response unless I put an undue amount of effort into [messaging] them ...that's gotten worse with COVID because before I could speak to them in person and it feels like it wasn't as hard to get a response"* (P2) followed by *"I feel out of touch. I wish I could reach out to [our team] as I know they may feel uncomfortable reaching out to me"*(P4). On the other hand, some participants liked the change, *"...the quality, efficiency and accessibility all improved both within and outside the department"* (P5). (P1) echoed this. As for productivity, all participants felt an increase in their productivity except for (P2), *"Our jobs have basically turned into operations, all the time, which is the worst part of the job for me, and that's probably a major part of why [my] productivity is down."*

During the second round, we wanted to uncover analysts' perceptions surrounding our derived themes (e.g., endpoint security management and end user autonomy). Regarding endpoint management, out of the seven employees (one employee transferred positions between the interviews and three employees were initially unavailable), three participants mentioned the lack of transparency amongst user devices. To note, three additional participants did not comment on transparency due to their responsibilities on access management. The remaining participant focused on motivation overcoming the company's culture. In fact, five participants pointed out COVID-19 was a motivator for deploying better features. Five participants also agreed that the motivation behind content handling was similar to endpoint management. All employees have not deeply considered endpoint exposure or administrative accountability although they were in agreement these should be done.

6 Quantitative Survey Summaries

Since participant observation is limited to one SOC, we note that this can be a major limitation. To help generalize our ethnographic findings, we conducted quantitative surveys (July 26 to August 5, 2021) with seven other SOCs.

Relevancy and Representativeness: To ensure anonymity, we cannot provide the SOCs' names, but some of our participants oversee multi-layered SOCs for Forbes 500 companies, academic institutions, and government entities. Seven SOCs may not constitute a sufficient statistical sampling size, but we put forth that the variety of our participants help generalize our ethnographic findings (e.g., differing sectors, activities, policies, user base, and funding). For ethical purposes, we did not ask about budgets, salaries or training opportunities.

To ensure our participants' relevancy towards our study, we asked about access to endpoints and WFH policies. Six SOCs reported they have access to endpoints, and six SOCs had a partial or hybrid WFH structure prior to COVID-19, yet seven SOCs converted to WFH. Although seven SOCs immediately transitioned operations to entirely remote work, three support WFH fully after the initial WFH adaptation, and four support a partial or hybrid setup. Since this survey's completion date, COVID-19 WFH slowly approaches its end with new return policies (n=2), hybrid work (n=6), and returning to the office (n=1). Thus, we determined that of the eight total responses seven participants are relevant as they perform endpoint security management (e.g., endpoint detection and response, email monitoring). The eighth respondent did not answer enough questions for the study, thus we excluded their response.

Findings Summary: Although COVID-19 caused drastic moves towards WFH, endpoint transparency altered under specific circumstances where four of six participants reported a decrease in transparency. It appears that the *biggest determination towards decreased endpoint transparency lies within SOCs who have a mostly local, centralized workforce*. SOCs did not report decreased transparency if they (1) could be defined as a Managed Security Service Provider or (2) worked with a highly distributed user base. We found that COVID-19 affected projects, and of the six affected participants, three participants explicitly reported projects pausing due to reprioritization. Four participants experienced projects dropping, progressing slower, but also progressing faster. To further generalize our findings, we also found that (1) all SOCs who monitor emails (six respondents) experienced malicious emails containing COVID-19 content, (2) six SOCs experienced other departments needing more assistance than normal, and (3) five participants encountered an increase in meetings. We summarized the results in Table 4.

7 Discussion and Action Items

Our historical analysis highlighted that organizational means and forms of automation potentially indicate a new period of increased endpoint security management. Based on our ethnographic methods, we identified our SOC's trajectory change from maturing (e.g., training staff, configuring SIEMs, automating redundant tasks) to solely deploying and configuring automated endpoint security management tools.

The semi-structured interviews contributed to confirming that the motivation of this shift was COVID-19's WFH phenomena. Lastly, based on our surveys, other SOCs with a local, centralized workforce were similarly affected and worked towards improved endpoint security. With these findings, we suggest that this push *reflects an intensified period* of endpoint security management. Furthermore, we note that even though BYOD previously brought very similar challenges, many current endpoint security tools are costly, thus we also suggest this intensified period forced many lagging SOCs to, more permanently, invest into endpoint security [19].

A Regulatory Environment for SOCs: While the organizational management of endpoints is old, SOCs and their predecessors have, traditionally, used their technology to manage network components, not endpoints. This has spared them from some of the legal and social issues that arise when semantically rich *content* is handled (e.g., end user browsing behavior) [122]. We believe that this turn to endpoint control is extremely significant insofar as SOCs come to be expected or seen as a site of content-aware monitoring. With locally-installed applications on computers used for professional and potentially for personal use, not only does transparency increase but also the level of control a SOC can apply to these devices such as blocking URLs to websites, removing emails from inboxes, or opening well-known ports for better access. Content monitoring is more easily drawn into culture wars and could even spark calls for regulation [20]. Based on our study, we believe SOCs must cautiously proceed with technical actions and consider the sociotechnical aspect behind implementing endpoint security management.

Another Stimulus of Burnout: After the initial shock of COVID-19, a lot of pressures continued to weigh on the SOC analysts. We saw organization budget cuts resulting in a reduced salary across all SOC employees, restrictions upon adopting new (proprietary) security-oriented tools, a drop in training opportunities, and incidents over vacation days. Corroborated with various external events (e.g., [6] vulnerability, [39]), these factors weighed heavily in the decision of SOC personnel to leave their jobs.

Action Item 1 - Device coverage: Lack of transparency was prominent during COVID-19's WFH yet transparency is an important factor in securing systems [43]. Our case study SOC was able to reconfigure, re-purpose and integrate existing services into operations whilst recognizing their remaining inefficiencies. However, with such a distributed network boundary, endpoint security management focused tools may still not be enough to protect resources. Rather than control all endpoints from a network-focused perspective, a Zero Trust perspective may be more appropriate. Specifically, SOCs should already assume devices are compromised. This allows SOCs to focus more upon enforcing controls tailored to critical threats (e.g., lateral movement, data breaches etc.) rather than protecting all endpoints [95]. Our SOC and its parent organization started dedicating resources to enabling such a shift.

Action Item 2 - Tracking time for training: Although a Zero-Trust-oriented effort may be warranted, we note that this approach requires processes, technology, and people to implement [95]. As we found through participant observation and interviews, many pressures during COVID-19 led to burnout, and these needed resources may not be available to SOCs. Thus, we also propose that SOCs should track time spend on training. Many SOCs may have quickly adopted endpoint security management yet may have failed to provide training - particularly towards user-device monitoring challenges (e.g., continuous browsing history to user attribution). We believe this will help realign SOCs towards increasing maturity.

Action Item 3 - Documentation and data needs: Managing complex controls in modern endpoint management systems can be burdensome [73]. Thus, SOCs should ensure that restrictions upon semantic content are strictly security-related rather than motivated by other factors. We believe this can be accomplished by documenting policies surrounding the expectations of end user privacy. We also believe that these policies can help the SOC formulate their precise data needs and in turn potentially reduce user-device content-aware-related challenges. Our studied SOC has recognized these challenges as permanent, especially since the new monitoring tools and the reconfigured tools aimed at increasing visibility on endpoints during COVID's WFH became part of their everyday alert handling process. Moreover, even if most of the organization returned back to an in-person, in-office mode, there are some groups that were reorganized into a permanent WFH mode. Thus, policy-adjustments at the organization level, documenting these changes, and establishing security data needs from end-user devices can be viewed as continuous efforts.

8 Conclusion

This paper identifies and analyzes a major SOC trend intensified by WFH, namely endpoint security management. By combining historical and ethnographic analysis and methodologies, we highlight not only another catalyst to SOC endpoint security management (i.e., COVID-19's WFH), but we also pose that these abrupt changes push SOCs towards a new environment of user privacy that they may not be equipped to readily address. To begin addressing this new climate, SOCs could start by assessing specific data needs from their endpoints as well as documenting processes for accountability.

Acknowledgements

We are grateful to all of our collaborators in this work and to our anonymous shepherd and reviewers for their thoughtful and constructive comments, which vastly improved this paper. This work was supported by the National Science Foundation (NSF) under Awards 1915824, 1915822, and 1850406. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the NSF.

References

[1] A. Aarness. What is Endpoint Management? [link], (09/22).

[2] J. Abbate. *Inventing the Internet*. MIT Press, 1999.

[3] N. Abdi and J. M. Ramokapane, K. M. Such. More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants. In *SOUPS*. USENIX Association, 2019.

[4] N. Abramson. The ALOHA System Final Technical Report. Technical report, ARPA, 1974.

[5] ACM. ACM Proceedings. [link], (10/22).

[6] C. S. I. Agency. Apache Log4j Vulnerability Guidance. [link], (09/22).

[7] E. Agyepong, Y. Cherdantseva, P. Reinecke, and P. Burnap. Towards a Framework for Measuring the Performance of a Security Operations Center Analyst. In *Conference on Cyber Security and Protection of Digital Services*, 2020.

[8] B. Aiken, J. Strassner, B. Carpenter, I. Foster, C. Lynch, J. Mambretti, R. Moore, and B. Teitelbaum. Network Policy and Services: A Report of a Workshop on Middleware. RFC 2768, Cisco Systems, 2000.

[9] O. Akinrolabu, I. Agrafiotis, and A. Erola. The Challenge of Detecting Sophisticated Attacks: Insights from SOC Analysts. In *ARES*. ACM, 2018.

[10] J. Allen, D. Gabbard, C. May, E. Hayes, and C. Sledge. Outsourcing Managed Security Services. Technical report, CMU, 2019.

[11] J. Arkko, S. Farrell, M. Kühlewind, and C. Perkins. Report from the IAB COVID-19 Network Impacts Workshop 2020. RFC 9075, Internet Architecture Board, 2021.

[12] J. Ashworth. Abuse @Virginia.Edu: Going Where No One Wanted to Go. In *SIGUCCS*. ACM, 1998.

[13] H. Axlerod. Creating an Atmosphere of Responsible Computing. In *SIGUCCS*. ACM, 1997.

[14] S. Baker. The Making of an Unmonitored 24 Hour Access Computer Lab. In *SIGUCCS*. ACM, 1993.

[15] B. G. Baumgart. SAILDART. [link], (10/22).

[16] B. Bragdon. Pandemic Impact Report: Sec. Leaders Weigh In. [link], (10/22).

[17] H. Braun. The NSFNET Routing Arch. RFC 1093, Merit, 1989.

[18] M. Bromiley. SANS Institute InfoSec Reading Room. [link], (10/22).

[19] C. Brooks. Cybersecurity in 2022 – A Fresh Look at Some Very Alarming Stats. [link], 02/23.

[20] F. Brunton. *Spam: A Shadow History of the Internet*. MIT Press, 2013.

[21] Buffer, Doist, Remotive, and We Work Remotely. State Of Remote Work 2021. [link], (10/22).

[22] Buffer, Nomad List, and Remote OK. 2022 State Of Remote Work. [link], (10/22).

[23] P. Cain and D. Jevans. Extensions to the IODEF-Document Class for Reporting Phishing. RFC 5901, The Cooper-Cain Group, Inc., 2010.

[24] M. Campbell-Kelly. *Computer: A History of the Information Machine*. Routledge, 2018.

[25] J. Case, M. Fedor, M. Schoffstall, and J. Davin. A Simple Network Management Protocol. RFC 1067, Univ. Tennessee-Knoxville, 1988.

[26] L. N. Cassel, C. Partridge, and J. Westcott. Network Management Architectures and Protocols: Problems and Approaches. *Journal on selected Areas in Communications*, 1989.

[27] R. P. Center. https://www.rfc-editor.org/. [link], (10/22).

[28] V. Cerf. IAB Recommended Policy on Distributing Internet Identifier Assignment and AB Recommended Policy Change to Internet "Connected" Status. RFC 1174, CNRI, 1972.

[29] T. R. Chen, D. B. Shore, S. J. Zaccaro, R. S. Dalal, L. E. Tetrick, and A. K. Gorab. An Organizational Psychology Perspective to Examining Computer Security Incident Response Teams. *IEEE S&P*, 2014.

[30] Computer History Museum. Catalog Search. [link], (10/22).

[31] C. Crowley. Common and Best Practices for Security Operations Centers: Results of the 2019 SOC Survey. [link], 2019.

[32] DARPA. ARPA Becomes DARPA. [link], (10/22).

[33] K. M. M. de Leeuw and J. Bergstra. *The History of Information Security: a Comprehensive Handbook*. Elsevier, 2007.

[34] Defense Communications Agency. ARPANET Information Brochure. Technical report, DDN, 1976.

[35] Defense Communications Agency. ARPANET Information Brochure. Technical Report NIC 50003, SRI International DDN Network Information Center, 1985.

[36] Defense Technical Information Center. Products & Services. [link], (10/22).

[37] Q. DuPont and B. Fidler. Edge Cryptography and the Codevelopment of Computer Networks and Cybersecurity. *IEEE Annals of the History of Computing*, 2016.

[38] E. Elsam. COINS II/ARPANET: Private Line Interface (PLI) Operations Manual, 1980.

[39] K. Fendorf and J. Miller. Tracking Cyber Operations and Actors in the Russia-Ukraine War. [link], (09/22).

[40] B. Fidler. The Evolution of Internet Routing: Technical Roots of the Network Society. *Internet Histories*, 2019.

[41] B. Fidler and M. Currie. The Production and Interpretation of ARPANET Maps. *IEEE Annals of the History of Computing*, 2015.

[42] B. Fidler and A. L. Russell. Financial and Administrative Infrastructure for the Early Internet: Network Maintenance at the Defense Information Systems Agency. *Technology and Culture*, 2018.

[43] T. Field. Cybersecurity: Redefining Visibility and Transparency. [link], (10/22).

[44] C. Finseth. An Access Control Protocol, Sometimes Called TACACS. RFC 1492, Univ. of Minnesota, 1993.

[45] T. J. Foley. Developing a Computing & Information Policy. In *SIGUCCS*. ACM, 1990.

[46] S. Frankel and S. Krishnan. IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap. RFC 6071, NIST, 2011.

[47] K. Gallagher. Upwork Study Finds 22% of American Workforce Will Be Remote by 2025. [link], (10/22).

[48] R. Ganesan, A. Shah, S. Jajodia, and H. Cam. *A Novel Metric for Measuring Operational Effectiveness of a Cybersecurity Operations Center*. Springer International Publishing, 2017.

[49] Google. Books Ngram Viewer. [link], (10/22).

[50] Google. Google Books Ngram Viewer: AUP. [link], (10/22).

[51] Google. Google Books Ngram Viewer: endpoint enc. [link], (10/22).

[52] Google. Google Books Ngram Viewer: WFH. [link], (10/22).

[53] J. Hadden, L. Casado, T. Sonnemaker, and T. Borden. 21 Major Companies that have Announced Employees can Work Remotely Long-term. [link], (10/22).

[54] E. Haleplidis, K. Pentikousis, S. Denazis, J. H. Salim, D. Meyer, and O. Koufopavlou. Software-Defined Networking (SDN): Layers and Architecture Terminology. RFC 7426, Univ. Patras, 2015.

[55] Harvard Kennedy School's Belfer Center for Science and International Affairs. Applied History Project. [link], (10/22).

[56] M. J. Haughney. Arpanet Newsletter No. 6. Technical report, Defense Data Network (DDN), 1981.

[57] M. M. Hennink, B. N. Kaiser, and V. C. Marconi. Code Saturation Versus Meaning Saturation: How Many Interviews Are Enough? *Qualitative Health Research*, 2017.

[58] K. Horning, S. Calcari, P. Smith, and D. Katz. LINK LETTER: The Merit/NSFNET Backbone Project. Technical report, NSFNET, 1990.

[59] IEEE. IEEE Xplore. [link], (10/22).

[60] R. S. Jhangiani, I. A. Chiang, C. Cuttler, and D. C. Leighton. *Research Methods in Psychology*. Kwantlen Polytechnic Univ., 2019.

[61] D. Johnson. NOC Internal Integrated Trouble Ticket System Functional Specification Wishlist. RFC 1297, Merit Network, Inc., 1992.

[62] A. R. Jones. Computer Use Policies: The Challenge of Updating Lab Software Security. In *SIGUCCS*. ACM, 1993.

[63] D. Kaplan. Security Operations Center Burnout: A Guide for SOC Professionals. [link], (10/22).

[64] B. B. Kawulich. Participant Observation as a Data Collection Method. In *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research*, 2005.

[65] A. Kershenbaum, M. Malek, and M. Wall. *Network Management and Control*. Springer US, 2013.

[66] P. T. Kirstein. University College London ARPANET Project Annual Report, 1 January 1977 - 31 December 1977. Technical Report INDRA Technical Report 1978, Univ. College London, 1978.

[67] L. Kleinrock and W. E. Naylor. *On Measured Behavior of the ARPA Network*. AFIPS '74. ACM, 1974.

[68] J. Koebler. It's September, Forever. [link], (10/22).

[69] F. B. Kokulu, A. Soneji, T. Bao, Y. Shoshitaishvili, Z. Zhao, A. Doupé, and G. Ahn. Matched and Mismatched SOCs: A Qualitative Study on Security Operations Center Issues. In *CCS*. ACM, 2019.

[70] D. Kreutz, F. M. V. Ramos, P. E. Veríssimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig. Software-Defined Networking: A Comprehensive Survey. *Proceedings of the IEEE*, 2015.

[71] K. Lougheed and Y. Rekhter. A Border Gateway Protocol (BGP). RFC 1105, Cisco Systems and T.J. Watson Research Center, IBM, 1989.

[72] A. Mai, K. Pfeffer, M. Gusenbauer, E. Weippl, and K. Krombholz. User Mental Models of Cryptocurrency Systems - A Grounded Theory Approach. In *SOUPS*. USENIX Association, 2020.

[73] ManageEngine. What is Modern Management? [link], (10/22).

[74] A. McKenzie. The ARPA Network Control Center. *Fourth Data Communications Symposium, Quebec City, Canada*, 1975.

[75] A. McKenzie, B. P. Cosell, J. M. McQuillan, and M. J. Thrope. The Network Control Center for the ARPA Network. *Proceedings of the First International Conference on Computer Communication*, 1972.

[76] J. M. McQuillan and D. C. Walden. The ARPA Network Design Decisions. *Computer Networks*, 1977.

[77] Microsoft. Microsoft Defender for Endpoint. [link], (10/22).

[78] Microsoft. Microsoft Teams. [link], (10/22).

[79] K. Miller, J. Voas, and G. Hurlburt. BYOD: Security and Privacy Considerations. *IT Professional*, 2012.

[80] M. A. Miller. *Managing Internetworks With Snmp: The Definitive Guide to the Simple Network Management Prot.* M&T Books, 1997.

[81] U. NARA. National Archives. [link], (10/22).

[82] NSF. THE NSFNET BACKBONE SERVICES ACCEPTABLE USE POLICY, 1992.

[83] H. of Computer Communications Group. The History of Computer Communications. [link], (10/22).

[84] U. of Minnesota. Charles Babbage Institute Archives. [link], (10/22).

[85] Office of the Inspector General. Review of NSFNET. Technical Report 9301, National Science Foundation, 1993.

[86] PaloAlto. What is an Endpoint? [link], (10/22).

[87] C. Partridge. The Technical Development of Internet Email. *IEEE Annals of the History of Computing*, 2008.

[88] J. Peterson and A. Cooper. Report from the IETF Workshop on Peer-to-Peer (P2P) Infrastructure. RFC 5594, NeuStar, 2009.

[89] J. Postel. Domain Names Plan and Schedule. RFC 881, ISI, 1983.

[90] J. Postel and J. Reynolds. Domain Reqs. RFC 920, ISA, 1984.

[91] J. L. Rankin. *A Peoples History of Computing in the United States*. Harvard Univ. Press, 2018.

[92] J. Rekhter. EGP and Policy Based Routing in the New NSFNET Backbone. RFC 1092, T. J. Watson Research Center, 1989.

[93] J. Reynolds and J. Postel. ARPA Internet Protocol Policy. RFC 902, ISI, 1984.

[94] A. S. Ridolfo. HP OpenView Network Management. *Hewlett-Packard Journal*, 1990.

[95] S. Rose, S. Mitchell, and S. Connelly. Zero Trust Framework. Technical report, NIST, 2020.

[96] E. C. Rosen. Exterior Gateway Protocol (EGP). RFC 827, Bolt Beranek and Newman Inc., 1982.

[97] J. Saltzer. On the Naming and Binding of Network Destinations. RFC 1498, M.I.T. Laboratory for Computer Science, 1993.

[98] J. Scarborough. ke4roh/internetHostCount. [link], (10/22).

[99] W. Schneider. Computer Viruses: What They Are, How They Work, How They Might Get You, and How to Control Them in Academic Institutions. *Behavior Research Methods, Instruments, & Computers*, 1989.

[100] H. Schulzrinne, E. Marocco, and E. Ivov. Security Issues and Solutions in Peer-to-Peer Systems for Realtime Communications. RFC 5765, Columbia Univ., 2010.

[101] Siemplify. The State of Remote Security Operations. [link], (10/22).

[102] Sophos. Intercept X. [link], (10/22).

[103] J. Staddon and N. Easterday. "it's a generally exhausting field" A Large-Scale Study of Security Incident Management Workflows and Pain Points. In *PST '19*, 2019.

[104] A. Strauss and J. Corbin. *Grounded Theory Methodology: An Overview*. Sage Publications, Inc, 1994.

[105] Z. Su and J. Postel. The Domain Naming Convention for Internet User Applications. RFC 819, SRI and ISI, 1982.

[106] S. C. Sundaramurthy, A. G. Bardas, J. Case, X. Ou, M. Wesch, J. McHugh, and S. R. Rajagopalan. A Human Capital Model for Mitigating Security Analyst Burnout. In *SOUPS*. USENIX, 2015.

[107] S. C. Sundaramurthy, J. Case, T. Truong, L. Zomlot, and M. Hoffmann. A Tale of Three Security Operation Centers. In *SIW*. ACM, 2014.

[108] S. C. Sundaramurthy, J. McHugh, X. Ou, M. Wesch, A. G. Bardas, and S. R. Rajagopalan. Turning Contradictions into Innovations or: How We Learned to Stop Whining and Improve Security Operations. In *SOUPS*. USENIX Association, 2016.

[109] S. C. Sundaramurthy, M. Wesch, X. Ou, J. McHugh, S. R. Rajagopalan, and A. Bardas. Humans are dynamic. Our tools should be too. Innovations from the Anthropological Study of Security Operations Centers. *IEEE Internet Computing*, 2018.

[110] A. O. I. Team. Take a "NetWalk" on the Wild Side. [link], (10/22).

[111] R. Thayer, N. Doraswamy, and R. Glenn. IP Security Document Roadmap. RFC 2411, Sable Technology Corporation, 1998.

[112] R. H. Thomas. Advanced Fleet Command Control Testbed Planning. Technical report, dtic.mil, 1977.

[113] Trellix. What Is a Security Operations Center (SOC)? [link]. (10/22).

[114] Trellix. Endpoint Security, (10/22). [link].

[115] Trellix. Trellix Endpoint Security. [link], (10/22).

[116] UCLA. UCLA Library. [link], (10/22).

[117] R. van Os. *SOC-CMM: Designing and Evaluating a Tool for Measurement of Capability Maturity in Security Operations Centers*. Dissertation, Lulea Univ. of Tech., 2016.

[118] M. Vielberth, F. Böhm, I. Fichtinger, and G. Pernul. SOC: A Systematic Study and Open Challenges. *IEEE Access*, 2020.

[119] VMware. VMware Carbon Black Cloud Endpoint. [link], (10/22).

[120] D. Walden and R. Nickerson. *A Culture of Innovation*. Waterside Publishing, 2011.

[121] M. Weber. Happy 25th Birthday to the WWW! [link], (10/22).

[122] B. Wolford. What is GDPR ... ? [link], (02/23).

[123] E. S. Yuan. Zoom. [link], (10/22).

A Appendix

A.1 Historical Analysis - Initial Entities

The historical analysis captured *a periodized chronology of endpoint management functions* from the 1970s to the end of 2019 (before COVID-19 restrictions). This section is focused on providing additional details about the initial involved entities such as ARPA/DARPA and DCA. Moreover, Table 5 captures the list of keywords resulting from our historical analysis methodology.

The Early Operational Arpanet (1972-1979): The US Advanced Research Projects Agency (ARPA) became the Defense Advanced Research Projects Agency (DARPA) in 1972, with a brief 1993-96 return to ARPA [32]. ARPA began its life as a four-node testbed in 1969, and reached basic functionality by late 1972 with working host software for common operating systems, remote login (telnet), file transfer (FTP), electronic mail (SNDMSG and CPYNET) and the formal role of the Network Control Center (NCC) [2, 76, 87]. However, end systems were often shared mainframe systems [76]. Outside of limited TCP/IP experiments, LAN endpoints directly connected to a local Arpanet host, and were not nameable or addressable on the Arpanet itself [4, 66].

Bolt Beranek Newman (BBN), the contractor that built the subnetwork and operated it through its Network Control Center (NCC; the direct predecessor to the Network Operations Center), knew the topology through a combination of manual and technical means that were increasingly automated over time [41]. The NCC could disconnect any host if it caused problems for the network [74, 75]. In 1975 the Defense Communications Agency (DCA, current DISA) introduced formal rules for local management of end systems, which were implemented by a "network liaison" at each site for all Arpanet-connected systems [34, 35, 42], all coordinated through another DARPA contractor, the Stanford Research Institute (SRI) and its Network Information Center (NIC).

The ARPA Internet (1980-1986): The Arpanet served as the main testbed for the TCP/IP suite from the mid-late 1970s, and became the Internet's backbone from 1983-86 (the Arpanet's last nodes were decommissioned in 1990) [96]. The Arpanet era also initiated the Internet's globally unique addresses mapped to network interfaces [97], an open application layer, global name mapping to addresses [2, 120], end-to-end cryptography [37], Local Area Networks [67], and new routing demands [40] (it garnered the name "ARPA Internet" [93] in some official documentation). The Arpanet also served as a template for other networks [120].

The NSFNET Before Privatization (1986-1990): A wave of automation hit network monitoring with the spread of Simple Network Management Protocol (SNMP) and Hewlett-Packard's first Network Node Manager (NNM), HP OpenView, both developed from the late 1980s [25, 94]. Triggered by the explosion in network size, complexity, and use, SNMP-based NNMs automated basic network monitoring and control tasks. This automation, in turn, permitted further division of labor between more and less skilled analysts. This process, as well as ticketing systems to help organize hierarchical work, became especially visible in the late 1980s [58, 61, 65]. It also permitted more automated management of heterogeneous networks, with new protocols such as Asynchronous Transfer Mode (ATM) and Multiprotocol Label Switching (MPLS) now in widespread use for and between enterprise networks [80].

A.2 Additional Field Notes Statistics

As detailed in Section 3.2, for 34 months (June 10, 2019 to May 16, 2022), we embedded one fieldworker to collect field notes. These field notes are comprised of recollections of attended meetings, discussions with SOC employees whilst working on projects, and personal observations of the fieldworker. The majority of these personal observations stem from performing similar work to the SOC employees (e.g., monitoring network traffic, developing machine learning scripts for increased protection, integrating security tools). Due to our unique perspective, these field notes contain rich, longitudinal descriptions of the studied SOC environment and, therefore, are our main source of ethnographic data.

During this study, we analyzed 352 field notes where 57 of the field notes are from 2019, 121 field notes are from 2020, 131 are from 2021, and 43 are from 2022. These field notes cover over 1,000 hours of the analyst embedded in the SOC and contain observations from more than 550 SOC meetings.

A.3 Semi-Structured Interviews

Our interviews intend to validate or invalidate our themes/findings resulting from the Grounded Theory Method (GTM). When interviewing, we used a list of questions as a guide and did not ask each question in order nor did we cover all of them in each interview depending on the time.

Table 8 captures our list of questions. Prior to starting the interview, we forwarded the questions to each interviewee and clarified that they may either interview live (face-to-face) or write their answers. Upon interviewing, we reiterated that each question is voluntary. Furthermore, we did not record video or audio rather the interviewer (our fieldworker) took notes and typed participants' quotes during the interview process. When an employee asked for something to be removed or not explicitly stated, the interviewer removed or stopped writing and continued when instructed to do thus.

Since the SOC we studied is short staffed, and with the increased pressure from multiple facets, the lack of resources prevents this SOC (at times) from covering their daily operations, troubleshooting unique cases, learning new tools in light of WFH, and proactively preventing new attacks. This includes the ability to participate in interviews and surveys.

Research Works	Keywords	Era
[4,34,35,37,38,41,42,66,74–76,112]	Arpanet, NOC, network control, secure facility, secure access, electromagnetic shield (physical security), access control policies, regulating network access, controlling remote access, authentication, management control	1972-1979
[2,24,40,44,56,82,89,90,93,96,105]	ARPA-Internet, Defense Communications Agency, host naming, scalable, centralized access, policies and procedures	1980-1986
[2,15,24,26,33,45,82,83,98,99]	NSFNET, distributed network, nodes, anti-virus, permissions, host monitoring, reformat, quarantine, network encipherment, acceptable use policies, distrust, identity management, security policies	1986-1990
[12–14, 17, 25, 28, 41,58,61,62,65,68,71, 80, 85, 92, 94]	OpenView management, private sector, scale, growth, network isolation, access controls, user behavior, surveillance, inventory management, video security cameras, physical security box, ID badges, updating software, viruses, automation, anti-virus, responsible use policies, ethics, privacy concerns, middleware	1991-1999
[8,23,37,46,54,70,88, 100, 111, 121]	SDN, IP security, endpoint encryption, network security, reputation management systems, phishing, fraud, sandbox	2000-2019

Table 5: Historical Analysis Works – Keywords resulting from our historical analysis methodology. Representing (1) major technological advances that help depict each era, and (2) the relatability to endpoint security management, we note the time period where security functions are *first applied* within the context of endpoint security management. As detailed in Section 3.1, these research works are derived from the various sources.

Disclaimer Provided	*This survey is completely optional, thus you may quit answering questions at anytime if you feel uncomfortable. The following questions will be used for general analytical use only. As these results are intended for scientific publication, your specific responses will not be connected to you in any way whatsoever upon publishing the finalized results. Your individual responses will not be given to any third party whatsoever. If you feel uncomfortable with any of the questions but want to continue, you may skip the question (some questions are marked required, thus pick the 'Other' options and type 'opt out').* -- Optionally, we requested the participant's first name in the even something happens with their response, so we could contact them.
Quantitative Interview Questions (Survey)	1. What is your job title? 2. How long have you held your current title? 3. Which of the following activities does your SOC oversee? Select all that apply: i) Incident response, ii) Security monitoring, iii) Data protection and monitoring, iv) Security administration, v) Alert and incident remediation, vi) Security road map and planning, vii) SOC architecture and engineering, viii) Threat research, ix) Compliance support, x) Digital forensics, xi) Pen-testing 4. Choose what best fits your SOC: i) The SOC has a privacy policy. It is set up externally. ii) The SOC has a privacy policy. The SOC sets that policy. iii) The SOC has a privacy policy. We are unsure who set that policy. iv) The SOC does not have a privacy policy. 5. Does your SOC possess access to endpoint systems: i) Yes, ii) No 6. Did your SOC support WFH prior to COVID-19: i) No, ii) Partially / Hybrid, iii) Fully 7. When COVID-19 began...: i) the SOC was deemed essential and thus worked on-site, ii) the SOC temporarily stopped operations. Operations continued on-site, iii) the SOC temporarily stopped operations. Operations continued entirely remote, iv) the SOC immediately transitioned operations to entirely remote, v) nothing happened. The SOC was already entirely remote. 8. Did your SOC support WFH after COVID-19: i) No, ii) Partially / Hybrid, iii) Fully 9. If you answered "partially" or "fully" on the prior question, has your SOC... (select all that apply): i) Created a policy to return to the office, ii) Continued to work-from-home, iii) Returned to the office, iv) Allowed a hybrid schedule between on-site and remote work. 10. If your SOC transitioned to WFH, how would you describe the transparency of endpoints before COVID-WFH... What about after COVID-WFH...: i) Very good, ii) Good, iii) Bad, iv) Very bad 11. If you answered the previous question, can you provide a few details? 12. How did your SOC respond with the nation-wide WFH shift? Select all that apply: i) New services/solutions/tools, ii) Repurposing prior existing services/solutions/tools, iii) New processes and/or procedures, iv) Repurposing prior processes and/or procedures, v) New documentation and/or policies, vi) Repurposing documentation and/or policies, vii) Increased SOC employee training, viii) Not applicable or N/A 13. If you answered the previous question, please elaborate on your answers. 14. If tools and/or processes changed, was training involved? Select all that apply: i) Not applicable or N/A, ii) Formal online training sessions, iii) Meetings with vendors, iv) Online webinars or videos. 15. Are alerting baselines established in your SOC? Select what best describes your environment: i) We don't have alerting baselines, ii) Alerts decreased when WFH occurred, iii) Alerts stayed relatively the same when WFH occurred, iv) Alerts increased when WFH occurred. 16. Select what best describes your environment: i) We do not manage/monitor email, ii) We manage/monitor emails. The content in malicious emails stayed relatively the same. iii) We manage/monitor emails. The content in malicious emails chainged, but nothing out of the ordinary. iv) We manage/monitor emails. The content in malicious emails changed. Some emails mentioned COVID-19. 17. Are meetings conducted? If so, choose what best describes your SOC: i) We do not conduct or attend meetings, ii) The number of meetings on my calendar decreased when WFH occurred, iii) The number of meetings on my calendar stayed the same when WFH occurred, iv) The number of meetings on my calendar increased when WFH occurred. 18. If your SOC works with other departments, which of the following did you experience: i) We do not work with other departments, ii) We did not need to help other departments when WFH occurred, iii) We needed to assist other departments more so than normal, iv) We needed other departments to assist us more than normal. 19. If you work with vendors, were their responses before WFH and after the WFH shift...i) Quick, ii) Somewhat Quick, iii) Normal, iv) Somewhat Slow, v) Slow, vi) We do not work with vendors 20. Were projects impacted by COVID-19? Select all that apply: i) COVID-19 did not affect our projects, ii) Some projects were paused, iii) Some projects were dropped, iv) Some projects progressed slower, v) Some projects progressed faster 21. If you answered the previous question, could you elaborate on your answers?

Table 6: Quantitative (Survey) Interview Questions – We created this question and answer set using the BRUSO method.

Axial Codes	Open Codes
(Operations) Endpoint Management	implementing proof of concepts for new endpoint management services/tools, increased monitoring (endpoints, DNS, multi-factor authentication, lockouts, email), building and testing proof-of-concepts, endpoint protection, rewriting the acceptable use policy, endpoint patching, new perspective on old tool, agentless rollout
(Operations) Data Handling	handling misinformation, internal conditional access, access de-provisioning, blocking (urls, malware, applications, emails), content filtering, developing CUI policies, determining conditional access, managing permissions, firewall rules, privilege escalation, tracking end of life, PCI compliance, improving encryption, pulling emails
(Operations) Internal SOC Organization	writing and editing documentation, developing metrics, altering policies, developing and documenting workflows, developing incident response procedure, creating tickets as documentation, developing strategic planning
(Operations) Privacy	preventing monitoring spyware among users, providing a password manager for the organization
(Operations) Business as Usual	automation, sharing public news, security awareness training, integrating service/solution/tool, compliance reporting, increasing VPN capabilities alert and incident handling, malware analysis, vulnerability patching, self motivated learning (webinars, at-home deployments), developing baseline, searching for IOCs, troubleshooting, whitelisting, advising other departments, preventing known attacks, scanning, external security assessment, attending meetings, ticket handling, scheduling peer assessments, moving towards cloud infrastructure, reaching out for external help, assisting other departments, user identification, identifying the scope and potential impacts, account password resets, decommisssioning service/solution/tool, vendor consulting
Social Limitations	physical location limitations and restrictions, disruption at home during WFH, issues with vendors, uncertainty, privacy versus security, insufficient training, policies, difficulties with external departments, tired, slow progress, overwhelming, pushback on security changes, increased meetings, reliance on external department, SOC accidents causing disruption, stressed external departments, busy external departments, stale project rollouts, balancing work, privacy implications, emotional burdens, scared, conflicting values, developing new policies, political issues impede security controls, intense, reliance on external departments, budget cuts, privacy concerns, prioritizing affecting progress, too many tickets, unrepsonsiveness, silos, external department layoffs, dropped projects, lack of transparency, lack of documentation, lack of money, lack of communication, employee turnover, salary cuts, budget cuts, limited budget, burnout, re-organization
Technical Limitations	unstable service/solution/tool, false positives, resource contention, license limitations, too many alerts, backlog of work, alerts requiring additional context, technical outages, decentralization, mismatched service/solution/tool, out-of-date devices, email bypassing the junk filter, lack of data, lack of logs
(Src. of Priorities) Worries and Pressures	public news, incidents at peer organizations (ransomware, breaches), ransomware, malicious emails (phishing, impersonation), external audits, COVID-19 malicious emails, external scan, BYOD, PII, vulnerabilities, increased attacks, incidents at peer organizations, VIP status changes alert significance, account lockous, data privacy, government-issued laws (i.e., blocking TikTok and WeChat), external data breach, attackers are evolving, new attacks (Zoom bombings), external vendor breach, politics, external pen testing, malware infecting cloud file storage, alerts and incidents, service/solution/tool changing, service level agreements, external security reports (audits, scans), perspective of users
(Src. of Priorities) Desires	more transparency, usable metrics, need documented policies, need documentation, follow best practices, external help, inventory management, need baseline, returning to the office, following best practices, increasing the security posture, increasing efficiency, better user passwords, honeypot, integration, agentless, desire automation, boundaries with meetings, better network segregation, block TOR, end WFH, prevent misinformation, conditional access
COVID-19/WFH Social Aspects	working from home, group WFH training, placing boundaries on meetings, planning WFH shifts, returning to the office

Table 7: Codebook – By analyzing the captured field notes using Grounded Theory, we noticed a change in operations impacted by social and technical limitations. Furthermore, we observed that these new operations are motivated by various factors.

Rounds	Semi-Structured Interview Questions
First Round	1. How do you feel about the level of work since COVID-19 started? When WFH started?
	2. Has your level of responsibility increased, decreased, or stayed the same?
	3. How is the communication amongst the team? With other departments?
	4. Have priorities shifted since WFH? How so? If priorities have shifted, did it make sense as to why this occurred?
	5. How has productivity been since WFH happened? Based on the current environment, what change might help improve your productivity?
	6. Do the current tools support WFH? Would a certain feature provide more help?
	7. What would you say is the big weakness of the SOC with WFH? How do you think this should be addressed?
Second Round	1. One of the priorities during the initial transition to WFH was endpoint management (i.e., leveraging [organization's tool] to apply better security policies). What initially motivated this change? After altering the policies within [organization's tool], are you content with this implementation?
	2. Previously, most of these machines were behind the campus firewall, now a lot of them are on external networks. Have you evaluated the exposure due to the remote management systems? For instance, the new [organization's tool] system is opening up hosts quite a bit so that IT staff can connect to these hosts.
	3. With the shifts to remotely manage devices, has accountability been considered? Specifically, who has access to and management privilege on these remote machines? A few management accounts with admin privileges are shared by IT staff.
	4. Another transition I noticed was an increased discussion of data loss prevention techniques and how those can be implemented by the current solutions and services. Was this similarly motivated with endpoint management?

Table 8: Semi-Structured interview questions – We conducted two rounds of semi-structured interviews within our SOC. During the first round, we focused on analysts' perceptions; whereas, the second round revolved around themes obtained through GTM.