A Tale of Three Security Operation Centers

Sathya Chandran Sundaramurthy
Kansas State University
sathya@ksu.edu

Jacob Case
Kansas State University
jacobcase94@ksu.edu

Tony Truong
University of Arizona
vtruong@email.arizona.edu

Loai Zomlot
HP Labs
loai.zomlot@hp.com

Marcel Hoffmann
HP Global Cyber Security
marcel.hoffmann@hp.com

ABSTRACT

Security researchers have been trying to understand functioning of a security operation center (SOC) and how security analysts perform their job. This effort is motivated by the fact that security monitoring and analysis is not just a technical problem. Researchers must take into consideration the human and organizational factors for their research ideas to succeed. Much work towards this direction has been through interviews of security analysts in SOCs. Interviews, however useful, will not be always possible as analysts work in a high-stress and time constrained environment. Thus the understanding of operational challenges through interviews is quite shallow. There is also an issue of trust that limits the amount of information an analyst shares with an interviewing researcher. In our work, we take an anthropological approach to address this problem. Students with Computer Science background get trained in anthropological methods by an anthropologist and are embedded as security analysts in operation centers. Embedded students perform the same job as an analyst and see the operational world from the view point of an analyst. Through reflection on the observations made by the students we gain a holistic perspective of the challenges in operation centers. In this paper we report preliminary results on the ongoing fieldwork at two corporate and a University SOC.

1. INTRODUCTION

There is an ongoing interest among security researchers to understand how a Security Operation Center (SOC) functions. The knowledge of SOC operations is essential to understand how to develop effective policies and tools for SOC operations. SOC operational knowledge is not written down explicitly. The knowledge is transferred among the operational personnel, who establish and manage SOCs, and the analysts who perform security monitoring. As a result security researchers have not been able to study and understand SOC environments as they would in any research. This lack of understanding leads to development of tools that barely meet the operational needs. One of the main barriers for security analysts in communicating with researchers is the lack of trust. Questionnaire and interview methods do not yield enough information exactly for this reason. Analysts feel skeptical about revealing information on the attacks and their investigation techniques to an interviewing researcher who is an outsider. To gain the trust of an analyst, one has to become and perform the job of an analyst.

Security analysts make use of their hunch feeling and intuition during analysis, which drives the investigation in most cases. This knowledge is called "tacit knowledge" and is acquired through years of experience performing the job in an environment. It is highly contextual to the environment where it is generated and is hard for a person to articulate and express [**?**]. For example, a person who can recognize his/her friend's face cannot explain *how* he/she did it. It has been found that to acquire this knowledge one has to be embedded in the environment where the knowledge is generated for a period of time. Explicit knowledge on security operations is available in a number of forms such as academic papers, operating procedures, and tools. But analysts do not just rely on the knowledge that they acquire through training. The acquired knowledge becomes useful only after it is put to practice in operations. This is the difference between *knowledge* and *knowing* and that the process of knowing generates more knowledge, the knowledge generation spiral thus goes on. Tools that are built based on explicit security operational knowledge will fail in practice as they do not take into consideration the iterative knowledge conversion process.

With the above mentioned goals, we take an anthropological approach to address this problem [**?**]. Anthropologists study culture of a community by embedding themselves as members of the community. They become one among the group, perform the same tasks as the group members, and try to understand the underlying culture and behavior of the community. We take a similar approach in our work where we embed students with Computer Science background trained in anthropological methods as security analysts in academic and corporate SOCs. The goal is to see and understand the operational environment from the view point of an analyst. Such techniques have lead to groundbreaking innovations in the past. Charles Leinbach and Ron Sears camped with Recreational Vehicle (RV) campers to find out features of

the RV the campers actually find useful. For example, they found that most campers never use the shower on board (they prefer the high pressure showers offered at the campgrounds that do not waste their limited water supply), and instead use the shower as an extra closet. They made more such discoveries through their fieldwork and thus revolutionized RV design [?]. Genevieve Bell, a cultural anthropologist at Intel studied how people around the world used the technology. Her work [?] along with Paul Dourish explored the social and cultural aspects of ubiquitous computing, significantly shaping the ubiquitous computing research methodologies. Taking an anthropological approach will better inform us of the internal dynamics of SOCs and shape, in fundamental ways, our understanding of the SOC operations and personnel issues.

Towards this approach, we have been conducting fieldwork at three different SOCs and report our findings in this paper. Two SOCs, referred henceforth as Corp1-SOC and Corp2-SOC, belong to two corporations offering Information Technology Services, headquartered in the United States. The third SOC, referred hereafter as U-SOC, is an operational center at a public university in the United States. One student is embedded in each of the SOCs as security analyst for over two months now. The students are trained to perform the operational tasks as analysts. This enables them to experience the SOC from the view point of an analyst. The students document their daily observations in a digital document. The field notes are periodically analyzed with the anthropologist in our team, Prof. Michael Wesch (Kansas State University). Thus the fieldworkers play the dual role, as an analyst in the SOC and as a researcher performing reflection on their experience and observation in the SOC. In this paper we report the results obtained so far from the ongoing fieldwork at the three different SOCs.

2. RELATED WORK

There have been prior work on studying the human, organizational, and technical aspects of operation centers. Werlinger et al. [?, ?, ?, ?] studied different operational challenges through interviews of practitioners from academic and non-academic operational centers. They report on a number a issues like challenges posed by interactions between different stakeholders in operations centers, difficulty in installing and configuring an intrusion detection system, and the importance of tacit knowledge in operations.

Jaferian et al. [?] provide guidelines for designing security management tools through literature survey and interviews of practitioners. Velasquez et al. [?] report on the observations they made about the tools used by administrators to accomplish various system administration tasks. Botta et al. [?] use the concepts of cues (signals that trigger an analyst into action) and norms (adopted standards in IT security practice) to explain distributed cognition in SOC environments through interviews.

A collaborative effort [?] from researchers at Dartmouth College, George Mason University, and Hewlett-Packard supported by the Department of Homeland Security (DHS) is trying to study the various factors that influence the formation and sustaining of CSIRTs. Their research uses interviews and psychological techniques to address the problem.

3. CORPORATION-I (CORP-I) SOC

A graduate student in Computer Science has been working as an L1 analyst at the Corp-I SOC for over two months now. Corporation-I is a multinational firm with work locations all over the world. The SOC in the United States is the only monitoring station for around 350,000 devices on the network. This SOC has been operational for almost a year now and is growing in terms of personnel and infrastructure.

3.1 Teams

A SOC does not function by itself and is supported by a number of teams ensuring successful operations. Following is the description of each of the teams that work alongside Corp-I SOC. Each team is headed by a manager and all the teams are headed by one manager.

3.1.1 Operations (SOC)

The mission of the operations center is the monitoring, analysis, and mitigation of significant information security events to protect the confidentiality, integrity, and availability of the information technology enterprise, and its subscribed partner business units. The operations team is comprised of L1 and L2 analysts headed by an operations manager. Operations is run 24 hours a day and 365 days a year. The operations team is currently comprised of 20 L1 and 2 L2 analysts. Each analyst works 4 days a week and 10 hours a day. There are three shifts each day, early, mid, and night shifts. Shifts are scheduled such that there is at least 2 L1 analyst on each shift.

3.1.2 Engineering

The engineering team is responsible for providing and supporting the SOC with the necessary hardware and software infrastructure. One of the main infrastructure they provide support with is the Security Information and Event Management (SIEM) system. The team also makes sure the sensors that feed data into the SIEM are in good health and also troubleshooting performance issues in the SIEM. Engineering also writes and tunes correlation rules that identify security critical events from raw log data.

3.1.3 Incident Management

The incident management team handles events that are escalated from operations requiring in-depth investigation. For example, taking a memory snapshot of suspicious hosts and conducting memory analysis to understand the malware behavior, investigate compromised accounts *etc.*

3.1.4 Intelligence

The intelligence team provides information on various threats that might affect the organization, such as the following.

- IP addresses that are known sinkholes for malware C&C server communications.
- List of IP addresses that are known to host malicious content.
- Execute malware in sandbox and identify indicators of compromise (IOC).

Besides the in-house intelligence team, the SOC also benefits from open source and paid intelligence services providing similar information.

3.1.5 Red Team

The Red team actively probes for any vulnerabilities in the corporate IT infrastructure. If the team finds a vulnerability that they were able to exploit, the team sends an email to operations containing information on the vulnerability exploited and the type of exploit used. Incidents reported by Red team usually involves a joint call between the Red team, incident management, and operations.

3.2 Software and Tools

Security operations depends on a variety of software applications and tools. In this section we will describe each of the tools and their purpose.

3.2.1 Security Information and Event Management (SIEM)

The SIEM is the most important software application used for operations. The SIEM solution uses a concept of Enterprise Security Manager (ESM) with which the analysts interact to issue queries across various log sources. Data from variety of event sources such as, firewalls, proxy-servers, intrusion prevention systems (IPSes) *etc.* are collected at each source, forwarded to the ESM where it is normalized for storage and analysis. There are two different ESMs in use, the correlation ESM or ESM-C collects the raw events from different sources and applies the various correlation rules. The correlation rules are threat patterns written by the engineering team based on use cases. The correlated events are then forwarded to global ESM or ESM-G. The L1 analysts process alerts from ESM-G. They reach out to ESM-C if they need more information on the rule that triggered the correlated event or if they need more information on infection history for a host or IP address.

3.2.2 SOC Inbox

The SOC has a dedicated email inbox where all emails related to security operations are received and processed. The following types of emails are usually received in the inbox:

- Information on new threats from intelligence team.
- Reports on stolen devices.
- Virus scan and re-image responses.
- Case communications.

An L1 analyst is always on the inbox processing the emails as they come in.

3.2.3 Wiki knowledge base

A wiki is maintained where all the teams–operations, engineering, incident-management, and intelligence–share their information. L1 analysts document information such as new host infection, IP address not found in any black lists, case creation, or ticket filing to locate the owner of infected device. The is the official shiftlog for the analysts. Information on handling various types of events, new analyst onboarding, setting-up analyst work environment, and links to various reading material are also documented in the wiki. The engineering team documents different use cases used for correlation in the ESM, technical details of the different event sources feeding into the SIEM system, information on operational hardware, and other SIEM related technical details. Incident management team documents in detail the procedure they follow for incident response. The intelligence team documents information about on-going threats that may be of significance to the organizations along with the indicators of compromise (IOC). This collaborative nature of the wiki helps the analysts working on the investigation to quickly search and find the relevant information.

3.2.4 Ticketing Systems

A number of ticketing systems are in use with each satisfying a specific purpose.

- Incident tracking system - used by L1 analysts to create and track tickets for security incidents.
- Engineering ticketing system - used by L1 analysts to notify engineering team requesting modification in a correlation rule.
- Networking ticketing system - analysts file tickets here requesting to locate the owner of a host or block of a host (potentially infected and spreading infection) to the networking team.

3.3 SOC Workflow

The ESM uses a concept called *channels* to display the events filtered by a query. The L1 analysts process events from *channel 1* in ESM-G, also called the *Main Channel*. The Main Channel displays the correlated events sent from ESM-C. If it takes more than 3 minutes to process an event from the Main Channel, the event is annotated and moved to *channel 2* in ESM-G, also called the *Events of Interest* channel. Another L1 analyst conducts in-depth investigation on events in this channel. The L1 analyst on the Main Channel is called the *pilot* and the analyst on Events of Interest Channel is called the *co-pilot*. The pilot and co-pilot exchange roles every two hours. The co-pilot also takes care of the SOC inbox if there is no dedicated analyst on the inbox.

3.3.1 Annotation Stages

Annotation is the process of marking the event based on the analysis performed by an analyst. The event arriving into the Main Channel is annotated by default as *queued*. These events are not processed by any analysts so far and are ready for processing. An L1 analyst if he/she wants to analyse an event marks the event as being reviewed (the event is marked with analyst's name so that no other analysts pick the same event for analysis) and conducts the analysis. Based on the analysis he/she will annotate the event with the following:

- Added to List - The event is suspicious but detailed analysis does not lead to anything conclusive. Usually the source or destination IP address is added to a watch list.
- Added to Case - Either this event requires a new case to be created or it can be part of an existing case. In both the situations event details are added to a case and the case number is also mentioned in the annotation comments.
- Content Modification Requested - The event is a false positive and better ways to correlate have to be found.

A rule modification request is sent to engineering and the ticket number is included in the annotation
- Content Addition requested - The analysis of this event results in request to the Engineering team to create a new rule.
- Suppression requested - The pilot finds that the event is a false positive and suppresses any event associated with the IP address or hostname showing up in the channel for a few hours.
- Events of Interest - This event requires more than 3 minutes to analyse and is moved to Events of Interest channel for the co-pilot to analyze.
- No Filter Possible - This event does not fall into any of the categories above, sort of a default category.

For the events annotated as "Events of Interest" the following annotation stages apply.

- Added to List - Same as before
- Added to Case - Same as before
- Content Modification requested - Same as before
- Content Addition requested - Same as before
- Suppression requested - The co-pilot wants to suppress this event for a longer time.
- No Filter Possible - Same as before
- Second Level Assist - This event requires the support of L2 analyst for further investigation.

For events that were annotated as "Second Level Assist" the following annotation stages apply.

- Added to List - The L2 analyst confirms the entries in a list for permanent suppression using this stage.
- Anomaly - The L2 analyst finds that this event is due to a rule change that resulted in a flood of events in the Main Channel that are not actionable.
- No Filter Possible - This event is found to be a false positive and cannot be filtered out.
- Added to Case - The event becomes part of an existing or a new case.

3.3.2 Note on case severity

As we have seen before, one of the annotations for an event can be a case is created. A case usually is created for the following events: (1) incident requires device owner communication to get a virus scan of the host; (2) the compromised device has to be located in the network by network team; (3) a critical incident that requires involvement of incident management team. Each of the cases have a severity attached to them. The severity determines the teams that will be involved for remediation of the incident: (1) Sev-4 - case solved by L1 analysts; (2) Sev-3 - incident needs L2 assistance; (3) Sev-2 - incident management team needs to be involved; (4) Sev-1 - the incident may involve participation of legal authority or cause massive reputation loss to the corporation.

3.3.3 Staging Channel

The Main Channel is supposed to contain at any given time only actionable events. The channel should not be flooded with a lot of false positive events as it might lead the analysts to not noticing the real attacks, the needle in the haystack problem. To prevent this, before an event source is added to the main channel it is tested in a *Staging Channel* in ESM-C. Analysts at the L2-level, sometimes L1 analysts, analyze events in this channel, identify a possible analysis technique and measure the true and false positive rate of the events (qualitatively). Sometimes a rule modification request will be sent to Engineering to either include more information in the alert or fine-tune performance by modifying the rule. After sufficient analysis and determining that the alerts from the rule are actionable, the event source will be migrated to the Main Channel. It is important to notice here that the emphasis is more on the event being actionable rather than the sensor being accurate, as we all know no sensor is accurate enough for perfect intrusion detection.

3.4 Rationale behind the workflow

The SOC believes that the human security analyst is the most critical element in operations. This reflects on how the analysts are asked to perform their job. The SIEM solution used in the SOC is preferred mainly because it provides features to build a workflow with enough human intervention. The events in the Main Channel are generated based on the correlation rules in ESM-C and it is the job of the analysts to process each correlated event and classify as either true or false positive. The SOC does not believe in a tool prioritizing the events and showing only those alerts above certain thresholds. They believe that a human being has to make the decision when analyzing each security incident, from their experience. The experts who are building this SOC have worked with other SIEM solutions in the past that prioritize and show events based on thresholds. Later they stopped using that product as it did not allow sufficient analyst intervention in the workflow.

3.5 Description of two real security incidents

In this section we describe two security incidents that our student intern worked on as an L1 analyst. The two incidents reiterate the following: (1) security monitoring does not start and end with a single sensor alert; (2) incident response participation of multiple teams; (3) contextual knowledge and hunch feelings help move investigations to the next step;

3.5.1 Incident-1

The Red team sent an email to the SOC alerting that one of Corp-I's web server is vulnerable to SQL injection. They also included in the email what type of attacks they were able to perform and the IP address of the web server. The SOC analysts used the ESM to look for traffic to and from the vulnerable web server. This was due to the fact that if the Red team was able to compromise a system it should be assumed that an attacker on the internet would be able to do the same. The analysts found that at least one other IP address, besides the Red team events, that was launching SQL injection attacks against the same server. The SOC reported the IP to incident management. Meanwhile, incident management was on call with the Red team to get more details on the attack. The programmer who wrote the code for the web server was also contacted to get details of the source code. A remediation plan is on progress to secure the web application from such vulnerabilities in the future.

3.5.2 Incident-2

An analyst was monitoring the Main Channel and picked an alert from an Intrusion Prevention System (IPS). The alert said that a file exploiting a vulnerability in Java clients was downloaded. The IPS found that a server was hosting the vulnerable file that then got downloaded by a client, potentially a Java Client. The analyst first found out that the server in question was running a web server as the source port in the alert was 80. The analyst navigated to that website using a browser and noticed that the server was hosting a well known Linux terminal emulation client for Windows. The page by itself looked odd as there was just one hyperlink that said it was a terminal emulation client and the file was linked off it. The analyst then downloaded the file and uploaded to malware scanning websites. The scans pointed out that the file was classified as a malware by a majority of the scanners. This increased the confidence of the analyst that the host was compromised. The incident got reported to the operations manager who then asked the analyst to analyze the logs for all hosts in the subnet. Hosts in this particular type of subnet have been found to be compromised as a whole in the past (here we see the hunch feeling and contextual knowledge in action). After searching through the logs in the ESM the analyst found that a few other hosts in that subnet were indeed sending and receiving suspicious traffic. A case then was created with severity-2 and incident management is performing a root cause analysis on the possible compromise.

3.6 Analyst Training

There is a well defined training procedure followed for onboarding newly hired L1 analysts. First day is spent on setting up the laptop, security analysis tools, necessary virtual machines, and requesting access to a number of portals. These portals contain information that help the analysts during their investigations. From the second day onwards, the analyst goes through a self-study training programme. The training consists of reading material followed by tasks on a number of topics, such as UNIX commands, boolean logic, network protocols, Wireshark, Nmap, Snort *etc.,* Once the self-training programme is completed, the analyst is asked to shadow the experienced L1 analysts. The analyst watches the experienced analysts as they process alerts from the ESM and asks questions during the process. After a few weeks of shadowing, the analyst is shadowed by experienced L1 analysts. This double shadowing routine ensures that the analyst learns and follows the right procedures. After the shadowing process, the analyst is ready to go on shifts. The entire process takes at least 2 months.

4. CORPORATION-II (CORP-II) SOC

An undergraduate student in Management Information Systems has been working as a security analyst and conducting fieldwork at corporate SOC in the United States. We describe the operations of Corp-II SOC based on the observations made by the student analyst for the past two months. The Corporation SOC Incident Respond (IR) team partners with internal and external service organizations to provide first level response and validation of information security threats with minimal impact to business operations or performance. The SOC is distributed globally to provide 24x7x365 incident response services. The SOC's mission is to restore and maintain normal production and business continuity, improve security and survivability against future incidents, deter and prevent future incidents by acts of investigation and prosecution, and educate analysts through acts of intelligence or counter-intelligence action.

4.1 Teams and organization

Corp-II SOC has team members in three sites located in Asia/Pacific, Europe and the United States. The goals of the SOC teams include intelligent coordination of incident response resources, accurate and timely identification of information security risks, and reduced recidivism through strategic risk mitigation. A follow-the-sun model is adopted by the SOC: US SOC covers 1pm-1am (UTC); Asia/Pacific SOC covers 12:30am-1pm (UTC). Thirty minutes overlap is added at the end of the US shift to allow for transfer/delegation of matters to the Asia/Pacific team. Transferring all open/in-progress cases towards closure is the responsibility of the functional SOC group that is operating during the coverage periods defined above. All three SOCs have tasks and projects that are specific to them, besides the usual operational tasks. The Asia/Pacific team has a strong emphasis on ticket work and the other two SOCs focus more on projects that can improve the SOC efficiency. Currently the US SOC team is comprised of nine members and each member performs several functions and have various specialized skills. There are two managers that supervise the global team. One of them focuses on incident response and the other on threat intelligence.

4.2 Software and Tools

The SOC has invested a significant amount of resources into a log aggregation tool, with the hope of improving the workflow process. The aggregator can collect and index almost any data from the host machine and store it to a repository. Once the data is available in the repository, an analyst can connect to the aggregator via web browser and run searches across that data. The analyst can also make reports or graphs based on the data, from within the browser. Both managers make great use of these features to make reports about the team and the ticketing system performance. The aggregator is also heavily used by analysts working on tickets. The SOC has installed a commercial intrusion detection system (IDS) that monitors for internet bound traffic at the corporation's major egress points. Alerts from the IDS devices are delivered to the log aggregator and from where they are used for further analysis. The workflow system automatically creates tickets for alerts from the IDS so an analyst can do additional examination. The corporation mandates that every host has the company approved antivirus installed. Whenever a AV client identifies a threat, it automatically reports the threat to workflow system so a ticket can be created for that threat. Tickets that are created by AV clients are assigned a predefined name and tickets that are created for events from the IDS are named tier 1. A ticket should be escalated to the tier 2 queue in the event that a direct threat is identified, blatant misuse is identified (intentional/repeated violation of policy or blatant inappropriate use), and the scope of the detection involves HVT, critical infrastructure, or Crown Jewel data. tier 1 and AV tickets are handled by Managed Security Services Provider partner. The US and Asia/Pacific SOCs handle the tier 2 tickets.

4.3 Analyst Training

On the first day of work, new members go through every item on the onboarding list located on a wiki. This process guides new members through processes to acquire tools and authorizations that are needed to perform Incident Response tasks. The main training approach for new analysts is to shadow a senior analyst and learn about the processes and procedures from him. After a few days, the new analysts are left on their own to work on simple tickets and they can always ask for assistance from the senior analyst. As the new analysts get more comfortable with the workflow process and security tools, they are challenged with tickets with higher severity that require additional analysis. New analysts are trained until the senior analyst and SOC manager agree that additional training is unnecessary.

4.4 SOC Workflow

The SOC follows a workflow built around an incident management system. New events/alerts are processed First-In, First-Out (FIFO) for validation. Priority is given to any alert that indicates that a direct threat agent should be prioritized over others. Common detection sources that are known for yielding alerts of this nature are but not limited to Mandiant Incident Response (MIR) Sweep, industry intelligence, ePolicy Orchestrator detections on a server, suspicious email received by a High Value Target (HVT) *etc.*. Analysts can access the workflow system through a web browser to open and work on tickets. Within each ticket, there are multiple automations that pull resources about the incident and display it in the ticket for the analyst. Alerts or Incidents can be closed through automated processes or by analysts. There are currently some automatic processes that close out tickets with low severity in the system, created by automation, not owned by an analyst, and are older than seven days.

5. UNIVERSITY SOC

An undergraduate student in Computer Science has been working as an analyst at the SOC for over two months now. For Anthropological training, the student has been and is taking Anthropology classes, as well as working with the Anthropology professor on the research team. The fieldwork site is a Public University in the United States and the U-SOC is the only security monitoring centre for the whole campus. The student has worked on several projects, including writing tools in Python and documenting procedures. Observations were done by taking notes on regular events, as well as interviewing employees when available. At any given time there will be 50,000 devices online in the campus. We now describe the observations we made on various aspects of U-SOC through the fieldwork process.

5.1 Teams and organization

The U-SOC is part of a layered team structure that constitute the security operations personnel. There are three layers of support and in the following sections we describe each team along with their responsibilities and the layer they fall into. The layers of support are more focused around a group of responsibilities, rather than having higher level groups try to solve problems that lower level groups look at but can't solve. Because of this, the levels themselves are not important, because they have mostly independent roles any ways.

5.1.1 Operations

Operations is one of the teams that constitute the layer 3 support. The operations is a team of 4 analysts headed by a Chief Information Security Officer (CISO). Most analysts specialize at certain tasks, yet there is a lot of overlap. All analysts handle incidents and perform tasks of other analysts occasionally. There is a goal to cross-train all analysts across various operational tasks, but progress on this goal has been slow due to being stretched thin for time, thus not being able to make any available for training. The analysts primarily perform the following: Analysts A1 - forensics and sysadmin; Analyst A2 - firewall management, VPN, and network security architecture; Analyst A3 - firewall management and payment card industry (PCI) compliance; Analyst A4 - PCI compliance as well as acts as a manager under the CISO. The sysadmin work that analyst A1 does is on security appliances that the U-SOC uses. In previous years analyst A1 wasn't required to perform sysadmin work, that was left up to other groups that focus more on that type of work. As other groups became too busy to maintain the security appliances, they became the U-SOCs responsibility, thus causing more time being spent maintaining them rather than using them for incidents. The U-SOC no long has time to do forensics and investigations like it used to.

5.1.2 Infrastructure Maintenance

(**** Jacobs comment: I almost think that either datacenter maintenance or system administration might be a better title? ****) This is a tier 3 office in charge of University data center, security hardening of hosts, and maintenance of campus servers. The office also provide campus wide services such as email, Active Directory, and DNS as well as hardware and software monitoring of enterprise servers and software.

5.1.3 Networking

This is another tier 3 office in charge of networking on the campus. They set up wireless access points and controllers, handle routing, configure VLANs, allocate address blocks, and sometimes block hosts from the network.

5.1.4 Miscellaneous Operations

This is a tier 2 office in formation and their responsibilities are still being determined. Currently they deal with phishing scams and anti-virus management. In the near future, they will also sign personal certificate requests and manage VPN groups.

5.1.5 Help Desk

Help Desk forms the tier 1 support. This is the office students, staff, and faculty visit or call to get help on computer and technology issues. They also function as the face of IT at the U-SOC so they have a heavy focus around customer service.

5.2 Software and Tools

The U-SOC team uses a number of tools in their day to day operations, some of which are also used by other support groups. The software applications used are subject to change frequently, and the features of many of the applications themselves seem to be volatile. This has been an issue

in documenting procedures that use many of these applications because it has to be updated frequently as the tools change. This is partly due to the fact that the operations team is still in procure mode and working on identifying the best set of tools that will serve their needs. Although the tools used might change, the tools will fall into the following categories nevertheless. Following is a description of the current tools used in daily operations.

5.2.1 Log Management

There is a commercial SIEM solution in place that collects and aggregates logs from a number of networking equipments. Most logs are forwarded to the SIEM via Syslog, though it has the capability to understand a number of input formats. The retention period for the logs is configured based on various data classifications and there is an automated data compression process for efficient storage. For example, logs from devices that are within PCI scope are retained for at least 1 year, while logs from devices not in PCI scope may be purged after 3 months. The SIEM manager also provides access control to logs based on enterprise groups so that groups can be provided access to only to those logs that are from equipments their group manages. The SIEM solution also has a query interface which analysts can use to issue queries on the logs to identify potential intrusion attempts. This feature is facilitated by a well defined query language and a powerful regular expression support. Currently the U-SOC is investing other SIEM solutions from various other vendors because the currently solution cannot hand the log volume. The current solution can only handle about 5000 logs per second, while we need to be able to handle at least 4 times that much. We have also been asked to investigate open source solutions, which at this point seems promising, but needs more work. One downside of open source SIEM solutions is that they are not drop in solutions. Most of them seem to require at least a simple pipeline composed of a program to receive and parse logs, store logs in a database, and a web interface. As requirements grow, this may include database sharding, distributed log pipeline, and branches in the pipeline depending on the log type.

5.2.2 Ticketing System

A ticketing system is used to create and manage incidents across different teams. There are four categories of tickets created in the system: (1) incident - an anomaly that needs to be solved once, (2) problem - any incident occurs frequently in a short amount of time, (3) change management - requests to review changes for compliance requirements before infrastructure changes are made, (4) communication requests - request to add a firewall exception to allow inbound communication to a specific server on specific port for specific period of time. The ticketing system also enables calculation of metrics, such as time spent on a ticket. The system also supports groups which can be used to enable access control and handle ticket escalation within a group. While the tool is very customizable, many of its features have yet to be understood and activated, even those that are wanted by the U-SOC. Time spent on tickets is recorded as a method to determine where time resources are being used.

5.2.3 Security Appliances

The U-SOC also manages several other security appliances on campus, such as the Network Access Control (NAC). The NAC is used ensure that students using resident hall networks on the campus meet compliance requirements. Requirements include running the University approved antivirus, a patched and up-to-date OS, and running only patched installed programs that could otherwise be exploited. The appliances allow the SOC to block users that are running peer to peer and (P2P) other restricted applications. Finally, all traffic to the internet from the campus network is inspected by a packet inspection appliance. The packet inspection appliance inspects and blocks restricted protocols, such as P2P. Since the NAC is only used on resident hall networks due to cost and scaling restrictions, the WiFi and department networks still need enforcement.

5.3 Analyst Training

Analysts are trained by a combination of several strategies, depending on the prior experience. The SOC strives to maintain good documentation of all information related to operations as it helps in the analyst onboarding process. New analysts also shadow more experienced analysts and assist them when they can, such as teaming up to change a huge set of firewall rules together. Analysts are encouraged to learn through self-study and use the online resources to get the necessary technical information. There is a plan for a new promotion pathway that would require obtaining certifications to be eligible for the next promotion, though it has not been finalized. Some things that are not considered effective include sitting down and watching someone else work while only taking notes. Performing different functions in the SOC can be long and sometimes mind numbing, so without engagement it can be easy to lose attention and interest.

5.4 SOC Workflow

At the beginning of the week, there is a stand-up meeting to discuss project assignments for the rest of the week, thereby estimating project time. Much of the remaining time is used for operations such as processing incident tickets. If a system administrator knows the office responsible for an incident, a ticket is created and assigned to that office. In rest of the cases, tickets go through an escalation process. If someone has a computer or network problem, they may call the Help Desk, the tier 1 support. The issue either gets resolved at the Help Desk or gets escalated to tier 2 or 3 support personnel. Incident tickets are processed by the analyst who has the necessary expertise to do so. For example, firewall requests will be processed by analyst A2 while tickets for malware infected hosts are processed by analyst A1. On processing the ticket, analysts annotate the ticket with sufficient information so that there is enough information for someone interested in understanding the activity log for that incident. Similar to the Corp-II SOC, the ticketing system is the starting point for any security operations.

5.5 U-SOC Observations

5.5.1 Time reporting

When investigating how the analysts feel about time reporting on tickets, the results were actually slightly positive. The reason one analyst gave was that, because they are so short on time, if someone in a higher position wanted to add or cut

a project or get an idea what funds are being used on, the analysts have something concrete to present to aid in making the decision, as well as show where funding resources are needed since it's currently not clear where the best place to spend money is. My impressions of a few analysts feelings are that it's a good way to CYA (cover your ass). That being said, other analysts did seem a little uneasy, and I believe that deserves more investigation. While the assumption a lot of times is that recording time on tickets will be used to fire bad employees or turn the system into a game, I don't get the impression that's why some analysts don't like it, especially since all the analysts seem to be doing a quality job, though I haven't investigated that enough.

5.5.2 *Reflections*

There have been several hurdles in the research thus far that need to be overcome in the U-SOC. It's difficult to get a broad perspective on what goes on in the U-SOC because field researches tend to fall into an analyst position. This is good when you want to analyse what it's like to be a single analyst interacting with others, but it's difficult when you want to take a step back for a bigger view of operations or observe individual employees. The reason this happens is the U-SOC is stretched so thin for time and resources, they can't afford to have researchers possible getting in their way by shadowing or asking questions, especially when the researchers could be working on something independently. Additionally, field researchers thus far are not as permanent as analysts. From the analyst's perspective, why should they spend their time to train someone that will not be around the SOC for a long duration of time. Additionally, we may not be viewed at the same level as other analysts since we are just students to them, much like other student employees, even though we are really there for research. There may not be a lot that can be done about this, but we can still leverage the positions that we have. At this point it's difficult to come up with a concrete analysis, but there are a few important observations. For one, the analysts prefer to pay for commercial software if they can because they get support. That has actually been one of the biggest hurdles to developing tools and has caused tool development in the U-SOC to get shut down entirely for a while. Unlike some larger SOCs, the U-SOC is too small to hire their own full time developer, and the University group that does development for the university is too busy working on other projects, such as the online learning platform. For me, that raises the question if paying for their own developer is more cost effective than shelling out hundreds of thousands of dollars for solutions that could be done almost as well with open source tools. Than of course raises a few questions on what happens when the developer leaves and they need to hire a new one to take over: Will the new developer understand the existing code base quickly enough (issues us field researchers have actually ran into) and how long will the new developer take to understand what the tools are trying to accomplish. I'm sure there are more questions, but those can be left up to further investigation

6. REFLECTIONS ON THE FIELDWORK

Reflection is an important process in understanding the observations made during the fieldwork. With two months' worth fieldwork data from three different SOCs we make a number of observations through the reflection process.

Each SOC is structured differently. The Corp-I SOC has two layers of analysts and incident management forming the third top layer while in Corp-II SOCs there is no such hierarchy. All the analysts in Corp-II are in the same job role but process events based on their experience. For example, an experienced analyst will process an event of higher severity compared to an analyst of lesser experience. Whereas in Corp-I SOC all the events are first processed by L1 analysts and goes through the escalation chain: first to L2s and if needed incident management depending on the severity and complexity of the event. The analysts in both Corp-I and Corp-II SOCs perform nothing other than security event analysis. The U-SOC is very different from this aspect. The analysts not only multitask, performing IT management tasks like handling firewall requests, but also indulge in cross-training where each analyst gets comfortable performing tasks of other analysts. The reason for this multitasking is due to the small size of the U-SOC team, which has only four analysts in its team. This brings up an interesting question to answer, *what are the factors that affect the SOC structure as we observe in three different SOCs?*

From our fieldwork so far we also observe that each of the SOCs follow a very different workflow. For example, Corp-I SOC follows a hierarchical workflow and every incident starts with an alert in the ESM. Corp-II SOC on the other hand works differently wherein the main interface for the analysts is the ticketing system. Through conversation with the SOC personnel at the field work site (Corp-I) we found out that the type of tools used in the SOC directly influences the workflow adopted. While the corporation SOCs perform continuous monitoring throughout the year, the U-SOC operates only five days a week. Operational workflow must take into consideration the operating mode of the SOC as this directly affects staffing and shift scheduling. This raises another question, *can we develop an operational workflow that is agnostic to the tools used in a SOC?*. There has been some effort by CMU SEI [**?**] on modeling SOC workflow independent of tools and they turned out to be too abstract to be actually used in practice. We found that SOCs follow the general known steps for incident response, which are detection, triage, respond, and follow-up. But there are more informality and details involved in their day-to-day processes. Incident analysis is highly dependent on the team's contextual-knowledge about the place (the client's network and machines) and the time (the current activities on the client's networks). This knowledge is embedded in the organization's team and its clients, and it is very decisive in incidents' investigation processes. Therefore, it is specific and can not be generalized to other organizations.

The SOCs do have another challenge, measuring analyst productivity. We observed that one of the SOCs is trying to measure the amount of time an analyst spends on an incident as an indicator of productivity. This directly relates to the number of incidents processed by an analyst at the end of the day. One of the pitfalls of using incidents processed as a metric is the variable amount of time it takes to process each incident. Some incidents take much more time to analyze compared with others due to the type of threats they represent. An analyst processing such a complex event will not feel that his/her effort is justified. Our fieldworker at Corp-I proposed to the manager of the SOC to consider

finding interesting events to analyze as a metric of productivity, rather than processing n events a day. The manager agreed that it might be a metric worth experimenting. We thus observe through our fieldwork that measuring analysts' efficiency is still a problem waiting to be addressed.

Some of the other challenges we note are maintaining communication between the night shift analysts and the rest of the team. Special effort must be taken by the SOC to ensure that the night shift analysts do not feel left behind and isolated. For example, in Corp-I SOC analysts rotate shifts every 2 months. An analyst is on night shift for two months and he/she will be shifted to early or mid shift for the next two months. Also, SOCs need to make sure the analysts feel motivated and excited about their job everyday, especially the L1s. Looking at an ESM console for 10 hours a day can be extremely demanding for an analyst. One of the ways analysts are kept motivated is through career progression. An L1 analyst performing well in his/her job after a period of two years will be eligible for recruitment into incident management or the engineering team. This is being followed at Corp-I SOC currently.

7. CONCLUSIONS AND FUTURE WORK

In this work we take an anthropological approach to understand how SOCs operate and how security analysts do their job. Three students with Computer Science background trained in participation observation methods by an anthropologist have been embedded as analysts in a University and two Corporate SOCs. We make a number of observations on the people, process, and technology aspects in three different SOCs. Reflection on the observations made thus far sheds some light on challenges underlying operational environments. In this paper we make observations on operational tools/teams, workflow, and on how teams come together in solving security incidents. The fieldwork is ongoing and we hope to report deeper insights in the final version of the paper.

8. ACKNOWLEDGEMENTS

This material is based on research sponsored by the Department of Homeland Security (DHS) Science and Technology Directorate, Homeland Security Advanced Research Projects Agency, Cyber Security Division (DHS S&T/HSARPA/CSD), BAA 11-02 and the Air Force Research Laboratory, Information Directorate under agreement number FA8750-12-2-0258. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon.

This research is supported by the National Science Foundation under Grant No. 1314925. 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 National Science Foundation.

We thank Prof. Xinming Ou and Prof. Michael Wesch (our team anthropologist) at Kansas State University in helping conduct the fieldwork at the University SOC. We also thank Sandeep Bhatt and Bill Horne of HP Labs for supporting and providing feedback on the fieldwork at the corporation SOCs.