David Murillo Santiago

9 Dec 2024

IS-4943-001

Professor Kaufman

Introduction

As organizations continue to integrate more technology into their operations, their exposure to cyber threats increases. To mitigate these risks, Security Operations Centers (SOCs) serve as the first line of defense against digital threats. SOCs maintain the security posture of organizations by continuously monitoring, documenting, and responding to alerts, ensuring the protection of confidentiality, integrity, and availability while preventing security incidents and breaches.

Core Components of an Effective SOC

A Security Operations Center (SOC) is the core of an organization's cybersecurity infrastructure. The modern SOC plays a critical role in safeguarding assets, systems, and data from increasingly sophisticated cyber threats. To effectively fulfill this role, a SOC must integrate people, processes, and technologies to rapidly detect, understand, and mitigate risks. As mentioned in 11 Strategies of A World-Class Cybersecurity Operations Center, "The key to effective security operations is having the people, process, and technology to enable the SOC to detect, understand, and respond to the adversary rapidly, both proactively and reactively" (Knerler, 2022). One example of this would be through the implementation of an Endpoint Detection and Response (EDR) tool. According to Cisco's article *What Is Endpoint Detection and Response (EDR/MEDR)?*, an EDR is a "system that helps security teams detect, investigate, and respond to cyberattacks on endpoints like laptops, desktops, and mobile devices" (Cisco, 2024). This approach strengthens the security posture of an organization by enhancing attack preparedness through preventative and reactive measures. Alerts generated by the endpoint tool allow SOC analysts to more easily identify threats within their environment. Other ways which SOCs can improve their preparedness is by leveraging tools such as SIEM systems, assessing vulnerabilities, and creating playbooks to facilitate threat response, thereby ensuring that threats are addressed swiftly and comprehensively.

The functions within a SOC are diverse and cover everything from alert monitoring to threat hunting. According to *Splunk's 10 Essential Capabilities of a Modern SOC*, these capabilities include "ingest, detect, predict, automate, orchestrate, recommend, investigate, collaborate, manage cases, and report" (Splunk, 2024). Each of these functions supports the SOC's mission of minimizing the time between detection and response. Minimizing time between tasks is key as efficiency is required in effective SOCs. The need for efficiency is driven by the fact that events grow in severity over time. Therefore, a SOC must manage alerts in a timely manner to minimize risk. The urgency of time in the SOC is revealed through Splunk's quote: "The ability to predict a security event allows the SOC to proactively escalate the incident to a human" (Splunk, 2024). In this statement, Splunk highlights the critical nature of the detection and response steps, emphasizing the necessity of predicting an event. This is because predicting an event minimizes the time available for an attack to escalate. This predictive capability enhances the SOC's readiness and improves overall efficiency.

SOC teams make an effort to streamline their work in order to boost their productivity. One way this is achieved is through automation. Automation plays an essential role in modern SOCs by reducing the time spent on repetitive tasks. As highlighted by Matthew Shutock in *Security Operations Centers: A Holistic View on Problems and Solutions*, "Processes are the standardized workflows that SOCs and incident response teams follow to investigate and remediate alerts, which should be documented in the SOC's procedures" (Shutock, 2022). These processes often take the form of playbooks that help analysts follow consistent and repeatable steps when responding to incidents. Playbooks allow SOC team members to work through alerts thoroughly and quickly. Effective playbooks detail how to handle specific alerts by documenting which resources to utilize, where to look, and how to respond. By following a playbook, teams reduce time spent strategizing on how to address or remediate an alert, thereby decreasing the time spent on repetitive alerts and allowing more time for unusual alerts that appear out of the ordinary. Automation is especially helpful to SOCs because, when working alerts, time is of the essence. Once again, the urgency behind the SOC is the fact that attacks grow in severity when they are allowed to persist in time. Additionally, because thousands of alerts are generated daily, if a SOC team is inefficient, they will fall behind and may allow critical alerts to escalate in severity. Therefore, automation is essential not only for efficiency, but for effective security. Despite the value that they bring to the SOC, automation should not replace human resources. Instead, automation should complement human analysis. As Knerler puts it, “automation assists, but does not fully replace, the judgment of advanced human analysts” (Knerler, 2022). Balancing automation and human judgment is crucial because alerts can be wrong. Most of the alerts received by the tools used in the SOC are benign. Without the use of human judgment, the organization would dedicate an unreasonable amount of resources to the remediation of systems that do not require it. Therefore, SOC teams should use automation as effectively as possible to reduce the time spent on repetitive tasks, but should maintain a knowledgeable staff who can confirm the validity of the tools.

Collaboration is another cornerstone of a successful SOC. Effective communication between SOC teams, other departments, and even external partners ensures a cohesive defense strategy. As noted by Splunk, “Security is a team sport that requires coordination, communication, and collaboration” (Splunk, 2024). This collaboration enables the sharing of critical, time-sensitive information and enhances the overall security posture. As mentioned previously, speed is important when working in the SOC, and collaboration is a significant way to improve speed. However, even if collaboration did not impact speed, collaboration is still required to maintain an effective SOC. For example, if a high-severity alert were to be detected, all team members would be expected to work on said alert. In doing so, the team would look across different tools and systems to gain a better understanding of the situation. Collaboration is important during this process for two reasons: it reduces redundancy in the investigative process and helps the team be more informed about the situation. If all members were to spend time looking over the same logs from the same source, time would be wasted, and the alert may grow in severity. Therefore, SOC teams should be encouraged to collaborate during and after their investigation process and share their findings to raise the team's awareness of the situation.

A SOC functions as the first line of defense for an organization’s cybersecurity infrastructure. Therefore, the daily tasks performed by SOC analysts are designed to ensure the rapid detection, investigation, and mitigation of threats. These tasks typically include monitoring alerts, conducting threat analysis, responding to incidents, and documenting findings. As stated in *11 Strategies of A World-Class Cybersecurity Operations Center*, effective SOC operations rely on “the people, process, and technology to enable the SOC to detect, understand, and respond to the adversary rapidly, both proactively and reactively” (Knerler, 2022). One core daily task is continuous alert monitoring. As described by Matthew Shutock, Tier 1 analysts are responsible for “continuous monitoring, triage, and remediation of incoming alerts” (Shutock, 2022). By constantly monitoring and responding to alerts, Tier 1 analysts ensure that potential threats are identified promptly. Becoming familiar with the types of alerts generated by typical network operations is crucial for detecting anomalies. Anomalies reveal abnormal, potentially malicious traffic. Therefore, a SOC’s ability to detect anomalies in its organizational traffic is crucial because it serves as a spotlight for potentially malicious activity. This is further proven through Splunk’s description of their UBA tool. According to Splunk's *10 Essential Capabilities of a Modern SOC*, “Splunk User Behavior Analytics (UBA) is a machine learning-powered solution that finds unknown threats and anomalous behavior across users, endpoint devices, and applications” (Splunk, 2024). As demonstrated through their use by SIEM tool creators like Splunk, anomalies are important to detect in order to prevent malicious activity.

Another critical task of the SOC is documentation. Documentation serves as the backbone of effective communication, knowledge transfer, and efficient threat mitigation. Proper documentation ensures that current and future analysts can quickly access essential information when encountering similar alerts. This process helps determine whether an alert is benign or malicious and outlines the appropriate steps to take. Thorough yet concise documentation improves efficiency by reducing the need for repeated investigations and minimizing delays caused by ambiguity. As noted by Splunk, "Having the right reporting tools helps inform on what's performing, so security teams can accurately measure where they are and where they need to go" (Splunk, 2024). New members of SOC teams can look back on previous documentation to more quickly understand how they should proceed with an alert. A key aspect of effective documentation is striking a balance between detail and conciseness. Each report should include a clear alert description, what triggered the alert, and why it is or is not suspicious. For example, an alert might state, "Impossible travel detected for Professor Bill Nye." The subsequent investigation steps should be thorough and should analyze artifacts such as login timestamps, user behavior patterns, and IP addresses. In contrast, the findings section should provide a concise explanation of what occurred during the alert, who was involved, what systems, and any information that can serve to contextualize the alert. Clarity is especially important when working with non-technical parties outside the SOC. Once again, if Professor Bill Nye were to generate an impossible travel alert, it would be crucial to communicate the situation to him in simple, understandable terms. Overly technical jargon may confuse the professor, leading to delays caused by back-and-forth emails. Instead, a concise explanation like, "We detected a login from a foreign location. Was this you, or do you use a VPN?" ensures the professor understands the situation and can provide a timely response. As noted by Alwashali in *A Tour Inside a SOC Analyst Mind*, "The ability to accurately write about the events timeline is crucial. Analysts sometimes make the mistake of writing content to prove their sophistication, where it should have been easy-to-follow, actionable instructions" (Alwashali, 2024). Poor documentation can have serious consequences that can lead to inefficiency and miscommunication. Incomplete or unclear documentation forces analysts to repeat investigations or miss critical details, wasting time and delaying response. Therefore, effective documentation eliminates ambiguity, streamlines processes, and ensures that everyone understands the situation and next steps.

A Security Operations Center must be structured with the right tools and processes to ensure effective threat detection, analysis, and mitigation. At the core of SOC operations are Security Information and Event Management (SIEM) systems. These systems aggregate data from various sources, such as endpoints, servers, and network devices, to provide a centralized view of the organization's security landscape. SIEM solutions facilitate real-time monitoring and threat detection by applying correlation rules that link events together in order to identify potential security incidents. For example, a SIEM can detect an unusual login pattern across multiple devices and flag it as a potential breach. This enables the SOC team to respond quickly. As described by Knerler, a well-run SOC must "detect, understand, and respond to the adversary rapidly, both proactively and reactively" (Knerler, 2022).

Therefore, SIEMs create effective SOCs by allowing analysts to connect alerts generated across various platforms. This allows SOC teams to quickly investigate flagged incidents and take immediate action to mitigate any potential threats. To supplement SIEM systems, modern SOCs also deploy User and Entity Behavior Analytics (UEBA) tools. These tools leverage machine learning to analyze patterns of behavior among users and devices. By establishing a baseline of normal activity, UEBA tools can detect deviations that may indicate malicious behavior. These tools allow SOC analysts to uncover subtle threats that traditional detection methods might miss. For example, unusual login times or access to restricted resources can be flagged for further investigation. By integrating UEBA with SIEM, SOCs improve their ability to identify both known and unknown threats, thereby strengthening the organization's security posture.

Another essential component of a well-run SOC is orchestration, which coordinates workflows across multiple security tools. For instance, when an alert is triggered, an orchestration platform can automatically gather contextual data from different systems, quarantine a suspicious endpoint, and update the incident response ticket. As described in *The 10 Essential Capabilities of a Best-of-Breed SOAR*, orchestration “is defined as the machine-based coordination of complex workflows across different security tools” (Splunk, 2024). For example, when a SIEM detects a potential threat, orchestration can automate the response by triggering actions like blocking an IP address or isolating affected systems. This seamless integration of tools ensures that all systems work together cohesively and enhances response speed.

Risk-based alert prioritization is another key recommendation for running an efficient SOC. As mentioned previously, alerts may grow in severity as time progresses. Therefore, it is important to understand that not all alerts pose the same level of threat, and addressing the most critical incidents first reduces potential damage. According to Splunk, 'Intuitive security tools aid an analyst’s human ability and help them prioritize what needs to be investigated,' meaning that by using these tools, analysts can focus on high-priority threats and respond more effectively to minimize risk. Prioritization can be achieved through automated risk scoring, where alerts are ranked based on factors like the sensitivity of affected systems and the potential impact of the threat. This practice helps analysts focus their attention on the most pressing issues. Therefore, by addressing high-risk alerts first, SOC teams can prevent these issues from escalating in severity.

Common Pitfalls in SOC Operations

Despite the role that SOCs play in safeguarding organizations, they are often hindered by flaws that reduce efficiency and effectiveness. These flaws arise from issues in alert selection, analysis, communication, and decision-making. Recognizing these weaknesses is essential for improving SOC operations and mitigating risks. One major flaw in SOCs is the tendency of analysts to prioritize alerts based on familiarity rather than risk. Analysts may gravitate toward alerts they feel comfortable handling, rather than those that pose the greatest threat. As Alwashali notes in *A Tour Inside a SOC Analyst Mind*, “Alerts should be selected based on risk, but analysts often choose alerts based on what they think they know how to analyze” (Alwashali, 2024). This misallocation of resources can lead to critical threats being overlooked while low-risk issues receive unnecessary attention. To combat this, a tasking list should be created. Tasking lists detail which alerts should be prioritized based on the organization’s current security needs. Instead of allowing analysts to choose alerts at random, tasking lists provide an added layer of alert priority by specifying exactly which alerts should be worked on first. Therefore, no type of alert is left out, as the tasking list guides analysts in selecting alerts appropriately.

Another significant issue is the tendency to generalize conclusions when multiple alerts fire simultaneously. Analysts may quickly assess a few and assume the same conclusion applies to all. According to Alwashali, “When multiple alerts coincidentally fire at the same time, analysts may quickly generalize their conclusions about all alerts by only checking one or two” (Alwashali, 2024). This bias can lead to missed threats, which can put the organization at risk. For example, if multiple alerts are triggered for an updater running with elevated privileges, an analyst might quickly assume it's part of a routine software update process. However, this generalization could overlook the possibility of malware masquerading as an updater, attempting to gain unauthorized access through exploiting elevated privileges. Therefore, it is important for SOC analysts to treat each alert as though it is a compromise and trust only the data they uncover during their investigation. This would help combat the bias of simultaneous alerts and reduce the likelihood of missed threats.

SOC analysts must also embrace continuous learning and be encouraged to take on alerts they are unfamiliar with. Sometimes, analysts make the mistake of avoiding complex alerts because they fear the complexity of investigating them. As Alwashali points out, “Analysts may avoid selecting alerts for PowerShell obfuscation because they fear that it may be difficult to decode and analyze” (Alwashali, 2024). Analysts' reluctance to investigate unfamiliar alerts can create gaps in threat detection and leave vulnerabilities unaddressed. Therefore, SOC teams must encourage continuous learning and provide training to ensure analysts are confident in handling complex alerts. One way SOC teams can overcome this challenge is through the use of playbooks. One way playbooks are helpful to analysts is by guiding them through working specific alerts. If an analyst is not confident in working PowerShell obfuscation alerts, then the playbook can provide step-by-step procedures and recommended actions to properly investigate and respond to the alert.

Another area where SOCs falter is in asking the right investigative questions. Effective analysis requires a systematic approach where each question leads to the next logical step. Alwashali explains, “Analysts have to actively think about the right question to be asked, knowing why/how the answer will help to ask the next question” (Alwashali, 2024). Failure to follow a structured line of questioning can lead to incomplete investigations and incorrect conclusions. Therefore, it is encouraged to use frameworks such as the OODA loop to properly investigate an alert. The OODA loop stands for Observe, Orient, Decide, and Act; it is a decision-making model designed to help analysts process information efficiently and respond effectively. When an alert is generated, analysts must first observe the data, then orient themselves by understanding the context and potential implications. Afterwards, they decide on the best course of action and act accordingly. As new information becomes available, analysts who use the OODA loop continuously reassess the situation. By applying the OODA loop, analysts can maintain a logical and adaptive approach to threat detection.

UTSA’s SOC Environment

At the University of Texas at San Antonio (UTSA), the Security Operations Center (SOC) plays a crucial role in protecting the university’s network infrastructure and sensitive data. The SOC team consists of a range of individuals assigned to different tiers, who work cohesively to ensure comprehensive security monitoring and swift incident response. UTSA’s SOC operates under a tiered system, with responsibilities divided across three main levels. Tier 1 is composed of interns like me, who are tasked with monitoring alerts and conducting initial investigations. Tier 2 includes both full-time and part-time security analysts who review the work of the interns and handle more complex investigations. Tier 3 consists of senior security engineers, cyber operations analysts, and resource managers, with oversight from the director, Brad Cooper. Key figures in the SOC include senior security engineers like Robert Ripley and cyber operations analysts like Patrick Harris, who play pivotal roles in managing the SOC’s operations. This structured hierarchy ensures that incidents are escalated appropriately and that all alerts are investigated thoroughly. As Shutock explains, "some SOCs are smaller in size... with staff separated into tiers with defined responsibilities for their respective positions... Tier 1 (Alert Analyst): continuous monitoring... Tier 3 (Threat Hunter): proactively identify and investigate threats" (Shutock, p. 7556). This tiered system allows SOCs to function efficiently by ensuring that each team member is assigned tasks appropriate to their skill level, while more complex cases are escalated to higher tiers for deeper investigation. In my experience, tier 2 must be alerted as soon as an alert is validated as malicious, so that the SOC team can respond to the incident effectively. To achieve the SOC’s security goals, UTSA leverages both subscription-based tools and Open-Source Intelligence (OSINT) tools, which assist in the detection, investigation, and mitigation of security incidents. The most critical tools in UTSA’s SOC environment include ServiceNow, Microsoft Defender, Carbon Black, ExtraHop, Splunk, Active Directory, Duo Admin, Account Claim, and Abnormal Security. These tools enable the team to gather evidence, receive alerts for potentially malicious activity, and either validate or escalate alerts as necessary. Automation of the alert generation process helps reduce response times and allows analysts to dedicate more time to their investigations, ensuring that threats are addressed promptly and efficiently. As a result, the team can focus on more complex threats, rather than being slowed down by routine tasks. Research supports this approach, with MITRE emphasizing the importance of incorporating orchestration and automation to respond faster and minimize dwell times for potential threats. Additionally, Splunk notes, "Automation is one of the newer technologies to help SOC analysts... Processes that used to take 30 minutes... can now be done in as little as 40 seconds" (Essential Capabilities of a Modern SOC, p. 6). This demonstrates how automation not only increases response speed but also frees analysts to focus on higher-priority tasks, thereby improving the overall effectiveness of the SOC. Additionally, UTSA utilizes OSINT tools like VirusTotal and MetaDefender to investigate file hashes and IP addresses, while Any.Run is employed to analyze whether a URL is malicious. These tools are vital for enhancing the SOC's investigative capabilities and enabling thorough incident response.

UTSA's Security Operations Center operates under a unique set of circumstances that differ significantly from those of a typical corporate SOC. In corporate environments, networks are often highly restricted. They employ strict whitelists of approved applications, block traffic from unknown or potentially malicious sites, and flag any activity that deviates from predefined security standards. This strict approach minimizes risk by limiting the potential attack surface and reducing the likelihood of unauthorized activity. In contrast, UTSA's SOC must accommodate the open and diverse nature of an academic institution. Students, faculty, and researchers are allowed to bring their own devices and use the university's network for a wide range of applications. This flexibility is essential for supporting learning, research, and innovation. Unlike corporate SOCs, which typically restrict such activities, UTSA permits the use of tools and operating systems that are integral to cybersecurity education. For example, penetration testing distributions like Kali Linux are commonly used by students for coursework and research. In a corporate setting, any traffic originating from Kali Linux would likely be flagged immediately as a threat, possibly triggering disciplinary action.This openness means that while UTSA embraces a more relaxed policy on applications and network traffic, the SOC must remain highly vigilant and responsive to potential threats. Alerts generated by tools like Kali Linux or other penetration testing software require careful analysis to differentiate between legitimate academic use and genuine malicious activity. During my time as an intern, we consistently received alerts detailing port scans or hacking tools detected on endpoints. In other environments, unless the activity had been previously announced by IT, such alerts would be considered highly suspicious. However, at UTSA, these types of alerts were generally normal. Although UTSA is a cybersecurity university, targeting the university's systems with hacking tools is not permitted. Therefore, it was our responsibility as SOC interns to investigate the cause of these alerts. UTSA allows students to download almost any application onto their personal devices, which means we were responsible for ensuring that these tools were not downloaded onto UTSA owned devices and were not being used against the university. Additionally, understanding a user's position within the environment is crucial. For example, when handling a potential hacking tool or malicious script alert, determining whether a user is a network engineer, or a biology student is key to identifying malicious activity. Oftentimes, alerts related to malware or hacking tools may seem alarming but are considered normal behavior for IT professionals who use tools like RDP or PowerShell scripts. Therefore, SOC analysts must have a deep understanding of the university environment and the context in which these tools are used. They must also be prepared to respond quickly because the same tools used for educational purposes can be exploited by malicious actors. Furthermore, the unique environment at UTSA demands a proactive approach from the SOC. The SOC must balance the need for security with the university's commitment to academic freedom and technological exploration. Due to the diversity of devices and applications on the network, the urgency of monitoring increases. Analysts must rely heavily on research and contextual investigation. In my experience, the freedom to use various applications meant that several apps unknown to the SOC would generate alerts. As a result, the most time-intensive task during my shifts was researching these unknown applications. During investigations, I contextualized the app's use by analyzing the user's role and ensuring it aligned with the app's functionality. This research was often lengthy because the applications were obscure and not widely documented. Their hash values were rarely recognized by standard hash databases like VirusTotal, which made them harder to identify. Additionally, many apps had identical or similar names, which made it difficult to pinpoint the exact application. As a result of the constant research and investigation, UTSA has formed a SOC environment that sharpens analysts' research skills and their ability to distinguish between benign activity and genuine threats. As Steven from Tier 2 mentioned, UTSA SOC members conduct more investigations due to the network’s openness. In his experience, corporate SOCs are more locked down, with most systems pre-configured for analysts. In contrast, UTSA SOC analysts must constantly investigate new applications and the potentially malicious use of different tools not commonly seen in corporate SOCs.

While UTSA operates in a more open environment compared to corporate SOCs, it still closely follows industry best practices and recommendations. One way UTSA’s SOC adheres to these best practices is through the use of advanced security tools like Splunk, Microsoft Defender, Carbon Black, ExtraHop, and Abnormal Security. These tools provide comprehensive monitoring, detection, and analysis capabilities. For example, Splunk's real-time monitoring features align with the recommendation that a SOC must “detect the event” as soon as it enters the system (Splunk, 2024). However, Splunk is not the only event monitoring tool used in the SOC. The team also utilizes tools like ExtraHop to monitor network traffic and anomalies, while Carbon Black assists with endpoint detection and response. By using multiple tools, UTSA takes a layered approach to strengthen the SOC, covering different aspects of the network and endpoints.The UTSA SOC also embraces automation to enhance efficiency and reduce response times. Integrated automation tools streamline the alert generation process and assign priority levels to generated alerts. This priority assignment is helpful for analysts, allowing them to focus on the most critical alerts. In my experience, the risk-level assignment feature helped me prioritize high-severity events, such as impossible travel or malicious URL clicks, which were more likely to be true positives compared to events like “email reported as not junk.”At UTSA, automation is further supported by playbooks created using LucidChart. These playbooks serve as guidelines for analysts working on alerts. At the start of my internship, playbooks were incredibly helpful in teaching me where to look when investigating different types of alerts. For example, when I first began, I had no prior experience with Splunk. Therefore, when working on ExtraHop alerts, such as “Data Exfiltration to Discord,” I wasn’t sure where to look or what to search for. This is why UTSA follows Splunk’s recommendation of using standards and playbooks. As mentioned in their article, “automation tools take standard operating procedures and turn them into digital playbooks to accelerate investigation, enrichment, hunting, containment, and remediation” (Splunk, 2024). Although UTSA’s playbooks are not created by automation tools, they still provide valuable guidance for investigating alerts. Using these playbooks, I was able to determine which Splunk queries would be most helpful for my investigation, what information to include in my report, and the threshold of allowed exfiltration before considering it possibly malicious. Additionally, the UTSA SOC’s tiered structure further supports best practices by assigning responsibilities based on skill level. As described by Shutock, a tiered system typically includes Tier 1 analysts for initial monitoring, Tier 2 for complex investigations, and Tier 3 for proactive threat hunting (Shutock, 2022). At UTSA, interns handle initial alert triage, while senior analysts and engineers work on firewall rules and escalate significant threats. By implementing this tiered structure, UTSA ensures efficiency in the SOC, by allowing higher tiers to handle more technical operations and respond to escalated alerts deemed severe enough. Moreover, UTSA’s SOC emphasizes collaboration and communication among team members. Intern analysts are encouraged to share findings and coordinate efforts during investigations. One way UTSA facilitates communication within the SOC is through the use of Microsoft Teams. From the moment the SOC begins operations, a Teams meeting is initiated between the main campus SOC and the downtown SOC. Throughout the day, interns and other team members are constantly asking questions and helping each other with their alerts. This approach reflects the principle that “security is a team sport that requires coordination, communication, and collaboration” (Splunk, 2024). There are also times when the entire team works together to solve an alert. This typically occurs when a tier 3 member informs us of a compromise and asks us to collaborate as a team to investigate the incident. In these cases, we work together by announcing the tools we are using and sharing our findings. Announcing the tools is essential to prevent everyone from looking in the same place. Effective collaboration ensures that no critical detail is overlooked and that there is no redundancy in the investigation. Had we not announced our actions or shared our findings, the investigation would have been hindered by inefficient management; a lesson we learned during our first project, the Goose malware investigation.

Goose malware, also known as "Goose Desktop," is an "anti-productivity" application that spawns a goose animation on the screen. The application would auto-start at random times during the day, producing the animation, which occasionally interfered with the cursor or dragged unwanted images onto the screen. When we first noticed the goose animation, we were confused about its nature and purpose. Eventually, when enough interns were present, a tier 2 member announced that we were assigned a project to report on the goose malware: its functionality, the devices it affected, how it spread, and who was responsible. Initially, the project seemed exciting because it provided an opportunity to showcase our understanding of the UTSA environment and the tools at our disposal. However, we quickly realized there was a vast amount of information to analyze in order to find answers. Instead of collaborating as a team to cover all tracks and leave no stone unturned, we worked individually, hoping to find the answers on our own. Unfortunately, the sheer volume of logs we had to analyze, combined with the lack of communication, led to fatigue among team members, which only slowed us down. By the end of the investigation, different interns had come to different conclusions due to our varying levels of understanding, which stemmed from our lack of collaboration. The Goose malware investigation taught me the importance of communication and collaboration. A lack of coordination resulted in redundancy in the logs we investigated and delays that ultimately prevented us from solving the case. In future investigations, I will ensure that team members are assigned specific roles, tools, or systems to analyze. This will ensure that everyone contributes unique insights, helping us create the most complete picture of the event.

My Experience as A SOC Intern

My time as a SOC intern at UTSA was an invaluable experience that significantly enhanced my understanding of cybersecurity operations and the inner workings of a Security Operations Center. This opportunity allowed me to gain firsthand experience with a variety of Endpoint Detection and Response (EDR) tools, such as Microsoft Defender, Carbon Black, and ExtraHop, which are essential for monitoring and safeguarding networks against cyber threats. In addition to mastering these tools, I had the chance to apply my theoretical knowledge in practical, real-world scenarios by protecting UTSA's large institutional network. Prior to this internship, my main goal was to utilize the expertise acquired through my coursework to benefit real-world organizations, but during my time at the SOC, my objectives evolved. The experience not only reinforced my original goal of safeguarding organizations through the application of my skills but also expanded my initiative to align with the UTSA SOC's overarching mission: securing and protecting the university's complex information systems. This role allowed me to see how theory translates into practice and helped me understand the importance of continuous learning, teamwork, and proactive threat mitigation in maintaining network security. Through this experience, I cultivated a deeper appreciation for the critical role SOCs play in cybersecurity and gained insights that I can carry forward into future roles, making me more confident and prepared to face the dynamic challenges of protecting organizational assets in real-world environments.

My position as a SOC analyst intern for the downtown SOC provided a dynamic and challenging environment where I refined my investigative and analytical skills. My daily responsibilities involved actively monitoring, analyzing, and documenting alerts for potential security incidents. My efforts ensured that each event was assessed thoroughly and escalated when necessary. One thing I prioritized during the internship was documentation. Oftentimes when I would look into related events on ServiceNow, there was not much information relayed by interns who worked on similar alerts. Therefore, leading to redundant research. For example, if I worked on a port scan alert, there would be documentation written by previous interns stating that the scan was not malicious, but not providing any reasoning or explanation behind why they came to that conclusion. Therefore, I made it my priority to document my investigations as best as I could, so that future interns would not have to conduct redundant investigations over previously identified events. This was my part in making the SOC more efficient.

At the SOC, I collaborated closely with my team. We tackled alerts generated by security platforms like Microsoft Defender, Carbon Black, and ExtraHop, while employing investigative tools such as Splunk, Microsoft Defender, and Abnormal, alongside open-source resources like VirusTotal, AlienVault, and Any.Run. This combination of tools allowed us to cross-reference information, verify threat indicators, and make informed decisions. When faced with complex alerts, we often used Microsoft Teams meetings to brainstorm and bridge knowledge gaps. Screen-sharing sessions became a regular practice, during which I would articulate my analysis, outline my thought process, and seek input on the best course of action. This collaborative approach not only improved my investigative techniques but also strengthened my communication skills. Also, when I did not know how to work an alert, the playbook on LucidChart proved to be an invaluable guide. I would follow the playbook as it offered step-by-step procedures and detailed query instructions for different alert types. For instance, during my first encounter with a data exfiltration to Discord alert, my lack of experience with Splunk posed a challenge. However, the playbook provided clear, structured queries to help identify the affected device and user. Additionally, its “if this, then that” format allowed me to explore multiple investigative paths and adapt to the path most relevant to my investigation. This experience taught me the importance of leveraging documented procedures.

My intern supervisor was Steven Ordaz, an IT professional with decades of experience. His knowledge of the processes behind UTSA Tech Café, common user behavior, and his drive to become a professor made him a great leader for the interns. Steven consistently gave helpful advice that aided our investigations and deepened our understanding of the differences between an academic SOC and a corporate SOC. He also provided valuable feedback after our projects. For example, after our communication blunder during the Goose project, Steven pointed out that we needed to be more vocal and open to collaboration. The higher-tier analysts noticed our lack of communication and identified it as the deciding factor behind our inability to complete the project. This lack of communication was surprising, as we collaborated well during normal operating hours. From this project, I learned that people are often willing to work together but hesitant to take initiative in leading the collaboration. I also realized that due to the sheer amount of data necessary to analyze for an effective investigation, communication and collaboration are essential. Teams that fail to apply these principles are bound to struggle. Therefore, in my next SOC position, I will ensure the team remains collaborative. This can be facilitated by a leader who assigns roles and directs team members to apply their efforts effectively. We applied this lesson to our next project, where we needed to create a virtual machine configured to run MITRE Caldera. During this project, Vincent was assigned as the manager and directed us to work on different parts of the project, checking our progress and offering help when needed. Thanks to our collaboration and Vincent’s leadership, we successfully completed the project.

Ultimately, I fulfilled my goal with the internship by protecting a real organization’s information systems through applying my knowledge and dedication to continuous learning, which I implemented in every investigation I undertook. Throughout the experience, I discovered the significance of team collaboration and the critical importance of leadership in a Security Operations Center. I gained valuable insight into SOC best practices, knowledge that extends beyond professional environments and into my personal life. Motivated by the tools and techniques I learned; I have begun configuring similar security tools within my home network to “practice what I preach” and enhance my personal network’s security. The internship also allowed me to bridge the gap between theoretical concepts from my coursework and their practical, real-world applications. For example, although I understood hashes in theory, it was only during my SOC experience that I truly grasped their significance in cybersecurity. Hashes are essential for validating and identifying files and applications, and using hash databases like VirusTotal greatly aided my investigations by identifying file names and related signatures. This hands-on exposure deepened my understanding far beyond classroom learning, giving me a comprehensive perspective on cybersecurity principles. As a result of this internship, I am confident that the skills, knowledge, and collaborative techniques I cultivated will prove invaluable in my next Security Operations position.

Conclusion

My experience as a SOC intern at UTSA taught me the value of integrating people, processes, and technology to effectively detect, investigate, and respond to threats. I learned firsthand how critical collaboration, documentation, and automation are to maintaining an organization’s security posture. Through my work with tools like Microsoft Defender, Splunk, and Carbon Black, I developed practical skills that enhanced my ability to protect information systems in real-world environments. This experience also underscored the importance of leadership and communication in fostering efficient SOC operations. By bridging the gap between academic knowledge and practical application, I gained a deeper understanding of cybersecurity principles such as threat detection, anomaly analysis, and incident response. Moving forward, I am confident that the insights, skills, and best practices I acquired during this internship will empower me to contribute effectively to any future SOC role, ensuring robust protection against evolving cyber threats.

Citations

Alwashali, Ali. *A Tour Inside a SOC Analyst's Mind*. HackDefend Labs, www.hackdefendlabs.com/analysis/A-Tour-Inside-a-SOC-Analyst-Mind/.

CrowdStrike. Endpoint Protection Buyer's Guide. CrowdStrike, www.crowdstrike.com/en-us/resources/white-papers/endpoint-protection-buyers-guide/.

Cisco. *What Is Endpoint Detection and Response (EDR/MEDR)?* Cisco, www.cisco.com/c/en/us/products/security/endpoint-security/what-is-endpoint-detection-response-edr-medr.html.

Knerler, John. 11 Strategies of A World-Class Cybersecurity Operations Center. 2022.

Shutock, Matthew. Security Operations Centers: A Holistic View on Problems and Solutions. 2022.

Splunk. 10 Essential Capabilities of a Modern SOC. Splunk, 2024.

Splunk. The 10 Essential Capabilities of a Best-of-Breed SOAR. Splunk, 2024.

Steven Ordaz. Personal communication. 15 Oct. 2024.