Education Pathways to Reduce the Gap in the Cyber Security Workforce

Brandon R. Brown
bbrown118@coastline.edu

Tobi West
twest20@coastline.edu

Coastline College
Fountain Valley, CA 92708, USA

Ronald E. Pike
rpike@cpp.edu

Cal Poly Pomona
Pomona, CA 91768, USA

Abstract - Security Operations Centers are the first line of network defense for many organizations and therefore require highly skilled personnel. However, with the lack of skilled workers, many positions go unfilled due to both the lack of skilled workers and the high salaries these workers can command. This paper reports on ways to bridge this gap through leveraging the Centers of Academic Excellence for Cyber Defense Education (CAE-CDE). We will also explore a typical curriculum at one of these institutions and explain opportunities that can be gained through the effective use of talent coming from CAE-CDE institutions.

Keywords

Cybersecurity Education, Security Operations Center, IS Curriculum

1. INTRODUCTION

A recognized problem in the United States workforce has been the lack of skilled workers in cyber security. This is supported by many studies such as Morgan [1], Furnell, Fischer and Finch [2], Julisch [3] as well as an ongoing study by the U.S. Bureau of Labor [4]. Additional evidence is apparent through literature review of this phenomenon and poses the question as to why the gap exists and solutions for filling this gap. One possible explanation for the gap between demand and supply of cyber security talent is offered by the examination of entry-level skillsets and barriers of entry into the profession. Furthermore, a microcosm of this effect lay within an example of entry-level positions within Security Operations Centers or SOCs.

This is an examination of the gap that exists within these entry-level positions and potential solutions to bridge the gap by developing education pathways via curriculum at Centers of Academic Excellence in Cyber Defense Education (CAE-CDE) institutions. This pathway will be examined to provide insight for two critical constituencies to break the barrier to entry into cyber security positions, which will provide a new source of labor that can more quickly fill the needs of organizations for cyber security professionals.

The skills required for entry-level positions in Cyber Security Operations positions vary but a sampling of job postings in 2018 from several online employment boards shows a trend with the reduced threshold of barriers in terms of required skills. In effect this is creating more positions that are in need of fulfillment which until recently have been reserved for those candidates who obtain or possess four-year college degrees. This trend supports Anderson [5] and Microfocus [6]. These two independent studies articulate the need for security analysts with little experience who can quickly rise within an organization to fill higher level positions within a short span of time, thus re-opening the

original entry-level positions for new talent entering the workforce. This premise rounds out the background of the literature which defines roles, skills, and appropriate placement within a Security Operations Center.

2. LITERATURE REVIEW

Security Operations Center positions consist of technical and managerial skill sets where there is a focus on three general roles and responsibility areas: analysts, engineers, and managers. Specifically, Microfocus [6] outlines additional roles as seen in Figure 1; however, many of these are rooted in one of the two general technical roles such as analyst or engineer.

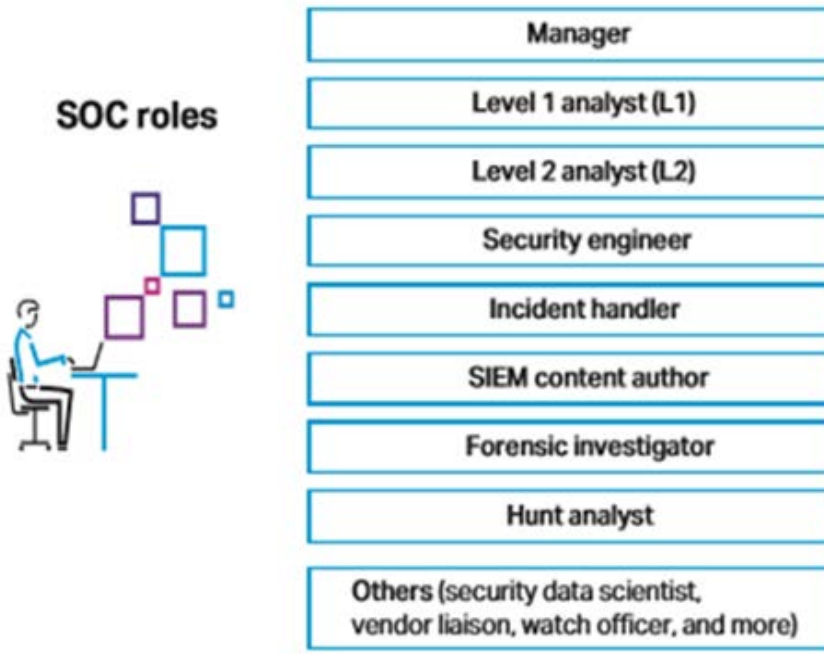

Figure 1: soc Roles. (Microfocus, 2018).

This analysis goes further by outlining more senior positions such as Security Engineer, Incident Handler, SIEM content author, Forensic Investigator, and Hunt Analyst. Additionally, other subject matter experts may be called upon in consulting roles to give expertise in niche' situations. The purview of this analysis will focus on the Level I and Level II analysts, their required skills, how they fit into a SOC, and how 2-year CAE-CDE institutions can bridge the gap to quickly fill these much-needed positions.

In addition to Microfocus, Dwyer [7] outlines a staffing model based on inputs from ancillary devices such as SIEM units but does not bridge the divide between technical skill and competency. Other notable contributors to the literature include Nathans [8], who again outlines more technical components and only touches on staffing levels and requirements. Kowtha et. al. [9] developed an analytical model that captured common and significant details of SOCs but again did not dive into staffing skills and responsibility levels.

There is a genuine theme in the literature where many articles and books revere the makeup of a SOC from technical control and managerial need but do not address staffing or skill requirements. Except for Dwyer [7], there is little in the way of answering, in statistical form, the requirement levels. Few studies provide insight into the required skills, level of education, or job definitions for Security Operations Centers.

Of these exceptions, Microfocus [6] and Anderson [5] stand out. Given the fact that these two works have been published within the last five years is noteworthy as to the infancy of the specific cyber Security Operations Center (SOC) organization and practices. The notion of a SOC for the purpose of information security dates back in reference to a period around the late 1990's [10]. Many operational endeavors around security were integrated into Network Operation Centers or NOCs but few were documented. The earliest of those was Sherwood [11] in which the author examined operations for events supervised by the FBI for anti-terrorism

activities that included policies for monitoring Internet communications and activities.

Linking these themes to practical methods for developing hands-on skills needed in the workforce is eased when examining the curriculum of two-year institutions that have cyber security programs. Some of these technical skills include incident response handling, event monitoring, and log parsing. These are just a few examples of the required characteristics listed in job descriptions for entry-level SOC positions. Perez et al. [12] is the seminal source for this research in that these researchers began the linkage of the curriculum with the needs of the cyber security field within the United States and correctly predicted the expansion of cyber security, and specifically in the area of information assurance, noting skills needed for both government and industry roles. Continuing along this path was Hoffman et al. [13] who expanded the work of Perez et al. into the practical approach for developing strategies for cyber security skills. Hoffman et al. [13] also stated that a logical path would be to incorporate cyber security skills into a collaborative effort that would include various stakeholders such as industry partners, academia, employers, and government policymakers to develop strategies relative to the cyber security workforce. This premise can filter down into the Security Operations Center as we examine the needs as laid out by Microfocus [6] and Anderson [5] with the curriculum pathway set out by Perez et al. [12], Hoffman et al. [13] and others who have explored these concepts in other fields such as healthcare with McGettrick [15] or Dodge et al. [16].

3. GAP ANALYSIS FOR ENTRY-LEVEL AND LOW-LEVEL POSITIONS IN SECURITY OPERATIONS CENTERS

Depending on which report or study you focus upon; Morgan [1], Goldman [16], the U.S. Department of Labor [17], or any other source there is compelling evidence of a dire need for cyber security skills in the U.S. labor market. This need is compelling and continuing and requires a mid- to long-term solution. Keeping in mind that examining the pathways for

entering this labor market has been difficult due to the fact that the desired skills come with many pre-requisites. The pre-requisite knowledge and skills include a solid understanding of networking, system administration, systems analysis, and programming languages. The traditional approach of simply pursuing only individuals with the complete skill set and work experience has been ineffective and is not improving the long-term outlook for filling the gap in cyber security talent.

There is evidence that the previously myopic focus on finding a cyber security savant is giving way to organizations understanding the breadth of talent and levels of talent that are needed in the workforce. A simple search on many leading job boards shows that roughly forty-five percent of Security Operations Center jobs are entry level. A sampling of these positions show that the main skills sought are those dealing with incident response (IR), Security Incident and Event Management (SIEM), intrusion detection / prevention systems operation (IDS/IPS), and a general knowledge of system administration and networking. Entry-level positions in the sampling of one hundred entry-level SOC positions nationally had an average salary of $62,400 [18].

At many organizations these positions typically have a title of Cyber Security Analyst I which aligns with the titles in the studies previously mentioned. According to Microfocus [6], an Analyst I position will execute operations procedures as a matter of daily responsibility. Furthermore, the role of a SOC analyst is defined as detailed and repeatable execution of all operational tasks as documented in processes and subordinate procedures. Specifically, the Analyst I role will be responsible for monitoring the SOC, situational awareness and automation systems for security events, and closing or escalating those events as necessary. An Analyst I will maintain the group email address and distribution lists, answer SOC main phone lines, and update all relevant documentation such as shift logs and tickets.

Specifically, the Analyst I will identify, categorize, prioritize, and investigate events rapidly utilizing triage and response guidelines for the enterprise using commonly available SOC log sources that include:

- Firewalls and network devices
- Infrastructure server and end-user systems
- Threat intelligence platforms
- Web proxies
- Application logs and web-application firewalls
- Identity and access management systems
- Cloud and hybrid-IT provisioning, access, and infrastructure systems
- Antivirus systems

Another position that is potentially achievable along this path in a SOC is that of an Analyst II position. This is a more mid-level position incorporating greater responsibility and authority. However, it is still considered entry-level and students completing Certificate or Associate degree programs can attain this job position given additional work-study, apprenticeship, or superior achievement in such areas as cyber competitions.

According to Microfocus [6] “These senior analysts will gather information, collate it into an accessible format, and ensure its full dissemination. Level 2 analysts are responsible for the event processing and long-term analysis. This includes any deep dive investigation into network activity that is deemed suspicious.”

Specifically, the Level 2 analyst will:

- Monitor level 1 analyst performance by investigating incoming events using SOC-available tools.

- Ensure level 1 event(s) are addressed in a timely manner using available reporting and metrics.
- Approve and, if necessary, further investigate level 1-escalated events.
- Mentor level 1 analysts to improve detection capability within the SOC.
- Manage SOC event and information intake to include gathering intelligence reports, monitoring ticket queues, investigating reported incidents, and interacting with other security and network groups as necessary.
- Serve as detection authority for initial incident declaration.
- Function as shift Subject-Matter Experts (SMEs) on incident detection and analysis techniques, providing guidance to junior analysts and making recommendations to organizational managers.
- Drive and monitor shift-related metrics processes ensuring applicable reporting is gathered and disseminated per SOC requirements.
- Conduct security research and intelligence gathering on emerging threats and exploits.
- Serve as a backup analyst for any potential coverage gaps to ensure business continuity

Beyond these positions, organizations must look to more advanced programs for education and training, especially when individuals want to make the jump to engineering and managerial positions [19]. This can be addressed by continuing education at the university level in attainment of Bachelor's and/or Master's degrees which provide advanced skills training and knowledge from accredited CAE-CD 4-year institutions.

4. TO THE RESCUE, CAE CERTIFICATE AND AS PROGRAMS TO FILL THE GAP

Given the gap analysis outlined previously; it is safe to assume that two-year institutions of higher learning can help to fill this void in education leading to reducing the shortage of skilled cyber security workers. However, it is important for these institutions to follow standards in cyber security education to meet the needs of industry in a way that is proven and accredited. One such way to address this gap is to leverage institutions that follow the National Initiative for Cybersecurity Education (NICE) Workforce Framework and are certified by the National Security Agency and Department of Homeland Security program for Centers of Academic Excellence (CAE). In particular, those institutions that meet cyber defense education standards (CAE-CDE) and are accredited two-year institutions can quickly turn out certificated professionals to fill the cyber security workforce gap.

The major shortcoming of the CAE-CDE program is the lack of participation by two-year institutions of higher learning. Of the roughly 267 institutions in the CAE program, only 68 of those are two-year institutions. Take into consideration that this is a small sample of over four thousand institutions of higher learning nationally, and one can conclude that institutions with the CAE designation are the leaders in this field. Given this, examination of a model curricula is extremely important for providing a pathway for graduates to attain employment in upwardly mobile positions. Examples of these curricula are easily obtained via the different institutions' websites as nearly all two-year CAE institutions offer information and enrollment information via the Web.

One such example of cyber security curricula at a two-year CAE institution is Coastline College in southern California. The College's website can be viewed at https://www.coastline.edu. As a typical example, Coastline's Associate's degree in Cybersecurity maps to the NICE

Workforce Framework via the knowledge units for two-year CAE institutions and is outlined as follows.

Per Coastline's program website "The Computer Networking Cybersecurity program will give the student a solid background in the field of Computer Security. The focus on Cybersecurity will provide the student with some of the basic skills needed for an entry-level career in Cybersecurity. The courses provide an overview of the entire field. Topics covered will include Cisco Security, Windows Operating System security, Linux security, Firewalls, Intruder Detection systems, Security policies and procedures, e-mail & Web security, and designing and building a secure computer network" (Coastline, 2018).

Furthermore, upon completion of the Cybersecurity program at Coastline College, students will be able to demonstrate the ability to locate technical resources to solve problems with networking hardware and software. Additionally, students will be able to demonstrate proficiency with various software packages to solve common networking problems using theories learned in the classroom to design and implement a workable solution. Finally, the students should be able to show the capability to build and maintain secure networks.

Coastline's students will complete a course track of both Core and Elective courses as outlined in Table 1.

Table 1
Associate Core and Elective Courses

Requirements	**Dept. #**	**Name**	**Units**
Required Core (12 Units)	CST C128 CST C230 CST C158 CST C157	Network+ / Intro to Networking Introduction to Security Server+ Intro to Python Programing	
Electives (9 Units)	CST C232 CST C245 CST C242 CST C255 CST C231 CST C260 CST C191 CST C258 CST C253	Ethical Hacking Exploring Computer Forensics PenTest+ Cybersecurity Analyst+ CompTIA Adv.Sec. Practitioner CISSP CompTIA Linux+ Linux Networking and Sec. Cisco ASA, PIX, & Net. Sec.	

Furthermore, it is important that proper pacing be followed so as to complete the curricula in a timely and non-fractured manner. Coastline's suggested Pathway Sequence is outlined in Table 2.

Table 2 2 Yr. Pathway Sequence			
Fall Yr. 1	**Spring Yr. 1**	**Fall Yr. 2**	**Spring Yr. 2**
CST C128 & CST C157	CST C230 & CST C158	CST C232 & CST C245 Or CST C191 Or CST C245 & CST C260 Or CST C245 & CST C191	CST C242 Or CST C255 Or CST C258 & CST C232 Or CST C231 Or CST C253

5. THEORETICAL IMPLICATINS AND CONCLUSIONS

If the expansion of SOCs continues as the Bureau of Labor Statistics and other research agencies foresee, then a paradigm shift needs to occur to fill this void where human resources of skilled positions do not yet exist. SOC designers and managers operate in many of the same ways that older

Network Operations Centers (NOCs) have for years. Security professionals will enhance professional capabilities either internally through employee development or through external training providers. Either way, the demand for skilled labor in this market will continue to grow.

In this scenario, security practitioners will have the ability to exercise much greater control over their environments by automating tasks via scripts and potentially by using artificial intelligence where appropriate to manage variation in tasks designed to meet predefined criteria (Pike and Brown, 2018). In this case, a new class of information systems / information technology (IS/IT) theories becomes possible. Mid-range theories with a limited scope leading to testable hypotheses are needed in any discipline (Merton, 1968). The IS/IT field is in greater need of such theories than most given the relatively scant theoretical foundation for much of the work in the field. A universal SOC structure such as those that leverage lower-end labor and skill sets may also open the door to a more general (grand) theory of IS Security which has so far eluded this and similar disciplines (Weber, 1997).

These changes to the mindset of management, especially in enterprise and Fortune 1000 companies, can greatly enhance the dynamics within their organizational culture, in turn fostering a learning environment by instituting this structure. In doing so, the organizations will develop a holistic mentoring that can self-perpetuate into a self-sustaining model within the organization. Couple this with the opportunity to build relationships with the two-year and four-year CAE-CDE institutions as feeder programs for talent, as well as ongoing development partners, and the microcosm is complete.

6. OPPORTUNITIES FOR FOLLOW-ON RESEARCH

Looking back at the needs of IS/IT security professionals, the ways that organizations define, develop, and recruit for these positions has changed greatly over time. This is due in part, as shown here, to the demand

in the industry for sheer numbers of skilled professionals. This is prevalent across all industries, government sectors, and institutions. The success of SOC programs now rely on lower-level, yet highly skilled, and trained personnel to be in the correct positions with proper skillsets to provide stewardship of assets and be the first proverbial canary in the coal mine. This type of organizational construct provides greater awareness and flexibility while reducing reaction time to security threats. Tracking this trend is important for administrators, faculty, and staff of CAE-CDE institutions for the purpose of continuously updating curricula and programs to meet workforce needs. Therefore, ongoing statistical analyses of job descriptions, position openings, and competencies is needed along with industry and government partnerships to ensure students enter the workforce with the appropriate skills and are provided with clearly defined paths to ongoing career development.

REFERENCES

[1] Morgan, Steve. (2017, June 8) Cybersecurity labor crunch to hit 3.5 million unfilled jobs by 2021 Retrieved from: https://www.csoonline.com/article/3200024/security/cybersecurity-labor-crunch-to-hit-35-million-unfilled-jobs-by-2021.html

[2] Furnell, S., Fischer, P., & Finch, A. (2017). Can't get the staff? The growing need for cyber-security skills. Computer Fraud & Security, 2017(2), 5-10.

[3] K. Julisch, "Clustering intrusion detection alarms to support root cause analysis," ACM Transactions on Information and System Security (TISSEC), vol. 6, pp. 443-471, 2003.

[4] Bureau of Labor Statistics, U.S. Department of Labor, Occupational Outlook Handbook, 2016-17 Edition, Information Security Analysts. Retrieved from https://www.bls.gov/ooh/computer-and- information-technology/ information-security-analysts.htm

[5] Anderson, Brandie (2014). Building, Maturing & Rocking a Security Operations Center. Hewlett-Packard Presentation via SANS Institute Reading Room. Retrieved from: https://digital-forensics.sans.org/summit-

archives/DFIR_Summit/Building-Maturing-and-Rocking-a-Security-Operations-Center-Brandie-Anderson.pdf

[6] Microfocus. (2018). Intelligent Security Operations: A Staffing Guide. SANS Institute. 2018. Retrieved from: https://www.microfocus.com/media/white-paper/intelligent_security_operations_a_staffing_guide_wp.pdf

[7] Dwyer, P. J. (2015). U.S. Patent Application No. 14/246,543.

[8] Nathans, D. (2014). Designing and Building Security Operations Center. Syngress.

[9] Kowtha, S., Nolan, L. A., & Daley, R. A. (2012, November). Cyber security operations center characterization model and analysis. In Homeland Security (HST), 2012 IEEE Conference on Technologies for (pp. 470-475). IEEE.

[10] Ptacek, T.H. and Newsham, T.N. (1998) Insertion, Evasion and Denial of Service Eluding Network Intrusion Detection, Technical Report. Secure Networks Inc. January 1998.

[11] Sherwood, C. W. (1998). Security management for a major event. FBI L. Enforcement Bull., 67, 9.

[12] Pérez, L. C., Cooper, S., Hawthorne, E. K., Wetzel, S., Brynielsson, J., Gökce, A. G., ... & Philips, A. (2011, June). Information assurance education in two-and four-year institutions. In Proceedings of the 16th annual conference reports on Innovation and technology in computer science education-working group reports (pp. 39-53). ACM.

[13] Hoffman, L., Burley, D., & Toregas, C. (2012). Holistically building the cybersecurity workforce. IEEE Security & Privacy, 10(2), 33-39.

[14] McGettrick, Andrew. "Toward effective cybersecurity education." IEEE Security & Privacy 11.6 (2013): 66-68.

[15] Dodge, R., Toregas, C., & Hoffman, L. J. (2012). Cybersecurity Workforce Development Directions. In HAISA (pp. 1-12).

[16] Goldman, Jeff. (2017). Cybersecurity Workforce Gap to hit 1.8 Million by 2022. Retrieved from: https://www.esecurityplanet.com/network-security/cybersecurity-workforce-gap-to-hit-1.8-million-by-2022.html

[17] U.S. Department of Labor. (2018. April, 13) Occupational Outlook Handbook Information Security Analysts. Retrieved from: https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

[18] PayScale. (2018). Average Security Operations Analyst Salary. Retrieved from: https://www.payscale.com/research/US/Job=Security_Operations_Center_Analyst/Salary

[19] Kelley, D., & Moritz, R. (2006). Best practices for building a security operations center. Information Systems Security, 14(6), 27-32.