Exploring Depth in Cybersecurity Education Through the Lens of a SIEM

Michael R. MacDonald
mmacdonald@cpp.edu

Nathan D. Pike
ndpike@cpp.edu

Ronald E. Pike
rpike@cpp.edu

Computer Information Systems
Cal Poly Pomona
Pomona, CA 91768, USA

Abstract

This paper explores the addition of specific hands-on technologies, such as SIEM (Security Incident and Event Management) systems, into cybersecurity curriculum. SIEM coverage is needed because cybersecurity education is often perceived by students to be fragmented and disjointed as there are many seemingly overlapping, conflicting and diverging topics. SIEM systems demonstrate an overview and dashboard displaying the current cybersecurity posture providing a framework to students allowing them to understand the relationship among the many components and topics within cybersecurity. Such topics are often covered in extra-curricular activities; however, the integration of such technologies into the curriculum would ensure consistent coverage of topics, provide a framework to understand topics and their relationships to the cybersecurity operations/practices and empower students to extend their cybersecurity education into research, competitions, and more.

Keywords: Cybersecurity, Competitions, Certifications, SIEM, SOC, NIST

1. Introduction

This paper addresses the value of attaining hands-on experience in SIEM & compliance in college and discusses why cybersecurity programs may want to incorporate hands-on learning as part of the classroom experience. The premise for the paper is that federal standards are growing and increasingly impact practice in the cybersecurity field. As a result, education practices related to cybersecurity need to be evaluated in light of the growing regulation. The lead authors of this paper are May 2020 graduates focusing on cybersecurity within the Computer Information Systems program in the business college at Cal Poly Pomona. One of the authors just completed a master's degree while the other completed a bachelor's degree.

SIEM (Security Incident and Event Management is critical to cybersecurity education as it is the monitoring platform for cybersecurity. An argument is provided in the abstract noting that SIEM coverage is needed in cybersecurity education to provide an overview of the field and providing students with the ability to make sense of the myriad security devices, protocols, frameworks etc. The requirement and need for SIEM is also spelled out by the National Institute of Standards and Technology (NIST).

The National Institute of Standards and Technology (NIST) guidelines for cybersecurity provide guidance from the federal government pertaining to the operations of technical systems from nuclear reactors to IT systems which are critical to cybersecurity education as they define the proper implementation and use standards for cybersecurity. If and when our graduates are pressed in court for why they did or did not complete a specific task or attend to a detail in their cybersecurity practice, the NIST guidelines are the only line of defense for showing that a task or process was completed correctly. Technical training from academia, independent certification training sources can help a student understand how to do something. The NIST guidelines define what to do and SIEM systems are part of these guidelines.

While the prescribed curriculum at Cal Poly Pomona offers some opportunities for hands-on learning, more extensive hands-on experience with compliance tools and Security Incident and Event Management (SIEM) systems is attained by students through volunteering in the student Security Operation Center (SOC). We decided to invest our time into these systems as they are purported to be valuable security tools that many organizations incorporate into their cybersecurity practices. In addition to volunteering in the student SOC, other opportunities to obtain hands-on learning were through cybersecurity competitions via Cal Poly Pomona student clubs or through other vendors.

Over the past several years Cal Poly Pomona has built a student hybrid-cloud data center as well as a student security operations center that are equipped with leading-edge systems that students operate. The intent of these facilities is three-fold. First, we created a learn-by-doing environment giving students real-world experience on industry-grade systems with real workloads and real customers. Second, we want students to lead the process of designing changes to the facilities and work with industry and government organizations to gain insight in this task. The interaction with professionals in the field is designed to help students explore current changes in the field and insights that can be inferred.

Third, we wish to have this environment as a research and test bed to permit students and faculty access to the same tools and technologies available to industry. This paper was driven by students working in the student security operations center and their interactions primarily with federal agencies. Both students were in a program of study (Scholarship For Service – SFS) that mandated a period of federal service after school which made the federal agencies more interesting. The students were also ingesting threat feed data from federal sources as part of their work which provided them insight into operations within federal agencies.

In this paper, we argue that in-depth cybersecurity experience gained through installing, maintaining, and operating SIEM systems (we use IBM QRadar, LogRhythm, and Splunk) should be integrated into the curriculum as opposed to merely extra-curricular activities. We will discuss why SIEM/SOC is important as well as the tools we were able to utilize during our research. We are focusing on a SIEM tool because so many different parts of the IT infrastructure interact with the SIEM which monitors cybersecurity operations and maintains compliance outputs. Federal guidance also calls for the use of SIEM systems to monitor information systems.

We believe the process of installing and configuring this tool provides students with the ability to encounter a diverse range of cybersecurity technologies and understand their relationships. Finally, we will also discuss the importance of cybersecurity competitions as well their drawbacks in providing hands-on experience in cybersecurity.

2. Literature Review

2.1 NIST Special Publication 800-137(NIST SP 800-137)

NIST SP 800-137 is a framework that is focused on risk management. In this risk management strategy, NIST outlines a three-tier system for creating an organization's security controls called Information Security Continuous Monitoring (ISCM). There are different ways an organization may choose to perform ISCM though SIEM platforms are at the heart of this process.

A SIEM tool ingests network traffic logs, aggregates data, and provides dashboards. SIEM tools can be used to address many controls mentioned in NIST 800-53. NIST 800-137 recommends the use of NIST 800-53 to determine methods for creating controls on information systems and business processes. Before an organization implements a SIEM system, NIST SP 800-137 calls for the development of a knowledgeable workforce. There are different ways of building this knowledgeable workforce though one way is contrasting skills that already exist in the organization with a list of total skills needed. One method that helps in gauging whether someone has knowledge in a given area is seeing if individuals possess industry-recognized certifications. Recent literature reveals that traditional SIEM platforms are giving way to complete data management platforms that organizations can implement in house or consume from a cloud provider (Preimesberger, 2020).

There are many roles for users and NIST SP 800-137 has a plethora of descriptions demonstrating how these different roles complement and support each other. While there are many important tasks for personnel performing these different roles, an important concept for assisting people and improving monitoring is in the automation of security controls. While not all controls can be automated, there are many different tools and methods available for automating tasks. A SIEM system is a great tool to add to an organization's IT infrastructure as they look to automate continuous monitoring

2.2 NIST Special Publication 800-53 (NIST SP 800-53)

NIST SP 800-53 assists organizations in implementing controls and procedures that are geared towards security. Within NIST SP 800-53 some references speak about advantages to automating many security controls. One such control type is the Security Content Automation Protocol (SCAP). Following this standard, along with other automation standards, will likely assist in automating security controls.

While NIST SP 800-53 is designed to guide organizations in designing security controls, there are references to NIST SP 800-53a which assists in assessing security control effectiveness. NIST SP 800-53a provides a checklist along with explanations on measurements of different controls that are important and contains recommended scoring scales if your organization wants to use all NIST specified guidelines and recommendations.

2.3 NIST Special Publication 800-181 (NIST SP 800-181)

NIST SP 800-181 presents the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. NICE serves as a framework for describing and sharing essential information regarding cybersecurity work and the Knowledge Skills and Abilities (KSAs) needed for an organization to have a competent security posture. The NICE framework provides guidelines to develop an effective cybersecurity workforce. The intended audience/users of the framework are broad including employers, current and future cybersecurity workers, educators/trainers, and technology providers. The framework can be adapted to suit an organization's needs. Critical aspects of the publication include the different ways the framework can be used. The NICE framework has four main areas of utilization.

First, it is important to have the proper identification of cybersecurity workforce needs, such as career progression, qualification requirements, training requirements, human capital planning, and the development of cybersecurity job descriptions. Cybersecurity educators, employers, and employees can use the NICE framework to clarify communication between themselves. Organizations can then run a criticality analysis and a proficiency analysis. A criticality analysis identifies important KSAs and the proficiency analysis helps determine what the level of experience a candidate should have in a position.

The second area of utilization is the recruitment of cybersecurity talent. Using the NICE framework, organizations develop strategic hiring processes. Additionally, organizations concerned with gaps in their workforce can use the NICE framework to help identify specific areas that need strengthening. The framework goes into detail on the position types and their relevant KSAs. The workforce categories are: Securely Provision, Operate and Maintain, Oversee and Govern, Protect & Defend, Analyze, Collect and Operate, and Investigate. The job listings corresponding to these categories are then further defined.

The third area of utilization relates to the education and training of workforce members. With the NICE framework, educators have a guide for curriculum development. The NICE framework empowers collaboration between the private and public sectors through its common knowledge and skills base. Academic institutions will have a common core curriculum to prepare students for the workforce.

Finally, the NICE framework addresses the retention and development of the workforce. It discusses methods of supporting the workforce to develop the employee. After an employee leaves their position, the employer must consider the different expenses as hiring costs, training expenses, reduced productivity and team morale may be substantial. The NICE framework supports development and retention in numerous ways including thorough identification of KSAs where an employee can recognize gaps in their skills and what they can work toward to grow their skills.

Another important aspect of the NICE framework is the ability to measure the skills and competency of individuals. In the NICE framework, there is a list of skill descriptions that assists administration in declaring whether an individual has a skill. The NICE framework draws upon the National Institute of Standards and Technology (NIST) and defines a skill as “the observable competence to perform a learned psychomotor act” (NIST SP 800-181).

2.4 Professional Certifications and Curriculum

A review of *Maintaining a Cybersecurity Curriculum: Professional Certifications as Valuable Guidance, b*y Knapp, Maurer, and Plachkinova provides insight on the development of cybersecurity curriculum through professional certifications. Academia must be able to quickly adapt to changing demand in skills and knowledge in a manner similar to professional certifications. The authors present a case on how helpful certifications can be in creating and maintaining cybersecurity curriculum. They provide a literature analysis, a case study, and a discussion of other topics such as cybersecurity capstone courses.

2.5 Cybersecurity Job Demand

The skills needed to operate a SIEM/SOC are currently in high demand and will continue to grow substantially in the years to come. According to the U.S. Bureau of Labor Statistics, there were 112,300 information security analyst jobs in 2018. There is expected to be a 32% increase in these positions by 2028. That is an average higher growth rate than any other occupation.

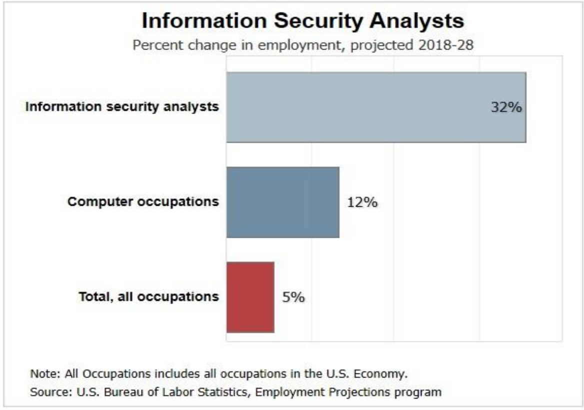

Figure 1.

Figure 1 demonstrates growth in demand for personnel skilled in information security.

3. Considering Different Learning Approaches

3.1 Traditional and Vocational Education

Often higher education is focused on theory and research teaching. However, an interesting case study to review is that of the German higher education system. According to (Baethge and Wolter) there are two distinct higher education systems. The first system is called the Vocational Education and Training (VET) and the second is a more traditional academic university system. Over the latter half of the twentieth century, the German economy flourished under these two systems. According to this paper, *The German skill formation model in transition: from dual system of VET to higher education* Germany has been a country focused on high-value manufacturing and products as time has approached modern time a large number of German workers have shifted from working in factories to more service sector jobs. Beginning in the 90s and into the early 2000s employer preferences have shifted away from the tradition of hiring individuals out of the VET system and moving more towards hiring German individuals who are graduating with degrees from universities in Germany. This is due in part to the growing complex needs of work in Germany. While many students coming out of universities in Germany have good analytical skills, they sometimes lack the ability to apply the knowledge acquired in the classroom to real industry problems. This has caused both students and universities to blend elements of the traditional and VET education systems.

Blending elements of the traditional and VET education systems allowed German students to receive an education that utilized both systems, which helped them be more suited for the complex needs of the German workforce. Applying a similar approach to cybersecurity curriculum can help alleviate problems such as the barrier to entry for new cybersecurity professionals. Cybersecurity employers demand a highly educated and experienced workforce. 84% of cybersecurity postings require at least a bachelor’s degree, and 83% require at least three years’ experience (Burning Glass). More extensive hand-on learning in conjunction with traditional higher education will better prepare students to apply their knowledge to real industry problems. Students will then be in a better position when seeking employment.

3.2 Cybersecurity Competitions

Participating in cybersecurity competitions benefit students in several ways. According to *Effectiveness of Cybersecurity Competitions,* by Cheung, Cohen, Lo, et al. research has indicated that cybersecurity competitions are highly effective in promoting student interest in the cybersecurity field. Competitions are also an avenue for students to obtain hands-on experience while under pressure to perform well. Some competitions are team-based, which allow students to build their teamwork skills. These are all excellent benefits, unfortunately, there are drawbacks to competitions that render them an incomplete solution for students to gain hands-on experience.

To perform well in cybersecurity competitions, it often requires one to possess advanced knowledge and skillsets at the start of the competition. The content of competitions can vary greatly and require different combinations of skills and knowledge. Traditional curriculum offered by most universities often lacks relevant material to prepare students for skills they would need in a cybersecurity competition. Additionally, most universities consider cybersecurity competitions to be extracurricular, so it is up to the student to decide to prepare and participate in a competition. For these reasons, universities should incorporate more hands-on learning in the core curriculum, which will expose students to the material they will need to participate in these competitions.

At Cal Poly Pomona, two popular cybersecurity competitions students participate in are the Collegiate Cyber Defense Competition (CCDC) and the Collegiate Penetration Testing Competition (CPTC). These two competitions allow students to choose from two different routes- defensive or offensive security. Recruiting and practice sessions typically begin in the summer. We have observed strong attendance at the practice sessions for these competitions. After talking with the students, some of them shared that they had a lack of confidence that they had the necessary skills and knowledge to be a competent competitor. They felt intimidated by the seemingly advanced content and tasks other students were completing. However, encouraging students to stay and dive into the material regardless of their level of expertise would be well worth it, as they would begin to progress by leaps and bounds.

Competitions provide exposure to many different cybersecurity topics, which is great for beginners. However, they are also designed to push one’s level of skill, empowering them to go further than they have before. Incorporating hands-on learning into the core curriculum will further elevate interest in cybersecurity competitions as well as reduce the perceived barrier of entry. The stronger the foundational skills students have, the more they will be able to achieve in a competition.

4. SIEM

In today’s complex business market and the ever-increasing need for cybersecurity, the ability to automate and streamline compliance is extremely important. A tool that was called out in NIST SP 800-137 as a valuable tool for IT network and infrastructure monitoring is a Security Incident and Event Management (SIEM) system. SIEM systems monitor network traffic and aggregate logs. Having the capacity to centralize network monitoring and perform real-time metrics is very valuable.

Many organizations use SIEM tools for maintaining their network security and assisting with compliance activities. NIST 800-137 has identified many advantages to using a SIEM tool; however, finding talent to operate and maintain this tool is not always easy and skills are required to operate these tools. Building a framework for individuals to learn these skills is extremely valuable and requires both theoretical and applied components.

At Cal Poly Pomona we have access to SIEM tools and the ability to monitor traffic at the university’s student data center, but these activities are extra-curricular and only available to students working beyond the designed curriculum. There are many different SIEM tools ranging from open source to the enterprise level. At Cal Poly Pomona we install open source solutions as well as IBM QRadar, Splunk, and LogRhythm which each have different capabilities. Whether an organization chooses to use an open-source SIEM or an enterprise SIEM there are resources available to get started.

The NICE framework clearly lays out the government’s desire for individuals with applied skills in cybersecurity. Universities can leverage a SIEM tool in their curriculum to teach many aspects of security while demonstrating the connections between each of the areas. With a proper environment, students would be able to gain hands-on skills in dashboards, threat hunting, network traffic monitoring, audit reporting, digital forensics, compliance, log analysis, and much more. Learning core skills in an industry-relevant environment that demonstrates the connection between these areas brings added value. While individual students may only be able to study a small group of these topics, they will be working alongside others working in supporting areas providing at least an initial orientation to these many topics.

5. CONCLUSIONS

In this paper, we make two key arguments, first is for the use of SIEM systems in curriculum helping students to view cybersecurity from the perspective of the measured outcomes. This perspective allows students to recognize the relationship between disparate cybersecurity systems, tools, protocols etc. Students will also be able to view related work (i.e. configuring a firewall) from the perspective of the SIEM platform that monitors the systems and creates compliance related reports. This serves to build good habits in understanding that cybersecurity work has two distinct outcomes, completing the task at hand, and ensuring that the task completion is recorded in the SIEM providing the organization with the ability to monitor the activity and add it to compliance reporting. Demands surrounding compliance reporting are exploding in government and industry and students must be exposed to this process and trained to manage related tasks.

The second argument is for more applied hands-on learning content in and out of the formal curriculum. Students are inundated with new knowledge, the application of knowledge to develop solutions, and implementing solutions to meet organizational needs and demands. Instead of empowering students, these demands sometimes overwhelm students leaving them to believe the task at hand is too large. Competitions can be implemented withing curriculum as well as in extra-curricular formats. Industry partners and academic organizations are adding increased numbers of competitions that can be started in a class but then continued by students beyond the class providing students the ability to continue to explore learning in areas of interest. Splunk for instance created the Boss of the SOC competition that can be played in class, in an intramural sports context and continued by students after graduation through industry conferences.

The NIST 800-137 publication cited earlier calls for the development of Information Security Continuous Monitoring (ISCM) and SIEM systems are the tool designed to handle this task. The requirements for compliance with this requirement are growing and becoming relevant to a larger percentage of graduates and is therefore a learning challenge that we believe all schools teaching cybersecurity will need to face.

6. LIMITATIONS

This paper argues for the implementation of SIEM systems in curriculum with sparse support. The most specific support is in the form of NIST guidance in SP 800-137 regarding SIEM systems. Each of the organizations that participated in this research is using a SIEM but none were allowed to be identified or cited.

The literature review for this paper is purposefully nontraditional. The cybersecurity frameworks used in academia come from many sources but the most critical source on “what” needs to be done in cybersecurity is the NIST guidance. Therefore, NIST guidelines were used to support the arguments.

It is important to note that that the two students who participated in this paper completed their contributions before starting their current cybersecurity roles with the federal government and had no interactions in the review process.

7. REFERENCES

Baethge, M., Wolter, A. The German skill formation model in transition: from dual system of VET to higher education?. *J Labour Market Res* **48,** 97–112 (2015). https://doi.org/10.1007/s12651-015-0181-x

Bureau of Labor Statistics. (2020, April 10). Information Security Analysts: Occupational Outlook Handbook. Retrieved May 09, 2020, from https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

Burning Glass. (2015). Job Market Intelligence: Cybersecurity Jobs, 2015. Boston, MA: Burning Glass Technologies

Cheung, R. S., Cohen, J. P., Lo, H. Z., Elia, F., & Carrillo-Marquez, V. (2012). Effectiveness of cybersecurity competitions. In *Proceedings of the International Conference on Security and Management (SAM)* (p. 1). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

Dempsey, K. L., Johnson, L. A., Scholl, M. A., Stine, K. M., Jones, A. C., Orebaugh, A., . . .

Johnston, R. (2011, September 30). *NIST Special Publication 800-137* [PDF]. NIST Pubs.

IBM Security QRadarVersion 7.3.2User Guide [PDF]. (2019). Armonk, NY: IBM Corporation

Joint Task Force Transformation Initiative. (2014, December 18). NIST Special Publication 800-53A Rev.4 [PDF]. NIST Pubs.

Kelley Dempsey, Nirali Shah Chawla, Arnold Johnson, Ronald Johnston, Alicia Clay Jones, Angela Orebaugh, Matthew Scholl, Kevin Stine (2011) Title. (National Institute of Standards and Technology, Gaithersburg, MD), Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations (NIST 800-137) , Ed., Information Security, Rev.1, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf

Knapp, K., Maurer, C., & Plachkinova, M. (2017). Maintaining a Cybersecurity Curriculum: Professional Certifications as Valuable Guidance. *Journal of Information Systems Education, 28*(2), 101-113.

NIST 800-53 Compliance Module: Deployment Guide [PDF]. (2016). Boulder, CO: LogRhythm Inc.

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-53r3.pdf

Preimsberger, C. (2020). AT&T Cybersecurity vs. Splunk: SIEM Head-to-Head. EWeek N.PAG.

William Newhouse, Stephanie Keith, Benjamin Scribner, Greg Witte (2017) National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-181, Rev. 1, https://doi.org/10.6028/NIST.SP.800-181