Command and Control – Revisiting EATPUT as an IS Model for Understanding SIEM Complexity

Anthony Serapiglia
Anthony.Serapiglia@stvincent.edu
CIS Department
St. Vincent College
Latrobe, PA 15650

Abstract

Automation of network security systems has led to ever increasing complexity and opaqueness. Ceding command and control actions to systems that are fully or even partially unknown to administrators can lead to possibly catastrophic results. Theoretical abstract models can aid in gaining visibility and insight into the construction and operations of these systems. This paper will utilize the early command and control information system~~s~~ model EATPUT to allow a better understanding of the stages and operation of a modern Security Incident Event Management (SIEM) system.

Keywords: EATPUT, Information Systems, SIEM, Cybersecurity Models

1. INTRODUCTION

The "4 V's" of Big Data – Volume, Velocity, Variety, and Veracity (Cerniauskas, 2022) also affect the practice of cybersecurity. The past several generations of computing have all seen paradigm shifts in these areas that have demanded change in how hardware, software, process, and people deal with the deluge. Much of this change has been to increase automation and look to solutions of scale that can respond to events in real-time (Andrade & Tores, 2018). This has led to ever increasing complexity and "black box" solutions that do not allow for much, if any, visibility of the system to administrators or end users. While this may be convenient in terms of end users who just want working systems and protection and are little concerned with what is under the hood, for system designers and administrators the lack of visibility is a vulnerability itself.

Projecting to abstract models is an accepted and time honored method of systems analysis and understanding of complex systems (Dorodchi et al., 2021; Thomas et al., 2021). As cybersecurity systems have evolved to adapt to the increasing demands of the current environment, what were once stand alone and isolated components have developed into integrated solutions with a much broader scope of engagement. Security Incident and Event Management (SIEM) systems are the current standard for a robust and comprehensive security solution. Combining elements of network and end host security solutions, the SIEM can extend tentacles into every element of a system to include cloud, data center, workstation, and mobile systems and devices. The SIEM is the essential "Command and Control" nexus for administrators and cybersecurity operations of today. Many current SIEM solutions include aspects of artificial intelligence and machine learning to automate response to detected suspicious activity. If this essential activity of command and control is being allocated to automated systems, those systems should be completely understood and known to those who are administering them. Unfortunately, with the increased complexity of these systems, this is often neglected out of difficulty or ignorance.

The purpose of this paper is to highlight how an abstract information system model can be used to project the components and actions of a modern SIEM to allow for insight and visibility into the system so that the "system" can be "known"

and more effectively configured and optimized, especially for student unfamiliar with the system.

An early model of a command-and-control Information System, EATPUT, will be used. This model was developed in the early 1960s as part of foundational efforts in defining Decision Support Systems (DSS), Advanced Data Information and Knowledge (ADIK) systems, and the field of Information Science (NATO Advanced Study Institute in Information Science, 1974). The acronym EATPUT represents an information system defined by the focus areas of Event World, Acquisition, Transmission, Processing, Utilization, and Transfer. Having origination ties to the development of military command and control systems, EATPUT is an ideal candidate model to allow insight into the complex SIEM systems of today.

2. AN EVOLUTION OF VISIBILITY

Network Security provides an area for a stark example of the progress in the evolution of Cybersecurity as technological advances in both hardware and software have allowed more automated solutions. In *The Cuckoo's Egg* (1989) Stoll provides a view into how a network intrusion could be detected and traced in a time before the commercial Internet of today. In it, Stoll describes a process of data capture in which he manually connected teletype machines and printers to modem lines in an effort to capture traffic generated by an intruder to the system. By the end of the 1990's, Intrusion Detection Systems (IDS) were common in most consumer grade router equipment. But just like the efforts of Stoll in the 1980s, all of those logs were meaningless unless someone laid eyes on them and took action on what they saw. With an ever-increasing volume of data leading to ever increasing volumes of logs, the workload quickly overcame the ability of humans to lay eyes on everything.

IDS/IPS

Enter the Intrusion Detection System (IDS). As detection systems continued to develop and gain sophistication, they became very proficient at being able to identify threats on multiple platforms from in the network stack to an individual host. Unfortunately, seeing an attack as it occurs is one thing; stopping it is another. Preventing downtime is one of the highest priorities of any administrator (See the "A" in CIA…), in the end, an IDS on its own often does little to meet this demand. As features continued to be added to these systems, however, their ability to react also continued to grow. Early advances led to the ability to simply reset a connection or blacklist an originating IP Address. While effective in a short window of an attack in progress, these are inherently reactive responses and are easily worked around by a persistent or intelligent threat actor. However, anything more sophisticated requires more logic and also more data, requiring deeper packet inspection which in turn requires more horsepower from the networking equipment. Access Control decisions made by firewall/router devices began to be informed by the greater insight provided by the deeper inspection of packets on the IDS side. Equipment manufacturers eager to move on from a product line that was seen as insufficient were quick to brand a new product line – the IPS (Gartner, 2016). An Intrusion Prevention System (IPS) is an in-line networking product that focuses on identifying and blocking malicious network activity in real time (Fuchsberger, 2005). With the pace of development spurred by the appearance of more cyber threats in the early 2000's, nearly all modern router devices began to contain an integrated firewall feature expanded to include some IPS components in the system by 2005, according to the Gartner Group, as they termed the solution the Next Generation Firewall (NGFW) (Hils, 2015).

Much has changed in the threat landscape in the past 20 years. To borrow a phrase, the landscape is 'everything, everywhere, all at once.' While "visibility" into network traffic has always been a challenge, even dating back to the era of Stoll and his typewriters hooked to modems, the challenge facing administrators of this current system evolution is the need to have visibility, really, for everything – everywhere – and —all at once. Distributed systems have placed devices, processes, storage, and vulnerabilities across the globe and into the cloud. Tracking traffic and threats must happen in all of these places. The "in-line network appliance" can only see so much. To gain full insight and vision into a modern system, agents, clients, daemons, widgets must be integrated into end-user devices and applications at all levels.

How to be everywhere?

Security Incident and Event Management (SIEM) systems are a solution that helps organizations recognize potential security threats and vulnerabilities before they have a chance to disrupt business operations. It surfaces user behavior anomalies and uses Artificial Intelligence to automate many of the manual processes associated with threat detection and incident response and has become a staple in modern-day security operation centers (SOCs) for security and

ISSN: 2473-4901
v8 n5771

compliance management use cases (IBM, 2022). SIEMs have matured to become more than just log management tools. A modern SIEM offers advanced user and entity behavior analytics (UEBA) leveraging the power of Artificial Intelligence and machine learning. A SIEM is a highly efficient data orchestration system for managing ever-evolving threats as well as regulatory compliance and reporting that can function across locations, networks, and device infrastructures. A SIEM system gathers data from many sources, correlating all the available information available. This lets it not only detect active threats but find hidden weaknesses and threats. Its inputs include system and application logs as well as live IDS and IPS data.

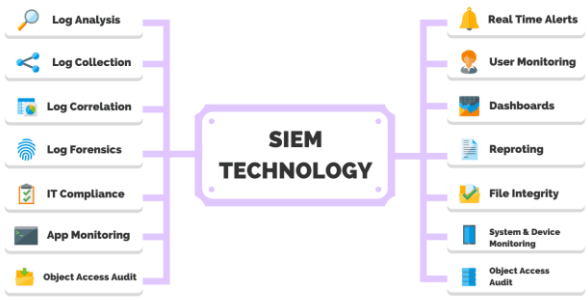

Figure 1 – SIEM Model (Firch, 2021).

The core capabilities of a SIEM include: log event collection and organization including contextual data sources; the ability to analyze log events and other data across disparate sources; operational capabilities such as incident response, dashboards, and reporting; support for threat detection; and compliance commitments including security incident reporting for management.

Implementing SIEMs at the highest level has allowed many security controls to be automated within organizations. This automation has allowed faster reaction times to threat actors achieving more efficiency in Information Security management overall. The inclusion of automation tools has reduced the complexity of command chains that are often involved in the response process (Montesino, Fenz, & Baluja, 2012).

3. EATPUT

Dr. Anthony Debons was an experimental psychologist and early pioneer in Information Science. Debons worked closely with the Army Air Corps and US Air Force in the years after World War II developing command and control systems. These were heady days of advancements in Information Systems, Decision Support Systems, and ADIK (Advanced Data Information Knowledge) systems. While these specific labels may have gone out of favor, their core simplicity in structure and framework is worth revisiting as models for modern "complex" systems.

Beginning in 1960, Debons led a project to establish a conceptual framework for the design of an information system to support command and control for the Strategic Air Command. This project was a contemporary of the time of the group led by J.C.R. Licklider at DARPA, with Debons and Licklider both having backgrounds in psychology and wide interdisciplinary views of information systems. According to Debons, they conferred on a number of occasions at the time, including consultations on funding devoted to projects to develop better software and to train more computer programs that would benefit both of them (Asprey, 1999). These efforts in developing command and control systems for the military had great influence on the development of early management information systems and decision support systems leading to Management Information Systems of today (Asprey, 1999).

Command and Control

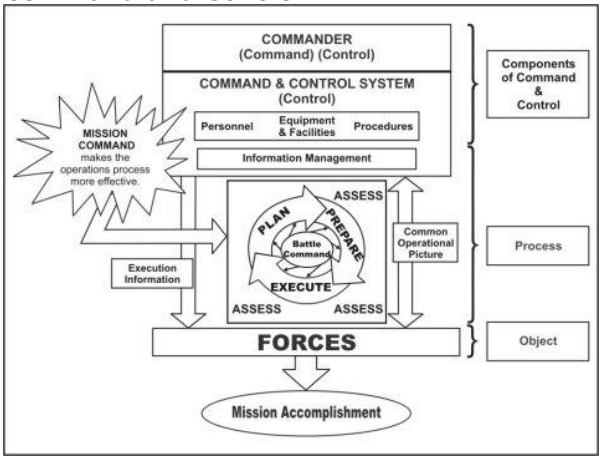

Figure 2. Command and Control (US Department of the Army, 2003).

It was during his work with the Strategic Air Command that Debons and his team of junior officers developed an intellectual framework for the structure of a hypothetical information system. There was agreement that the computerization of a command-and-control system might be considered as an information system (Aspry, 1999). As such "…the science and technology related to the command-and-control functions is primarily directed in achieving one objective, namely, aiding man to make the best use of the data about his environment for decision

making (Debons, 1971).

"Command and control is the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of a mission. Commanders perform command and control functions through a command-and-control system" (U.S. Department of the Army, 2003).

Three characteristics of effective command and control are: ability to identify and react to changes in the situation; ability to provide a continuous, interactive process of reciprocal influence among the commander, staff, and available forces; and ability to reduce chaos and lessen uncertainty.

The Model

The generalized Information System model that Debons arrived at is known as EATPUT. Consisting of six basic components, the first letters of which produce the acronym. The six components of EATPUT are:

Event World – The occurrences that are relevant to the objective and functioning of the information system. It includes the classifying and categorizing of events and the representation of them in symbolic form.

Acquisition – The initial physical component of the system, used to capture matter and energy describing an event from the external environment (data).

Transmission – The actual movement of signals (data) within and between components of the system.

Processing – The ordering, storage, and retrieval of data for the ultimate purpose of applying it to problem solving, decision making, or general development (knowledge formulation).

Utilization – The component that represents the evaluative, interpretive requirement of information systems

Transfer – the action component of the system; the implementation of the decider function through the system's transfer medium. The Transfer function in this model can be seen as communication or information transfer (Debons, Horne, Cronenweth 1988).

As a model, there are obvious similarities to computing models that were contemporary of the time, such as a simplified Von Neumann model of Input – Processing – Storage – Output construction. However, Debons refused to be constrained by restricting his model to computer constructs. S.J. Keyser, a former Rhodes scholar and specialist in linguistics was part of Debons's team in the early 1960's with the US Air Force. It was Keyser who introduced the idea to Debons that human beings existed as information systems. An organism, such as a human, had all the necessary functional elements to form an information system. The integration of human factors into the theoretical work of constructing an automated information system was novel at the time. According to an interview with Debons in 1988, "Command and Control had not achieved a synthesizing construct. The major concept of command and control rested on computer development to support machine data processing – given presence through the electronic display technology. The basic fallacy of this construct was its lack of attention to the role of sensors, teletransmission, and other technological constituents that assume presence to augment human organismic capabilities" (Aspray, 1999).

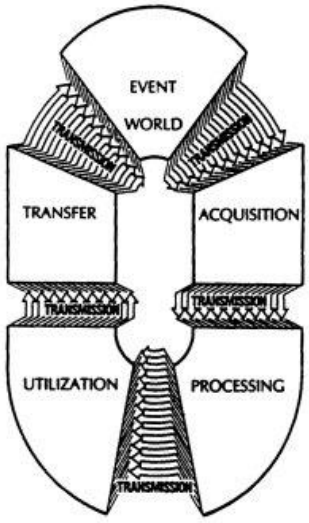

Figure 1 EATPUT as a cyclical model (Debons, Horne, Cronenweth 1988).

4. SIEM – C&C – EATPUT

A SIEM system can be one of the most complex components of a layered cybersecurity solution. Even in the most basic of implementations, a SIEM aggregates log data, security alerts, and

event logs from multiple different devices from multiple different manufacturers, utilizing multiple different protocols into a centralized platform to provide real-time analysis for security monitoring (Gast, 2021). Next-Gen SIEMS are already in place that are leveraging AI techniques with User Entity Behavior Analytics (UEBA) to automate sophisticated responses to detected deviations from standard baseline operations (Cooper, 2022).

Given this level of complexity, it is no wonder that many students view the SIEM as a black box without actually understanding the inner components. Yet it is that complexity that can be utilized in cybersecurity education as an evaluation tool in gauging the student's depth of understanding of systems, their components, interactions, and complexity. "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" (MacDonald, 2020.)

One of the driving factors of Debons' work of the 1960s was Electronic Systems Command. As part of the Strategic Air Command, this early work on Information Systems led to command-and-control systems that helped to prevent a nuclear holocaust during the Cold War. When comparing the stakes, securing a corporate system is not quite on the same level as preserving humanity. However, the comparison holds in looking at the generalities of the complex event environment, range of possible input data, need of data processing/analytics, tuning and validation of possible responses, and the transfer of a probable solution out of the system and into the hands of an entity that can take action. Projecting a SIEM to EATPUT is possible, and natural.

SIEM to EATPUT

Mapping the concept of a modern SIEM to a foundational model of an information system such as EATPUT is a valuable exercise that can help identify gaps in a student's understanding of the complex system. The six components of the EATPUT model easily map intuitively to the components and stages of operation of a SIEM. This projection can be utilized as an instrument to aid in a systems analysis assignment.

To begin, it is important to recognize from the outset that a SIEM is an information system whose purpose is to aid decision making in responding to security events. Stating this from the start establishes the premise and can act as a type of hypothesis statement that is then proven through the subsequent mapping of components and actions to the stages of EATPUT. The event world of a Cybersecurity landscape is endless. The system is always bigger than one thinks it is. Yes, it runs from the known knowns to the unknown unknowns. A SIEM will exist within a network. It will be up to the administrator to establish the scope of the environment that the SIEM will be monitoring. Understanding the "Event World" of the specific environment will inform the extent to which the SIEM should extend. This is not about identifying all potential threat actors or even threats. It is about identifying the assets within your network and work environment that will need to be protected. You cannot protect it properly if you do not know it exists.

One of the key differences between the modern SIEM and traditional IDS/IPS is positioning. IDS/IPS are primarily found in line with the networking stack. More software solutions have been implemented as a part of all-in-one protection suites, but the primary positioning is away from the user and at the border of the network. As an administrative tool, pieces of the SIEM can exist anywhere. The more devices and locations agents and probes can exist, the more robust the SIEM can be. The more data a SEIM collects, the more insight it can provide. The "Acquisition" stage of EATPUT is the piece of the model that focuses on the need to bring representations of activity in the Event World into the system. SIEMs have been able to flourish in an environment of greater interoperability. For generations, many device manufacturers were very proprietary with their products. Management tools and dashboards had to be from within the family of products. Open-source platforms and standard protocols have led to a greater ability to reach to many different areas within your environment. Many open source SIEM products exist that will enable the collection of event logs and data from Microsoft, HP, Dell, and even Apple products.

The word system has a natural inference that multiple components exist. If there are multiple components, then it is necessary that those components must be connected. If lines of communication have not been intentionally established, then it cannot be assumed that they exist. There are a number of communication and networking protocols to allow for data transfer

today. From protocols such as SMB, SNMP, TCP/IP, UDP – all can facilitate background data transfer locally or across distributed systems. Ethernet, Wi-Fi, 5G Wireless data, Bluetooth – all can serve as a channel of communication between devices and collection points. The ability to move data has never been more robust in capacity, speed, or flexibility. The key in the "Transmission" phase of EATPUT theoretically and a SIEM practically is that connectivity between components is addressed. Even with all of the options available, too often this stage, or component, is just assumed to be in place. Often it is too late when it is discovered that it has been ignored or put on the back burner and forgotten. This can lead to costly overruns in time and budget while a possible workaround is devised, if one is even possible.

The "Processing" stage in both EATPUT and within a SIEM is very direct. It is the logic component of the SIEM where data is massaged, sorted, shifted, and otherwise worked with. The intelligence of the application is located here. This is the collected and customized set of rules that have been created to interpret the data. Concrete rules, adaptive logic, heuristics, and now some form of Artificial Intelligence can all be combined to identify threats and possible reactions. It is important to note, the result of processing is a possible solution to the problem or issue at hand. The result of processing is not the end – it is a stage. More needs to be done with the possible solution before it can be moved outside of the information system/SIEM and applied in the Event World.

The "Utilization" stage of EATPUT can be looked at in two different ways. From the perspective of working with the possible solution – this is a moment to remember that at this stage the possible solution is still within the system. This is a "check your work" break point opportunity to do some validation and verification of the result of processing. At this point, there is a possibility to spot-check the possible solution to ensure that it is at least in a range of feasibility. If a program is intended to be a calculator and the result of processing 2+2 is Blue – then there is no sense forwarding the possible solution outside of the system for action as it is not a feasible or viable solution to the question. In terms of the SIEM, this stage can take the form of validation of alarms and the tuning to behavioral norms for the system and environment.

From a systems builder point of view, utilization can be a reminder that every component of the system is being utilized. There has been no superfluous junk included, that the system is as compact and eloquent as possible. This is important in multiple ways. It first ensures there has been no wasted time, effort, or expenditure. It also ensures that there are no orphaned components that have been left on the side and forgotten. These are the components that may never be updated and may not even be monitored. They become a security vulnerability in their own right. In constructing a SIEM, whether open-sourced or purchased off the shelf, it can be easy to get distracted by the bells and whistles, all of the add-ons that sound great but may never be used. A SIEM system designer/implementor should build in only necessary components. Future proofing is not necessary. A good SIEM design should be flexible and the ability to bolt on extra agents or data inflows should be a painless process as needed.

A possible solution cannot be put into action until it is transferred out of the system. This is the "output" equivalency of the general computing model. Unless there is some mechanism included to display, print, or otherwise pass on a result of processing to the event world, it can never be acted upon as it would simply stay within the system and a user may never even be made aware a situation existed that needed addressing. In terms of the SIEM, this may be autonomous action through APIs and control agents, or alerting to administrators who may evaluate and determine action to maintain a layer of human decision making within the chain of command. "Transfer" does not have to be direct action, though direct action can be combined with notifications and recommendations. If a malware detection piece of a SIEM identifies that a specific workstation may have downloaded a malicious file, a robust and integrated SIEM system may quarantine the workstation by disabling the network interface card/Wi-Fi adapter on the workstation, disabling the port on a physical switch that the workstation may be attached to, begin a full anti-virus scan of the workstation, trigger an alert to a SOC/NOC/Network or Systems Administrator for follow-up and an alerting screen and messaging to the user that their workstation is temporarily out of service until cleared by the administrators.

5. CONCLUSION

In combating cybersecurity threats, network and systems administrators must employ ever more sophisticated approaches and information systems that allow for command and control over their network and computing environments. Increasingly, these systems are becoming more

and more automated to allow for quicker response times to an exponential growth in data traffic, the increase in attack vectors, and the growth and variety of threat actors. An unfortunate side effect of automation is often a lack of transparency into the complex automated system (Creel, 2020). For those on the front lines using these systems every day, their intimacy allows some to eventually know every aspect. For students and beginners who have limited or no hands-on experience with these complex systems, the challenge of understanding their intricacies and parts is compounded and can be overwhelming (Sterman, 1994). By utilizing abstracted models and projecting the components and action of an automated system to it, it becomes easier for neophytes to understand and can lend to more insight in developing and optimizing the system for those familiar with it.

The EATPUT model was originally devised by Debons through work in developing Command and Control systems for the United States Air Force Strategic Air Command. It is a model that can be used in the current digital landscape to allow greater visibility and understanding of complex cybersecurity systems such as a SIEM. It allows for segmenting each stage of the process flow: identifying the scope of the environment; intake of data; movement of data within the system; processing to determine a possible solution; validating the system and solution; and transferring actionable intelligence back into the environment. A SIEM system is a command-and-control system. To be as effective as possible it must be understood on both a direct practical level, as well as conceptually and logically – especially as they evolve to include more Artificial Intelligence and direct-action components. Utilizing EATPUT as a conceptual model can allow for a direct systems analysis process and afford a greater understanding of the modern SIEM system.

9. REFERENCES

Andrade, R., & Torres, J. (2018). Enhancing intelligence SOC with Big Data Tools. 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON). https://doi.org/10.1109/iemcon.2018.8614779

Aspray, W. (1999). Command and control, documentation, and library science: The origins of information science at the University of Pittsburgh. IEEE Annals of the History of Computing, 21(4), 4–20. https://doi.org/10.1109/85.801528

Černiauskas, J. (n.d.). Council Post: Understanding The 4 V's Of Big Data. Forbes. Retrieved September 15, 2022, from https://www.forbes.com/sites/forbestechcouncil/2022/08/23/understanding-the-4-vs-of-big-data/?sh=7320be6d5f0a

Cooper, S. (2022, May 2). 6 best next-gen siem. Comparitech. Retrieved June 9, 2022, from https://www.comparitech.com/net-admin/best-next-gen-siem/

Creel, K. (2020). Transparency in Complex Computational Systems. Philosophy of Science, 87(4), 568-589. doi:10.1086/709729

Debons, A. (1971). Command and Control: Technology and social impact. Advances in Computers, 319–390. https://doi.org/10.1016/s0065-2458(08)60634-8

Debons, A., Horne, E., & Cronenweth, S. (1988). Information science an integrated view. G.K. Hall.

Dorodchi, M., Dehbozorgi, N., Fallahian, M., & Pouriyeh, S. (2021). Teaching Software Engineering using Abstraction through Modeling. Informatics in Education, 515–532. https://doi.org/10.15388/infedu.2021.23

Firch, J. (2021, July 23). Siem vs ids: What's the difference? PurpleSec. Retrieved July 11, 2022, from https://purplesec.us/siem-vs-ids/

Fuchsberger, A. (2005). Intrusion Detection Systems and Intrusion Prevention Systems. Information Security Technical Report, 10(3), 134–139. https://doi.org/10.1016/j.istr.2005.08.001

Gartner_Inc. (2016, September 20). Defining intrusion detection and Prevention Systems. Retrieved July 11, 2022, from https://www.gartner.com/en/documents/3449317

Gast, K. (2022, April 29). What is Siem? and how does it work? LogRhythm. Retrieved June 11, 2022, from https://logrhythm.com/blog/what-is-siem/

Headquarters, Department of the Army. (2003). Mission Command: Command and Control of Army Forces (FM 6-0).

Hills, A. (2015, December 29). For 2016, Should We Retire the "Next Generation Firewall"? [web log]. Retrieved March 2, 2022, from

https://blogs.gartner.com/adam-hils/for-2016-should-we-retire-the-term-next-generation-firewall/.

MacDonald, M., Pike, D., Pike, R. (2020). Exploring Depth in Cybersecurity Education Through the Lens of a SIEM, 2020 Proceedings of the EDSIG Conference ISSN 2473-4901 V6 n5327, November, 2020.

Montesino, R., Fenz, S., & Baluja, W. (2012). Siem-based framework for Security Controls Automation. Information Management & Computer Security, 20(4), 248–263. https://doi.org/10.1108/09685221211267639

Quigley, E. J., & Debons, A. (1999). Interrogative theory of information and knowledge. Proceedings of the 1999 ACM SIGCPR Conference on Computer Personnel Research - SIGCPR '99. https://doi.org/10.1145/299513.299602

Stoll, C. (1995). The Cuckoo's Egg: Tracking a spy through the maze of Computer Espionage. Doubleday.

NATO Advanced Study Institute in Information Science, & Debons, A. (1974). Information science: Search for identity : proceedings of the 1972 NATO Advanced Study Institute in Information Science held at Seven Springs, Champion, Pennsylvania, August 12-20, 1972. New York: M. Dekker.

Sterman, J. D. (1994). Learning in and about complex systems. System Dynamics Review, 10(2-3), 291–330. https://doi.org/10.1002/sdr.4260100214

Thomas, P. J., Patel, D., & Magana, A. J. (2021). Characterizing Student Proficiency in Software Modeling in Terms of Functions, Structures, and Behaviors. ACM Transactions on Computing Education, 21(3), 1–25. https://doi.org/10.1145/3458039

What is Security Information and Event Management (SIEM)? IBM. (n.d.). Retrieved June 6, 2022, from https://www.ibm.com/topics/si