Progressing from the SOC to the EOC

Emergent Research Forum (ERF)

Nathan Pike
Cal Poly Pomona
ndpike@cpp.edu

Ronald E. Pike
Cal Poly Pomona
rpike@cpp.edu

Abstract

This paper leverages the many advances in information systems security management and applies them to broader organizational needs. Specifically, SIEM (Security Incident and Event Management) systems collect log data pertaining to security and uses data science tools ranging from business intelligence, machine learning and artificial intelligence to glean useful insights. The paper explores the potential to apply the data collection and processing capabilities of SIEM platforms to KPIs in the healthcare sector to provide managerial insight into a wide range of organizational processes.

Keywords

Software defined networks (SDN), NFV, SOC, EOC, KPIs.

Introduction

The recent move toward cloud computing along with software defined networks and network function virtualization have completed a decades-long process of virtualizing the information technology platforms of organizations. This paper argues for a subsequent evolutionary change in security, compliance and organizational performance monitoring that leverages modern computing architectures. Such computing architecture provides for centralizing comprehensive data that when analyzed using modern data science infrastructure offers exciting new insights into cyber security as well as physical security and KPIs within the organization.

This paper starts with four research propositions that lay out the pathway the researchers are following in the development of an extended research program. A hybrid-cloud data center is in place to test and experiment with cloud architectures with the four propositions representing initial research projects. The purpose of this paper is to theorize regarding the synergistic effects of these sets of changes and lay a groundwork for the interconnectedness of these separate research projects. A brief review of pertinent literature is offered followed by an extended review of the concepts driving the research program. One of the authors has five years of experience as an ERP business analyst and is working in the healthcare domain so healthcare is used as an exemplar to show potential impacts of the theorized systems. While the outcomes are valuable to a wide variety of industries and market sectors, it is clear that these outcomes have greater value to industries that operate with extensive regulatory oversight.

Research Propositions

Proposition 1: The complete virtualization of IT infrastructure, coupled with data science capabilities such as machine learning and artificial intelligence, allow organizations to monitor information systems in a comprehensive manner.
Proposition 2: Modern SIEM platforms, infused with log data from across the IS domain, provide a platform for viewing organizational security and compliance in a holistic manner.
Proposition 3: The modern Security Operations Center (SOC) utilizing a SIEM with information from across the organization (cyber security, physical security, ERP, etc.) could transform into an Enterprise

Operations Center (EOC) that monitors KPIs across the organization in addition to physical and cyber security outcomes.
Proposition 4: Ingesting data from all systems across the IS domain into a SIEM, and monitoring business KPIs as well as security outcomes, will allow and EOC to provide more broad and powerful security and compliance outcomes.

Literature Review

Cloud Computing

Cloud computing has been perhaps the most researched topic since the introduction of the Internet and the World Wide Web. Cloud computing continues to evolve and provide an expanding portfolio of capabilities. NIST Special Publication (SP) 800-145 defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Mell & Grance, 2011, p. 2). NIST SP 800-145 defines four cloud computing deployment models including hybrid-cloud, which is "a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability" (Mell & Grance, 2011, p. 3).

Software Defined Networks (SDN)

Software Defined Networks (SDN) require little introduction as they have been the focus of significant academic research and industry activity over the past decade. Readers wanting to learn more about the technical contributions of SDN may wish to review the work of Kreutz and colleagues who provide an excellent survey of the topic (Kreutz et al., 2015). Network Function Virtualization (NFV) provides automation/control functions in an SDN environment, and usher in an entirely new set of capabilities in IT infrastructure.

Traditional computer networks are growing increasingly insufficient as needs for agility, scale, virtualization and automation in communications networks continue to rise. New topics such as the Internet of Things (IoT), service function orchestration, correlation between events, replication and end-to-end reliability require automation and integration with the rest of the IT infrastructure, which is made possible with SDN and NFV (Bijwe, Machida, Ishida, & Koizumi, 2017; Casellas, Vilalta, Martínez, & Muñoz, 2017; Jadhav et al., 2017; Theodorou & Mamatas, 2017; Wen, Yu, & Du, 2017).

Security Information and Event Management (SIEM)

A SIEM solution provides an organization with a centralized method of monitoring security needs and the activities of users (Michelberger & Dombora, 2016). A SIEM ingests log data from disparate systems across the IT infrastructure such as servers, routers, firewalls, desktop computers and even mobile devices. The SIEM platform applies data science tools such as artificial intelligence to analyze the ingested data to ensure that activities on the systems are consistent with the organizations policies, develops compliance reports and sends alerts when activities deviate from expected outcomes. Many organizations and industries utilize SIEM systems; however, we will focus on the healthcare industry as one of the author's works in healthcare IT and this study is a step toward a larger project aimed at this industry sector.

In an interview, Patrick Voon, CISO at Loma Linda University Health, shared insights into the operations and threats facing the healthcare industry. Patrick stated that one of the largest issues facing the healthcare industry today is ransomware. Ransomware often infiltrates an organization's network using a method called phishing and is a particular threat to healthcare facilities given the highly sensitive data on their systems. Another threat to the healthcare industry is the protection of Patient Health Information (PHI). Healthcare organizations must be careful to restrict PHI to only individuals with a need to view it and track any each occurrence of access for compliance reporting given the scope and complexity of the security and organizational factors related to data breaches in healthcare (McLeod & Dolezel, 2018).

Security Operations Center (SOC)

SOCs are the lifeblood of an organization's security operations. Within the SOC, one will find many different security tools, and typically, the backbone of the SOC is a SIEM platform. All of the organization's compliance and monitoring tools will feed into the SIEM, which reports on operational status. Monitoring is becoming increasingly sophisticated with artificial intelligence (AI) playing an increasing role in supporting SOC operators (JASK, 2018; Montesino, Fenz, & Baluja, 2012). Patrick Voon indicated that the trajectory of the SOC for healthcare is moving towards a Managed Service Provider (MSP) model in the near future as the cost of maintaining a SOC is high and there are formidable challenges when trying to find the talent pool needed to operate a SOC effectively (Voon, 2019). A managed service provider would reduce the burden related to operating the SOC and would provide the organization with access to a larger pool of talent when handling critical tasks.

Body

In this paper, we contend that the traditional Security Operations Center (SOC) should transform into an Enterprise Operations Center (EOC). We argue that an EOC is a facility that is responsible for monitoring across the organization. This includes the traditional cyber security monitoring activities of a SOC as well as monitoring physical security and operational performance and potential threats. While the EOC would likely be even more costly to operate then todays SOC, it also represents a far greater value to organizations. This move toward a single EOC facility to monitor across an entire organization stems from advances in IT infrastructure and data analytics.

An EOC would require organizations to develop three key capability sets:
- The ability to ingest log data from systems across the IT landscape
- The ability to employ data science tools to make real-time decisions related to stated organization rules
- The ability to push changes to the IT infrastructure in real time to gain or maintain compliance with stated organization rules

An effective EOC would require that an organization develop and deploy definitive rule sets that govern decision-making. Rule sets governing the ways in which IT infrastructure will serve to meet the organizations interests allow data science tools to automate the implementation of changes that serve the organizations interests. Figure 1 highlights the fact that efficiency and effectiveness requires both the virtualization of the IT infrastructure and the effective implementation of data science (AI) tools.

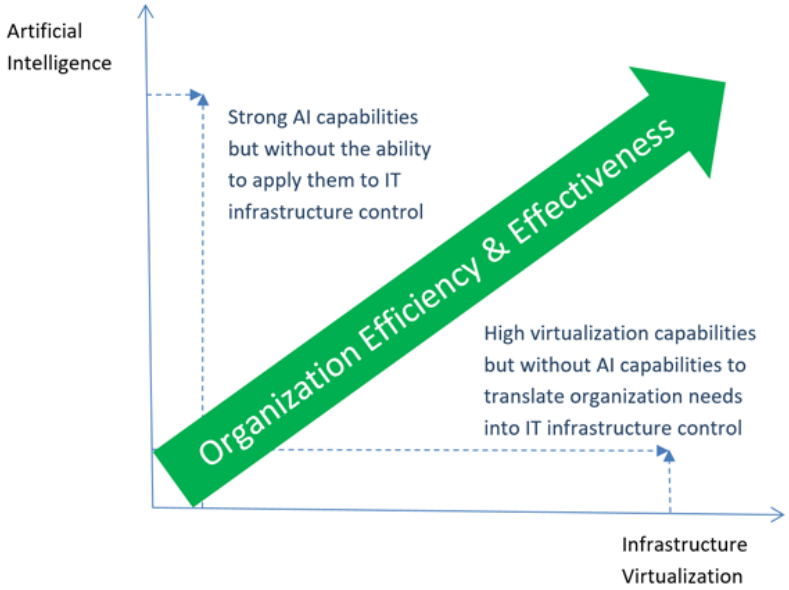

Figure 1: The combined impact of artificial intelligence and the virtualization of IT infrastructure lead to organizational efficiency and effectiveness

The exploration of artificial intelligence capabilities depicted in Figure 1 is beyond the scope of this paper. Instead, this paper focuses on the virtualization of IT infrastructure. Our research program relies upon hybrid cloud as a compute platform and SDN/NFV to abstract and virtualize communications while allowing direct control between the network and the rest of the IT infrastructure.

SDN/NFV is managed through a centralized controller that is able to view and control communications across the entire organization. The controller is also able to be linked to applications and link these users to operations and security needs across the entire IT landscape. Such linkage allows capabilities such as security systems to tie users and their systems access to location, network access, physical security monitoring etc… The impacts of these capabilities may not be initially clear so we offer exemplars from the healthcare industry indicating potential organization impact.

Hospitals with neonatal facilities face the threat of individuals wanting to kidnap a baby from its nursery. Hospitals take significant measures at significant expense to protect newborns, however, staffing irregularities and external activities can draw attention away and create gaps in monitoring. However, IoT devices embedded in the child's wristband and the badges of employees coupled with monitoring of IT systems and wireless controllers in communications networks can track when a newborn is moving and the credentials of the badge of the person moving with the newborn. If the newborn is travelling with an unauthorized person then security systems sound and staff are alerted to the activity. This interaction is made possible by the fact that the hospital's patient records systems, employee records, IoT devices and IT wireless infrastructure each provided real-time data to an artificial intelligence tool that determined the movement of the child did not meet established rules and mitigating action was taken.

IoT-equipped badges also have the ability to sense biometrics of the person wearing it to ensure that a badge in not being used by anyone other than the authorized user. IoT wearable devices also have the ability to monitor biometric attributes of the wearer. The ability to link these biometrics with medical records systems allow an AI system to customize responses. For instance, an accelerating heart rate may trigger an alert earlier for one patient than another given the medical conditions of the patients and the potential impact of an accelerating heart rate. The issuance of an alert is also impacted by whether the patient is lying in bed or walking about the hospital. Once again, the IoT platform, the communications network and the patient records systems each contribute unique information that allow an AI process to determine if an alarm is sounded.

The term Enterprise Operations Center (EOC) is not new and the literature reveals a couple of examples leading toward the concept we are theorizing. One example using the concept of an EOC is the city of Anaheim in California (Barrett, 2005). In June 2004, they created an Enterprise Virtual Operation Center that allows them to centralize the operations of all of the emergency services the city provides to its residents and businesses. Having this capability allows them to create a "war room" like center so they can have Fire, police and ambulatory services respond in a prompt manner. This example only addresses physical security which is one of the three pillars (cyber security, physical security, operational effectiveness) upon which our concept of an EOC is established.

Another example of an EOC that already in place is provided by Diageo Plc and is an Enterprise Operation Center hosting all of the company's accounting, finance, business intelligence, analytics and data services into one area ("Diageo opens fifth enterprise operations centre in Bengaluru," 2017). Diageo Plc is monitoring organizational effectiveness including KPIs, which is another of the three pillars of our concept of an EOC (cyber security, physical security, operational effectiveness).

The third pillar of our concept is cyber security, which is well established in the literature and addressed in the literature review above. The literature review addresses the regulatory compliance requirements of healthcare organizations. Pat Voon mentioned during an interview that Governance Risk and Compliance (GRC) strategy is very important, especially in healthcare. Some aspects to consider in the organization's GRC policies are dashboards & reporting, response strategy and risk assessment. With these strategic needs, it is very important that we consider the capabilities of an EOC and evaluate how a healthcare provider can mitigate their risks. A SIEM platform ingesting data from across the organization and monitoring activities based on established rules, can also be building compliance information in real time.

There are many other examples in which an EOC can improve operations and this is especially true of organizations that operate in highly regulated industries. However, even largely unregulated industries operate with silos leading to inefficiency that would benefit from an EOC.

Conclusion

Software defined networks and network function virtualization are being used in many areas today. Their full potential is only starting to be realized by many organizations. SDN and NFV within in hybrid-cloud computing environment offer an unprecedented ability to leverage data science (AI) capabilities to control operations. We are painting a picture in how these technologies can be used to create an Enterprise Operation Center and boost the overall capabilities and efficiencies of a hospital and organizations across different industries.

References

Barrett, L. (2005). Nothing Goofy about Keeping Disneyland Safe. *Baseline*, (43), 46–47.

Bijwe, S., Machida, F., Ishida, S., & Koizumi, S. (2017). End-to-End reliability assurance of service chain embedding for network function virtualization. In *2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)* (pp. 1–4).

Casellas, R., Vilalta, R., Martínez, R., & Muñoz, R. (2017). Highly available SDN control of flexi-grid networks with network function virtualization-enabled replication. *IEEE/OSA Journal of Optical Communications and Networking*, *9*(2), A207–A215. https://doi.org/10.1364/JOCN.9.00A207

Diageo opens fifth enterprise operations centre in Bengaluru. (2017, February 21). *Mint*. Retrieved from http://proxy.library.cpp.edu/login?url=https://search.proquest.com/docview/1870370498?accountid=10357

HIPAA Forum Boston Helps Health Care Industry Prepare for Medical Records Privacy Rule Implementation. (2002, May 6). *PR Newswire*, p. 1.

IBM QRadar Content Extension for Compliance (Theme) - United States. (2018, June 16). [CT742]. Retrieved February 23, 2019, from http://www.ibm.com/support

Jadhav, V., Kumar, K. N., Alias Rana, P. D., Seetharaman, A., Kalia, S., & Maddulety, K. (2017). Understanding The Correlation among Factors of Cyber System's Security for Internet of Things (IoT) in Smart Cities. *Journal of Accounting, Business & Management*, *24*(2), 1–15.

JASK. (2018). JASK Expands Platform Beyond SIEM to Transform How SOC Operators Visualize Cyber Attacks. *Business Wire (English)*.

Kreutz, D., Ramos, F. M. V., Veríssimo, P. ., Rothenberg, C. E., Azodolmolky, S., & Uhlig, S. (2015). Software- Defined Networking: A Comprehensive Survey. *Proceedings of the IEEE*, *103*(1), 14–76.

McLeod, A., & Dolezel, D. (2018). Cyber-analytics: Modeling factors associated with healthcare data breaches. *Decision Support Systems*, *108*, 57–68.

Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud Computing* (No. SP 800-145). National Institute of Standards and Technology. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-145/final

Michelberger, P., & Dombora, S. (2016). A Possible Tool for Development of Information Security--SIEM System. *Ekonomika*, *62*(1), 125–140.

Montesino, R., Fenz, S., & Baluja, W. (2012). SIEM-based framework for security controls automation. *Information Management & Computer Security*, *20*(4), 248–263.

Theodorou, T., & Mamatas, L. (2017). CORAL-SDN: A software-defined networking solution for the Internet of Things. In *2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)* (pp. 1–2). https://doi.org/10.1109/NFV-SDN.2017.8169870

Voon, P. (2019, February 21). SIEM and Security in Healthcare.

Wen, T., Yu, H., & Du, X. (2017). Performance guarantee aware orchestration for service function chains with elastic demands. In *2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)* (pp. 1–4). https://doi.org/10.1109/NFV-SDN.2017.8169854

Wikipedia contributors. (2019). *Security information and event management* — Retrieved from https://en.wikipedia.org/w/index.php?title=Security_information_and_event_management&oldid=8845314 87