Chapter 9
Socio-Technical SIEM (ST-SIEM):
Towards Bridging the Gap in Security Incident Response

Bilal AlSabbagh
Department of Computer and Systems Sciences, Stockholm University, Stockholm, Sweden

Stewart Kowalski
Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Gjøvik, Norway

ABSTRACT

This article discusses the design and specifications of a Socio-Technical Security Information and Event Management System (ST-SIEM). This newly-developed artifact addresses an important limitation identified in today incident response practice—the lack of sufficient context in actionable security information disseminated to constituent organizations. ST-SIEM tackles this limitation by considering the socio-technical aspect of information systems security. This concept is achieved by correlating the technical metrics of security warnings (which are generic in nature, and the sources of which are sometimes unknown) with predefined social security metrics (used for modeling the security culture of constituent organizations). ST-SIEM, accordingly, adapts the risk factor of the triggered security warning based on each constituent organization security culture. Moreover, the artifact features several socio-technical taxonomies with an impact factor to support organizations in classifying, reporting, and escalating actionable security information. The overall project uses design science research as a framework to develop the artifact.

INTRODUCTION

In this paper, the authors expand on the Socio-Technical SIEM (ST-SIEM) artifact prototype that was first presented at the 2016 European Intelligence and Security Informatics conference (Alsabbagh & Kowalski, 2016). Since then, the artifact has been developed and deployed as an extension to an open source security information and event management system. The design and specifications of the artifact are discussed here to explain its promising contribution in solving a well-known limitation identified in

DOI: 10.4018/978-1-7998-7705-9.ch009

today security incident response practices. The very-well-established Gartner Magic Quadrant report provides an annual state-of-the-art account of the latest SIEM tools capabilities. From the authors' review of the year 2016 report, it was obvious that current SIEMs do not yet consider the socio-technical nature of information systems security for organizations at different maturity levels (Kavanagh, Rochford, & Bussa, 2016). One demanding requirement to improve incident response practice is to provide necessary context reports that adapt the actionable security information to each constituent organization's situation.

Recent research reports from the European Union Agency for Network and Information Security (ENISA) recommend adding more context to the actionable security information to ensure the information's relevance, timeliness, accuracy, completeness, and 'ingestibility' (ENISA, 2015). ST-SIEM addresses this recommendation by taking into account the socio-technical aspect of information systems security at organizations. The security warning technical metrics are now correlated with social metrics which the authors have been developing, to model the security culture of different organizations. This socio-technical correlation is the premise for improving the context provided by actionable security information.

Two social security metrics are currently supported by the artifact: Risk Escalation Maturity Models and Security Spending Mental Models. The first metric measures the maturity of security risks escalation within an organization and how risk information is communicated between the strategic, tactical, and operational tiers of the organization. The second metric assesses the organizational appetite for security spending by measuring how a given security budget is distributed among the primary five security access control categories: deter, protect, detect, correct, and recover. Moreover, the specifications take into account the recommendations from the ENISA (2017) report (A good practice guide of using taxonomies in incident prevention and detection) to further improve the quality of actionable security information. The artifact features a number of socio-technical taxonomies to indicate the impact of a security warning as dependent on the constituent organization's business sector.

SECURITY INCIDENT RESPONSE

Security incident response is concerned with the preparedness, identification, containment, and recovery from security incidents. Developing an information systems security incident response capability is hardly optional for organizations. Without an effective incident response capability, organizations are simply risking their entire business. According to NTT Security's (2016) Risk Value Report, one security breach can cost an organization a financial loss up to USD $10 million and priceless reputational damage which might be impossible to recover from.

Today, to provide security incident response functionality, organizations typically rely on either internal or external security incident response organizations called Computer Security Incident Response Teams (CSIRTs). These organizations function under different categories, depending on their scope of work and the constituents they support (West-Brown et al., 2003). To mount an effective security incident response, CSIRTs need to provide timely and reliable information about existing security threats and incidents. Timely incident response is a requirement critical to enabling organizations to quickly respond to potential threats. Reliable information is required to ensure organizations' staff stay focused on the existing threat risk and avoid confusion and distraction.

For threat intelligence, CSIRTs utilize a variety of tools to collect, prepare, process, enrich, and disseminate actionable security information in a human-friendly format. SIEM (Security Information and