Chapter 18
Mitigating Risk:
Analysis of Security Information and Event Management

Ken Lozito
GSK, USA

ABSTRACT

Business Intelligence (BI) has often been described as the tools and systems that play an essential role in the strategic planning process of a corporation. The application of BI is most commonly associated with the analysis of sales and stock trends, pricing and customer behavior to inform business decision-making. There is a growing trend in utilizing the tools and processes used in the analysis of data and applying them to security event management. Security Information and Event Management (SIEM) has emerged within the last 10 years providing a centralized source to enable both real-time and deep level analysis of historical event data to drive security standards and align IT resources in a more efficient manner.

INTRODUCTION

Security event management and response is something that all IT organizations struggle with due to the multitude of events created by security technologies. Limited resources and tight budgets require organizations to strategically deal with security event data to protect the enterprise’s ‘crown jewels’. Business Intelligence (BI) based technologies, applications, and processes utilized in various industries easily transfer into Security Information and Event Management (SIEM). It is important to first understand the threat landscape that led to the requirement to centralize security event analysis.

DOI: 10.4018/978-1-4666-2650-8.ch018
Over the past few years there has been a growing awareness of internet based threats that could have a significant negative impact to an organization. This increased visibility has been brought to the forefront through numerous embarrassing media stories where consumer data has been compromised and by regulatory mandates that have emerged in the face of major corporate scandals. Further compounding this problem is a steady increase in insider theft of valuable corporate information by unethical employees. A Google search for ‘consumer data theft’ returns almost 7 million results. Among the top results is TJX consumer data theft which disclosed in January 2007 that at least 45.7 million credit and debit cards were stolen by hackers. TJX is the parent company of retailer T.J. Maxx. The theft actually occurred over a period of time from January 2003 – December 2006 and was able to occur due to glaring security holes in the computer systems that process and store payment information (Cheng, 2007). TJX is certainly not alone in this arena where data theft resulted in significant costs both in capital and consumer confidence.

Because the threat landscape for digital assets is constantly evolving and a multitude of security technologies are often deployed to mitigate these threats, a strategy for using the event data from all security technologies should be implemented that is equipped to perform event correlation and provide insight into the internal threat landscape down to the regional level. There is a growing struggle among enterprise IT organizations to manage security risks given the limited resources available. The ability to focus resources by utilizing existing log data to develop more effective endpoint protection policies to protect digital assets is extremely valuable. Most enterprise security technologies have the ability to process their own event logs and export them to an external system. In addition, most vendors of Security Incident and Event Management (SIEM) systems use agents that interface with the management consoles of security software to process the event data from the source system to the SIEM system. It is important to first examine a bit of recent history of security technologies and the threat landscape.

SECURITY TECHNOLOGY—PAST 10 YEARS

Organizations have invested heavily in targeted security solutions including firewalls, VPNs, intrusion detection and prevention systems, and vulnerability scanners. Unfortunately these solutions alone have not been able to completely protect organizations from the evolving landscape of threats. Recently there has been a steady increase in the complexity of threats, including zero day attacks, worms and trojans that span many systems and are difficult to detect using existing security solutions (Q1Labs, 2009a). Many companies have implemented some or all of the following security technologies:

- Network Intrusion Detection and Prevention Systems
- Firewalls
  - Perimeter
  - Application
  - Endpoint
- Antivirus and AntiSpyware
- Host Intrusion Prevention – HIPS
- Behavioral Heuristic Detection
- Information/Data Leakage Protection.

Most of these systems were implemented separately utilizing different vendors with varying logging and reporting capabilities. The common limiting factor for all these solutions is the apparent lack of these technologies to effectively correlate their events with one another, which in turn limits one of Security’s primary roles within an organization, to mitigate risk. Dan Borge states in his book, “The purpose of risk management is to improve the future, not to explain the past” (Borge, 2001). Security Metrics are used to justify