

TRACK: IT Security
SESSION #: IT#6
DATE: Tuesday April 20, 2010
TIME: 9:50-11:05am
SESSION TITLE: "Applying a Pattern-Based Strategy to IT Security and Risk Management"
SPEAKER(S): Mark Seward, CISA – Director of Security and Compliance Solutions
ORGANIZATION: Splunk

ABSTRACT: "Applying a Pattern-Based Strategy to IT Security and Risk Management"

Humans are primarily visual thinkers. We 'see' patterns in our everyday lives and they are imprinted on us from birth. A spate of recent publications (primarily Q4/2009) from the Gartner group on applying a pattern-based strategy to business have offered a new way of thinking about data generated within the business along with business external and internal environmental factors. More specifically a publication called Pattern Discovery With Security Monitoring and Fraud Detection Technologies provided insight into what combination of technologies to use for fraud detection in an enterprise.

Their premise is that by looking for and combining several types of "weak signals of malicious or inappropriate activity that are hidden in the deluge of normal events from the network, systems, database servers and applications," patterns form that can indicate bad (or good) behavior. In interviews with people caught performing insider fraud, most indicated that they started small, got used to doing it, and increased the fraud level over time. There were these weak indicators that when looked at as a pattern it could have been warning signs of bigger things to come. Most of these indicators are in system, database, and application log data. The Gartner Group goes on to recommend that having a combination of solutions – Data Loss Prevention (DLP), Security Information and Event Management (SIEM), and Database Access Management (DAM), to address this problem.

While this premise is sound, the three solutions mentioned above are limited in ways that don't allow the combination to be useful together as a solution. This 'one-plus-one-plus-one' solution doesn't handle or present information in a way that can get you past the sum of it's parts for a variety of reasons not inherent in the solutions themselves but due to cultural silos and lack of interoperability. Also, SIEMs force a number of false choices on a user that in some ways predefines the limitations of the overall solution package. Finally, this three-system picture seems incomplete without the ability to include the forth type of data found in change monitoring/management information. For instance, some insider threats require collusion between someone that can momentarily change the system configuration in a way that allows a third-party to access key data on a system.

Among the SIEM limitations identified are:

- Inability to really scale to see patterns across wide time ranges
- A focus on events coming from traditional security devices or software to the exclusion of data from applications and/or physical security systems
- Inability to weight events based on temporal information, and
- A lack of flexibility to respond to changing business conditions -- M&A activity for example

A secondary set of problems exists around getting people to think through the patterns that can mean nefarious behavior or overall business risk. This means thinking through what-if scenarios that can affect business reputation, top line revenue, and regulatory compliance with an understanding of business systems and processes for a specific vertical.

All of this points to the need to use a single scalable solution that can retain and watch for patterns in real time and alert us to one or more (or a specific set of) 'weak indicators.'

The CIO/CSO along with the CFO will need to be the executive sponsor for Pattern- Based Strategy for Security and Risk with support from each department head. IT operations and security together will enable the strategy in a system that can scale to terabytes of data per day while maintaining situational awareness through continuous monitoring of weak signals that can lead to trouble for the business. Think of this visually as a Vegas slot machine with constantly rotating wheels where you hope a certain set of conditions don't all align for an unwanted jackpot. You may see a few wheels stop at unwanted conditions but you can influence the other wheels to keep spinning while you investigate why the first couple stopped and then get them spinning again.

SPEAKER BIO(S): Mark Seward currently Director of Security and Compliance Solutions marketing has over 10 years of experience in the IT security management profession as a security practitioner and product manager with experience in log management and vulnerability management. Mark has a Masters of Science in IT and a Federal CIO certification from the University of Maryland.