



## **SENSAGE UNVEILS SECURITY INTELLIGENCE CAPABILITY MATURITY MODEL TO BENCHMARK AND IMPROVE ENTERPRISE SECURITY MANAGEMENT**

### ***New Approach Offers Roadmap to Unify and Refine Compliance Monitoring, Real-time Alerts and Forensic Investigation Practices***

SAN FRANCISCO, March 2, 2010 – SenSage, Inc. today announced the SenSage Security Intelligence Capability Maturity Model, a methodology for assessing and improving enterprise decision support practices that support information security and compliance operations. SenSage is introducing and demonstrating the methodology at the RSA Conference, Booth No. 845, at San Francisco's Moscone Convention Center.

The concept of Security Intelligence is best understood by comparing it to business intelligence solutions built atop data warehouses to provide decision support information and context to business managers over the last 20 years. Similarly, Security Intelligence solutions leverage security event data warehouses to provide decision support information and context to cyber-security, risk and compliance managers. However, whereas most business intelligence applications have not progressed beyond periodic reporting and free-form querying, Security Intelligence solutions must combine periodic compliance reporting with real-time dashboards and alerts, rule-based notification mechanisms, and historical forensic investigation.

“We have leveraged SenSage’s ‘Security Intelligence’ approach to converge our real-time alerting, incident investigation and compliance reporting processes,” said Dan Ritari, vice president of enterprise information risk management at Deluxe Corporation. “By deploying SenSage, we have improved our fraud detection capabilities and enhanced our visibility across our entire IT environment.”

The Security Intelligence Capability Maturity Model provides a five-level evolutionary path of increasingly organized and systematically more mature processes, and incorporates nearly a decade of experience that SenSage has developed while providing large corporations with SIEM and log management software to improve security and

compliance management practices. Organizations using the model may pursue advancement in the individual component disciplines – Log Enablement and Management, Compliance Monitoring, Real-time Alerting, Forensic Investigation, and Incident Response – but the greatest efficiency and effectiveness gains are unlocked when all disciplines are pursued in a concerted effort.

The general structure of the model is based on the original Capability Maturity Model developed by the Software Engineering Institute (SEI) to improve the process for developing, acquiring and maintaining heavily software-reliant systems for the U.S. Department of Defense. It establishes a framework for continuous process improvement with explicitly defined requirements.

“Many enterprises are struggling to overcome the internal silos of security technology, information, people and processes that impair their cyber-security efforts,” said Joe Gottlieb, vice president of marketing and business development for SenSage.

“Constrained budgets and reduced headcounts have exacerbated the problem and driven the need to open these silos and adopt more efficient and effective approaches. The Security Intelligence Capability Maturity Model provides a practical methodology to prioritize, plan and measure results in these security and compliance improvement efforts.”

SenSage Security Intelligence solutions include security information and event management (SIEM), log management, and SAP continuous controls monitoring, all supported by a single data management architecture, access model and console. The SenSage Security Intelligence Capability Maturity Model is employed by SenSage Professional Services project teams in baselining and sustaining engagements for SenSage customers.

“SenSage provides a highly efficient and effective way to consolidate real-time and historical log and event management,” said Philip Howard, research director at Bloor Research. “The approach taken fits well with the emerging requirement for “business intelligence for IT” that can serve multiple use cases such as security monitoring, fraud detection, forensic investigation and compliance reporting.”

## **About SenSage**

SenSage®, Inc. delivers Security Intelligence solutions that provide essential decision support to cyber-security, risk management and compliance operations. These solutions enable the necessary convergence of security information and event management (SIEM), log management and continuous controls monitoring through a single console and data management architecture. Over 550 organizations and government agencies around the world rely upon SenSage to combine these functions in support of more holistic IT oversight, real-time alerting and investigation, incident response and compliance reporting. Combining a patented event data warehouse platform and interactive analytics environment, SenSage Security Intelligence solutions are more scalable, flexible and affordable than traditional SIEM, log management and data warehouse point products. SenSage goes to market with industry-leading OEMs and strategic alliance partners including Cerner, Cisco, EMC, HP, McAfee and SAP. Visit [www.SenSage.com](http://www.SenSage.com) for more information.

# # #

**PR Contacts:**

Julia Sinykin  
[The Hoffman Agency](http://TheHoffmanAgency.com) for SenSage, Inc.  
(508) 329-3319  
[jsinykin@hoffman.com](mailto:jsinykin@hoffman.com)

Rozanne Bonavito  
SenSage, Inc.  
(415) 808-5917  
[rozanne.bonavito@sensage.com](mailto:rozanne.bonavito@sensage.com)