

Sensage Study Again Reveals Lack of Consistent Measurement and Process Improvement in Security Management

Security Practitioners Cite Issues With Data Access and Analysis as Key Challenges in Proactive Threat Management; Security Confidence Drops Considerably in 2012

REDWOOD SHORES, CA -- (Marketwire) -- 08/28/12 -- Sensage, Inc., the leading provider of advanced Security Information and Event Management (SIEM) and founder of Open Security Intelligence, today announced results of its third annual industry survey, entitled "The Buried Truth: State of Security Information and Event Management Processes." The study finds a downward trend in IT's ability to consistently coordinate, measure and improve security data management processes, including log management, compliance reporting, real-time monitoring, forensic investigation and incident response -- areas that are critical to sustaining effective Security Intelligence.

While resourcing was cited as a major issue this year, as compared to 2011 results, limited access and poor data fidelity were the top barriers preventing organizations from achieving a more sustainable, consistent security management program. The Sensage report, which analyzes results over a three year period, indicates that the massive (and mostly manual) effort associated with collecting and interpreting security data has created a severe downturn in both the mood of security teams, as well as perception of their effectiveness by stakeholders.

"While many referred to 2011 as 'The Year of the Breach,' we see 2012 shaping up to be 'The Year of Inspection,'" said Joe Gottlieb, CEO of Sensage. "Given the responses highlighting the need for better data access, and revealing inconsistent measurement and process improvements, this year's respondents appear to be much more honest, realistic and self-aware. This is a significant change compared to previous years, as professionals are becoming more vocal about their dissatisfaction with traditional security practices' inability to provide the intelligence necessary to counter evolving threats and address organizations' changing requirements."

The Sensage survey further highlights the demands placed on resource-constrained security teams, identifying a close relationship between the fidelity of security data and work required to analyze and act on information. Many practitioners want more actionable information faster and there is an overall lack of trust in the data they collect. In 2011 and 2012 Sensage asked if respondents needed better data access and analysis:

In 2011, 57% said "Yes" which clearly indicated a prevalent challenge in this area.

In 2012, awareness of this challenge appears to have grown significantly, with 79% noting that they need better data access and analysis.

When studying responses stating that professionals had "inconsistent" and "consistent" measurements and comparing them year over year, Sensage discovered that, while slightly more than 50% of the respondents felt they were inconsistently measuring in 2010 and 2011, 61% shared that challenge in 2012.

This corresponded with a drop in consistent measurement from 31% in both 2010 and 2011 to only 21% in

2012.

When evaluating reports of "light or no measurement" compared to "heavy measurement," the numbers were close year over year, but the trend is going in the wrong direction:

More respondents are taking a light measurement approach -- 75% in 2012 compared to 69% in 2010 and 73% in 2011.

Accordingly, fewer are taking a heavy measurement approach, 25% in 2012, compared to 30% in 2010.

While responses in 2010 and 2011 reflected a close split between those who consider their processes coordinated and those that don't, that was not the case in 2012, where 66% of respondents felt that they were resorting to reactive triage or had no coordination at all.

2010 and 2012 shared a similar percentage of teams who had no proactive process improvement. Inside the numbers, the data yielded troubling findings:

The bad news: A massive drop -- from 18% in 2010 to 5% in 2012 -- of those who felt they had a consistent and adequately staffed process improvement program.

More bad news: When comparing respondents who maintain consistent process improvement, there was a significant drop, from 65% in 2011 to 40% in 2012.

Worse news: 96% of 2012 respondents had no process, inconsistent process or consistent process that was understaffed.

In 2012, Sensage asked a new survey question to gauge how effectively security practitioners felt they were dealing with security risks. Responses were less than ideal:

The majority (78%) feel they are under less than ideal circumstances or improving, but still face a lot of heavy-lifting.

Only 22% of respondents said they were "very effective."

Sensage initiated this annual survey in 2010, and every year since has collected over 350 responses to a set of questions about log management, compliance reporting, real-time monitoring, forensic investigation and incident response processes. The objectives of the survey are to understand how well these processes are working, understand the interdependencies between these processes, and identify barriers likely obstructing process effectiveness.

To download the complete study, please visit:

Sensage®, Inc. helps organizations collect, store, analyze and interpret complex information to identify new threats, improve cyber-security defenses, and achieve industry and regulatory compliance. Sensage serves our customers' most advanced Security Information and Event Management (SIEM), log management, Call Detail Record (CDR) retention and retrieval and Continuous Controls Monitoring (CCM) use cases. Hundreds of customers worldwide leverage patented Security Intelligence solutions from Sensage to effectively identify, understand and counteract insider threats, advanced persistent threats, cyber threats, fraud and compliance violations.

Combining powerful data warehousing with scalable, clustered multiprocessing and robust analytics,

Sensage solutions handle all event data types, scale to petabytes, minimize storage costs and perform sophisticated data analysis. Sensage has achieved Federal Common Criteria and FIPS 140-2 Certification. Sensage partners include Cerner, Cisco, EMC, McAfee and SAP. For more information, visit , follow us on Twitter: @Sensage, and watch for us on .

CONTACT:

Joyson Cherian
703-218-3555

further information:

<http://www.sensage.com>

Diese Seite kommt von

<http://www.firmenpresse.de>

Die URL für diese Seite ist:

<http://www.firmenpresse.de/pressrelease178292.html>