

How to move from a reactive to a proactive state of security information management

As recent threat research from Verizon¹ and Sensage² indicates, many organizations take a siloed approach to five critical security processes: log management, compliance reporting, real-time monitoring, forensic investigation and incident response. Below are ten useful points to help make the move from reactive to proactive:



LOG EVERYTHING

KEEP RAW DATA

CONSISTENCY IS KEY

NO WEAK LINKS

START WEEKLY

LET DATA TALK

NO EXCUSES

FLEXIBILITY IS A MUST

AVOID AUDIT HELL

1 Log everything. This is especially important since you don't always know what you have—or what you will need—in the way of forensic data analysis. Your log management solution should allow you to maintain at least five years worth of event data. This allows you to analyze data over time, for example, identifying a vulnerability that may look new every 90 days but is actually a recurring risk.

2 Maintain fidelity. If the event data you store is not exactly as it was generated, you run the risk of stripping the data down to an unusable form. Ensure that you maintain data in its original form so that you can go back and analyze events as they really happened.

3 Get going. While SIEM technologies seem complex, don't let the technology drive your agenda. It's pretty simple to establish consistent processes for log review and engage in practicing those. Just as we've seen in quality initiatives and business data analysis practices, you can't improve what you don't measure.

4 Avoid weak links. Don't get too fancy in any single area without maintaining consistent vigilance across all areas... just as security defenses are only as strong as their weakest link, security monitoring is only as perceptive as its shortest sight.

5 Don't belittle weekly reviews. While there is much talk about why weekly reviews are not useful, data shows that often threats that evolve over time are not so obvious in the day-to-day analysis. It's in deeper reviews each week or month that you can spot attacks forming over time. Besides, it's a good place to start: if you don't have time for daily analysis, weekly reviews will yield positive results and get you into the rhythm for more frequent reviews.

6 Use data as a weapon. Break down organizational or process silos by using forensic analysis to show where teams can better link together to shore up security practices. Since data can be correlated and analyzed regardless of where it is generated, let it do the talking. It can also be used to show changes to your security posture over time and

help answer questions like “how did this policy change affect our security?”

7 Make no excuses. Just because the events or data is sensitive does not mean you should stick your head in the sand and avoid sharing it with key stakeholders. Access controls exist for a reason—so apply the same model to event data.

8 It's not a “one-size-fits-all” approach. Each team in your organization—from the incident response unit, to the compliance guys, to the domain leads—need to access and analyze data differently. Don't drive the lowest common denominator rule when you don't have to—and certainly, don't make the access or analysis process so complex that only a few experts can get to it. Your security information solution should allow data to be queried and visualized in the context and environment most familiar to your stakeholders.

9 The rearview mirror exists for a reason. If you are only focused on the road ahead, you are missing half the journey. Having a historical reference of your security posture helps you set baselines. Baselines help you highlight variances. Analyzing trends within those variances helps you with predictive modeling, answering questions like “what impact would this security policy have had?”

10 Don't be audit-driven. Why wait to be penalized for not responding to requests about what really occurred? If you can confidently maintain a clear record of your events, suddenly the audit is not so bad.

Sensage Security Intelligence Solutions enable large enterprises and government agencies to coordinate—and even converge—security processes with a single data architecture that scales to petabytes and beyond. If you would like to learn how organizations leverage Sensage to enhance their visibility into security and compliance operations while reducing their costs, please [contact us for a demo](#).