

Agencies are moving 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. Here are ten best practices proactive agencies are employing to manage security information:



LOG EVERYTHING

Log everything. Consider logging any data with a time stamp including security events, call center data, and more. 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 with high data compression rates... but even two years will help analysts account for seasonal variances.

KEEP RAW DATA

Maintain fidelity. Ensure that data is maintained in its original form, particularly when dealing with compliance regulations. If the event data you store is not exactly as it was generated, you run the risk of stripping the data to an unusable form. Raw, clean data lets you avoid unnecessary delays when you need to go back and analyze events as they really happened.

CONSISTENCY IS KEY

NO WEAK LINKS

Get going. The scale of IT data within agencies is massive. It is very easy to quickly become overwhelmed. 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 efforts, you can't improve what you don't measure.

START WEEKLY

LET DATA TALK

Avoid weak links. Within an asymmetric threat environment, consistency is key. 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.

ACCESS CONTROL MAKES SENSE

Don't belittle weekly reviews. Recent insider threat behavior shows that many attacks evolve over time and are not obvious in the day-to-day analysis. While daily log review is a necessary evil, it's the expanded analysis of the landscape over time which often uncovers slow and methodical attacks.

FLEXIBILITY IS A MUST

AVOID AUDIT HELL

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?"

Access control makes sense. 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 security event data.

It's not a "one-size-fits-all" approach. Scale breeds specialization, which often leads to organizational barriers in large government agencies. Every team—from the incident response unit to the security operations team—needs to access and analyze data differently. Create security information management work flows that make sense to your stakeholders.

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 you don't even know to ask.

Don't be audit-driven. Proactive agencies understand the dangers of being audit-driven and, in fact, are driving advanced use cases to stay miles ahead. By maintaining a clear records of events, responding to an audit is not so challenging.

Sensage Security Intelligence Solutions enable government agencies and large enterprises 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 agencies leverage Sensage to enhance visibility into their security and compliance landscape, please **contact us for a demo**.

