Privacy is Not the Enemy of Accountability

When the IT industry discusses compliance, nearly everyone envisions efforts aimed at either retaining records or fortifying customer, healthcare or financial data.

But regardless of your industry, new legislation in multiple corners of the globe now requires special attention to watching the watchers – in other words, limiting what internal security operations center analysts can actually see during the normal course of their log management duties.

GDPR as well as upcoming provisions in the California Consumer Protection Act (CCPA) that are set to go into effect in January 2020, include requirements that organizations protect personally identifiable information (PII) and offer the right to be forgotten – including within log management tools. That translates into a need to keep all data truly private in order to be compliant.

Organizations must be to able remove the identity that is connected to logged actions or data, while retaining the required log data. These requirements are substantial, and the fines are steep for non-compliance. Yet it's a hurdle that hasn't yet received the attention it requires, especially among IT managers and analysts in security operations centers.

And perhaps that's not surprising given the nature of these very specific privacy requirements that actually have just as much to do with what an organization's own security analysts can access as it does with what criminals can get their hands on.

Today, most organizations are not compliant – and the reason is clear. GDPR and the CCPA require that PII is protected and only brought to light when an investigation is required. Without pseudonyms, it is impossible for a log management tool to be compliant, regardless if standalone or part of a SIEM/SOAR product.

And that's where the problem lies: organizations are not using mandated pseudonyms despite the clear fact that pseudonyms are the only definitive security control to implement privacy correctly, in part believing their vendors have integrated these capabilities into their tools.

Alarm Bells Coming from New Source

These new laws don't seek to hamper businesses, and in fact they seek out to make them more ethical and transparent. It's that focus on principles and fairness as well as the associated big fines that make general counsels and chief legal officers among the top initiators who seek to revamp their organization's approach to data privacy and tools such as log management.

In essence, the laws have created a welcomed scenario where the C-suite and legal departments are aligned, ensuring that security operations centers are implementing privacy regulations correctly. Business executives must now pay attention to how IT is protecting privacy rights literally within their business.

This means that general counsels are leading the charge in revamping SOCs to properly handle privacy. Counsels are diving in and quickly realizing that security analysts can often see everything – names, locations, actions, etc.

And that's not permitted given the new rules. Proper data handling shouldn't allow analysts to see someone's identity unless they have the proper grounds and privileges to do so.

Fluency Offers a Proven Path to Compliance

Fluency stands as the industry's only log management offering with correct pseudonyms execution built-in supporting both compliance and privacy laws.

Fluency's log management solution is easily used standalone with its consolidated single-pane-of-glass view integrated into existing SIEM investments rendering them compliant with privacy, storage and real-time tracking requirements.

The Q3 2018 Forrester Security Analytics Platforms report covered current SIEMs and Security Analytic (SA) tools, and noted, "Despite the perennial requirement for compliance, some of the newer SA vendors don't adequately address this use case, focusing on detection instead. This means that S&R (security & risk) pros who invest in these tools will need separate compliance solutions."

Fluency stands as the only solution that complements these existing tools ensuring CISO's meet these requirements. 2019 will quickly begin to expose those IT environments where these requirements aren't implemented correctly – bringing unwanted attention and risk of substantial fines/penalties.

Most cybersecurity insurance policies have clauses that exempt them from paying when laws are not complied with correctly.

Ensuring that compliance and privacy are mapped into existing security plans is no longer an option. The imperative is clear – Do not wait, act now.

"We are a corrupt industry if we keep doing things in a non-private way. Privacy is not the enemy of accountability. SOC's must embrace the use of pseudonyms to properly address today's privacy laws."

Chris Jordan
CEO, Fluency

To discuss a no-cost proof-of-concept, contact:

Collin Miles
collin.miles@fluencysecurity.com
T: (214) 334-2670

Al Wissinger
al.wissinger@fluencysecurity.com
T: (512) 630-8990

Fluency Corp

387 Technology Drive Suite 3119 College Park, MD 20742
www.fluencysecurity.com