A Fluency Success Story

Leading U.S. Insurance Company Looks to Fluency for Threat Hunting Capabilities

American National Insurance Company

Founded in 1905, American National Insurance Company offers both longevity and stability to its policyholders. Standing as the parent of the American National family of companies, American National Insurance Company is headquartered in Galveston, Texas and has more than 3,000 employees in Texas, Missouri and New York. The company's national network of agents stretches across all 50 states and Puerto Rico, and provides service to more than 5 million policyholders.

With a complex network environment, American National prioritizes its ability to proactively seek out potential cyberthreats before they impact its business. Fran Moniz serves as the company's Network Security Architect and is tasked with all network monitoring. In 2015, the company began to look at a number of different SIEM products, but opted to build their own and not buy a SIEM off the shelf.

Moniz said they then needed a correlation engine – and Fluency was exactly that. After meeting Fluency at an RSA Conference and learning what Fluency had to offer, he soon decided on a three-year deal and they've now successfully used Fluency for about two years.

"Fluency was easy to deploy and was relatively painless in regard to integration," Moniz said. "A picture is worth a thousand words – and if you saw the data flow and the amount of data I have going in our environment, you would understand how Fluency helps paint that picture. Fluency does not require us to go write stuff into Splunk to go do it. I use Splunk as my reporting metrics, but from a correlation standpoint I use Fluency because it's a big part of my visibility strategy. There's never going to be a silver bullet, so multiple tools are needed. But with Fluency, I've gained noticeably more visibility."

He continued to explain that Fluency helps transform the members of his Security Operations Center into proactive personnel.

"So, my whole thing is I'm getting people away from just monitoring and instead turning them into threat hunters," Moniz continued. "To understand how to hunt for the APT guys, etc., whether you have them in your environment or not, you have to understand what's going on. Buying a product that just says 'yeah, we've blocked this' but you don't know why you've blocked it – that's not all that helpful. Fluency offers significant visibility, especially via their machine learning. With AI and machine learning, the more data you give it, the better it gets."

He said he's going down the machine learning avenue in order to help and improve his monitors.

"I heard a phrase that was coined some time ago: you take your security professional and you change them into a centaur, which is basically augmenting the monitoring with machine learning," he said. "With Fluency, they become better at their job because you're turning them into a proactive SOC team instead of a reactive team. That's what machine learning can get you if you give it the needed data. The big difference we see with Fluency is that the people in our SOC don't need to go searching for as much data because Fluency provides much of it all in one place. And that's significant for us because it translates into far greater visibility that dramatically increases efficiency."

Fluency is used as a daily tool for Moniz's team of monitors. Moniz said that he also frequently uses Fluency from a forensic standpoint, saying, "It's the first place that I go to when I want to see what's happening with a particular host or IP address."

Moniz added that no one can prevent all attacks, but you must be able to understand what's going on in your environment and be able to identify outliers. "It all goes back to visibility – visibility is absolutely crucial," he reiterated. "And we're happy to have Fluency as one of our key tools."

About American National Insurance Company

American National is a family of companies that has $25.9 billion in assets. American National, founded in 1905 and headquartered in Galveston, Texas, and its subsidiaries offer a broad line of products and services, which include life insurance, annuities, health insurance, credit insurance, pension products and property and casualty insurance. Visit www.AmericanNational.com.

About Fluency

A pioneer in security audit and automation technology, Fluency® delivers unmatched speed, data retention, and storage capacity not available through SIEMs. Some of the nation's leading financial, healthcare, and government entities rely on Fluency's patented technology that unites Artificial Intelligence (AI) and Machine Learning (ML) with the ability to retain and organize data to meet regulations and support investigations in sub-seconds – not minutes or hours. The result is a smarter, continually-improving view of your network, host data and device alerts. Fluency's customers routinely praise Fluency for making data useful while simultaneously offering a uniquely cost-effective subscription-based pricing model with by-default 90-day and 365-day storage options. Founded in 2013 by former McAfee threat intelligence executives, Fluency is headquartered in College Park, Maryland.

Fluency's Decision-Based Approach to Orchestration

We think analytics and not automation. Other SAO products typically focus only on the playbook, chaining integration from one device to another. A pure playbook approach maintains silo decision making that orchestration is meant to remove. Fluency focuses on security analytics, fusing all incoming data, providing a merged view, and assigning risk scores. The focus on the decision is pivotal in preventing the amplification of false positives as well as improper responses to low-risk events.

In order to make decisions, all data must be available. Fluency's cloud analytics comes with the industry's only by-default 365 cold storage. Fluency's enterprise solution also comes by default with 90 days searchable. Not only does this translate into the compliance that's lacking in today's SIEMs, but it also provides true analytics. Fluency is all about making data useful.

www.fluencysecurity.com

Fluency