With Insider Threats, Context is Everything

One of your employees hasn't taken a vacation in two years. Another recently started working at 6 a.m. and doesn't leave until after 8 p.m. Someone else in your organization has changed his or her home address three times this year. You have a contractor whose contract ends in two weeks.

It's not easy to discover the malicious insider. In most organizations, employees are credentialed users of an agency's system and are assumed to be trusted. That's because the prevalent technology used to help pinpoint security threats—intrusion detection systems, data loss prevention systems, security incident and event management tools, anti-spyware software, and data from firewalls, routers and switches—don't provide the context required to know the difference between innocent behavior and the actions of a malicious insider.

You can systematically identify cases of insider fraud by thinking differently about your data and asking the right questions of a big data system that can collect any type of data, even from external publicly available databases. You must combine system, application and log data with data generated from security point solutions and adding contextual data locked in business systems and other third party sources. Then ask the right questions to understand who may be perpetrating fraud.

Context is key to knowing intent. An employee may do something against policy, but may not know he or she is committing an act that could be perceived as a data breach. It's not enough to know that an employee started using printers on another floor or sent a large document to a new address. If you know the employee's credit score dropped 200 points over two months, their home address or banking information changed multiple times in a short period, or they spent hours online researching travel in a specific country, the picture changes.

Finding the smoking gun

Three types of data are required to separate what is normal from abnormal: Statistical analysis that can highlight behavioral outliers; log data, which is the definitive record of machine-to-machine and human-to-machine interactions; and contextual data. Collecting and correlating this data allows you to understand potential motive.

Many agencies already have the technology to do this, whether they realize it or not. Employment agreements give the employer the right to review or gather credit data or data from other publicly available sources.

Splunk, a leading platform for operational intelligence already in use by hundreds of government agencies, is more than just a big data platform that gathers and analyzes a variety of machine and database data. Applying it to this use case and asking the right questions can help you guard against insider fraud.

Splunk software collects, indexes and performs statistical analysis on data sets. For example, an analyst searches for the term "fail" and Splunk returns all data with that word. The analyst then drills into specific sources for more details. He or she also inputs a query to find all failed logins across a specific set of systems from a specific department over a specific time. In one case, an organization

discovered an insider threat during a preliminary proof-of-concept with Splunk Enterprise by first detecting suspicious activity around his communications and then examining his access to a code repository. He was fired.

None of this eliminates the need for monitoring changes of routine, lack of vacation time use (which can mean an employee doesn't want to pass responsibility to another), and emotional and psychological stresses, such as marital status changes. By combining conscious awareness with sophisticated security tools and big data analytics, agencies will make more progress in detecting and mitigating insider threats.