the Viewpoint business

Insider threats pose unique cyber challenge

Q How are insider threats to government different from those in other sectors?

Enoch Long, Principal Security Strategist, Splunk Inc.

A The most important difference is motivation. While the motivations for insider threats in private industry might be financial gain or willful destruction, the biggest threat to government is the conscientious objector—someone who disagrees with an agency's policies and seeks to thwart them. The second biggest insider threat to government is financial; the government also has a lot of private data that could be breached for personal gain. And it can happen to any type of agency as every agency has data that's potentially valuable to private business or to individuals for financial gain or strategic advantage. An agency reviewing drug efficacy, for example, could be at risk of having advanced copies of test results stolen and distributed.

Q Should all agencies attack the insider threat problem in the same way?

A The way of attacking the problem is basically the same, but the groundwork is different, and it's critical. It's important to know what your agency has that is potentially valuable to an insider. To do that, you have to think through what kinds of data a malicious insider would want, along with potential motivators. From there, you can come up with 20 or 30 different kinds of IT risk scenarios that represent actions an insider might take. Only then can you start analyzing the right data and monitoring for the right anomalies in behavior and access.

Q What role does technology play in thwarting insider threats?

A Once you have your IT risk scenarios figured out, technology takes it the rest of the way. The key is big data—all of the data that agencies possess. This data comes from a variety of sources, both structured and unstructured. If you can collect and analyze this data while providing the context necessary to eliminate false positives and unintentional actions, you can more accurately identify possible insider threats. You can better pinpoint and act on what constitutes a real insider threat by combining technology that you already have, such as data loss prevention (DLP) and security information and event management (SIEM), and then complement them with a big data technology that allows you to analyze log data, run statistical analysis and create visualizations.

Q Agencies have a lot of data. Isn't data collection complicated?

A Yes. But big data technology and automation can help. For comprehensive analysis, agencies need to analyze three levels of data. First is machine-generated data that IT collects every day—the credentialed activity of your users. The second level is all of the internal context inside of the agency—things like HR records, time management systems and browsing habits. The third level is other external content that may help you understand what's going on in that person's world, such as what countries they have been traveling to, whether their credit score has recently dropped significantly or whether they are starting their own company.

Q To what extent can the insider threat process be automated?

A Probably about 80 percent can be automated. The rest of it is about setting expectations and enforcing policy and procedures. The first step is developing the policies: what you are going to monitor, how you are going to monitor it, and what the rules are for employees on accessing and sharing information. Next, explicitly spell out and regularly remind people what those policies are. Third, train employees to know the potential signs of a malicious insider by explaining the different types of behaviors in hypothetical scenarios appropriate to your agency.

the Viewpoint technology

Getting the edge on insider threats

Q If government agencies could do one thing to reduce insider threats, what should it be?

A Change their mindsets. To catch criminals, you have to think like a criminal. That requires thinking creatively about how and why someone might want to steal information from your agency. What does your agency have that someone would want to steal? What would their motivations be? How could they do it? With that kind of thinking, an agency will be able to develop IT risk scenarios that represent actions an insider might take, and be on the look out for those specific actions.

Enoch Long, Principal Security Strategist, Splunk Inc.

Q Do most government agencies have the technology they need to effectively deal with insider threats?

A Most have some sort of security information and event management system (SIEM) and a number have data loss prevention (DLP) systems, which are a good start. These systems work pretty well at watching for the transfer of specific types of documents through the network perimeter and being able to audit hosts and desktops to make sure you don't have documents there that are sensitive, but they don't provide enough context to be able to build a case. They get you far enough to understand that you have a problem, but not far enough to help you understand why. This means a lot of potential false positives and a lot of effort to tune the DLP systems to reduce noise. We can't get to root cause analysis without using a big data system to get additional context and perform statistical analysis on the data.

Q What do agencies need to finish the job?

A They need a way to analyze log data and big data, and the ability to run statistical analysis and visualization alongside of that. That's what provides the context you need to find legitimate cases of insider fraud and eliminate false positives. A DLP system, for example, isn't going to take into account whether or not a person changes home addresses four times in the last three months, hasn't taken a vacation in the last two years or has had a stressful event such as a personal relationship change. Those are critical factors to determining context for insider threats.

Q What is the relationship of big data to insider threats?

A When people talk about big data, they are really talking about structured and unstructured machine data—the data in log files generated constantly by applications, IT architectures that support them and traditional security point solutions. Important examples include social media, emails and web logs. This data is then seen in the context of HR vacation time records, personnel reviews and layoff notices. Collected and analyzed properly, this data provides the missing link to solving insider threats. What big data gives you is context, which can help understand the intent of the fraud. For example, when an employee does something against policy, a log is generated. But was it due to ignorance of policy or was it malicious? Big data systems can help you understand the difference.

Q What is the technology that can make those kinds of connections?

A It's about combining big data with statistical analysis, threat modeling and forecasting, and visualization so that you can analyze any set of data, from any source. You should also be able to search for any term throughout all of your data and look at standard deviations over a specific period of time to find outliers. For example: "Find me all of the failed logins across these types of systems that didn't happen on a Saturday, in this specific department and check this against any individuals on a layoff notification list." That's the type of specificity you need.