Welcome to our new series, in which we offer monthly time-saving tips for security professionals. This month, we’re going to focus on insider threat investigations. The process of investigating an insider-caused alert can be time-consuming, confusing, and frustrating if not handled properly. Worst of all, according to insider threat statistics, the longer an insider threat investigation takes, the costlier it becomes for the organization. This is true both in terms of man-hours and fallout from the incident itself. On the other hand, with the right level of visibility and context, investigations can be a straightforward process, enabling the organization to mitigate risks in a timely fashion. Here are three ways to save time when conducting insider threat investigations.

1. Ensure You Are Notified in a Timely Fashion

The worst way to slow an investigation down is not to know one should be happening… In some cases, organizations learn about an incident from the outside (e.g. a customer notifying you of a likely breach) or from an internal tool significantly after the fact. If you do not have an insider threat alerting system in place, you will not find out about an incident in a timely fashion. Regardless of its origin the alert kicks off the investigation, so getting it quickly is the key to a timely investigation.

To decrease your mean time to know, focus on implementing a system that will understand what an insider threat specifically looks like and send an appropriate and timely alert. There are tools like SIEMs out there that can trigger alerts for all types of security events, but it’s a good idea to have an insider threat-specific tool in place due to the unique nature of these threats. A network intrusion can be pretty easy to detect, but an employee or contractor attempting to exfiltrate data via a legitimate channel can be very difficult to spot using traditional security alerting tools. Invest in a proactive insider threat solution, and your investigations will be much faster because you will know about incidents in near real-time.

2. Get the Context You Need

The next step is to gather more intel. Many security alerting tools will let you know “what” has happened, but won’t give much context. Analysts may need to dig around quite a bit to figure out:

- Where did this happen? (In an app? On the network?)
- What systems are affected?
- When did it take place?
- What else was going on at the time? (The necessary context)

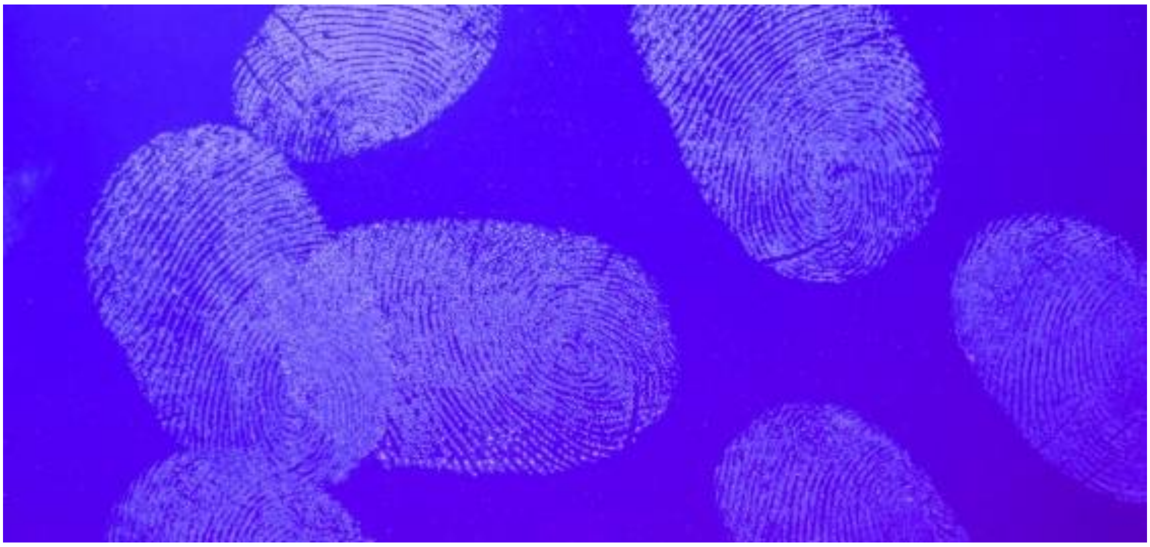
As you can imagine—or may know from going through this process yourself—investigating an alert in this manner can be very time-consuming. It requires the security team to go through many different tools, often searching through massive amounts of logs under significant time pressure.

That’s not to mention the reality that an alert may be one of literally hundreds coming in every day. It can be quite a challenge to sort through them, identify which ones represent real problems, and gather the necessary context.

Ineffective investigational tools can really slow down the entire process, and in the meantime, the threat may continue to evolve and put the business at great risk.

Instead, ideally, you want to invest in tools that are purpose-built for insider threat management. This is a very common threat source today, and having tools that can quickly provide the appropriate context can protect your organization's reputation and resources.

3. Focus on The "Why" & Gather Evidence



Once you have gathered context, you will need to determine what the perpetrator was up to—and understand their "why." For example, if a user was involved, you will need to figure out whether there is any history around this user that will help you understand what they did better. Is it a disgruntled former employee attempting to exfiltrate data? Or someone on the inside who simply slipped up and did something off-policy by accident? Understanding the why is the most efficient way to conclude an investigation.

Finally, when it is clear what happened and why, you will need to build up evidence. You can't simply go to leadership (or the authorities if it is a legal issue) and say, “This is what happened.” You need proof, and this can be especially hard to provide when all you have to work with is logs.

Again, the key is to use a purpose-built insider threat platform that can provide enough context to illuminate the why. Ideally, this platform will enable you to quickly build the evidence you need to take action if it’s required.

Speedier Investigations, Less Risk For the Organization

With the three tips above, you can dramatically shave down the amount of time it takes to investigate an insider threat incident, come to a conclusion, and take the appropriate action. A purpose-built insider threat platform can be the difference between a timely investigation that preserves the organization’s assets and reputation, and an insider threat incident that ends in a dramatic tailspin.