observe it

8 Commonly Misunderstood Concepts Around Insider Threats

Insider Threats are in the news, a lot these days. With the rising attention to this pervasive and costly problem have come many myths and misconceptions. It's hard for security professionals to weed these out when you have many projects, priorities and vendors vying for your time. Today, we'll tackle eight of the most common myths around the Insider Threat problem and what it takes to address this all-too-common risk.

What is an Insider Threat?

First of all, let's discuss what we mean by an Insider Threat, to make sure we're on the same page. An Insider Threat can happen when someone close to an organization with authorized access misuses that access to negatively impact the organization's critical information or systems. This person does not necessarily need to be an employeethird party vendors, contractors, and partners could pose a threat as well.

Myth: It's a Data Problem

When companies think about data loss, they naturally think of it as a data problem. They prioritize visibility into data, which can again lead them down the DLP path, with consequences described later on.

The Reality: Insider threat is not a data problem. It's a people problem. Data does not move itself; people move data. So if you want to address data loss and leakage, you need to come up with people-centric Insider Threat Management (ITM) strategy—one that offers complete visibility and context into what users are doing when, where, why, and how. You need a dedicated Insider Threat management solution to solve a people-centric problem, as people attempt to leak data or cause system failures.

Myth: Detection Will Always Lag

Sometimes, the complicated setup and the maintenance costs of DLPs & UAMs will lead teams to settle for incomplete visibility and detection. Before you throw up your hands, consider the reality of many Insider Threat scenarios. There are often early warnings that can be addressed to prevent worst-case scenarios.

Reality: Real-time detection of Insider Threat incidents is not just possible but relied upon by many leading security teams. If you're able to identify early indicators of an Insider Threat, you may be able to intervene before the risk spirals out of control. The sooner you can see that a departing employee has copied a bunch of sensitive files to his personal cloud drive, the sooner you can respond.

Myth: You Can Ignore Linux/UNIX Systems

There are certain solutions on the market that bill themselves as Insider Threat tools but do not cover Linux and UNIX systems…

The Reality: Linux and UNIX based systems are almost surely in use by your privileged users — engineers, system admins, and other team members who have access to the code base, IT systems and other valuable IP, as well as have intimate knowledge of your network. So any Insider

Threat “solution” that fails to cover Linux and UNIX leaves a gaping hole in your risk management program.

Myth: Only the Security Team Needs to“Get It”

A lot of the tools out there are log-driven, as we have discussed. Incomplete forensic logs might be okay for a security team to comb through (slowly), but they won’t help your legal or HR teams see what happened. When it comes time to conduct an Insider Threat investigation, the security team is just the front line.

The Reality: Your entire team needs to be able to understand what happened with clear forensic evidence, including timeline views and visual activity replay of the wrongdoing. If your investigations involve piecing things together with incomplete forensic logs of file movement, odds are you will not be able to respond in a timely manner, and you may struggle to produce the evidence necessary in the event of a prosecution or other outcome.

Myth: It’s OK to Sacrifice Privacy

Privacy’s just a normal casualty of the security mandate, right? Yikes. Even before GDPR went into effect, smart organizations emphasised their users privacy, even during an Insider Threat incident investigation. The Reality: Any ITM platform worth its salt should have privacy front and center. You need to take significant protections to balance security and privacy adequately, including:

- User anonymization
- Role based access controls
- Comprehensive audit logging & regular audits

- Watch the watcher" mechanisms Compliance with relevant egulations
- Strong data security

Without these, your Insider Threat program could leave your organization open to serious cultural, legal and financial risk.

Myth: Endpoint DLP is the Answer

One of the most common types of Insider Threats deals with data loss and leakage. It makes sense that those with access to an organization's most sensitive data and intellectual property (Insiders) would have the most potential to exfiltrate it, whether intentionally or accidentally. After all, many of your insiders are supposed to have access to this data in order to do their jobs. Companies need to know when that access is abused and data loss becomes a risk.

The Reality: In theory, traditional endpoint DLPs can look like the answer. That's just a mirage today. If you've ever used a traditional endpoint DLP, then you've felt the pain of data loss caused by insiders continuing unabated. DLPs are heavy on endpoints, and can sometimes user and data activity. They are trivial for power users to circumvent. For these reasons and more, endpoint DLPs alone are not the answer.

Myth: UAM is the Answer

User activity monitoring (UAM) is another common category that companies turn to when looking for an Insider Threat solution. Again, this makes complete sense on the surface. You need to know what your users are doing if you want to identify, investigate, and respond to Insider Threats.

The Reality: However, many of the solutions that bill themselves as UAM again do not provide the necessary level of context and visibility to identify, investigate, and respond to Insider Threat incidents. This isn't to say that you shouldn't look for user activity monitoring as a capability within an Insider Threat platform, but rather to point out that most of the tools that claim the title of UAM fall drastically short of what is required for Insider Threat management (ITM).

Myth: An All-Purpose Security Tool Will Work

Odds are good you already have a SIEM or other type of security platform in place. While these types of tools can be useful for external security and as a part of the larger security stack, they can't solve the visibility and context problem presented by Insider Threats.

Reality: Even if you have a SIEM or similar tool in place, you still need a dedicated ITM solution if you want full visibility and context into Insider Threat incidents. A robust ITM solution will offer irrefutable visual evidence during the course of an investigation and make it easier to stakeholders. Often customers integrate the visibility, alerts and evidence from ITM solutions into a SIEM.

Busting Myths to Clear the Air for Insider Threat Management

The myths above are pernicious and common, so we hope it's helpful to take the time out to address them head-on, so you can better define your Insider Threat program based on the reality of this common and complex type of risk.