DTEX
WORKFORCE CYBER INTELLIGENCE

INSIDER THREAT SOLUTION EVALUATION GUIDE FOR CRITICAL INFRASTRUCTURE

Guidelines for evaluating Insider Threat Mitigation technology solutions and considerations for building an effective Insider Threat Detection and Response Program that respects the Workforce

IDENTIFYING AND CONFRONTING THE INSIDER THREAT

Organizations of all types continue to struggle with the development of an effective approach to insider threat mitigation. In this world of rapid innovation and increasing foreign interference, there is a seemingly infinite number of variables and risk factors to account for within public and private entities. And even for those who believe they have a comprehensive insider threat defense established, changes in technology and public discourse are forcing a complete reexamination of their security strategies.

Introducing another layer of complexity is the fact that "insider threats" are actually a much broader category than many people realize. And while it may sound obvious, the first step in effectively detecting and mitigating these types of threats is fully understanding them.

They can be broken down into three distinct types:

- **Malicious Insiders** - These are the "traditional" insider threats as most people define them. These are users who intentionally hurt the organization, whether that be through data theft or by sabotage.
- **Negligent Insiders** - These are employees who unintentionally put security at risk. While often overlooked, these threats are actually the most common - driving more than 60% of insider-related security incidents.
- **Credential Thieves** - These are outside infiltrators who enter the organization through a user account. While these are technically external threats, they're doing damage from within the organization, and catching them is a matter of understanding insider user behavior.

Once security teams recognize the diverse, widely varied nature of insider threats, the challenges of creating an effective insider threat management strategy quickly snap into focus. After all, it's easy – or at least easier – to develop a protection plan against one highly specific type of scenario, such as the stereotypical rogue employee in a black hoodie stealing IP from a darkened office building. That task becomes more complicated if the stereotypical insider may actually be a naive employee accidentally downloading malware from a phishing email and letting an outside infiltrator into the network, or a disgruntled user quietly renaming and downloading files over a personal mobile hotspot to take to a competitor.

> **It is imperative that critical infrastructure entities prioritize and dedicate resources to preempt and/or mitigate insider threats.**
>
> *National Counter-Intelligence & Security Center*

KEY REQUIREMENTS

Recent guidance by the US National Counter-Intelligence & Security Center makes it clear that insider threats are a human problem and require a human solution. Technology can enable organizations to get a better sense of workforce behavior, particularly in its virtual domains, but the most important resource an organization has to counter insider threats is the workforce itself. To help mitigate these threats, an organization must, at a minimum, achieve two things:

1. Have a program that identifies individual anomalous behavior and the resources to respond
2. Respond to anomalous behavior in a way that fosters trust and leverages the workforce as a partner

It is possible to build an insider threat mitigation program that follows the NCSC's latest guidance. The key is choosing a purpose-built solution, developed from the ground up with these specific goals in mind: shining a light on insider threats by understanding workforce behavior and conducting monitoring and surveillance with respect for personal privacy and full transparency.

In order to find a purpose-built solution, however, there must be a clear understanding of the elements that comprise one. The answer lies in these five keystones:

VISIBILITY

In order to find and mitigate insider threats, security teams need to have the ability to quickly see potential red flags as they arise. This requires complete visibility into what is happening across an entire organization at any given moment. And because all users are equally capable of putting a business at risk, the same level of visibility can and should be consistently applied – regardless of role, location or designation of privilege.

All users are capable of putting the organization at risk, so an effective insider threat program begins with enterprise-wide, real-time visibility.

Furthermore, real-time visibility is no longer optional. Critical Infrastructure entities, financial services organizations and pharmaceutical enterprises are learning this faster than others – but it is something that all industries will need to integrate into their security strategies.

QUESTIONS TO ASK:

- *What will I be able to see? How quickly will I be able to get answers to questions like:*
  - *Who touched a given file in the last 24 hours?*
  - *How many files have left the organization in the last 24 hours? And how did they get out?*
  - *Which individuals are logging in to system admin accounts?*
  - *What files have recent "joiners" brought into my system?*

  Purpose-built solutions should be able to provide answers to these types of questions quickly, and provide necessary context around them.

- *Where does this solution pull its data from?* - The only way to understand what exactly you'll have visibility into is to understand where exactly the solution is pulling data from – whether it be other systems and log file repositories or directly from the endpoint or user.
- *What type of data does this solution collect?* - Some insider threat solutions collect metadata, some collect content data (like screenshots or keylogging), some collect log data, and some don't collect any data at all. In order to catch insider threats, a solution needs to be collecting user behavior data from the endpoint.
- *Does this solution provide visibility both on and off of the corporate network?* - Nearly every modern workplace has some degree of remote workforce, which means that your visibility can't just stop once a company laptop leaves your headquarters.

INTELLIGENCE

"Intelligence" can be a vague and overused term in the cybersecurity world, but it has a very specific and important meaning: the powerful combination of context, knowledge and flexibility. And an intelligence-driven approach to insider threat management means decisions are made based on actionable insights, not just a high volume of data.

Insider threats can come in so many different forms. Security teams cannot afford to be paralyzed by information or bogged down in manual analysis. They quickly need to know what slips through the cracks. They need to know exactly where their most vulnerable data is, and how users interact with it. And most importantly, they need to be able to understand these things without picking through an overwhelming amount of data.

QUESTIONS TO ASK:

- *Is this a rules-based or analytics-based solution?* - Insider threats are, by definition, human – and human behavior is too intricate to be boiled down to a series of written rules or policies. Analytics are necessary to understand and detect anomalies in events and behaviors. In order to be most effective, a tool needs to be smart enough to learn what's truly normal or abnormal and adapt as needed (which means that it needs to employ some form of machine learning).
- *Does this solution understand and provide context around an activity / event?* - Context is critical, both when it comes to triaging alerts and when it comes to forensic investigations. This means a solution needs to offer human-readable, easily accessible context that answers the important questions: the "who," "what," "where," "when" and "how."
- *Does this solution prioritize alerts? On what basis?* - Analysts aren't able to fight threats if they're buried beneath noise. Alerts should be answers, not a continuous loop of false positives. It's critical to understand what a solution does in order to cut down on noise and enable swift action.

SCALABILITY

If there's one thing that continually proves itself to be true, it's that there is no single type of "high-risk" user. Any insider has the ability – intentionally or unintentionally – to put an organization at risk. So, an effective insider threat tool must be scalable enough to be deployed enterprise-wide and fully function across the company's environment. If it significantly impacts network performance, or hinders user productivity in such a way that it is constantly being disabled or worked around, then the tool isn't really protecting the user or the organization.

QUESTIONS TO ASK:

- *Can this tool be deployed across the entire organization? What is the impact on a network? On user productivity?* – The only truly scalable solutions are those that have a near-zero impact on network, system and user performance. Be wary of tools that generate excessive amounts of data, as the heavy footprint associated with that kind of data collection is likely to hinder scalability and usability. The same goes for tools that advise you to deploy only to selected users or disable core features in order to make enterprise-wide scalability manageable.
- *How many people does managing this solution require? Will it require additional dedicated manpower?* – A sustainable solution needs to have a high enough signal-to-noise ratio that it doesn't require excessive man hours to manage alerts or tuning. Your chosen solution should be tailored to the available staff and expertise you have on hand, instead of requiring you to hire additional team members.
- *Is this solution able to support / adapt to cloud environments?* – In order to support today's most forward-thinking organizations, a tool needs to be capable of adapting to modern security architectures and frameworks – which means it needs to clearly demonstrate flexibility, agility and the ability to support automation requirements.
- *Does it provide performance metrics?* – This should go without saying, but numbers speak louder than any sales pitch.

AGILITY

Modern threats move quickly, so organizations need to be able to pivot just as quickly if they hope to keep up. This also means that security measures – and insider threat tools – need to be agile enough to adapt to changing priorities and conditions if they hope to be effective.

It's only realistic to expect that any solution or tool – especially one that is analytics-based – will require some time to tune and customize. But, being stuck in an endless loop of tuning and configuration means that tool isn't providing enough value or delivering return on investment.

Modern threats move quickly. Organizations need the ability to pivot just as easily and understand activity in real time.

QUESTIONS TO ASK:

- *Does this solution require tuning before it starts to show value? If so, how much?* - While it's inevitable that some tools require some degree of tuning before they provide actionable insights, find out exactly how long that tuning will take and what value you'll see – if any – in the interim. Look for a tool that provides value while it continuously tunes, instead of one that traps you in a perpetual tuning cycle.
- *Is this solution capable of learning or self-tuning, or does it rely completely on manual tuning?* - For a solution to generate continued value, it needs to incorporate advanced analytics and machine learning capabilities, which in turn make it capable of self-tuning. If it relies only on known and available information without seeking out additional context or intelligence, there will inevitably be things that fall through the cracks.
- *How frequently is data uploaded and processed? How long does it take for an alert to process after an activity?* - Some products only upload data a few times a day, meaning that visibility and alerts are far from real time. And in some cases, analytics may take hours to run, which means alerts and insights are always far behind the activity or event that occurred. Modern enterprises need a solution that processes data in real time, or near real-time, in order to proactively defend against threats.
- *What happens if our organization needs to change priorities or focus?* Be wary of products that require lengthy re-tuning if you choose to re-prioritize. Most security teams will inevitably need to adjust threat criteria, so your chosen solution should allow you to change priorities (such as alert criteria) quickly and easily.

PRIVACY

Employee privacy has become a topic of increased interest and scrutiny for both governments and enterprises – and should be given strong consideration when building an insider threat program. Here's why:

Increasing Regulations: Organizations in the EU – as well as any doing business there - must comply with the requirements of the General Data Protection Regulation (GDPR) legislation. Other countries have even stricter privacy laws that dictate what kinds of information organizations can collect about their users and employees, how they can use it and how they can store it. With digital privacy becoming such a high-profile conversation topic, it's impossible to believe that there won't be more legislation on the way.

Public Opinion: In the past year, highly public discussions about data and privacy have sprung up seemingly everywhere – largely stemming from news (and controversy surrounding Facebook and similar technology providers). In general, people are more aware and have stronger opinions about how their behavior is collected and used.

Company Culture: Creating a culture of intense surveillance and treating every employee as a subject of distrust is likely to seriously hurt employee morale. And it can backfire in very tangible ways that go beyond moral responsibility.

In a survey conducted in conjunction with Harris Poll, we found that most people - 64% - do believe that it is acceptable for organizations to monitor user activity... but only if that monitoring is conducted with transparency.

QUESTIONS TO ASK:

- *Does this solution have core privacy-conscious features and capabilities?* - Sophisticated insider threat solutions should take advantage of privacy-related innovation such as data anonymization, which can keep a user's identity hidden and behavioral data protected until suspicious activity is detected. These capabilities not only help alleviate employee privacy concerns but also provide a layer of protection at a time when behavioral data is increasingly considered sensitive, personally identifiable information.
- *Does this tool provide the ability to anonymize data?* - Anonymization is a mandatory requirement for global organizations because it helps with compliance on GDPR and other privacy laws. Outside of GDPR, it can also reduce liability and put employee morale at ease. Specifically, look for a solution that anonymizes data from the server, not within the UI, and that allows for de-anonymization by only a strictly controlled set of keyholders.
- *Can this tool be deployed in a GDPR-compliant manner? Would that entail any special changes to the functionality or deployment?* - Any company that does business in the EU must select tools that can be deployed in a GDPR-compliant manner. This means the tool must have been constructed with a core focus on the principles of "Privacy by Design" or "Data Protection by Design and by Default." Any tool that requires extensive changes in order to be deployed under GDPR is a risk and potential red flag.

CONCLUSION

With investments in intelligent, behavior-based solutions – that prioritize actionable visibility, scalability, agility and privacy – organizations can stop insider threats while enabling their greatest assets (their employees) to remain their greatest assets. Security does not need to come at the expense of users or the rest of the organization. And it's entirely possible to build an insider threat program, from the ground up, to support the business as a whole... not stifle it.

LEARN MORE ABOUT DTEX AND WORKFORCE CYBER INTELLIGENCE

DTEX Systems is the world leader in Workforce Cyber Intelligence and committed to helping enterprises run safer and smarter. Only DTEX dynamically correlates data, application, machine, and human telemetry to stream context-rich user behavior and asset utilization analytics that deliver a first-of-its-kind human-centric approach to enterprise operational intelligence. Hundreds of the world's largest enterprises, governments and forward-thinking organizations leverage DTEX to prevent insider threats, stop data loss, maximize software investments and deployments, optimize workforce engagement, and protect remote workers. DTEX has offices in San Jose, California, and Adelaide, South Australia, and is backed by Northgate Capital, Norwest Venture Partners, Wing Ventures, and Four Rivers Group.
To learn more visit: www.dtexsystems.com.