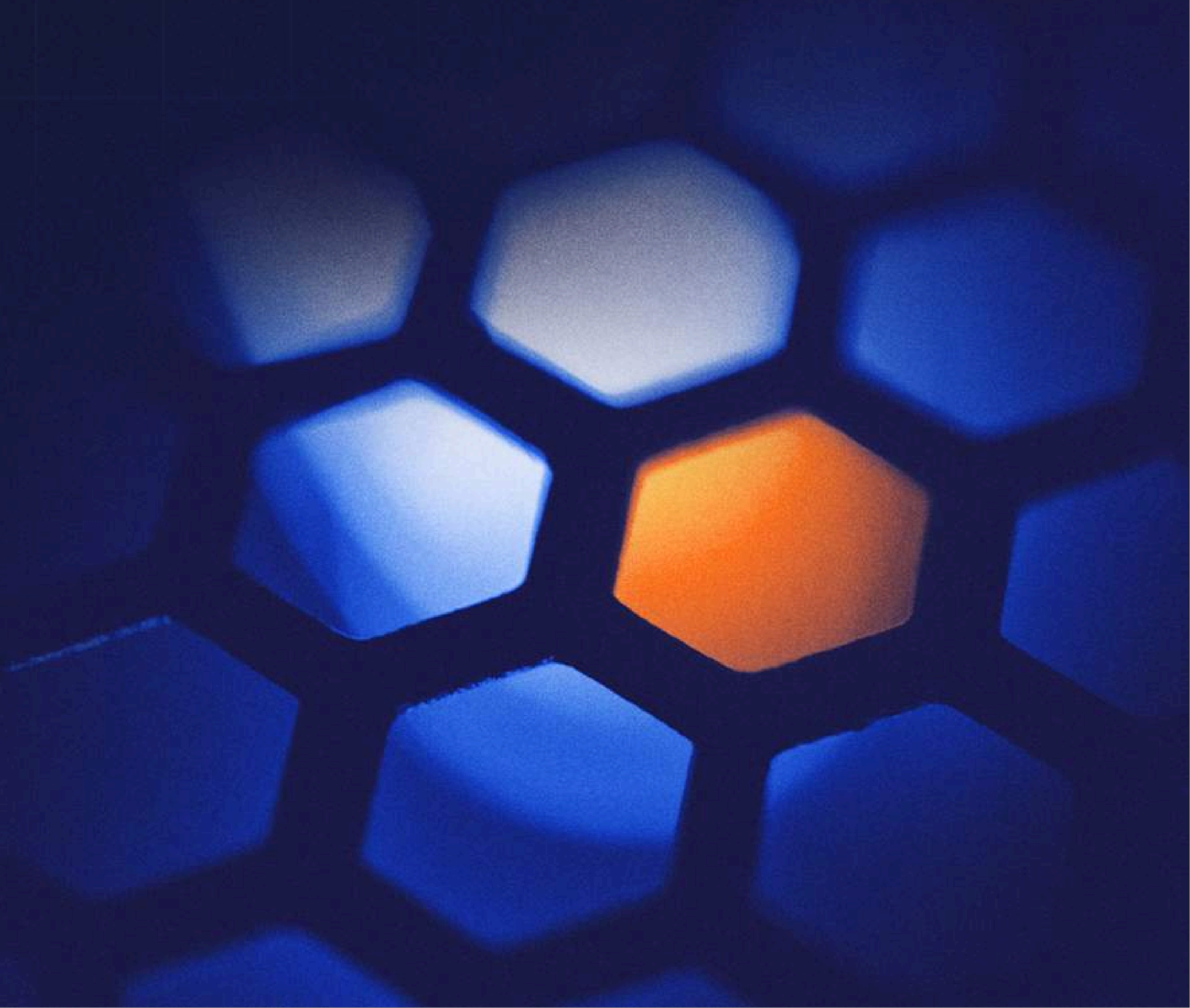
TERAMIND

Reducing Insider Risk Through Positive Deterrence



Preventing insider risk requires **insight that enhances user data.**

Enterprise security leaders leverage sophisticated security tools to gain visibility into user behaviors. Technologies like User Entity and Behavioral Analytics (UEBA) help control insider risk by triggering alerts when users deviate from their established routines.

These tools are powerful in identifying and mitigating risk, but an effective mitigation strategy is company-wide. Consistently preventing insider risk means taking a proactive approach to accompany the detection and response workflow. The most successful organizations treat cybersecurity risk reduction and mitigation as a multi-layered strategic initiative. While tools and technologies are an essential part of the solution — cross-discipline collaboration and reducing silos is another.

Positive deterrence is a company-wide approach to cultivating values that lead to improved insider risk resilience. It builds on the technological capabilities of UEBA platforms, facilitating collaboration between insider risk teams and the people they rely on to address insider risk proactively.

Positive deterrence addresses the root cause behind insider risk.

No model can accurately make an unbiased prediction about whether an individual will commit a crime in the future—although not for lack of well-funded academic research.

> **Positive deterrence isn't about detecting future wrongdoers,** but building a foundation for a constructive and enriching employee experience.

This matters because happy, well-adjusted employees are statistically less likely to commit crimes against their employers. These people are less inclined to exhibit concerning or toxic behaviors like harassing other employees or violating company policy.

Overall, this reduces the number of issues that the insider risk team has to address. It leverages the power of company culture to prevent insider threats from developing in the first place. Additionally, it provides a layer of early warning protection against people who commit themselves to carrying out negative actions despite the company's best efforts.

Employee referrals are key to preventing insider risk.

BBy the time an insider commits an observable fraudulent act, it's too late for prevention. Highly collaborative teams that cultivate relationships with other business units will often receive warnings about insider risk well before they decide to act against the company's interest.

Those types of warnings come from managers, team members, and other employees. Every team cultivates its own microculture, with its own expectations and implicit behavioral baselines. An employee who suddenly changes their psychological or social behavior may represent a serious insider risk without triggering a single log-based alert.

To form a truly robust insider risk team, security leaders need to recognize that employees are more than network assets and user accounts. Human insights—like the ones co-workers routinely share with HR leaders—can provide insider risk teams with actionable data well before log activity shows suspicious activity.

Security leaders who partner with HR can build an insider risk management workflow that is far more than the sum of its parts. Identifying psychosocial risk indicators and building a framework for positive deterrence can dramatically change the way insider risk is identified and addressed.

Insider threats tend to share **psychosocial characteristics.**

Insider threats do not happen in a vacuum, and they rarely happen outside a psychosocial context. That context includes a variety of behavioral issues that correlate to heightened insider risk.

Studies consistently show that in real-life insider threat scenarios, co-workers are often aware of behavioral issues like tardiness, belligerence, and poor performance well before the insider attack occurs. According to one study, work colleagues were aware of behavioral issues prior to insider attacks in 97% of cases.

These behavioral issues come in a variety of forms, **most of which are well-known to HR professionals:**

Disengagement

Employee engagement has dropped to an 11-year low, putting organizations at a disadvantage when addressing insider risk. Disengaged employees lack supportive bonds with their co-workers and organization, and may feel like their career is a dead end. All of these issues can translate to increased insider risk.

Lack of motivation

Unmotivated employees are likely to be less productive. If the situation worsens, they may simply stop showing up to work altogether. Habitual absenteeism has a profound impact on insider risk, especially for employees with access to sensitive files and assets.

Disgruntlement

Disgruntled employees are an obvious source of insider risk, yet job satisfaction is rarely included in security metrics. If the organization has done something to make an employee angry, the insider risk team should be aware of that situation.

Toxic behavior

Experts have begun to pay a great deal of attention to the impact of workplace toxicity on employee well-being. Harassment, bullying, and other toxic behaviors are a powerful indicator of insider risk, especially when left unresolved for long periods of time.

Inappropriate responses to stress and conflict

Healthy workplace environments have strict, self-policed boundaries on how people should express themselves when experiencing conflict. Employees who use foul language or act in threatening ways may represent pronounced risk—both for the company itself and the physical safety of its employees.

Antisocial behaviors outside of work

Most leaders are hesitant to pry into the personal lives of employees, but certain issues like violence, hate speech, or criminal activities cannot go unaddressed. These behaviors are critical warning signs of insider risk and demand in-depth investigation.

Despite the serious security implications of these activities, they often remain siloed in HR. By the time an employee actually dedicates time and energy to planning an insider attack and carrying it out, these warning signs may be well-documented by Human Resources team members.

The reason for this is clear. Excellent HR leaders go to great lengths to establish a positive, trusting environment for employees. People are not afraid to voice their concerns about co-workers to HR. They're encouraged to make confidential reports without fear of reprisal or punishment.

What does positive deterrence look like in practice?

Positive deterrence is a company-wide cultural strategy that mitigates insider risk by addressing the factors that cause it. This gives insider risk teams the ability to detect and address problematic behaviors before they create undue risk for the organization.

In this model, insider risk teams work closely with HR to build accurate baseline models that include psychosocial factors that impact insider risk. Together, both teams establish a culture of transparency and communication while driving human productivity and collaboration.

As the product of collaboration between security and HR, positive deterrence has both technological and psychosocial elements. When responsibly implemented, it uses these elements to cultivate a self-policing security culture defined by transparency and communication supported with robust, enforceable policies.

As an insider risk leader, employee referrals are your best source of information on potential risks. **The closer and more deeply employees interact with one another, the more likely they are to flag suspicious behavior in a positive deterrence environment.**

The following three initiatives are just a few examples of programs that can help promote a strong positive deterrence culture:

1. Actively support and cultivate team microculture.

The concept of a monolithic "company culture" may be fading in importance. According to researchers, small, team-based microcultures may be better-suited to meeting the social needs of individuals in a workplace environment.

71%

of respondents to Deloitte's 2024 Global Human Capital Trends survey reported that individual teams and workgroups are the best places to cultivate culture.

One-half of executive respondents said that culture is more successful when there is moderate variation between teams.

For security leaders and insider risk program owners, that means defining and promoting cultural values is a high-priority team effort. It requires buy-in from leaders throughout the organization, and its success depends on their ability to support sustainable change over time. Often, that means directly contributing to the HR team's efforts to transform internal company culture.

Security leaders are invaluable to the effort of creating positive microcultures and can create a positive culture of deterrence on their own teams. Doing this in coordination with HR establishes the foundation for a meaningful, trusting relationship between the two departments. If HR has a seat at the table during security discussions, it is more likely to come forward when it detects security issues of its own.

Even more important is the act of showing solidarity with other teams and leaders. Because they are constantly bombarded with problems and alerts, security teams can sometimes devolve into a negative perspective of the rest of the company. It's essential to limit negative or critical comments in front of one's team, for example, to help stoke the fires of comradery and positive company culture.

2. Invest in volunteering activities and personal projects – ideally alongside other teams.

Employees care about causes, values, and missions beyond what they do at work. Security leaders who actively support team microcultures can seek out employees who express their values and support them on the company's behalf.

Supporting employee volunteer efforts can provide a profound sense of human value and accomplishment to individuals outside of their strictly defined business role. Weekly or monthly recognition events can instill positive values while reinforcing engagement, collaboration, and communication.

Encouraging employees to open up about personal projects also provides many of the same benefits. It builds a safe space for people to broadcast the things they care about and connect with other people on those topics.

Topic-oriented groups and activities can also benefit from company support. Many organizations already offer official support and recognition for a company sports team. The same framework could extend to any cultural activity shared by multiple employees.

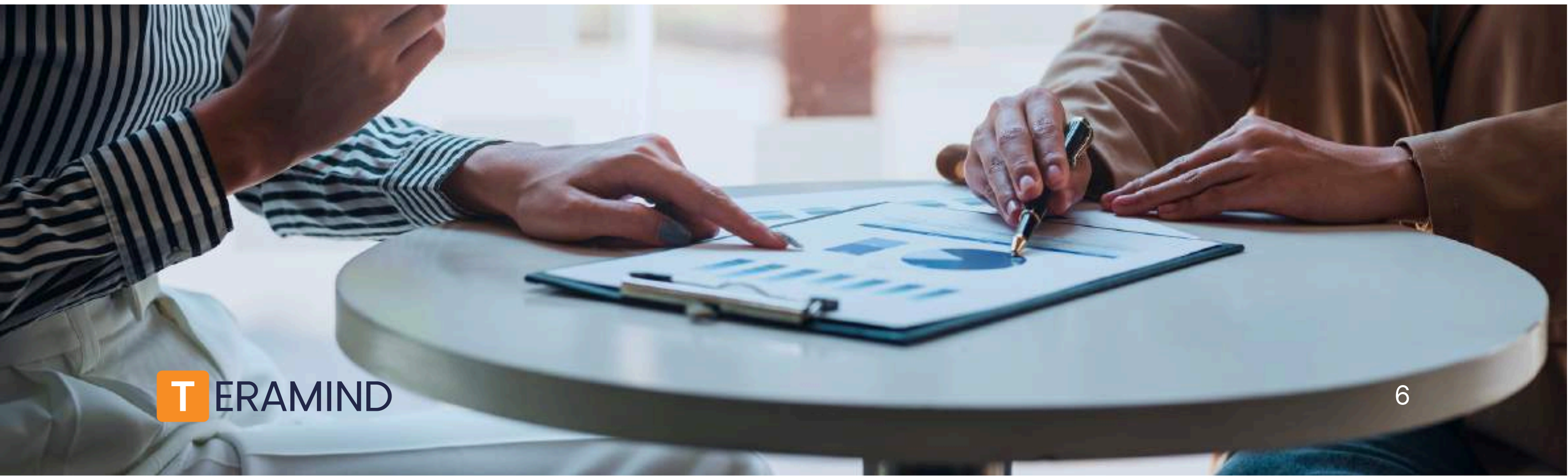
3. Use one-on-one meetings for more than reviews and task assignments.

One-on-one meetings with managers and leaders can be intimidating for employees. This is especially true when reviews or assignments include negative feedback. Some people are especially sensitive to criticism, and that sensitivity can translate to increased inside risk.

One-on-one meetings should include time for connection and support. Taking time to establish meaningful social connections with people can help reduce the risks associated with negative feedback and make employees less likely to bear long-term grudges against the company.

When pursued alongside other initiatives like supporting personal projects and cultivating team microcultures, establishing rapport with employees in one-on-one meetings is a small and easy step to take. Management already knows what interests individual team members have and understands the values that drive them.

This rapport is important because it has a profound impact on the decision to communicate insider risk concerns about other employees. It takes a great deal of trust to reach out to the insider risk team and suggest that a co-worker's activities should be investigated. Without rapport, that trust cannot exist.



Positive deterrence includes new technologies and productivity metrics.

Technologies like UEBA have a role to play in positive deterrence, but User Activity Monitoring (UAM) augments the insider risk program by providing on-demand context into user behaviors. Instead of piecing together behavioral activity using logs, UAM solutions can grant visibility into what people are actually doing with their devices on a case-by-case basis.

This allows UAM technology to drive value that goes beyond security and insider risk. Executive leaders in every department can better understand employee productivity on a much deeper level.

For example, activity monitoring may uncover obstacles to production that generate user experience friction for employees. By proactively addressing these issues, business process owners can unlock productivity gains that may otherwise never be addressed.

UAM implementation can lead to dramatic changes in the way company leadership measures risk, productivity, and culture. It paves the way towards a deeper understanding of the value employees truly generate, with impacts across the entire organization.

User activity monitoring makes "looking busy" less relevant.

With 60% of the global workforce reinforcing the trend towards quiet quitting, trying to look busy gives disengaged employees an easy way to avoid scrutiny.

Yet employee disengagement is a strong predictor of insider risk, and security leaders need to know when employees reduce their efforts to the bare minimum.

For some disengaged employees, putting in a day's work involves programming their device to randomly click a few times per minute. They may use mouse jiggler software to keep their connection active without even being physically present at their computer.

Capturing disengagement metrics is of value to HR, which gives insider risk teams an opportunity to provide that data directly. This gives the HR team a chance to re-engage employees and offer them support before they start exhibiting more concerning behaviors.

This kind of combined approach can mitigate a potential future insider risk and prevent it entirely. UAM tools can bridge the gap between security and HR and support collaboration between the two teams in a measurably proactive way.

Quiet leaders and change champions can get recognition they deserve.

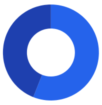
Tech and HR leaders are already well aware of the important role change champions play supporting new technology implementations, policy updates, and enterprise growth.

In many cases, these people are quiet leaders whose expertise and knowledge makes them a valuable asset to the team. These are people who teach other employees how to complete complex tasks and interface with leaders from other departments on technical topics.

Identifying the people who champion change isn't always easy. Their direct managers usually know who they are, but that recognition doesn't always extend past the boundary of that specific team.

UAM technology makes it much easier to identify these people based on their engagement, interactions, and productivity.

Formal programs for recognizing these influential performers can help inspire others to follow their example, improving morale and performance on a company-wide scale.



44% of HR leaders surveyed by Gartner said **their companies don't have clear promotion paths / career development for high-performing employees.**

Human sustainability is the new norm, and it requires everyone's participation.

Technologies and systems play a huge role generating value for organizations, but it's ultimately human beings who do the work. Human connections are responsible for all of the value that an organization produces, and leaders who understand that are well-equipped to optimize that value through human sustainability.

Three-fourths of respondents to a Deloitte survey recognize the importance of human sustainability, yet only **10% of those respondents report making significant strides towards those goals.**

This gap will not remain open indefinitely, as leaders come to recognize the value of treating employees as willing partners in their enterprise.

It's difficult to overstate the impact of human sustainability on insider risk. An employee who feels their employer is actively and positively contributing to their well-being has no reason to act against the organization's interests. If their interests are truly aligned, any kind of malicious insider activity would be self-defeating.

But human sustainability doesn't come strictly from executive leadership. It has to come from everyone, including mid-level managers, team leads, and new hires. Like positive deterrence, it is a company-wide value that informs policies on every level.

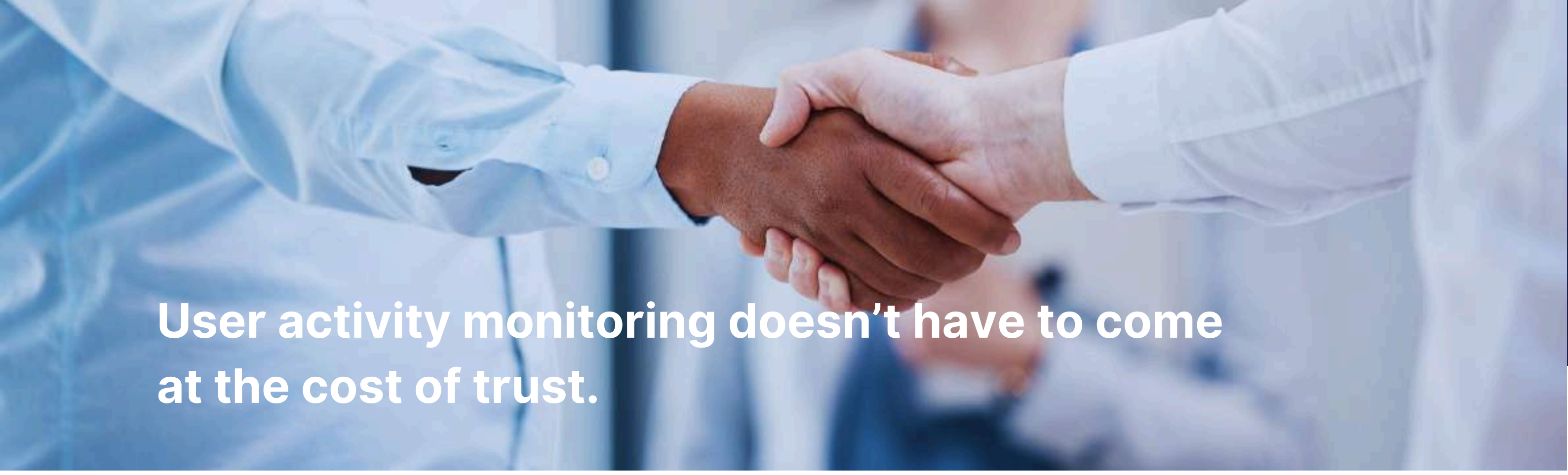
Alert-only investigations balance discretion and safety.

22% of workers report that non-consensual employee monitoring is an obstacle to human sustainability. **The feeling that organizations do not trust their employees makes building positive deterrence much more difficult.**

It's true that new technologies carry the potential for misuse. Invasive surveillance and constant monitoring increase employee stress without necessarily generating positive security outcomes. Consent is critical to the human sustainability project, and a major element of positive deterrence.

Responsible policies are vital for building and maintaining trust. Security leaders can advance positive deterrence initiatives by developing policies that operate based on consent and respect for users' privacy.

Triggering UAM tools to record users' screen activity in response to policy violations is a much better rule than secretly recording everyone in the company at all times. Security leaders who work with HR to develop and communicate insider risk policies will be able to establish alert-only workflows.



User activity monitoring doesn’t have to come at the cost of trust.

When responsibly managed in a positive deterrence framework, user activity monitoring and behavioral analytics can create a safe, transparent environment for employees and employers alike. At the same time, these tools can unlock human performance and help align business goals with employees’ personal needs and motivations.

Employees who understand the policies and technologies that support positive deterrence are more likely to see it as a powerful benefit. This kind of company-wide cultural initiative is designed to empower people, not take away their sense of agency.

Here are four key characteristics that successful insider risk initiatives are likely to share under this framework:

⟶ No single data point is enough to accuse someone of wrongdoing.

Traditional security technologies are often designed to look for “smoking gun” evidence of cyberattacks, data breaches, and malicious activity. Insider risk professionals almost never get that level of clarity from a single datapoint.

Circumstantial evidence is far more common, and this type of evidence can be interpreted in a variety of ways. It takes many different pieces of evidence gathered from multiple sources to truly establish malicious intent.

Insider risk professionals who collaborate with HR to identify and address psychosocial predictors of insider risk will need to take a much more subtle approach. Giving people the benefit of the doubt and providing them with education and support will help prevent insider threats from occurring altogether.

⟶ Employee safety is part of insider risk, too.

Employees are understandably concerned about the prospect of being under constant surveillance. Yet almost one-fourth of workers experience violence and harassment at the workplace.

Insider risk programs don’t focus exclusively on investigating cyberattacks, data exfiltration, and corporate espionage. They also have a role to play preventing employees from harming one another — verbally, emotionally, physically, or otherwise.

Configuring user activity monitoring and behavioral analytics tools to trigger alerts in response to these risks demonstrates the organization’s commitment to maintaining a safe, productive, and transparent working environment for everyone.

Empower employees by proactively identifying and addressing points of friction.

Redundant tasks, unnecessarily complex policies, and technical workarounds are a routine part of many employees' daily lives. These problems may not immediately impact productivity or workplace satisfaction, but they do have a significant influence.

User activity monitoring software can help business process owners analyze employee workflows in ways that help eliminate obstacles and redundancies. Proactively eliminating unnecessary points of friction for employees makes their job easier, building trust and improving productivity across the board.

Modern UAM platforms can provide in-depth detail into the work performed by individual employees without including their personal information. Anonymized productivity-capturing screen recordings can provide valuable information to product owners without compromising employee well-being and privacy.

Look for trends that point toward disengagement and proactively address issues.

The ability to identify psychosocial indicators of increased risk allows security and HR leaders to address those risks together. By acting on the data early, the organization prevents situations of increased risk from taking place altogether.

That means supporting teams and employees with productivity metrics trending towards disengagement. It means intervening to support employees when they feel the organization is somehow failing them.

Even under a positive deterrence framework, punitive actions may be taken if employees refuse to change problematic behaviors and their issues continue to escalate. The act of extending trust to someone comes with the risk of withdrawing it if that trust is not respected.

Conclusion

Insider attacks rarely occur without a psychosocial context around them. Insider risk professionals who pay attention to the behavioral indicators that predict malicious activity can act earlier, mitigate damage, and enforce good policies with greater effect.

The concept of positive deterrence offers a structured, company-wide cultural framework for addressing early signs of insider risk. It also unlocks human performance and enables organizations to demonstrate their commitment to human sustainability.

Taking positive, proactive measures to address insider risks early on is more effective than trying to perform damage control after a breach has already occurred. At the same time, empowering people to engage with their workplace yields productivity outcomes that stress and pressure fail to produce.

TERAMIND

Request Your Custom Demo Now

Get Demo