ENHANCED INSIDER THREAT:

Using AI as an Accelerator to Address Today's Emerging Threats

ENHANCED INSIDER THREAT: USING AI AS AN ACCELERATOR TO ADDRESS TODAY'S EMERGING THREATS

In this document, we explore our perspective on developing a more comprehensive Insider Threat program that is enhanced by the benefits of Artificial Intelligence (AI) and Machine Learning (ML). We introduce the concept of the 360-degree profile, how that concept can improve an organization's visibility into its overall culture, and behavioral theories that factor into and/or contribute to insider threats. We present a concept of operations and provide considerations for stakeholders who seek to implement a more complete solution required to address today's emerging insider threats. Our pragmatic approach considers the organization's existing capabilities and investments and is based on our experience leading, supporting, and operating Insider Threat programs for other organizations.

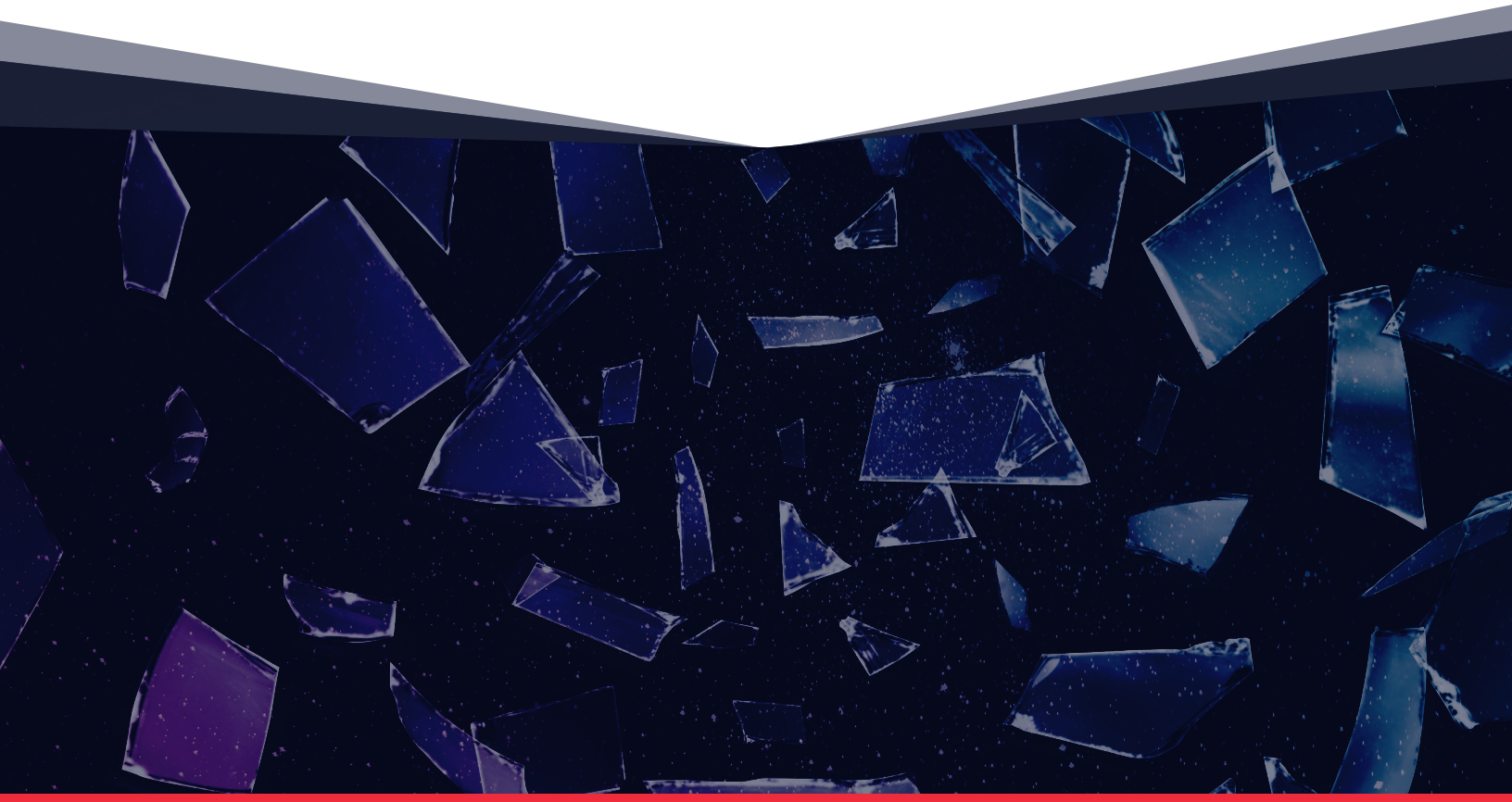
Insider threats require a different strategy to detect and resolve risks to organizations, going from human to machine speed. All organizations face a highly dynamic, ever-evolving landscape of insider threat risks. From deliberate espionage to accidental data leaks, the potential damage insider threats may cause organizations is limitless. Traditional security measures are designed to protect organizations and respond to threats. Insider threat training and other security tools help reduce risks, but the human element remains a key factor to the overall effectiveness to all policies and procedures. Insider threats are more complex, which requires innovative solutions to detect and resolve issues. To be effective, solutions must catch and resolve threats faster, advance the learning curve, adapt to changing scenarios, and quickly scale.

ORGANIZATIONS SEEKING TO IMPROVE EFFECTIVENESS OF THEIR INSIDER THREAT PROGRAM CAN DO SO WITHOUT A LARGE FINANCIAL INVESTMENT IN TOOLS AND TECHNOLOGY; INSTEAD, THEY SHOULD RE-ENVISION AN ANALYTICAL APPROACH THAT CONSIDERS A 360-DEGREE VIEW OF PEOPLE'S POSITIVE AND NEGATIVE BEHAVIORS.

Risk management tends to focus on user activity monitoring (UAM), user and entity behavior analytics (UEBA), and data loss prevention (DLP). This approach allows organizations to understand what happened and how it happened, but typically falls short of predictive analysis. With a reactive approach, the damage has already occurred. The goal of organizations is to move to a proactive approach by understanding and addressing the underlying contributing cause(s). Provided the right datasets and analyst talent with an inquisitive mindset, an Insider Threat program can apply ML techniques to identify patterns and trends in individuals' activities to build risk profiles of insiders across the organization. This progressive approach can shape an organization's ability to deal with insider threats by illuminating early indicators of potential malicious actions at pace with the volume and variety of individuals' behaviors, tendencies, and activities.

A progressive approach to insider threat involves advancement beyond a purely reactive stance to the proactive identification of possible threats through the assistance of ML. In combination with UAM, UEBA, and DLP, ML serves as a transformative technology for Insider Threat program analysts to achieve that proactive posture. Numerous analytical models derived from historical insider threat events can be developed to consider the conditions surrounding actual threats and improve confidence in the correlations between information in an individual's profile. Models can also identify trends and patterns which will significantly enhance the necessary human analysis. ML and AI models can identify activities over a much greater time frame; call out anomalies and patterns in many more data points; and find connections across multiple profiles. With the combined knowledge of what, how, and why, organizations can put in place countermeasures and awareness campaigns to deter and counter potential attacks before they happen. This approach also allows Insider Threat programs to effectively respond to indicators of compromise when future attacks occur.

Organizations benefit from considering all aspects of an individual's behavior. Understanding both positive and negative behaviors of individuals within organizations can reduce investigative time and false positives; as well as enhance focus on higher priority threats. Gathering a baseline of positive and negative behaviors is part of what we call the 360-degree profile—a holistic view of people with a deeper understanding of their motivations. For example, by taking proactive actions to improve a person's mood based off of what brings them joy they are less likely to be impacted negatively by an action, event, or situation in the workplace. As a result, the overall risk of that person becoming a malicious threat is minimized. The organization benefits from a reduced threat level, with the added benefit of improved morale and workplace satisfaction, when it builds a 360-degree profile of its people and takes steps to influence positive behaviors within its environment.



CHANGING PERSPECTIVE

Traditional Insider Threat programs and tools are static and standardized across all employees. Additionally, current Insider Threat programs tend to focus on negative behaviors individuals exhibit as indicators to potentially commit insider threat actions. These programs and tools are only effective in responding after a general identifier has been triggered as defined depending on how the program or tool was designed. The damage has often already been realized by the time the threat has been discovered. While these tools and processes are important, they do little to prevent the impact of the threat. A proactive program, with customized tools and inclusive of other factors of the individual, enables organizations to improve the prevention of threats and intervene before the threat is acted on. Furthermore, this approach has the added potential of providing stakeholders with a better understanding of the organization's overall culture. This additional insight can help the organization's stakeholders determine how to allocate resources more efficiently.

A hybrid approach leveraging traditional methodologies while implementing new ones creates a robust and innovative solution to moving Insider Threat programs from a "reactive" to "proactive" environment. While it is crucial to understand the potential indicators which can signify negative actions, it is also important to implement an Insider Threat program focused on identifying indicators of positive behaviors: "What makes us happy?" or "What do we value?" An individual's actions originate from emotion, whether it be positive or negative. A person's behavior is not a direct reflection of what type of person they are, but how their environment affects them in relation to their personality. Thus, it is important to understand a person's emotional state is ever-changing. Even the most balanced individuals can present a high threat with the right conditions in place. This is because when there is a potential risk of a negative impact to something in which a person holds individual value, the natural human reaction allows the mind to bypass core logic and integrity allowing actions to be guided by reactional emotion. Ultimately, everyone is equally at risk if they feel their core values are threatened. As such, **insider threats can fall into three general categories:**

1. **Malicious Insiders** with access to sensitive data and intention to use that access to cause harm. Widely known examples include Edward Snowden, the former NSA consultant who leaked highly sensitive information, and Robert Hanssen, the former FBI agent convicted of espionage.
2. **Careless Insiders** who through human error, lack of situational awareness, lack of attention to detail, and other factors cause harm. A common example is the employee who sends an email without first verifying the content or marking it properly.
3. **Unknown/Compromised Insiders** with compromised accounts are hacked and unwittingly used by cyber criminals, such as the nation-state attack on Sony Pictures in 2014, which resulted in a leak of sensitive employee PII, copywritten content, and business plans.

There are several human psychology and behavioral theories being studied in the academic field which should be considered to understand what motivates an individual to carry out an attack from the inside. For example, the General Deterrence Theory, which has been studied for decades in the criminal justice field, tells us an insider may attack if the perceived benefits to the individual outweigh the expected costs or deterrents. Through the Theory of Planned Behavior, the insider's intentions (e.g., attitude, projected norms, and behavior control) towards crime can predict behavior. Social behavioral theories consider the effects peers can have on the insider. Insiders whose bonds of attachment, commitment, or involvement within the organization are weak (Social Bond Theory), or those associating with delinquent peers who condone negative behavior (Social Learning Theory) may be especially motivated to attack. In addition, there are several studies and models taken from the behavior analytics communities we consider in our approach, to include: Predictive Mitigation of Timing Study (Cornell University), The Fogg Behavior Model (Dr. BJ Fogg), The Transtheoretical Model (Prochaska and DiClemente), and Health Action Process Approach Model (Ralf Schwarzer).

Given that insider threats are a direct result of an individual's behavior and behavior is influenced by how an individual's environment affects their mood over time, it is difficult to understand what motivates an individual unless we understand what factors impact them dynamically. Whether it is positive or negative, all aspects of a person's behavior must be obtained. This allows for Insider Threat programs to move away from a reactive model to more comprehensive and proactive. This model improves an organization's ability to stay ahead of threats before they can affect negative outcomes.

APPLYING CONCEPTS

While a 360-degree profile considers an individual's risk scale across a variety of categories and elements, it takes the process a step further by enabling organizations to mitigate threats before they are acted on. To build an accurate individual profile, organizations need to have a deeper understanding of individual associated characteristics. To find these characteristics, we must determine a common denominator that is not unique. Communication is one characteristic every human has in common. Regardless of what language is used, how an individual communicates is unique to that person. By baselining how a person uses "their language," we can create a behavior trend based on the context of words used. Any anomaly outside of this trend can be an identifier of behavioral or mood changes. Organizations may benefit from introducing additional options to proactively mitigate risks caused by insider threats.

So, why do the factors that change individuals' moods matter? Simply put, every person is a unique individual. While there may be some similarities between individuals, people are not exactly alike. In addition, environmental changes often influence one's outlook and reaction to situations or events. This reduces the ability to predict outcomes due to the unpredictability of how environmental variables impact an individual's reaction to a particular situation. People change in real time.

To effectively defend against damages, Insider Threat programs require a solution designed to focus on what improves individual's mood and behaviors, not to stop the threat, but to dissolve the threat before it can be acted on.

When organizations only focus on identifying an insider threat based on the actions of individual's negative attributes, it is inevitable the reaction a person takes to an event will be negative because of the perception that the impact is inherently negative. By improving an individual's environment, we create a more balanced mood. When we proactively insert a positive environment based only off the individuals' driving characteristics, we provide the individual the emotional balance needed to guide their decision-making process. Positive reinforcement drives positive behavior. This solution presents the Insider Threat program in a positive manner and move it away from the enforcement arm which traditionally may have a less positive inference.

CONCLUSION

Organizations seeking to improve the effectiveness of their Insider Threat program can do so without a large financial investment in tools and technology; instead, they should re-envision an analytical approach that considers a 360-degree view of people's positive and negative behaviors. This solution concept is intended as an enhancement to traditional Insider Threat programs. Predicting does not necessarily mean detection. Insider Threat programs that rely on trend-based prediction for identifying potential insider threats are designed to detect an event after it has become an incident. When an organization shifts the approach from trying to predict when a threat will be impactful to detecting when a threat is developing, the opportunity to mitigate the risk opens sooner. It is impossible to remove all risk of a threat from an organization because risks are dynamic and are determined by too many unknown environmental elements. As such, to be more effective in managing insider threat risks, we must look at ways to intervene before an insider threat can act on a situation that has negatively impacted them.

When applying the 360-degree approach, we create a model that understands people are unique individuals, further allowing us to understand what drives them—instead of statistically grouped into general categories based on overall related similarity. While there are many benefits that can result by taking the 360-degree approach, most notable is the ability to have a more personalized interaction with the potential insider threat. The 360-degree approach provides the opportunity to intervene before an insider threat can respond to a negative situation. Additionally, the 360-degree approach gives organizations the ability for more insight and understanding of the "state" of their workforce.

The concepts discussed in this paper are innovative solutions to improve the effectiveness of how insider threats are managed and improve traditional Insider Threat programs or models designed to respond to an incident. The need for a reactive solution will always remain. However, by applying the 360-degree concept, we introduce the ability to proactively engage with an insider threat, before they are able to take negative action against an organization. Organizations advance to a more holistic approach by leveraging traditional methods and implementing analytical solutions. This allows for a more comprehensive Insider Threat program to mitigate risks and protect an organization's assets, resources, and information.

AUTHOR PROFILE

Dave Boswell
Director, Cyber & Engineering

Joseph Bradley
Director, Law Enforcement Programs

Ketan Mane, PhD.
Chief Digital and AI Architect

Stephen Erikson
Vice President, Strategic Solutions

ECS is a leading information technology provider delivering solutions in cloud, cybersecurity, software development, IT modernization, and science and engineering. The company's highly skilled teams solve critical, complex challenges for customers across the U.S. public sector, defense, and commercial industries. ECS maintains partnerships with leading cloud and cybersecurity technology providers and holds specialized certifications in their technologies.

CONTACT OUR EXPERTS