Using AI to Detect Insider Threats in Your Organization

AI PROTECTS: INSIDER THREAT DETECTED!
Using AI to Detect Insider Threats in Your Organization
AI
User Behavior Analytics

Introduction

An insider threat is a cyber security risk originating from within an organization. While the external threats are real, the insider threat within the organization is also existent, and equally as dangerous.

Insider threats can originate from current or former staff, contractors, or other internal stakeholders with authorized access to sensitive company information such as its database systems and security protocols. In a digital, data driven era, combating insider threats effectively, requires a tool as sophisticated as the threat itself: Artificial Intelligence (AI).

Types of Insider Threats

There are various categories of insider threats. These include:

- **Calculated Insider Threats:** These are threats from persons that deliberately act to destroy or harm and organization. The motives might defer. For example, it can be for financial reasons (trading company secrets or selling intellectual property to a competitor), or for revenge (retaliation for denied promotions).
- **Accidental Insider Threats:** This is far more common but equally damaging. Examples of accidental insider threats includes an ignorant employee clicking on a phishing email, a staff who accidentally sends sensitive information to the wrong person, or misconfigures a server, exposing sensitive customer data. In these instances, the intention was not to cause harm, but the damage is done.
- **Collusive Threats:** These are threats originating from a combination of malicious insiders and external threats, for example outright espionage activities.

An insider threat is a betrayal of trust, and because it comes from a trusted source, it is difficult to detect using traditional security methods.

The High Stakes of an Inside Job

Key decision makers in organisations read news or articles related to insider threats and think **"*This wouldn't happen at my company.*"** The statistics related to this challenge suggest otherwise. According to a report by Cybersecurity Insiders, **83%** of surveyed companies reported at least one insider attack within the previous year.

So how does this affect *you*?

With insider threats on the rise, organisations should be concerned about impact of this trend. This can include financial impact from business interruption, cost of conducting forensic investigations, legal or regulatory fines, and associated devastating reputational damage.

- **For an employee,** a data breach caused by a colleague could create a culture of mistrust and put jobs at risk if the company suffer significant financial losses.
- **For a customer,** personally identifiable information such as debit or credit card details, health records etc. could be exposed and obtained by malicious actors.
- **For a business owner or CEO,** the very survival of your company could be at stake. The loss of sensitive data might attract negative attention or result in law suits. The loss of intellectual property can also erase the competitive advantage built over time.

The summary? Insider threats have the potential to affect everyone and everything connected to an organization.

How AI can help to detect the undetectable

Smart AI systems can help to detect patterns in instances where traditional security or physical security checks do not. AI systems are not just focused on a single “smoking gun”. Instead, it learns the normal "behavioral pattern" of every user and every device on the network.

Let's follow "Jasper," a mid career financial analyst, to see this in action.

- **Monday to Friday, 9 to 5:** For months, the AI systems has observed Jasper. This is Jasper’s typical pattern: He logs in from his office laptop to access the internal financial reporting database, uses his approved accounting software, and occasionally sends emails to colleagues and clients. This is Jasper’s "baseline normal."
- **Waving the Red Flags:** Now, suppose Jasper has decided to leave the company and take valuable client data with him. Over time, maybe a two week period, he starts acting differently. The AI system, continuously analyzing terabytes of log data, detects a series of subtle anomalies. In isolation, it seem harmless, but together form a highly suspicious pattern:
- **Unusual Access:** At 08:30 p.m. on a Friday, Jasper logs in remotely from a home device he has never used before and accesses (read only) the "Merger & Acquisition" project folder, which is outside his usual responsibility.
- **Data Download:** On Monday afternoon, Jasper downloads thousands of files containing sensitive client lists and financial projections to a USB drive.
- **Accelerated Activity:** Jasper’s network traffic logs spikes dramatically. He is accessing and retrieving data at a speed and volume far beyond normal work requirements.

Individually, each event might be explained away. Maybe Jasper is working on a special project with an approaching deadline. Perhaps the USB drive is for a legitimate presentation to management. But the AI doesn't see these as isolated events. The AI system sees a ***correlation* and a *deviation from the norm, the learned baseline*.** It automatically flags this sequence of events as high-risk and alerts the information security team.

- **Context and action:** A security analyst receives an alert. Instead of sifting through volumes of generic log entries, they are presented with a clear, prioritized case: "User Jasper: High Probability of Data Exfiltration." The information security team are now in a position to investigate the challenge.

AI Tools and Techniques for Detecting Insider Threats

Here are four key AI tools and techniques at the forefront of detecting insider threats.

1. User and Entity Behavior Analytics (UEBA)

We reviewed the behavioural pattern of a finance manager deviating from the norm, using an AI system that leverages on **User and Entity Behavior Analytics (UEBA).** UEBA is the cornerstone of modern insider threat detection. It uses machine learning to establish a behavioral baseline for every user and entity (like servers or applications).

UEBA also analyzes activities such as login times and network traffic volume.

These systems will flag significant deviation from a baseline and its power lies in correlating multiple low-risk inconsistencies into a single alert, prioritizing the most serious risks for security teams.

2. Natural Language Processing (NLP)

NLP techniques are helpful for analyzing unstructured data, which constitutes most organizational communication.

NLP models can scan emails, chats, and documents content to detect and highlight potential threats. Beyond simple keyword matching. Sophisticated AI powered models NLP can be used for:

- **Sentiment Analysis:** To detect increase in levels of employee frustration or hostility in communications.
- **Topic Modeling:** Flag debates or dialogs about confidential projects by unauthorized persons or groups.
- **Intent Classification:** Identify potentially malicious instructions buried in seemingly benign emails. This can be a social engineering attempt from one employee to another to bypass controls.

3. Deep Learning for Anomaly Detection in Data Flows

UEBA focuses on user behavior, but deep learning models are exceptionally good at identifying complex patterns in vast data pipelines. These models can be trained on network traffic to recognize what is defined as "normal" data exfiltration versus legitimate business activity.

They can also be trained to detect data being smuggled out slowly over time (a "low and slow" attack) or hidden within encrypted tunnels, patterns that are nearly impossible for humans or simpler systems to find.

4. Predictive Analytics and Risk Scoring

For organisations that would like to move from detection to prediction, machine learning models can be deployed to generate a dynamic risk score for every employees in the company.

This score isn't based on suspicion but on measurable risk factors, such as frequent policy violations, and access to sensitive data.

In such instances, the information security team will shift from a “actual incident and response” approach to a proactive risk based management model, focusing awareness campaigns and monitoring resources on the segments of the workforce that present the highest statistical risk.

Next Steps: Where do you go from here?

Implementing AI for insider threats is a strategic process. It is not just buying and installing software and here are some recommendations on how to get started:

- **Start with Data, Not the Algorithm:** AI systems are only as good as the data they are trained on. Ensure the collection of relevant and comprehensive logs from data sources such as email, network, cloud applications, and endpoint devices. An integrated, comprehensive data source is the foundation.
- **Define the "Normal" for Your Organization:** Work with the information security team and key stakeholders to understand what legitimate user activity looks like. This helps fine-tune the AI systems and reduces false positives.
- **Focus on the mission critical "Crown Jewels":** Identify your most critical asset, such as intellectual property, customer databases, and financial systems. Ensure the AI systems focuses its behavioral analysis on access to these specific resources.
- **Prioritize the privacy of oganisaztional data from the onset:** Be transparent with employees. AI monitoring system should be designed to respect privacy. It should focus on metadata and behavior patterns, not the content of personal communications
- **Don’t forget to add a human in the loop:** AI systems should augment security teams, not replace it. Allow your AI to filter noise and provide insights. However, your information security experts should conduct the final investigation and make judgment calls.

The journey to understanding insider threats teaches us a crucial lesson: **trust, but verify**. In this regard, Artificial Intelligence is like flipping on high end floodlights. It allows us to verify vast details and immediately spotting when something is out of place. It transforms insider threat detection from a reactive game into a proactive, intelligent defense.

Remember, the most significant risks can come from within, human behaviour (calculated or negligent) follows patterns, and we now have the technology to understand and protect against those patterns.

Leverage the ability of AI systems to detect anomalies and combine the experience of human experts to build organizations that are not only secure from the outside and resilient from within.