Intelligence agencies and DOD employing Real-time behavioral analytics, for detecting advanced external and internal threats and mental health

Market research company Forrester report found,"U.S. organisations suffered $40 billion in losses due to employee theft and fraud." " 46% of nearly 200 technology decision-makers reported internal incidents as the most common cause of the breaches they experienced in the past year," writes Chloe Green in Information Age article.

The insider threat has posed significant challenges to US DOD from millions of documents unearthed by former contractor Edward Snowden to recent breach where sensitive personal data of tens of millions of federal employees has been lifted that not only puts individuals at risk, but compromises certain operational practices of the U.S. military/intelligence complex.

Organizations and Intelligence agencies are now using User Behavior Analytics or UBA to detect when legitimate user accounts/identities have been compromised by external attackers or are being abused by insiders for malicious purposes. DARPA, earlier had launched a program known as Cyber Insider Threat (CINDER) that proposed to monitor the "keystrokes, mouse movements, and visual cues" of insider threats.

The National Security Agency has significantly enhanced its capabilities for detecting cyber-threats in the two-plus years

since former NSA contractor Edward Snowden pilfered and disclosed classified information. The multi-layered capabilities, which include user behavior analytics, now protect a private cloud that provides storage, computing and operational analytics to the intelligence community, told CIO Greg Smithberger.

Technology to Find the Next Insider Threat

Organizations must implement ways to monitor and evaluate employees continually. Advanced monitoring tools that identify life stressors, strong emotions, and atypical behavior can provide early warning of potential misconduct or spot small-scale malicious acts before they become something more sinister, writes Daniel McGarvey a counterintelligence expert at Alion Science and Technology.

An initially loyal employee does not suddenly transform into a malicious insider. “The path to a significant destructive act is marked by small infractions that grow in response to mounting personal and professional stress. Employees who engage in one type of counterproductive behavior will often engage in others. Minor misdeeds can escalate into severe transgressions,” writes Daniel McGarvey .

Data on an employee’s non-work activities – such as arrest records, court records, and credit bureau reports – can also reveal concerning behavior. Personality-mapping tools use psycholinguistic analysis to identify personality traits that may predispose an employee to commit destructive acts.

No single technology or technique will be a panacea. Through carefully designed programs that involve technology, human resources, comprehensive security policies, and effective leadership, government agencies and private companies can mitigate insider threat risks in ways that preserve employee

privacy and assist at-risk employees before they can do damage. It may prevent the next Edward Snowden – a development that would benefit both the country and the individual who is diverted from a destructive path, writes Daniel McGarvey .

User behavior Analytics (UBA)

The idea behind UBA is that there's no way to know which users or machines are good or bad. So you assume they're all bad, that your network has been compromised, and you constantly monitor and model everything's behavior to find the bad actors. UBA focuses on what the user is doing: apps launched, network activity, and, most critically files accessed (when the file or email was touched, who touched it, what was done with it and how frequently).

"Old security models have no room for insider threats. As companies pour millions into preventing outside attackers from gaining entrance to their network, they operate under the assumption that those who are granted internal access in the first place are trustworthy," writes Chloe Green. One survey of 355 IT professionals found that 61% said they couldn't deter insider attacks, and 59% admitted they were unable to even detect one.

UBA employs modeling to establish what normal behavior looks like. It searches for patterns of usage that indicate unusual or anomalous behavior – regardless of whether the activities are coming from a hacker, insider, or even malware or other processes. While UBA won't prevent hackers or insiders from getting into your system, it can quickly spot their work and minimize damage.

Derek Lin, Chief Data Scientist at Exabeam, and his team use a variety of supervised and unsupervised machine learning algorithms to detect anomalous patterns of user behavior, as

gleaned from a variety of sources, like server logs, Active Directory entries, and virtual private networking (VPN) logs. UBA then uses big data and machine learning algorithms to assess the risk, in near-real time, of user activity.

Lin tells Datanami. “For every user and entity on the network, we try to build a normal profile—this is where the statistical analysis is involved. And then on a conceptual level, we’re looking for deviations from the norm….We use the behavior based approach to find anomalies in the system and surface them up for the security analyst to look at.”

Next, UBA performs risk modeling. Anomalous behavior is not automatically considered a risk. It must first be evaluated in light of its potential impact. If apparently anomalous activity involves resources that are not sensitive, like conference room scheduling information, the potential impact is low. However, attempts to access sensitive files like intellectual property, carries a higher impact score.

“Consequently, risk to the system posed by a particular transaction is determined using the formula Risk = Likelihood x Impact,” says Saryu Nayyar, CEO, Gurucul. Likelihood refers to the probability that the user behavior in question is anomalous. It is determined by behavior modeling algorithms. Meanwhile, impact is based on the classification and criticality of the information accessed, and what controls have been imposed on that data.

“As insider and persistent threats become more sophisticated and frequent, organizations must employ security intelligence capabilities that can quickly assess, identify and analyze user behavior against risk tolerance,” said Mike Armistead, general manager, HP Security, ArcSight.

Mind-reading AI is the newest defense against cyber attacks

Empow, a security startup, just patented a ‘mind-reading’ approach to cyber-security in order to try and discover these attacks the moment they start. CEO and Founder Avi Chesla says today in a press release:

The innovative technology behind the patent enables a human security expert to understand actual the intentions of any attacker. This “mind reading” is accomplished initially by data gathering – we read the data generated by a variety of tools inside the organization – which is then enriched by Internet data sources which yield more signals and cues. These are harvested from good guys and bad. On top of that we apply of NLP algorithms to draw definitive conclusions about what the attacker is after. No one signal lets us read the attackers’ mind, but we connected the dots to generate intention.

The AI uses all the data it can gather to determine what an attack might look like, specific to the system it is protecting, and constantly monitors everything happening on the entire network. When it doesn’t have enough data from internal sources, it begins searching outside of your network for information that fills in the gaps.

It learns to understand what suspicious behavior looks like at the moment it starts. This allows it to react within the first couple of seconds of an attack with a solution tailored to best defend your network and data. The AI is like a guard dog that comes well-trained and never stops learning how to do a better job of guarding your assets.

NSA’s analytics capabilities thwart internal, external threats

Smithberger says the NSA is using automated capabilities “to up our game” for detecting and responding to anomalies, including anything from external attacks to suspicious internal activity. The NSA is conducting real-time forensic analysis of cybersecurity software and appliances, including firewalls, VPNs and audit logs on every network device “so that we can observe things that humans cannot put together on their own,” Smithberger says.

“But it’s a matter of understanding what is normal on your network, what is authorized on your network with pretty fine granularity … and comparing the observed, in real time, to what has been authorized and what is normal.” Smithberger says that one of the obvious examples includes the capability to spot anomalies as when a credentialed user accesses the network at a strange time and from an unusual geographic location

The agency faces a challenge in balancing the need for maximum security while addressing the privacy concerns of individual users, NSA Director Adm. Mike Rogers said, during a keynote address at the 2016 Billington Cybersecurity Summit

DOD using behavioral analytics to thwart insider threats

One of the technological approaches DOD is working on to mitigate the insider threat is behavioral analytics. Mark Nehmer, deputy chief of implementation for DITMAC said, to compile the indicators, characteristics and behaviors associated with insider threats, including “how they’ve written, where were they in social media, where were they in their work life, where were they in their personal life that

we know of that we can find – as deep a dive as we can get on the individuals that we know have actually committed insider threat behaviors." But despite the push of what Nehmer called this "human science," he said he's not sure when DOD will be able to establish verifiable metrics for identifying insider threats.

The other component to the behavioral issue is tying it to authorizing users within the network. The network can understand and take a benchmark on all kinds of normal behavior based on analytics. Whenever any anomalous activity takes place in network then in real time, the network can respond by either stopping traffic and calling for more analytics or shutting down operations until a human authorizes the activity.

VA contracts with DARPA-backed startup for real-time behavioral analytics, mental health app

The U.S. Department of Veterans Affairs has contracted with Boston-based startup Cogito for use of its real-time behavioral analytics mobile app that analyzes voice recordings and mobile phone usage to create clinically validated behavioral indicators of mental health.

The agency said it will use the Cogito app to detect veterans in need of mental health care, including suicide prevention. The predictive behavioral model has been validated through research by agencies including the Defense Advanced Research Projects Agency (DARPA) and The National Institute of Mental Health (NIMH).

The Cogito technology was developed in more than 15 years of research at the MIT Media Lab; the Companion app is intended to reveal unconscious signals in the human voice that disclose

information about relationships and state of mind.

References and Resources also include:

http://www.defenseone.com/ideas/2017/04/want-plug-intelligence-leaks-let-modern-technology-background-checks/136729/?oref=defenseone_today_nl

https://thenextweb.com/artificial-intelligence/2017/09/11/mind-reading-ai-is-the-newest-defense-against-cyber-attacks/#.tnw_sTeBiwiH