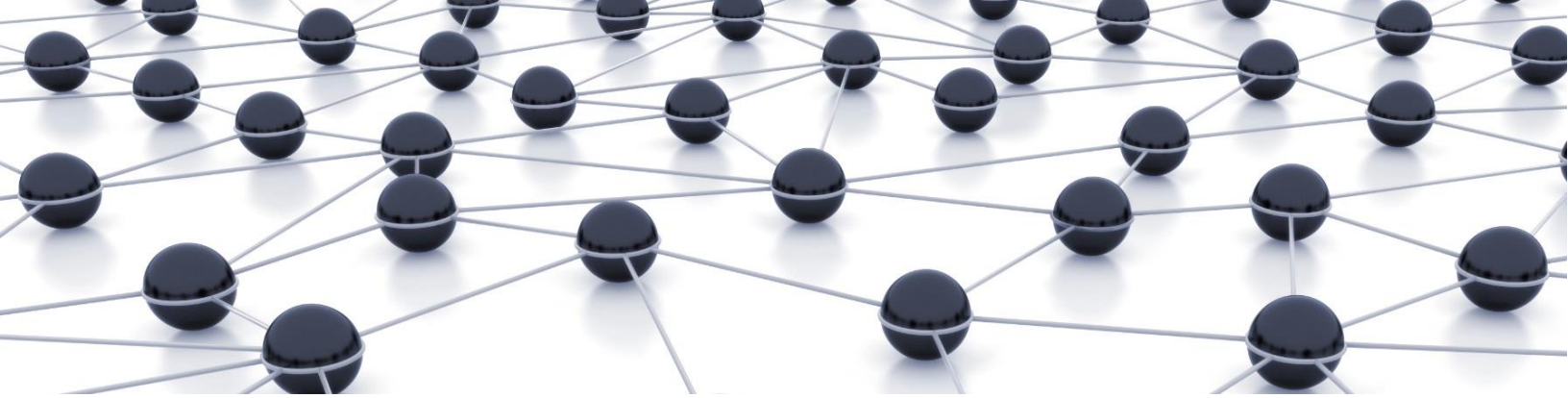

IntelliSyn

Desktop-to-Cloud Business Communications

Detecting Enterprise Threats with the Applications Behavioral Analytics

By Merv Perry MBA MSc CISSP CISM

We are all aware of valuable assets that have sensitive data content and are critical to a company's survival. Their loss as a result of unauthorized access and distribution by cyber criminals or negligent employees and others means are a challenging forensic effort and an expensive ligation to obtain a conviction without substantial proof. The use of a real-time behavioral analytics engine to track the risk and sensitivity of accessing a device's information content by users can score and prioritize real high-risk activities within the vast amount of daily activities occurring within a system. There are algorithms to get beyond the noise of day-to-day operations, which minimize false positives by optimizing risk modeling through machine learning to adjust risk weights with changing business processes. These algorithms produce a clear picture of the true risk and threats before they become very high threatening anomalies, and provide policy alerts on violations. Currently, there has been a reliance on Harmonized Threat Risk Assessments (HTRA), with them being conducted on an annual or semi-annual basis to determine what exposure the organization has been subjected to. However, this activity comes far too late when the enormous volume of data in log files reveals past exposure or vulnerabilities.

Everyone is a target and nobody can be trusted if there is an opportunity for abuse or negligence.

Detecting Enterprise Threats

The biggest transformation in businesses today is comprehensive IT security and protection of valuable assets, which have sensitive data content and are critical to a company's survival. It is not the size of the company but more what a company has that is valuable to the marketplace. You can be a small chain of restaurants with a secret chicken recipe, a large department store with customer credit card numbers, or a little medical clinic with private health records. Everyone is a target and nobody can be trusted if there is an opportunity for abuse or negligence. The sooner you can detect the start of an attack, the

lesser the chance of severe damage. However, if you can detect changes in behavior, then you might mitigate the attack before it begins.

The use of a real-time behavioral analytics engine to track the risk and sensitivity of accessing a device's information content by users can score and prioritize real high-risk activities within the vast amount of activities performed daily. A behavioral analytics engine uses a series of algorithms which scores the risk of breach and prioritizes the events it deems as high risk while filtering out background noise and false positives. Through machine learning, it optimizes the risk model by adjusting the weighting assigned to risky events in real-time business processes. Therefore, a clearer picture of the actual risk and threats emerges before an attack occurs. The event's metadata is collected from across the enterprise and the policy engine alerts to violations. Anomalous behaviors will surface and show in the dashboard display, making it easy for non-technical personnel or senior management to grasp the significance of the threat.

Many companies are working on detecting enterprise threats with behavioral analytics.

Intellisyn Communications is a managed service company with a desktop-to-cloud approach to managing a client's enterprise information system. We regularly explore new technologies to determine if our clients might have an interest and to understand better the technological changes in the marketplace. Companies are working on detecting enterprise threats with behavioral analytics. Their analytics software tools may eventually replace the need to perform Harmonized Threat Risk Assessment. Such an assessment is only valid to the date it was performed as circumstances can immediately change.

The threats we are facing becoming increasingly more complex as insiders or privileged users include customers, business and technology partners, and service providers. The volume of legitimate user behavior makes detecting real user-based threats nearly impossible when combined with the malicious activity. However, with the right tools, specific threats such as inappropriate insider activity, abuse of privileged accounts, abnormal user behavior, and compromised credentials become indicators for an early warning system. Security administrators can detect and neutralize user-based threats before such behavior results in a major impact on the business.

One of the biggest potential security hole or threat in any organization's network is user compromised or stolen credentials, even when they belong to a legitimate insider. Outlined below are the compromises to user credentials that a behavioral analytical engine can detect. Some firewalls have this built-in capability, but this ability tends to be towards defense against outsiders, not insiders.

Account Takeover
This occurs by stealing legitimate credentials and the taking over user accounts by hackers who try to infiltrate IT's defenses. An abnormal behavior pattern with a user account might indicate that it has been compromised and is being used for malicious activity. The behavioral analytics engine uses automated profiling to baseline what it considers as "normal" user behavior based on security policies. The engine immediately notifies the security team of abnormal account activity, such as authentication from a strange location, unparalleled access to sensitive data, or the use of unauthorized endpoint devices. It might initiate an action where it disables the account and/or quarantines the device.

Privilege Abuse
A significant insider threat occurs when account privileges are escalated for short term access and may be forgotten. This poses an ongoing means of providing administrative access and high clearance levels with direct access to sensitive data systems and privileged user accounts. The abuser can potentially steal sensitive data, intellectual property, health records, and credit card data. The advanced behavioral engine uses analytics rules and activity reports specifically to monitor privileged user activity. These tools can detect and automatically neutralize threats by disabling or quarantining privileged user accounts. The tools may send mobile alerts to the security staff on the threat and request the next action.

Behavioral analytics can associate any activity that might be indicative of a potential breach based on the account activity.

Account Creation/Deletion/Modification
Once a hacker has broken through the IT perimeter, they will start to determine ways to escalate the privileges of a compromised account, or create new accounts and move laterally within the network to conduct a broad range of malicious activities. Once their objective is accomplished, these escalated privileges and new accounts are frequently deleted. They will make efforts to hide any evidence of their presence, which makes both real-time detection and forensic reconstruction difficult. Behavioral analytics can detect the addition of new accounts, as well as changes to existing accounts based on policy rules like one account per person and limiting the number of highly restricted access accounts. Also, behavioral analytics can associate any activity that might be indicative of a potential breach based on the account activity. An administrator is automatically alerted to sophisticated user account manipulations so they can rapidly investigate and take corrective action before significant damage occurs.

Suspicious Remote User Activity

The expansion of mobile workers has made remote access easier to exploit and harder to detect. The implementation of multiple rules to detect activity, including multiple VPN logins for the same user, multiple password resets, and even multiple login attempts from different locations, are indicators of account takeover attacks. The behavioral analytical engine can help organizations quickly modify existing rules to detect the aforementioned scenarios in real-time to follow a prescribed action to minimize access and damage. Especially when a user's access badge is being used within a short period of time before or after that same user logged in via VPN from a remote location.

Brute Force Compromises

Despite increased user awareness of the importance of security, organizations still remain vulnerable to attacks that exploit default or weak passwords. An attacker can apply one of many simple automation tools to crack a password. These tools are obtained for free and downloaded via the Internet. They are used to make brute force and repeated access attempts using common or overly simple passwords. A behavioral analytics engine is able to detect unauthorized access attempts with rules that detect malicious activities like distributed brute force attempts, an abnormal number of failed logins on the same host, or an unusual number of failed login attempts using the same account from different machines. Other rules can be used to identify activity that may be indicative of a successful attack and block it, such as a brute force attack followed by one or more successful logins from the same point of origin.

Patented algorithms apply probability equations with Bayesian probabilities as the underlying determination of risk

There are algorithms to get beyond the noise of day-to-day operations, minimizing false positives by optimizing risk modeling. This is done through machine learning to adjust risk weights with changing business processes to detect the more sophisticated insider attack. They use patented algorithms that apply probability equations with Bayesian probabilities as the underlying determination of risk. They examine the folder and file metadata to determine if the user has rights of access based on the probability of whether the user has ever accessed it before and the frequency and likelihood of them needing to do so again (if it calculates the probability of risk to allow access as low). Security policies and privileges are set by the data owner and weights are applied to determine if a notification of access is to be given and the identity of the user is recorded. The engine can tag the file or folder and track where and when it is opened again within the system, what action is being requested, or where it went to. This is all done without the user knowing they are being watched in real-time for violations. The accumulation of even minor infractions of security policy can trigger alerts to security staff to increase monitoring or call the user in for questioning.