Implementing a User Activity & Behavior Monitoring program

Introduction

Monitoring user activity & behavior has significant benefits:

- Increased security against insider threats
    - o Detection, the number one priority when dealing with insider threats, requires visibility into user activity and detecting for anomalies in user behavior
    - o Responding to insider threats requires detailed, contextual activity data that can be easily digested by the extended response team

- Productivity increases driven by:
    - o Identifying employees having trouble staying on task so that they can be managed effectively
    - o Identifying the top "time drain" activities enterprise-wide; implementing and tracking adherence to policies designed to maximize productivity

- More efficient and effective employee investigations, leading to:
    - o Termination protection – documentation of justification to head off wrongful termination claims
    - o Reduced cost associated with investigations through less time spent assembling evidence and reducing reliance on expensive, specialized skill sets forensic tool sets require

Security & Risk professionals recognize the value and benefits of analyzing user behavior and monitoring user activity. At times, legal and HR staff have questions that must be addressed prior to implementation.

This document is intended to assist company executives determining how to best implement a user activity monitoring and / or user behavior analytics program.

Decision Point:
Why Monitor Employee Activity & Behavior?

The decision to begin monitoring employee digital activity is usually made for one of two reasons:

- **Reactive Investigation:** Something bad has happened or there is suspicion that something bad has happened or is about to happen. The organization has cause to investigate a person or group of people.
- **Proactive Strategy:** The organization seeks to improve its internal security against insider threats, improve productivity and efficiency, or both.

The Reactive Decision

When an investigation is required, the decision to implement an employee monitoring solution is easy. Something triggered the need to look more closely at employee activity. While there is no cookie-cutter approach to employee investigations, Management, HR, and Legal are generally heavily involved and upfront in the decision on how an organization handles investigations in general, and whether to kick one off specifically.

The Proactive Decision

The decision to implement proactive employee recording has the potential to be more complex than kicking off an employee investigation. The proactive approach requires logging digital activity of employees in the absence of a trigger. In addition, for maximum effectiveness, proactive monitoring must be widely deployed.

Without a trigger or "probable cause" (any known reason to take a closer look), the organization may be less comfortable collecting user activity data.

Decision Point:
What is Right for Your Organization?

Is there a way to implement user activity monitoring and behavior analytics that aligns to your corporate culture and values, the legal considerations where you do business, and the needs and goals that have you considering employee monitoring?

Where to Start

While every organization is unique, there are some broad guidelines that can help you make the best decision for your company.

1. Determine your goals
2. Review your Acceptable Use Policy
3. Consider involving your employees
4. Decide whether to implement activity monitoring, behavior analytics, or both
5. Decide what to monitor and what data to retain
6. Decide how to handle escalation and review

Get the Stakeholders Together

Company size and structure will determine who needs to be in the room when working through the 6 guidelines.

As a general rule, include the most senior person in the organization in these decisions.

- **Senior Management:** The CEO or someone designated in his/her stead.s
- **Human Resources:** The head of HR as someone who balances the needs of the company and of the employees every day.
- **Legal:** Your General Counsel or whomever you go to for advice on legal matters.
- **Information Technology:** An IT expert who will be involved both in evaluating possible solutions and implementing the solution you select.

Decision Point: What are Your Goals?

Detect Insider Threats

If you are concerned about insider threats, it's important to talk through the challenges of detecting and deterring them. Non-technical stakeholders may not know coming in that traditional security solutions are (a) largely focused on perimeter security and (b) not intended to identify or prevent problems stemming from insiders who have been granted authorization to access sensitive data or systems.

So, for example, data theft by an insider may go undetected for a long period, or, in the worst case, until you read about it in the news. Employee fraud may go unnoticed until the annual audit, if it is noticed at all.

Inadvertent vs. Malicious Activity

Expect a discussion on monitoring activity to touch on the fact that it's likely only a small number of employees intentionally engaged in behaviors that are problematic. Be prepared to talk about the difference between inadvertent breaches or policy violations and intentional, malicious ones.

Focus on the resultant damage, not the intent.

Resources for Discussion

There are some great resources available to help frame the discussion and help you establish the right goals for your organization.

The Association of Certified Fraud Examiners ("ACFE") Report to the Nations on Occupational Fraud and Abuse is a fantastic source of information on the various types of fraud being committed, and the damage that fraud causes to a companies bottom line.

The www.cert.org website is an outstanding resource for insider threat related information.

Action Item: Review Your Acceptable Use Policy

If your company does not have an Acceptable Use Policy, now is the time to put one in place. An Acceptable Use Policy ("AUP") serves multiple purposes. It spells out your policies clearly, so that your employees know what is acceptable or not. In this document, you disclose to employees or others you grant access to your corporate network and resources (contractors, for example) that all electronic communication taking place, and all information stored, on company resources is monitored and subject to review.

Make sure all employees receive a copy your AUP, and acknowledge that receipt – either in writing during their onboarding, or more ideally every time they logon via a click through.

The two relevant federal laws in the US to review prior to publishing your AUP are the Electronic Communications Privacy Act of 1986 ("ECPA") and the Computer Fraud and Abuse Act.

The ECPA has two relevant titles – Title I is the Wiretap Act, and Title II is the Stored Communications Act. Both include Consent and Course of Business exemptions.

A few states have laws that require disclosure of monitoring – Connecticut and Delaware were the first to pass this type of law. Colorado and Tennessee have laws specifically regarding the monitoring of public sector employees.

As a best practice, disclosure is recommended whether local law requires it or not.

Action Item: Review Your Acceptable Use Policy

It's up to you whether or not to disclose the means by which you monitor. Some companies do, others believe that disclosing the means can lead to employees seeking ways to get around the monitoring, and so choose not to.

Decision Point:
Consider Involving Your Employees

Your employees are invested in your success and want to contribute to it.
Employees will feel the negative impacts of successful insider threat activity.

Consider having employee representation in the meetings where you are weighing the proactive decision.
If your goals are clearly articulated, you will find more support than expected - especially if you do a good job of balancing the needs of the company with employee privacy.

Needs of the Company vs. Employee Privacy

Every organization needs to determine the right balance between the needs of the company and the privacy of their employees. Remember, the vast majority of employees have the companies best interests in mind. Remember, too, that many policy violations and internal security problems are the result of inadvertent mistakes, or lack of knowledge of what is expected or allowed. Finally, remember that employees can be deceived or their credentials compromised. An adversary, no matter how skilled, will cause a deviation from normal behavior patterns when they attack.

To strike a balance that's right for your organization, you need options. User Behavior Analytics looks at patterns of behavior, and does not require inspection of the content of an employee's activity to deliver on its promise of detecting insider threats. User Activity Monitoring includes the ability to capture, and review, the specific actions of an insider's activity – including the content of their communications if desired / needed. Look for a User Activity Monitoring solution that enables you to configure the types of activity monitored to align to your goals, and that has privacy protections woven throughout to address the concerns.

Decision Point:
Consider Involving Your Employees

User Activity Monitoring

A User Activity Monitoring solution records employee digital activity, making the collected data available for review, reporting, and retention. Sometimes referred to as user or employee surveillance, it is typically employed where there is cause to do so.

Causes for User Activity Monitoring include three main types:

Investigatory Cause

Similar to probable cause in the criminal justice world, Investigatory Cause exists where there is a reason to suspect an employee or group of employees is engaging in behavior detrimental to the interests of the organization.

Role-Based Cause

Some positions within the organization have elevated privileges, with the ability to access information that would otherwise be off limits for their functional role. System Administrators and Database Administrators are two examples of highly privileged users (sometimes referred to as "super users"). The definition of an insider threat is use of authorized access in an improper way. Given the disproportionate amount of damage that can be caused by a highly privileged user, many companies apply significant scrutiny to the activities of users in these roles. Employees / Insiders that have a role-based cause to be monitored are generally users that belong to the "higher risk pool" within your organization. For more information on assessing and assigning risk, please read Risk Mitigation: Keeping employee risk from becoming insider threat, a Veriato whitepaper.

Conditional Cause

Numerous studies, along with research by the highly respected CERT Insider Threat Center, teach us that employees leaving an organization, whether by their choice or by the organization's, take Intellectual Property and other proprietary corporate information with them when they leave. This is a prime example of Conditional Cause – a condition, or situation, exists that requires additional protections be put in place. Other examples of Conditional Cause are found in Risk Mitigation: Keeping employee risk from becoming insider threat, a Veriato whitepaper.

User Behavior Analytics

A User Behavior Analytics solution looks at patterns of human behavior, as relates to interactions with company resources and information, and detects for anomalies that suggest insider threat. User Behavior Analytics exists to detect insider threats; as such the only cause typically required to warrant deployment is a desire to protect the company from the damage an insider attack causes. User Behavior Analytics does not require the retention and review of user activity to perform its function. That said, having the capability to review user activity data when needed is a powerful compliment and offers significant benefits for identifying distinct threats and for responding quickly.

The Right Mix

Some organizations will determine that User Behavior Analysis is sufficient to accomplish their goals. Others will determine that a mix of User Behavior Analytics and User Activity Monitoring makes sense for them— combining broad deployment of the behavior analysis capability with more targeted use of the activity monitoring capability as needed to provide the proper coverage. Finally, some organizations, seeking to receive the maximum benefits from their employee monitoring strategy, will broadly deploy an User Activity Monitoring solution as well as a User Behavior Analytics solution.

As you determine which mix is right for you, you are beginning to define requirements for a solution and the characteristics you are looking for in a provider.

Decision Point: What to Monitor?

The goals you have should dictate which employee activities are monitored and behaviors analyzed. Employee privacy concerns usually revolve around collecting data on some very specific employee activities, such as visiting personal websites or sending personal email.

For example, if you were concerned about what is being done by employees with access to sensitive data, you would want to monitor program activity and track documents. If you have productivity concerns, you might want to monitor websites visited and applications used.

Since all employees are insiders, with some level of risk associated with them, choosing to deploy behavioral analytics across your entire user base will typically make the most sense.

Privacy of Personal Activity

To maintain employee privacy, you can take simple steps, such as not recording your employees' online banking sites or an HR portal where personal information is visible. By aligning what you monitor with your goals, you can achieve them without unduly compromising privacy.

Privacy of Passwords

Unless one of your goals is monitoring for improper use of someone else's credentials, most monitoring of employee activity is about what they access and what is done with data, rather than the credentials used. Look for a solution that gives you the option to capture or not to capture things like personal web passwords. There may be times that capturing a password is necessary, but it is not necessary all the time.

Decision Point: Retention and Storage

Now that you have determined how and what to monitor, you need to decide how long you retain the collected information, and where it is stored. User Behavior Analytics will retain the baseline data, and continuously build upon it to improve the accuracy of anomaly detection. User Activity Monitoring solutions, since they collect significantly more data, require some additional thought.

How Long?

Some organizations retain the user activity data recorded for only a short period of time. These companies are interested in having enough data to determine what happened before, during and after an alert or other trigger – but do not wish to maintain an archive of employee activity. Shorter-term retention makes sense if your goals include having enough data available to get a fast start on investigating an employee when needed – for example, when your User Behavior Analytics solution detects anomalous behavior or during the high risk period just prior to an employee giving notice of resignation / departing the company.

Companies engaged in User Activity Monitoring are often interested in maintaining a longer record of employee activity data, to enable audits, prove compliance, or support longer term investigative needs. Make sure the solution(s) you select allows you flexibility in defining the retention period.

Where?

Where the data is retained is another key decision point. Cloud based solutions offer lower infrastructure burden, but may not enable long-term retention without incurring additional costs. Additionally, depending on the activity you are logging and retaining, you may be putting data in the cloud that you otherwise would not.

If you are deploying a User Behavior Analytics solution, consider one that temporarily stores the activity data that underpins the baselining and anomaly detection – so it is accessible if you need it to investigate and respond to an incident.

Decision Point: Alerts, Escalation and Review

Establish review and escalation procedures related to user activity data. Just because IT is essential to the evaluation and implementation of your chosen solution does not mean you have to task them with reviewing all of the data. Determine who in your organization should have access to the employee activity data, and under what circumstances.

Who Receives Alerts?

Here again, your goals and organizational structure will inform your decisions.

Anomaly alerts from your User Behavior Analytics solution should always be routed to the people in charge maintaining security in your organization. Since User Behavior Analytics is all about insider threat, you need the people primarily charged with response to receive the alerts.
In larger organizations, alerts are routing to your SIEM and to you Security Analysts in your SOC. Organizations that do not have a SOC or might not be employing a SIEM will want these alerts to route, most likely, to your IT team.

User Activity Monitoring alerts related to securing resources and information should follow the same routing as User Behavior Analytics alerts. Beyond that, if you are using alerts as part of an employee investigation, you will want to route them to the person or team conducting that investigation. If you are monitoring for productivity purposes, the employee's supervisor or manager is likely the best person to receive alerts and reports.

As a general rule, alerts should be routed to the experts in your company who are in the best position to determine the severity of a potential problem, so that the appropriate response can be formulated.

Who Receives Activity?

One of the compelling benefits of user activity monitoring is that review of what was done, by whom, and in what context, can be conducted quickly, accurately, and efficiently. This does not mean that review should be taken lightly, however, or that "anyone can do it."

Perhaps the most important decision you will make is determining who has the ability to review detailed employee activity records.

In situations where user activity monitoring is being conducted, the review processes and procedures are in use continuously. A look back at the "causes" for active monitoring is useful here.

Investigatory Cause

In the event of an investigation into a suspected incident, your company's employee investigation procedures go into effect. Who can initiate an employee investigation? Who needs to be informed that an investigation is needed? Starting? Concluded?

A best practice for companies conducting passive monitoring, that have determined sufficient probable cause exists to warrant tilting the balance from employee privacy towards the needs of the company, is to employ a "two missile key" approach. Require at least two approvals prior to kicking off an employee investigation – ideally one from HR or Legal, and the other from a senior manager or their designee. Split the ability to access the employee activity data into two pieces as well, to insure proper procedure is not circumvented.

Role-Based Cause

Using the same highly privileged user example referenced earlier, consider having regular, random, reviews of sys admin or database admin activity conducted by someone outside of the IT chain of command (your CISO, for example), if your company structure allows for it. If that is not an option, have the most senior person in your organization that is directly responsible for protecting the company's data and sensitive information conduct the reviews. The disproportionate amount of damage highly privileged users can cause requires a proportionate amount of scrutiny be applie.

Conditional Cause

Given the powerful statistical evidence that departing employees take corporate IP with them when they leave, having IT security review the digital activity of employees in this high risk exit period is not only prudent – it should be mandatory.

Action Item: Ensure Adherence to Policies and Procedures

Whatever policies you put in place, make sure you are auditing compliance with those policies. And make sure you select a solution that supports that need. By having controls in place that both prevent changes from being made by unauthorized personnel and log (and alert on) any changes made, you gain the piece of mind that your controls are not being circumvented, and the ability to confidently assure anyone who may have concerns that you've taken appropriate steps to implementing employee activity monitoring the "right way."

Veriato 360 Resources

Free Trial

Go to www.veriato.com for a Free Trial or email us at: sales@veriato.com

Corporate Offices

Veriato, Inc.
4440 PGA Boulevard, Suite 500,
Palm Beach Gardens, FL 33410
1.888.598.2788
1.772.770.5670

International

United Kingdom
C2, Dukes Street
Woking
Surrey, GU21 5BH
+44 1483 397744