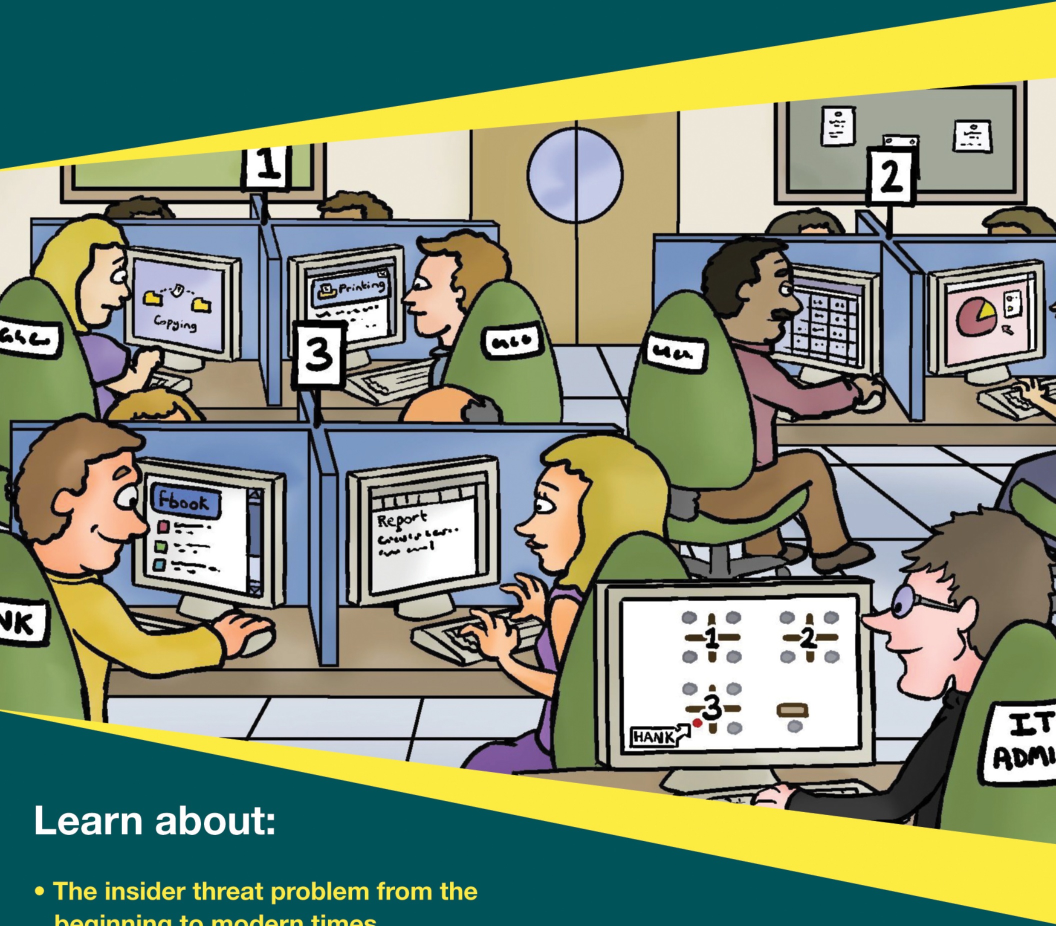
Conversational
User Behavior Analytics

A ConversationalGeek® Book



Learn about:

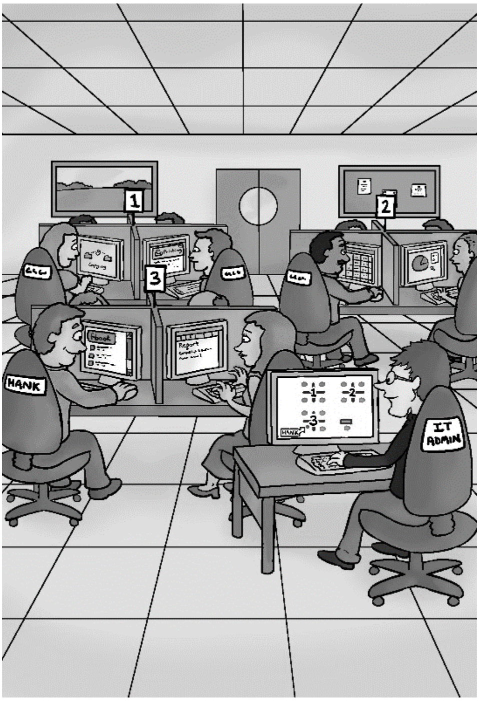
- The insider threat problem from the beginning to modern times
- How User Behavior Analytics can efficiently and effectively address Insider Threats
- The value of using a third-party solution like Veriato Recon

By Derek A. Smith (Certified Information Systems Security Professional)

Conversational User Behavior Analytics

By Derek A. Smith

Copyright© 2016



ConversationalGeek™

Conversational User Behavior Analytics

Published by Conversational Geek Inc.

www.conversationalgeek.com

All rights reserved. No part of this book shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without written permission from the publisher. No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

Trademarks

Conversational Geek, the Conversational Geek logo and J. the Geek are trademarks of Conversational Geek™. All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. We cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an "as is" basis. The author and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or programs accompanying it.

Additional Information

For general information on our other products and services, or how to create a custom Conversational Geek book for your business or organization, please visit our website at ConversationalGeek.com

Publisher Acknowledgments

All of the folks responsible for the creation of this guide:

Author:	Derek A. Smith
Project Editor:	J. Peter Bruzzese
Copy Editor:	John Rugh
Content Reviewer(s):	Karla Reina

Note from the Author

Since the dawn of shared computing people have pushed to expand the envelop of productive group thinking. What once took an army of engineers and mathematicians a week to compute could be done in minutes, then in seconds, then in milliseconds, and now virtually instantaneously. And with that expanded envelop of productivity has come an explosion of data to be mined, analyzed, sifted, and reorganized into yet greater productivity.

Shortly after the dawn of shared computing another interesting phenomenon developed: insider threats. As a special agent with various government and military agencies, I spent years chasing the malicious, and not so malicious insider.

For years, cyber security has focused its resources on stopping the intrusive attack from without. But very little has been done to stop attacks perpetrated from within the system. As perimeter defenses have become increasingly insurmountable, cybercriminals have switched to more insidious tactics whereby they can enter the front door as if they were trusted friends. Once in, it may only take a few minutes for them to cause significant damage to a company's finances, reputation, and relationships. And they can often keep up their attacks at their leisure, in complete anonymity, from a safe location far from where they are striking.

But what if we could teach the security system to look at users like we might look at an individual whom we know well? Then the system might notice slight elevations in a person's stress level that indicated something was wrong. The system might learn to question why a user is logged in three times from three separate locations that are miles apart. It might even perceive that a user really isn't who he claims to be.

If all this were possible, then the profound security weakness common to all perimeter defenses – the virtual area inside the defense perimeter – would be watched over by a security guard who knows each user personally, by name, and by habit.

Welcome to the reality of User Behavior Analytics!

Derek A. Smith

The “Conversational” Method

We have two objectives when we create a “Conversational” book: First, to make sure it’s written in a conversational tone so it’s fun and easy to read. Second, to make sure you, the reader, can immediately take what you read and include it in your own conversations (personal or business-focused) with confidence.

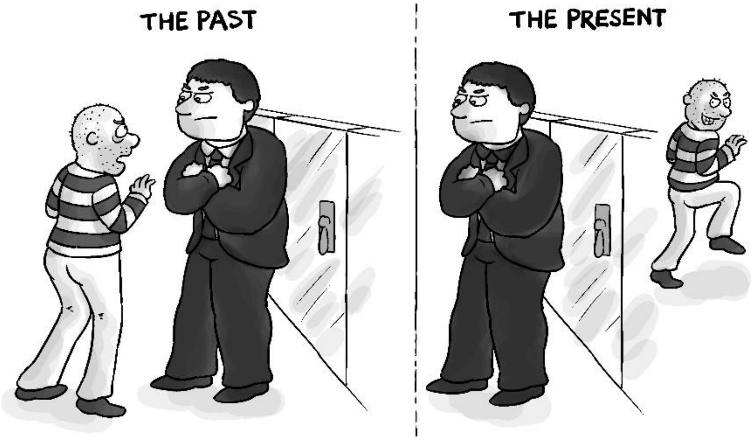
These books are meant to increase your understanding of the subject. Terminology, conceptual ideas, trends in the market, and even fringe subject matter are brought together to ensure you can engage your customer, team, co-worker, friend and even the know-it-all Best Buy geek on a level playing field.

“Geek in the Mirror” Boxes

We infuse humor into our books through both cartoons and light banter from the author. When you see one of these boxes, it’s the author stepping outside the dialog to speak directly to you. It might be an anecdote, it might be a personal experience or gut reaction and analysis, it might just be a sarcastic quip, but these “geek in the mirror” boxes are not to be skipped.

Within these boxes we can share just about anything on the subject at hand. Read ’em!

Chapter 1: The New Level of Threat



Computer security has changed as much as the computers they secure. I remember back when I was a special agent and high-security meant two locked doors and an imposing guard. On a heightened alert day, the guard might even check your briefcase as you entered and again when you left.

Presumably he was checking to ensure no sensitive materials were "inadvertently" smuggled in or out. And here I thought that guy was looking for my Snickers…

But whatever he was doing, I was always fully aware of one inscrutable fact. That guy was scary. He was a singular bulwark against malfeasance. I am sure the deciding factor for his hire was his seemingly innate power to produce great beads of fear and intimidation on the upper lip of anyone foolish enough to approach the sacred doors in an unworthy manner.

As exciting as they were, those simple, carefree, computing days are gone. Against today's security threats that guard is no more threatening than a field full of daisies on a warm spring day. And the double locked doors are less than a speed bump for those getting away on the information superhighway.

Since the first days of shared computing, IT professionals have worked hard to keep honest people honest and others out of the system. Yet, human nature is what it is. If you tell people they can't do something, someone will set out to prove you wrong. If you tell people they can't get in, someone will make it their mission in life to prove you wrong. If you tell people that information is private, you're just begging for someone to take it public.

In the early 1960s MIT produced one of the first ever time-sharing computers, the CTSS. For this system a simple password security system was set up to help multiple users keep their own work separate from that of others. One of those users, a Dr. Allen Sherr [(1)], was frustrated that he only was allotted four hours per week on the computer. That was not nearly enough crunching time to work through his analysis of the new computer system. So, like any good, dedicated employee faced with an unreasonable restriction to getting useful results, he simply found a way around.

Late one night in 1962, Sherr printed out all the computer passwords, thereby granting himself unlimited access to the computing time.

Of course such a work-around was utterly unethical since he was stealing computing resources from other users. Surely those pesky security people would soon discover his actions and … well, this was the glory days of intimidating security guards. Ah, but the good Dr. Sherr was a smart one. In order to cover his tracks, he distributed the password list to other users. And just like that, his computing problems were solved! Sherr had the access he needed to get his very important work done, and security could not possibly pin the breach on him as half the users were also taking advantage of the security gap. One of those other users, J. C. R. Licklider, used his newly enhanced access to log into the account of the computer lab’s director and leave “taunting messages.”

And with Sherr’s “perfectly understandable” response to unreasonable resource restrictions came the birth of a whole new IT activity. Since then it has been an unending cat-and-mouse game between security and hackers. This game has progressed and evolved in perfect sync with every advance in technology. Sherr was one of those IT professionals working for MIT to advance computer technology. Ironically, he became the first known “insider” threat to security.

Where the Threats Reside

When faced with the possibility of failing to complete the top-level analysis of MIT’s new CTSS multi-user computer system because of a lack of computer resources, computer scientist, Dr. Allen Sherr invented a “harmless” work-around. In the end, the tech savvy IT insider was the first significant insider threat. Just as it was back in 1962, the REAL security threat is already ***INSIDE*** *the system.*

Typically, when we consider security threats we focus on outside attackers. For example, when the Internet was young and innocent an MIT graduate student, named Robert Morris, decided to determine the size of the Internet. To do so he created a small program that had a singular purpose – to replicate. The so-called Morris Worm traveled out of his MIT terminal and serendipitously entered every computer it could. The idea of a self-propagating program that “counted” internet users was harmless enough. But the worm did not always replicate and count as Morris intended. On some systems the worm would reproduce like an out-of-control parasite, resulting in a system crash. Morris contends that the resulting chaos was purely unintentional. Yet the damage had been done. The Internet was no longer an innocent place.

These days' outsider attacks are far more sophisticated than Morris' "no payload" worm. There is, for example the brute force attack. With this strategy the attacker uses a sophisticated algorithm to guess at passwords where usernames are known. Using modern computing power and off-line resources, hackers can churn through 30 million password variations in the blink of an eye. It is only a matter of time before matching credentials are discovered. As soon as that happens the hacker has open access to potentially sensitive company and customer information. The time from when an attacker identifies a potential target to the time exfiltration happens is, in computer time, almost instantaneous.

A brute force attack is so boorish, though. It's like a bull walking through a china shop. Not at all how James Bond would do it.

Some attackers prefer a more suave approach. Once possibility is to launch a Rogue Update attack. This strategy makes use of some password guessing, but the real target is other software, possibly a POS system. Once the attacker has access to the POS system a fake update is uploaded that actually downgrades the POS system to a more vulnerable version. The attackers then can come and go at their leisure to collect sensitive information. Because the attacker has the proper credentials to upgrade (or downgrade as the case may be) the attacked system software, it does not matter if the administrator applies security upgrades. The attacker simply comes back and reapplies the downgrade and re-establishes the vulnerabilities.

Once the attacker has identified a potential target, it takes about six hours to begin exfiltration.

Other attack strategies exist that do not depend on brute force. From the familiar phishing attempts to con individuals out of their credentials, to exploitation of known & new vulnerabilities, to network protocol and application attacks, the attackers' goal is to extract sensitive information. Of particular value are user credentials that can be utilized for further attacks.

More patient attackers can do an inestimable amount of damage through a so-called Watering Hole attack. One possible scenario happens when a legitimate user goes online seeking to download a driver for a specialized system. A downloaded executable file then launches a malicious DLL, leading to the user's computer being compromised with a remote access trojan (RAT). Once the RAT is operational, anywhere the user thereafter roams also becomes infected. Under such attacks, legitimate users going about legitimate business can become unwitting servants of the attacker. Attacks of this nature take advantage of trusted relationships and can easily spread beyond the reach of the initial user or the user's system. The time from identifying a potential target to exfiltration may be around two months and the extent of the damage that can be done in such an attack is hard to estimate.

Computers Cannot Tell Friend from Foe

Once an actor is on the inside it does not matter his intents. As soon as an actor's credentials are verified the computer sees him as a trusted user. Convenient for cyber attacker.

When considering the foregoing outside attack methods, an obvious pattern quickly emerges. IT security measures have increased with the sophistication of outsider attacks. Firewalls have been constructed. Stronger passwords with short lifecycles are now required. Security upgrades are regularly installed. The hardware and software developed to keep illegitimate users at bay is now at a level which conceivably cannot be overwhelmed within an attacker’s lifetime. A frontal assault will be turned back every time.

But cyber attackers are not stupid. Some attackers are even among the MIT elite.

The goal of serious outside attackers is to appear like they belong, to hide in plain sight, to go about their nefarious business right alongside those doing legitimate business. If frontal attacks have been effectively negated, then other, more insidious methods will be utilized. Cyber attackers will go after the weakest link in modern security: user credentials. If a user’s credentials can be compromised then attackers appear, even to the strongest standard defenses, to be trusted users.

Outside attackers compromising credentials are not the only threat, though. Insiders can be just as problematic, if not more so. Some insiders are unintentional actors, as in the case of a Watering Hole attack. Through carelessness, negligence, or inattention to security measures such individuals accidentally expose sensitive information. Accessing secured data on a public Wi-Fi is a prime example of an unintentional threat.

All Attackers are Inside Threats

Today there is no essential difference between an outside user utilizing compromised credentials and an inside actor threatening security. Both seize upon sensitive information from inside the system.

Worse, inside threats can come from an emotional attacker who intentionally seeks to harm a company for some supposed infraction committed by the company or its management. A typical attack takes the form of uploaded malware or a "logic bomb" planted by a laid-off employee on the employee's last day of work. The preponderance of such attacks is actually quite high.

An emotional attacker may or may not be tech savvy. Imagine a person who believes their job is in doubt. Maybe they've been written up and it's just a matter of time before they are shown the door. Typically, within that 30 day range prior to their leaving they might steal IP (intellectual property) in any number of ways, technical or otherwise.

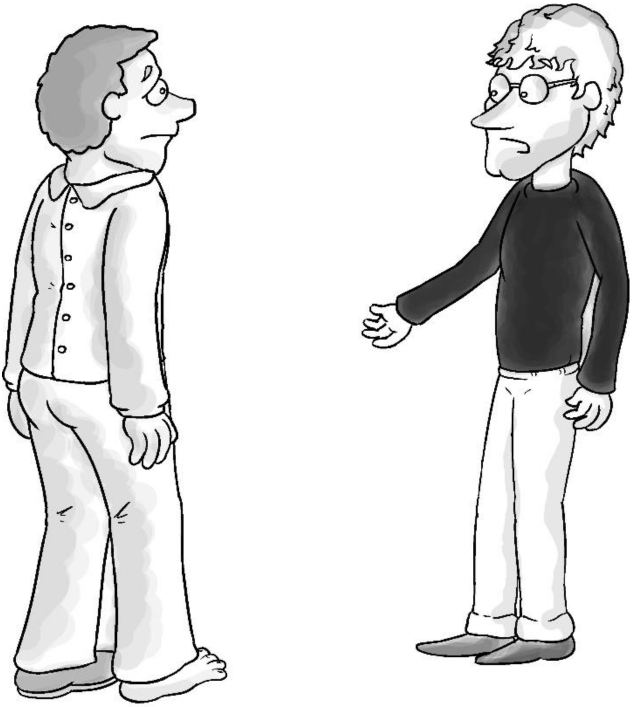
But the most dangerous inside threat is the savvy professional who is capable of using insider knowledge of specific weaknesses and vulnerabilities to bypass securities and gain access to sensitive information. Often the goal is to sell confidential information to the highest bidder. Through their knowledge of existing security measures, the savvy inside actor can proactively react to security challenges and escape detection for an extended period.

Whatever the threat source, getting past the traditional security measures means the attacker is now on the inside. Such actors are accepted by the system as one of the good guys, just as was Dr. Sherr when he made available all the login credentials of MIT's CTSS computer. Back then the worst that happened was a few "taunting messages" given to an unsuspecting individual. Today the potential harm that insider threats pose is exponentially greater. Companies can be collapsed. The life savings of millions can be wiped out in an instant. And, without being the least bit hyperbolic, it is safe to say that global power can be altered overnight.

Whatever the threat source… the attacker is now on the inside. Thus the inevitable evolution of user behavior analytics.

Security challenges have taken a significant step forward. Traditional intrusion countermeasures are falling short. The enemy is no longer at the gate – he is inside the gate. New measures are required to identify and neutralize the new internal threats. Thus the inevitable evolution of user behavior analytics.

Chapter 2: How User Behavior Analytics Addresses Insider Threats



"Hey buddy, are you ok?"

Do you remember the 3 ½ inch floppy disk? An outstanding 250 Mb of reliable data storage safely tucked away in a plastic case and accessed through a really cool, sliding metal panel. When I migrated from the 5 ¼ inch floppies with their 720 kb capacity, I wondered how anyone could ever use up an entire floppy ever again!

My last digital selfie would have blown the sliding access panel off five of those unfillable disks. And yet that selfie is irreverently tossed aside in my cell phone's 16 Gb of available storage.

Back in Sherr's day (predating the "unbelievable advancements" that brought about the 5 ¼ inch floppy) data storage was at a premium. Computer administrators needed to weigh the tradeoff between tighter security measures and the already stretched computing resources. The 1960 era balance was to make passwords nothing more than a string of eight numbers. On a brute force basis, that would have given an outside attacker the daunting challenge of trying more than a billion combinations. But Sherr found an easy way around that "impossibly huge" technical difficulty, didn't he?

Today's brute force methods could blow away the best 1960s-era defenses in less than 36 seconds.

Out on technology's cutting edge, today's storage capacity is having difficulty keeping up with Moore's Law [(2)], yet everyday enterprise-level computing has more than enough storage and redundancies to keep going for quite a while. Unlike the CTSS, we have the capacity to explore new ideas in security without causing a noticeable hiccup in user performance.

Suppose you have a friend you have known for some time. You even like this friend and actually pay attention to what he says, to what he does, and to how he reacts to your lame jokes (I'm sure he tries to laugh). Now suppose this friend just got some really, really bad news – worse than his team losing the Super Bowl. Suppose one of his kids just went into drug treatment. This is obviously not news he wants broadcast on the six o'clock news. He wants to keep this quite. It's embarrassing and distressing. I imagine your friend wouldn't even want to discuss it with you, his good friend.

Don’t you think it would be rather easy for you to notice that your friend is forcing a more enthusiastic response to your lame joke all of the sudden? Don’t you think you’d notice that his interactions with others has become somewhat sharper lately? If you have been paying any level of attention at all, such noticeable changes in outward behavior will elicit a natural response in you of mixed empathy and curiosity – “Hey, friend, I’ve noticed you’ve been a bit ‘off’ lately….”

As a human, you have a natural and phenomenal capacity to take in a complex set of dynamic information, establish multiple baselines for different situations and actors, compare the incoming information to those baselines, and determine an appropriate response when variations from the baseline are beyond a given tolerance point. Whew! That was a mouthful…. But there you have it – you are a highly complex, ever learning, always analyzing, and ready-at-the-response kind of person!

What if we could develop a security system so that computers – those dumb machines that can’t tell friend from foe – could do the same? What if we could teach the machine to pay attention to how each user typically acts, behaves, and communicates so that it could take notice if something – or someone – was not quite right?

We’re a long way from creating artificial intelligence where we make “friends” with machines like we do with people – my phone can store a lot of selfies, do many useful things, but it’s not my friend. I’m not opposed to tossing it out the car window if it acts up again. However, we are at a point where we can realistically engage sophisticated psycholinguistic security algorithms to build a database of what constitutes “normal” user behavior on a given system, and to build a baseline behavior profile for each user.

User Behavior Analytics Provide Early Warnings

Using sophisticated algorithms and statistical analysis, UBA systems can help predict insider attacks, especially from so-called emotional attackers.

By paying attention to the words used, the sentence structure developed, even what is not said, psycholinguists gain dynamic insight the interworking of an individual's private thought life. The formal field of study was developed in the late 50s and early 60s. Only recently, though, has it been applied to cyber security. By analyzing a user's language over time, the new algorithms can measure a user's change in emotion, attitude, and personality. [3] IT security professionals thereby gain a quantifiable, pre-emptive "heads up" that an employee or other user may be at risk for becoming an insider threat.

Psycholinguistic software provides scientific, real-time tracking of users' written communication through the computer system. A dynamic profile is continuously updated on every user. The software then compares the live profile to that individual's baseline and the current communications of the user's peers. But don't worry – Big Brother hasn't implemented a "no-tolerance" policy for email wise-cracking about company senior management (at least not yet). The software is sophisticated enough to differentiate between expected, occasional employee sarcasm, for example, and patterns that may signify a genuine threat is developing.

Psycholinguistics are not just for Eggheads Anymore

Psycholinguistics glimpses at our private thought life through what we say and don't say. The field is well-enough established to allow creation of a sophisticated security applications that can analyze user written communications in real-time.

And, to date, the psycholinguistic security algorithms are not enabled to take “corrective action” against suspected threats. So don’t expect any darker scenes from the movie I Robot to become your reality just yet. However, the software will flag potential threats for further investigation – by humans of course.

Psycholinguistics is but one aspect of the new frontier in cyber security. User Behavioral Analytics (UBA), the class name, gives cyber security a broad range of tools to spot anomalous behavior of credentialed users.

UBA can analyze suspicious geolocation sequences. It is not uncommon in today’s work world for busy users to log into a system from home, different locations at work, airports, hotel rooms, or customer locations. In such an environment, asking IT personnel to consider the legitimacy of every remote login would be overwhelming. But UBA software can do it without batting an eye.

Likewise, most security systems do not pay attention to service accounts. After all, such accounts are typically used only by the system for automated background tasks. But what if the credentials of such an account were compromised? The attacker would then have high-level system access on an essentially unmonitored account. UBA does not care if the account is just a “system” account. It will monitor every account for anomalous activity based on the baseline established for each account.

Here’s a good one – employees sharing passwords or snooping around the system where they have no business being. Merely setting HR policies will not deter such behavior, and since such activity does not move large blocks of data, infringements of this type are very hard to detect. But UBA systems can detect – in real time – simultaneous user logins and unjustified user access in areas unrelated to their job duties.

Looking Where Humans Cannot

UBA can spot anomalous activity that would be too subtle to catch the attention of even the most diligent security professionals. Threats can be neutralized before the damage is done.

The real power of UBA is its real-time detection of threat activity. Suppose someone does get in using compromised credentials. Suppose they know exactly what they’re looking to acquire and they know exactly where it is. In less than a minute the bad guys are at the sensitive information with their FTP moving truck. How long will it take to download a couple thousand customer names and credit card numbers? Certainly the attack will be faster than human response times. Often the first evidence of the data theft will be large volumes of calls from frantic customers regarding identity theft. Only then will the forensic team start to pour over the system logs in an effort to catch the crooks – but the damage to your organization’s reputation is done, not to mention the damage to your customer’s credit ratings.

While UBA is designed to monitor individual users, it can also monitor across the entire organization as a whole. Unusual data movements can alert the system to a potential live attack. The system can halt the data flow almost immediately. The only downside is that your customers will never know that they should thank you.

Stopping attackers in their tracks – awesome! But what if, rather than just detecting an attack as it happens, an attack can be defeated before it happens? What if threats could be more accurately predicted and prevented? It almost sounds like science fiction, but it’s not.

Consider again your well-known friend whose kid was just put into drug rehab. You are able to note the change in his stress level without him ever saying a word about his family issues. And, good friend that you are, you gently press for more information. Your motivation is not morbid curiosity. You are looking to relieve a potential, albeit unspecified, issue before it erupts into something serious. Without even knowing it, you have used behavior analytics proactively to deter potentially regrettable future behavior in your friend.

The continuing rise in attacker sophistication is quickly making traditional cyber security measures obsolete. User Behavior Analytics has become the new line of defense.

User behavior is like a retinal scan – it cannot be faked. Again, when I was a federal agent we used polygraphs to determine if a “perp” was telling the truth or not. Polygraphs work by comparing four observational points to a baseline (heart rate, breathing rate, blood pressure, and skin conductivity). It’s tough to beat an experienced “lie-detector” analyst.

That’s why they’re useful. But UBA looks at an extensive set of points of user behavior and compares each observation point to specific baselines. Even if a set of credentials were not compromised, subtle changes in the trends of these observation points will occur before the malicious activity takes place.

Chapter 3: How UBA Interacts with Existing IT Activities

“Well,” you may be saying, “all this UBA stuff is good and fine, but we already employ the best SIEM system available. Why do we need UBA?”

Answer: Think Edward Snowden vs the NSA.

A security information and event management system (SIEM) is a great piece of cyber security that is here to stay. It can process through all kinds of security-related information quickly and efficiently to produce security alerts related to authentication events, malware threats, intrusions, or any other event flagged by a system's various intrusion detection systems. Snowden, however, effortlessly pushed aside all the NSA's toughest SIEM defenses and perpetrated the costliest information leak in US history.

Edward Snowden

In 2013 a young man who worked for an NSA contractor became the greatest security liability in US history.

In 2013 Edward Snowden was an employee of Booz Allen Hamilton doing contract work for the NSA from Honolulu. [4] Snowden accessed the NSA mainframe 5,000 miles away via a "thin client" computer. In a "thin client" setup a personal computer emulates a mainframe terminal. Typical NSA employees and contractors have "top secret" clearance specific to their job and projects. Using their legitimate login credentials each person can only access information relative to specific projects and the user's pay grade. Snowden, however, found himself in possession of system administrator credentials. Logging in as a system administrator, he could access any document, on any project, and even fool the system into thinking that he was a different user – all without leaving a single trace for the standard SIEM defenses.

Perimeter Defenses have a Common Weakness

The NSA undoubtedly has one of the best perimeter cyber defenses in the world. Target had a lesser security system. Both were breached from the inside where the perimeter defenses are at their weakest.

One night after normal hours, Snowden simply walked up to a thin client, logged in, and downloaded a boat load of ultra-sensitive documents onto a couple of thumb drives. Amazing. And what did we learn from the whole Snowden espionage fiasco? Besides the fact that even the NSA can get caught with its britches down, it is clear that even the world's best security, if it focuses on outside intrusion, is useless against insider threats.

Avivah Litan is a vice president and distinguished analyst at Gartner, a research and advisory firm specializing in cyber security. At a recent cyber security summit, Litan highlighted how behavioral analytics could have prevented Snowden's breach.

Snowden may or may not have been flagged for abnormal access stemming from the actual times he logged into networks. However, there was definitely a good deal of abnormal file transfer activity when he downloaded 1.7 million files to USB sticks in Hawaii. He probably should and would have been flagged for achieving super root level access at NSA headquarters in Maryland. Abnormal account usage across some 25 peer accounts all linked to Snowden's IP address would have almost certainly triggered alarms had the proper ones been implemented. (5)

SIEMs are only as good as the information fed into them. And the majority of that information is perimeter defense centric (leading some to think of SIEMs as a perimeter defense). Once a user is in the system, such defenses are essentially nullified if inside defense centric things like UBA are not being aggregated into your SIEM. UBA detects anomalies inside the perimeter. Analysis is focused on user-specific activities. It can detect if a user is, for example, downloading 1.7 million documents onto a thumb drive and alert security if such behavior is deemed unusual – even if the behavior is performed by a "super administrative" user.

Printing, Downloading, Emailing, or on the Cloud…

UBA is a set of mathematical tools that looks at the user, not the system upon which the user is working. Whether a user is printing in the local office, downloading to a personal device, emailing across the country, or working on the Cloud, UBA can spot the insider threat in milliseconds, before the damage is done.

The NSA has – or perhaps I should say had – one of the most secure intranets in the world, the so-called NSAnet. It resisted all (known) outside intrusion. And information stored on their intranet could not be easily removed – printing and data downloads to portable devices was prohibited by “air gap” technology. But Sherr in 1962 and Snowden in 2013 clearly demonstrated that with higher security privilege comes heightened security risk potential. The NSAnet air gap prevented normal users from downloading information – Snowden came in with super administrator privileges. The system freely allowed him to do what others could not. Had the NSA employed UBA technology, Snowden’s unusual activities would have been flagged and stopped; and US state secrets would have remained secure.

Now that’s all good and fine for relatively closed systems like intranets and enterprise systems. But what about working on the cloud?

BYOD (bring your own device) computing and Cloud storage are cyber evolutions that are becoming increasingly more important as processing advancements, following Moore’s Law, [2] are making corporate data centers an ineffectual and costly bottleneck. By utilizing a more virtualized and federated SaaS Cloud model, companies gain tremendous cost efficiencies and the freedom to focus on what they do rather than on how to store more data.

Yet even on the Cloud, UBA is effective in handling insider threats. It is possible, for example, to simultaneously analyze transactions at company location 3 with applications and servers at locations 4 – 7. The same analytics that work behind the scenes on the enterprise system and closed intranets can be chained to learn “normal” behaviors across a full IT stack. Once a baseline is established the UBA system can find in real-time, suspicious activity across all linked users, their devices, and all associated resources.

Going forward cyber security professionals will need to employ both traditional perimeter defenses and UBA systems.

Traditional security focuses on system performance, and they will continue to be needed to protect computer systems from outside intrusions. But UBA focuses on internal user behavior. It does not make any difference if that behavior is internal office activity like printing and emailing, psycholinguistic UBA will spot the disgruntled or distressed employee before things get out of hand. It does not matter if the user is working with personal storage devices or on the Cloud, it is the behavior that is analyzed, not the system upon which the user is working. Once the user is inside the perimeter defenses, those defenses are useless to prevent malicious activity. The day has come when cyber security must take insider threats seriously.

Note to CIO's: You do not need UBA if you are certain no internal threats exist within your system. Ahem… are you?

The Big Takeaways

Since the first days of shared computing insider threats have been an unanswered security risk. As defenses against external attack have become increasingly fortified, those intent on malfeasance have turned to ever more insidious methods to gain access to sensitive and valuable data.

User Behavior Analytics is changing the face of cyber security by closing the greatest vulnerability of traditional security systems – what do you do with someone who is in the system with legitimate credentials.

By comparing the real-time activity of each individual user to an established baseline of what is normal for that user, UBA is able flag suspicious activity long before trouble manifests and stop attackers in their tracks.

Resources

1. McMillan, Robert. The World’s First Computer Password? It Was Useless Too. Wired Magazine: Boone, IA. January 12, 2012.

2. Moore’s Law or How Overall Processing Power for Computers will Double every two Years. Mooreslaw.org. 2016.

3. Sims, Bill. Exploring The Role Psycholinguistics Plays In Identifying At Risk-Insiders Within Your Company. Managing Director, Head of Investigations & Business Intelligence Asia Pacific: Stroz Friedberg. November 24, 2015.

4. Esposito, Richard, et al. How Snowden did it. NBC News: Washington, DC. August 26, 2013.

5. Donohue, Brian. Avoiding Data Breaches with Context Aware Behavioral Analytics. Threat Post: Woburn, MA. December 3, 2014.

As insider threats become more sophisticated, organizations must employ security capabilities that can quickly assess, identify and analyze user behavior.

User Behavior Analytics (UBA) helps enterprises detect insider threats, targeted attacks and financial fraud. UBA gives responsible folk visibility into user behavior, allowing them to devise efficient ways to detect malicious or negligent users, and to fix the problem. The goal of this book is to help those involved in protecting data to understand UBA enough to converse about it

About Derek A. Smith

With over 30 years in the security industry, Derek A. Smith is a former government agent, cybersecurity SME, holds a variety of certifications (CISSP, CEH, C/CISO, Security+, etc.), eight college degrees, is a published author, conference speaker, cybersecurity analyst for several international and local television news stations, government program manager, and more. Follow him on Twitter @DerekASmith1

ConversationalGeek™

Visit conversationalgeek.com for more books on topics geeks love.