Veriato

How UEBA / UAM

Supports Monitoring High Risk Positions

By Derek A. Smith (CISSP)

www.veriato.com

Insiders – a company's employees, vendors, and contractors – may pose a greater threat to cyber security than all outside malicious actors combined. The reason, of course, is quite simple: Insiders already have system authentication and access to any number of the company's critical cyber assets. Outside actors, on the other hand, must penetrate the outer defensive technologies, map out the internal system architecture, and find a way to gain the necessary authentication level before they can access the targeted assets.

The Risks with Some Positions

Some positions within the company require elevated access to the system or certain digital assets. Payroll personnel, for example, necessarily need access to employee social security numbers, home addresses, wage information, and so forth. Information of this nature could easily be monetized.

Consider also the web content author whose regular job duties include uploading materials to the website intended for access only by certain individuals or intended to be accessed by the general public only after a specified date. Early release of this material, or release to unintended parties, could produce devastating financial or reputational damage to the company.

WHAT ASSETS ARE AT RISK?

What defines a "high-risk" position from the perspective of a company's cyber security depends greatly on the nature of the company's cyber assets. Cyber assets include more than digitized information. They may also include the capabilities of the IT system. For example, manufacturing or power companies may have any number of industrial control systems (ICS) monitoring critical systems, or which adjust complex processes based on inventory, demand, costs, or other parameters.

Cyber assets may be the company's digitized information – such as customer names or the company's strategic 10-year plan. They may be certain computer-controlled capabilities – such as controlling the temperature of a steel smelting process or balancing the load across the electrical power grid. The critical consideration for cyber security is who has access to these assets.

WHO HAS ACCESS?

Who are the individuals in your company in high-risk positions? The answer might surprise you.

You might first consider the company CEO and CFO as individuals cyber security professionals may consider to be in high-risk positions. Certainly, managing company officers need access to any number of high-value digital assets to perform their role.

However, the individuals that cyber security professionals consider to have high-risk positions are those who have privileged IT system access. These may be the system administrator, employees within the HR or payroll departments, or even one of the web content authors.

Sometimes companies provide privileged authentication credentials to vendors or consultants. Even former employees have been known to maintain privileged access after ceasing employment.

In addition to the heightened risk of data leakage, a recent national survey on the security risks posed by privileged users revealed that:

- **74% of individuals** whose work positions require that they have privileged access believe that they are "empowered" by their company to review anything they can access on the company system – even if the material has no bearing on their job duties

- **66% of users** with privileged access look at confidential or private information only to satisfy their curiosity

- **58% of companies** assign user privileges in excess of what is required to perform the employee's job duties

Furthermore, individuals in high-risk positions are frequently the target of malicious actors:

- **48% of external phishing scams** are specifically targeted toward individuals in high-risk positions who have privileged system access

- **46% of all malicious insider attacks** target known individuals in high-risk positions to obtain their privileged access credentials clandestinely

Why Trust is not Enough

Typically "insider threats" are defined as individuals with malicious intent: the employee who was passed over for a promotion, the developer who insists that code she was paid to develop belongs to her, the contractor who installs malware on the POS system, and so forth. However, there is another group of potential insider threats. These individuals may not have malicious intent and may be quite loyal to the company, its strategy, and its future success. They are in a position of trust within the enterprise.

From a cyber security perspective, however, the unfettered access these individuals have to some or all of the company's sensitive cyber assets is cause for concern. Consequently, these individuals are in what may be defined as "high-risk" positions. Not that the company has a reason to be concerned about the intent, motives, or loyalty of these individuals under normal circumstances. However, it is possible that the access these people have to high-value and critical assets may be used in ways other than for the intended company purposes.

Trusted insiders may use their access to satisfy their curiosity. Imposters may steal their authentication credentials. It may even be possible that these people may be placed under excessive duress – such as from a credible threat of physical harm against family members. Even if individuals in high-risk positions remained loyal and dedicated to the company, attackers could leverage their privileged access such that the company could be made to suffer irreparable harm.

Furthermore, malicious intent is not the root of insider threats. Consider, companies necessarily need some individuals with elevated system access to perform certain roles. The individuals in these high-risk positions are necessarily entrusted with access to valuable cyber assets – and most of these individuals perform their regular duties with loyalty and dedication to the company. Surprisingly, though, 68% of insider incidences are caused by these same people through simple negligence. Intent is not the root of insider threats – authenticated access to assets is.

Veriato Helps Companies Monitor High-Risk Positions

Most companies address the potential risk inherent in high-risk positions through deploying data loss prevention technologies. While these technologies have an established track record, they only provide, at most, a 10% return on investment.[iii]

Another preferred mitigation strategy, mandatory employee training, has a higher return on investment – primarily due to its lower deployment cost. However, survey results demonstrate that training only lowers the average annual cost of insider incidents by 7%.

A far better approach to mitigating the risks inherent in high-risk positions is to actively monitor the behavior and activity of individuals in these posts with Veriato's user and entity behavior analytics and user activity monitoring. UEBA / UAM provides early indications of potentially harmful situations. Companies utilizing the power of UEBA realize a 26% decline in the cost of insider threats.

Furthermore, it is well established that cyber attackers work hard to acquire the authentication credentials of individuals in high-risk positions to carry out their illicit activities. It is nearly impossible for traditional security and defensive tools to detect the movement of attackers using stolen authentication credentials. Veriato's UEBA algorithms, however, can alert companies when activities associated with an individual's system credentials fall outside of the usual or expected activities for that individual or a person in a particular position.

WHAT CAN COMPANIES DO?

The average company's annual cost from insider threats is $4.3M, though there have been cases of damages far in excess of this (i.e. the 2013 Target data breach). Most cyber security resources are focused on preventing the external actor from accessing the company system. However, employees and other insiders in high-risk positions already have the authentication credentials and access to high-value company assets.

The primary preventative response of most companies is to deploy data loss prevention tools and require mandatory employee cyber security training. Data loss tools have an average ROI of less than 10%; employee training only reduces the average annual cost of insider threats by 7%.

Other typical efforts to prevent insider threats include 3rd party vetting, threat analysis, and network traffic intelligence.

Why Choose Veriato

From a cyber security perspective, the critical issue is not the intent of the actor, but the individual's access to valuable and critical cyber assets. Detecting and stopping the malicious or negligent actor without hampering the necessary and legitimate activities of others in high-risk positions is one of the tremendous benefits of utilizing UEBA and UAM together. That is why Veriato Recon and Veriato 360 were developed to work together seamlessly.

Veriato Recon monitors all users' psycholinguists for anomalies – indications that a user may be under duress, developing a rogue mindset, or may be an imposter. Psycholinguistic variations, including shifts in tone, intensity, or even word choices, may be subtle but provide powerful insight to changes in a person's thinking. Furthermore, although the language "tells" may be subtle, they are impossible to hide from Veriato Recon's advanced algorithms and tireless monitoring.

Veriato 360 allows DVR-like playback of activity screenshots, providing actionable intelligence for an immediate incident response.

While companies cannot avoid having individuals in high-risk positions, with Veriato 360 and Veriato Recon, they can mitigate much of the associated risk inherent to these posts.

[i] Steinberg, Joseph. "Insider vs. Outsider Data Security Threats: What's the Greater Risk?" Nena Giandomenico, etal. Digital Guardian. Digital Guardian: Waltham. January 26, 2017. https://digitalguardian.com/blog/insider-outsider-data-security-threats

[ii] "The 2016 Study on the Insecurity of Privileged Users." Ponemon Institute. Ponemon Institute, LLC: Traverse City. August 2016. https://www.forcepoint.com/newsroom/2016/forcepoint-and-ponemon-institute-survey-finds-organizations-challenged-when-monitoring

[iii] "Korolov, Maria. "Average Business Spends $15 Million Battling Cybercrime." CSO Magazine. IDG Communications, Inc: Framingham. October 6, 2015. http://www.csoonline.com/article/2989302/cyber-attacks-espionage/average-business-spends-15-million-battling-cybercrime.html

[iv] "2016 Cost of Insider Threats." Ponemon Institute. Ponemon Institute, LLC: Traverse City. September 2016. https://dtexsystems.com/cost-of-insider-threat/

Veriato
www.veriato.com

Veriato USA
4440 PGA Boulevard , Suite 500
Palm Beach Gardens, FL 33410
+1 888 598 2788
sales@veriato.com

Veriato EMEA
3rd Floor,Crossweys House
28-30 High Street
Guildford, Surrey
GU1 3EL United Kingdom
+44 (0) 1483 662888
sales@veriato.com

https://plus.google.com/+Spectorsoft
https://www.linkedin.com/company/veriato
https://twitter.com/Veriato
https://www.youtube.com/SpectorSoft
https://www.facebook.com/VeriatoInc/