INTERSET

Are Snowden and Manning the True Face of Insider Threats?

A Comprehensive Guide to Understanding and Mitigating Insider Threat Risk

7/14/2014

Are Manning and Snowden the True Face of Insider Threat?

First Manning and then Snowden, two of the most public cases of successful insider attacks in history have brought great attention to the problem of insider threats. But are these headline grabbing cases the true definition of insider threat and do they represent the size and scope of the risks that your organization must understand and mitigate?

Unlike malware attacks, insider threats are not new. Industrial espionage, stolen intellectual property and disgruntled workers leaving with important information have been occurring since the industrial revolution. But like malware attacks, the age of the internet and digital data have made insider threat a much bigger problem than most security professionals realize, arguably a problem even greater than malware attack which seems to constantly grab the headlines.

What is the size of the problem – how big is it?

In the digital age we actually know very little about insider attacks and the threat they pose. Maybe the greatest authority on insider threat is Carnegie Mellon's US CERT team that studies these attacks. Since 2001 they have surveyed companies about insider attacks reviewing over 700 reported incidents. In addition to having learned a lot about how insider attacks occur, they have learned that each year almost 75% of known incidents go unreported[1] and the amount of attacks that occur and go undetected remains an unknown. Some simple math would say that, each year, that 75% represents roughly 800 incidents based on the data collected by the US CERT team, and if we conservatively conclude that another 30% of incidents go undetected, then our problem grows to 1200 incidents per year. When one considers the number of people that leave companies each year and take some amount of sensitive data with them, that 3400 incidents is probably a fraction of the unknown number. As Dan Geer is fond of saying "if someone steals your car, you know it is gone, but if someone steals your data there is often no way to know."[2] This is backed up by the fact that the Verizon Security report consistently finds that third parties alert companies to their data compromises 80% of the time – and that includes insider attacks.

Another approach to measure how big the problem is to consider that your employee population is representative of society itself, and if we look at FBI crime statistics[3] around theft we find that about 1 in every 500 people will steal something each year. You can argue that your employees are screened for illegal behavior, but in the FBI statistics, 88% of the incidents are first time offenders and with digital data, the ease of stealing is greatly increased. That means that if you have a 1000 person company, you are likely to have two cases of data theft from an employee each year – whether you find it or not. The US Census tells us that in 2008 there were over 9,000 firms with 1000 or more employees across the United States – so a number even greater than our 3400 is likely.[4]

The other important insider threat attack statistic is the cost of data loss per incident. Working in tandem with the FBI and Secret Service, the US Cert found the average loss was almost $400,000 per incident. When we combine incidents occurring each year with the average loss number the result is that insider threat attacks are costing companies in North America more than one billion dollars per year. That number is not surprising when you look at the companies that had data theft incidents by insiders reported including: Dow Chemicals, DuPont, AMD, Ford, GM, LG, and Motorola to name just a few.[5] One final piece of evidence in making the case for a renewed focus on insider threat - according to a 2010 study of trade secret related litigation, trade secret and IP theft doubled from 1988 to 1995, and doubled again from 1995 to 2004. Trade secret and IP theft is projected to double again by 2017 with losses approaching half a trillion dollars annually![6]

---

[1] http://www.cert.org/blogs/insider-threat/post.cfm?EntryID=60
[2] The Economics and Strategies of Data Protection, Dan Geer, V-Press 2010
[3] http://www.fbi.gov/stats-services/crimestats
[4] https://www.census.gov/econ/smallbus.html
[5] http://www.fbi.gov/about-us/investigate/counterintelligence/the-insider-threat
[6] A Statistical Analysis of Trade Secret Litigation in Federal Courts, Gorgonzola L.R. 2010

What is the scope of the problem?

The size of insider threat in terms of actual losses of IP and Trade Secrets is significant and growing, but what is the scope of the insider attack risk – who are the threats and what motivates them?

Manning and Snowden fall into a relatively rare category of "inside hacktivist." Where most hactivists are outsiders looking to shut down or deface a company website. Manning and Snowden stole very sensitive data from the US Government because of their belief that the government has done something wrong and because they want "social justice." Hacktivist of all types are motivated by political, environmental and social issues. With the Internet offering a variety of social justice websites like WikiLeaks, as well as traditional news media outlets, it has become very easy for an employee inside an organization to capture sensitive data and pass it to these sites while remaining anonymous or having their denies protected. These attacks can occur for any number of reasons, such as your organization's support of political parties, environmental damage caused by your company, or views on social issues like healthcare. It only takes one employee with strong personal feelings about any of these things to feel "wronged" and to feel justified in taking action.

Historically, the primary objective of sensitive data theft has been economic gain or espionage. This form of insider attack is not new, but because of technological advances in data storage and movement, the ease of successfully stealing very large amounts of data has dropped, while the impact of this data loss has grown exponentially. State sponsored economic espionage by the Chinese has hit an all-time high. In May of 2013, a report published on the behalf of the Commission on the Theft of American Intellectual Property claimed that China was behind 50 percent of the IP theft cases and was "80 percent of the problem."[7] A second 2013 study by the Center of Strategic and International Studies (CSIS.ORG) defined the reasons why China was so aggressive in their IP theft campaign.[8]

The CSIS report defined four primary reasons for their increase in activity:

- They have an overwhelming desire to catch up with and surpass the West
- They have no tradition of protecting intellectual property
- They have lost the capability to innovate and must depend on stolen technology
- Rapid economic growth is essential for the party to maintain its dominance

This last reason is critical to understand, China must sustain economic growth to support its 1.4 billion people, and if any large portion of the population revolts the semi-authoritarian government will likely fall. Chinese growth rates were running at an amazing 9 and 10%. One way to support those rates are to eliminate the cost of R&D. The US spends and estimated $400 billion annually on R&D – and if China can exploit that cost for their own gain it goes a long way to sustaining large economic growth rates. In Q-1, 2014 the Chinese economic growth rate fell to less than 8%. That is a likely catalyst to see increase espionage activities.

While hactivisim captures headlines and espionage accounts for a majority of the economic loss, it is ignorance, thoughtlessness and greed that account for the majority of the remaining insider attacks. These range from employees who violate corporate policies by moving sensitive data to unprotected locations like personal computers, public cloud storage or share it with contractors or partners who should not have access all the way to employees leaving an organization who take sensitive data with them to hopefully improve their chances of getting and succeeding in another job.

Employees that move data to unsecure locations in order to ease their work process create risk by unwittingly exposing this data to external hackers or bad actors that work within your own company, at supply chain partner companies or within contracted partner companies. These compromises are often the most difficult to discover

[7] http://thediplomat.com/2014/02/china-in-denial-about-addiction-to-ip-theft/
[8] http://csis.org/files/attachments/ts130709_lewis.pdf

and often remain unknown until a new competitor emerges or an existing competitor improves their products and/or processes.

How bad is the problem? A Cisco study found that 44% of employees share work devices with others, 46% of remote workers admitted to transferring work files to home computers and 18% admitted to sharing passwords with this number jumping to 25% in China, India and Italy. The study also established that IT teams found almost 40% of employees attempt to access unauthorized parts of the company's network.[9]

The "leaving" employee taking sensitive data with them is also a very common. Studies consistently find that almost 60% of former employees have taken sensitive company data when they depart an organization regardless of the reason why. One Symantec study found that 56% of workers believe it is okay to take data with them and use it at a competitor. This includes not only customer contact lists but also the IP and trade secrets related to the programs these employees where involved with.[10]

How concerned should you be?

The answer is evident – all companies should be concerned with and work toward implementing an insider threat prevention program. The questions are:

- How much of a target is your organization?
- What priority should you give to mitigating this threat?

If your company has an international presence (especially in Asia), works with contractors who have access to your sensitive data and employs people from multiple nationalities, then you *are* at risk. More importantly, if you have information that could be used by foreign governments or businesses to improve their strategic or competitive position then you are at an even bigger risk of being targeted.

Government espionage has traditionally focused on military, hi-tech and electronics research and design data, but with the need to support internal economies, the focus has widened to include bio-tech and drug, manufacturing and even consumer devices and products. Equally important and targeted are not the products themselves, but the process by which they are made. Commodity products (for example paints and construction materials) that compete on price require advanced manufacturing processes to build in the quantity and quality required while still being cost competitive. These processes are high value targets for government and corporate espionage. Another area of focus has been the oil and gas industry where information about international energy reserves and their potential productivity as well as the technology related to extracting those reserves are being targeted. Cheap energy is critical to driving an economy's growth so expect energy related companies to become even bigger targets in the future.

The final area to consider is your organization's role in the value chain of the industry you are in. Are you a supplier to companies that are targets? What sensitive partner information do you hold in your network? Another famous Dan Geer statement is "you cannot stop a motivated car thief, but you can make your car harder to steal than your neighbors." If you are in the supply chain of a top company with IP and trade secrets, you can be assured that they have invested significantly in security to protect their sensitive data. GE, Siemens, DuPont, BAE, General Dynamics and others spend millions each year protecting their data – the result is that you as a supplier will look a lot like the neighbors car**.**

[9] http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/data-loss-prevention/white_paper_c11-499060.pdf

[10] http://www.symantec.com/about/news/release/article.jsp?prid=20130206_01

What about the types of attacks? What are the most common insider attacks use cases?

"The Spontaneous"

This is the preferred attack method used by employees leaving an organization with sensitive data, as well as by insider hacktivists. (Snowden and Manning fall more into the long-term attack category.) This attack occurs in hours or in just a few days, and is accompanied by significant anomalous activity. A 2013 case is an excellent example of this type of attack. In this incident, AMD filed suit against four former employees, arguing that the group stole thousands of documents before leaving to go work for one of AMD's biggest rivals, Nvidia. The employees staggered their departures and each took data on the way out. The entire series of attacks took place over six months and none were detected. The civil complaint is linked below. In this attack, like many "quick-action" incidents, attackers will access data they have rarely or never accessed, execute events that change or obfuscate that data, and finally move large amounts of removable data to storage devices, personal machines or public cloud storage. These attacks can be detected by security technology and are best thwarted by monitoring users for anomalous behavior and having a strong employee exit process that connects IT and HR.[11]

"The Low and Slow"

Much more common in government or corporate espionage, these attacks have been known to last for years. In one attack against L-3, a senior engineer and his family stole sensitive U.S. Navy data and were undetected for over three years. The espionage was finally discovered by a U.S. intelligence agency and the company was alerted to the problem. To remain undetected, these attacks often move only small amounts of data and most commonly out of the network through removable media or BYOD programs. Existing security technologies are ineffective in detecting these attacks, so unless newer behavioral-based analytics technology is deployed, these attacks need to be mitigated through corporate processes, user-access controls and employee education and awareness.[12]

"The APT (Advanced Persistent Threat) Insider"

Considering the level of sophistication employed by nation state sponsored insider attacks and the growing number of targeted outside attacks by these same nation states, it's logical to conclude that the next big threat combines the strengths of the two. Where targeted outside attacks take months to penetrate an organization's defenses, compromise one or multiple machines and maneuver to the targeted data, this same attack takes minutes for a competent insider. Yet when the insider is captured, it is a public embarrassment to the perpetrating nation state. The scenario is simple: Have the insider introduce the malware behind the defenses and eliminate any associated links to the insider by facilitating control of the malware via a sophisticated, anonymous command and control (C&C) mechanism. With the malware present and obfuscated, the software now controlled by the C&C server is used to quietly and continuously exfiltrate data out of the organization. This approach greatly minimizes risk to the insider and the nation state sponsor by practically erasing the association between the data theft and the entities involved. This may very well be the preferred attack model of the future because of its relative strength against common defensive weaknesses, while also exploiting the prolific presence and capabilities of technically savvy nationalist sympathizers. These attacks will not be common, but they will be strategic and damaging when they occur.

[11] http://www.scribd.com/fullscreen/120535155?access_key=key-1r5r8a9w90qu7qnz9611

[12] http://www.washingtontimes.com/news/2005/nov/4/20051104-111851-2539r/?page=all

How do you build an effective insider threat mitigation program?

Considering the size and scope of the insider threat, it seems daunting to defend against it. In reality, there are many things an organization can do in terms of people, process and technology to mitigate these threats – things that every company that has critical IP and trade secrets should have in place or be in the process of deploying. Remember that when an attack against your sensitive data occurs – whether from the inside, outside or a mix of both – the attacker must complete multiple steps to succeed. You, as the defender, need only intercept and stop one to succeed in blocking the attack. That advantage can be the basis for your defense.

People

Your employees are on the front line in the fight to defend your organization from all types of threats. A large majority will "do the right thing" when trained to know what to look for and how to respond. This includes not only changing their own work behavior to reduce risky activity, but also to be on the lookout for actions and activities that might identify an employee or contractor gone bad.

All employees need awareness training on the damage and consequences of insider threat. The training should be interactive and reinforced throughout the year. Senior management must also be involved in the communications. Considerations should include:

- Develop and implement an enterprise-wide training program that discusses various topics related to insider threat.
- Train all new employees and contractors in security awareness – including insider threat – before giving them access to any computer system.
- Train employees continuously and vary how training is accomplished. Move away from the classroom and employ methods such as newsletters, alert emails, and brown-bag lunch programs.
- Establish an anonymous, confidential mechanism for reporting security incidents.

At a minimum, training should include the common signs of insider attacks based on studies by the US-CERT and SANS Institute, including:

- Threats or bragging about the damage one could do to the company.
- Use of USB sticks or other removable media by employees leaving the company soon.
- Use of company resources to support a side business.
- Discussion about starting a competing business.
- Attempts to gain employee passwords or obtain access to information through trickery, exploitation of a trusted relationship or other social engineering methods.

It should be remembered that in the Snowden case, access too much of the leaked sensitive data started by first collecting co-worker passwords and, in some of the cases, simply by asking. For an in-depth report on how to build effective employee threat awareness programs reference:

- "Common Sense Guide to Mitigating Insider Threat" by US-Cert [13]
- "People, Process, and Technologies Impact on Information Data Loss" by SANS Institute [14]

[13] http://www.sei.cmu.edu/reports/12tr012.pdf

Process

Corporate policies, governance and process-based controls make up the backbone of defenses against data loss at most organizations. Many of the processes focus on education as discussed, but critical processes that are easy to implement and offer a high return on mitigating insider threat can be easily deployed by companies of all sizes.

Process areas that should be in place in your organization:

- Policies concerning account creation, password management and account termination.
- Segregation and least privilege account access policies, especially those focused at IT administrative and high-value knowledge workers. Ensure that IT administrators have and utilize standard accounts for everyday usage.
- Have a standard process for evaluating third-party service providers, including outsourcers, cloud service providers and internal contractors. Conduct a risk assessment of the service provider before you enter into any agreements and make sure you fully understand how the third party conducts security checks for their own employees.
- Establish policies and procedures for addressing insider threats that include input from HR, legal, IT/security, management and internal audit departments.
- Develop and perform annual internal risk assessments that include corporate- and employee-owned mobile devices.
- Define sensitive areas within your organization where access is restricted and devices with cameras are prohibited.
- Create a standard off-boarding process that includes IT/security, business managers and HR.
- Consider contracting an outside consulting firm experienced in providing incident response support and work to develop this expertise in-house over time.

For more detailed information on these and other sound processes to follow reference the US-CERT and SANS links above.

Process Risk Example:

Jim is part of an analyst team working on a sensitive project within his organization. He is granted the necessary rights and access to all information regarding the project so he can complete his work. However, once Jim's portion is completed, he no longer requires the same level of access to the project's files. In fact, Jim should no longer have access to any of the project's materials. Jim's rights should be revoked, but oftentimes they aren't. This lapse in process oversight results in excessive privileges over time and is an all-too-common occurrence. Jim's excessive privileges do not mean he is ever going to capitalize on them, but in the event he does, the extent of the breach could be significant.

Technology

Stopping the insider threat is the most difficult data security challenge to solve from a technical point of view. Historically, IT security defenses were created to harden organizations from the outside in. Identity and access management systems were added to authenticate users and control their access to systems and applications, but they have not delivered the promised unified access controls and do not extend visibility or control to the data usage level.

Today, with the new awareness of malware and insider attacks, many organizations are adopting "assumption of breach" security strategies, which require data-centric risk mitigation approaches as opposed to the traditional "castle and moat." In this model, data not only requires protection from external actors, but internal ones as well. The tricky thing with internal actors is that their roles may change frequently and so should their eligibility to sensitive data based on characteristics they possess.

[14] https://www.sans.org/reading-room/whitepapers/dlp/people-process-technologies-impact-information-data-loss-34032

Data Loss Prevention (DLP)

DLP technology is intended to prevent data leaks, but is traditionally more suited for monitoring network-based communications for compliance with regulatory laws and industry rules like GLBA, PCI and HIPAA. DLP technologies do not have the ability to monitor how users interact with sensitive data prior to and after a policy violation. Instead they focus on inspecting files for pre-specified content. Assuming they are configured properly and able to read the file content, they can identify and, in some cases, prevent the file(s) from leaving the organization.

Intellectual property and trade secrets come in many different forms and change rapidly. Unfortunately the security teams are typically the last ones informed of new or changing projects related to IP, despite the fact that they are the ones responsible for configuring DLP content inspection policy. Without advanced knowledge of content, DLP solutions are blind. Conversely if DLP is configured with loose content inspection policies in an attempt to increase visibility into potential data loss events, the result is excessive false positives. Legitimate communication may be blocked, resulting in an impediment to business and making it an inadequate solution for detecting and mitigating risk posed by a persistent insider threat. For these reasons, this once-vaunted technology fails in a majority of production implementations because it's nearly impossible stay ahead of content definition and classification requirements.

Encryption Technology:

Companies have also deployed a variety of point technologies to encrypt hard drives, email, data or removable media. However, these systems decrypt the data if a user has authorized access and are useful as access-control solutions, but are ineffective against insiders, especially those in IT administrative roles.

Access Management

Access control systems play an important role in data protection by increasing the effort required to access information to which the user may not have legitimate access. They do not, however, eliminate the threat posed by insider attacks when the insider has proper access to the data or is able to manipulate others into giving them access. It is now known that Edward Snowden was able to manipulate at least three co-workers into giving him their access credentials allowing him even great access to the information he was planning to steal. A recent NSA report stated[15], "The civilian employee (of the NSA) was unaware that Snowden "intended to unlawfully disclose classified information." Nevertheless, by sharing with Snowden his personal "public key infrastructure" certificate -- a system of highly secure credentials that provided greater access to NSA's internal computer system -- the employee "failed to comply with security obligations." If employees fail to follow security policies, tools like access control systems become worthless.

SIEM

Context defines the "who," "what," "where," "when," "how" and sometimes even the "why" of a transactional event. Without this context, one cannot fully understand what has happened or why it is significant. SIEM tools attempt to collect and correlate contextual event data from firsthand witnesses as evidenced by log data from the involved technologies, including databases, network flows, firewalls and intrusion-detection systems. To date, Gartner reports most SIEM deployments have focused more on compliance than on either insider or targeted outside attacks. A major reason for the compliance focus in existing SIEM deployments is the copious amounts of white noise and excessively high numbers of alerts they generate. They are also difficult to deploy and properly tune. Security teams are challenged to find actionable and timely threat intelligence amidst all the noise, and

[15] http://www.nbcnews.com/news/investigations/exclusive-snowden-swiped-password-nsa-coworker-n29006

quickly become overwhelmed by this Achilles Heel. Oftentimes, the tool is relegated to regulatory compliance reporting and post-incident investigation.[16] [17]

Behavioral Analytics and Big Data in Security

Big data has successfully revolutionized the way companies market to consumers, research complex datasets on scales previously thought impossible, analyze and optimize supply chain management and provide complex risk management insights for better decision-making. Behavioral analytics leverage the previously unprecedented strengths big data provides to illuminate patterns and data relationships formed by regular user habits and activities. More importantly, it derives valuable insights by assembling complex mosaics from the individual tiles created from regular human behavior. Such patterns provide valuable insight into the following questions:

- How well are corporate security policies understood?
- How often are they being violated?
- Is that trend increasing or decreasing?
- Who interfaces regularly with our intellectual property?
- What do they do with the data they have access to?
- Are users putting our data at risk and, if yes, who?
- Has any portion of it ever been copied, screen-captured or otherwise exfiltrated from the company?
- If so, to whom was it sent?
- Where was it uploaded?

Behavioral analytics use machine learning techniques and statistical models to establish evolving baselines of user, file and machine behavior. These baselines are accurate depictions of "normal" events and actions by users regularly seen across the enterprise. It then compares historic activity patterns, such as those with current patterns to detect unusual pattern changes. For example, behavioral analytics understand when the user is working and during what hours of the day he or she is most busy. It can also recognize whether the application usage patterns of a user has changed significantly. For example, behavioral analytics can recognize whether someone is using a new application or an existing application at an increasing rate. It can also recognize when a user accesses and downloads data they have never accessed before, increases their data-usage activities, or moves data in a way they have previously never done.

It's not simply that the user's behavior patterns have changed – pattern variations are normal for data, business process and people, which are all dynamic by nature. With the ability to understand and use analytics to weigh the context of all the captured events, behavioral analytics surfaces only noteworthy differences as alerts. The significance of these deviations is akin to a logical decision-making process called Expected Utility Theory. Expected Utility Theory states that the decision-maker chooses between risky or uncertain prospects by comparing their expected utility values, i.e., the weighted sums obtained by adding the utility values of outcomes multiplied by their respective probabilities. When comparing objects for decision-making purposes, we logically rank the perceived value the insider would gain from the item compared to the risk of attaining it. Surprisingly this process can be logically computed.

[16] SIEM Market Trends, Solutions, Assessments and Select Product Profiles, Gartner 4 Jan 2013
[17] http://www.sans.org/reading-room/analysts-program/eventMgt-Feb09

The Interset Approach to Behavioral Analytics

Statistically, human decision-making processes can be observed, measured, and even predicted if tracked according to each person's unique decision-making patterns and risk-tolerance levels. Interset uses sophisticated models to do exactly that. The solution identifies that a pattern of behavior has deviated from its norm, but also quantitatively measures the probability that an observed behavior is risky. For instance, someone accessing a single important file more than they have historically accessed it is interesting, but not as interesting (or potentially as risky) as someone accessing 10 important files that they've never accessed before. Such examples are weighted even higher as they are identified in close proximity with other anomalies involving the same entities, including time of activity, applications involved and storage devices.

User anomalies are detected by:

- Comparing individuals, files and machines against their historic behavior.
- Determining like user patterns across the enterprise and comparing behavioral patterns between the two.
- Detecting dissimilar patterns between members of the same group or job role.
- Comparing individuals against the entire organization.

Not only are these anomalies leading indicators of insider threat activity, but they require no foreknowledge or configuration to detect. Using a weighted anomaly approach in combination with machine learning effectively minimizes and, over time, reduces the noise and false positives that plague other solutions relying on predefined patterns.

Interset utilizes big data architecture to capture much larger, richer datasets used in the machine learning process. The platform enables consumption of seemingly unrelated disparate datasets to discover correlated patterns that result in consistent outcomes. Enriching such datasets with information from enterprise applications, other security technologies, demographic data, threat feeds, social media reputation technologies and more provides additional insight into human behavior, motivations and insider threat precursors.

By analyzing three types of attacks – spontaneous, low and slow and APT – we find that Interset's behavioral analytics offers valuable insight:

- Spontaneous – The comparison of the user against their historic activities will easily surface the attack.
- Low and slow – Despite the fact that the user may intentionally attempt to prevent detection, analytics are used to compare the user to his or her peers to detect and surface indicators well before an attack.
- Insider APT – In cases where machines are compromised with stealth software that is attempting to siphon sensitive information externally, Interset is able to interpret normal user and machine behavior. It is then able to identify altered machine behavior apart from user interaction and alert on these anomalies in real-time.

The net result is an easy-to-use, highly accurate solution that requires little to no configuration. Its use lowers the number of required full-time employees to interpret findings and security analyst workload, while providing visibility where none existed previously.

Interset Insider Threat Detection

The Interset platform includes monitoring sensors, an advanced behavioral analytics engine and complete forensic capability to offer a unique and highly effective solution for insider threat detection. Interset starts with specialized connectors to enterprise applications like Perforce and SharePoint, as well as endpoint collectors – small sensors that can be deployed across your organization on desktops, laptops, workstations and servers. Once deployed, thousands of interactions are recorded every day, ranging from which applications are opened, what projects are accessed to what users have taken screenshots or attempted to print a sensitive document. Interset

Connectors and endpoint sensors are lightweight, stealth, non-intrusive, and unimpactful to machine performance. Endpoint sensors are designed for passive collection and run on Windows and Mac operating systems. Interset Connectors seamlessly pull log data from enterprise applications including source code management and product lifecycle systems to enterprise content management platforms. The collected events are aggregated as metadata in the Interset data warehouse. The warehouse optimizes the metadata for analysis and forensic investigation.

Interset Behavioral Analytics Engine

The Interset Behavioral Analytics Engine observes activities across an organization to gain understanding of and the relationships between users, data assets and machines. The Analytics Engine maintains an irrevocable relationship between these entities. As Interset observes activities and builds relationships, the Analytics Engine continuously creates and refines metrics that drive the baselines. Using these baselines, it discerns which activities or behaviors are anomalous. Through statistical analysis, it quantifies just how risky an observed behavior is. As usage and anomaly patterns are refined, the Analytics Engine learns which users pose greater risk, which files are the most at-risk, and which endpoints are most often part of risky activities.

Unlike any other solution, Interset actively maintains risk scores and models for all entities. The more an entity is involved in high-risk anomalous activities or rule violations, the more it increases the risk score of the entities involved. Conversely, an entity that is not involved in high-risk activities or rule violations will have its risk score decrease over time. Anomaly alerts and rule violations are presented in a prioritized list ranked by highest risk score. The scoring algorithm is a unique, patented approach that makes it easy to operationalize the solution in production by focusing limited security resources on the most impactful findings. Anomalies and rule violations are easily identifiable in natural language alerts and dynamically generated risk scores This shrinks the haystack and increases the needle size to make finding actionable threat intelligence a far simpler process. Interset's new approach vastly improves an organization's ability to quickly determine the root cause of a threat and respond proactively before critical data is compromised.

Interset Proactive Forensics

Leveraging end-user behavioral analytics is also the key to lowering the cost of the forensic investigations. By capturing the relationships between identities, activities, assets (files and machines) and the movement of the data, an investigation can quickly and accurately identify the information that defines the risk or threat down to the user, application or file in question. Since all activity is captured as metadata, a complete historical record of the events related to the threat or incident and all relationships is immediately available. The interface enables you to pinpoint and reconstruct the relevant activities that led up to the event, compressing the time it takes to determine the root cause and extent of a breach. Interset forensics dramatically lower the cost to investigate an incident and enable fast pursuit of legal action and/or adjustments to policies or security tools to prevent or reduce the risk of a future breach.

Manning and Snowden are not the true case of insider threat – the problem is much greater

The fact is Manning and Snowden are not the true face of insider attacks, but their activities have created a much greater awareness of the problem and helped reduce the "it will not happen to me" mentality of many organizations. The true face of insider threat is much more complex and much more costly than the work of these two insider hacktivists. Equally as important, it must be understood that existing security technologies alone cannot effectively mitigate the risk posed by insider threats. DLP, access control, encryption and SIEM technologies are not even slowing down this billion-dollar problem.

To effectively detect and mitigate the insider threat, companies must look to new technologies that bring to bear real-time monitoring and intelligence through behavioral analytics. They must also remember to connect these new technologies with employee training and improved insider threat detection policies. All must take into account the changing technology landscape of cloud services and BYOD.

Interset's approach offers significant advantages, including:

- Reducing noise and false positives so security teams can focus on material risks and actual threats.
- Reducing the time required to forensically investigate unusual activities.
- Expanding protection to include all types of IP and trade secrets, including files created by specialized applications without requiring foreknowledge or configuration of these file types or pre-defined content.
- Expanding protection to machines, whether they are on or off the corporate network.
- Accurately detecting inside and outside attacks during their early stages, enabling the attack to be stopped before sensitive data is compromised.

These values reduce the overall cost and complexity of a threat detection and data protection program while increasing a security team's ability to reduce risk and surface actual threats to the organization. Interset enables security teams of all sizes to be more effective at protecting their IP and trade secrets.

About Interset

Interset provides efficient and effective enterprise threat detection through broad event collection, advanced behavioral analytics and accurate anomaly detection, enabling companies of all sizes to eliminate the noise and false positives of existing security tools and to focus limited security resources on true threats and risks. Interset offers a truly unique solution to secure intellectual property, trade secrets, classified data, PII and PHI from accidental or intentional data compromise by insider and outside threats

www.Interset.com

16 Fitzgerald Road, Suite 150
Ottawa, ON K2H 8R6
Canada
Phone: (613) 226-9445
Fax: (613) 226-5299

INTERSET
THE SCIENCE OF THREAT DETECTION