Whitepaper

Raytheon

Best Practices for Mitigating and Investigating Insider Threats

Only by viewing and analyzing behaviors in context can organizations mitigate the full range of risks posed by trusted users

insiderthreat@raytheon.com | www.raytheon.com keyword: insider threat | 801.733.1100

Table of Contents

The Introduction: A New Approach to Insider Threat Incident Investigations

Insiders with intimate knowledge of an enterprise's business practices, systems and applications are increasingly presenting the greatest security risk and potential to do harm.

This document will outline a new approach to long-term insider incident investigations. The actions taken by the perpetrator of malicious fraud, theft or sabotage are usually complex, fully utilizing technologies and insider knowledge to obfuscate their behaviors and circumvent existing security infrastructure. While this is typically a very small number of insiders, the challenge most enterprises face is that they don't have detection tools, policy enforcement mechanisms or incident visualization technologies that allow them to detect, monitor and act on serious violations.

The reality is that technologies are readily available now that allow an enterprise to get visibility into previously unmonitored incident vectors (such as USB storage, offline activities or encrypted data) and use visualization tools to replay incidents like a DVR — all while respecting employee privacy guidelines.

Fundamental to best practices for the investigation and remediation of an insider threat is the role that a strong foundation of enterprise monitoring provides.

Vigilant monitoring across the enterprise for leading indicators of threats — whether on the network or individual desktops — greatly streamlines the investigations process by parsing out non-serious violations, easily identifying false-positives and documenting timelines of minor incidents or even trigger events that assist in an eventual investigation.

The first five steps outlined in this document involve laying the foundation necessary to monitor and mitigate risk. The five steps assume that an incident has occurred and walks you through essential investigative strategies for appropriate remediation.

Laying the Foundation with Enterprise Monitoring

Best Practice 1: Identify Assets at Risk

Identify and discover all content inside your network that represents risk. Effective insider threat management requires an organization to locate and classify its assets and to remain continuously watchful of insider behavior and associated risks.

Key members of your organization should meet to prioritize critical areas of concern. You could use a simple scoring system such as 1 to 10, or low, medium and high to assist in your prioritization. Your focus, of course, should center on those assets that receive the highest priority or those that would be most costly to your organization if jeopardized.

This content should include all data and files containing personal or customer information and intellectual property or other sensitive data. Each organization may define these assets and incidents differently as they'll vary depending on the industry or focal point of your organization.

Example Assets at Risk by Vertical Market

- Banking and credit companies: Identity theft, account skimming, funds diversion
- Financial firms: Mergers and acquisition plans, non-public financial information, private research
- Retail organizations: Pricing information, personal information on credit card holders, CCVs on cards.
- Public companies: Earnings information not yet distributed to the market, new product information before release, intellectual property.
- The government: National secrets, classified and personal information.

Once identified and prioritized, this content should be fingerprinted and inventoried to ensure that it is not sent out via e-mail, instant messaging (IM) or copied to USB or other mobile storage devices. Security risks are not circumvented through simple data-leak prevention, as they are fair detectors of mostly one vector of communications: outbound data streams, mostly e-mail. Look for more sophisticated solutions that monitor and detect the types of actions a user determined to cause harm would perform. Best Practice 2 will go into more detail on this.

Best Practice 2: Think Through and Anticipate "Typical" Investigations

Now that you've identified your assets at risk, you can overlay the types of incidents you anticipate having to deal with based on the nature of your assets. Thinking through and articulating potential incidents will help greatly in terms of creating effective policies, weeding out false-positives, collecting data

for timeline reconstruction, monitoring for correlated events, and determining what triggers and alerts should be built into investigation policies.

Typical Customer Data-Loss Investigations

- Deliberate theft of customer lists for profit by employees with access to customer data (ID theft)
- Malicious leak of customer data by a vengeful insider
- Lost or stolen laptops with customer data

Customer data losses are sometimes accidental (e.g., losing a laptop containing tens or even hundreds of thousands of customers records), but the data loss that enterprises need to monitor most closely are the deliberate acts, such as theft of personal data for resale (ID theft). A laptop loss can happen to anyone, from a junior salesperson to the CEO, but there's no malice involved. For example, some deliberate customer data thefts involve contractors or outsourced services such as call centers — users who have little management oversight and little allegiance to the company. You'll want to monitor and log even remotely suspicious actions around customer data (for timeline reconstruction), and alert and record more serious actions such as cut and paste from databases and unauthorized downloads to USB drives.

Typical Intellectual Property (IP) Investigations

- Deliberate theft of IP for financial gain
- Malicious leaks of IP for revenge
- Unintentional leak follow-up

While also open to accidental disclosure, intellectual property such as CAD files, product plans, proprietary formulas, etc., are typically targeted for deliberate theft in a manner that either harms the company for reasons of revenge (deliberate press leaks, anonymous sending to competitors, etc.) or to further the perpetrators' own direct objectives (taking IP to a competitor for a new job). Policies that monitor anomalous off- hours activity (hundreds of pages printed at 3 a.m.), unusual mobile storage use (gigabyte transfers daily), or suspicious activities with applications (taking a screenshot of a custom CAD design window) are helpful with investigations.

As with customer data, it's helpful to "log only" a wide variety of leading indicator actions — such as unauthorized IM sessions—that can be mined to reconstruct an activity timeline for investigations.

Typical Fraud Investigations

- Records, files, other data manipulation
- Fraudulent account access
- Collusion, coercion

At a bank, brokerage or business, any tampering of financial records or data is an act of fraud. Each organization must be alerted to any signs of modifications of invoices, financial statements or other records. Under the requirements of the Sarbanes-Oxley Act, executives must certify a company's financial results and report on the effectiveness of internal controls over financial reporting. Many national and internal banks wire-transfer billions of dollars daily; enterprises need policies to detect suspicious behaviors. Effective measures include reporting on all user activities that might be leading indicators of potential fraud and placing alerts on anything that indicates unscrupulous behavior, such as:

- Users deliberately disconnecting their computer from the network
- Inappropriate or unusual use of encryption
- Off-hours access to sensitive databases

Those committing fraud will undertake great pains to hide their tracks or disguise what they're doing as legitimate activity. These investigations require sophisticated tools that cover all endpoint activities, not just simple e-mails or USB copies. The detailed collection of all activity and data provides not only powerful evidence and grounds for prosecution, but also the insight to deploy policies to proactively monitor for similar behavior across the enterprise.

Abuse by Privileged Users Investigations

- False account creation and abuse
- Backdoors, logic bombs
- Corporate or infrastructure sabotage

Users with advanced access rights, such as network and database administrators, could leverage their privileged access to systems, putting customer data, intellectual property and infrastructure integrity at risk. Since these employees pose a greater threat potential, they deserve more focused observation because their access and technical sophistication is greater, the investigation can be much more challenging. To make investigations truly effective, enterprises must create very specific policies for administrators that monitor activity within applications, such as logons, user account creation and log file alterations. In addition, they need to document and

replay investigations for acts of clear malice, such as deliberate data theft, creating backdoor access or planting harmful code.

The ability to go back and "mine" event logs is of particular importance in investigating sophisticated users (such as system administrators or database administrators) so that: 1) seemingly innocuous events might be correlated to demonstrate harmful behavior or 2) gather additional evidence of subversive or even unproductive activity to justify further investigation or resolution.

Compliance Investigations/Demonstrations

- PII/PHI compliance/violations
- Corporate governance adherence
- General compliance audits

Compliance investigations can be much different than the other examples cited here. Rather than investigating incidents of known violations, enterprises might be simply looking for evidence of "non-violations," or proving adherence to policy, or even logging and recording "best practices" for compliance with specific regulations.

Hospitals, financial institutions, and retailers are all highly regulated due to the high volumes of confidential data each organization manages. For example, a regional-healthcare provider must ensure the protection of patients' Personal Health Information (PHI), as required by the federal Health Insurance Portability and Accountability Act (HIPAA). Banks and financial institutions must protect customers' confidential Personally Identifiable Information (PII). Internally, enterprises need to monitor adherence to corporate governance issues (i.e., employee handbook issues like harassment) that might also put the company at legal risk.

Compliance investigations can more closely resemble classic data or IP theft incidents, or even be a result of a customer-data loss. Either way, having detailed incident logs as well as detailed replay of serious violations will make investigations easier and faster.

Best Practice 3: Profile of Those Most Likely To Put Assets at Risk

There is no question that the majority of your employees are trustworthy, but it's vital to understand and focus your efforts on the much smaller number of users who would deliberately harm your company. Some examples:

- Employees who have resigned or about to resign
- Contractors, outsourced call or service center employees
- Former employees given access for any reason
- Technically sophisticated users
- Employees with privileged access, such as system administrators

Theft of Confidential or Proprietary Information

Cases involving theft of confidential or proprietary information include cases in which current or former employees or contractors intentionally exceed or misuse an authorized level of access to networks, systems or data, with the intention of stealing confidential or proprietary information from the organization.
A recent Carnegie Mellon study found the following about insiders:

Who were the insiders?

Eighty percent of the insiders who stole confidential or proprietary information were male and over half held technical positions. Twenty-five percent were former employees; the other 75% were current employees when they committed their illicit activity. Interestingly, 45% of the insiders who were current employees at the time of their theft had already accepted positions with another company.

Why did they do it?

Some insiders were financially motivated, for example, stealing information to commit credit card fraud or selling information to their company's competitors. Others were about to start new jobs or form their own companies, and felt entitled to the information. Still others were disgruntled and chose to embarrass their employers by revealing private, sensitive or confidential information.

How did they do it?

More than 75% of the insiders had authorized access when they committed their theft. Only one had system administrator access. One former employee was given authorized access to do some additional work; he used that access to commit his theft. The rest of the authorized users were fairly evenly split between privileged and unprivileged users. More than 75% of the insiders used their own usernames and passwords to commit thefts. Thirty-two percent used someone else's account, 14% used a shared account, and two insiders used a company computer account.

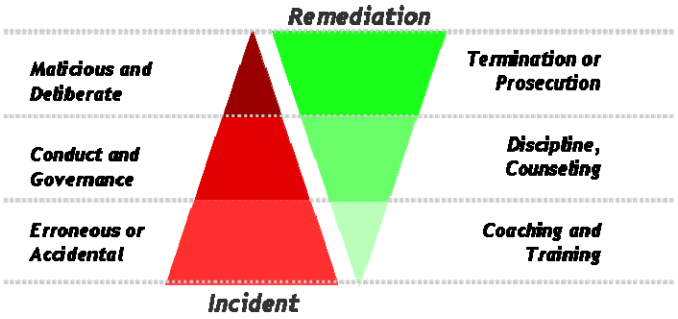
An important factor in dealing with insider threats is understanding the profiles (job, status with company, etc.) of typical violators, as well as their motivations. In a recent Carnegie Mellon study[1] on insider threats, the authors provided great insights into the three most common incidents and the perpetrators.
Clearly, having an idea of user and behavioral profiles makes investigations easier. In the case outlined in the Carnegie Mellon study above, an enterprise could have built strong general monitoring policies around its core intellectual property, while deploying more stringent policies around those with constant access to core IP. Additionally the enterprise can work more closely with its Human Resources department to identify at-risk employees and deploy even more focused policies to those users that specifically look for anomalous activities, such as high-volume printer output after hours, or large file copies to USB drives, or other leading indicators of taking IP out the door to their new job.

Best Practice 4: Lay an Enterprise Monitoring Foundation for Investigations

Given the complexity and sheer number of use cases for how insiders work with IT resources, every organization needs to have a capability in its insider risk management solution to define, monitor and enforce these policies for access, user actions, data movement and data handling to "trust, but verify" that insiders are not putting the organization at risk. In addition, the solution must have a way to investigate the context of attempted or actualized policy violations to determine whether the act was malicious, so that the organization can appropriately manage the underlying problem.

Next, you need to be able to analyze user activity on both the internal network as well as on endpoint devices. This requires deploying a network device to inspect network traffic as well as agents on individual computers – at least with high-risk users - to ensure that even disconnected and mobile users are subject to the policies defined by the organization. The goal in monitoring insider activity is to identify both predictable and unpredictable policy violations, so that the organization can respond and proactively correct them. It's important to go further than just looking for matches of sensitive data, which may not catch risk scenarios that you can't anticipate. The key is to profile user activity and look for behavior that is out of the norm.

[1] Common Sense Guide to Prevention and Detection of Insider Threats 2nd Edition — July 2006



Best Practice 5: Decide Where and Whom to Monitor

Where do you deploy? This is a simple question, however, one that is answered incorrectly more often than correctly. It is not practical to capture and analyze all the data processed by your organization's computers or sent through your egress points. Therefore it is necessary to prioritize those assets that have the greatest value to your organization and develop a series of monitoring rules that reflect who has the most access to those assets or the most to gain from obtaining access to those assets.

- For example, for the highest level, you might have a policy on every single desktop that detects whether the company's future secret product plan document is sent out via instant message after hours. That's just simply something that should never happen, no matter whether the sender is the call center rep or the CFO.
- At the next level, you might want a large segment of the user population — say, everyone in engineering and production — to have policies that monitor their USB/mobile storage use, even if just to calibrate the level of exposure by volume of transfer.
- Outsourced call center representatives might need another set of policies that closely track any activities that attempt to extract customer data from the database, such as cut and paste to the clipboard, downloads to mobile storage or even unusual volumes of IM traffic.
- Administrators, as mentioned before, required more sophisticated monitoring, particularly around actions like logins, file alterations, even just high levels of non-business related activities (a leading indicator of job discontent).
- Resigning or terminated employees should be monitored extremely closely, especially those who might be suspected of leaving for a competitor.
- Investigations monitoring is a different business, as noted in the following section.

DECISION POINT: Show Your Cards?

Some industries and organizations believe that informing employees of their specific monitoring capabilities up-front will deter employees from committing malicious or possible criminal activity against their networks. This is a valid strategy in many cases, and also mitigates some concerns about monitoring individual employees.

Other organizations think that it is more advantageous not to inform employees about monitoring. Those that follow this philosophy think that they are more likely to catch those with criminal or dishonest tendencies, as individuals who are afraid of being caught from the existing monitoring techniques will simply seek out other avenues for their dishonest behavior. Think about it in the context of the temporary speed limit enforcement signs that are put up in trouble areas and flash your speed versus the actual speed limit. Most of us instinctively slow down, even though we're pretty sure there's no police officer waiting after the sign. However, there are some drivers who will not adjust their speed, gambling that there's really nobody watching at the other end. And there's a third group that will simply take another route where there is no speed monitoring and go as fast as they want to. It comes down to risk management. Does the behavior modification you get from going public with monitoring outweigh the increased risk from users who will simply circumvent the barriers they now know are there?

In the case of an active investigation, it's a different story—deciding whether to intervene, or to continue or even deepen monitoring. We'll get to that in Best Practice 11.

Best Practice 6: Analyze and Measure Vulnerabilities and Areas of Concern, Leading Indicators

Many organizations' biggest challenge is lack of visibility -- not even knowing what problems they have because their current solutions don't give them visibility into insider activity. So the first thing they'd like to do is simply assess their risk. Think about this as your first step into investigations.

One strategy is to start with a set of monitoring policies that would be "best practices" in any organization. Although it's an investigation, you're investigating the health of the enterprise and assessing your vulnerabilities along vectors that put your assets at risk, looking more for "leading indicators" of harmful behaviors rather than specific incidents.

Typical policies that an enterprise might set at this phase include:

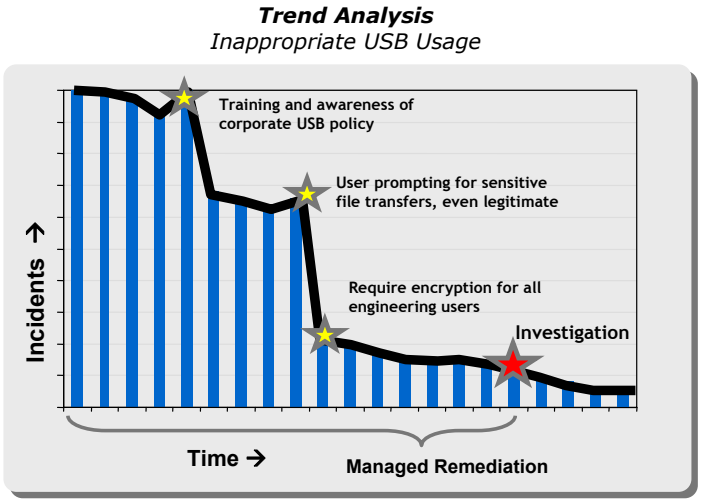
- Unusual network traffic spikes (off-hours, unusual protocols, non-business applications such as webmail, etc.)
- Traffic going to unauthorized geographic destinations (e.g., FTP site in China, where your main competitor is)
- Unauthorized or harmful content (hate sites, pornography, job search sites) that indicate low productivity, job discontent and potential legal liabilities
- High volumes of unmonitored USB/mobile storage use
- Inappropriate use of encryption
- Unusual offline activities
- High printing volumes off-hours

Luckily, tools exist to both monitor for these activities as well as display the results and implications in easy-to-interpret visual formats. Once you've investigated at a high level and determined where your problem areas are, you can start to take focused, efficient and informed action to remediate them.

Best Practice 7: Create Processes to Investigate and Remediate Non-critical Violations with Policy, Automatic or Guided Course Correction

To prevent becoming overwhelmed with false-positives, and to keep your investigations teams focused on what's important, you need systems in place to remediate minor violations automatically or with minimal intervention.

Automated remediation can take several forms. The least intrusive automated responses give users prompts to inform and educate them about a risk if the violation is not a critical one. In parallel, you can incorporate policies to escalate more serious violations. More serious violations might involve a control that stops the session or initiates a detailed workflow to quarantine the data, notify compliance officers and take other actions to ensure any unauthorized behavior can be stopped.



Successful insider risk management drives behavior to comply with policy

In this particular scenario, the company was most concerned about the risk from USB devices, specifically relative to proprietary CAD drawings. The company first deployed a general investigative policy that showed only the levels of USB activity versus what they expected. It was immediately able to see the unusually high levels of USB copies, which at that point were completely unmonitored.

The IT and HR staff took the first step and deployed a company-wide **awareness program** on corporate restrictions on USB usage. This resulted (like the speed limit sign) in an immediate, significant drop in USB incidents, but there still remained an unacceptable level of activity. The company fine-tuned the policies to record (for playback) a subset of user activities, particularly when data was transferred to USB drives after hours. What they found was a trend for users to deliberately ignore the corporate guidelines, but nearly always for quasi-legitimate reasons—taking work home at night, or offsite to a partner meeting.

Nonetheless, these actions still put the company at risk, so they took the extra step of instituting "user-prompting," where in the case of minor policy violations the user was shown a dialogue box reiterating the policy and giving the user opportunity to **self-correct or justify** their "bending" of the policy. As expected, this resulted in another significant drop in incidents. But the investigation results were disturbing enough that the company overlaid an **operational policy** of requiring that all USB devices be encrypted. This reduced the USB incidents to a very small number, which the company then decided to investigate in more detail. What they found were several cases that indicated potential malicious behaviors and potential IP theft attempts.

Incident Investigations

Best Practice 8: Identify Incidents for Investigation

Once you determine that an actual security policy violation has occurred, you must decide how to proceed: Do you continue to monitor and allow the data to leave the network? Do you stop the data from leaving the network and log the individual off his workstation?

Companies need to determine their individual thresholds for escalating incidents for investigations, but these are typically clear-cut once assets are identified and risk scenarios and potential violators are outlined. For example, continuing the USB transfer scenario, a simple USB copy of a CAD file probably does not warrant an investigation. However, a copy of a large number of CAD files, at 11:49 p.m. on a Saturday night, by a system administrator or recently terminated employee, definitely warrants an investigation.

However, there are often incidents that cannot be foreseen despite the best analysis, and in some cases, investigation situations arise through non-digital avenues. Your HR department might notify you that an employee has been complaining loudly about the company and how he can't wait to move on to his new job, and "just might take a few things with me." Or an outside source might notify the company that he had seen proprietary information in some place it shouldn't be, such as a competitor's office.

In any case it's best to have your organization's investigations process teed up and ready to execute with much more sophisticated policies for known violations, AND be able to mine the enterprise monitoring database for additional incidents from an identified violator.

At this point, you have a couple of decisions to make:

DECISION POINT: In-House or Outsourced?

A number of factors should be considered when deciding whether to conduct your own investigation or enlist the help of a firm specializing in the area of digital evidence recovery. For example, it would be wise to ask for assistance if individuals have made every attempt to remove or conceal their activities by either deleting the logs of their activities or the hacking tools they used.

Forensically recovering files that have been wiped is a difficult task; additionally you'll need to make sure that you keep

exhaustive records of your efforts. Also complex breaches are difficult for juries to understand; firms that have a great deal of experience in gathering and presenting this evidence will add to your ability to successfully assist in the prosecution of the individual(s).

It would be wise to hire an expert if you believe that your organization may end up prosecuting or seeking compensation through a civil action, or if the investigation will require very sophisticated disk-level forensics and event log analysis. The good news is that newer event visualization tools can give you all the information and documentation you need to pursue remediation.

DECISION POINT: Intervene? Continue or Deepen Monitoring?

Whether it's in-house or outsourced, another key decision is whether to take corrective action (intervene immediately), or to continue to monitor the identified individuals more aggressively.

Action	Pros	Cons
Intervene	• Stops incident immediately, if serious enough or evidence is conclusive • Might deter others involved in the harmful act	• Evidence might not be conclusive • Might lose data that could shed more light on incident, trend, or other surrounding trigger actions • Could allow others involved but not yet identified to avoid detection and continue harm
Continue to Monitor	• Can learn much more about the scope of the incident • Can learn about surrounding leading indicators of the harmful behavior • Can find others involved in the activity	• Additional harm might be caused, by the perpetrator or by others not yet identified. • Harm might have already taken place, and not acting immediately may worsen the condition

Best Practice 9: Mine Incident Logs and Alert for Historical User Activity/Timeline

Once an incident or incidents have been identified, and user(s) targeted, it is a best practice to go back through the users' historical timeline and look for other harmful behaviors. As most enterprise security practitioners know, the best leading indicator of bad behavior is bad behavior, and it's usually a good bet that someone who's been doing harmful things at one level has a history of harmful, or at least non-productive activities in their past.

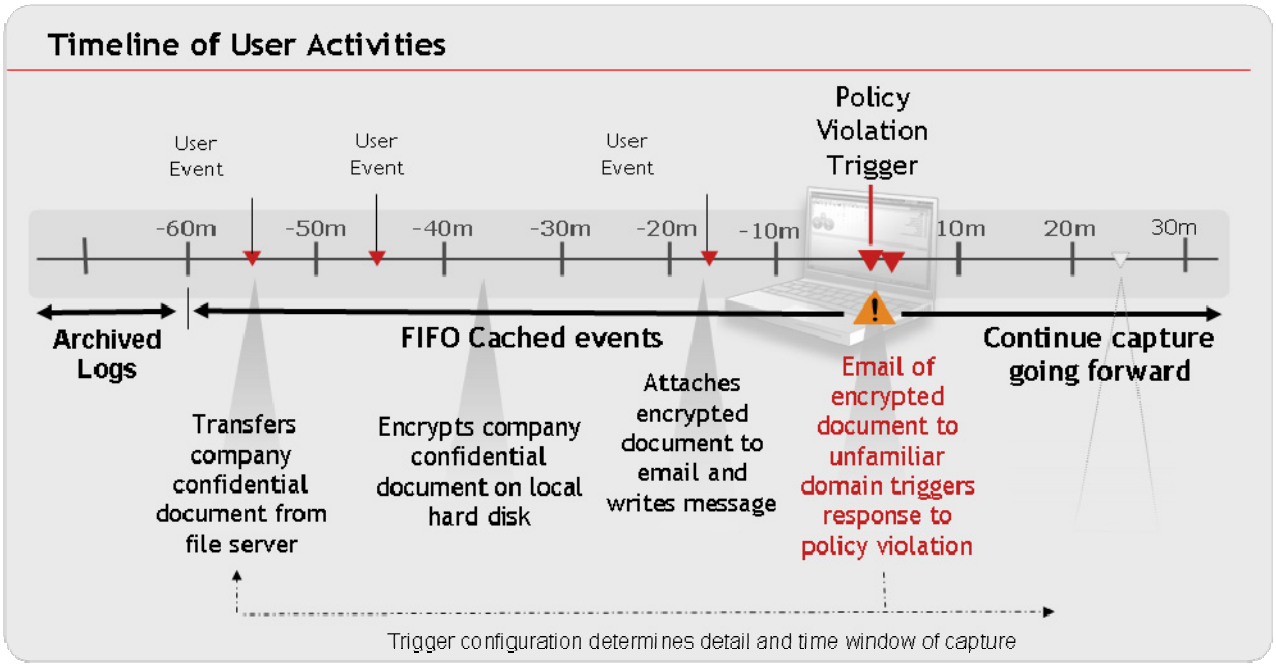
Earlier in this document we discussed the need for enterprise monitoring, and part of that initiative includes logging (but not necessarily alerting or acting on) certain actions that might be leading indicators of harmful or non-productive behavior. Extending the USB scenario we've been using, let's say that the incident under full investigation involves an off-hours copy of a large number of proprietary CAD files.

The investigation yields some interesting facts:

1. Many of the CAD files were encrypted, some weeks before the actual incident.
2. The encrypted files had been renamed with innocuous, non-business names such as "family_photos.zip."
3. E-mail communications associated with the incident referred obliquely to documents that had been "seen" by the eventual recipient, possibly in another format such as JPEGs, for confirmation.

Using that information, the company was able to mine from the enterprise monitoring database:

1. Several cases in which the user in question had done "screen captures" within their sensitive CAD applications. These screen captures were then traced to outbound web-based e-mails.
2. In one instance the incident was captured on replay, which showed the actual screen capture and file manipulation before it was encrypted.
3. By doing quick, Google-like searches on network traffic, the company was able to show that at least two other employees were receiving copies of the JPEG files and were able to add them to the investigations process.
4. Other data points included lots of web traffic on a single competitor's Web site, particularly the jobs section, indicating possible motives for stealing the IP data.



Best Practice 10: Evaluate Incidents in Full Context (And Why This is Important)

Historically, IT and security departments could only pore through endless log files and analyze excruciatingly detailed, disk-level forensics once incidents were discovered. Analysis usually took so long that by the time evidence was located, it was too late to do anything about it. The real breakthrough in insider threat investigations (and monitoring as well) are the visualization tools that allows enterprises to easily spot potentially harmful behaviors and reconstruct actual incidents exactly as they happened—playing them back just like a DVR.

This is critical for several reasons:

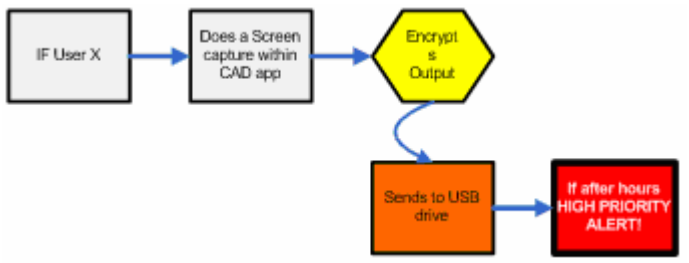
- Visual representation also allows the enterprise to spot "leading indicators" of potentially harmful behavior with just a simple scan. For example, job site webpages, pornographic images and other indicators of discontent or non-productive behavior.
- Visual representation of content moving over the network can be displayed in a way that non-technical users can understand and take action on, allowing management to take a more active role in security.
- Most importantly, video-like replay of incidents delivers multiple benefits from both a monitoring and investigations standpoint:
  - Easily parses out false-positives
  - Definitively exonerates clearly accidental behaviors or mistakes
  - Provides evidentiary proof of discernible, malicious activities
  - Allows for actions that have several components,(such as a screen capture that is saved to an obscure format, renamed, encrypted and then copied to a USB drive) to be completely documented.
  - Gives the enterprise exactly what's needed to take the most focused, efficient remediation possible, whether it's broad education and awareness, individual user coaching, operational intervention (e.g., user prompting), infrastructure modification (changing application access or feature disablement), or even termination and prosecution for truly serious incidents.

DECISION POINT: Rehabilitate, Terminate or Prosecute?

This decision is truly unique to each company, situation and individual, and this document makes no attempt to provide any guidance in this regard. This decision will dramatically impact how much historical data you need to mine from the enterprise monitoring database, at what stage you actually intervene or continue more focused monitoring, and what level of detail and duration you want in your incident capture and incident reconstruction and replay. In all cases though, the ability to mine the database or replay incidents in real time add tremendous value and streamline resolution.

Best Practice 11: Isolate True "Trigger" Events That Lead to This Behavior

This is a complex point, and entire papers can be written on correlation of disparate events that make up an incident. To keep it simple, we'll use the example we talked about earlier, in which a complex set of events led to sensitive documents being leaked via USB drives. A "policy" that would capture that activity would look something like this:



If you analyze this sequence of events, what you see is that the actual data copy to the USB — or whether it was sent out by e-mail or some other outbound communications — is only one small step in a multi-vector event. Solutions that looked only at outbound data streams or USB storage only could be easily circumvented, and probably would be, by this obfuscation. The point is that what the company learned was that the real "trigger event"—the real indicator of bad intention — was the screen capture within the CAD application. Clearly the user was using the screen capture capability to avoid detection (as opposed to saving the file in a different format, which might have been easier to detect).

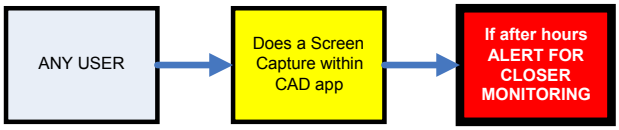
Alternatively, all other steps could have been innocuous, and the encryption "after hours" is what set off the alarm. Armed with this knowledge, companies can then take the next step, which is to build into their enterprise monitoring the policies to identify these events much earlier or prevent them entirely.

Best Practice 12: Build What You Have Learned Back "Upstream" into Enterprise Monitoring

Continuing the example, the company can develop an enterprise monitoring policy that triggers based on the event, "screen capture with CAD application," and use that as the trigger for:

- Alerting for other related CAD actions
- More focused monitoring
- Escalation to investigation

Since this policy will be deployed widely, the company can add the "After Hours" qualifier to reduce false positives.



Summary

A successful program requires constant vigilance, modifications and re-evaluation. Having a seamless platform that links monitoring and investigations while combining rich visualization tools that allow for immediate and accurate incident and trend analysis are key to long-term insider risk management.

Raytheon Solutions

Raytheon helps detect and prevent enterprise IP theft, data loss and other threats, as well as conducts deep forensic investigations into known violations and incidents.

That is why we are the insider threat protection standard for:

- Seven of the Fortune 100
- Top U.S. retailers and manufacturers
- U.S. Department of Defense

Raytheon SureView™ was the first solution to integrate both network and endpoint insider threat detection and prevention, and the only solution that provides a seamless platform for both enterprise monitoring and investigations.

The Raytheon SureView platform is the standard for insider threat detection and prevention, providing:

- Industry-leading endpoint monitoring and incident reconstruction with the SureView endpoint agent, developed and tested in the country's most critical, federal networks.
- The first and only DVR-like incident replay capability with the SureView Replay™ module.
- Hundreds of pre-built policies covering IP and customer data protection, fraud prevention, privileged user monitoring, corporate governance enforcement and legal compliance demonstration.

Additional Resources:

FBI/Cert Investigations Tips
http://www.cert.org/tech_tips/FBI_investigates_crime.html

High Tech Crime Investigation Association
http://www.htcia.org/

Department of Justice Cybercrime Information
http://www.usdoj.gov/criminal/cybercrime/searching.html

Use of Banner Notifications for Monitoring
http://www.cybercrime.gov/ssmanual/index.html

Investigations Involving the Internet and Computer Networks
http://www.ncjrs.gov/pdffiles1/nij/210798.pdf

For further information contact

Intelligence and Information Systems.
2755 E. Cottonwood Parkway
Suite 600
Salt Lake City, Utah
84121 USA
801.733.1100
insiderthreat@raytheon.com

www.raytheon.com
Keyword: insider threat

Raytheon
Customer Success Is Our Mission