ZoneFox

ZoneFox

Insider Threat Profiles

The Anatomy of The Biggest Threat to Your Business

Analyze. Detect. Protect.

WWW.ZONEFOX.COM

ZoneFox

Introduction

Insider threats can be detrimental to your organization, its data, and its brand reputation. One of the factors that makes this kind of threat so hard to detect is that it varies so much. You never know if a disgruntled employee is going to attempt to destroy data, if one of your employees is looking to earn some extra cash by selling your customer data, or if one of your less savvy colleagues will let the bad guys in to do their bidding on your network. Since perhaps the hardest part of managing the insider threat is understanding it, we've put together an overview of five key insider profiles that will help you to start identifying the insider threats in your organization - as well as what to do once you know you're dealing with one.

Disgruntled Dave

Dave was a promising candidate, hired straight out of college to work as a software tester for National Widgets, Inc. Dave learned quite fast, and within a year he became lead software tester for the latest project - a touch-enabled SmartTV, called the SmartTouch.

As lead tester, Dave's duty is to ensure that the software for the SmartTouch is stable and secure, as this is a LAN-capable TV, controllable by any device on the same network through a web interface. The TV also requires Internet access to stream content and download updates.

Dave and his team have found multiple security vulnerabilities that may be exploited if a malicious user attempts to push an update to the TV from the Internet. Dave spends weeks attempting to shed some light on these vulnerabilities to the product managers, but his advice is not heeded as the code is stable. Dave broods over the results of his pleading and his mood turns sour. Dave the wiz kid is now, Disgruntled Dave.

Disgruntled Dave has administrative access to the SmartTouch code repository, and as such has power to manipulate the files as he wishes. In this case, Disgruntled Dave decides that if the organization won't listen to him, he needs to take action to ensure that the project does not move forward.

With a few keystrokes, Disgruntled Dave is able to delete the latest compiled version of the SmartTouch project, as well as the source code. The latest version is where the bug was created, after all, and if they refuse to write it securely, it simply shouldn't exist. Since the leadership at National Widgets wouldn't take his advice on cybersecurity, he can always say that it was probably an external threat actor; a nation state, most likely. After all, with his administrative access he was able to eliminate any logs that would point back to him.

About Disgruntled Dave

Dave was a bright employee who was promoted quite quickly. He thought he was helping the company by bringing to light a vulnerability in the company's software, but since there was no real-world exploit, the management team decided to accept the risk for now and push forward. Dave's advice was not heeded, although he thought he was really on to something. He tried several times to sway public opinion, and in the end his anger pushed him over the edge, causing him to resort to destroying a software release to prove a point. Some of the reasons that employees become disgruntled - and remember, these issues are from the employee's perspective.

1 **Unkept promises**

Perhaps the employee was told that there is room for advancement, and are upset when they are not promoted at the time that they feel it is deserved.

2 **Undervalue**

The employee may feel as though the employer is not providing the challenge and attention to the employee that they deserve.

3 **Unheeded advice**

If an employee constantly provides what they think is sage advice on pressing issues - and the advice is never taken - their opinion of the company or leadership may sour.

Detecting Disgruntled Dave

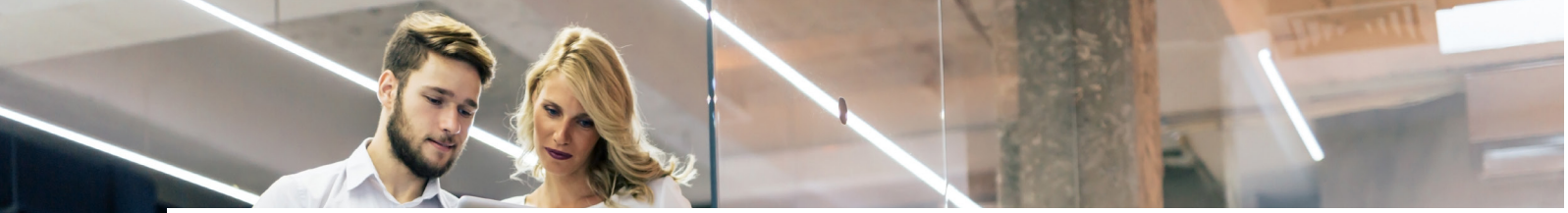
Detecting a disgruntled employee with technical controls is not always easy. The first step you should take, after noticing the human indicators (foul mood, constantly complaining, "wait and see" statements), is to start monitoring their network activity. If an employee is disgruntled, but is spending more time at the office after hours, they may be up to something. Who wants to spend more time in the office if they don't like their job?

They also may attempt to access information on your network that is outside of their scope of work. A disgruntled employee may also download or upload a lot of data for nefarious purposes. Here is how you can use technical controls to detect Disgruntled Daves.

1. **Endpoint monitoring and behaviour analysis**
   Is this user trying to access files that they normally wouldn't? Do they log on at abnormal times? Have there been batches of filesystem transactions, such as deletions?

2. **Data loss prevention solution**
   Monitor data in motion, data at rest, and data in use for policy violations. Is the user attempting to access files that they are not supposed to? Are you noticing attempts to copy or move confidential files?

> A disgruntled employee may or may not be tech savvy, so the trail they leave after attempting to pilfer data may be well hidden, or it may be visible from space. Your cybersecurity analysts only hope is that they'll be able to catch Disgruntled Dave in the act.



Handling Disgruntled Dave

Depending on the level of violation that your Disgruntled Dave has perpetrated, consequences may vary from a scolding and constant monitoring, all the way to dismissal or legal action.

Having an insider threat policy in place will help you classify the threat, assess damage, and administer appropriate consequences. You will require:

+ **Cybersecurity operations**
  To provide proof of insider threat.
+ **Human resources**
  To interview the perpetrator and hand out consequences.
+ **Management**
  To stand witness and sign off on consequences.
+ **Legal team and law enforcement**
  If criminal misconduct is evident.

Dealing with Disgruntled Dave can be problematic, because the damage may already have been done. Being able to detect your disgruntled employees before they can do lasting reputational damage is paramount. Remember, although you can use technical controls to detect nefarious activities, when it comes to disgruntled employees your management teams should be the first responders.

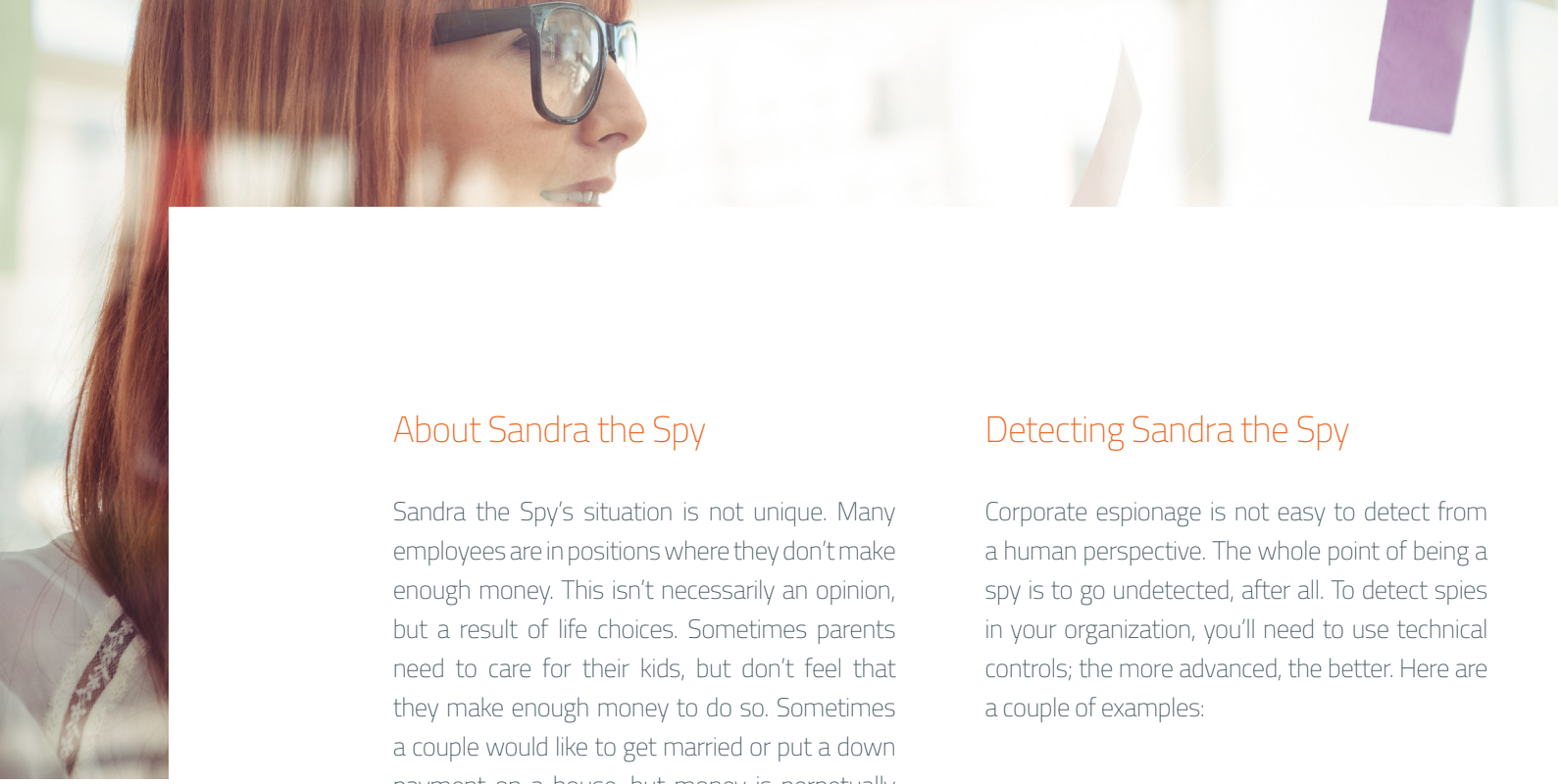
Sandra the Spy

Sandra is a team player, a leader in every sense of the word, and without her, many projects would fail. Luckily, Sandra is the lead architect of a brand new software project to revolutionize the way hospitals monitor their infrastructure. With her leadership skills and her technical mastery, MedMonitor-NG will make MedTech the leader in healthcare IT infrastructure. If you were to lose Sandra before this project is completed and the product launched, it would be catastrophic.

At a networking event for IT professionals, Sandra has a drink or two and confides in one of her peers that she's currently not making enough money. With her recent divorce and the added expenses to take care of the kids and the house that she was left with, her income is stretched quite thin. When one of her peers asks why she doesn't simply ask for a raise, Sandra says that the budget is quite tight, and she can't expect any more money until next year. Nearby, a shadowy character sips on his fine single-malt beverage and smiles. He can help Sandra out, but can she help him? He sends his right-hand man to find out.

Fast-forward two months: Sandra is about to close up shop for the night after putting in a long shift of debugging code for the MedMonitor-NG. She waits for the light to stop blinking on her USB thumb-drive, then ejects and unplugs it from her system. She then heads to her favourite local watering hole to meet up with a couple of friends - since she can now afford to. As she approaches her friends' table, a man approaches her, offering a cheesy pick-up line and putting a hand on her hip. She declines the offer, removing his hand, before heading to see her friends. The man nods to acknowledge the hand-off, and slips the USB stick into his pocket before mumbling an apology and heading out the door. Sandra the Spy goes on with her night.

Three months later, MedTronics, a direct competitor to MedTech, releases new software called HealthTech Monitor, a full month ahead of MedTech's MedMonitor-NG release date. How could this have happened?! The board of directors at MedTech are furious; the VPs of IT and develop-ment are dismissed, as well as the CISO and chief operating officer of the company. There must have been a hack! How could this theft of intellectual property not be detected? Sandra the Spy is promoted to the new VP of development, and she thanks her lucky stars that she has not been caught.



About Sandra the Spy

Sandra the Spy's situation is not unique. Many employees are in positions where they don't make enough money. This isn't necessarily an opinion, but a result of life choices. Sometimes parents need to care for their kids, but don't feel that they make enough money to do so. Sometimes a couple would like to get married or put a down payment on a house, but money is perpetually tight. On occasion, a competing entity with few morals may take advantage, presenting an offer that the potential spy can't (or feels they can't) refuse, turning them to their side. Corporate spies don't always have to be turned, mind you, they may also be planted in your organization early on by a competitor or a nation state to await further instruction. Fortunately, corporate espionage is not an ubiquitous threat to all organizations in all lines of business, but it's always a possibility if your business revolves around intellectual property.

Detecting Sandra the Spy

Corporate espionage is not easy to detect from a human perspective. The whole point of being a spy is to go undetected, after all. To detect spies in your organization, you'll need to use technical controls; the more advanced, the better. Here are a couple of examples:

1. **Endpoint monitoring with behavioural analysis**
   Ensure that you're monitoring your users' activity. Employing user behaviour analysis will provide you with a baseline of activities that are performed by a user on a regular basis, and any deviations from that norm will be flagged as alerts. If a user connects a USB drive to their system, you should know about it, and identify any files copied to said drive. From there you can determine whether or not the data should or should not have been copied.

2. **Endpoint DLP**
   Most endpoint DLP solutions will provide some sort of monitoring or prevention of USB drive usage. If you have data that should not be copied, you should implement a policy that will permit read-only access, and block and report any other actions on the files.

Handling Sandra the Spy

Depending on your line of work, Sandra the Spy's actions could be seen as policy violations, criminal misconduct, or even treason (if you're a government organization). Dismissal is almost always the base consequence, but depending on the level of infiltration and perpetration, you may need to call in the cavalry.

- **Cybersecurity operations**
  To provide information as needed.
- **Human resources**
  To gather information about the employee, perform interviews, and dole out the consequences.
- **Legal team**
  To determine if a lawsuit is imminent.
- **Law enforcement**
  In case there are criminal charges to be doled out.

When it comes to handling a case of industrial espionage, you may need to perform forensic analysis on Sandra the Spy's system, so the first thing you may want to do is create a clone image of the user's hard drive and dump the memory from their system to a file as well. If you don't have the expertise on hand to do this, you should contract it out. Your endpoint monitoring solution should be able to provide history on Sandra the Spy's actions. In the end, you're going to have to use your best judgment, but having an insider threat management program in place will prove valuable.

Careless Caroline

Caroline is an exemplary employee. Caroline is a project manager at R.G. Financial Solutions, and she's the grease that keeps many of the gears turning at R.G. Accounting software needs to be released on time every year, and Caroline is one of the reasons that R.G. keeps making their deadlines. With so much on her plate, however, Caroline can be a bit scattered. Who has time to remember passwords for all of the systems she needs to access, when programmers, graphic designers, and web developers always need someone to light the fire under their butts?

Called away often, Caroline doesn't always lock her workstation. Instead, she relies on the screensaver to kick in and lock it for her. When she comes back she'll check her top desk drawer (not locked) for the sticky note with her network password written on it. Unfortunately, one of her co-workers has noticed Careless Caroline's tendencies, and has decided to capitalize on the opportunity presented to her. When the time is right, she will strike.

Overhearing Careless Caroline complaining about having to run to a last-minute meeting to get various stakeholders aligned to meet yet another deadline, and how long this meeting will take, Caroline's malicious cubicle-neighbour decides that she is going to make her move. As soon as Caroline leaves for her meeting, Malicious Meg sits down to get to work. After a few minutes, she's exploited the top-drawer sticky note (the password is now recorded in her phone), as well as Careless Caroline's file access permissions, and has a full portfolio of project plans and notes that Caroline is planning to present. A little bit of data massaging, and Malicious Meg will be the one they look to for the upcoming internal job opening as lead project manager.

About Careless Caroline

Caroline is definitely not a malicious actor. There is no motivation to steal, destroy, or otherwise harm her organization's data. Unfortunately, Careless Caroline is a very ubiquitous character in today's organization. Whether it's leaving a workstation unlocked, leaving passwords on sticky notes, allowing strangers to tailgate when she swipes into the office, or clicking on malicious links without first understanding who sent the link or why, Careless Carolines everywhere are letting the bad guys in regularly. Even if they don't mean to. Few technical controls can actually help stem this tide; if you want to help Careless Caroline be more careful in her day-to-day dealings, education is key.

Detecting Careless Caroline

In the case of Careless Caroline, you aren't so much detecting her activities as you are someone who exploits her carelessness. If you think that one of your less security-aware users is being exploited, you can use behavioural analysis and endpoint monitoring to be sure.

1. **Endpoint protection with behaviour analysis,** understand how often Careless Caroline is using her workstation. If a user such as Caroline is most often in meetings, they shouldn't be performing mass file transactions throughout that time. If you see Careless Caroline accessing your network resources at odd hours, chances are their credentials have been compromised and someone is trying to modify or steal data off-hours

2. **SIEM/Data analytics Data** such as geolocation, timestamps, and IP subnets can be useful in detecting whether or not someone other than Careless Caroline is using her credentials to access network resources from different geographic locations (or different floors of the same building), or at odd hours.

> While it's not generally Careless Caroline who will be performing any malicious acts on your network, it's imperative that you're able to identify whether or not her credentials have been used for any misdeeds.

Handling Careless Caroline

These situations call for a gentle hand, yet a stern warning. Careless Caroline should be informed that under no circumstances should she be providing avenues for infiltration by malicious actors. You don't want to make Careless Caroline feel as though she has done something terrible, but you should be able to provide enough fear to help highlight the importance of security awareness. Once the offences are listed off, and the point has been made, it's time to provide security awareness training to (hopefully) ensure that these incidents are minimized. The team you'll need are:

+ **Cybersecurity operations**
  Provide security event data where required, and provide security awareness education.

+ **Management team**
  Provide a performance improvement plan for Careless Caroline from a security awareness perspective.

+ **Human Resources**
  Provide oversight in creation of the performance improvement plan, highlight consequences if compliance is not achieved.

Handling insider threats caused by Careless Caroline are hard, because she's not a malicious actor. With a malicious actor, insider threat policy can dictate what happens when said actor crosses the line. If there's no malicious intent, all you can do (at first) is educate, monitor, and hope for the best. Repeat offenders, of course, may face dire consequences, but how many "mistakes" is too many?

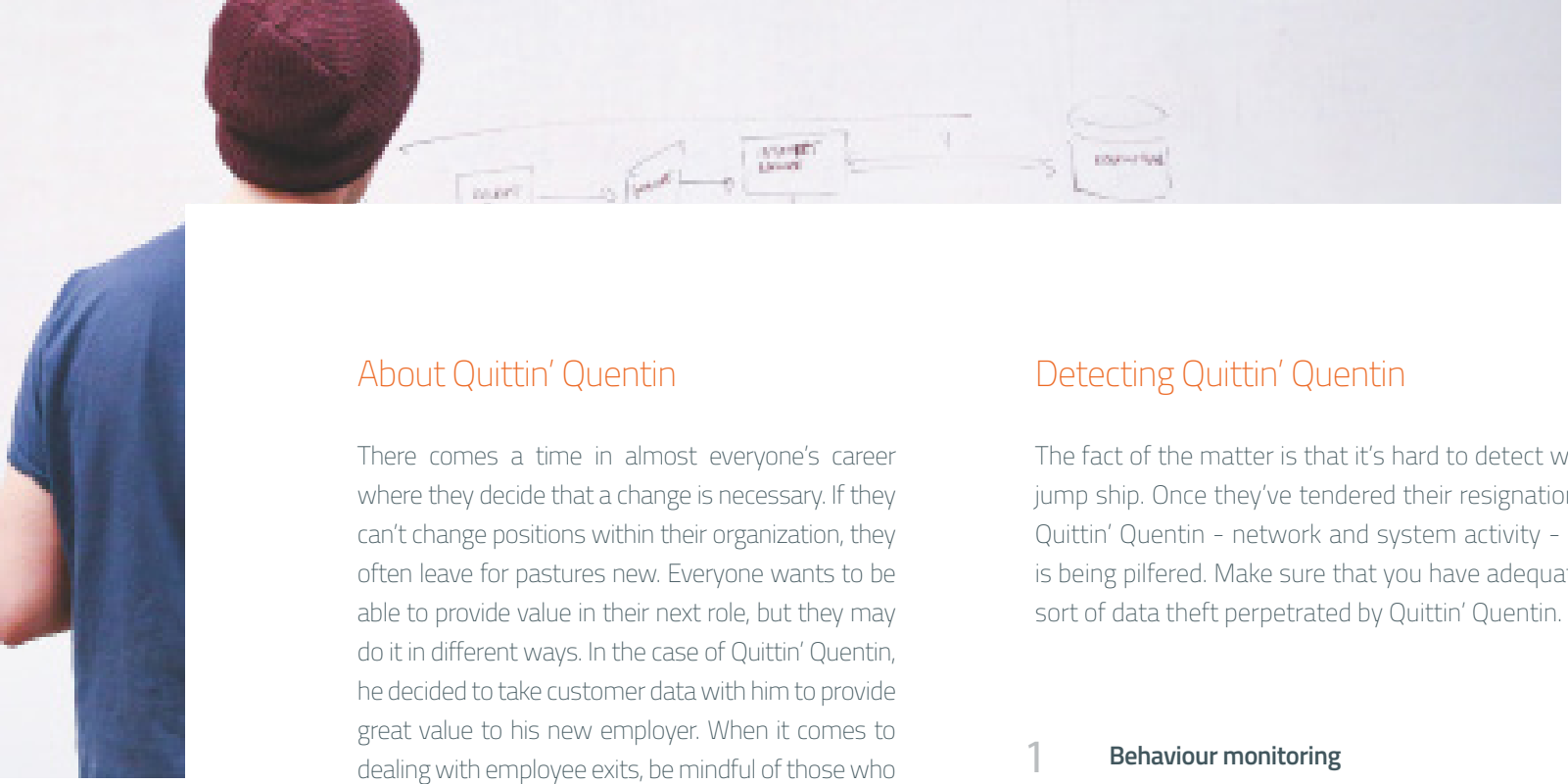
Quittin' Quentin

Quittin' Quentin is a security engineer at Zen Valley Consulting who has been instrumental in moving several major projects forward, keeping a rather large portfolio of clients happy. Having shown significant mastery in the field of big data and advanced analytics, Quentin is becoming quite popular with recruiters. Quentin decides that maybe it's time to check out his options, and so he interviews with a few potential employers. One value-add reseller called Future Insights stands out, and they express great need of his analytical expertise. After being offered a generous base salary and a great commission rate, Quittin' Quentin tenders his resignation to his leaders at Zen Valley.

Since Quentin will be joining a sales team, he decides that bringing along a portfolio of clients can only help his cause in his new gig. Before saying farewell to his teammates, Quittin' Quentin copies much customer information to his favourite cloud storage account.

Customer contact info, network topologies, and sensor configurations are copied up to the cloud for Quentin to retrieve and carry with him to his new job at Future Insights. The management at Zen Valley is none the wiser.

After starting his new job it's apparent that Quittin' Quentin will be leading the consulting practice. Providing consultation, pre and post-sales assistance and quarterly checkups will be part of the role. Quentin's superiors are very happy with the data that he's given them, and the sales team moves forward with contacting each of the clients from the list that Quentin has provided. The main selling point: Quittin' Quentin will be leading the charge when it comes to big data and analytics. Naturally, many of these potential clients leap at the chance to have Quentin back in their environment, to get the level of service that they once had when Quittin' Quentin was with Zen Valley. As a result, Zen Valley loses millions of dollars in annual revenue.



About Quittin' Quentin

There comes a time in almost everyone's career where they decide that a change is necessary. If they can't change positions within their organization, they often leave for pastures new. Everyone wants to be able to provide value in their next role, but they may do it in different ways. In the case of Quittin' Quentin, he decided to take customer data with him to provide great value to his new employer. When it comes to dealing with employee exits, be mindful of those who have access to:

+ **Customer data**
  Contact information, budgets, or price lists.

+ **Intellectual property**
  Code, schematics, business processes.

+ **Technical data**
  Configuration data, vulnerability data.

Detecting Quittin' Quentin

The fact of the matter is that it's hard to detect when one of your best people might jump ship. Once they've tendered their resignation, though, it is time to act. Monitor Quittin' Quentin - network and system activity - to ensure that no proprietary data is being pilfered. Make sure that you have adequate protection in place to detect any sort of data theft perpetrated by Quittin' Quentin.

1 **Behaviour monitoring**
Ensure that you can see if Quittin' Quentin is starting to access customer data on a more frequent basis than is normal, and provide alerts. Are you noticing any frequent movement of data from Quentin's system to the cloud? Is his usual behaviour out of the ordinary?

2 **Data loss prevention**
Monitor access to data stores that contain customer data. Are your client databases being accessed more frequently? Is data being written to file, or are files being copied from client-specific directories?

3 **Web content filtering**
Is Quittin' Quentin frequently connecting and sending a lot of data to cloud storage providers? Are there times before the end of their tenure where they are sending bulk loads of data to the cloud?

Handling Quittin' Quentin

If you've detected Quittin' Quentin's misdeeds on your network, the first thing you need to do is to revoke any privileges he may have on your network. Deleting their account outright might tip them off that you're on to them, so it would be prudent to simply remove permissions on specific file repositories (something you should probably do as soon as they resign anyway), and then approach them for further investigation.

- **Cybersecurity ops** - Intelligence gathering, provide data as required by investigators.
- **IT operations** - Modify user account privileges, provide file access records.
- **Management team** - Provide data on current projects and data access requirements.
- **Human Resources** - Interview the culprit, hand out the consequences.
- **Legal team** - Determine if there are any charges or lawsuits that could come from Quittin' Quentin's actions.

Firing someone who has already resigned is redundant, although if they give you a period of two weeks' notice or some such, you can dismiss them ahead of time. If you know that they're taking company data with them to provide to their next employer, you can sue them - depending on the laws in your region. Ultimately, your best bet is to alert the troops as soon as an employee becomes Quittin' Quentin and start monitoring their activities and limiting their account privileges.

Fraudster Frank

Frank has been a customer service rep for Great West Telecom for two years, working in their call centre. Frank takes calls for nine hours a day, answering questions, resolving issues, but mostly getting yelled at. Frank manages to maintain a smile when he speaks to the clients who blame him for every telco issue that they have ever experienced. At the end of the day, Frank goes home to a small apartment where he lives with his wife and child. Barely able to make ends meet, Frank realizes that there has to be another way.

Over the course of the next six weeks, Frank will be moving to a position on the sales team, where he will be fielding calls from prospective clients looking for mobile phone and Internet service plans. Frank has been working day in and day out at Great West for two years and is really looking forward to his new role, but not just because he won't be getting yelled at as much. You see, Frank has been monitoring some nefarious websites on the "dark web", where he has noticed that he can make money by selling his customers' personally identifiable information, or PII. With his new position at Great West, Frank decides that he could augment his current salary by selling data to which he will now have access.

Once Fraudster Frank starts in his new role, he's shown the ropes by a senior sales representative, given all of the access he needs to process transactions, and shown how to search the database for currently existing clients as well as add new ones. Happy with his new powers, Fraudster Frank starts to execute his plan immediately. With a few simple search queries, our fraudster friend is able to harvest customer PII with ease by simply exporting each query to a comma-separated values (CSV) file. These files are his product on the dark web now, and while this data doesn't fetch quite as high a price as, say, personal health information, he manages to make enough money to do much better than simply make ends meet.

About Fraudster Frank

Fraudster Frank may be malicious by nature, or driven to do bad things by circumstance. Sometimes, Fraudsters will turn to the dark side because their situation calls for desperate measures. Other times, they will be opportunistic and pounce on the chance to make a little extra money doing something unsavoury - if the reward outweighs the risk. If your organization provides the opportunity, Fraudster Frank will definitely capitalize.

Detecting Fraudster Frank

Fraudster Frank can be fairly easy to detect if you understand normal behaviour and monitor database and file transactions on your employees' systems and your network. Detecting a database query that fetches many records, followed by the creation of a spreadsheet file may be the evidence that you require to pinpoint how and when data is being exfiltrated, and by whom. There are multiple tools that you can use to detect Fraudster Frank:

1. **Endpoint monitoring and behaviour analysis**
   Monitor Fraudster Frank's file access, database query frequency, and compare to a baseline of known behaviour. Monitor for the creation of spreadsheet files, and their movement to external storage such as a USB drive or cloud storage service.

2. **Data loss prevention**
   Monitor data at rest to understand which databases are being queried regularly, look for any anomalies in frequency of queries.

3. **SIEM/Data analytics**
   As long as you are sending database logs to your analytics toolset, you should be able to understand the date/time of any queries, the user performing the query, and the data queried.

Monitoring Frank's activities at the endpoint level will provide a level of visibility that would not be otherwise possible. Being able to compare his behaviour with a baseline of previous activity would also augment the accuracy of any alerts.

Handling Fraudster Frank

Dealing with Fraudster Frank will almost definitely require outside help. If someone in your organization has stolen and sold customer PII, they're a criminal. Best to let the authorities handle things once you've gathered sufficient data to prove that they have, in fact, stolen data. Here's the suggested team to handle these threats:

+ **Cybersecurity Operations** - Provide security event data as required.
+ **IT Operations** - Provide hard drive image, as well as database and file access logs.
+ **Human Resources** - Provide any collected info about the employee.
+ **Legal Counsel** - Work with the authorities to avoid legal action taken against the organization.
+ **Law Enforcement** - Interview the employee, assess damage and determine consequences.

Fraudsters in your organization can be bad news indeed. At the very least, your information is being stolen and sold on the black market. If worst comes to worse, you will likely face a class-action suit for mishandling customer PII.

ZoneFox

Conclusion

We know that the insider threat is the greatest risk to your organization's security, and to be truly effective at securing against it, your insider threat management program must include a robust understanding of the various profiles that fall under this threat umbrella *and* the motivations and situations that give rise to them. With this understanding, and the right tools, your business stands a far greater chance of mitigating these threats and keeping your business-critical data safe.

About ZoneFox

ZoneFox is a market leader in User Behaviour Analytics that help secure your business-critical data - and backing it all up with a proven track record of protecting reputation, sales revenue, and competitive advantage. Bottom line? Really great Insider Threat protection that works the way your business needs it to, and not the other way round.

Like to Learn More?

www.zonefox.com

youtube.com/zonefoxvideo

@zonefox

info@zonefox.com

Argyle House,
Edinburgh,
EH3 9DR

0845 388 4999