White Paper

Tackling Insider Threats

intel Security

Table of Contents

Insiders are responsible for almost as many losses, breaches, and thefts of sensitive and confidential data as cybercriminals. According to a recent Intel® Security data exfiltration study, more than 40% of data loss is caused by insiders, roughly half intentional and half accidental. The latest insider thefts have even prompted the US Department of Defense to require affiliated companies to have a program that can "Gather, integrate, and report relevant and available information indicative of a potential or actual insider threat."[1] Whether you do business with the defense industry or not, tackling insider threats is not only a critical challenge to address, but it's also a team effort, necessitating work in data classification, policy development, and incident response, backed by a strong set of data loss prevention tools.

Building a Defensive Formation

Insider activity generates a significant percentage of the incidents that security teams triage and investigate every day. As a result of their job function and responsibilities, insiders have access to the data and processes that the company wants to protect. This access leads to accidental data losses when corporate policies and controls are not adequately defined or enforced. It also provides the opportunity for intentional data theft by insiders.

Most intentional data thefts, whether insider or external, tend to be primarily motivated by some type of financial gain. However, insiders often have secondary objectives, ranging from spying for a competitor to revenge. As a result, intentional insider thefts by disgruntled employees present the broadest possible threat, according to the Intel **Field Guide to Insider Threat.** Their range of access, potential motivations, ability to maneuver, and social engineering opportunities combine to produce every possible type of security event, including espionage, financial fraud, product alteration, and sabotage. So if you can detect and protect your organization from insiders, you are well positioned to catch externally-driven incidents as well.

Focus on the Data

Security defenses often focus on potential egress points, but with insiders, it is more important to identify and monitor the data that you want to protect. Many of the confidential data types are common across many organizations, such as payment card information or customers' personal information. Data types unique to your industry or company are at risk of being overlooked if you rely on standard data templates. For example, companies have caught insiders illegally trading coupons, discount codes, and product activation codes.

Focusing on the data means identifying where your sensitive and confidential data lives, and monitoring when and where it moves. This requires checkpoints at more than just the potential egress points. Data repositories and network switches that watch for data types and keywords can augment endpoint and gateway monitoring, alert the security team to actions that appear to be in violation of corporate policies, block actions that are definitely prohibited, and inform users that their actions are considered a potential misuse of the data.

Coaching a Security Culture

In many organizations, these actions aimed at stopping unauthorized insider activity can be perceived as a negative. If you just start monitoring and blocking actions, without discussing why and how, you run the risk of alienating the people you are trying to protect. Instead, emphasize that you are watching the data, not the users. Put the appropriate tools in place, such as data encryption, and coach your users how to work with sensitive data.

You need to earn trust, and it takes time to change the attitude and culture. Start by discussing who has access to confidential data, and potential threat vectors. From there, build rules and policies that match the scenarios and support the business. For example, many organizations prevent sensitive employee data from being put on a removable drive. However, Human Resources (HR) works with a benefits partner that analyzes employee data twice a year. Instead of leaving HR to find a workaround, try working together to identify the risk points and improve their business process. It will help the HR department to understand and embrace data loss prevention, and develop a more secure business process.

Zone and Player Coverage

Effective data loss prevention against insider threats requires more than just coaching. The disappearance of the network perimeter means you need to cover critical zones and important players. Expand coverage from endpoints and gateways to include the other places that data is used, including storage, cloud apps, and user devices. Pay special attention to those areas and activities that are difficult to monitor, such as secure shell (SSH), encrypted traffic, and USB drives. Is an SSH session carrying a lot of data? Is this encrypted file or data stream consistent with corporate policies?

In addition to these critical zones, you also need watch the players, analyze their behavior, and build a baseline of normal activity. Which ones have access to confidential data? How do they normally use the data? Is this anomalous action trivial or suspicious? This eventually leads to profiling the people in your organization, building broader and deeper visibility around their activities.

Profiling the Players

Opportunity profiling is primarily about identifying roles that have the opportunity to access confidential or sensitive data. You have more surveillance resources and access controls around the restricted parts of a building. You should also apply additional monitoring and more restrictive policy on those people who have confidential data access. However, if you just enable blanket policies you will end up with too many false positives to effectively investigate. So you need to reduce the set of potential insider threats by also looking at potential motivations.

Opportunity profiles based on potential motivation will require collaboration with HR and Legal departments. Carefully working with this sensitive employee information, your team will focus their insider data loss prevention efforts on those with the highest risk. This includes attributes such as income levels, investment activity, negative attitudes, major life events, and other behavioral characteristics associated with potential misuse or abuse of corporate resources.

Armed with this information, the security team can correlate the threat potential against security events. For example, developers often want to use actual data for testing applications. This is not in itself suspicious, but does warrant additional monitoring of both groups involved. In another example, you get a new alert that a sales person emails a confidential spreadsheet to her private email address. Leveraging the historical records captured by your security tools, you notice that this has happened every Friday, and is only being captured now because the data definitions were updated. Instead of pushing the alarm, you reach out and teach her how to work remotely using the VPN. Finally, when a senior manager who is leaving the organization tries to copy large numbers of documents to a USB drive, an alert is sent and the activity is immediately blocked.

Building the Defensive Playbook

All of the activity up to this point results in a series of events for the security team to evaluate, prioritize, investigate, and possibly remediate. Detecting inappropriate data access and preventing data exfiltration are the primary goals. Too often, organizations spend time and effort crafting detailed data classification and control policies, without planning what to do when a policy violation is detected. Best practices for insider incident response include triaging events, integrating with Active Directory, working with HR and Legal, and defining critical escalation paths.

Fast and effective triage of security events is the first stage of incident response. At this stage, the job is to quickly but accurately determine whether an incident requires further investigation, the severity level, and the appropriate remediation team. With insider threats, the potential attacker is already inside the system, so many of the related alerts will be classified as high priority. Reducing the number of false positives by reviewing and fine-tuning policies is a critical activity. However, the biggest single action to reduce the overall volume of insider incidents is setting your data loss prevention tools to give immediate feedback to users that they are trying to do something that is a violation of corporate policy.

When creating profiles, Active Directory should be part of the defense team. Active Directory integration makes it easy to increase the monitoring criteria and strengthen the blocking conditions in your data loss prevention tools, and apply them to specific roles or other user attributes. This enables you to quickly apply profiles across the organization, without having to analyze each individual. Integration with HR systems enables faster linkage between data policies and job changes, including department changes, resignations, and terminations.

Human Resources and Legal departments are two special teams that should be an integral part of your insider threat defenses. Restricting data loss information to the security team is a common practice that limits the value to the business and significantly reduces effectiveness. Sharing the information brings additional perspectives, helping to remove false positives and identify new threat vectors and risk areas. These two teams are also important points on the escalation path, and their capabilities and responsibilities should be part of the incident response plans.

Finally, the human element is a fundamental part of insider theft that should be at the forefront of your planning. Social engineering and credential theft are much easier for internals than externals, so additional precautions and visible checks and balances are necessary to protect your most sensitive data. For example, multi-person controls make it much more difficult for a lone insider to access and exfiltrate restricted data. Or the simple mechanism of copying the manager as well as the user when a policy violation is detected.

Setting the Plays in Motion–Defensive Capabilities from Intel Security

Data protection solutions from Intel Security provide your organization with a wide range of defensive capabilities, providing excellent coverage against both intentional and accidental insider threats. These tools cover the whole playing field, from the endpoint to the cloud, from specific data to security and policy management. Essential functionality includes data loss prevention, browser protections, removable storage controls, data encryption, and database activity monitoring.

Data Loss Prevention

Data loss prevention solutions incorporate sophisticated rules to watch for attempted theft of sensitive files, and can block requests to copy the file to a USB drive, send it to an external email address, or upload it to a file-sharing service. Or, the data can be quickly and automatically encrypted, to make it unreadable from an unauthorized machine or if it is off the corporate network. Centralized management, covering both network and endpoint controls, keeps the solution up to date, including regular discovery of new data, current policies, and real-time analytics. Active Directory groups can be leveraged to quickly build profiles of who can access sensitive documents in the office, who can use them over a VPN, who can print them, and how they can be shared.

Browser Protections

For cloud services, browser protection functions are aware if the user is on a file-sharing site, and provides the option to block files from being uploaded or encrypt the data automatically before it leaves the system. If the user has file sharing apps installed, hooks into the file system prevent sensitive files from being synchronized to the cloud, or encrypts them in less time than it would take to transfer the file, making it transparent to the user. This enables sensitive files to be shared among authorized machines and locations, but leaves them unreadable from personal machines or vulnerable locations.

Removable Storage Device and Media Control

Physical media and devices remain the most common method of data exfiltration by insiders, whether accidental or intentional. Data and device controls identify which types of devices can and cannot be used, and enforce corporate policies on what information can be transferred to them. In addition to physical connectivity, wireless connections, such as Bluetooth and infrared, are also monitored and regulated. Similar to other controls, options are provided to completely block data transfers or automatically encrypt it, depending on the user's role and the category of data. Polices and controls are tied in with centralized management, enabling physical media and devices to be monitored and restricted as part of overall corporate data protection activities.

Encryption

Encrypting data extends data loss prevention well outside the corporate boundaries, greatly reducing or eliminating the value of exfiltrated data. Encryption options range from individual files or folders to full disk encryption for Macs and PCs, and is done automatically and transparently as information is moved and shared. Centrally managed encryption, integrated with other data protection tools, makes it easier to manage and apply consistent policies and controls throughout the organization.

Database Activity Monitoring

Discovering and protecting data throughout the organization requires database activity monitoring functions that can locate, identify, and protect multiple types of data stores, whether they are physical, virtual, or in the cloud. Protection options include virtual patching to defend unpatched systems, known attack libraries, and session termination capabilities to stop policy violations and zero-day attacks.

Application protection rules can even prevent certain apps from touching sensitive files, such as the file transfer features within messaging, telephony, and online meeting apps. The database of security events is open and easily integrated with internal tools or security information and event management (SIEM) solutions. By correlating events across several attributes, you can quickly determine the severity and priority of an incident. For example, you can distinguish between a single, possibly accidental attempt and a user who has made multiple, different attempts to exfiltrate a file.

The goal of these capabilities is not necessarily the complete lock down of all access, which can seriously disrupt business processes and negatively impact productivity. Instead, the focus is on slowing down intentional or accidental exfiltration actions, so that you can detect and mitigate it before any significant damage is done.

Conclusion

We may never block 100% of insider threats, but it is certainly possible to substantially reduce the likelihood of successful data exfiltration, without negatively affecting business processes. Doing this while preserving trust throughout the organization requires a broad effort, involving policy development, user profiling, event monitoring, incident response, and forensic investigation. With well-developed plans and open collaboration with other departments, insider incidents can be resolved quickly, and feedback to the department involved will improve the business process and reduce future threats.

1. Defense Security Service, Industrial Security Letter ISL 2016-02, U.S. Department of Defense, **http://www.dss.mil/documents/isp/ISL2016-02.pdf**

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com

NOVEMBER 2016