CyLab Carnegie Mellon University Security and Privacy Institute

Microsoft

Using Endpoint Signals for Insider Threat Detection

Our research and best practices suggest that insider threat analysts should have access to a myriad of both technical and behavioral data sources. One critical data source to collect comes from endpoint servers and workstations. Aggregating system logs is just one very important piece of this puzzle; however, the fidelity of these logs is often lacking in terms of the standard operating system logging capability. It is often the case that security and insider threat analysts and hunt teams must turn to third party auditing tools to enhance their visibility into endpoint activity because the operating systems themselves lack this functionality. This typically results in additional complexity in the form of more servers and systems to manage for those third-party tools, as well as the added burden of maintaining client endpoint software that must be included in system baselines and upgraded or patched like any other piece of client software.

One such category of software to increase the visibility into system activity is Endpoint Detection and Response (EDR) software, which is designed to monitor endpoints for cyber threats. EDR typically translates to detecting threats that originate outside of the organization, such as malware or other known adversarial behaviors. However, much like many other cybersecurity tools, the focus of EDR software can also be turned inward to detect, prevent, and respond to insider threats.

One example tool that potentially can address both concerns in an organization (minimize the complexity of managing multiple third-party tools and collect endpoint activity data) is Microsoft Defender for Endpoint. Microsoft Defender for Endpoint is a comprehensive endpoint security solution that includes threat and vulnerability management, endpoint protection (EPP), and endpoint detection and response (EDR) designed to monitor endpoints for cyber threats. It is a cloud-based solution that detects suspicious patterns and behavior and offers security teams the ability to investigate and respond to this potentially malicious activity. It does this by collecting data using sensors that are built-in on Windows (i.e. no additional client software to manage) and can be deployed on other platforms, including Linux, macOS, Android, and iOS. In a recent exploration, Carnegie Mellon University sought to determine the feasibility of using this software for insider threat detection purposes. Once configured, Microsoft Defender for Endpoint makes client telemetry available to query from a cloud-based advanced hunting portal using the Kusto Query Language which is also implemented on the Azure Data Explorer. This data augments standard Windows event logging and provides additional detail on several key areas such as processes events, file activity events, and network events. Taking this a step further, Microsoft 365 Defender extends this same kind of threat detection and response capabilities for endpoints to email, identity, and cloud application events.

Much like other data sources for monitoring activity, the data collected by a tool such as this still must be incorporated into a larger analytic platform or pipeline to fuse other technical and behavioral data. For example, we have crafted a sample advanced hunting query that supports the CERT National Insider Threat Center's 30-day rule (most exfiltration occurs within 30 days of an employee's termination date) demonstrating the detection of a terminating employee who downloads a large number of files:

- An insider was employed as a design engineer but was seeking employment with a competitor organization. After announcing a plan to resign, the insider used accrued vacation time to close out the remainder of their employment. During this vacation, however, the insider remotely accessed their company's network to download confidential and proprietary documents valued by the victim at about $1 billion.

The query combines two technical data sources, network traffic and file activity. The network logging is used to infer that the action took place over a non-local connection, such as a VPN. The file activity logging is used to detect a large number of file actions (create/copy or delete) that occur within a 5-minute timeframe. Using this example, we have used one tool to fuse activity logs that may have originated from multiple other sources, such as VPN or network traffic logs to determine the network location of the user, as well as operating system or DLP logs to determine the file actions.

This detection could be further strengthened by dynamically or automatically searching for any employees with an upcoming termination versus manually executing the query for each specific employee account and respective termination date. Otherwise, this type of analysis should be applied as part of a robust employee termination procedure (see Best Practice 20: Develop a comprehensive employee termination procedure from the Common Sense Guide to Mitigating Insider Threats, Sixth Edition.) Moreover, the example query uses an absolute threshold signature for what seems like an anomalous number of file activity events (in this case anything over 1000 files), however this implementation could still benefit from a dynamic scale adjusted based upon this particular user's past activity history.

Another example query incorporates email data to determine when particular files have been sent as attachments to suspicious recipients, which we represent as a "competitor", but this could also include personal or webmail domains which was the case in the following incident:

- The insider was a contractor at a large insurance company. The insider exfiltrated several confidential files containing contracting rates and PII to their personal email account by attaching compressed .zip files to outgoing messages. One of the files within the .zip archive contained over 20,000 names and social security numbers of current and former employees at the victim organization.

These types of signature queries require that an organization first understand and identify high risk recipients, such as personal webmail or competing organizations that may indicate attempted data exfiltration. As part of insider threat month, it is great time to re-examine the goals and focus of the analytic component of your insider threat platform to understand where your critical assets and information exist, the risks insiders pose to those assets, and what tools you have available to provide data that can help prevent, detect, and respond to potential insider threats.