Success Story

Identifying Data Ownership Where There Once was None

Healthcare Testing Company

Hospitals, clinics, doctor's offices and other healthcare providers outsource many testing tasks to external organizations, and when they do so, they must provide their patients' personal healthcare records (or at least a portion of them) - files that contain sensitive information. The hospitals and other organizations exposing their customers' sensitive information to 3rd party medical services companies often audit those organizations to assure they are handling sensitive information appropriately.

One such medical testing organization, to enhance the protection of its customers' patients' data and satisfy compliance requirements, deployed an industry-leading DLP (Data Loss Prevention) system as well as GRC (Governance, Risk, and Compliance) software. The DLP product was able to scan all files on the company's thousands of file shares, identifying those that contained sensitive data (e.g. social security or credit card numbers, insurance and medical information, birthdates, addresses). For each sensitive file identified by the DLP software, the account listed in the "created by" metadata field was assumed to be the owner of the file. That information was passed to the GRC product, and an email was sent to the email address associated with the "created by" account, along with a list of those with access to the sensitive file. The presumed "owner" could then certify that access to the sensitive file was set appropriately.

However, after deployment, the Company realized that the DLP product was identifying tens of thousands of files containing sensitive information with no owners or identifiable, current, Active Directory accounts with email addresses. Explained Kyle Enman, STEALTHbits Professional Services Senior Engineer, "They especially had trouble with files that were created by service accounts, or created by administrator or other elevated-privilege accounts with no email address associated with them." Service accounts are those created to automate interactions with applications, and can create files in the course of their daily activities.

In Brief:

- Healthcare Testing Company
- 40,000 Employees
- Handle the medical records of their customers' patients and are subject to customer audits
- Gaps in DLP sensitive data scan needed to be addressed

Quotes:

- "They especially had trouble with files that were created by service accounts, or created by administrator or other elevated-privilege accounts with no email address associated with them."
- "The Company is very pleased with the results of our product, and our Professional Services integration. There's no way this could have been done without our Team making everything work together."

For example, an application may be set up to create a nightly report and export data to an Excel file. That nightly-created Excel file would have no "human" owner, and if it contained sensitive information, would have no one that could attest to its appropriate access.

Additionally, files created and "owned" by Administrator Accounts were also problematic to the health services company. As Kyle further described, "Administrator accounts don't belong to any specific employee, typically, but are used to access the most critical systems in the organization. Usually, an IT manager may have access to an Administrator account, but that IT manager also has his own account with his email attached. The Administrator account may be used by multiple IT managers over the course of time; it has no email account or single 'owner.' So, if an IT Manager creates a document or other file while logged in using the Admin account (most likely accidentally), the owner of that file would be unclear. That's where STEALTHbits Professional Services team came in."

Led by Kyle, the STEALTHbits Professional Services team built seamless connections between three independently-developed applications: the DLP software, STEALTHbits software, and the GRC product, leveraging the value each brought to the overall security objective. Added Kyle, "We built two interfaces between STEALTHbits software and the other applications: one to accept sensitive file location information from the DLP product, and one to deliver probable owner information to the GRC product to enable the attestation and certification process. Then there was STEALTHbits in the middle, collecting file data, calculating effective access, and conducting probable owner analysis."

The Company's DLP product would identify sensitive files, and then provide the folder locations of those sensitive files to STEALTHbits via the interface built by the STEALTHbits Professional Services Team. Using analysis rules developed in conjunction with the Company's IT personnel, STEALTHbits identified the files in the target folders that were created by service or admin accounts. Then, employing the Data Collection and Activity modules from its flagship StealthAUDIT product, the Professional Services team would identify "probable owners" of the files based on analysis of the collected data, including identifying who owned the majority of other files in that folder, who is accessing files in the same folder, managers of owners of files in the same fold, or who last accessed or modified the specific file in question.

Adds Kyle, "Once we identified the probable owner, we added that name to the 'created by' field, and then we updated the 'last write time' field by one minute, so the next time the DLP product scanned, it pulled in the owner, and we just reduced the number of files without owners. We've done this for tens of thousands of files, and the Company is very pleased with the results of our product, and our Professional Services integration. There's no way this could have been done without our Team making everything work together."

About STEALTHbits Technologies

STEALTHbits is a data security software company. We help organizations ensure the right people have the right access to the right information. By giving our customers insight into who has access and ownership of their unstructured data, and protecting against malicious access, we reduce security risk, fulfill compliance requirements and decrease operations expense.