CLOSING THE DOOR ON OPEN ACCESS

Identifying & Remediating Risk on Unstructured Data

STEALTHbits Technologies, Inc.
200 Central Avenue | Hawthorne, NJ 07506
+1.201.447.9300
www.stealthbits.com

2013

STEALTHbits TECHNOLOGIES

INTRODUCTION

Open access to Unstructured Data is consistently identified by IT professionals as a critical challenge that is as difficult to articulate as it is important to resolve. Often, IT administrators and security auditors alike are overwhelmed by the challenge and may feel paralyzed by the sheer size and complexity of the problem.

For the past decade, STEALTHbits has been working with many of the largest, most complex organizations in the world to perform content collection and analysis across their technology infrastructure. As part of the Access Governance solution built on the StealthAUDIT Management Platform, STEALTHbits has developed an advanced workflow process to identify, prioritize, and reduce risk associated with Unstructured Data.

The STEALTHbits solution, proven at the world's largest organizations, provides a methodical and pragmatic approach that generates quick results addressing the very complex problem of Open Access.

WORKFLOW FOR CLEANUP OF UNSTRUCTURED DATA

This workflow was developed to support large, complex organizations but is also suitable for more streamlined organizations. And each step in the process is configurable to meet specific requirements.

No two organizations are structured exactly the same and we have found similar disparity in security models, access controls, and audit requirements. It was a clear requirement, then, that this workflow must adapt to diverse environments as well as to support dynamic environments over time.

STEP 1, GENERAL ACTIVE DIRECTORY USER & GROUP CLEANUP

Users

Identify Dormant Accounts: Potentially disable accounts and move to a specified OU.
Orphaned SIDs: Locate across unstructured data and auto-replace. Enables removal of SID History.
Password Policy: Identify toxic conditions such as Password-Change-Not-Required, Must-Change, Currently Locked, and User Enabled/Disabled state.
Attribute Verification: Find invalid Manager, Department, Title, Employee Number, or other attributes.

Groups

Identify Toxic Nesting Conditions: Circular Relationships, Cross-Domain, Global Groups within Local.
Size: Large groups (by percentage of user population), Small groups (0-2 users), Empty groups.
Dormant Groups: No permissions assigned or populated with dormant or disabled User accounts.
Duplicate Groups: Similar Memberships by percentage of overlap. Similar permissions assigned.
Identify Group Owners: Advanced workflow to identify and engage group owners.

STEP 2, DISCOVER CONTENT SERVERS

Automated process to discover servers via network scan, network browsing, Active Directory query, or imported list with the ability to customize and/or scope the scans as appropriate. This process generates automatic host lists that groups servers by OS and installed applications.

STEP 3, DISCOVER RESOURCES

Automated process to identify resources such as file shares, SharePoint sites, and installed services such as SharePoint, Exchange, and SQL Server.

STEP 4, DATA CLASSIFICATION/IDENTITY SENSITIVE INFORMATION

The data classification process begins by leveraging content metadata such as file type, size, and location. It then imports data from the STEALTHbits or 3rd party data classification solution. These solutions scan for sensitive content within files based on customizable algorithms. Content identified as sensitive or confidential is classified as such and prioritized appropriately.

In addition to automated solutions, additional classification information can be imported via white list or target list integration if certain assets are already known to be either public or sensitive. This classification process supports advanced use-case scenarios such as ethical wall reporting or remediation workflows around high priority content.

STEP 5, IDENTIFY SHARE TYPE

File shares are identified as being one of three types: Application Share, User Business Share, or User Personal Share. The criteria and taxonomy are customizable but are, by default, based on the following:

Content Types: Application data (EXE, DLLs, CSV, XML, DB files), Business Data (DOC, XLSX, PDF, PPTX), and Personal Data (MP3, graphic and video files)
Permission Levels: Explicit rights assignments on Domain Users or Groups, Built-in Security Principals, and Service Accounts – identifying how rights are applied.
Authors & Access Activity: Identifies where service accounts are creating content, analyzes user activity based on department, manager, etc. Is there one primary author or many?

STEP 6, DETERMINE EXPOSURE

Exposure is primarily determined based on two factors. The first consideration is openness. How open is the access? Is it open to all users? What are the trustee types that have been assigned rights? Is it assigned full permissions or read-only? The other factor is surface area or footprint. How many folders or files are exposed? How many Lists or Libraries are exposed within a SharePoint site?

STEP 7, DETERMINE PROBABILITY OF RISK

Armed with data classification, share type, and exposure level, the next step is to add a few more ingredients such as content age, number of contributors, and recent activity and to ultimately generate a risk score. This risk probability determines prioritization and may drive decisions within the implementation plan.

STEP 8, DETERMINE OWNERS

Resource ownership is primarily based on permissions and user activity. However, in cases where the result may be ambiguous, a deep dive into security group memberships, group owners, and the user's manager field helps generate a list of probable owners. Based on that list, an automated workflow process enables contact with probable owners to verify ownership and/or to solicit recommendations on ownership. This workflow is auditable via reports that show process status, which resources have been reviewed, and where owners have not yet been confirmed.

STEP 9, IMPLEMENTATION PLAN

With a thorough understanding of the risk profile across the unstructured data within the environment, and having assigned data owners, an implementation plan is generated to address high-risk conditions and establish a baseline of user entitlements to support on-going audit and review requirements.

Tasks may include automatically removing open access, monitoring user activity, automating group and/or permission changes, assigning resource-based group permissions, validating configuration against golden images, and automating the content owner entitlement review process, commonly referred to as attestation.

CONCLUSION

The workflow process described above is not a one-size-fits-all prescription or set of project requirements, but many of the steps within can provide tremendous value for any organization beginning to identify, analyze, or remediate unstructured data across their environment.

The solution logic enables answers to critical questions that are not otherwise possible to achieve. And where an organization already has certain answers about where sensitive data exists or who might own it, for example, that information can be easily plugged into the process where appropriate.

STEALTHbits welcomes an opportunity to discuss how this process might provide value for your organization. Please visit us online for more information.

STEALTHbits TECHNOLOGIES

P. +1.201.447.9300 | E. sales@stealthbits.com | W. http://www.stealthbits.com