stealthAUDIT

STEALTHAUDIT® ACTION MODULE FRAMEWORK

stealthbits
NOW PART OF netwrix

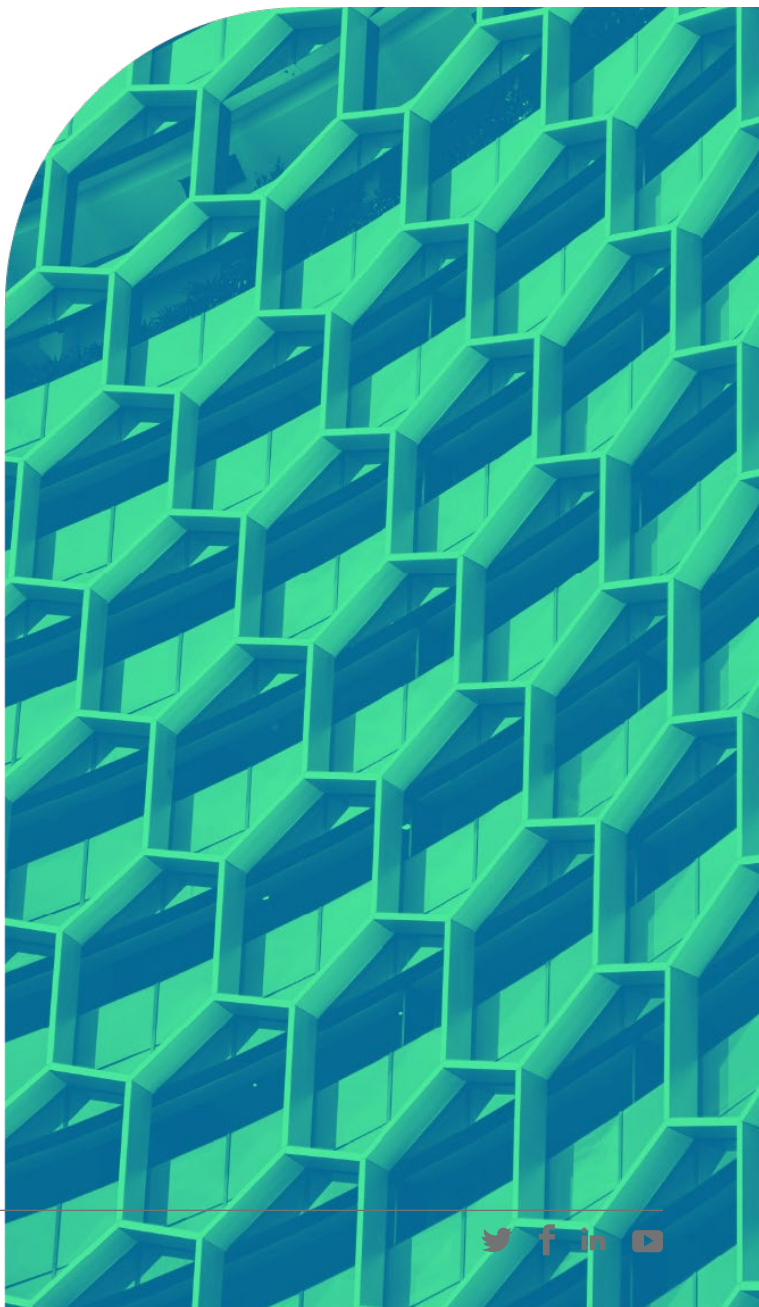
Remediation & Orchestration

StealthAUDIT "Action Modules" enable users to remediate various conditions identified via StealthAUDIT data collection and analysis routines in bulk, as well as orchestrate workflows to automate otherwise manual processes and procedures corresponding to Active Directory, File Systems, SharePoint, Microsoft Exchange Server, and more.

This document details the functions of each Action Module contained within StealthAUDIT, as well as use cases Action Modules are commonly leveraged for.

StealthAUDIT Action Modules

- **Active Directory**
- **Exchange Public Folder**
- **File System**
- **SendMail**
- **SharePoint**
- **Survey**
- **Exchange Mailbox**
- **ServiceNow**



Active Directory Action Module

Operations

- Clear/Set SID history
- Change Computer object details/attributes
- Create Users
- Delete Objects (User, Group, Computer)
- Disable/Enable Users
- Change Group object details/attributes
- Modify Group Membership
- Remove all members from a group
- Move objects
- Set/Reset user passwords
- Unlock users
- Change user details/attributes

Sample Use Cases

Business Process Automation (Terminations):

When your employees are terminated or leave an organization, the off-boarding process can many times involve manual tasks, the involvement of custom scripting routines, and multiple technologies. Using StealthAUDIT and the Active Directory Action Module, many organizations automate the account de-provisioning process by allowing StealthAUDIT to take a feed from their HR system, and then configuring the Active Directory Action Module to disable and move the account to a designated Organizational Unit (OU) within AD. This OU is also often protected by Stealthbits' StealthINTERCEPT for Active Directory, where users and administrators are blocked from moving, re-enabling, or otherwise tampering with disabled accounts.

Active Directory Clean-up:

Stale and unwanted objects within Active Directory make the environment more difficult to understand, manage, and secure. They can also affect a variety of processes associated with important technologies like Identity & Access Management platforms and Disaster Recovery solutions. As StealthAUDIT identifies stale objects and those that are no longer needed according to end-user feedback or organizational definitions, the Active Directory Action Module can be configured to automatically disable, move, or delete them. StealthAUDIT can also enrich Active Directory by synchronizing AD Object Attributes with more reliable sources of user metadata like HR Systems, ensuring important attributes like departments, titles, managers, and physical locations are populated with reliable information.

File System Action Module

Operations

- Change attributes
- Change permissions and auditing
- Change permission inheritance
- Change share permissions
- Copy
- Delete
- Launch remote process
- Move
- Remove permissions
- Remove share permissions
- Rename
- Add/remove tags

Sample Use Cases

Stale Data Clean-up (Data Lifecycle Management):

Stale data consumes massive amounts of storage space on file servers, forcing unnecessary expenditure on additional storage resources to accommodate growing data creation trends. Leveraging the File System Action Module in conjunction with StealthAUDIT analysis of stale files, users can automatically reclaim storage space consumed by stale files by moving and deleting stale data in bulk. As part of automated, customizable workflows, the File System Action Module can facilitate full stale data clean-up campaigns, providing options such stubbing and shortcutting to move data permanently or temporarily as part of a staged program. Shortcut files can be subsequently monitored for activity, allowing for automatic rehydration of files that are still in use.

Data Classification:

The ability to mark files with metadata indicating the type or sensitivity of the data contained within them is critical to successful outcomes for major initiatives like Data Loss Prevention (DLP) and Business Intelligence (BI). In conjunction with StealthAUDIT's Sensitive Data Discovery capabilities, the File System Action Module can automatically tag files with their associated classifications in bulk, enriching document metadata and increasing the efficiency and effectiveness of other technology investments.

Sharepoint Action Module

Operations

- Add site trustee
- Remove site trustee
- Add list trustee
- Remove list trustee
- Add library trustee
- Remove library trustee
- Add group member
- Remove group member

Sample Use Cases

Access Governance

Stale Ensuring access rights are limited to only the right individuals is a critical component of an effective data security program. In conjunction with StealthAUDIT SharePoint permissions scans and entitlement reviews, users can leverage the SharePoint Action Module to automatically remove unused or undesirable permissions based on data owner feedback.

Mailbox Action Module

Operations

- Delete mailbox contents
- Add/change permissions
- Remove permissions
- Add delegates
- Remove delegates
- Remove stale SIDs

Sample Use Cases

Privileged Access Remediation

Mailboxes within Microsoft Exchange Server are one of the largest repositories of unstructured data within any organization. Given the nature of email, its inherent record of conversations between individuals both within and outside of the organization, and the prevalence of documents in the form of attachments contained within many messages, privileged access to Mailboxes through high-level rights like Delegates should be reviewed regularly and limited to only those who need it. In conjunction with StealthAUDIT Exchange access scans and entitlement reviews, the Mailbox Action Module can automate the removal of Delegated Access Rights, limiting end-user exposure to inappropriate data access.

Public Folder Action Module

Operations

- Rename
- Change permissions
- Modify custom attributes
- Reduce replicas
- Modify limits
- Delete

Sample Use Cases

Public Folder Clean-up

Exchange Public Folders have long been deprecated as a collaboration mechanism within the Microsoft ecosystem. Public Folder were often created but rarely deleted, and have also been left in a state of limbo as organizations moved to technologies like SharePoint. In conjunction with StealthAUDIT collection and analysis of Public Folder data, users can completely eradicate Public Folders from their Exchange environments, reducing replicas, obtaining feedback about desired remediation options from identified folder owners, and deleting no-longer needed folders in bulk.

Sendmail Action Module

Description

The SendMail Action Module provides StealthAUDIT Administrators a method of communicating with end users en masse by facilitating the creation and distribution of email messages containing dynamic, user-specific content from selected audit data.

Sample Use Cases

Security Process Support (Password Policy)

To help end users manage the process of changing their passwords according to organizationally-defined policies, a series of emails can be delivered to each user based upon information collected via StealthAUDIT scans (e.g. password expiration date) informing them of how many days they have before a password change is required. Additionally, instructions on how to craft a strong password in accordance with the organization's password policy can be provided, along with additional resources like links to internal or external websites, videos, etc. The end result is greater awareness, increased security, and reduced helpdesk traffic associated with password-related issues.

Survey Action Module

Description

The Survey Action Module provides StealthAUDIT Administrators a method of soliciting feedback from end users to expedite and aid in various decision making processes.

The Survey Action Module will automatically build a customized, web-based survey, distributed via email, for users to answer questions you've design. Preconfigured templates and survey samples are also provided out-of-the-box to help get you started.

Sample Use Cases

Solftware License Reclamation

Software licenses can often be very expensive, and even more so when they've been purchased and not utilized. Leveraging software installation and usage data collected and analyzed by StealthAUDIT, users can create customized surveys distributed to system owners via email that allow end-users to provide feedback as to whether or not they still need the licenses of software they no longer or have never utilized. The answers they provide in turn allow the business to reclaim or reallocate software licenses, offsetting costs and saving money for their organizations.

ServiceNow Action Module

Description

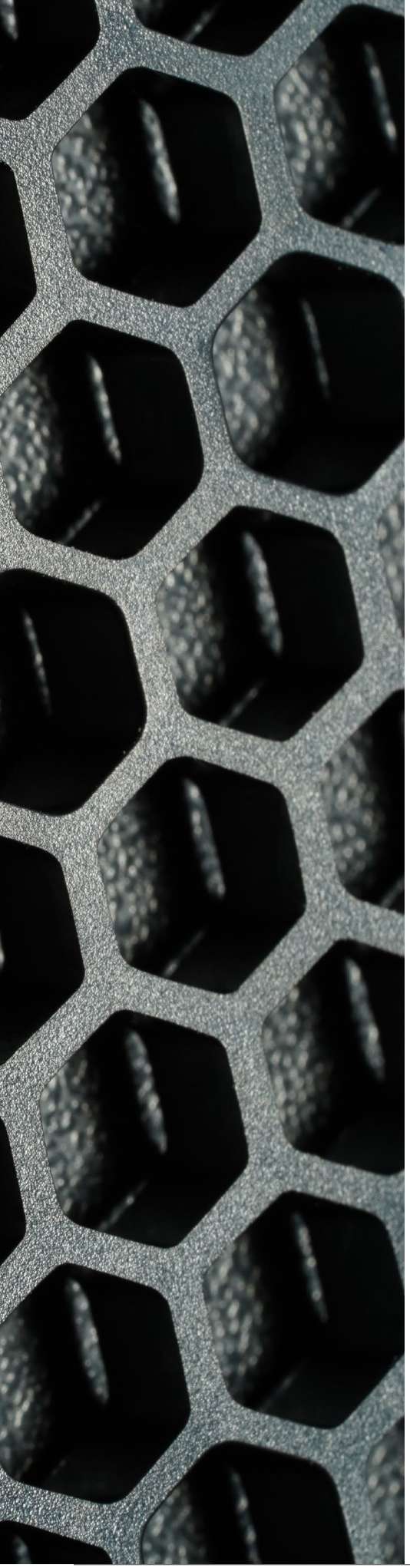
The ServiceNow Action Module enables StealthAUDIT Administrators to automatically create ServiceNow Incidents (i.e. tickets) based upon StealthAUDIT scan data or analyses.

With the ability to inject data dynamically into various incident fields and set priorities based on the nature of the condition found, organizations can proactively identify, track, and remediate issues through their preferred IT Service Management system, ServiceNow.

Sample Use Cases

Local Administrator Access Changes

Privilege escalations at the endpoint often go unnoticed, and are a leading cause of data breaches and insider theft. Using the ServiceNow Action Module in conjunction with StealthAUDIT privileged access scans across desktop and server infrastructure, users can automate the creation of Incidents and review each privilege escalation. By revoking rights to align with least privilege principles, organizations can effectively and proactively reduce their threat surface.



NEXT STEPS

Schedule a demo
Stealthbits.com/demo

Download a free trial
Stealthbits.com/free-trial

Contact us
info@Stealthbits.com

IDENTIFY THREATS. SECURE DATA. REDUCE RISK.

Stealthbits Technologies, Inc. is a customer-driven cybersecurity software company focused on protecting an organization's sensitive data and the credentials attackers use to steal that data. By removing inappropriate data access, enforcing security policy, and detecting advanced threats, our highly innovative and infinitely flexible platform delivers real protection that reduces security risk, fulfills compliance requirements, and decreases operational expense.

stealthbits
NOW PART OF netwrix