SOLUTION BRIEF

National Institute of Standards and Technology (NIST)

Cybersecurity Framework

The National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) provides a policy framework of computer security guidance for how private sector organizations in the United States can assess and improve their ability to prevent, detect, and respond to cyber attacks. NIST CSF encompasses security best practices from several security documents, organizations, and publications, and are designed as a framework. Following NIST CSF guidelines and recommendations can help organizations ensure compliance with other regulations, such as HIPAA, FISMA, or SOX.

HOW STEALTHBITS CAN HELP

STEALTHbits Technologies provides a comprehensive set of tools to enable our customers to execute the NIST CSF. Building on security best practices that are build into the framework, we have enabled customers to detect, assess, govern, and mitigate threats to your organizations sensitive data.

In this document, we have mapped NIST CSF to our set of solutions to help you in leveraging the framework:

IDENTIFY (ID)				
Category	**Subcategory**	**Report Mapping**	**Capability Mapping**	**STEALTHbits Applicability**
ASSET MANAGEMENT (ID.AM) The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization’s risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried	Governance Configuration	Configuration Baseline Analysis Data Access Governance	STEALTHbits provides built-in, agentless discovery capabilities to identify and inventory many different types of systems, applications, and devices connected to an organization's computer network.

IDENTIFY (ID)				
Category	**Subcategory**	**Report Mapping**	**Capability Mapping**	**STEALTHbits Applicability**
ASSET MANAGEMENT (ID.AM) The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-2: Software platforms and applications within the organization are inventoried	Governance Configuration	Configuration Baseline Analysis Data Access Governance	STEALTHbits' deep, OS-level visibility across Windows, Unix, and Linux systems provides organizations the ability to inventory systems themselves, as well as any application installed, configuration, or process.
	ID.AM-3: Organizational communication and data flows are mapped	Governance Configuration	Data Access Governance Data Classification	STEALTHbits provides deep visibility into unstructured data repositories and their contents, as well as directories and their objects, enabling organizations bi-directional visibility into data and user access and activity.
	ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	Governance Configuration	Data Access Governance Data Classification	STEALTHbits provides embedded data classification capabilities and the ability to integrate with alternative data classification solutions. Additionally, STEALTHbits provides analysis facilities that can incorporate additional risk logic according to customer specifications for prioritization of risk and/or efforts.
RISK MANAGEMENT (ID.RA) The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ID.RA-1: Asset vulnerabilities are identified and documented	Auditing Configuration	Configuration Baseline Analysis Data Access Governance	STEALTHbits provides patch validation to determine compliance with patch and anti-virus updates to identify and remediate security vulnerabilities.
	ID.RA-3: Threats, both internal and external, are identified and documented	Access Auditing Configuration Credentials Governance Privileged Access	Change & Access Monitoring Configuration Baseline Analysis Data Access Governance Data Classification File Activity Monitoring Privileged Account Auditing Sensitive Data Discovery Stale File Clean-up Threat Detection User Behavior Analytics	STEALTHbits is capable of detecting advanced threats and suspicious activity patterns indicative of Brute Force Attacks, Horizontal/Lateral Account Movement, Breached Passwords, Concurrent Logins, Account Hacking, and more.

PROTECT (PR)				
Category	**Subcategory**	**Report Mapping**	**Capability Mapping**	**STEALTHbits Applicability**
ACCESS CONTROL (PR.AC) Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	PR.AC-1: Identities and credentials are managed for authorized devices and users	Access Auditing Credentials Governance Privileged Access	Change & Access Monitoring Data Access Governance Privileged Account Auditing	STEALTHbits catalogs all users and details about their authorizations to data resources, enabling governance over data access and the enforcement of a least privilege access model.
	PR.AC-3: Remote access is managed	Access Auditing Credentials Governance Privileged Access	Change & Access Monitoring Data Access Governance Privileged Account Auditing	STEALTHbits provides real-time monitoring and alerting on all authentication activities, including the protocols being leveraged to connect to system and data resources.
	PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	Access Auditing Credentials Governance Privileged Access	Change & Access Monitoring Data Access Governance Privileged Account Auditing	STEALTHbits provides deep-level inspection of system, data, and application access rights and permissions across File Systems, SharePoint, Office 365, Dropbox, Box, Active Directory, Window, Unix, and Linux operating systems, and SQL databases. STEALTHbits additionally provides automated workflows to transform access rights in alignment with least privilege models and analyze the violation of ethical wall boundaries.
DATA SECURITY (PR.DS) Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-1: Data-at-rest is protected	Access Auditing Configuration Credentials Governance Privileged Access	Change & Access Monitoring Configuration Baseline Analysis Data Access Governance Data Classification File Activity Monitoring Privileged Account Auditing Sensitive Data Discovery Stale File Clean-up Threat Detection User Behavior Analytics	STEALTHbits enables an organization to understand every aspect of their data at rest, providing the ability to discover where this data exists to begin with, who has access, what level of permission users have, monitor activity, discover and classify sensitive data, audit file metadata, establish and assign ownership, calculate risk, govern access, and more. STEALTHbits' automated access transformation workflow enables organizations to establish least privilege access controls over their unstructured data, which not only ensures the fewest number of people have the least of amount of access to the data they need, but positions the environment for inclusion in Identity & Access Management programs.

PROTECT (PR)				
Category	**Subcategory**	**Report Mapping**	**Capability Mapping**	**STEALTHbits Applicability**
DATA SECURITY (PR.DS) Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	Configuration Governance	Configuration Baseline Analysis Data Access Governance	STEALTHbits efficiently locates content that has not been modified in a defined period of time to identify areas where clean-up efforts can be focused. Clean-up of data can help to save costs associated with data storage and management, as well as in reducing risk. Additionally, STEALTHbits provides robust clean-up facilities for Active Directory, identifying not only stale objects like Users, Groups, and Computers, but toxic conditions and over permissive access to objects themselves.
	PR.DS-5: Protections against data leaks are implemented	Access Auditing Configuration Credentials Governance Privileged Access	Change & Access Monitoring Configuration Baseline Analysis Data Access Governance Data Classification File Activity Monitoring Privileged Account Auditing Sensitive Data Discovery Stale File Clean-up Threat Detection User Behavior Analytics	To protect against data leaks, STEALTHbits employs the following 5-stage methodology: **Discover** - Understand what you have, where it is, and what's putting you at risk (Open Access, Sensitive Data, Privileged Accounts/Access, Security Configuration) **Alert** - Alert on the most important events, activities, and behaviors (Ransomware, Suspicious Behavior, Authentication-based Attacks, Privilege Escalation) **Remediate** - Fix the problems you find to reduce risk and achieve compliance (Stale Data Clean-up, Stale Object Clean-up, Open Access, Overprovisioned Access) **Integrate** - Connect and enrich disparate systems and applications for enhanced ROI and effectiveness (IAM/PIM, SIEM, DLP, ITSM, CMDB) **Automate** - Automate manual process to save time and increase efficiency (Entitlement Reviews, Self-Service Access Requests, Data Classification & Tagging)

PROTECT (PR)				
Category	**Subcategory**	**Report Mapping**	**Capability Mapping**	**STEALTHbits Applicability**
PROTCTIVE TECHNOLOGY (PR.PT) Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	Auditing Governance	Data Access Governance Rollback & Recovery	STEALTHbits is capable of monitoring and harvesting File System activities such as file access events, creations, modifications, deletions, and moves, as well as permission changes. Organizations can query and report upon all collected file activity such as who accessed a particular folder or file, at what time, and from where, as well as what administrators are doing with their access privileges. All or subsets of data can be fed to alternative technologies like SIEM in real-time for advanced analysis and correlation.
	PR.PT-2: Removable media is protected and its use restricted according to policy	Configuration	Data Access Governance	STEALTHbits can verify policies are established and implemented properly to prevent the use of removable media across all desktop and server infrastructure.
	PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	Access Auditing Configuration Credentials Governance Privileged Access	Change & Access Monitoring Configuration Baseline Analysis Data Access Governance Data Classification File Activity Monitoring Privileged Account Auditing Sensitive Data Discovery Stale File Clean-up	STEALTHbits provides the ability to assess and govern access to systems, highlighting who has administrative access and how, local policies that provide administrative rights, and more.

STEALTHbits Technologies is a cybersecurity software company focused on protecting an organization's sensitive data and the credentials attackers use to steal that data. ©2018 STEALTHbits Technologies, Inc. SB-NIST-0118