SOLUTION BRIEF

International Traffic in Arms Regulations (ITAR)

The International Traffic in Arms Regulations (ITAR) is a United States regulatory compliance standard that restricts and controls the export of defense and military related technologies to safeguard U.S. national security. The U.S. Government requires all manufacturers, exporters, and brokers of defense articles, defense services or related technical data to be ITAR compliant.

For a company involved in the manufacture, sale or distribution of goods or services covered under the United States Munitions List (USML), or a component supplier to goods covered under the USML, the company is required to be ITAR compliant, meaning the company must be registered with the State Department's Directorate of Defense Trade Controls (DDTC). Overall, the U.S. government is attempting to prevent the disclosure or transfer of sensitive information to a foreign national.

Specifically, ITAR [22 CFR 120-130]:

- Military items or defense articles
- Goods and technology designed to kill or defend against death in a military setting
- Space-related technology because of the application to missile technology
- Technical data related to defense articles and services
- Strict regulatory licensing

HOW STEALTHBITS CAN HELP

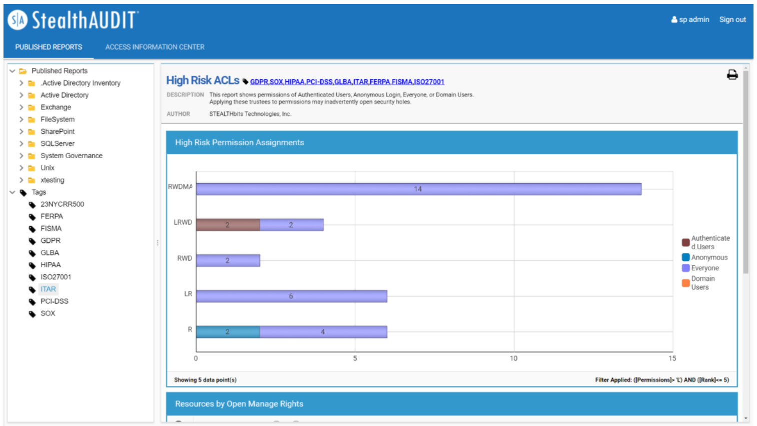
SENSITIVE DATA DISCOVERY & CLASSIFICATION

STEALTHbits Technologies provides a comprehensive sensitive data discovery and classification solution combined with robust governance, remediation, and monitoring facilities. STEALTHbits' sensitive data discovery capabilities provide organizations the ability to scan the contents of over 400 file types, including images using Optical Character Recognition (OCR), to identify sensitive information like Computer Aided Design (CAD), Credit Card Numbers, Social Security Numbers, Personal Health Information (PHI), and dozens of other types of Personally Identifiable Information (PII). Users can also search for unique criteria specific to their organization such as Employee ID numbers, trade secrets, product formulas, and more.

In order to apply the appropriate controls, classification cannot merely exist in the database itself. Sufficient data classification requires tagging file metadata to achieve persistence regardless of where that file resides currently, or at any time in the information lifecycle. With STEALTHbits, your organization will be able to collect file metadata including classification tags that have been implemented via internal processes or third party solutions, as well as tag files with classifications that denote the file's sensitivity levels, contents, or other designations.

Whether preconfigured or customized, any report can be tagged with standard or custom labels for easy filtering. Out of the box tags are provided for various standards, including GDPR, FERPA, FISMA, GLBA, HIPAA, ISO27001, ITAR, PCI-DSS, and SOX.

STEALTHbits also proactively fills in the missing pieces to the sensitive information security equation, identifying who has access to the data and how, who owns the data and can make decisions about it, who's accessing the data, and even where abnormal and nefarious activities may be occurring against sensitive information specifically.



High Risk ACLs GDPR,SOX,HIPAA,PCI-DSS,GLBA,ITAR,FERPA,FISMA,ISO27001

DESCRIPTION This report shows permissions of Authenticated Users, Anonymous Login, Everyone, or Domain Users. Applying these trustees to permissions may inadvertently open security holes.

AUTHOR STEALTHbits Technologies, Inc.

Showing 5 data point(s)

Filter Applied: ([Permissions]> 'L') AND ([Rank]<= 5)

ACCESS CONTROL

When analyzing an organization's sensitive information that falls under ITAR, STEALTHbits leverages a multipronged approach. Not only does sensitive data discovery and classification play a large role into meeting the regulation, but so does a holistic data access governance strategy. Included in this strategy to help meet ITAR requirements is identifying, remediating, and mitigating access risks like Open Shares, as well as monitoring file activity to obtain a forensic audit trail of every file touch.

If your organization's sensitive information is stored on file shares that are effectively "open" to everyone or large sums of people, the risk of unauthorized access to that data is drastically increased. STEALTHbits offers a methodical and pragmatic approach to generate quick results when addressing open access, enabling organizations to locate and subsequently secure their file shares using a least privilege access model, as well govern access easily and efficiently on an ongoing basis to keep access rights in alignment with ITAR requirements.

STEALTHbits also enables organizations to efficiently capture file activity across the entire organization and multiple platforms, as well as effectively derive meaningful insight from the activity to address security, compliance, and operational requirements. All file activity or specific activities of interest can be alerted, queried, or reported on, in addition to being fed to SIEM solutions through certified, direct integration with many of the market's leading providers including Splunk and QRadar.

THREAT DETECTION & VULNERABILITY MANAGEMENT

Threats to ITAR-related data can originate from rogue insiders or via vulnerabilities exploited by external attackers. STEALTHbits' behavioral analytics and proactive vulnerability assessment capabilities enable organizations to pinpoint areas of risk and eliminate excessive and undifferentiated warnings produced by native logs and other third-party solutions to surface truly meaningful trends and alerts on attempts to compromise sensitive data.

PEOPLE & PROCESS

The most essential piece of being ITAR compliant is having the right people and processes in place. Along with tools to discover and classify your data, you must be able to write in new policies, regularly test security systems, and implement measures to prevent the loss of ITAR-controlled data.

STEALTHbits provides the tools your people need to achieve compliance with ITAR requirements, as well as automate many of the processes associated ITAR such as the generation of compliance artifacts and enforcement of security policies.

STEALTHbits
TECHNOLOGIES

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-OS-1017