DISA STIG BRIEFING

SDS MAINFRAME SECURITY

z/OS Security using DISA STIGs

STIGs provide the optimal configuration settings to 'lock down' IT systems and software

Cybersecurity is in the news every day. Large well-known organizations are being hacked by criminals and large amounts of customer data are being stolen. Although it is unusual for mainframe sites to report being attacked, it doesn't mean it can't or doesn't happen. So where does a mainframe-using organization turn to for information and help enhancing their mainframe security? The U.S. Department of Defense (DoD) – who better to protect your security?

Official STIGs come from DISA, a DoD Agency that sets Cybersecurity Standards

Part of the DoD is the Defense Information Systems Agency (DISA). One of the services DISA offers is IT and communications support to the government and associated defense agencies. And part of that is to create and maintain security standards for computer systems and networks that connect to the DoD. Cybersecurity methodologies for standardizing security protocols within networks, servers, computers, and logical designs to enhance overall security is a major focus.

These methodologies or guides, when implemented, enhance security for software, hardware, physical and logical architectures to further reduce vulnerabilities. In other words, they prevent malicious attacks by providing the information required to fortify security and fully protect information systems and software. These guides are called Security Technical Implementation Guides (STIGs).

STIGs help Prevent Unauthorized Access and Malicious Attacks

STIGs also describe maintenance processes such as software updates and vulnerability patching. Adhering to the STIG is the standard that many DoD organizations set for themselves. If an organization isn't STIG-compliant, they may be denied access to DoD networks.

STIGs cover two main areas – policy requirements for security programs, and best practices for Information Assurance (IA)-enabled applications. A STIG might describe maintenance processes such as software updates or vulnerability patching. Or it might be a set of configurations and checklists describing how to minimize network-based attacks and prevent unauthorized system access.

Mainframe STIG Example

The mainframe product must:

- Use multifactor authentication for local access to non-privileged accounts.
- Implement organization-defined automated security responses if baseline configurations are changed in an unauthorized manner.
- Produce audit records containing information to establish the outcome of the events.
- Use an external security manager for all account management functions.
- Notify system programmers and security administrators when accounts are modified.

How a DISA STIG is Defined

STIGs come in three risk categories, indicating how severe the risk if an identified weakness remains. Category I (Cat I) is the most severe level, where an exploited vulnerability would result in loss of confidentiality, availability, or integrity.

DISA STIG BRIEFING

Currently, there are over 400 STIGs supplied by DISA. Each one describes how a specific application, operating system, network device, or smartphone should be configured. Some apply to mainframes, others apply to PCs, while the latest STIGs look at configurations for cloud computing systems.

STIGs are updated and added to regularly. There are quarterly updates and major updates may happen at any time. DISA regularly tests and researches to find the most secure configurations, and solutions for any new vulnerabilities that are identified are included in the next edition of a STIG. Other updates that might be included correct errors, highlight policy changes, or simply clarify earlier statements. Updated STIGs are released by the DISA FSO (Field Security Operations).

Complying with STIGs is a Tedious and Manual Process

Organizations wishing to remain compliant need to monitor regularly for updated STIGs. In addition, from time to time, organizations will upgrade and/or replace their software and hardware, which can mean that the required settings need to be changed or overwritten. The STIG needs to be downloaded and then the configuration changes identified by the STIG can be made.

STIG History and Process Improvements for Distributed Platforms

STIGs were originally simply PDFs listing the settings and configurations that were required to be compliant, but mistakes were often made by people trying to use them. The PDFs were replaced by Gold Disks, which would scan an operating system or piece of software to make sure they were configured correctly.

These have mainly been replaced by SCAP (Security Content Automation Protocol), which was developed by the National Institute of Standards and Technology (NIST). SCAP is a benchmark protocol used widely in information assurance, with more accurate reporting of STIG compliance. Not all application STIGs have a SCAP-compliant benchmark associated with them yet; some SCAPs require a DoD PKI Certificate to work properly.

STIGs and SCAP Compliance

System administrators need to use a SCAP-compliant scanner (e.g., SCAP Content Checker). The required STIG (in SCAP format) can then be downloaded and loaded into the SCAP tool. It makes sense to scan all IT assets at least once a month to see whether any configurations have changed. The SCAP Content Checker reports on the level of your system's security. It's worth noting that not every STIG requirement can be implemented without it having an impact on the overall functionality of the IT system.

Although STIGs were originally created to ensure that organizations connecting to DoD networks were using the most secure settings possible, they can now be used by any organization wanting to improve its security.

SDS Mainframe Security Software

SDS Mainframe Security solutions can be deployed in conjunction with STIGs to fill existing security gaps and make complying with data regulations much easier. Securing FTP, encrypting data at rest, and automating the STIG process are a few important tasks completed by SDS Mainframe Security tools.

About SDS

Founded in 1982, SDS supports over 25 mainframe products. SDS licenses hundreds of enterprise clients worldwide with quality mainframe software and offers award-winning technical support. SDS solutions focus on mainframe security, encryption, data compression, and network monitoring. To learn more, please visit www.sdsusa.com.