Cybersecurity Guidance Resources

Instructor: With the ever-changing cyber landscape, and new vulnerabilities discovered regularly, several guidance initiatives are supported to aid in securing cyber environments. There are suggested best practices, as well as directives that organizations may be required to adhere to for compliance purposes.

With the goal of improving defenses and thwarting cyberattacks, the Center for Internet Security maintains a list of security controls and detailed best practices for computer security.

Formally known as the Consensus Audit Guidelines and drafted by over 100 contributors from government agencies and commercial experts, 20 Critical Security controls are categorized 1-6 as Basic, 7-16 as Foundational, and 17-20 and organizational. The Center for Internet Security also offers guidance on applying the controls based on an organization's available resources and expertise, called implementation groups. There are several products that have incorporated CIS control and configuration guidance.

The federal government published guidance for securing systems; many agencies are required to adhere to, for devices connected to government networks.

Security Technical Implementation Guides, STIGs, are configuration standards for government systems. The STIG library maintained by the Defense Information Systems Agency, contains guidance for a plethora of operating systems and applications with details for their specific secure configuration settings. In addition, there are Security Requirements Guides, SRGs, which contain security recommendations for a technology versus a specific product. DISA works in coordination with other cybersecurity-focused agencies to draft STIG and SRG configuration guidance. Many government agencies are required to follow SRG/STIG guidance. There is a publicly available version of the library where any entity can leverage the valuable security guidance.

With hundreds of STIGs, each containing dozens or more controls; testing and validating can be cumbersome. To aid with implementing and verifying these security requirements, agencies use tools like the SCAP Compliance Checker SCC tool.

SCAP is the Security Content Automation Protocol; It has two main

parts, SCAP scanner and SCAP content. The scanner tool compares system configuration settings and patches against a standard or baseline and notes, or in some cases corrects, any deviations. SCAP content modules are secure configure baselines that can be used to compare to systems being scanned by SCAP tools.

The National Institute of Standards and Technology, NIST, manages the government repository of vulnerability management data to enable automation of compliance using scanning tools like SCAP. NIST Special Publication 800-126 defines SCAP requirements, component specifications, and characteristics of SCAP content.

NIST Special Publications are guidance and recommendation documents created in collaboration with industry experts detailing best practices; many of which federal agencies are required to follow. NIST also develops Federal Information Processing Standards (FIPS) documents that detail requirements for cybersecurity for federals systems.

The 800-series of the special publications includes guidelines, technical specifications, and reports related to the computer security. The 1800-series presents cybersecurity solutions for applying standards and best practices.

SP 800-53 is the recommended security and privacy controls for information systems and organizations. This publication has gone through revisions to ensure it provides the latest guidance on security controls designed to address threats and risks. The 800-53A publication details how to assess these controls.

NIST also maintains the National Checklist Program, a repository of publicly available secure-configuration resources. Per special publication 800-70, NIST manages an organized searchable resource that enables users to locate security guidance for platforms and applications, available in formats compatible with many compliance scanning tools.

There are many NIST special publications that entities can leverage to help with the security of their enterprise. The 800-series compiled information, results of collaboration with experts in the field, contains hundreds of publications from configuration management, to mobile security, trustworthy email, and many cryptography-related recommendations.

Secure configuration guidance is available from several trusted government agencies as well as application vendors.

Some organizations have specific industry-related compliance with regulation requirements. For

instance, healthcare and finance entities are required by law to protect consumer privacy and personal information. Security control and configuration guides specific to the protection of the data managed are available.

These resources detailing security controls and secure configuration settings have the common goal of addressing risks and potential vulnerabilities to information systems. Drafting of these guides, and the testing of the controls is a collaboration of industry experts. Implementing secure configuration best practice recommendations are a vital part of enterprise information security.

Notices