Everything You Wanted to Know about DISA STIGs but were Afraid to Ask

An EiQ Networks White Paper
Everything You Wanted to Know about DISA STIGs but were Afraid to Ask

Throughout this document, you’ll find a number of references to the U.S. Department of Defense (DoD) and Defense Information Systems Agency (DISA). As part of its mission to keep the infrastructure secure, DISA issues configuration standards known as Security Technical Implementation Guides (STIGs) that “contain technical guidance to ‘lock down’ information systems/software that might otherwise be vulnerable to a malicious computer attack.”¹

The STIGs specify how operating systems, applications, network devices, and other assets should be configured in order to be secure. For each asset type, the corresponding STIG contains a number of checks to determine if the current configuration meets DoD standards. For example, the Windows Server 2012 STIG contains several hundred checks to perform. It covers things like password settings, the granting of user rights, maintaining an audit trail, and much more. Each of the checks in the DISA STIG policy is also assigned a severity level as shown in the table below.

<table>
<thead>
<tr>
<th>Severity</th>
<th>DISA Category Code Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAT I</td>
<td>Any vulnerability, the exploitation of which will directly and immediately result in loss of Confidentiality, Availability, or Integrity.</td>
</tr>
<tr>
<td>CAT II</td>
<td>Any vulnerability, the exploitation of which has a potential to result in loss of Confidentiality, Availability, or Integrity.</td>
</tr>
<tr>
<td>CAT III</td>
<td>Any vulnerability, the existence of which degrades measures to protect against loss of Confidentiality, Availability, or Integrity.</td>
</tr>
</tbody>
</table>

Source: Windows Server 2012 STIG Overview, V1R5²

To audit a device, host, or application against the DISA STIG policies, a line-by-line assessment needs to be done for each of the required checks. This could be done manually by inspecting each applicable setting or registry key, or through the use of an automated configuration auditing tool such as EiQ Networks’ SecureVue® platform.
Why is configuration auditing so important?

The default settings of your routers, servers, and other IT assets were not necessarily designed with security in mind. Some vendors create defaults based on ease-of-deployment and other considerations. Other vendors may not have put much thought into the defaults at all. By using default vendor settings, you may be using weak configurations that can be exploited by even the most basic cyberattacks. The code for these attacks is readily available on the Internet and available to criminals, hostile nation-states, and so-called hacktivists.

Secondly, the threat environment is constantly changing. Even if you are diligent about configuring new systems properly, a configuration that was considered secure last year could be vulnerable to a newly discovered exploit today. In addition, each time there is a change to your assets, there is the potential to introduce new holes. Today's browser upgrade might contain a vulnerability that requires a patch tomorrow. DISA releases revisions to STIG policies on a quarterly basis. By continually auditing your IT assets against configuration standards like the DISA STIGs, you ensure that you are keeping up with the threat landscape.

Lastly, the configuration of devices, hosts, and applications may be the responsibility of a diverse set of teams and individuals within the organization. Change control and tracking can be a difficult task and might be outside the jurisdiction of your organization's IT Security personnel. By choosing a configuration standard and enforcing its use through configuration auditing, you can keep well-meaning colleagues from changing configurations in a way that weakens security and exposes your organization to costly threats.
What else do I need to know about DISA STIG auditing?

Adherence to the DISA STIG configuration standards is not optional for DoD organizations. DoD Instruction 8500.2 contains the requirements for Information Assurance (IA) Implementation and clearly references the STIGs as the authorized Configuration Specifications (Controls DCCS-1 and DCCS-2).  

A DoD reference document such as a security technical implementation guide or security recommendation guide constitutes the primary source for security configuration or implementation guidance for the deployment of newly acquired IA- and IA-enabled IT products that require use of the product’s IA capabilities.

(Note: A Security Recommendation Guide, or SRG, covers a broad technology category like “Firewalls,” and is used when a device-specific STIG is not available.)

DoDI 8500.2 assigns IA Managers and IA Officers the responsibility to implement and enforce IA policies. The career impacts of not meeting DoDi 8500.2 requirements are beyond the scope of this document.

Who else cares about configuration monitoring?

The security concerns that drive the need for configuration monitoring are not unique to the U.S. Department of Defense. The use of poorly or misconfigured systems can leave an open door for the unauthorized access and use of your organization’s data. This can have large and costly impacts even if you’re not storing secret plans for a new stealth fighter. Personally identifiable information (PII), health records, credit card numbers, and other sensitive information can be sold for big money on the black market. This type of data breach can result in regulatory fines, civil lawsuits, and loss of business.

As a result, a number of security frameworks such as PCI-DSS, HIPAA, and GLBA contain provisions for configuration monitoring and change control. For example, PCI Requirement 1 states that configuration standards are required for firewalls and routers in order to protect cardholder data. In addition, PCI Requirement 2 restricts the use of vendor-supplied defaults for important security parameters. These requirements can be met by implementing a process to regularly audit configurations against a known standard.

Another proponent of configuration auditing is the Council on Cybersecurity, which maintains a set of 20 Critical Security Controls (CSCs) for Effective Cyber Defense. The CSCs were developed by the SANS Institute to help organizations proactively improve security posture and reduce the risk of a data breach. CSC #3 calls for Secure Configurations for Hardware & Software on Laptops, Workstations, and Servers, while CSC #10 deals with Secure Configurations for Network Devices. Verizon’s 2014 Data Breach Investigation Report mapped security incident patterns to the CSC that could have prevented or mitigated the incidents. The authors found that Standard Configuration Controls would have a large impact across a wide range of industries, including Education, Finance, Manufacturing, and Professional Services.
How do I know which STIGs apply to my systems?

One of the biggest challenges facing IA Managers is how to determine which STIGs to apply to each of the devices and hosts on the network. The first step is to create an inventory of all systems and software. This is a good security practice anyway (Critical Security Controls #1 and #2) and gives you a good starting point to determine against which STIGs you will need to audit. Network mapping software may be of assistance when creating the inventory.

Unfortunately, tools like nmap will only give you basic information about each node. To do a thorough audit, you will need to gather more information about each individual node. Does the system have a Wireless LAN Controller? Is Oracle Database installed? What version of IIS is running? This can be a very tedious process that takes up a lot of the audit time.

The new SecureVue® STIG Profiler™ from EiQ Networks is a free tool designed to reduce this overhead cost of auditing by streamlining the system discovery and profiling process. The STIG Profiler automatically identifies IT assets and determines which DISA STIGs apply, based upon attributes such as installed software. The ability to do a detailed asset analysis in an automated fashion can save hundreds of hours spent every year on manual system profiling.

Free Download:  http://www.stigprofiler.com

About SecureVue

SecureVue from EiQ Networks is a continuous security intelligence platform that combines audit log management & SIEM capabilities with a powerful configuration auditing solution. By collecting a broad array of data elements, SecureVue can meet a number of the IA requirements in DoDI 8500.2 and NIST 800-53 at a fraction of the cost of acquiring multiple tools. SecureVue will automatically and continuously monitor devices against predefined configuration standards including DISA STIGs and CIS Benchmarks.

About EiQ Networks

EiQ Networks, a pioneer in security hybrid SaaS and continuous security intelligence solutions and services, is transforming how organizations identify threats, mitigate risks, and enable compliance. EiQ offers SOCVue, a security hybrid SaaS offering, and provides 24x7 security operations to Small to Medium enterprises who need to protect themselves against cyber attacks but lack resources or on-staff expertise to implement an effective security program. SecureVue®, a continuous security intelligence platform, helps organizations proactively detect incidents, implement security best practices, and receive timely and actionable intelligence along with remediation guidance. Through a single console, SecureVue enables a unified view of an organization’s entire IT infrastructure for continuous security monitoring, critical security control assessment, configuration auditing, and compliance automation.

For more information, visit:  http://www.eiqnetworks.com.

Notes:

6.  Verizon 2014 Data Breach Investigations Report, Figure 70