Center for Internet Security

Security Benchmarks Membership
New Member Promotional Discount

A 15% discount on all new Security Benchmarks Memberships

As part of CIS's effort in "Making best practice common practice," we are offering a promotional membership discount to align with National Cyber Security Awareness month in October. The discount is available through November 30, 2015.*

Experts agree that securing configurations is one of the most important actions an Enterprise must take to secure its data and systems. The CIS Critical Security Controls lists "Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers" as a specific and actionable way to thwart today's most pervasive attacks.

CIS is the industry recognized source for configuration content with over 100 published security baselines. Membership resources help companies compare and configure systems to recommended consensus-based settings. Membership benefits include:

- CIS Configuration Assessment Tool (CIS-CAT), a National Institute of Standards and Technology (NIST) certified SCAP 1.2 validated scanner
- CIS hardened virtual images in Amazon Web Services (AWS) EC2 environment
- Scripts to optimize workflows and automation
- Benchmarks in Word, Excel, and XML (XCCDF/OVAL) formats for customization
- Technical support

The Payment Card Industry Data Security Standard (PCI DSS) points to the Center for Internet Security Benchmarks for configuration standards.

Contact us today at SBPromo@cisecurity.org to enroll in this limited time offer or request a CIS-CAT trial. *For promotion terms, visit us at http://benchmarks.cisecurity.org/SB15Promo.

Center for Internet Security

CIS Security Benchmarks Resources

More Than 100 Benchmarks Covering 14 Technology Groups

http://benchmarks.cisecurity.org/downloads

Authentication Servers	• FreeRADIUS • MIT Kerberos[A]
Database Platforms	• IBM DB2 Server [A] • Microsoft SQL Server [A] • MySQL Database Server • Oracle Database Server [A] • Sybase Database Server [A]
Directory Servers	• Novell eDirectory • OpenLDAP Server
DNS Servers	• BIND DNS Server
Network Devices	• Checkpoint Firewall [A] • Cisco Firewall Devices [A] • Cisco Routers/Switches [A] • Juniper Routers/Switches • Agnostic Print Devices • Agnostic Wireless Devices
Mail Servers	• Microsoft Exchange
Mobile Platforms	• Apple Mobile Platform [R] • Google Mobile Platform
Productivity Software	• Microsoft Office[A R]
Virtualization Platforms	• VMware Server [A] • Xen Server • Agnostic VM Server
Web Browsers	• Apple Safari Browser • Microsoft Internet Explorer [A R] • Mozilla Firefox Browser [A] • Opera Browser
Web Servers	• Apache HTTP Server • Apache Tomcat Server [A] • Microsoft IIS Server[A]
Operating Systems: Desktop	• Apple Desktop [A] • Microsoft Windows Desktop [A R]
Operating Systems: Servers	• Amazon Linux[A R] • CentOS[A R] • Debian Linux Server [A] • FreeBSD Server • HP-UX Server [A R] • IBM AIX Server [A R] • Microsoft Windows Server [A R] • Novell Netware • Oracle Linux[A] • Oracle Solaris Server [A] • Red Hat Linux Server [A R] • Slackware Linux Server [A] • SUSE Linux Server [A R] • Ubuntu LTS Server[A R]
Collaboration Servers	• Microsoft SharePoint Server

Member Only Resources

Fully Supported - Saves you time and Money

Learn More http://benchmarks.cisecurity.org/tools

Assessment Tools

- **CIS Configuration Assessment Tool (CIS-CAT)**
  - Quickly identify security issues in your environment.
  - Routinely assess the configuration of production systems compared to over 50 CIS Benchmarks and internal security policies
  - Dashboard provides visual overall, device, or technology group of benchmark performance over time
  - Vulnerability Assessment (Windows & RHEL)
  - SCAP Validated as an Authenticated Configuration Scanner - SCAP 1.2 Compliant
- **Router Assessment Tool (RAT)**
  - Automatically identify security-related configuration issues in your network infrastructure
  - Coverage for Cisco ASA, and Cisco Pix

Remediation Content

- Quickly implement CIS security recommendations using CIS's automated remediation tools for:
  - Microsoft Windows 7, 8, & 8.1
  - Microsoft Windows Server 2003, 2008, 2008 R2, 2012 & 2012 R2
  - Microsoft Windows XP
  - Microsoft Outlook 2010,
  - Microsoft Office 2013, Access 2013, Excel 2013, Outlook 2013, Word 2013, Powerpoint 2013
  - Microsoft Internet Explorer 9, 10 & 11
  - IBM AIX 5.3-6.1 & 7.1
  - Red Hat Enterprise Linux 6
  - CentOS Linux 6
  - HP-UX
- Use CIS-Hardened Virtual Images in the Amazon Web Services Elastic Compute Cloud. AMIs are configured according to the following applicable CIS Security Benchmarks
  - Amazon Linux 2014.09 -2015.03
  - Microsoft Windows Server 2008 R2 & 2012 R2
  - Red Hat Enterprise Linux 5, 6 & 7
  - Suse Linux Enterprise Server 11 & 12
  - CentOS Linux 6 & 7
  - Ubuntu 12.04 & 14.04 LTS Server

Contact us for more information at members@cisecurity.org
Or visit http://benchmarks.cisecurity.org

31 Tech Valley Drive - East Greenbush, NY 12061 - 518.266.3460 - www.cisecurity.org

CIS CONFIGURATION ASSESSMENT TOOL (CIS-CAT)

Description

CIS-CAT is a configuration assessment/audit software tool available to CIS Members only. Written in Java, CIS-CAT: (a) reads those CIS Security Benchmarks that are expressed in XCCDF (XML) format; (b) reports the configuration status of a target system as compared to the technical controls defined in those CIS Benchmarks; (c) provides a comparative score based on a conformity scale of 0-100; and (d) features Report Aggregation (a CIS-CAT Dashboard).

CIS-CAT is SCAP Validated as an Authenticated Configuration Scanner! For more information on this, please see http://nvd.nist.gov/scap/validation/127.cfm and the CIS-CAT User's Guide.

CIS-CAT consumes XML representations of various CIS Benchmarks. The XML schemas used to express CIS benchmarks are XCCDF, OVAL, and ECL. The XCCDF schema is used to describe and group configuration states while OVAL and ECL are used to define how to test a system's conformance with the configuration state described in XCCDF. All CIS Benchmarks that are expressed in XML are expressed in XCCDF+ECL and/or XCCDF+OVAL. Vulnerability assessment capabilities available for Microsoft Windows Desktops and Servers, SUSE and Red Hat Enterprise Linux

For information on OVAL, please see http://oval.mitre.org/
For information on XCCDF, please see http://scap.nist.gov/specifications/xccdf/

System Requirements

CIS-CAT requires JRE v1.6 or later. The tool and the JRE can reside on the target system of evaluation or on a removable or network drive, provided it is accessible from the target of evaluation.

Distributed in both CLI and GUI versions, CIS-CAT is a host based (not a network or enterprise scanner) and scan only (doesn't change configuration settings) tool. CIS provides supplemental scripts that support CIS-CAT in assessing multiple systems simultaneously.

Platform Support

CIS-CAT can read customized input files, so members can compare the configuration of their systems with both the CIS benchmarks and their customized configuration policies. This feature is enabled by user modification of the Benchmark XCCDF files.

CIS-CAT reads: (a) Over 60 CIS Benchmarks currently available in XCCDF); (b) XCCDF configuration files distributed by NIST for Microsoft Win XP and Vista, and (c) user-modified CIS Benchmark XCCDF files. CIS distributes CIS-CAT with production version support for the following benchmarks (* denotes OVAL coverage)

- Amazon Linux 2014.09-2015.03*
- Apache Tomcat 5.5-6.0
- Apple OSX 10.5
- Apple OSX 10.6
- Apple OSX 10.8
- Apple OSX 10.9
- Apple OSX 10.10
- Cisco IOS 15 v4.0.0*
- CentOS Linux 6 *
- CentOS Linux 7 *
- Debian Linux
- HP-UX 11i
- IBM AIX 4.3-5.1
- IBM AIX 5.3-6.1
- IBM AIX 7.1
- Microsoft Internet Explorer 10*
- Microsoft Internet Explorer 11*
- Microsoft IIS 7/7.5*
- Microsoft IIS 8/8.5*
- Microsoft Office 2013*
- Microsoft Access 2014*
- Microsoft Outlook 2013*
- Microsoft Powerpoint 2013*
- Microsoft Word 2013*
- Microsoft Excel 2013*
- Microsoft SQL Server 2008 R2*
- Microsoft SQL Server 2012*
- Microsoft SQL Server 2014*
- Microsoft Windows XP*
- Microsoft Windows 7*
- Microsoft Windows 8
- Microsoft Windows 8.1*
- Microsoft Windows 2003 MS DC*
- Microsoft Windows 2008 Server*
- Microsoft Windows 2008 R2 Server*
- Microsoft Windows 2012 Server*
- Microsoft Windows 2012 R2 Server*
- MIT Kerberos KDC 1.10*
- Mozilla Firefox 3
- Mozilla Firefox ESR 24*
- Oracle Database 9i-10g
- Oracle Database 11g
- Oracle Database 11g R2*
- Oracle Database 12c*
- Oracle Linux 7*
- Oracle MySQL Community Server 5.6*
- Oracle MySQL Enterprise Edition 5.6*
- Oracle Solaris 2.5.1-9
- Oracle Solaris 10 v5.1.0
- Oracle Solaris 11
- Oracle Solaris 11.1
- Red Hat Enterprise Linux 4 v1.0.5
- Red Hat Enterprise Linux 5 v2.2.0*
- Red Hat Enterprise Linux 6 v1.4.0*
- Red Hat Enterprise Linux 7*
- Slackware Linux 10.2
- SUSE Linux Enterprise Server 9
- SUSE Linux Enterprise Server 10
- SUSE Linux Enterprise Server 11*
- SUSE Linux Enterprise Server 12*
- Ubuntu 12.04 LTS Server
- Ubuntu 14.04 LTS Server
- VMware ESX 3.5
- VMware ESX 4.1
- VMware ESXi 5.5*

Download Files & User Support

Members can download the CIS-CAT bundle from the community site downloads.
Additional guidance and support is provided to members via the member discussions, tutorials and support by CIS staff.
To learn more about membership or obtain a trial use of the CIS-CAT Tool contact us at members@cisecurity.org.