International Journal of Computer Trends and Technology
ISSN: 2231 – 2803 / https://doi.org/10.14445/22312803/IJCTT-V70I7P101

Volume 70 Issue 7, 1-7, July 2022
© 2022 Seventh Sense Research Group®

Original Article

A Case Study to Implement Windows System Hardening using CIS Controls

Rajeshkumar Sasidharan

Systems Engineering, Light & Wonder, Illinois, Chicago, USA.

Received: 12 May 2022 Revised: 30 June 2022 Accepted: 06 July 2022 Published: 21 July 2022

***Abstract* - *Cyber threats and attacks increasingly target today's IT infrastructure worldwide. Organizations are constantly pressured to secure their infrastructure, data, and services from external attacks. As a result, security and systems engineers continually focus on securing their infrastructure from the edge level (firewall, router, and switches) to the end-user component (server, systems, and storage) level using various security technologies, including system hardening at the component level. This case study focuses on hardening Windows systems with industry-standard Center for Internet Security (CIS) controls, security tools, a remediation tool kit, and frameworks. It helps to safeguard Windows servers from external and internal threats and provides comfort to the information technology and security teams in evaluating and maintaining the IT infrastructure's security baseline. Finally, this case study assists the client in safely and securely running thousands of Windows servers worldwide and generating security reports against the vulnerability and security baseline established by CIS Benchmarks and Controls. Applying any controls or adjustments to the new implementation would be simpler. However, the focus of this case study was on implementing CIS Windows system hardening on existing complex production Windows infrastructure, which is usually a difficult issue for chief information security officer (CISO) and chief information officer (CIO) organizations.*

Keywords* – *Operating system auditing, Compliance, CIS benchmarks, Vulnerability, Windows security.

1. Introduction

Our client is a large corporation with a global presence and an infrastructure of around 5000 Windows servers. The purpose of Windows hardening is to assist in closing undesirable ports, disabling unnecessary services, and managing user access control. Client security scanning software already scans the Windows infrastructure. It gives a vulnerability report, but the repair is difficult owing to the lack of centralized administration of hardening policies and benchmarks. Furthermore, without suitable hardening controls, tools, and benchmarks, adopting, maintaining, and monitoring Windows system hardening rules and duties are difficult.

In this case study, we use the Center for Internet Security (CIS) SecureSuite of tools and technologies to establish a simple methodology, processes, and stages to implement industry-standard CIS hardening controls and benchmarks on the current Windows infrastructure. The purpose is to easily deploy Windows system hardening on existing infrastructure, manage hardening controls and benchmarks centrally, and easily alter and apply them while handling the security audit and compliance procedure with ease and confidence.

2. Overview of CIS Controls and Components

2.1. CIS Secure Suite

CIS SecureSuite Membership provides scalable, customizable tools and resources to suit different organizations' needs. Members can assess endpoint configurations, measure compliance to the CIS Benchmarks, and conduct, track, and assess their implementation of the CIS Critical Security Controls (CIS Controls) quickly and effectively.[1]

2.2. CIS Controls

CIS Controls^{TM} is a prioritized set of actions that comprise a defense-in-depth set of best practices that mitigate the most prevalent threats against systems and networks. CIS Controls are created by a group of IT specialists who use their first-hand experience as cyber defenders to produce these widely recognized security best practices. The CIS Controls' specialists come from various industries, including retail, manufacturing, healthcare, education, government, and defense.[2]

Each of the 20 CIS Controls is further broken into sub-controls, for a total of 171 sub-controls. The 20 controls are classified as i) basic, ii) foundational, and iii) organizational. Because the number of sub-controls is relatively high and it is difficult to expect them to be suitable for everyone, implementation groups, three in all, were established beginning with version 7 of the CIS Controls specification. Small businesses adopt only Implementation Group 1, whereas the larger businesses implement all three implementation groups.[3]

2.3. CIS Benchmarks

CIS Benchmarks are recommended practices for securing a target system's configuration. CIS Benchmarks are available for over 100 CIS Benchmarks spanning 25+ vendor product families. They are established through a unique consensus-based approach comprising cybersecurity professionals and subject matter experts worldwide. The CIS Benchmarks are the only consensus-based, best-practice security configuration guides produced and endorsed by the government, business, industry, and academia. [4]

2.4. CIS Build Kits

The Build Kits are intended to cover the vast majority of benchmark settings. CIS provides Build Kits for specific technologies to aid in the automation of system hardening. Build Kits are Group Policy Objects (GPOs) for Windows technologies and basic shell scripts for Linux and Unix.[5]

2.5. CIS Dashboard Server

The CIS-CAT (Configuration Assessment Tool) Pro Dashboard automatically allows the import of assessment results from the CIS-CAT Pro Assessor. There are several ways to arrange the interaction of the CIS-CAT Pro Assessor and CIS-CAT Pro Dashboard to allow assessment results to be uploaded to the CIS-CAT Pro Dashboard database. From CIS-CAT Pro Assessor v3 and v4, results in reports from a single CIS-CAT assessment can be uploaded (using either the graphical user interface in v3 or the command-line user interface in v3 or v4). Additionally, customers scanning multiple Windows or Unix/Linux targets with the "centralized" technique in v3 or v4 can automatically alter the supporting files to submit the results to the CIS-CAT Pro Dashboard. Because the CIS-CAT Pro Dashboard is a java-based program, it requires a compatible java runtime environment (JRE). Versions of OpenJDK are also supported.[6]

2.6. CIS Assessor Server

The CIS-CAT Pro Assessor saves users hours of configuration review by scanning against a target system's configuration settings and reporting the system's compliance to the corresponding CIS Benchmark.[1] CIS-CAT Pro Assessor java application files in Assessor Server can be shared by the Assessor Server with a Windows client through SMB and then executed from the local machine through Assessor Command Line Interface (CLI). Utilizing the CIS-CAT Pro Assessor CLI, users can perform host- and remote-based (local) assessments.[7]

2.7. CIS Dashboard Web Server

Apache Tomcat is primarily used to run an application server and an Apache web server to proxy the Tomcat instance and respond to traffic on port 80/443.[8]

2.8. CIS Dashboard DB Server

MySQL Database Server should be installed to store user and CIS Assessment details. MySQL client in the Dashboard Server should be installed to test database connectivity and develop the schema for the CIS-CAT Pro Dashboard.[9]

3. Problem Statement

Our client uses basic Windows hardening controls in their Windows domain for thousands of servers. Moreover, there is no centralized reporting, and management and monitoring facilities against Windows security and vulnerabilities are missing. Our client runs mission- and business-critical applications and services on the Windows domain. Modifying the existing Windows hardening or applying highly secured hardening CIS Controls may prevent their applications from working or make them inaccessible without proper testing. Applying the CIS Controls User Access Controls may affect the existing user access or behavior. These issues are always fears of IT and security organizations applying highly secured hardening controls to existing Windows servers. In summary, CIS hardening controls need to be tested properly in the test setup, and IT and security departments and their leads must be convinced of their usefulness. Server end users and owners must be educated and confident.

4. Requirement Analysis and Decision

We discussed CIS Remediation and Benchmark benefits with the client organization security and IT head and obtained their professional opinion and suggestions concerning the infrastructure and organization policy. We were carefully instructed not to undertake any operations in the production environment until they had been thoroughly tested in the test environment. We had received consent from the IT and database administrators, application developers and users, and end users.

First, we agreed to implement the CIS test on the test setup and showed the IT and security heads the Assessment, Remediation, and Vulnerability results. Based on the results, they agreed to proceed with the real user acceptance test (UAT) in the test infrastructure with the support of stakeholders.

4.1. Test/UAT High-level Plan

a. Implement CIS Remediation and Benchmark on only two servers and get agreement from sponsors.
b. Implement CIS Remediation and Benchmark on all test servers and get agreement from application/Database/IT administrators.

5. Solution Design

5.1. UAT & Test Setup Architecture

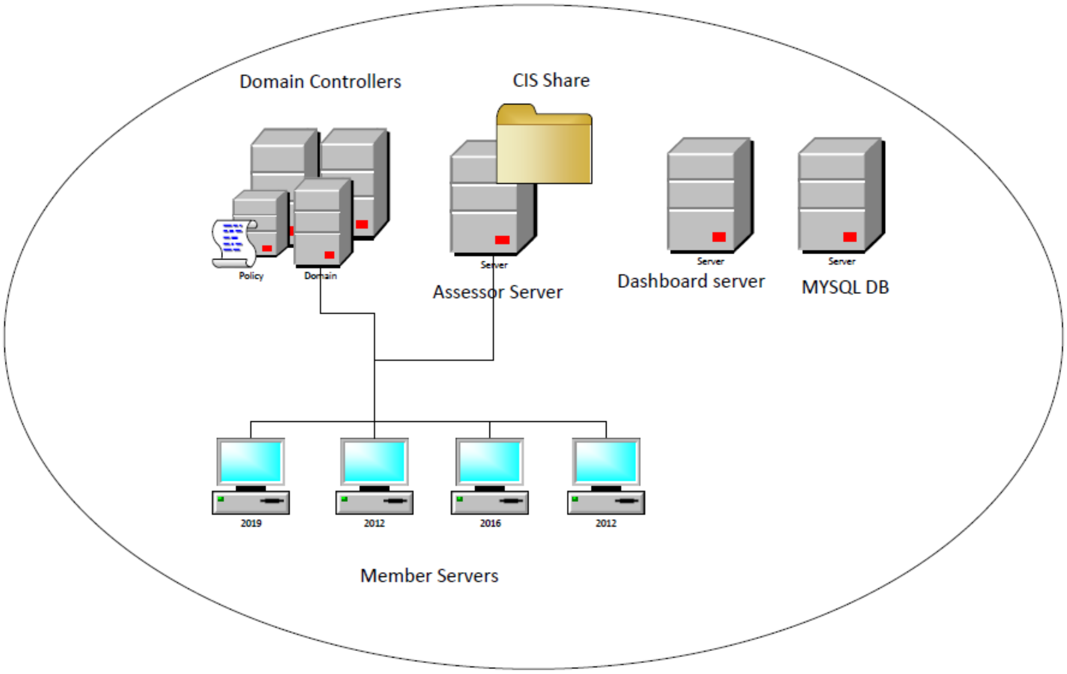


Fig. 1 Test setup architecture diagram

Table 1. Details of test domain servers.

S. No	Function	OS Version	Comments
1	DC01	2019	Domain Controller
2	DC02	2019	Domain Controller
3	2016 Client	2016	Member Server
4	2019 Client	2019	Member Server
5	DFS Server	2019	File Server
6	SQL Server	2019	SQL Database Server
7	Windows IIS (Internet Information Server) + MySQL	2019	Web & Database Server
8	2012 Client	2012	Member Server

Table 2. CIS components were used.

Component	Version
CIS-CAT Pro Dashboard	v4.0.0
CIS-CAT Pro Assessor	v4
Tomcat	Latest stable version
Apache Web Server	Latest stable version
Java - JRE	1.8.0_202
MySQL	Latest stable version
CIS Controls Version	6.1 / 7.0

5.2. Test Setup Implementation

We have created a test Windows Active Directory domain cistest local for implementing CIS secure hardening. There are two Domain Controllers, the Assessor Server, the Dashboard Server, the MySQL DB Server, and multiple member servers for running different versions of the Windows operating system.

CIS Controls are applied through Group Policy Management from Domain Controllers to all member servers, including Domain Controllers.

- CIS SecureSuite Membership from cisecurity.org is required to proceed with the below activities.
- Download and install the CIS-CAT-Pro-Assessor file in the Assessor Server from the Cisecure.org website and share the “CIS share” folder with member servers as mentioned in the above test architecture (Fig. 1).
- Update the cis-cat-centralized-ccpd.bat file for the centralized Windows implementation option.
- Set the authentication token value parameter “AUTHENTICATION_TOKEN='<Generate_An_Authentication_Token_In_CCPD>' to the one generated from the CIS-CAT Pro Dashboard.

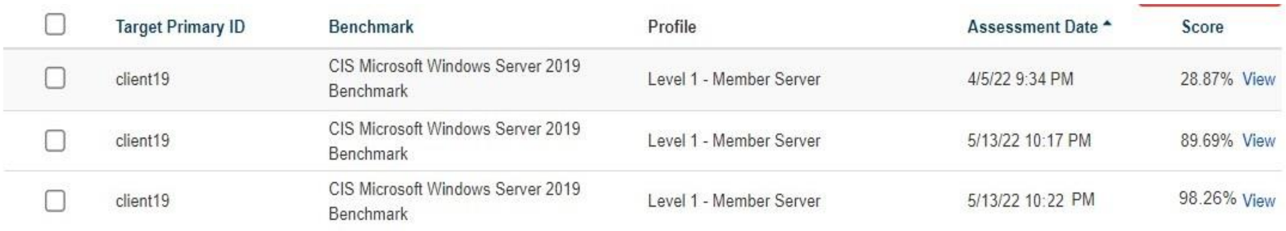
After completing the above steps, navigate to one of the Windows members and use the following command to map the share:

```
net use Z: \\Assessor-Server\CIS-Share
set JAVA_HOME=Z:\Java64\jre1.8.0_202
```

Z:\>cis-cat-centralized-ccpd. bat (Command to assess the member server and upload the result to the CIS Dashboard Server).

Import the downloaded Windows Build Kit (Group Policy files) from the Cisecure.org member website into the Domain Controller using GPMC.MSC.

Before we applied the CIS security settings to the member server, we assessed the server using the CIS Assessor and uploaded the result into the CIS Dashboard. First, we applied the CIS Benchmark setting to one of the member clients (2019 client) through GPMC.MSC and did some basic testing on that member. Then, we ran the Assessor result by running cis-cat-centralized-ccpd.bat from the Assessor Server share and uploading the data into the CIS Dashboard, as mentioned above. The results were shocking: without applying the CIS Benchmark settings, the value was “28.87,” and after applying CIS Remediation, it was “89.69,” indicating a great improvement. We disabled multiple controls in the CIS Group Policy during the initial test, so we got “89.69,” but after those settings were re-enabled, it reached 98.26% (see Figure 2 below).



☐	Target Primary ID	Benchmark	Profile	Assessment Date ▲	Score
☐	client19	CIS Microsoft Windows Server 2019 Benchmark	Level 1 - Member Server	4/5/22 9:34 PM	28.87% View
☐	client19	CIS Microsoft Windows Server 2019 Benchmark	Level 1 - Member Server	5/13/22 10:17 PM	89.69% View
☐	client19	CIS Microsoft Windows Server 2019 Benchmark	Level 1 - Member Server	5/13/22 10:22 PM	98.26% View

Fig. 2 Pre-test CIS report

We asked to proceed with the Test/UAT phase based on the above result. We identified the project team for the test phase and created and shared the table below with all stakeholders based on sponsor approval.

Table 3. Stakeholder details

Project Team	**Roles**
Sponsor	Information Security Head (CISO) / Information Technology Head (CIO) / IT Director
Project Implementation Team	CIS–Subject Matter Expert (SME) / GPO Administrator
Customers & Users (Location Wise)	IT Manager, IT Administrators, Engineers, Application Developers/Users, Database Administrators, and End Users

Table 4. Test/UAT phase details

Phase	Activity	Roles
UAT and Test Phase 1	Apply CIS Controls in DB, App, DFS, Web, and DCs of the test setup	CIS-SME / GPO Administrator
	Apply CIS Remediation	CIS-SME / GPO Administrator
	Test UAT & test setup and certify	Customers & Users
UAT and Test Phase 2	Address Phase 1 issues and reapply CIS Remediation	CIS-SME / GPO Administrator
	Test UAT & test setup and certify	Customers & Users
UAT and Test Phase 3	Address Phase 2 issues and reapply CIS Remediation	CIS-SME / GPO Administrator
	Test UAT & test setup and certify	Customers & Users
	Create a golden image of CIS Controls	
Reports	Assess CIS reports using Assessor Server and share and upload to CIS-Dashboard	CIS-SME
	Generate reports from CIS-Dashboard for all test setup servers.	CIS-SME

5.3. Production Implementation

Using the CIS test implementation reports, all project stakeholders mentioned in Table 3.0 (Stakeholder details) were convinced and agreed to proceed with production implementation. Thus, we raised a Change Request for the CIS production setup implementation activity, starting from development and UAT and going from less critical servers to highly critical servers.

5.3.1. Architecture Diagram for Production Setup

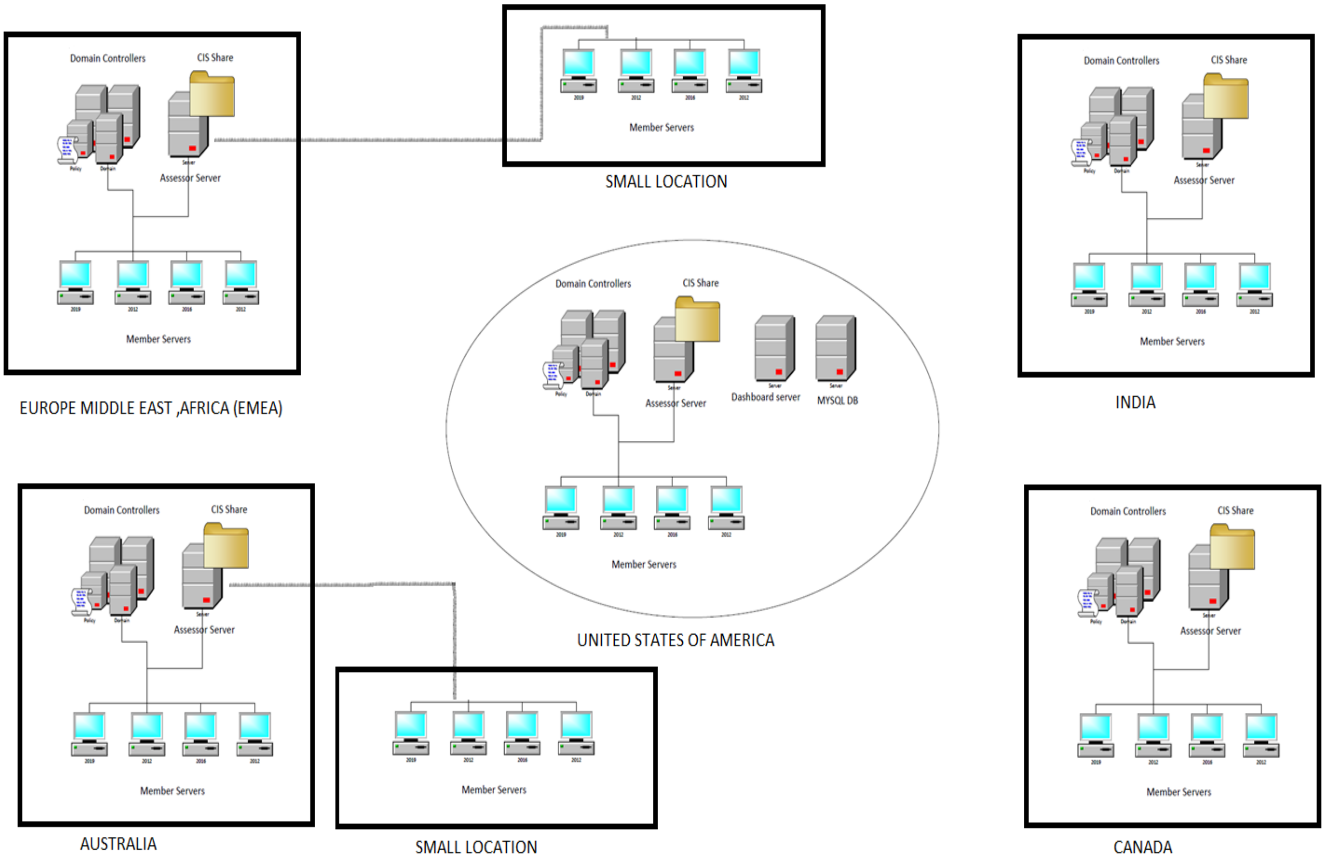


Fig. 3 CIS production implementation architecture

Similar to the Test/UAT architecture, the production setup was implemented in an office in the USA, which is the primary location for our client, and the CIS-Dashboard Server, Assessor Server, and MySQL Database server were implemented. All CIS Controls tested in the Test/UAT setup were imported in the production Domain Controller GPOs, so they were replicated to all Domain Controller locations. We applied CIS Controls GPOs to their respective OU or Windows servers during the activity.

The rest of the larger locations had an Assessor Server with a shared folder for local clients to mount and assess the CIS Controls applied and updated the results to the Central Dashboard Server. Smaller locations assessed the CIS Controls using a nearby larger location's Assessor Server and uploaded the results to the Central Dashboard Server.

5.4. Production Phases and Implementation Details

- Implement CIS Remediation and Benchmark in production setup on less critical servers like development and UAT in small locations.
- Implement CIS Remediation and Benchmark in production setup on critical servers in small locations.
- Implement CIS Remediation and Benchmark in production setup on less critical servers like development and UAT in large locations.
- Implement CIS Remediation and Benchmark in production setup on critical servers in large locations.
- Repeat the above steps until all the locations (globally) in the client organization are complete.

6. Reports

All the reports below fulfill the requirements of management, engineers, the information security team, and auditors.

- Remediation Report: The Remediation Report shows all the recommendations in the CIS Benchmarks that failed during the assessment. It is designed to give operators all the Remediation steps in an easy-to-read format.
- Complete Report: The Complete Report shows all the CIS Benchmarks' recommendations, and the overall pass/fail result. It is designed to give auditors a complete picture of a target system's latest assessment results.
- Assessment Results List: The Assessment Results List shows all assessed servers with details of the profiles, assessment dates, and scores.
- Job Status Report: The Job Status Report shows the status of all jobs (i.e., in-progress, error, and assessment completed). It helps administrators to rerun error status jobs and wait and watch in-progress status jobs to ensure the necessary activities are completed.

7. Results Summary

After applying CIS Controls in the existing infrastructure using the CIS Dashboard, Assessor, Benchmarks, and Build Kits, it is very easy to manage and monitor all the servers in a single pane of glass dashboard web interface. The details of the reports produced by the CIS Dashboard are used for auditing and compliance processes. Some auditors or security firms use CIS Controls to perform security audits (Washington State Auditor's Office uses CIS Controls to perform effective security audits).[10] These CIS tools from CIS SecureSuite Membership allow organizations to download CIS Benchmarks in machine-readable formats, including XML. It helps analyze endpoints against the CIS Benchmarks for conformance, which is a huge time-saver.[11]

8. Conclusion

The newly implemented CIS Controls hardening can give comfort and confidence to IT and security management, engineers, and end users. The above case study and method can help users to implement CIS Controls in existing and complex production environments across the globe. The Test/UAT setup can facilitate the implementation of new CIS Controls and the testing for existing control issues in the production setup. Companies can show the reports available in the CIS Dashboard as evidence during audits for compliance certification. Moreover, the hardening helps to protect the Windows environment from internal and external threats. Due to the above implementation's success, we plan to apply CIS Controls to Linux operating systems and network devices and appliances in the near future.

References

[1] The Cisecurity website, 2022. [Online]. Available: https://www.cisecurity.org/cis_securesuite

[2] The Cisecurity website, 2022. [Online]. Available: https://www.cisecurity.org/controls/v7

[3] S. Gros, "A Critical View on CIS Controls," *in Proc. 16th Int. Conf. Telecommun. ConTEL 2021*, pp. 122–128, 2021.

[4] The Cisecurity website, 2022. [Online]. Available: https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-faq

[5] The Cisecurity website, 2022. [Online]. Available: https://www.cisecurity.org/cis-securesuite/cis-securesuite-build-kit-content/build-kits-faq

[6] The Cisecurity website, 2022. [Online]. Available: https://ccpa-docs.readthedocs.io/en/latest/Configuration%20Guide/#cis-cat-pro-dashboard-integration

[7] The Cisecurity website, 2022. [Online]. Available: https://www.cisecurity.org/insights/blog/remote-assessment-comes-to-cis-cat-pro-v4

[8] R. McCool, 1995. Apache HTTP Server. [Computer software]. Available: https://httpd.apache.org/docs/

[9] J. Letkowski, "Doing Database Design with MySQL," *J. Technol. Res.*, vol. 6, pp. 1, 2015.

[10] The Cisecurity website, 2022. [Online]. Available: https://www.cisecurity.org/insights/case-study/washington-state-auditors-office-uses-cis-controls-to-perform-effective-security-audits

[11] The Cisecurity website, 2022. [Online]. Available: https://www.cisecurity.org/insights/case-study/bank-relies-on-industry-recommended-cybersecurity-best-practices

[12] The Cisecurity website, 2020. [Online]. Available: https://www.cisecurity.org/insights/white-papers/2020-nationwide-cybersecurity-review

[13] A. Echeverría, C. Cevallos, I. Ortiz-Garces, and R. O. Andrade, "Cybersecurity Model Based on Hardening for Secure Internet of Things Implementation," *Appl. Sci*., vol. 11, no. 7, p. 3260, 2021.

[14] The Cisecurity website, 2020. [Online]. Available: https://www.cisecurity.org/insights/case-study/tackling-audits-and-cloud-security-efficiently-and-at-scale

[15] The Cisecurity website, 2019. [Online]. Available: https://www.cisecurity.org/insights/case-study/cis-hardened-images-help-anitian-automate-fedramp-compliance

[16] The Cisecurity website, 2018. [Online]. Available: https://www.cisecurity.org/insights/case-study/infralert-uses-the-cis-controls-for-remediation-and-planning

[17] The Cisecurity website, 2018. [Online]. Available: https://www.cisecurity.org/insights/case-study/oklahoma-city-and-the-cis-controls

[18] The Cisecurity website, 2018. [Online]. Available: https://www.cisecurity.org/insights/case-study/cis-controls-inspire-law-graduate

[19] The Rapid7 website, 2022. [Online]. Available: https://www.rapid7.com/fundamentals/cis-critical-security-controls/

[20] The Netwrix website, 2022. [Online]. Available: https://blog.netwrix.com/category/cybersecurity-standards/

[21] The Cybersaint website, 2022. [Online]. Available: https://www.cybersaint.io/blog/cis-controls-list

[22] The UC Berkely website, 2022. [Online]. Available: https://security.berkeley.edu/education-awareness/center-internet-security

[23] The Microsoft website, 2022. [Online]. Available: https://docs.microsoft.com/en-us/compliance/regulatory/offering-cis-benchmark

[24] The Amazon website, 2022. [Online]. Available: https://docs.aws.amazon.com/inspector/v1/userguide/inspector_cis.html

[25] The Tripwire website, 2022. [Online]. Available: https://www.tripwire.com/state-of-security/controls/center-for-internet-security-cis-controls-v8-your-complete-guide-to-the-top-18/

[26] The Diligent website, 2020. [Online]. Available: https://www.diligent.com/insights/compliance/what-is-cis-compliance/

[27] The Cisecurity website, 2022. [Online]. Available: https://www.cisecurity.org/cis-benchmarks/#microsoft_windows_server