Xylok
Cyber Testing Simplified

Baking RMF into a Security Assessment with Xylok Scanner

Kevin A. Pridgeon | Xylok Cyber Champion

11 December 2018

Xylok
Cyber Testing Simplified

TABLE OF CONTENTS

INTRODUCTION

The Department of Defense's (DoD) new implementation of the Risk Management Framework (RMF) is intended to provide a common language to discuss the security posture and manage the cybersecurity risk within an organization. This new framework leads to a more protected system, but at a cost for resources and money. The ultimate goal is to protect DoD systems from attack and denial of use.

Utilizing the Defense Information Systems Agency's (DISA) Security Technical Implementation Guides (STIG) and Security Requirement Guides (SRG) allows an organization an easy way to check the technical controls on a system. The STIGs contain automated and manual checks that examine the configuration of a system and allow for comparison against the DoD configuration standards. With the STIGs, an organization is also able to "lock down" their system to protect against a computer attack. For more generic systems or for systems where no STIG exists, DISA provides the SRGs that allow an organization to tailor what they are checking against the baseline that DISA defines. SRGs require the organization to build their own automated and manual checks to evaluate their system.

The DoD RMF also requires an organization to evaluate their processes and documentation. These non-technical checks are intended to ensure that an organization is not only protecting their system through technical means, but also creating an environment where people know what to do in a given situation. This means that organizations need to define and document actions to execute in given certain situations. These actions include everything from defining how equipment is acquired to how and when security assessments are conducted.

DISA Control Correlation Identifiers (CCI) are a bridge from the high-level policy down to the actionable statements of how to implement a control. CCIs can be covered through technical STIGs or through documentation or processes. The CCIs can be rolled back up into the overarching National Institute of Standards and Technology's (NIST) 800-53 controls to simplify the verification of a system's overall security posture. The NIST Special Publication 800-53 provide the steps in RMF that cover the control selection that apply to a system. By selecting the controls that apply to a system, an organization is able to determine exactly what technical and manual checks would need to be accomplished.

Using RMF, an organization is required to do both an initial assessment to determine their baseline security posture and they are required to continuously monitor and update that security posture. The intent of continuously monitoring is to make sure a system is adequately protected against new and emerging technical threats and constantly evaluating the processes an organization utilizes to keep their people aware, trained, and reacting to real-world threats that exist and that are developed.

RMF allows for the DoD to evaluate systems for their security posture without having to develop unique criteria for widely disparate systems. The DoD is able to assess the security posture of a space system and the security posture of an F-35, which may be conducted in completely different manners, but report the findings in a unified manner that is consistent and repeatable.

BACKGROUND

The major problem that exists with DoD's implementation of RMF is the time and resources required to achieve the desired end state of continuously monitoring and evaluating a system. The method for most organizations is to utilize the same tools that were used before RMF and hire more people to cover down on the limitations of those tools.

The limitations of the tools ranges from not automating as many as possible of the required checks to not outputting the information collected in a standard format with the RMF information included. With the tools not automating as many of the technical checks as possible, organizations are hiring cybersecurity professionals to manually assess devices within a system. This is a time consuming and error prone process that lacks visibility for the individuals who ultimately have to sign off on the security posture for each device. The individual sitting at the device and running commands is subject to all kinds of conditions that can call the results into question. The individual could be tired, sick, have a lack of knowledge about a device, or just be disgruntled. Running manual checks is a tedious process especially on large systems. Even with the automated checks with existing tools, there are still possibilities of false positives or false negatives. The false findings require an individual to go back to the device where the automated checks were run and verify the findings.

The tools and methods for handling the non-technical means are even more lacking in their ability. Most organizations tackle this issue by using spreadsheets to track and document the non-technical findings. This becomes error prone quickly; for a large system there are usually multiple spreadsheets that are created that eventually have to be combined and reviewed for accuracy.

Even after all the data collection has been completed, the current toolsets do not allow for easy consolidation of technical and not-technical checks. The tools also do not easily map all the findings to the DISA CCIs or to the NIST 800-53 families. Someone within the organization is then required to manually do this mapping before reporting can be accomplished.

Because RMF requires continuous monitoring, the process for technical and non-technical controls must be completed on a regular basis. This results in yet more time and resources needed to stay compliant within the new framework.

SOLUTION

The Xylok Scanner is created with RMF built-in and is designed to support a single tool for maintaining all the information about an organization's security posture. The Xylok Scanner does not install anything on a system being evaluated, so there are no changes to the baseline to check the security configurations. The Xylok Scanner does not attach to a system's network, so there is no need to open ports or provide the tool administrator passwords. All of this leads to a cleaner and safer way to assess a system.

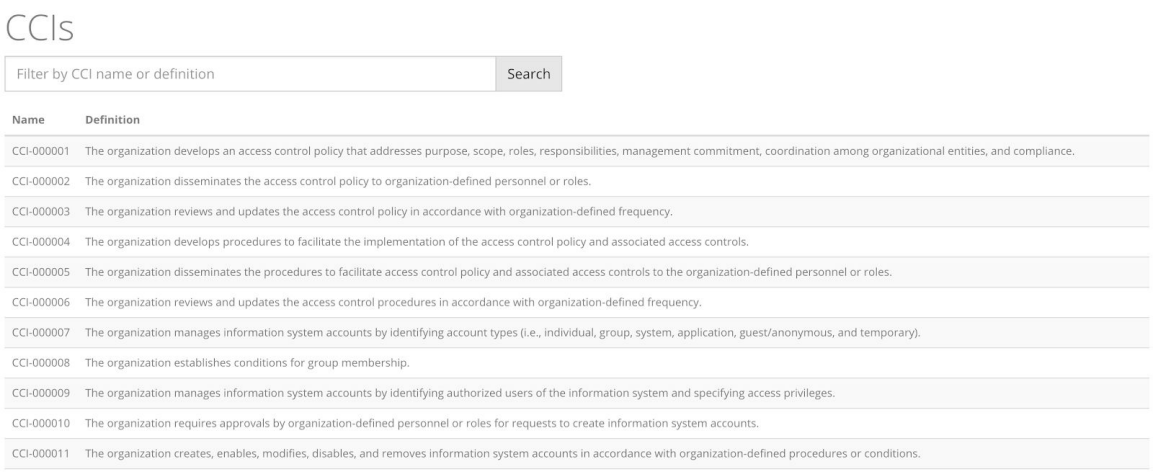
Xylok built the scanner for their own use as an Agent for the Security Control Assessor (ASCA) and for customers who require Xylok to perform Quick Look assessments. By using the tool, Xylok personnel are able to provide real-time feedback to how the tool should work and grow.

Xylok implements all of the RMF information that an organization needs to complete a full cybersecurity assessment of a system.

CCIs

To be able to have a complete picture of what a system's security posture looks like using RMF, Xylok discovered that the scanner needed to have the CCIs built in at the lowest level.

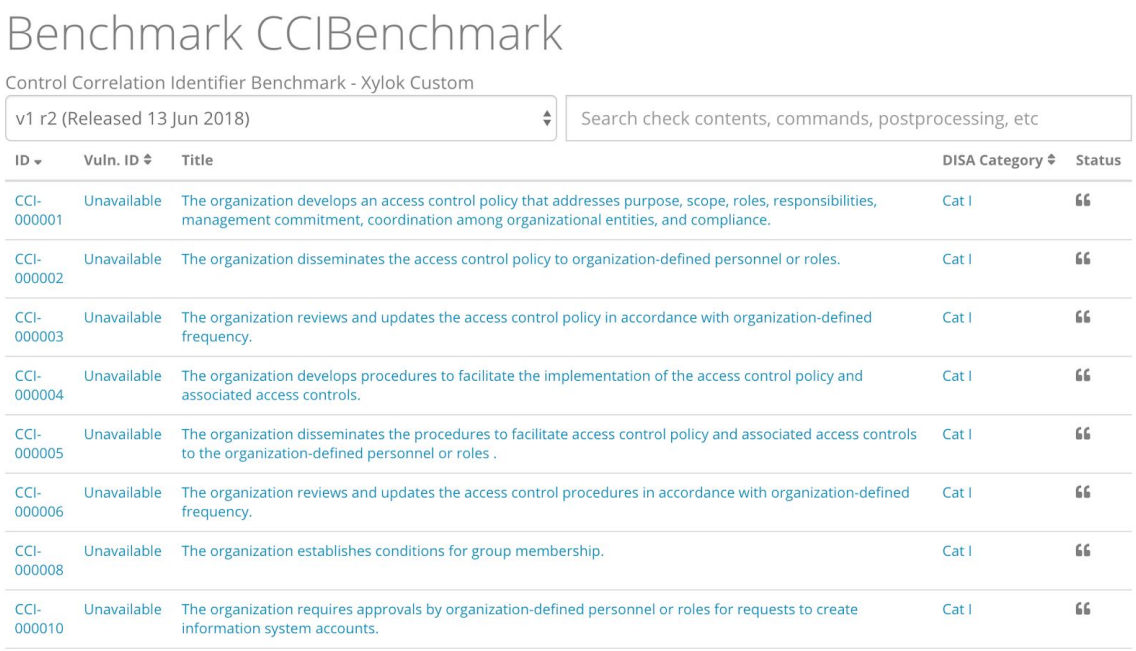
All CCIs are stored within Xylok Scanner and are searchable to aid in the ability to find exactly what low-level detail needs attention.


CCIs

Filter by CCI name or definition Search

Name	Definition
CCI-000001	The organization develops an access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
CCI-000002	The organization disseminates the access control policy to organization-defined personnel or roles.
CCI-000003	The organization reviews and updates the access control policy in accordance with organization-defined frequency.
CCI-000004	The organization develops procedures to facilitate the implementation of the access control policy and associated access controls.
CCI-000005	The organization disseminates the procedures to facilitate access control policy and associated access controls to the organization-defined personnel or roles.
CCI-000006	The organization reviews and updates the access control procedures in accordance with organization-defined frequency.
CCI-000007	The organization manages information system accounts by identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary).
CCI-000008	The organization establishes conditions for group membership.
CCI-000009	The organization manages information system accounts by identifying authorized users of the information system and specifying access privileges.
CCI-000010	The organization requires approvals by organization-defined personnel or roles for requests to create information system accounts.
CCI-000011	The organization creates, enables, modifies, disables, and removes information system accounts in accordance with organization-defined procedures or conditions.

But Xylok did not stop there. Because the Xylok ASCA and Quick Look teams use the tool to assess real systems, Xylok recognized the need to incorporate the CCIs into the risk assessment. So, Xylok built a CCI benchmark to keep all the analysis and findings about a security assessment within the tool.



Benchmark CCIBenchmark

Control Correlation Identifier Benchmark - Xylok Custom

v1 r2 (Released 13 Jun 2018)

Search check contents, commands, postprocessing, etc

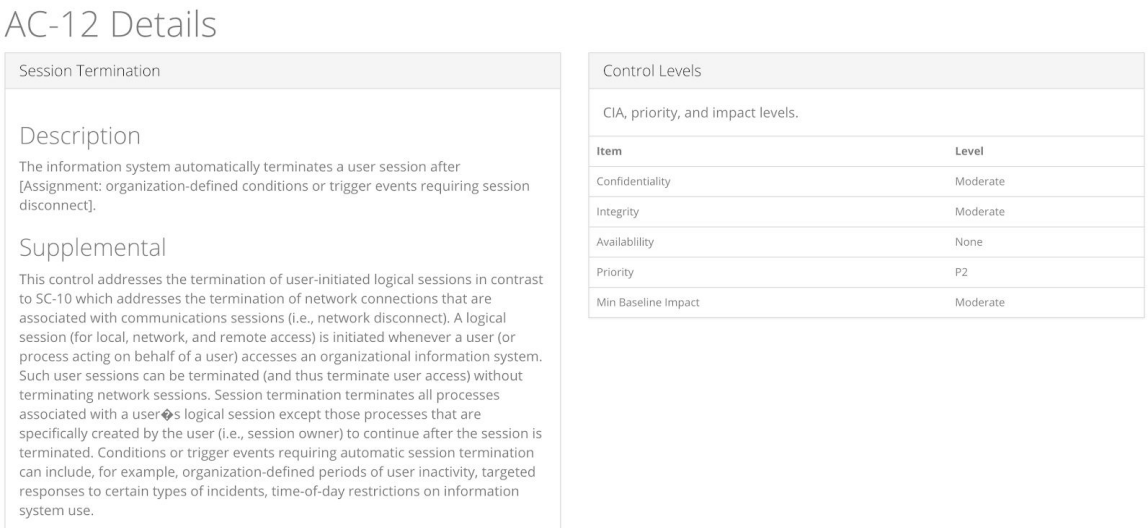
ID	Vuln. ID	Title	DISA Category	Status
CCI-000001	Unavailable	The organization develops an access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	Cat I	
CCI-000002	Unavailable	The organization disseminates the access control policy to organization-defined personnel or roles.	Cat I	
CCI-000003	Unavailable	The organization reviews and updates the access control policy in accordance with organization-defined frequency.	Cat I	
CCI-000004	Unavailable	The organization develops procedures to facilitate the implementation of the access control policy and associated access controls.	Cat I	
CCI-000005	Unavailable	The organization disseminates the procedures to facilitate access control policy and associated access controls to the organization-defined personnel or roles .	Cat I	
CCI-000006	Unavailable	The organization reviews and updates the access control procedures in accordance with organization-defined frequency.	Cat I	
CCI-000008	Unavailable	The organization establishes conditions for group membership.	Cat I	
CCI-000010	Unavailable	The organization requires approvals by organization-defined personnel or roles for requests to create information system accounts.	Cat I	

NIST 800-53 Rev 4

The FISMA defines three security goals for information systems: Confidentiality, Integrity, and Availability (CIA). Using NIST's FIPS 199, the owner's of systems can categorize each goal with a high, medium, or low depending on the nature of their system. Once a system's CIA level has been determined, the owner of the system can use the NIST SP 800-53 Rev 4 to determine which controls are applicable and should be assessed.

Xylok Scanner makes it easy to determine what controls need to be assessed based on a system's defined CIA level. The NIST 800-53 Rev 4 is built into the Xylok Scanner and it can handle overlays that may apply to special systems.

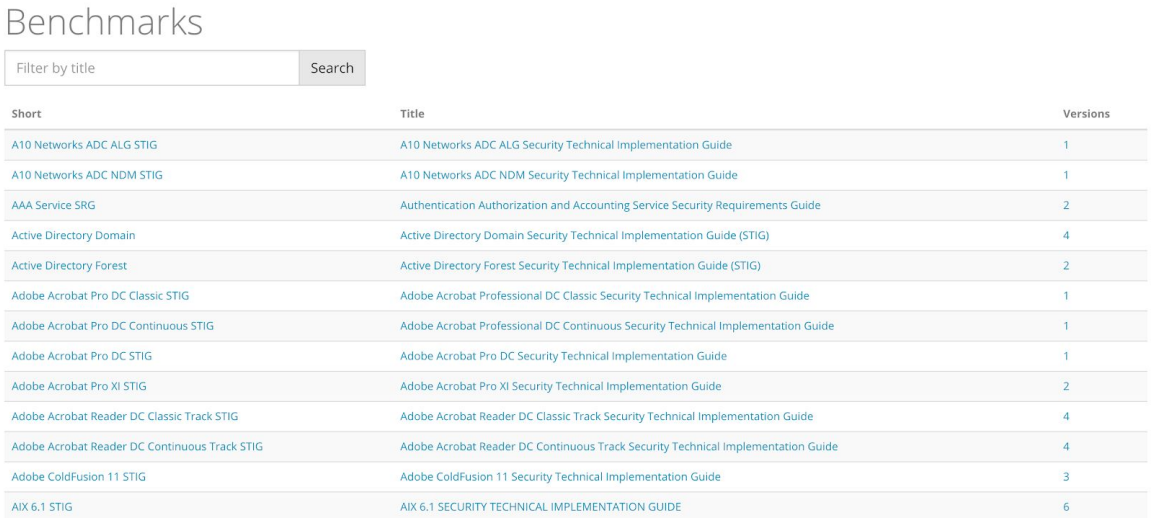
Using the built-in NIST 800-53 Explorer, it is easy to find what controls are contained within a given benchmark. This allows an organization to quickly see what controls are covered with a technical check.



STIGs

DISA maintains the repository of STIGs for the DoD. STIGs are updated on a quarterly basis and are modified to meet the new and emerging threats against information systems.

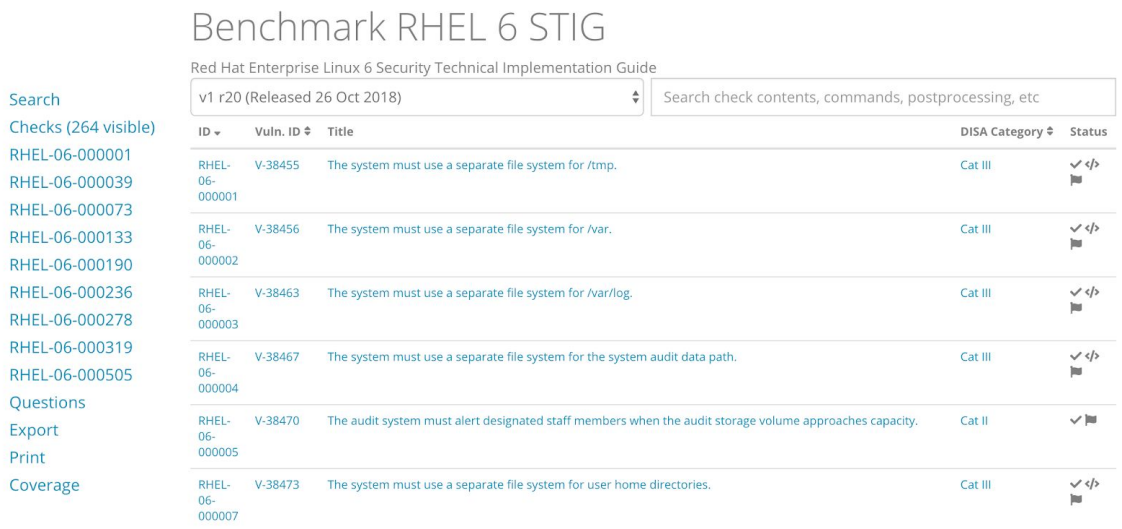
Xylok daily scans the DISA STIG repository for updates and adds to or modifies the STIGs that are stored within the Xylok Scanner. The process also provides the ability to compare previous versions of the STIGs so a user can determine what has changed and if configuration changes are need to a system to stay compliant.



Benchmarks

Filter by title | Search

Short	Title	Versions
A10 Networks ADC ALG STIG	A10 Networks ADC ALG Security Technical Implementation Guide	1
A10 Networks ADC NDM STIG	A10 Networks ADC NDM Security Technical Implementation Guide	1
AAA Service SRG	Authentication Authorization and Accounting Service Security Requirements Guide	2
Active Directory Domain	Active Directory Domain Security Technical Implementation Guide (STIG)	4
Active Directory Forest	Active Directory Forest Security Technical Implementation Guide (STIG)	2
Adobe Acrobat Pro DC Classic STIG	Adobe Acrobat Professional DC Classic Security Technical Implementation Guide	1
Adobe Acrobat Pro DC Continuous STIG	Adobe Acrobat Professional DC Continuous Security Technical Implementation Guide	1
Adobe Acrobat Pro DC STIG	Adobe Acrobat Pro DC Security Technical Implementation Guide	1
Adobe Acrobat Pro XI STIG	Adobe Acrobat Pro XI Security Technical Implementation Guide	2
Adobe Acrobat Reader DC Classic Track STIG	Adobe Acrobat Reader DC Classic Track Security Technical Implementation Guide	4
Adobe Acrobat Reader DC Continuous Track STIG	Adobe Acrobat Reader DC Continuous Track Security Technical Implementation Guide	4
Adobe ColdFusion 11 STIG	Adobe ColdFusion 11 Security Technical Implementation Guide	3
AIX 6.1 STIG	AIX 6.1 SECURITY TECHNICAL IMPLEMENTATION GUIDE	6



Benchmark RHEL 6 STIG

Red Hat Enterprise Linux 6 Security Technical Implementation Guide

Search
Checks (264 visible)
RHEL-06-000001
RHEL-06-000039
RHEL-06-000073
RHEL-06-000133
RHEL-06-000190
RHEL-06-000236
RHEL-06-000278
RHEL-06-000319
RHEL-06-000505
Questions
Export
Print
Coverage

v1 r20 (Released 26 Oct 2018) | Search check contents, commands, postprocessing, etc

ID	Vuln. ID	Title	DISA Category	Status
RHEL-06-000001	V-38455	The system must use a separate file system for /tmp.	Cat III	
RHEL-06-000002	V-38456	The system must use a separate file system for /var.	Cat III	
RHEL-06-000003	V-38463	The system must use a separate file system for /var/log.	Cat III	
RHEL-06-000004	V-38467	The system must use a separate file system for the system audit data path.	Cat III	
RHEL-06-000005	V-38470	The audit system must alert designated staff members when the audit storage volume approaches capacity.	Cat II	
RHEL-06-000007	V-38473	The system must use a separate file system for user home directories.	Cat III	

SCANNING

Xylok Scanner is unique in the way that it accomplishes the scanning of devices. Instead of installing software on each device or connecting a device to a system's network, the Xylok Scanner produces a script for each device that contains all the benchmark checks needed to accomplish the security scan. These scripts are written in the default operating system language of a given device (i.e. bash scripts for Linux, Powershell scripts for Windows 10 and newer, Batch scripts for earlier Windows versions) These scripts run on each device and collect the required configurations and security settings needed to analyze

and verify the compliance to the benchmark. The single results file from a scan can then be imported in a standalone instance of the Xylok Scanner.

By not installing anything or connecting any new equipment to the system, the baseline configuration is not changed or security holes created for the purpose of validating a security posture.

ANALYSIS

Analysis is where the Xylok Scanner shines. Unlike many of the tools available on the market today, the Xylok Scanner provides the raw details of each device's security configuration in a centralized location. This means that you can scan a device, import the data to Xylok Scanner, and then analyze the data without the need to spend hours or even days at a device.

The Xylok Scanner allows an organization to define their security baseline even if it differs from the STIGs being used in the assessment. This baseline, once defined, can be used to auto-analyze across all similar devices on a network.

POST-PROCESSING

Xylok also created a way to reduce the amount of rework needed when analyzing similar devices. By introducing Xylok's post-processing in the Xylok Scanner, raw data can be manipulated to reduce the information that changes from device to device, but does not affect determining if the device is in compliance with the benchmark.

One example is determining the ownership of files in Linux. The command run is 'ls', but this command returns more information than just the owner. It also returns the file size and the date/time the file was last changed. These two attributes are going to be different on every machine even if the owner is the same. Xylok Scanner's auto-analyze would evaluate the returns as different because of the file size and date/time. But with post-processing, which occurs within the Xylok Scanner and does not affect the raw results, the file size and date-time attributes can be removed and now auto-analysis can evaluate the results without that information. This is a huge time savings when comparing multiple like devices.

REPORTING

One of the hardest parts of a security assessment is creating a report that brings everything together and ties it back the RMF standards. With RMF built-in,

reporting is simple and easy. The Xylok Scanner takes all the information entered about all of the controls and produces reporting that includes details down to the CCIs if needed.

Xylok also recognizes that reporting needs are different for organizations, therefore Xylok Scanner exports all the data and associated RMF control information in spreadsheet format to allow for easy customization.

CONTINUOUS MONITORING

RMF requires an organization to continuously monitor the system for changes and upgrades to the baseline. The Xylok Scanner makes this effort simple by scanning the devices again, uploading the results, and auto-analyzing. Once this is complete only the configuration items that have changed will be shown to the analyst. This means assessments that use to take weeks and months will be shortened to minutes.

CONCLUSION

Xylok designed and built the Xylok Scanner with RMF completely embedded in the tool. Xylok provides a user or assessor with a complete tool set that does not require the use of another tool or spreadsheets to validate and report a system's security posture.

Using the Xylok Scanner saves an organization time and resources to complete security assessments. Comparing the process with other tools and Xylok Scanner shows an organization can save 95% reduction in time and reduce the cost by up to 90%.

30 Machines
1 Benchmark (258 Checks)

Manual Method
- ➔ 5 Minutes per Check
- ➔ 2 Engineers Full Time
- ➔ Approximately 16 weeks to complete
- ➔ Total Cost - $51,600

Xylok Scanner
- ➔ <1 Minute per Check
- ➔ Approximately 2 days to complete
- ➔ Total Cost - $5,400

ADDITIONAL RESOURCES

- https://iase.disa.mil/Pages/index.aspx
- https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf
- https://nvd.nist.gov/800-53
- https://iase.disa.mil/stigs/pages/a-z.aspx
- https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001_2014.pdf?ver=2017-07-28-134447-703

Xylok
Cyber Testing Simplified

FOR MORE INFORMATION

For more information, please contact kevin@xylok.io