Assessment Report

Prepared For

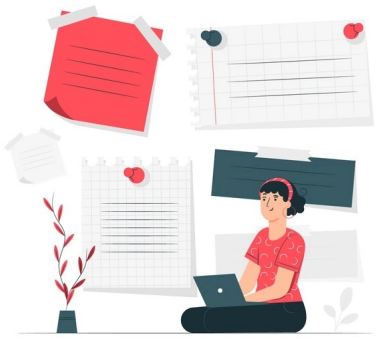
S.U.R.E. IT

Scan Performed On: 23 Nov 2022

Executive Risk Summary

Asset Summary			
No. of Assets discovered	18	No. of Vulnerable Assets	7
Active Directory Summary			
Enabled Computers	7	Disabled Computers	0
Computers With Expired Passwords	0	Locked Out Computers	0
Computers - Never Logged In	0	Computers Not Logged in for 30 days	1
Computers - Password Never Expires	0	Computers - Password Expires	7
Computers - Password Not Required	0	Total Computers	7
Enabled Users	13	Disabled Users	2
Users With Expired Passwords	2	Locked Out Users	0
Users - Never Logged In	3	Users Not Logged in for 30 days	8
Users - Password Not Required	0	Total Users	15
Users - Password Never Expires	11	Users - Password Expires	2
Empty OUs	0	Non Empty OUs	3
Total OUs	3	Total GPOs	2
Empty Groups	39	Non Empty Groups	12
Privileged Access Groups	46	Total Groups	51

- 10 out of 18 assets with remote access enabled.
- 0 out of 18 assets missing advanced protection.
- 3 out of 15 users never logged in.
- 1 out of 12 storage devices with hard drive space utilized over 90% while 4 other storage devices with hard drive utilized over 75%
- 0 out of 18 assets with Antivirus not installed.



- 0 out of 15 users did not login for last 90 days.
- 1 out of 18 assets running end of life OS.
- 2 out of 12 storage devices with hard drive space utilized between 50-75%.
- 0 out of 18 assets with Antivirus installed but not up to date.

- 8 out of 15 users did not login for last 30 days.
- 1 out of 18 storage devices with hard drive space utilized between 25-50%.

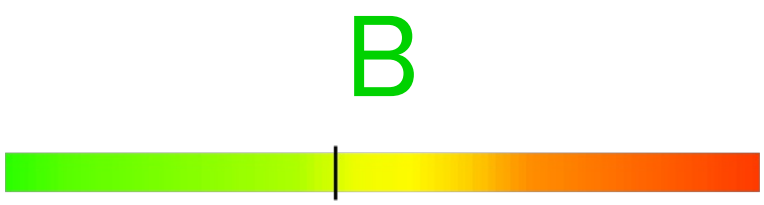
- 8 out of 18 assets with basic Antivirus protection.
- 5 out of 18 assets with firewall protection.

Table of Content

Security Assessment

Assessment report for S.U.R.E. IT provides visibility into specific weaknesses and deficiencies in the security controls employed within or inherited by the information system. Such weaknesses and deficiencies are potential vulnerabilities if exploitable by a threat source. The findings generated during the security control assessment provide important information that facilitates a disciplined and structured approach to mitigating risks in accordance with organizational priorities.

Risk Dashboard



The Consolidated Risk Report aggregates risk analysis from multiple assessments performed on the network, providing you with both a Consolidated Risk Score and a high-level overview of the health and security of the network. The report details the scan tasks undertaken to discover security issues. In addition to the overall Consolidated Risk Score, the report also presents separate impact scores for all area of assessments.

Vulnerability Assessment

A vulnerability assessment is the process of defining, identifying, classifying and prioritizing vulnerabilities in computer systems, and network infrastructures and providing the organization doing the assessment with the necessary knowledge, awareness and risk background to understand the threats to its environment and react appropriately.

Critical

2 were unique critical severity vulnerabilities. Critical vulnerabilities require immediate attention. They are relatively easy for attackers to exploit and may provide them with full control of the affected systems

2

High

274 were unique high severity vulnerabilities. High severity vulnerabilities are easy to exploit and may provide access to affected systems.

274

Medium

125 were unique medium severity vulnerabilities. These vulnerabilities often provide information to attackers that may assist them in mounting subsequent attacks on your network. These should also be fixed in a timely manner but are not as urgent as the other vulnerabilities.

125

Low

13 were unique low severity vulnerabilities. These should also be fixed in a timely manner but are not as urgent as the other vulnerabilities.

13

Risk Detected: High Risk Score

Top 5 Vulnerabilities

Vulnerability	Asset Count	Risk
Crash in the OPUS protocol dissector in Wireshark 3.6.0 to 3.6.8 allows denial of service via packet injection or crafted capture file	4	HIGH
Ubuntu Security Notification (USN-4194-1)	1	HIGH
CredSSP (NTLM) Authentication Request With Null Credentials	6	MEDIUM
HTTP Security Header Not Detected	4	MEDIUM
Web Server Fingerprint and Version detection over 80/TCP	4	MEDIUM

Critical

Apply patches within 30 days of release

High

Apply patches within 30 - 60 days

Medium

Apply patches within 60 - 90 days

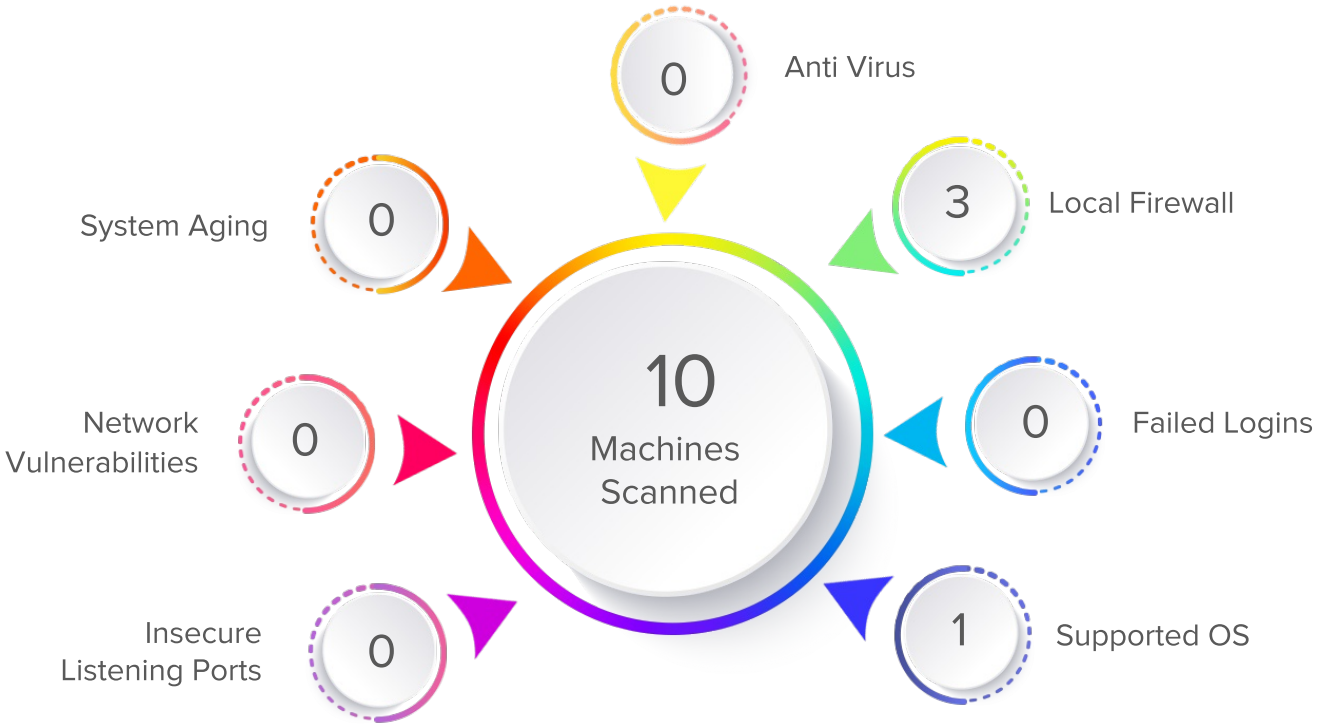
Low

Apply patches within 180 days

Endpoint Assessment

In today's time end-users have become a prime target for cyber criminals. But the real tangible target is the end-user's workstation, and organizations would be remiss not to regularly validate the security of their endpoints. To close the gap, we have developed an endpoint assessment methodology that accounts for each area of the attack. The identification of vulnerabilities and gaps in security controls that may have gone unnoticed will assist you in tuning detection or protective controls to handle user activities. Associated remediation efforts will enhance incident response capabilities and further strengthen your overall security posture.

Security Report Card



Anti Virus
0 assets with AntiVirus Not installed.

Local Firewall
3 assets with Local Firewall Disabled.

Supported OS
1 assets with Some OS not supported

Insecure Listening Ports
0 assets with More than one insecure listening port

Network Vulnerabilities
0 assets with CVSS greater than or equal to 9.0.

System Aging
0 Computers over 8 years old.

Failed Logins
0 or more failed logins in the last 7 days

Compliance Report Card

LLMNR

8 Assets with LLMNR Enabled.

NTLMV1

0 Assets with NTLMV1 Enabled.

NBTNS

8 Assets with NBTNS Enabled.

SMBV1 Server

0 Assets with SMBV1 Server Enabled.

SMBV1 Client

1 Assets with SMBV1 Client Enabled.

SMB Signing

7 Assets with SMB Signing Disabled.

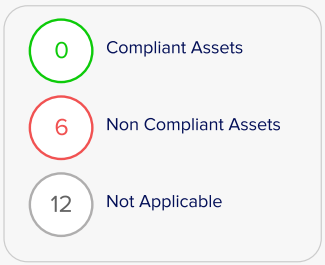
Compliance Assessment

CIS

The Center for Internet Security (CIS) benchmarks are a set of best-practice cybersecurity standards for a range of IT systems and products. CIS Benchmarks provide the baseline configurations to ensure compliance with industry-agreed cybersecurity standards.

PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a security standard used to ensure the safe and secure transfer of credit card data.The regulations include security management provisions that cover policies, network architecture, software design and other critical safety measures.



GDPR IV

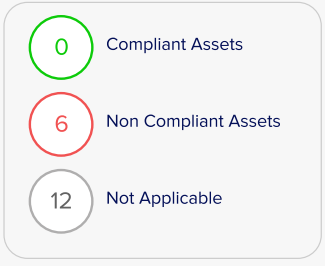
General Data Protection Legislation(GDPR) is the legislative force established to protect the fundamental rights of data subjects whose personal information and sensitive data is stored in organisations.

GPG 13

The Good Practice Guide 13 (GPG 13) is a protective monitoring framework. It provides a framework for treating risks to systems, collecting log information and configuring logs to provide an audit trail of security relevant events of interest.

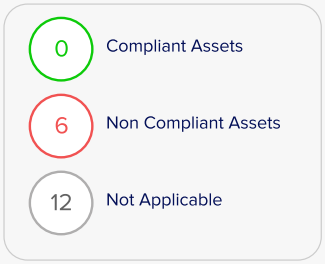
NIST 800 53

National Institute of Standards and Technology (NIST) NIST SP 800-53 provides a list of controls that support the development of secure and resilient federal information systems. These controls are the operational, technical, and management standards and guidelines used by information systems to maintain confidentiality, integrity, and availability. The guidelines adopt a multi-tiered approach to risk management through control compliance.



HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.

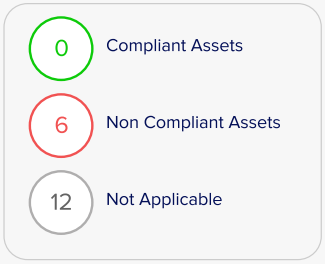


ISO 27002

International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) ISO/IEC 27002:gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s).

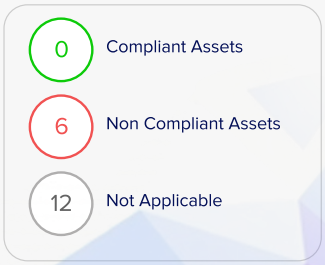
CIS 8 0

CIS Controls v8 has been enhanced to keep up with modern systems and software. Movement to cloud-based computing, virtualization, mobility, outsourcing, Work-from-Home, and changing attacker tactics prompted the update and supports an enterprise's security as they move to both fully cloud and hybrid environments.



NIST 800 171

The National Institute of Standards and Technology (NIST) created Special Publication 800-171 to help protect Controlled Unclassified Information. NIST 800-171 standardizes how federal agencies define CUI: data that is private and sensitive but not classified per federal law.



Patch Assessment

Patch assessment is the process that helps acquire, test and install multiple patches on a computer, enabling systems to stay updated on existing patches and safeguards the IT environment from vulnerability and exploit.

Risk Detected

18 Assets Scanned

24 Patches Missing in 18 Assets

Impact Level High

Apply Patch to Stay Protected

2 Critical Missing Patches

Apply patches within 30 days of release

8 High Missing Patches

Apply patches within 30 - 60 day

8 Medium Missing Patches

Apply patches within 60 - 90 days

3 Low Missing Patches

Apply patches within 180 days

Top 5 Missing Patches

Vulnerability	CRITICAL	HIGH	Asset Count
Wireshark 3.6.8 64-bit	0	8	8
Microsoft Teams	0	0	6
Adobe Acrobat Reader DC MUI	0	6	3
Opera Stable 92.0.4561.43	0	0	2
Windows 11 Build 22000	1	104	2

Password Policy Summary

Policy	Setting	Domain
Enforce password history	24 passwords remembered	sureit.local
Maximum Password Age	42 days	sureit.local
Minimum Password Age	1 days	sureit.local
Minimum Password Length	7 characters	sureit.local

Password history not remembered

Issue: Short password histories allow users to rotate through a known set of passwords, thus reducing the effectiveness of a good password management policy.

Recommendation: Increase password history to remember at least six passwords.

Maximum Password Age

Issue: Passwords that are not changed regularly are more vulnerable to attack and unauthorized use. Minimizing the allowed password age greatly reduces the window of time that a lost or stolen password poses a threat.

Recommendation: Modify the maximum password age to be 90 days or less.

Password length less than 8 characters

Issue: Passwords are not required to be 8 or more characters, allowing users to pick extremely short passwords which are vulnerable to brute force attacks.

Recommendation: Enable enforcement of password length to more than 8 characters.

Inconsistent password policy

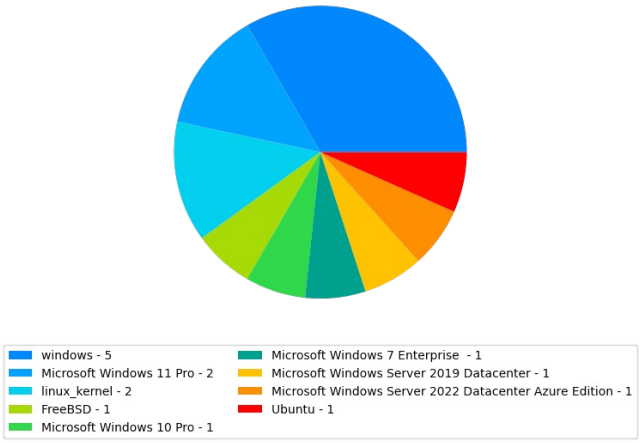
Issue: Password policies are not consistently applied from one computer to the next. A consistently applied password policy ensures adherence to password practices.

Recommendation: Eliminate inconsistencies and exceptions to the password policy.

IT Infrastructure Assessment

Asset discovery is simply the process of discovering and collecting data on the technology assets connected to a network for management and tracking purposes

Assets - Operating System



Risk Detected

18 Assets Scanned

1 STORAGE DEVICES WITH DISK SPACE UTILIZED OVER 90%

4 STORAGE DEVICES WITH DISK SPACE UTILIZED OVER 75%

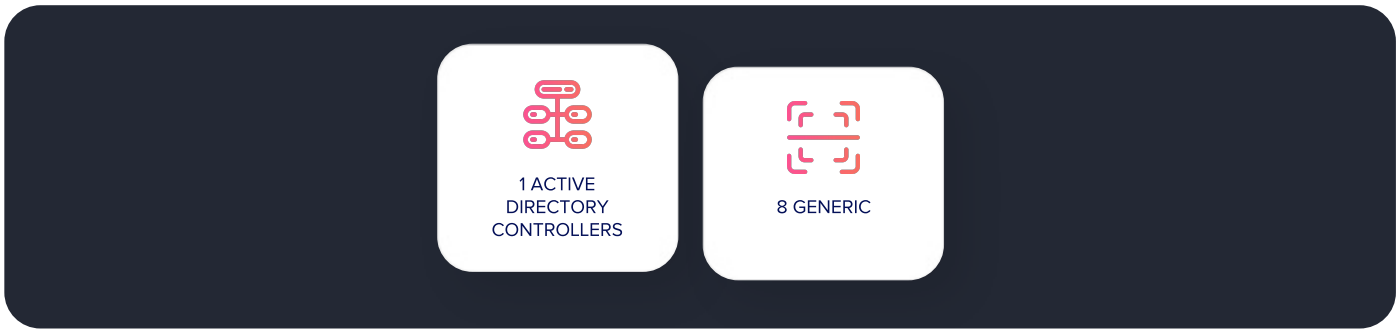
Storage Devices by Disk Space

Disc Space Utilized	Device Count
Up to 25%	5
25 – 50%	1
50 – 75%	2
75 – 90%	3
More than 90%	1

Storage Device Encryption Status

Status	Device Count
Encrypted	0
Not Encrypted	0
Unknown	12

Asset Breakdown



Assets by OS

OS Name	Asset Count
windows	5
Microsoft Windows 11 Pro	2
linux_kernel	2
FreeBSD	1
Microsoft Windows 10 Pro	1
Microsoft Windows 7 Enterprise	1
Microsoft Windows Server 2019 Datacenter	1
Microsoft Windows Server 2022 Datacenter Azure Edition	1
Ubuntu	1