STRATADEFENSE

Network Security Focused. Customer Driven.

Assessment Report

Prepared For

Your Organization Name Here

Scan Performed On

29 Sep 2023

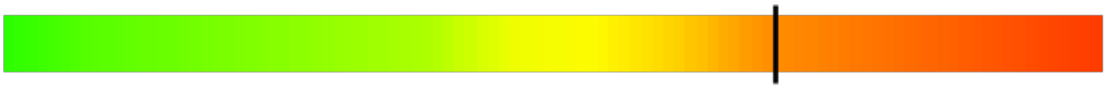
Executive Risk Summary

Asset Summary	
No. of Assets discovered	29
Vulnerability Summary	
No. of Vulnerable Assets	14
Active Directory Summary	
Enabled Computers	24
Disabled Computers	28
Computers Not Logged In 30 Days	24
Total Computers	52
Enabled Users	39
Disabled Users	11
Users Not Logged In 30 Days	30
Users with Non-Expiring Password	26
Users with Expired Password	0
Locked Out Users	0
Users with Passwords Expiring Soon	1
Total Users	50
Linked GPO’s	3
Unlinked GPO’s	0
Total GPO’s	0
Empty Groups	47
Non-Empty Groups	24
Total Groups	71

Company Level Risk Score

D

Company Grade



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.

The Company Level Risk Scores are assigned grades based on the following Risk Score Criteria:

- Risk Score Grade: A (0 - 40):
  A represents **Very Low** (Issues are present and an organization should aim to be in the 0-40 range, however broadly all significant issues have been taken care of).

- Risk Score Grade: B (40 - 45):
  B represents Low (Issues are present and the value ranges from 40-45, however significant issues have been taken care of).

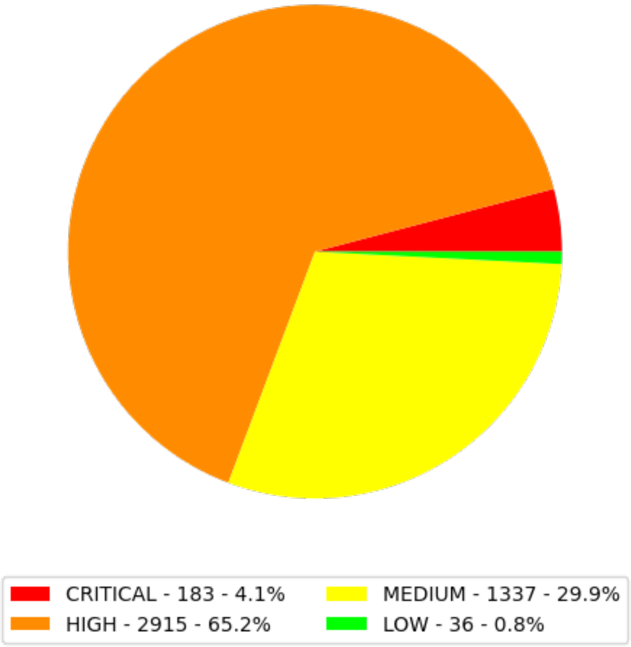
- Risk Score Grade: C (45 - 60):
  C represents Medium (A small number of issues that need immediate attention and the value ranges from 45-60).

- Risk Score Grade: D (60 - 75):
  D represents a High (Significant number of issues that require attention and the value ranges from 60-75).

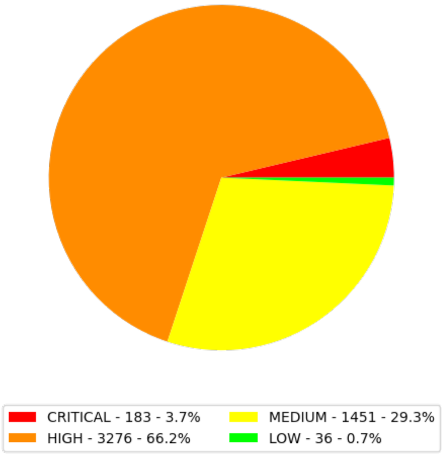
- Risk Score Grade: E (75 - 90):
  E represents Critical (The network is susceptible to attack and needs remediation to be performed on a war footing and the value ranges from 75-90)

- Risk Score Grade: F (90 - 100):
  F represents Very Critically (The network is highly susceptible to attack and needs remediation to be performed on a war footing and the value ranges from 90-100)

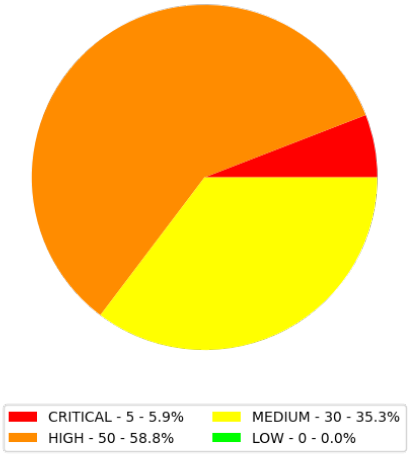
Vulnerability Assessment



Remediation Summary



Remediation Summary for Last 30 Days



Remediations Resolved in Last 30 days

No Resolved Remediations.

Vulnerability Assessment

Top 5 Vulnerabilities

Sl. No.	Vulnerabilities	Vulnerabilities Count	Risk
1	CVE-2023-35385	10	CRITICAL
2	CVE-2023-36735	10	CRITICAL
3	CVE-2023-36903	10	CRITICAL
4	CVE-2023-36910	10	CRITICAL
5	CVE-2023-36911	10	CRITICAL

Network Summary

Security Report Card Summary

	Asset Count	Description	
Anti-virus / Anti-spyware	14	5	Installed and updated
	0	4	Installed but not updated
	0	1	Not installed
Local Firewall	3	5	Enabled for both public and private networks
	0	4	Disabled for private networks
	11	3/1	Disabled
Insecure Listening Ports	1	5	No insecure listening ports
	12	3	1 insecure listening port
	1	1	More than one insecure listening port
Failed Logins	0	5	None in the last 7 days
	0	4	7 or less in the last 7 days
	0	3	14 or less in the last 7 days
	0	1	15 or more in the last 7 days
Network Vulnerabilities	14	5	No vulnerabilities
	0	4	Minor vulnerabilities (CVSS < 4.0)
	0	3	Major vulnerabilities (CVSS >= 4.0)
	0	1	Critical network vulnerabilities (CVSS >= 9.0)
System Aging	6	5	Computers are less than 2 years old
	8	4	Computers between 3 and 4 years old
	0	3	Computers between 4 and 7 years old
	0	1	Computers over 8 years old
Supported OS	4	5	All computers have supported OS
	0	4	Some OS are in extended supported
	6	3	Some OS with end of life less than 1 year
	4	1	Some OS are not supported
Backup Software	0	5	Backup Software Enabled
	0	1	Backup Software Disabled
	0	-1	Not Applicable

Operating System Breakdown

Sl. No.	Operating System	Asset Count
1	Microsoft Windows 10 Pro	10
2	Microsoft Windows Server 2019 Standard	4

Compliance Report Card Summary

	Asset Count	Description	
LLMNR	0	5	LLMNR Disabled
	0	2	LLMNR not Allowed
	14	1	LLMNR Enabled
NBTNS	0	5	NBTNS Disabled
	0	2	NBTNS not Allowed
	14	1	NBTNS Enabled
NTLMV1	14	5	NTLMV1 Disabled
	0	2	NTLMV1 not Allowed
	0	1	NTLMV1 Enabled
SMBV1 Server	14	5	SMBV1 Server Disabled
	0	2	SMBV1 Server not Allowed
	0	1	SMBV1 Server Enabled
SMBV1 Client	14	5	SMBV1 Client Disabled
	0	2	SMBV1 Client not Allowed
	0	1	SMBV1 Client Enabled
SMB Signing	0	5	SMB Signing Enabled
	0	2	SMB Signing Disabled
	14	1	SMB Signing Disabled
TLS 1.2	0	5	TLS 1.2 Enabled
	0	1	TLS 1.2 Disabled
TLS 1.0	0	5	TLS 1.0 Disabled
	0	1	TLS 1.0 Enabled
TLS 1.1	0	5	TLS 1.1 Disabled
	0	1	TLS 1.1 Enabled

Compliance Summary

Compliance	Compliant	Non-Compliant	Not Applicable
CIS	0	14	15
CIS_8 0	0	14	15
GDPR IV	0	14	15
GPG 13	0	14	15
HIPAA	0	14	15
ISO 27002	0	14	15
NIST 800 171	0	14	15
NIST 800 53	0	14	15
PCI DSS	0	14	15

Top 5 Missing Patches

Sl. No.	Application	Critical	High	Asset Count
1	Google Chrome	79.0	1889.0	12
2	Windows 10 Build 19043	4.0	89.0	11
3	Microsoft Edge	10.0	370.0	10
4	Windows Server 2019 Build 17763	37.0	509.0	8
5	Microsoft Teams	0.0	0.0	6

Password Policy Summary

Domain	Enforce password history	Maximum password age	Minimum password age	Minimum password length
your_internal_domain.local	24 Passwords remembered	90 Days	30 Days	8 Characters

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.