

Secure Health- Final Cybersecurity Audit Report

1. Introduction

This project provides a complete cybersecurity audit and basic infrastructure for **SecureCart Health**, a small healthcare-related organisation. The goal of the audit was to review the company's security posture, identity risks, and implement controls to improve protection across the network.

During this audit, I reviewed password policies, account lockout settings, audit logs, remote-access configurations, and firewall rules. I then implemented security enhancements to mitigate vulnerabilities and enhance the company's overall defences.

2. Company Background

SecureCart Health is a healthcare support service that maintains sensitive patient-related data such as customer information, internal staff accounts, and operational systems. Because healthcare data is considered sensitive, the company needs to maintain strong cybersecurity practices.

Although SecureCart Health is small, it still faces common security risks like weak passwords, unauthorised access attempts, and insecure network services. This project focuses on simple and effective controls to protect the organisation.

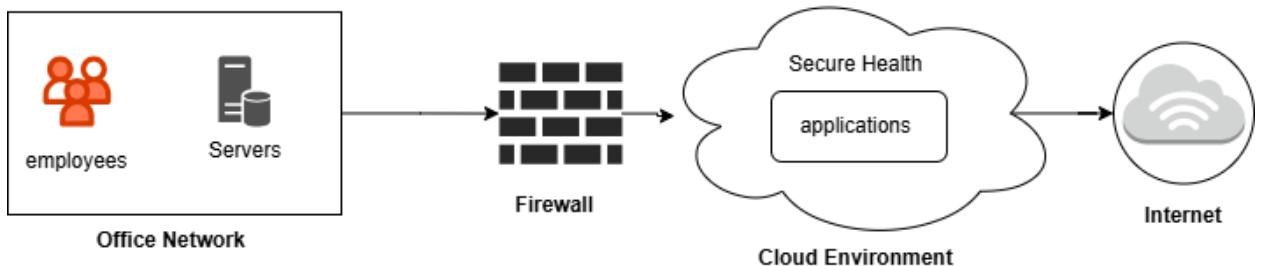
3. Project Scope

The scope of this project includes:

- Reviewing the organisation's existing security posture
- Identifying key risks and vulnerabilities
- Applying five security controls inside the virtual environment
- Documenting changes with screenshots
- Providing future recommendations for the organisation

This project does **not** include penetration testing, data recovery, advanced incident response, or cloud architecture design.

4. Network Diagram



5. Project Objectives

- Strengthen user authentication
- Reduce the risk of unauthorised access
- Improve system visibility through logging
- Limit the number of exposed network services
- Create clear documentation showing implemented security controls.

6. Tools Used

- Windows Server 2022 (Domain Controller)
- Windows 11 Client
- Group Policy Management
- Event Viewer
- Windows Defender Firewall
- Virtual Box or VMware environment

7. Identified Risks and Vulnerabilities

During the audit, I identified five key security risks that could affect SecureCart Health:

Risk 1: Weak or Easy-to-Guess Passwords

Users may select passwords that are too short or predictable, which increases the chance of unauthorised access.

Risk 2: Brute-Force Login Attempts

Attackers can try passwords repeatedly until they find the right one if no limit is set.

Risk 3: Lack of Logon/Logoff Tracking

Without proper logging, the organisation cannot detect suspicious login behaviour or investigate incidents.

Risk 4: Unsafe or Unnecessary Ports Open

Leaving insecure ports (like FTP or HTTP) open exposes the system to attacks/

Risk 5: Too Many Remote Services Enabled

Unneeded remote access services increase the attack surface and create entry points for attackers.

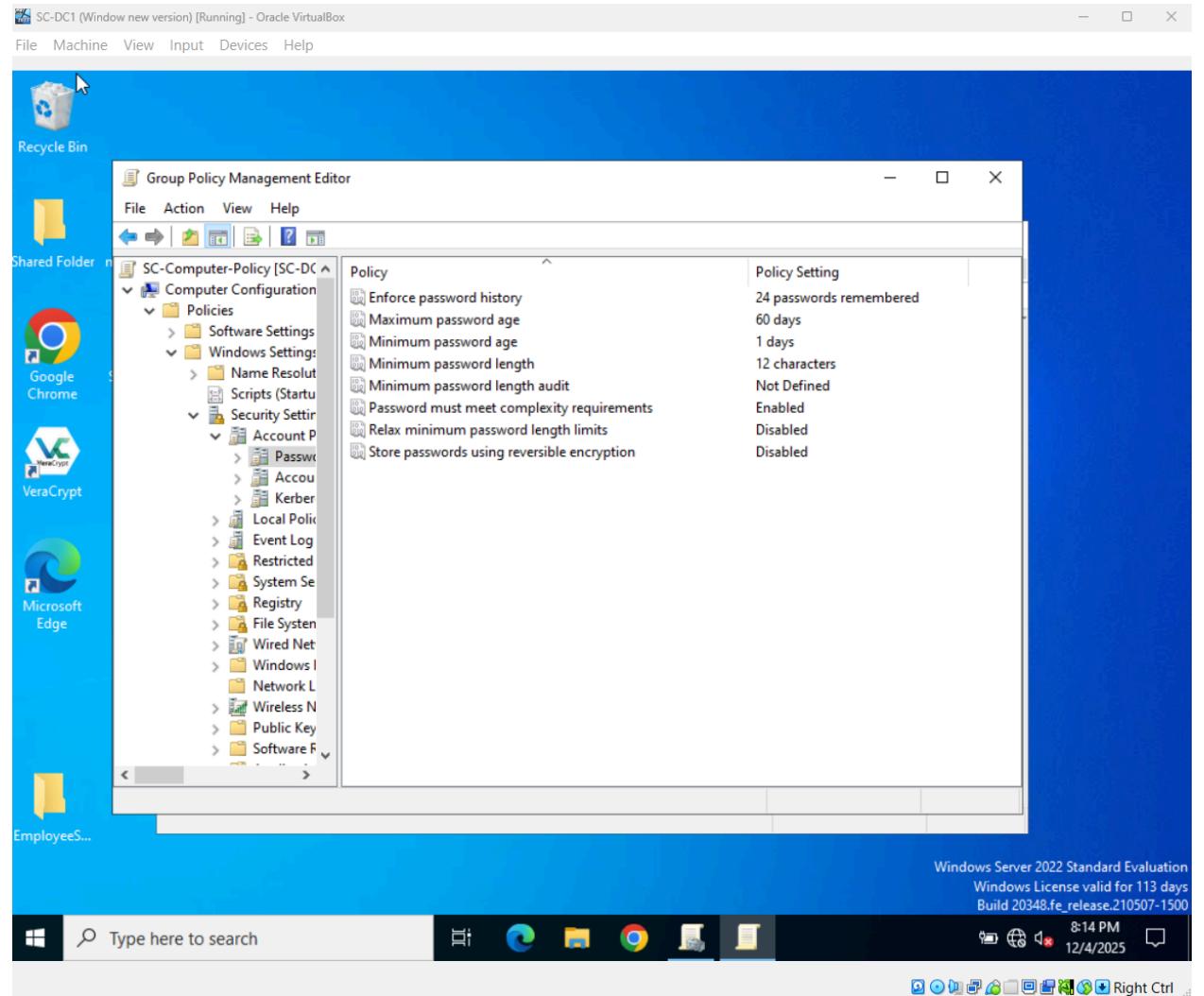
8. Security Controls Implemented & Evidence

To reduce these risks, I applied five security controls in the virtual environment. Each control includes a screenshot from the environment showing the applied configuration.

Control 1: Strong Password Policy

Risk Addressed: Weak Passwords

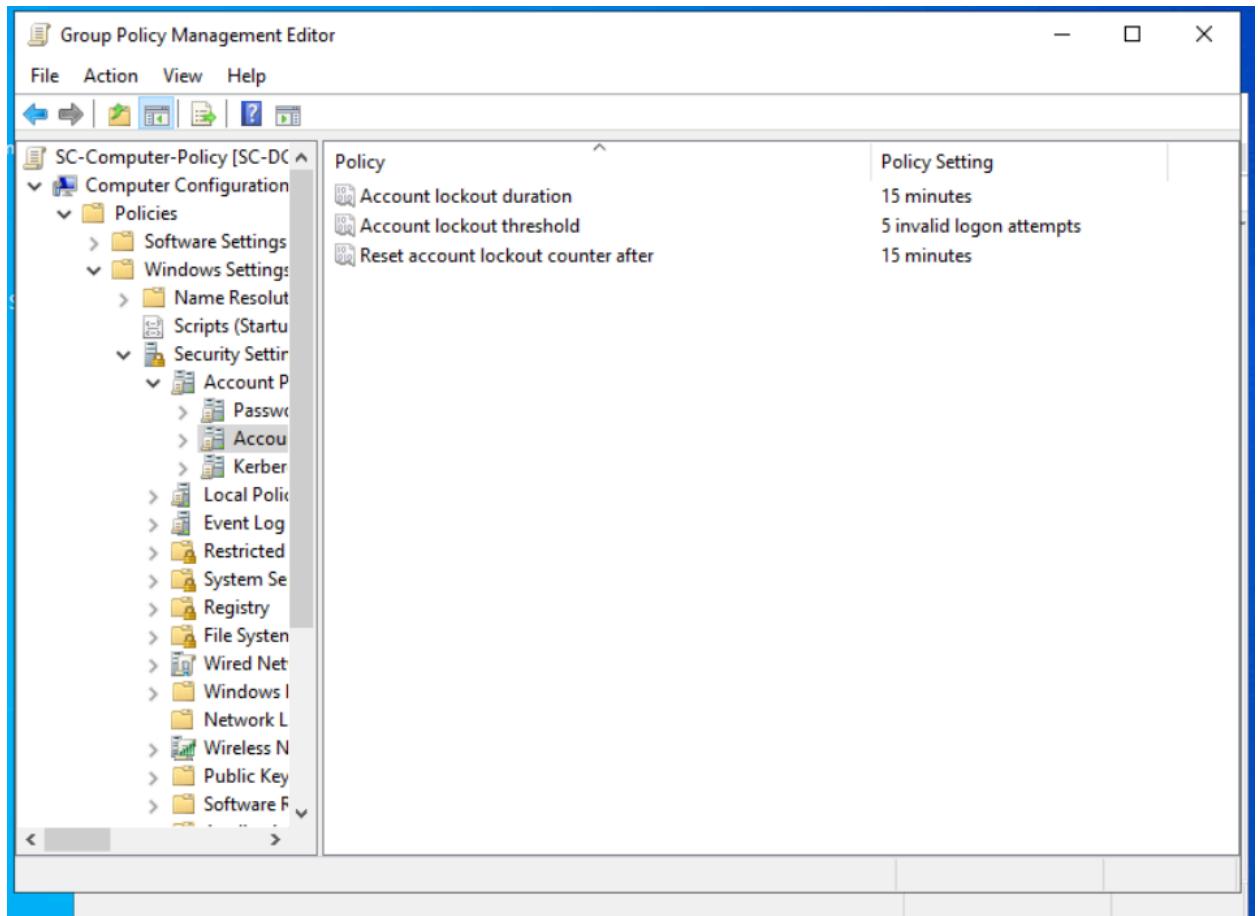
I configured a stronger password policy requiring complexity, minimum length, and password history.



Control 2: Account Lockout Policy

Risk Addressed: Brute Force attacks

I set the account lockout threshold to five failed attempts, with a 15-minute lockout duration.



Control 3: Logon/Logoff Auditing

Risk Addressed: No Security visibility

I enabled auditing so logon and logoff events are recorded in Event Viewer.

The screenshot shows the Windows Event Viewer interface within the Computer Management console. The left pane displays a tree view of system tools, with 'Event Viewer' selected under 'System Tools'. The right pane shows a list of audit events. A specific event, 'Event 4634, Microsoft Windows security auditing.', is selected and expanded, showing its details in the bottom pane. The details pane shows the event type as 'An account was logged off.' and provides information such as Log Name: Security, Source: Microsoft Windows security, Event ID: 4634, Task Category: Logoff, Level: Information, and User: N/A.

Keywords	Date and Time	Source	Event ID	Task Category
Audit Succ...	12/4/2025 8:31:57 PM	Microsoft Wi...	4634	Logoff
Audit Succ...	12/4/2025 8:31:57 PM	Microsoft Wi...	4624	Logon
Audit Succ...	12/4/2025 8:31:57 PM	Microsoft Wi...	4672	Special Logon
Audit Succ...	12/4/2025 8:30:57 PM	Microsoft Wi...	4634	Logoff
Audit Succ...	12/4/2025 8:30:57 PM	Microsoft Wi...	4624	Logon
Audit Succ...	12/4/2025 8:30:57 PM	Microsoft Wi...	4672	Special Logon
Audit Succ...	12/4/2025 8:30:48 PM	Microsoft Wi...	4634	Logoff
Audit Succ...	12/4/2025 8:30:37 PM	Microsoft Wi...	4624	Logon
Audit Succ...	12/4/2025 8:30:21 PM	Microsoft Wi...	5379	User Account ...
Audit Succ...	12/4/2025 8:30:21 PM	Microsoft Wi...	5379	User Account ...
Audit Succ...	12/4/2025 8:30:21 PM	Microsoft Wi...	5379	User Account ...
Audit Succ...	12/4/2025 8:30:14 PM	Microsoft Wi...	4634	Logoff
Audit Succ...	12/4/2025 8:30:14 PM	Microsoft Wi...	4634	Logoff
Audit Succ...	12/4/2025 8:29:57 PM	Microsoft Wi...	4634	Logoff
Audit Succ...	12/4/2025 8:29:57 PM	Microsoft Wi...	4624	Logon
Audit Succ...	12/4/2025 8:29:57 PM	Microsoft Wi...	4672	Special Logon

Control 4: Firewall Hardening - Custom Allow/Block Rules

Risk Addressed: Unsafe ports left open

I blocked insecure services like FTP and HTTP, and allowed only HTTPS traffic for secure communication.

The screenshot shows the Windows Defender Firewall with Advanced Security interface. The left sidebar has options: Inbound Rules (selected), Outbound Rules, Connection Security Rules, and Monitoring. The main area displays the 'Inbound Rules' table with the following columns: Name, Group, Profile, Enabled, and Action. The table lists numerous rules, many of which are Active Directory Domain Controller-related. A detailed view of one rule is shown on the right: 'Allow WinRM' (Group: WinRM, Profile: All, Enabled: Yes, Action: Allow). The Actions pane on the right includes options like New Rule..., Filter by Profile, Filter by State, Filter by Group, View, Refresh, Export List..., and Help.

Name	Group	Profile	Enabled	Action
ALLOW HTTPS		All	Yes	Allow
allow rule		All	Yes	Allow
Block FTP		All	Yes	Block
Block HTTP		All	Yes	Block
Block Rule		All	Yes	Block
Active Directory Domain Controller - Ec...	Active Directory Domain Ser...	All	Yes	Allow
Active Directory Domain Controller - Ec...	Active Directory Domain Ser...	All	Yes	Allow
Active Directory Domain Controller - LD...	Active Directory Domain Ser...	All	Yes	Allow
Active Directory Domain Controller - LD...	Active Directory Domain Ser...	All	Yes	Allow
Active Directory Domain Controller - Net...	Active Directory Domain Ser...	All	Yes	Allow
Active Directory Domain Controller - SA...	Active Directory Domain Ser...	All	Yes	Allow
Active Directory Domain Controller - SA...	Active Directory Domain Ser...	All	Yes	Allow
Active Directory Domain Controller - Sec...	Active Directory Domain Ser...	All	Yes	Allow
Active Directory Domain Controller - Sec...	Active Directory Domain Ser...	All	Yes	Allow
Active Directory Domain Controller - W3...	Active Directory Domain Ser...	All	Yes	Allow
Active Directory Domain Controller (RPC)	Active Directory Domain Ser...	All	Yes	Allow
Active Directory Domain Controller (RPC-In)	Active Directory Domain Ser...	All	Yes	Allow
Active Directory Web Services (TCP-In)	Active Directory Web Services	All	Yes	Allow
AllJoyn Router (TCP-In)	AllJoyn Router	Domai...	Yes	Allow
AllJoyn Router (UDP-In)	AllJoyn Router	Domai...	Yes	Allow
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...	All	No	Allow
BranchCache Hosted Cache Server (HTTP...)	BranchCache - Hosted Cach...	All	No	Allow
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove...	All	No	Allow
Cast to Device functionality (qWave-TCP...)	Cast to Device functionality	Private...	Yes	Allow
Cast to Device functionality (qWave-UDP...)	Cast to Device functionality	Private...	Yes	Allow
Cast to Device SSDP Discovery (UDP-In)	Cast to Device functionality	Public	Yes	Allow
Cast to Device streaming server (HTTP-St...)	Cast to Device functionality	Public	Yes	Allow
Cast to Device streaming server (HTTP-St...)	Cast to Device functionality	Private	Yes	Allow

Control 5: Remote Access Rules Review

Risk Addressed: Too many remote services enabled

I reviewed the inbound firewall rules to make sure only necessary remote access features were enabled.

The screenshot shows the Windows Defender Firewall with Advanced Security interface. The left sidebar has options: Inbound Rules (selected), Outbound Rules, Connection Security Rules, and Monitoring. The main area displays the 'Inbound Rules' table with the following columns: Name, Group, Profile, Enabled, and Action. The table lists numerous rules, many of which are for Remote Desktop, Event Log Management, and various service management protocols. The 'Actions' pane on the right shows options like New Rule..., Filter by Profile, Refresh, and Export List... A status bar at the bottom indicates the build number (Build 20250.1000) and system information (8:35 PM, 12/4/2025).

Name	Group	Profile	Enabled	Action
Remote Desktop - (TCP-WSS-In)	Remote Desktop (WebSocket)	All	No	Allow
Remote Event Log Management (NP-In)	Remote Event Log Manage...	All	No	Allow
Remote Event Log Management (RPC)	Remote Event Log Manage...	All	No	Allow
Remote Event Log Management (RPC-EP...	Remote Event Log Manage...	All	No	Allow
Remote Event Monitor (RPC)	Remote Event Monitor	All	No	Allow
Remote Event Monitor (RPC-EPMAP)	Remote Event Monitor	All	No	Allow
Remote Scheduled Tasks Management (R...	Remote Scheduled Tasks Ma...	All	No	Allow
Remote Scheduled Tasks Management (R...	Remote Scheduled Tasks Ma...	All	No	Allow
Remote Service Management (NP-In)	Remote Service Management	All	No	Allow
Remote Service Management (RPC)	Remote Service Management	All	No	Allow
Remote Service Management (RPC-EPM...	Remote Service Management	All	No	Allow
Inbound Rule for Remote Shutdown (RP...	Remote Shutdown	All	No	Allow
Inbound Rule for Remote Shutdown (TCP...	Remote Shutdown	All	No	Allow
Remote Volume Management - Virtual Di...	Remote Volume Management	All	No	Allow
Remote Volume Management - Virtual Di...	Remote Volume Management	All	No	Allow
Remote Volume Management (RPC-EPM...	Remote Volume Management	All	No	Allow
Routing and Remote Access (GRE-In)	Routing and Remote Access	All	No	Allow
Routing and Remote Access (L2TP-In)	Routing and Remote Access	All	No	Allow
Routing and Remote Access (PPTP-In)	Routing and Remote Access	All	No	Allow
Secure Socket Tunneling Protocol (SSTP-I...	Secure Socket Tunneling Pr...	All	No	Allow
SNMP Trap Service (UDP In)	SNMP Trap	Private...	No	Allow
SNMP Trap Service (UDP In)	SNMP Trap	Domain	No	Allow
Software Load Balancer Multiplexer (TCP...	Software Load Balancer	All	No	Allow
Start	Start	Domai...	Yes	Allow
Start	Start	Domai...	Yes	Allow
TPM Virtual Smart Card Management (D...	TPM Virtual Smart Card Ma...	Private...	No	Allow
TPM Virtual Smart Card Management (D...	TPM Virtual Smart Card Ma...	Domain	No	Allow
TPM Virtual Smart Card Management (TC...	TPM Virtual Smart Card Ma...	Domain	No	Allow
TPM Virtual Smart Card Management (TC...	TPM Virtual Smart Card Ma...	Private...	No	Allow

9. Results & Analysis

The implemented controls significantly improved SecureCart Health's security posture:

- Stronger passwords make credential compromise harder
- Brute-force attempts are now limited
- Security logs provide visibility into account activity
- Firewall rules reduce the number of available attack points
- Remote access services are now properly controlled

These changes create a more secure and manageable environment for the organisation.

10. Conclusion & Recommendations

This cybersecurity audit helped SecureCart Health strengthen its basic security controls. While these updates greatly reduce the organisation's risks, continuous improvement is important.

Recommended Next Steps:

- Provide annual Cybersecurity awareness training
- Review password and account policies every 90 days
- Regularly monitor security logs
- Implement centralised log management or a SIEM
- Continue to remove or disable unused services

Overall, the organisation is now much better protected against common threats.