Report Title: Issue Details
Run Date and Time: 2024-06-25 14:56:20 Pacific Daylight Time
Run by: System Administrator
Table name: sn_grc_issue

Issue

Number:	IPT0020005	State:	Closed Complete
Assignment group:	GRC Business Users	Substate:	
Assigned to:	Alan Offerman	Priority:	3 - Moderate
Issue source:	Ad-Hoc	Issue rating:	
Issue type:	Control design effectiveness failure	Issue group rule:	
Classification:	Compliance	Parent issue:	
Issue manager group:	Risk Managers	Configuration item:	
Issue manager:	Abel Tuter	Location:	

Name:

Compliance Defect

Description:

The IT department was not compliant regarding the length and combination of root/admin account passwords.

Is reparenting group:

false

Details

Control/Risk:	Password-based Authentication	Control Objective/Risk Statement:	Password-based Authentication
Entity:	Windows Server		
Policy:	Remote Access Control policy		
Authority document:	CIS Controls ® V8		

Recommendation:

Based on our audit findings, I recommend that the organization takes immediate action to address the non-compliance with remote access control as outlined in CIS Controls V8. This critical security control prevents unauthorized access to sensitive data and systems. I propose a comprehensive action plan to resolve this issue, which includes implementing multi-factor authentication, restricting remote access to necessary personnel, and conducting regular security audits.

Action plan:

Action Plan: Remediate Non-Compliance with Remote Access Control (CIS Controls V8)
Objective: Ensure remote access to organization systems and data is secure, auditable, and compliant with CIS Controls V8.

Tasks:
Conduct a thorough risk assessment:

Identify sensitive data and systems accessible via remote access.Evaluate potential risks and threats.
Implement Multi-Factor Authentication (MFA):
Choose an MFA solution that meets organizational requirements.Configure MFA for all remote access points.
Restrict Remote Access:
Limit remote access to necessary personnel and systems.Implement role-based access control.
Configure Secure Remote Access Protocols:
Ensure secure protocols (e.g., SSH, SFTP) are used for remote access.Disable unnecessary protocols.

Regular Security Audits:
Schedule regular security audits to monitor remote access controls.Identify and remediate potential security risks.
Develop Incident Response Plan:
Create a plan for responding to remote access security incidents.Define procedures for containment, eradication, and recovery.

Train Personnel:
Educate personnel on remote access security policies and procedures.Ensure understanding of MFA and secure remote access protocols.

Timeline:
Risk assessment: 1 weekMFA implementation: 2 weeksRemote access restriction and protocol configuration: 3 weeksSecurity audits: Ongoing (quarterly)Incident response plan development: 2 weeksPersonnel training: Ongoing (as needed)
Responsibility:
IT Security Team: Implement MFA, restrict remote access, and configure secure protocols.GRC Team: Conduct risk assessment, develop an incident response plan, and monitor compliance.Personnel: Complete training and adhere to remote access security policies.

Dates

Planned start date:	2024-06-25 10:53:37	Actual start date:	2024-06-25 11:49:33
Planned end date:	2024-06-26 10:53:37	Actual end date:	2024-06-25 14:53:22
Duration(duration):	1 Day	Actual duration:	3 Hours 3 Minutes
Confirmed date:	2024-06-25 11:49:27	Created:	2024-06-25 11:14:08
Due date:	2024-06-28 12:18:25	Closed:	2024-06-25 14:53:22

Response

Response:

Accept

Explanation:

I would recommend remediation to prevent a reoccurrence.

Activity

Work notes:

Additional comments:

Engagement

Engagement:

Confidentiality

Confidential:	false	Allowed users:	
		Allowed groups:	

Settings

Functional domain:

Risk Event

Risk event:

Regulatory Task

Regulatory task:

Related List Title: Indicator Result List
Table name: sn_grc_indicator_result
Query Condition: Issue = Compliance Defect AND Result = false
Sort Order: None

None

Related List Title: Task SLA List
Table name: task_sla
Query Condition: Task = Compliance Defect
Sort Order: None

1 Task SLAs

Task	SLA definition	Type	Target	Stage	Business time left	Business elapsed time	Business elapsed percentage	Start time	Stop time
IPT0020005	Due date breach on issue	SLA	Resolution	Completed	1 Day 25 Minutes	2 Hours 34 Minutes	9.53	2024-06-25 12:19:02	2024-06-25 14:53:22

Related List Title: Evidence List
Table name: sn_grc_advanced_evidence_response
Query Condition: Sys ID in
Sort Order: Number in ascending order

None