Assessment Summary and Recommendations

The assessment evaluated the overall security posture of the environment, identifying risks across authentication, package management, bootloader security, access controls, and peripheral device use. Several high-risk findings—including authentication hardening, package updates, GRUB boot protection, restricted console access, and USB storage controls—have been remediated and verified.

Key Improvements

- Improved alignment with NIST CSF 2.0 and CIS benchmarks.
- Reduced the attack surface and enhanced system resilience.
- Established a foundation for ongoing security governance and monitoring.

Action Items

1. Enforce secure password standards for all accounts; regularly review and update the module to align with current best practices.
2. Remove unnecessary or unsupported software and implement a regular patch management process to mitigate exposure to known vulnerabilities.
3. Configure GRUB so only authorized users can modify boot options or enter single-user mode; verify password configuration and restrict console access.
4. Enforce least privilege for /etc/sudoers.d and regularly audit sudo configuration to detect unauthorized changes.
5. Restrict USB device use through endpoint controls and monitoring; regularly review USB access policies to protect sensitive data.

Remaining Risks

System issues persist that could compromise security if not addressed promptly. Immediate remediation is recommended to maintain a hardened environment.

Future Recommendations

- Regular patching and configuration audits.
- Integration of configuration management and monitoring tools.
- Continuous adherence to industry security standards and best practices.