Cybersecurity Log Analysis - Complete Audit Report

System: DESKOFSKYCRAWLE
OS: Windows 11 Pro (Build 26200)
Collection Date: October 31, 2025, 18:50:32 UTC
Audit Period: 30 days
Analyst: Komal
Report Date: January 11, 2026

Executive Summary

This report presents a comprehensive security audit analysis of a Windows 11 Pro workstation. The audit covered a 30-day period and analyzed 77 log files across multiple security categories including event logs, network configuration, system information, security settings, persistence mechanisms, and risk indicators.

Overall Security Rating: ■■ MODERATE

The system demonstrates good security fundamentals but contains critical issues requiring immediate attention.

Table of Contents

System Overview

- **Hostname**: DESKOFSKYCRAWLE
- **Operating System**: Microsoft Windows 11 Pro (Build 26200)
- **Architecture**: 64-bit

- **User**: Bharat (MIS)
- **Auditor**: Meet
- **System Type**: Desktop workstation (Dell OptiPlex Tower 7010)
- **Memory**: 16 GB RAM
- **Network**: Connected to local network (192.168.68.106)
- **Last Boot**: October 31, 2025, 11:34:24 AM

Key Findings

Total Files Analyzed: 77

Categories: - Windows Event Logs: 4 files (~46,000+ events) - Network Logs: 8 files - System Information: 10 files - Security Audit: 6 files - Persistence Mechanisms: 7 files - Risk Signals: 10 files - Browser Analysis: Multiple files - Network Analysis: 6 files

---

Security Strengths

1. Windows Defender Status ■

- Real-time protection enabled
- Antivirus and antispyware active
- AMService running
- **Status**: GOOD

2. BitLocker Encryption ■

- OS volume (C:) encrypted (100%)
- Data volume (D:) encrypted (100%)
- Uses TPM + password protection
- **Status**: GOOD (with exception noted below)

3. Failed Login Attempts ■

- Only 1 failed login in 30 days
- No evidence of brute force attacks

- Low security risk
- **Status**: EXCELLENT

4. Firewall Configuration ■

- 695 rules configured
- Most remote access rules disabled
- Core networking rules properly configured
- **Status**: GOOD

Security Concerns

1. BitLocker Encryption - Volume E: ■■ HIGH RISK

Issue: Volume E: (SOC_Auditor, 58.58 GB) is NOT encrypted

Details: - Volume E: is fully decrypted (0% encrypted) - Protection is disabled - No key protectors configured - Contains potentially sensitive security audit data

Risk: Data theft if device is lost/stolen
Impact: High - Contains potentially sensitive security audit data
Recommendation: Enable BitLocker encryption immediately
Compliance: May violate data protection requirements

2. Local Administrator Accounts ■■ MEDIUM RISK

Issue: Built-in Administrator account is enabled

Details: - Default Administrator account is active - 2 total admin accounts (Administrator, Dell) - Well-known account name (easy to target)

Risk: Common attack vector
Impact: Medium
Recommendation: Disable or rename the Administrator account
Best Practice: Use separate admin accounts for administrative tasks

3. Windows Defender Scans ■■ LOW-MEDIUM RISK

Issue: No full scan has been performed (never run)

Details: - FullScanAge: 4294967295 (indicates never run) - QuickScanTime: Empty (not recorded) - Real-time protection is active

Risk: Potential undetected threats
Impact: Low-Medium
Recommendation: - Configure daily quick scans - Schedule weekly full scans - Monitor scan results

4. Remote Access Software ■■ MEDIUM RISK

Issue: AnyDesk remote access software installed

Details: - AnyDesk Service is running - Service set to Automatic startup - Multiple firewall rules allow AnyDesk connections - Active connections detected

Risk: Remote access capability (potential attack vector)
Impact: Medium - Increases attack surface
Recommendation: - Verify legitimate business need - Ensure proper access controls - Monitor AnyDesk connections - Consider disabling if not required

5. PowerShell History ■■ REQUIRES REVIEW

Issue: PowerShell history contains suspicious references

Details: - Reference to "kali" (Kali Linux penetration testing tool) - Some Linux commands attempted (apt-get) - Normal development activities also present

Risk: Potential security testing or unauthorized activity
Impact: Unknown - Requires investigation
Recommendation: - Review commands referencing "kali" - Verify no malicious activity - Clean history if needed

---

Critical Security Issues

Priority: HIGH

1. **Unencrypted Volume (Volume E:)**

2. **Action Required**: Enable BitLocker immediately

3. **Timeline**: Immediate

4. **Owner**: System Administrator

Priority: MEDIUM

1. **Default Administrator Account**

2. **Action Required**: Disable or rename account

3. **Timeline**: Within 1 week

Owner: System Administrator

AnyDesk Remote Access

6. **Action Required**: Review and justify usage

7. **Timeline**: Within 1 week

8. **Owner**: IT Security Team

Priority: LOW-MEDIUM

1. **Windows Defender Scans**

2. **Action Required**: Configure scheduled scans

3. **Timeline**: Within 2 weeks

4. **Owner**: System Administrator

Detailed Analysis

Windows Event Logs

Security Events (events_filtered_Security.csv) - File Size: 1,436,860 bytes (~1.4 MB) - Record Count: ~40,000 entries - Time Range: 30 days - Key Events: - Event ID 4672: Special privileges assigned (SYSTEM account - normal) - Event ID 4624: Successful logons - Event ID 4625: Failed logon attempts (1 detected) - Event ID 4648: Logon with explicit credentials

System Events (events_filtered_System.csv) - File Size: 144,316 bytes - Record Count: ~1,200 entries - Contains: System-level events, driver installations, service events

Application Events (events_filtered_Application.csv) - File Size: 224,018 bytes - Record Count: ~4,800 entries - Contains: Application-level events, errors, warnings

Network Security

Firewall Rules (firewall_rules.csv) - Total Rules: 695 - Status: Most remote access rules disabled (GOOD) - Concerns: Some rules enabled on Public profile - Recommendation: Review and minimize Public profile rules

Active Connections (netstat_ano.txt) - Multiple services listening on network interfaces - AnyDesk connections detected - SMB shares active - Recommendation: Review and document all listening services

SMB Shares - 6 shares configured (4 administrative, 2 printer) - No encryption enabled (EncryptData: False) - Recommendation: Enable SMB encryption for sensitive shares

System Configuration

Local Administrators (local_admins.csv) - 2 administrator accounts: 1. DESKOFSKYCRAWLE\Administrator (default - should be disabled) 2. DESKOFSKYCRAWLE\Dell (user account with admin privileges)

Installed Software (installed_software.csv) - 30+ applications installed - Notable software: - AnyDesk (remote access) - Google Chrome, Microsoft Edge - Python 3.13.1 - Microsoft Office LTSC Professional Plus 2024 - Sophos Client Authentication Agent - Visual Studio Code

Running Services (services_running.csv) - 200+ services - AnyDesk Service: Running, Automatic - Windows Defender services: Running - BitLocker Service: Running

Security Audit

Windows Defender Status - AMServiceEnabled: True ■ - AntispywareEnabled: True ■ - AntivirusEnabled: True ■ - RealTimeProtectionEnabled: True ■ - QuickScanTime: Empty ■■ - FullScanAge: 4294967295 (never run) ■■

BitLocker Status - Volume C: (OS) - Encrypted 100% ■ - Volume D: (Data) - Encrypted 100% ■ - Volume E: (SOC_Auditor) - Not encrypted ■■

Persistence Mechanisms

Registry Run Keys (persistence/registry_run_keys.csv) - 13 entries total - HKLM Run Keys: 3 (all legitimate system components) - HKCU Run Keys: 5 (legitimate installed software) - RunOnce Keys: 5 (cleanup tasks) - **Status**: All entries appear legitimate ■

Scheduled Tasks - Multiple scheduled tasks configured - Non-Microsoft tasks detected - Recommendation: Review all scheduled tasks for legitimacy

Risk Signals

Failed Logins (risk_signals/failed_logins.csv) - Total: 1 failed login in 30 days - Source: 127.0.0.1 (localhost) - **Status**: Low risk ■

PowerShell History (powershell_history.txt) - 49 commands recorded - Suspicious: "kali" reference - Normal: Python development, file navigation - **Status**: Requires review ■■

USB Devices (risk_signals/usb_disks.csv) - USB device detected: VendorCo ProductCode - Serial: 4140621173264166078 - Size: 62.9 GB

Recommendations

Immediate Actions (Priority: HIGH)

1. **Enable BitLocker on Volume E:**

2. Encrypt SOC_Auditor volume immediately

3. Use TPM or password protection

4. Backup recovery keys securely

Timeline: Within 24 hours

Review AnyDesk Usage:

7. Verify legitimate business need

8. Review access logs

9. Consider disabling if not required

Timeline: Within 48 hours

Investigate PowerShell History:

12. Review commands referencing "kali"

13. Verify no malicious activity

14. Clean history if needed

15. **Timeline**: Within 48 hours

Short-term Actions (Priority: MEDIUM)

1. **Disable Default Administrator Account:**

2. Disable or rename Administrator account

3. Use separate admin accounts

4. Implement least privilege

Timeline: Within 1 week

Configure Defender Scans:

7. Schedule daily quick scans

8. Schedule weekly full scans

9. Monitor scan results

Timeline: Within 1 week

Review Scheduled Tasks:

12. Verify all tasks are legitimate

13. Remove unnecessary tasks

14. Monitor task execution

15. **Timeline**: Within 2 weeks

Long-term Actions (Priority: LOW)

1. **Implement Log Monitoring:**

2. Set up centralized logging

3. Configure security alerts

4. Regular log review

Timeline: Within 1 month

Security Hardening:

7. Review firewall rules

8. Minimize attack surface

9. Update security policies

Timeline: Ongoing

Compliance Review:

12. Ensure encryption meets requirements

13. Document security controls

14. Regular security audits

15. **Timeline**: Quarterly

Compliance Considerations

Data Protection

- **Issue**: Unencrypted volume (Volume E:)
- **Impact**: May violate encryption requirements (GDPR, HIPAA, PCI-DSS)
- **Recommendation**: Encrypt all volumes containing sensitive data

Access Control

- **Issue**: Default Administrator account enabled
- **Impact**: Violates security best practices (NIST, CIS Benchmarks)
- **Recommendation**: Disable default accounts, use separate admin accounts

Monitoring

- **Issue**: Limited log monitoring
- **Impact**: Reduced visibility into security events
- **Recommendation**: Implement centralized logging and alerting

---

Conclusion

The system demonstrates **good overall security posture** with: - ■ Real-time antivirus protection active - ■ Most volumes encrypted (2 of 3) - ■ Low failed login attempts - ■ Firewall properly configured - ■ Legitimate persistence mechanisms

However, **critical issues** require immediate attention: - ■■ Unencrypted volume (Volume E:) - **HIGH PRIORITY** - ■■ Default Administrator account enabled - **MEDIUM PRIORITY** - ■■ Remote access software (AnyDesk) installed - **MEDIUM PRIORITY** - ■■ No Defender full scan performed - **LOW-MEDIUM PRIORITY**

Overall Security Rating: ■■ **MODERATE** (with critical issues requiring immediate action)

Next Steps

1. Address HIGH priority issues immediately (Volume E: encryption)
2. Review and address MEDIUM priority issues within 1 week
3. Implement LONG-TERM recommendations for ongoing security
4. Schedule follow-up audit in 30 days

Appendix

File Inventory

Total Files Analyzed: 77

By Category: - Windows Event Logs: 4 files - Network Logs: 8 files - System Information: 10 files - Security Audit: 6 files - Persistence Mechanisms: 7 files - Risk Signals: 10 files - Browser Analysis: Multiple files - Network Analysis: 6 files

Tools Used

- **VOLDEBUG** - Windows security audit collection tool
- **PowerShell** - File processing and analysis
- **Git** - Version control and documentation

Report Metadata

- **Report Generated**: January 11, 2026
- **Analysis Period**: October 1-31, 2025 (30 days)
- **System Audited**: DESKOFSKYCRAWLE
- **Analyst**: Komal

END OF REPORT