PyCyberShield

Security Assessment Report

Report Generated:	2025-08-18 14:21:25
Scan Timestamp:	2025-08-18T14:21:25.041416
Assessment Type:	Comprehensive Security Scan
Report Version:	1.0

Overall Security Risk Level: High

Executive Summary

PyCyberShield conducted a comprehensive security assessment of the target environment. The assessment analyzed system processes, network configurations, and system logs to identify potential security risks and vulnerabilities. The overall security risk level is assessed as **High** based on 1 security findings across multiple categories. This assessment provides detailed analysis of system security, network vulnerabilities, and suspicious activities detected in system logs. Immediate attention should be given to high-risk findings, and all recommendations should be implemented according to organizational security policies and compliance requirements.

Key Security Metrics

Metric	Value
Suspicious Processes	345
Brute Force Attacks	0
Suspicious Log Entries	0
Overall Risk Level	High

Detailed Security Findings

System Security Analysis

Analyzed 347 running processes, found 345 suspicious processes.

Suspicious Processes Detected:

• kthreadd (PID: 2, CPU: 0.0%)
• pool_workqueue_release (PID: 3, CPU: 0.0%)
• kworker/R-kvfree_rcu_reclaim (PID: 4, CPU: 0.0%)
• kworker/R-rcu_gp (PID: 5, CPU: 0.0%)
• kworker/R-sync_wq (PID: 6, CPU: 0.0%)
• kworker/R-slub_flushwq (PID: 7, CPU: 0.0%)
• kworker/R-netns (PID: 8, CPU: 0.0%)
• kworker/0:0H-events_highpri (PID: 10, CPU: 0.0%)
• kworker/R-mm_percpu_wq (PID: 13, CPU: 0.0%)
• rcu_tasks_kthread (PID: 14, CPU: 0.0%)

Log Analysis Results

Found 0 suspicious log entries and detected 0 brute force attacks.

Compliance Mapping

Findings mapped to compliance frameworks:

Suspicious Processes
• ISO27001: Not Mapped
• NIST_CSF: Not Mapped

Security Recommendations

1. URGENT: Address all high-risk findings immediately.
2. Implement regular security monitoring and automated alerting systems.
3. Conduct periodic security assessments to identify new vulnerabilities.
4. Ensure all security services (firewall, antivirus) are active and updated.
5. Monitor system logs for suspicious activities and brute-force attacks.
6. Implement strong access controls and multi-factor authentication.
7. Regularly update and patch all system components and applications.
8. Establish incident response procedures for security events.
9. Provide security awareness training for all users.

Technical Appendix

This section contains detailed technical data from the security assessment.

Scan Summary:

• scan_completed: 2025-08-18T14:21:25.334466
• modules_run: ['system_security', 'network_security', 'log_analysis', 'risk_assessment', 'encryption']
• overall_status: completed
• output_directory: reports