PyCyberShield

Security Assessment Report

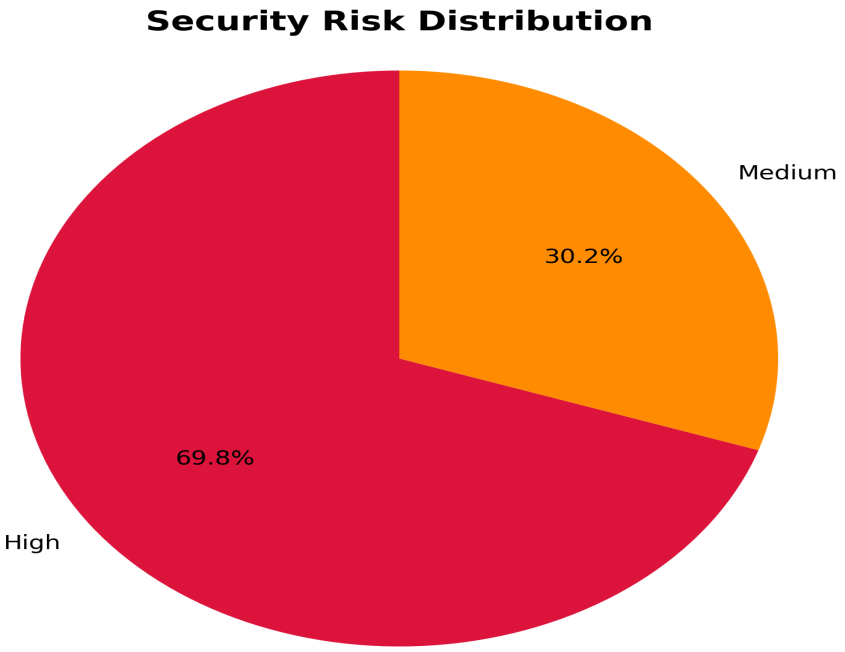
Report Generated:	2025-08-29 13:43:10
Scan Timestamp:	2025-08-29T13:25:51.340154
Assessment Type:	Comprehensive Security Scan
Report Version:	1.0

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 3 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.

Risk Distribution Overview



Key Security Metrics

Metric	Value
Suspicious Processes	42
Unusual Open Ports	7
Brute Force Attacks	2
Suspicious Log Entries	18
Overall Risk Level	High

Detailed Security Findings

System Security Analysis

Analyzed 330 running processes, found 42 suspicious processes.

Suspicious Processes Detected:

• pool_workqueue_release (PID: 3, CPU: 0.0%)
• idle_inject/0 (PID: 22, CPU: 0.0%)
• cpuhp/0 (PID: 23, CPU: 0.0%)
• cpuhp/1 (PID: 24, CPU: 0.0%)
• idle_inject/1 (PID: 25, CPU: 0.0%)
• cpuhp/2 (PID: 30, CPU: 0.0%)
• idle_inject/2 (PID: 31, CPU: 0.0%)
• cpuhp/3 (PID: 36, CPU: 0.0%)
• idle_inject/3 (PID: 37, CPU: 0.0%)
• cpuhp/4 (PID: 42, CPU: 0.0%)

Network Security Analysis

Unusual Open Ports Detected:

• Host 127.0.0.1: Ports 5763, 5939, 8834, 9000, 11434, 53755, 57621

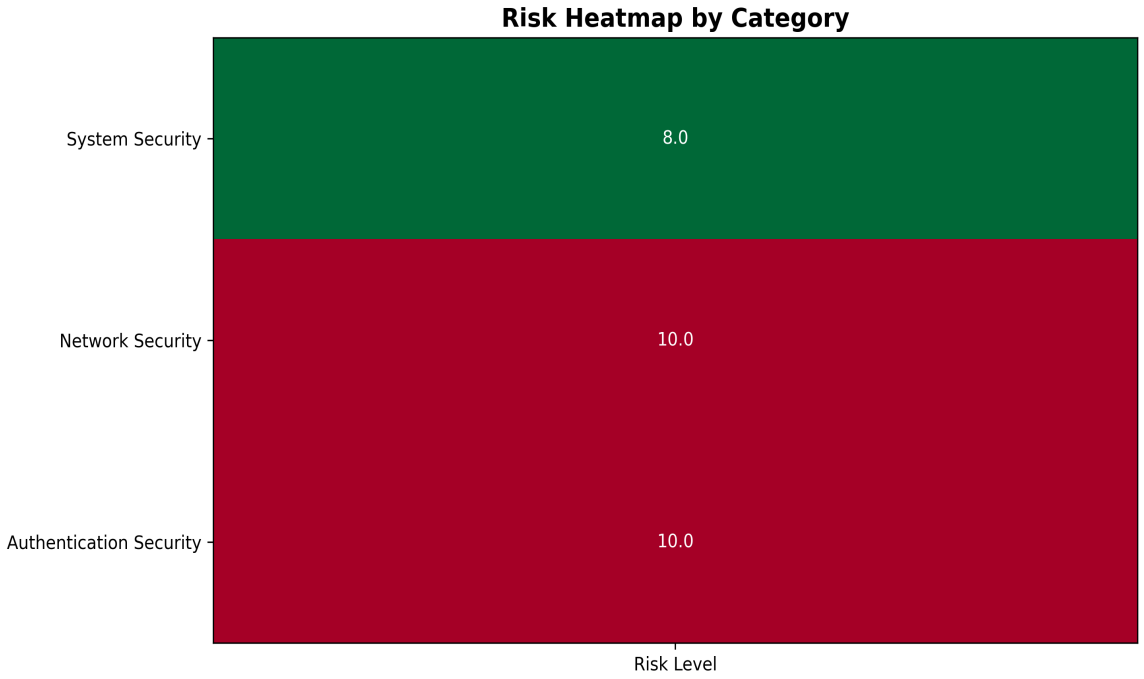
Log Analysis Results

Found 18 suspicious log entries and detected 2 brute force attacks.
■■ Brute force attacks detected - immediate attention required.

Risk Assessment

Overall Risk Level: **High**

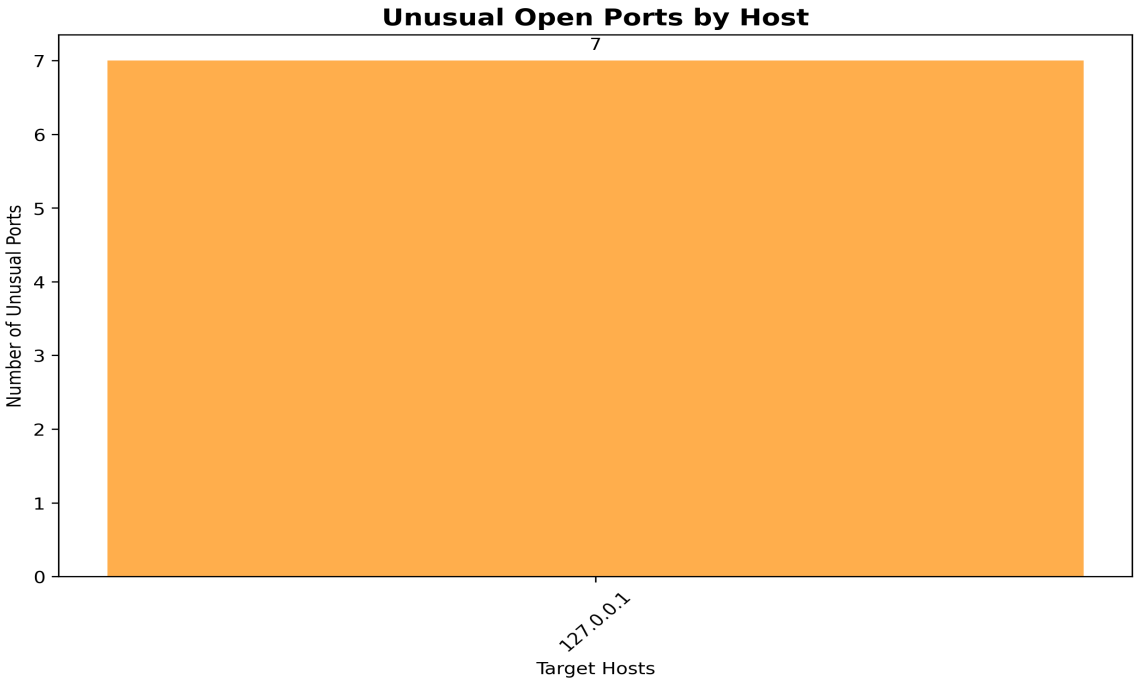
Risk Analysis by Category



Network Security Analysis

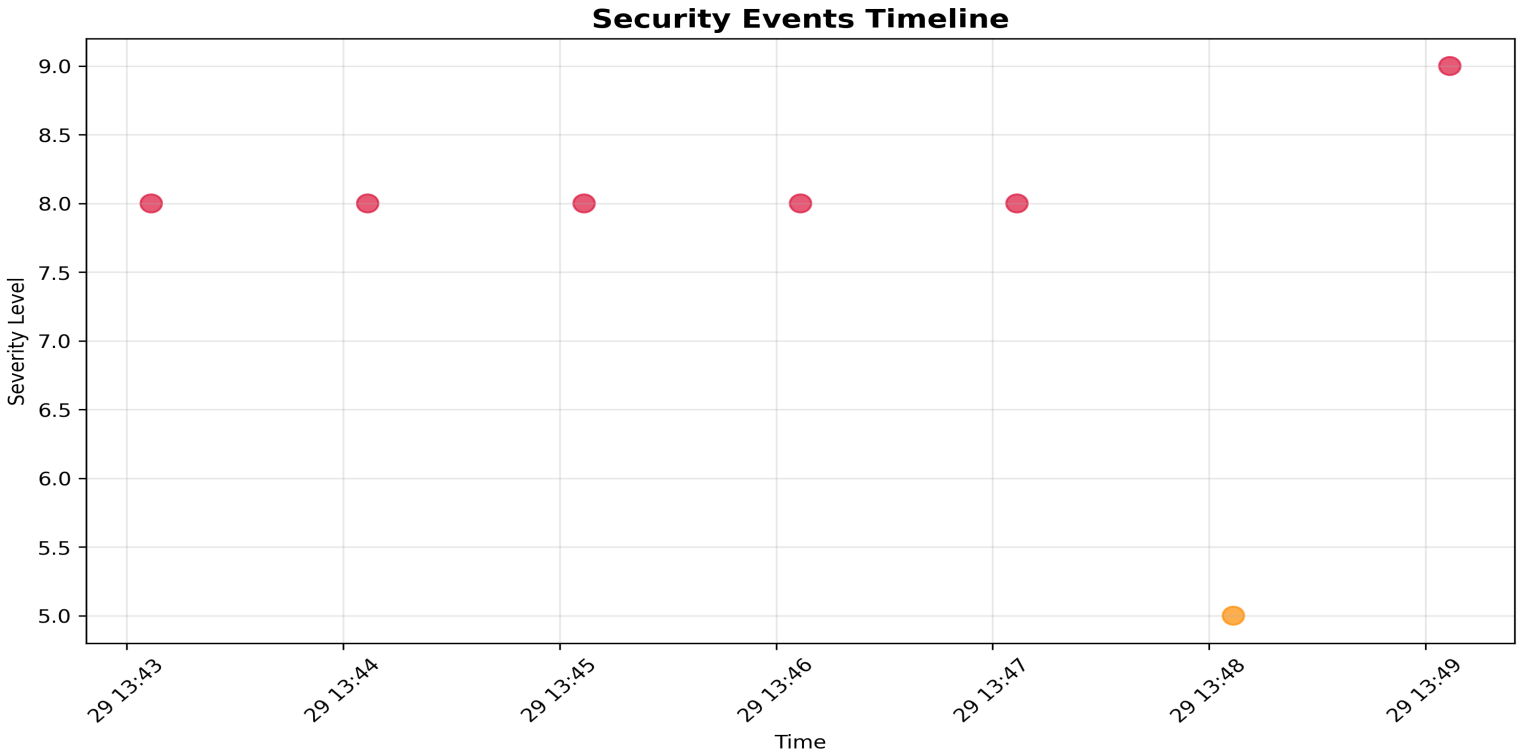
Network security analysis revealed unusual port configurations that require attention.

Network Port Analysis



Security Events Timeline

The following chart shows the timeline of security events detected during the assessment.



Compliance Mapping

Findings mapped to compliance frameworks:

Suspicious Processes
• ISO27001: A.12.2 - Protection from malware
• NIST_CSF: PR.PT-1: Audit/log records are determined

Unusual Open Ports
• ISO27001: A.13.1 - Network security management
• NIST_CSF: PR.AC-4: Access permissions and authorizations

Brute Force Attacks
• ISO27001: A.9.4 - System and application access control
• NIST_CSF: PR.AC-7: Users, devices, and other assets are authenticated

Security Recommendations

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

Technical Appendix

This section contains detailed technical data from the security assessment.

Scan Summary:

• scan_completed: 2025-08-29T13:43:05.604981
• modules_run: ['system_security', 'network_security', 'log_analysis', 'risk_assessment', 'encryption']
• overall_status: completed
• output_directory: reports