■■ ThreatOps SOC Report

Report Type:	Daily Summary
Generated:	2025-10-28 00:42:27
Period:	2025-10-27 to 2025-10-28

■ Executive Summary

Metric	Value
Total Alerts	175
Critical Alerts	16
High Alerts	17
Average Risk Score	95.86

■ Security Alerts

Rule Name	Severity	Host	IP	MITRE Techniqu
ML Anomaly Detection	High	WIN-PC01	192.168.1.100	T1055
ML Anomaly Detection	High	WIN-PC08	192.168.1.100	T1055
ML Anomaly Detection	High	WIN-PC02	192.168.1.100	T1055
ML Anomaly Detection	High	WIN-PC07	192.168.1.100	T1055
Privilege Escalation	Critical	WIN-PC03	unknown	T1078
Privilege Escalation	Critical	WIN-PC09	unknown	T1078
Privilege Escalation	Critical	WIN-PC01	unknown	T1078
Privilege Escalation	Critical	WIN-PC07	unknown	T1078
Privilege Escalation	Critical	WIN-PC07	unknown	T1078
Privilege Escalation	Critical	WIN-PC05	unknown	T1078
Privilege Escalation	Critical	WIN-PC08	unknown	T1078
ML Anomaly Detection	Medium	WIN-PC09	45.146.164.110	T1055
ML Anomaly Detection	Medium	WIN-PC05	45.146.164.110	T1055
ML Anomaly Detection	Medium	WIN-PC07	103.41.12.77	T1055
ML Anomaly Detection	Medium	WIN-PC06	103.41.12.77	T1055

ML Anomaly Detection	Medium	WIN-PC08	45.146.164.110	T1055
ML Anomaly Detection	Medium	WIN-PC07	103.41.12.77	T1055
ML Anomaly Detection	Medium	WIN-PC02	45.146.164.110	T1055
ML Anomaly Detection	Medium	WIN-PC10	45.146.164.110	T1055
ML Anomaly Detection	Medium	WIN-PC06	198.96.155.3	T1055

■ Recommendations

Implement Privilege Management - Critical
Implement proper privilege management to prevent unauthorized escalation.

Implement Account Lockout Policy - High
Configure account lockout policies to prevent brute force attacks.