

Cybersecurity Security Report

Report Type:	Comprehensive
Time Range:	24h
Generated:	2026-01-03 17:08:29
System:	AI-Powered Cybersecurity Platform

Executive Summary

During the 24h reporting period, the cybersecurity system processed 31 security events. • Critical incidents: 7 • High severity incidents: 8 • Medium severity incidents: 12 The system maintained continuous monitoring and automated response capabilities.

Recent Security Events

Timestamp	Type	Severity	Description
2026-01-03 16:46:37	incident_classified	high	AI classified incident: malware_infection
2026-01-03 16:40:02	incident_classified	medium	AI classified incident: suspicious_activity
2026-01-03 16:32:22	incident_classified	medium	AI classified incident: suspicious_activity
2026-01-03 15:31:24	incident_classified	medium	AI classified incident: suspicious_activity
2026-01-03 15:30:18	incident_classified	medium	AI classified incident: suspicious_activity
2026-01-03 15:30:15	incident_classified	medium	AI classified incident: suspicious_activity
2026-01-03 15:29:25	brute_force_attack	medium	SSH brute force attack from 203.0.113.45 - 342 failed attempt
2026-01-03 15:29:25	apt_activity	high	Advanced Persistent Threat indicators - Lazarus Group TTPs detected
2026-01-03 15:29:25	data_exfiltration	critical	Large data transfer detected to suspicious IP 212.60.192.186
2026-01-03 15:29:25	suspicious_network_t	medium	Unusual DNS queries to suspicious domains detected
2026-01-03 15:29:25	data_exfiltration	critical	Large data transfer detected to suspicious IP 192.227.74.134
2026-01-03 15:29:25	brute_force_attack	medium	SSH brute force attack from 203.0.113.45 - 342 failed attempt
2026-01-03 15:29:25	policyViolation	low	Data Loss Prevention policy violation - sensitive data in email
2026-01-03 15:29:25	brute_force_attack	medium	SSH brute force attack from 203.0.113.45 - 342 failed attempt
2026-01-03 15:29:25	vulnerability_scan	info	Scheduled vulnerability scan completed - 3 medium findings
2026-01-03 15:29:25	malware_detected	medium	Trojan.GenKryptik detected in downloaded file
2026-01-03 15:29:25	suspicious_network_t	medium	Unusual DNS queries to suspicious domains detected
2026-01-03 15:29:25	data_exfiltration	critical	Large data transfer detected to suspicious IP 208.129.47.251
2026-01-03 15:29:25	phishing_campaign	high	Targeted spear-phishing campaign detected - 47 emails blocked
2026-01-03 15:29:25	data_exfiltration	critical	Large data transfer detected to suspicious IP 218.84.131.158

Security Recommendations

- Continue monitoring for critical and high-severity incidents
- Review and update security policies regularly
- Ensure all security tools are functioning properly
- Maintain regular security awareness training
- Implement multi-factor authentication where possible
- Keep all systems and software updated
- Regular backup and recovery testing
- Network segmentation and access controls review