■ Security Report

Generated:	2026-01-03 17:12:29
Time Range:	24h
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 attemp
2026-01-03 15:29:25	apt_activity	high	Advanced Persistent Threat indicators - Lazarus Group TTPs d
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 attemp
2026-01-03 15:29:25	policy_violation	low	Data Loss Prevention policy violation - sensitive data in em
2026-01-03 15:29:25	brute_force_attack	medium	SSH brute force attack from 203.0.113.45 - 342 failed attemp
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 blocke
2026-01-03 15:29:25	data_exfiltration	critical	Large data transfer detected to suspicious IP 218.84.131.158

Security Recommendations

• * **• Isolate and Forensically Image Affected Systems from Data Exfiltration Incident(s):** Immediately isolate any systems involved in the data exfiltration incidents from the network to prevent further data loss. Create a forensic image of these systems for thorough investigation and evidence preservation.
• * **• Implement Multi•Factor Authentication (MFA) on All External•Facing Services:** The presence of brute•force attacks indicates a weakness in authentication. Enforce MFA on all services accessible from the internet, including VPN, email, and remote access portals, to significantly reduce the risk of successful brute•force attacks.
• * **• Deploy Intrusion Detection/Prevention System (IDS/IPS) Rules Targeted at Identified APT Activity:** Based on identified APT (Advanced Persistent Threat) activity, research and deploy specific IDS/IPS rules and signatures to detect and prevent further malicious activity associated with that specific APT group or identified tools/techniques. Update these rules regularly.
• * **• Review and Restrict Network Traffic Based on Suspicious Network Traffic Analysis:** Analyze the "suspicious network traffic" logs and identify patterns (e.g., unusual ports, protocols, destinations). Implement firewall rules to restrict or block this traffic based on the identified anomalies.
• * **• Segment Network to Limit Lateral Movement:** Segment the network into distinct zones based on function and sensitivity. This limits the potential damage of successful attacks by restricting lateral movement. For example, segment critical servers from user workstations.
• * **• Conduct Security Awareness Training Focused on Phishing and Social Engineering:** Since APTs often use phishing as an entry point, provide targeted security awareness training to employees. This training should cover identifying phishing emails, avoiding suspicious links, and reporting potential threats. Include practical exercises and simulations.
• * **• Enhance Logging and Monitoring for Data Exfiltration Attempts:** Implement or enhance data loss prevention (DLP) mechanisms. Configure alerts for unusual file access patterns, large data transfers, or attempts to copy data to removable media. Centralize log collection and analysis to improve visibility into potential data exfiltration activities.