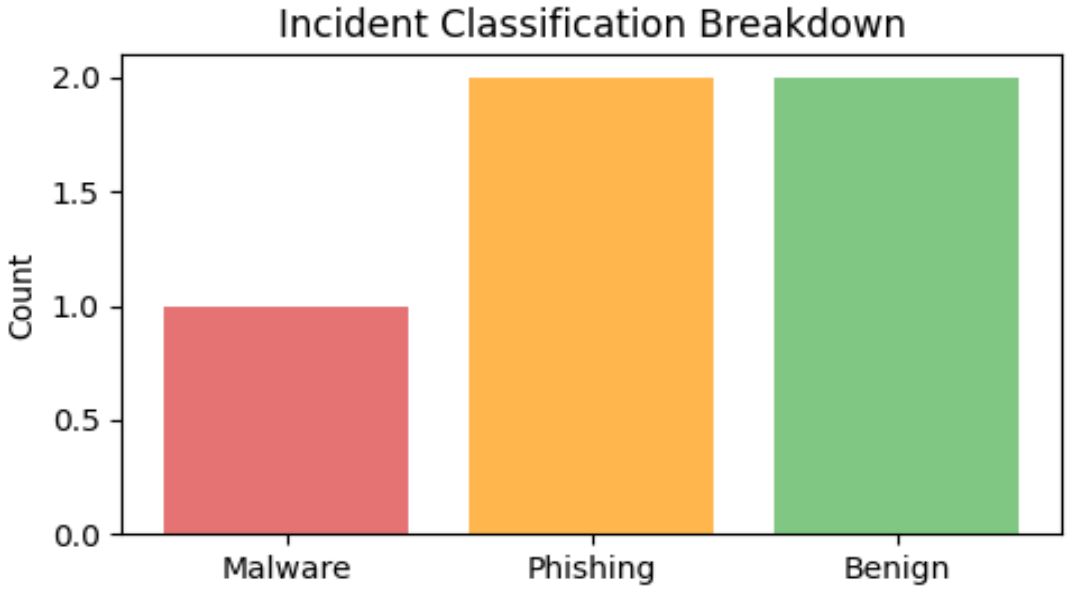
SOC Incident Report

Generated: 2025-09-09T19:02:33.176391 UTC

Executive Summary:
Total Alerts: 5
Malware: 1 Phishing: 2 Suspicious IP: 0 Benign: 2



Top Incidents

Alert ID	Timestamp	Source IP	Destination IP	URL	Classification	Recommended Action
1	2025-09-01T12:20:11	192.168.1.10	8.8.8.8	http://malicious-site.com	Malware	Isolate host, collect memory image, block hash on EDR, escalate to IR team
2	2025-09-01T12:21:15	10.0.0.5	13.107.21.200	http://login.microsoft.com	Phishing	Block URL/IP at proxy/firewall, force password reset for impacted users, scan mailbox
3	2025-09-01T12:23:40	172.16.0.7	142.250.185.14	http://phishingsite.xyz	Phishing	Block URL/IP at proxy/firewall, force password reset for impacted users, scan mailbox
4	2025-09-02T08:11:02	203.0.113.5	93.184.216.34	https://benign.example.com	Benign	Monitor and close if no further alerts
5	2025-09-03T14:45:00	10.10.10.10	192.0.2.50	http://suspicious-domain.test	Benign	Monitor and close if no further alerts