Security Event Log Review Checklist

Review Details

- □ Event log sources identified and collected
- □ Time range of logs is appropriate
- □ Critical systems’ logs reviewed
- □ Third-party/service logs included

Event Types Checked

- □ Unauthorized access attempts (failed logins, privilege escalations)
- □ Account lockouts or suspicious account activity
- □ Changes to system configurations or security settings
- □ Malware or security software alerts
- □ Network anomalies or unexpected connections
- □ Other detected suspicious or abnormal activities

Remediation & Reporting

- □ Detected issues investigated and documented
- □ Incidents escalated as necessary
- □ Log review activities documented

Notes

Add notes or findings here...

Reviewed by:

Name & Signature

Date: