## Audits and log reports of network

Identifying and recording security incidents, intrusions, and attempts

Regularly review logs and audit reports for suspicious activity. This includes looking for unusual login attempts, unauthorized access to sensitive data, and changes to critical system configurations.

Use a log management tool to collect and centralize logs from multiple sources. This will make it easier to search and analyze logs for patterns of suspicious activity.

Correlate logs with other security indicators, such as network traffic and firewall alerts. This can help to identify the scope of a security incident and determine its root cause.

Document all security incidents in a detailed incident report. This report should include the date and time of the incident, the type of incident, the affected systems, the impact of the incident, and the steps taken to remediate the incident.

Share incident reports with appropriate stakeholders. This will help to ensure that everyone is aware of the incident and can take steps to prevent similar incidents from happening in the future.

Performance tests to modify and debug

Review logs and audit reports to identify performance bottlenecks. This includes looking for long-running queries, slow database access times, and inefficient code.

Use a performance testing tool to simulate real-world user traffic and measure the performance of your application. This can help to identify performance issues that may not be apparent during manual testing.

Analyze performance test results to identify areas for improvement. This may involve modifying code, optimizing database queries, or upgrading hardware.

Document performance test results and recommendations for improvement. This will help to track progress and ensure that performance issues are addressed in a timely manner.

Countermeasures

Review logs and audit reports to identify potential security vulnerabilities. This includes looking for missing patches, weak passwords, and misconfigured security settings.

Implement countermeasures to address identified vulnerabilities. This may involve installing patches, changing passwords, and updating security settings.

Verify that countermeasures have been implemented correctly. This can be done by rescanning systems for vulnerabilities or by performing penetration testing.

Document countermeasures and their implementation status. This will help to track progress and ensure that vulnerabilities are addressed in a timely manner.

Spot checks and audits

Conduct regular spot checks to ensure that security procedures are being followed. This includes checking for compliance with password policies, access control policies, and data handling procedures.

Perform periodic audits to assess the overall security posture of your organization. This includes reviewing policies and procedures, testing security controls, and identifying potential risks.

Document audit findings and recommendations for improvement. This will help to track progress and ensure that security risks are addressed in a timely manner.