TIPS FOR CREATING A STRONG CYBERSECURITY ASSESSMENT REPORT

This cheat sheet offers advice for creating a strong report as part of your penetration test, vulnerability assessment, or an information security audit.

General Approach to Creating the Report

1. Analyze the data collected during the assessment to identify relevant issues.
2. Prioritize your risks and observations; formulate remediation steps.
3. Document the assessment methodology and scope.
4. Describe your prioritized findings and recommendations.
5. Attach the relevant figures and data to support the main body of your report.
6. Create the executive summary to highlight the key findings and recommendations.
7. Proofread and edit the document.
8. Consider submitting the report draft to weed out false positives and confirm expectations.
9. Submit the final report to the intended recipient using agreed-upon secure transfer mechanism.
10. Discuss the report's contents with the recipient on the phone, teleconference, or in person.

Analysis of the Security Assessment Data

Share your insights beyond regurgitating the data already in existence.

Consider what information provided to you is incomplete or might be a lie or half-truth.

Look for patterns by grouping your initial findings by the affected resources, risk, issue category, etc.

Identify for trends that highlight the existence of underlying problems that affect security.

If examining scanner output, consider exploring the data using spreadsheets and pivot tables.

Fill in the gaps in your understanding with follow-up scans, documentation requests, and interviews.

Involve colleagues in your analysis to obtain other people's perspectives on the data and conclusions.

Assessment Methodology Documentation

Document the methodology used to perform the assessment, analyze data, and prioritize findings.

Demonstrate a systemic and well-reasoned assessment and analysis approach.

Clarify the type of the assessment you performed: penetration test, vulnerability assessment, etc.

If applicable, explain what tools you used and how they were configured.

If applicable, describe what approach guided the questions you asked during interviews.

Describe the criteria you used to assign severity or criticality levels to the findings of the assessment.

Refer to the relevant frameworks you used to structure the efforts (PCI DSS, ISO 27001, etc.).

Scope of the Security Assessment

Specify what systems, networks and/or applications were reviewed as part of the security assessment.

State what documentation you reviewed, if any.

List the people whom you interviewed, if any.

Clarify the primary goals of the assessment.

Discuss what contractual obligations or regulatory requirements were accounted for in the assessment.

Document any items that were specifically excluded from the assessment's scope and explain why.

Documenting Conclusions

Include both negative and positive findings.

Account for the organization's industry, business model, and compliance requirements.

Stay consistent with the methodology and scope.

Prioritize the findings related to security risks and remediation steps.

Provide a practical remediation path, accounting for the organization's strengths and weaknesses.

Qualities of a Good Assessment Report

Open with a strong executive summary that a non-technical reader can understand.

Provide meaningful analysis, instead of merely presenting the output of the assessment tools.

Include the figures to support your analysis, placing non-critical information in the appendix.

Craft a professional, easy-to-follow look.

Offer remediation guidance beyond merely pointing out security problems.

Find and fix your typos. Ask for help, if you can.

Structure the report in logical sections to accommodate the different types of readers.

Additional Assessment Report Tips

Create templates based on prior reports, so you don't have to write every document from scratch.

Safeguard (encrypt) the report when storing and sending it, since its contents are probably sensitive.

Use concrete statements; avoid passive voice.

Explain the significance of your findings in the context of current threats and recent events.

Put effort into making the report as brief as possible without omitting important and relevant contents.

More Security Assessment Tips

Qualities of a Good Information Security Report

Tips for a Strong Executive Summary of a Security Assessment Report

Security Assessment Report as Critique, Not Criticism

Why Your Security Assessment Recommendations Get Ignored

Training to Improve Your Writing

Lenny Zeltser, the author of this cheat sheet, created a writing course for cybersecurity professionals, which you can take from SANS Institute.

Authored by Lenny Zeltser, who has written his share of security assessment and other reports. Thanks for the feedback on this cheat sheet to Dave Shackleford and John Strand. You're looking at version 1.1 of this document. For more security cheat sheets see zeltser.com/cheat-sheets.