TIPS FOR CREATING AN INFORMATION SECURITY ASSESSMENT REPORT

This cheat sheet presents recommendations for creating a strong report as part of an information security assessment project.

General Approach to Creating the Report

1. Analyze the data collected during the security assessment to identify relevant issues.
2. Prioritize your risks and observations; formulate remediation steps.
3. Document the sections of the report detailing the assessment methodology and scope.
4. Document the sections of the report describing your findings and recommendations.
5. Attach relevant figures and raw data to support the main body of the report.
6. Create the executive summary to highlight the key findings and recommendations.
7. Proof-read and edit the document.
8. Consider submitting the report’s 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 or in person.

Analysis of the Security Assessment Data

Your analysis should provide value beyond regurgitating the data already in existence.
Consider what information provided to you is incomplete or might be a lie or half-truth.
Group initial findings based on affected resources, risk, issue category, etc. to look for patterns.
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.

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

Qualities of a Good Assessment Report

Starts with a strong executive summary that a non-technical reader can understand
Provides meaningful analysis, rather than merely presenting the output of assessment tools
Includes supporting figures to support the analysis
Describes assessment methodology and scope
Looks professional and is without typos
Offers remediation guidance beyond merely pointing out security problems
Is structured in logical sections to accommodate the different groups who’ll read and act upon it

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 the security findings in the context of current threats and events.
Put effort into making the report as brief as possible without omitting important and relevant contents.

More Security Assessment Tips

6 Qualities of a Good Information Security Report: http://j.mp/m3AK9r
4 Tips for a Strong Executive Summary of a Security Assessment Report: http://j.mp/jsT669
Security Assessment Report as Critique, Not Criticism: http://j.mp/m6e6p0
Dealing with Misinformation During Security Assessments: http://j.mp/jv8jxz

Authored Lenny Zeltser, who writes a daily security blog at blog.zeltser.com; you can also find him on Twitter as @lennyzeltser. This cheat sheet was reviewed by Dave Shackleford and John Strand. It’s distributed according to the Creative Commons v3 “Attribution” License. You’re looking at version 1.0 of this document. For more security cheat sheets see http://j.mp/mrGgHJ.