

Including Key Elements in a Report



Gavin Johnson-Lynn

Software Developer, Offensive Security Specialist

@gav_jl www.gavinjl.me



Overview



Other report sections

Why are they there?



Who Are We Focusing On?



Chris: I.T. Manager

- High-level results
- Impact on the business
- What are the risks?

Business responses

- Not all technical
- Are processes in place?
- Any purchases or training requires?

Revisiting the Goals



Detail the vulnerabilities

- Done the technical side
- Help the business to understand them

Stated the mitigations

- Done the technical side
- Business requires context

Highlighting the risks

- Targets the business, not technical
- Need to address this

Third Party Test vs. Internal Team Test

Internal pen test team

Different report structure

More well-defined audience

Third party contract

Unknown technical /
security knowledge

Target less technical abilities



Test Details



High level information about the test

Why?

- Give context
- Understand why it was performed
- What was and wasn't tested

Scope

Scope document is the source

Agreement between two companies
Include key information from this

**Be clear about
what was tested**

When was testing performed

Identify genuine / test activity

Testing methodologies

Use links and appendices for detail
E.g. checklists like ASVS



Technical Team



Pen testers involved in the test

- Point of contact
- Transparency
- How qualified are they?

Caveats

Reasons the scope may not be followed

Anything not tested?

Must tell the client

Goal: Highlight the business risks



Test Limitations

**Limited
timescale**

**Point-in-time
results**

**Goal: Highlight
the risks**



Executive Summary



Key section to present risks

What do the findings mean to the business?

Draw conclusions from findings

Remove technical detail



Executive Summary

What could a genuine attacker do?

Focus on biggest impacts

Chain together findings

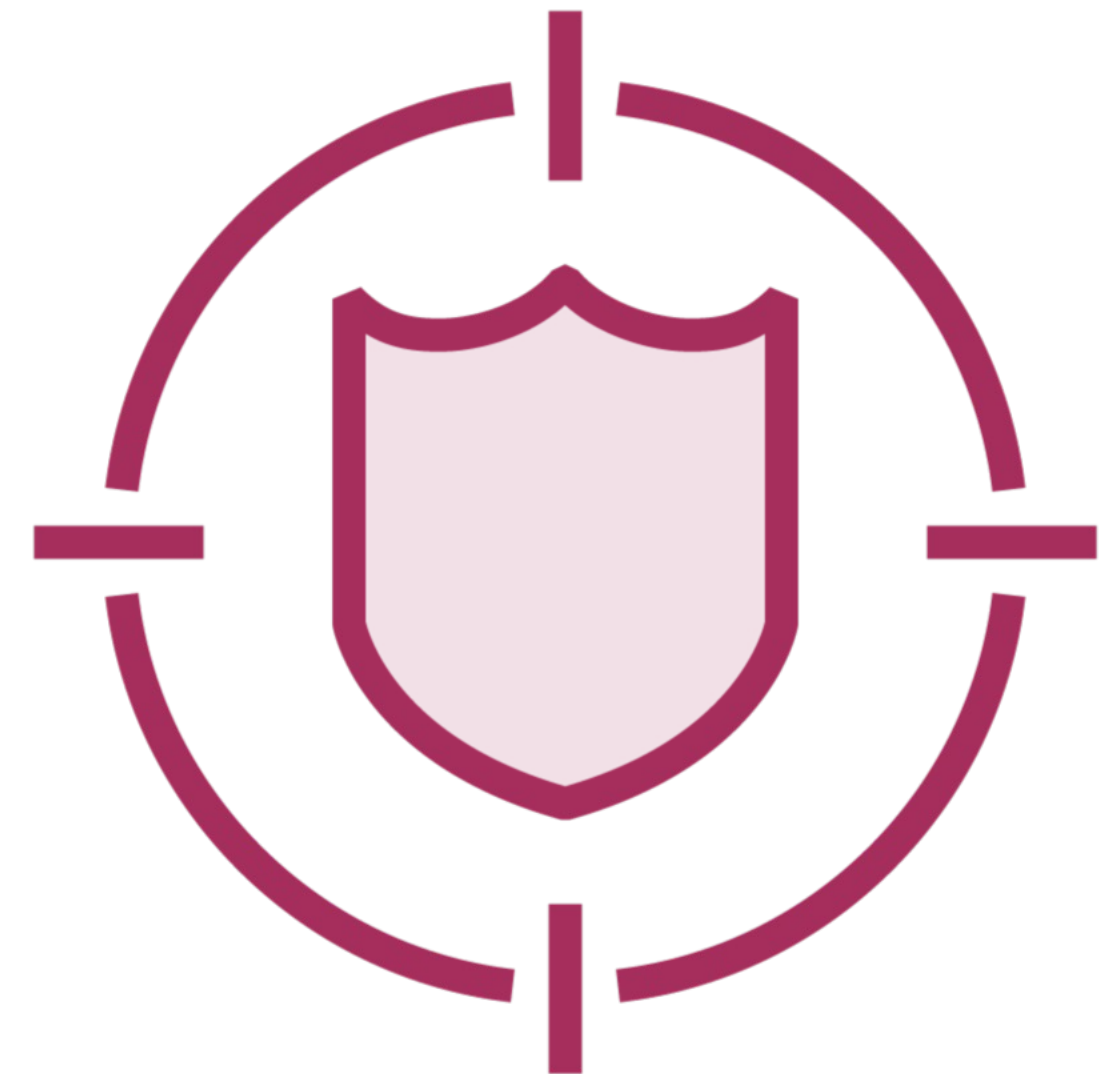
Show greater impact

Detail a path to damage

Potential repercussions

Impacts on the business

The path an attacker could take



Executive Summary – Why?



Detail the key risks

Highlight the importance of fixing them

Direction for mitigations

Touching on all 3 goals:

- Detail the vulnerabilities
- State the mitigations
- Highlight the risks

“Someone checked this report
for errors, that’s what I like to see!”
(Chris, I.T. Manager)



Appendices



Supplying additional information

- Keep the main sections concise
- Transparency
- Assist with repeatability

Include if it:

- Helps detail vulnerabilities
- States / assist with mitigations
- Highlights risks

Summary



Lots of non-technical focus

- Can be difficult for pen testers

Chris: I.T. Manager

- Executive summary is very important

Vincent: Senior Security Engineer

- Understand business risks
- More on mitigations and repeatability

