

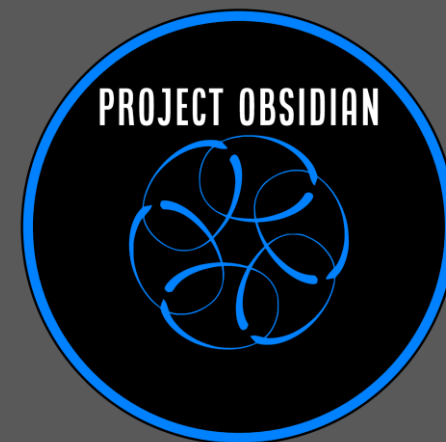


Project Obsidian

Incident Response

Final Reporting Made Exciting*

*Insert eye catching and compelling abstract on IR final reporting here.
Make it seem exciting and not at all a dreaded yet critical part of incident handling.



Incident Response Lifecycle

- Preparation
- Detection / Analysis
- Containment
- Eradication
- Recovery
- Post Incident Activities – You are here!

What goes into a final report?

- Executive Summary
- Detection and Analysis
- Containment
- Eradication
- Recovery
- Lessons Learned

Executive Summary

- Audience
 - Executive Leadership Team
- Components
 - Story
 - Communicate what happened in terms your audience will understand.
 - Impacts, business, operations, legal, reputation...
 - High-level timeline
 - Save the gory details for the technical teams
 - Ensure the leadership team knows the highlights
 - Recommendations
 - Define strategic and tactical tasks
 - This is how you ask the business to take action
- Annex or separate document
 - Full timeline
 - IOC

Detection and Analysis

- Audience

- Technical Leaders and Peers

- Components

- Detections

- List what was detected and how.
 - User report, external report, SIEM alarm?

- Analysis

- Document actions taken!

- Opportunities

- What could have been done better?
 - What would help detections next time?

Containment

- Audience

- Technical Leaders and Peers

- Components

- Actions Taken

- List what was was done to stop the bleeding.
 - Locked accounts, isolated hosts, etc..

- Opportunities

- What would help in the future?
 - Missing tooling, limited people resources?

Eradication

- Audience

- Technical Leaders and Peers

- Components

- Actions Taken

- How was the adversary removed from the environment?
 - Password resets, system rebuilds, etc..

- Opportunities

- What would help in the future?
 - Missing tooling, limited people resources?

Recovery

- Audience

- Technical Leaders and Peers

- Components

- Actions Taken

- How did we get back to business?
 - Testing that business and technical processes are working again

- Opportunities

- What would help in the future?
 - Missing tooling, limited people resources?
 - Did our backups restore and work?

Post-Incident Activities

- Audience

- Executives, Technical Leaders, and Peers

- Components

- Reporting
 - That's all of the above!
 - Opportunities
 - What would help in the future?
 - Document strategic and tactical recommendations

Reporting Pro-Tips!

- Use a template
 - This ensures consistency and completeness
- Just the facts, please!
 - Stick to what you can prove with the available data
 - Understand you may not have enough data and call that out
- Write out findings in report format as you work
 - This will save you time later and helps to keep you on track
- Map to framework used by your company (NIST, ISO2700x, MITRE...)
- Normalize time!
 - UTC is the only time zone :D

Kill Chain 3 Final Report

Demo Time!



Wrapping it up! - KC3 Recommendations

- Strategic
 - MFA
 - Policy Change
 - Staffing
- Tactical
 - Enhanced Logging

Highlight quick wins!

Thank you

Join the conversation

<https://discord.blueteamvillage.org>

