

School of Design and Informatics

BSc Ethical Hacking, 2022/23

**An Evaluation of Modular Incident Response Plans for Efficient Cyber Incident Mitigation in Businesses**

**Jigsaw Analysis**

**Author:** Martin Georgiev **Supervisor**: Natalie Coull

Head of Division of Cybersecurity Abertay

# **Section 1**

This research has led to the creation of incident response plans that can be customised for different types of cyber-attacks. The plans have two versions: one with basic information on how to respond generally to a cyber incident (based on the Scottish and Cyber Management Alliance incident response plans); and a second version with specific sections that are relevant to known cyber-attacks and their countermeasures. The sections that make up the second version can be added or removed depending on the type of attack. The project aims to make cybersecurity easier to understand for small and medium-sized enterprises, by using simple language and providing guidance on how to respond to different types of malware attacks.

Guidelines

This questionnaire is aimed at industry professionals with experience in digital forensics and incident response such as law enforcement and investigators from the private sector.

Participation is voluntary and the participant can withdraw at any time (please notify the researcher (1901560@uad.ac.uk) or their supervisor (n.coull@uad.ac.uk) if you choose to do so). Any questions can be omitted. No question in the survey is marked as "required".

The survey is entirely anonymous, and no personal data will be collected from the participants. The participants' position/organisation will also not be included in the project unless they specify otherwise.

After filling out the form the information will be handled carefully under the 1998 Data Protection law, will be analysed by the researcher, and used solely for this project. After completing the honours project, the data will be safely disposed of.

Due to time constraints, the deadline for answering the questionnaire is 30.04.2023.

## **Questions**

1. What is your position/organisation?

2. If the previous question was answered, would you like your position/organisation to be acknowledged in the report?

* Yes.
* Yes, but anonymised. (i.e., "higher-up in a cybersecurity department")
* No.

# **Section 2**

In addition to the incident response plans, the project has developed a robust malware analysis and forensics methodology that is both simple and effective. This methodology is designed to be easy to follow for SME executives who may not have extensive technical expertise in the field.

With its clear documentation and numerous examples, this methodology enables executives to analyse unknown malware samples during a cyber incident. Executives can utilise the obtained information to select an existing attack-specific module to address the incident or create their own. They can also provide the data to law enforcement or third-party incident response companies if they choose to do so. Furthermore, the methodology will also guide them in creating Yara rules and using them to scan suspicious files. To provide a comprehensive framework for this methodology, it will consist of the following sections:

1. Test Environment Setup (FlareVM and Remnux within a host-only network for communication)
2. Static Analysis - String (Floss) and in-depth (PEStudio - hashes, blacklisted functions/libraries, malicious indicators, etc.) analysis and packer identification (ExeInfoPE)
3. Dynamic Analysis and Digital Forensics - detonation symptoms, host-based forensics (procmon - file manipulation, processes, registry manipulation, evasion, and persistence mechanisms), network-based forensics (TCPView, Wireshark and Inetsim for Internet/DHCP server simulation), and RAM forensics (WinPMem and Volatility 3.0)
4. Yara rule creation - identifying malware-specific signatures and using them to scan unknown files.

## **Questions**

3. What is your opinion on the methodology? Would users with little experience be able to follow it? Would it be hard to keep it updated with the rapid development of malware? Could it be further simplified?

4. Do you think the methodology could lead to issues? (i.e. causing additional damage if the user does not accurately follow it)

# **Section 3**

## **3.1 Questions**

5. What is your opinion on the project idea (Combining easy-to-follow, attack-specific response modules with an analysis methodology)? Could it be beneficial for the industry and the overall security of SMEs?

6. Do you think that developing such a project could raise awareness among SME owners? - I.e., identifying how vital security is for the business and its users.

* Yes.
* No.
* Maybe.

7. Combining the modular plans with the methodology, do you think the project could be successful in real-life incidents? Why?

8. If your answer was no, why? Would you suggest any changes?