Forensic Duties of a Security Analyst

Reading

1h10m - 1h30m

Status | Incomplete

Introduction

As the digital world expands, the role of a security analyst becomes even more important. They are at the forefront of security incidents, creating the tools and techniques needed for the identification, collection, examination, analysis, and reporting of digital evidence. The outcome of their work can have significant impacts, from solving complex cyber crimes to supporting Cyber Security infrastructures.

In this reading, you will explore these multifaceted responsibilities, detailing how these security analysts transform raw data into a strong defense against cyber threats.

Reading

Security Analyst Roles and Responsibilities

Here is a look into the many hats that security analysts wear in Cyber Security, especially focusing on their roles related to digital forensics:

1. **Conduct forensic analysis** on digital devices: forensic analysts in IT and Cyber Security use specialized tools to look into devices such as computers, phones, or servers, and to find lost or deleted data. For example, they might use a program to find an erased file on a computer that shows where the cyber attack started.

2. **Collect digital evidence:** like treasure hunters, these analysts collect digital clues from different places like computers, network devices, and online storage. For instance, they might pull out unusual activity records from a server to catch any unauthorized actions.

3. **Analyze digital evidence:** security analysts are also digital puzzle solvers. They use specialized software and techniques to analyze digital evidence and identify patterns or anomalies that may indicate a security breach or cybercrime.

4. **Present findings in court:** sometimes, security analysts have to step into the shoes of a witness. They present their findings in court or give expert advice. It's like explaining how they tracked down a cyber criminal using traces of a specific malware.

5. **Conduct incident response:** security analysts quickly respond to security incidents like cyber attacks or data breaches. They work to lessen the harm and prevent such incidents from happening again. For instance, if a company's data is being stolen, they'll take action to secure affected systems and prevent more data loss.

6. **Provide recommendations** for security improvements: security analysts may provide recommendations for security improvements based on their analysis of digital evidence and investigation of security incidents.

According to the Cybersecurity and Infrastructure Agency (CISA), a security analyst role analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation. Security analysts play an important role in forensic investigations in IT and Cyber Security.

In short, being a security analyst in the field of digital forensics requires tech know-how, problem-solving skills, and a keen eye for detail. These skills help them make sense of digital clues, respond to incidents, and even provide legal support. It's a tough job but also a rewarding one.

Forensic Process, Techniques, and Tools

Forensic Processes

Decoding a cyber incident feels like solving a challenging jigsaw puzzle. You're sifting through a lot of data, using particular tools and tricks to spot the bits that fit together and complete the picture. And as with any good jigsaw puzzle, each piece and step is significant.

Now, you will go through the primary phases of this process, using an example:

1. **Identification:** this first stage is like finding potential clues at a crime scene. It involves pinpointing possible sources of relevant data such as devices, servers, network logs, and user accounts. For instance, in a hacking scenario, the affected system, along with any connected networks, would be the primary source of such data.

2. **Preservation:** once potential data sources are identified, they are collected and kept in a 'forensically sound' manner. This step ensures the data remains unchanged and legally acceptable. Following the hacking example, this could mean creating a mirror image of the affected system for analysis while the original system is preserved.

3. **Analysis:** now begins the investigative phase, which is like piecing together a puzzle. The preserved data is examined to identify relevant information and patterns that provide insight into the incident or crime under investigation. In our hacking case, this could mean identifying traces of unauthorized access or malicious code in the system.

4. **Reporting:** finally, it’s time to present the findings. This step involves documenting the findings of the analysis in a clear and concise report that can be used in legal proceedings or to inform incident response efforts. If you think of our hacking scenario here, the report will detail how the breach occurred, the extent of the damage, and potentially the attacker's identity.

5. **Recommendations:** recommendations on how to fix or protect against a similar attack being successful going forward to this list of items.

Throughout these processes, proper chain-of-custody procedures, much like the protocols used for physical evidence in a criminal investigation, must be followed. These preserve the integrity and admissibility of digital forensic evidence.

Popular Forensic Techniques and Tools

There are various forensic techniques and tools used for different types of investigations. Here are some popular ones:

- **Disk imaging:** creating a bit-by-bit copy of a digital storage device for analysis.

- **Memory analysis:** analyzing volatile data in computer memory to identify running processes, network connections, and other system activities.

- **Network forensics:** collecting and analyzing network traffic to detect and respond to security incidents.

- **Malware analysis:** analyzing the code, behaviour, and impact of malware to understand its purpose and origin.

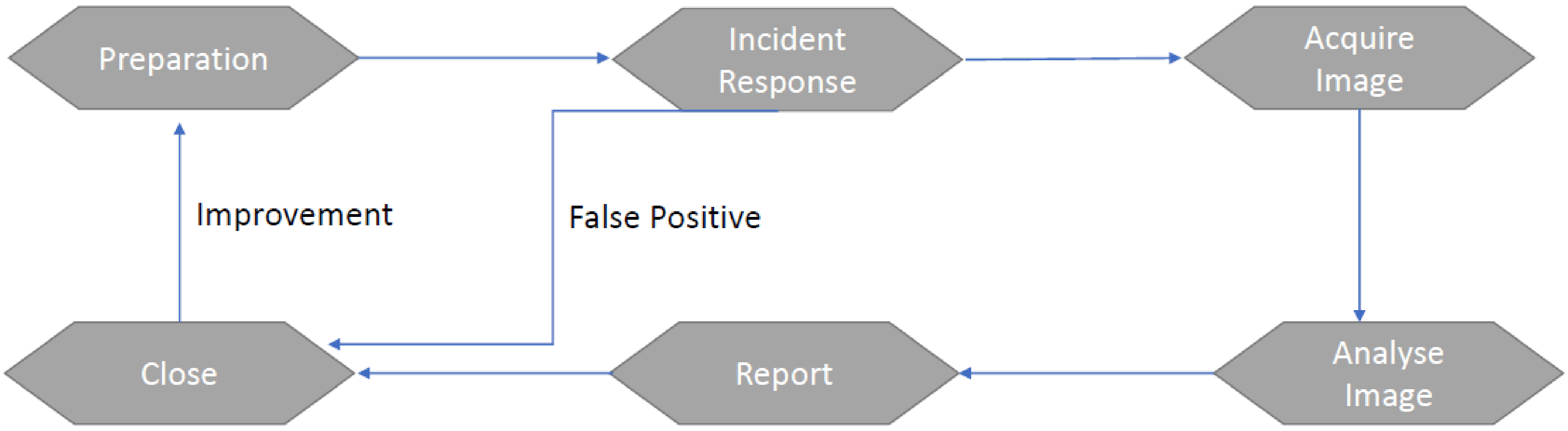
- **Data carving:** extracting files and data from a digital storage device based on file signatures and header information.

- **File analysis:** analyzing file metadata, contents, and structure to identify potential evidence.

- **Timeline analysis:** creating a chronological sequence of events related to a security incident using system logs and other data sources.

- **Forensic analysis tools:** there are various forensic analysis tools used in digital forensics investigations, such as EnCase, Forensic Tool Kit (FTK), Autopsy, and Sleuth Kit.
- **Password cracking:** using specialized software and techniques to recover passwords from encrypted data.
- **Hashing:** verifying the integrity of data by comparing the hash value of the original data with that of the copied data.

These are just some techniques and tools used by security analysts and investigators to collect, analyze, and report digital evidence in support of incident response, criminal investigations, and legal proceedings.



In the context of incident response, this is a high-level flowchart of the process

Characteristics of Digital Evidence

Digital evidence should meet the following criteria:

- Be admissible in court
- Authentic
- Complete
- Reliable
- Believable

Challenges with Forensics Analysis

- Ensuring rapid action is taken
- Recording of environment/crime scene without disturbing it
- Maintaining evidence integrity
- Compromises tools and/or software

Digital evidence of user identity or system activities can be found in device storage. Additionally, digital forensic evidence is not restricted to data saved on computer devices. It can encompass all digital activity connected to criminal conduct.

Based on these principles, a digital forensics specialist has a fundamental plan for locating, gathering, preserving, and examining digital evidence to be presented in court.

Writing the Forensics Report

Forensics reports can vary widely depending on the specific organization or industry requirements. In some cases, report formats may need to adhere to legal and regulatory requirements. The format therefore should be suitable for the audience that will be reviewing it.

While thinking about the audience, consider if they are technical or non-technical, if they are internal or external stakeholders, or if there are further legal requirements.

With these in mind, it is most important that the report is clear, well structured, and easy to understand by those who need to take appropriate action.

Here is an Example of the Basic Format of a Forensic Report

Introduction

- Provide a brief overview of the investigation and the purpose of the report.
- Include information such as the date and time of the investigation, the scope of the investigation, and the parties involved.

Evidence Collection

- Detail the methods used to collect evidence, including the date and time of each step.
- Include information about where the evidence was found, who collected it, and how it was preserved.

Analysis

- Detail the techniques and tools used to analyze the evidence.
- Explain the results of the analysis and how they support or refute the initial hypotheses or theories.

Findings

- Summarize the conclusions of the investigation based on the evidence collected and analyzed.
- Provide a detailed explanation of how the conclusions were reached and how they relate to the initial hypotheses or theories.

Recommendations

- Provide recommendations for future actions or measures that can be taken to prevent similar incidents from occurring in the future.
- Include information such as policies or procedures that need to be implemented, training that needs to be conducted, or changes to the infrastructure or software that need to be made.

Conclusion

- Summarize the main points of the report and emphasize the importance of the findings and recommendations.
- Conclude with any final thoughts or comments.

It's important to keep the report clear, concise, and organized. Use headings and subheadings to break up the report into manageable sections, and be sure to include any diagrams, charts, or tables that can help illustrate the findings.

Use clear and concise language, and avoid technical jargon or acronyms that may not be familiar to the reader. Finally, proofread and edit the report carefully before submitting it to ensure that it is free of errors and accurately represents the findings of the investigation.

Interactive Digital Forensic Report

Note: For a larger view, click the header above or right click the report and select Full Screen.

Digital Forensic report- sample - With File HTML_redacted

Further Reading: Forensic Report Samples

Explore the following links to learn more about different forensic report formats:

[Step by Step instructions to writing forensic reports]

[7 Free sample Forensic reports for business]

Key Takeaways

- The role of security analysts in digital forensics is invaluable. They are on the front lines gathering evidence and promptly responding to security events.
- Forensic work follows a process: spotting potential evidence, gathering and examining it, and analyzing the findings to prepare a report. To accomplish these tasks, analysts use an array of specialized techniques and tools.
- Putting together a precise and comprehensive forensic report is a big part of the process. It's much like painting a picture or narrating a story—every detail matters. To get it right, a sample report can be a trusty companion.

Conclusion

In essence, security analysts play a great role in digital forensics. Their duties span across careful collection, analysis, and reporting of digital evidence, all aimed at uncovering security incidents.

Their journey often involves several key steps, including identification, collection, examination, analysis, and reporting of digital evidence. It can be supported by various techniques and tools, such as network forensics, memory forensics, malware analysis, and narrating the findings in a forensic report.

Armed with diverse techniques, such as network forensics and malware analysis, they dissect the digital chaos to find meaningful patterns. Remember, every detail counts, and a well-crafted forensic report (clear and comprehensive) is a pivotal milestone in this detective journey.

References

> Check out these resources. They'll deepen your understanding and broaden your knowledge, offering essential insights:

- Digital Forensics and Incident Response (SANS Institute): Several free tools available here
- Review of Digital Forensic Methods (2022) by NIST
- Top 20 Free Digital Forensic Investigation Tools for SysAdmins – 2019 update (Andrew Tabona)
- NIST to Digital Forensics Experts: Show Us What You Got (June 2020)

✓ Mark Completed

← Previous
The Role of Forensics in IT

How well did this activity help you to understand the content?

Let us know how we're doing

☆ ☆ ☆ ☆ ☆

W08D5
Fri Aug 16

› Outline & Notes (1)

› Lectures (1)

⌄ Work (5)

6 hrs

- Project: Writing Investigation & Research Report
- Course Reflection
- Overview - Forensics
- The Role of Forensics in IT
- Forensic Duties of a Security Analyst

› Other (1)

W08D5 Schedule »