INDIVIDUAL ASSIGNMENT

NAME (TP NUMBER)	:	Koo Wai Kit (TP081761)
INTAKE CODE	:	APUMF2406CYS
MODULE TITLE	:	E-Investigation (072024-SDS)
MODULE LECTURER	:	Dr. Seyedmostafa Safavi
PROJECT TITLE	:	E-Investigation Individual Assignment
DATE ASSIGNED	:	19/8/2024
DATE COMPLETED	:	24/9/2024

Table of Contents

List of Tables

List of Figures

1.0 Introduction

A data breach occurs when unauthorised parties access sensitive information, such as personal data or corporate records (Kosinski, 2024). Data breaches can result from various factors, including human error, insider threats, or malicious hacking aimed at financial gain. The process typically involves researching targets to identify vulnerabilities, executing attacks using methods like phishing or exploiting system flaws, and ultimately compromising data for theft or ransom (Kosinski, 2024).

In Malaysia, data breaches are a significant concern, with the country ranking 31st globally and over 52 million compromised accounts reported since 2004, representing 0.3% of global breaches (Surfshark, 2024). In 2024 alone, 142 incidents were reported in Q1 and 117 in Q2, highlighting the ongoing threat to data security in the country (MyCERT, 2024). Given this context, understanding the dynamics of data breaches is essential for developing effective prevention and response strategies.

This report explores two critical areas: first, an evaluation of Indicators of Compromise (IoCs), Potential Digital Evidence (PDE), and their sources to support investigations into data breaches. The second area focuses on proposing a framework that integrates behavioural profiling with AI and machine learning (ML) technologies to enhance the effectiveness of investigations. Ultimately, the goal is to present a structured approach to effectively address and mitigate data breaches.

2.0 Contents

2.1 Task 1: IoCs and Relevant PDE to Collect from Internal and External Sources for Data Breach Investigations

This section explores the Indicators of Compromise (IoCs) and Potential Digital Evidence (PDE) essential for conducting data breach investigations. It highlights the role of OSINT tools in supporting the identification of these indicators and addresses the evaluation of sources and legal aspects related to data collection.

2.1.1 Indicators of Compromise (IoCs) and OSINT tools

Indicators of Compromise (IoCs) are crucial pieces of threat intelligence used to identify potential security breaches (Harrington, 2013). They are detected through observation, analysis, and known threat signatures (Cloudflare, n.d.).

2.1.1.1 Identification of IoCs

According to Noor et al. (2019), IoCs in data breaches can be divided into low-level and high-level categories. Low-level IoCs include technical details such as IP addresses, ports, and malware hashes, which are quickly actionable but have limited longevity due to attackers frequently changing their tactics. In contrast, high-level IoCs include behavioural signatures and Tactics, Techniques, and Procedures (TTPs), which impose greater challenges on attackers, as they require more effort to evade detection. Although lower-level IoCs are easier to identify, higher-level indicators provide more effective and sustainable defense strategies that force attackers to adapt their methods.

In addition, IoCs can be further classified into several common types, which include network-based, host-based, file-based, behavioural, and metadata indicators (Cloudflare, n.d.). There are several IoCs that can be used to identify potential data breaches, which can be identified as follows (SentinelOne, 2023):

Network-based

i. **Unusual outbound network traffic**: Anomalies in outgoing network traffic can indicate a security breach. Unexpected data transmission might suggest an intruder trying to exfiltrate information or an infected system communicating with a command-and-control server.
ii. **Connections to malicious IP addresses**: Communication with IP addresses known for malicious activity may suggest attempts to manage compromised systems or siphon off data.
iii. **Unauthorised network scanning**: Unauthorised scanning activities could signal reconnaissance efforts by attackers seeking to uncover system vulnerabilities.
iv. **Abnormal web traffic levels**: Unusual spikes in traffic to specific websites or IP addresses may suggest a compromise.

Host-based

v. **Unauthorised file changes**: Modifications to system files or unauthorised software installations can be signs of a breach, potentially allowing attackers to gain system control or steal data.
vi. **Unexpected system behavior**: Issues like random restarts, system crashes, or slow performance may signal ongoing security incidents, including denial-of-service attacks.

File-based

vii. **Suspicious files or running processes**: The presence of unfamiliar files or processes could hidden malware on the system.

Behavioural

viii. **Privileged account irregularities**: Unexplained actions from privileged accounts may indicate internal or external security threats.

ix. **Irregular account behaviours**: Uncommon login times, unauthorised access to sensitive resources, or an unusual number of failed login attempts could point to a security breach.

Metadata

x. **Phishing emails**: Emails that request sensitive information or contain suspicious links can be indicative of phishing attempts.

2.1.1.2 OSINT Tools for Investigation

When investigating data breaches, several OSINT tools significantly enhance the identification of vulnerabilities and threats. Shodan is a valuable search engine that helps users discover Internet-connected devices, revealing potential security weaknesses in exposed systems (Glamoslija, 2024). By scanning the internet for various device types and configurations, Shodan allows organisations to assess their exposure to attacks. Similarly, VirusTotal analyses files and URLs against multiple antivirus engines, enabling quick identification of potentially malicious content, while Censys provides detailed information about the configurations of internet-connected devices, assisting organisations in evaluating their security posture (VirusTotal, n.d.; Censys, n.d.).

In addition, PhishTank is instrumental in combating phishing threats by collecting and verifying data on phishing websites, offering real-time information that aids organisations in recognizing and avoiding phishing attempts (PhishTank, n.d.). Additionally, Maltego serves as a powerful data mining tool that facilitates the gathering and analysis of information from diverse sources, creating visual link analyses that reveal relationships and potential security threats (Maltego, n.d.). Together, these OSINT tools provide a comprehensive approach to enhancing security and effectively investigating data breaches.

2.1.2 Potential Digital Evidence (PDE) and Evaluation of Sources

According to Guttman et al. (2022), digital evidence can be grouped into four main categories: physical media, digital images and files, other digital objects, and law

enforcement-generated evidence. Digital evidence includes physical media like hard drives, mobile devices, and external storage. Digital images and files are copies extracted from physical or remote systems such as cloud storage. Other digital objects consist of intangible data from online accounts. Law enforcement-generated evidence involves records from body-worn cameras, in-car videos, and other electronic documentation.

2.1.2.1 Internal sources

Potential Digital Evidence (PDE) from internal sources plays a crucial role in data breach investigations by providing insights into unauthorised access, data exfiltration, and other malicious activities. Key PDEs from internal sources include log files, which consists of system logs, application logs, and security logs that document events and activities across networks, revealing unauthorised access attempts or anomalies (ABA, 2021). Network traffic data, consisting of captured packets and flow data, can indicate data exfiltration or other suspicious activities. Forensic images of hard drives and memory provide snapshots of a system's state, while system artifacts such as registry entries and configuration files highlight changes or irregularities (ABA, 2021).

Furthermore, email data can offer evidence of phishing attempts and other malicious communications, while cloud data from service providers tracks user activities and data access (ABA, 2021). Endpoint data from devices such as computers and smartphones contributes further by capturing details about installed software, running processes, and user actions (UNODC, n.d.). These internal sources collectively provide a comprehensive view of the breach.

2.1.2.2 External sources

External sources also significantly enhance the investigation. Pryimenko (2024) states that threat intelligence feeds aggregate data about known threats and vulnerabilities, providing a broader understanding of potential risks. Third-party logs from external service providers offer context about breaches, while public databases reveal compromised data that might be linked to the incident (Pryimenko, 2024). Engaging external forensic services can further enhance the investigation by providing expert analyses.

2.1.3 Legal Aspects of Data Collection

Legal aspects of data collection is a crucial consideration, including the necessity to comply with data protection laws like GDPR, which mandate transparency and legal grounds

for data collection (Alford et al., 2020). According to Forensic Science Simplified (n.d.), specialised training is required for those handling and analysing digital evidence, as untrained individuals can inadvertently destroy or alter data, rendering it unusable in legal proceedings.

Organisations must also adhere to notification requirements for affected individuals and regulatory bodies after a breach (Iron Mountain, 2018). Ensuring proper preservation of evidence is essential for legal proceedings, while engaging legal counsel early helps protect sensitive communications under attorney-client privilege (Hutnik, 2020). Lastly, compliance with regulations regarding cross-border data transfers is important to avoid legal complications (Alford et al., 2020).

2.2 Task 2: A Proposed Framework Incorporating Behavioural Profiling and AI / ML Technologies for Data Breach Investigations

Data breaches pose significant threats to organizations by compromising sensitive information and exposing vulnerabilities, especially because human errors are a major risk as untrained users often fall victim to social engineering attacks that compromise their credentials (Zhang et al., 2022). This vulnerability underscores the need for more robust protection measures. According to Pryimenko (2024), data breach incident response involves systematically managing the aftermath of a breach to minimise damage, recovery time, and costs. A key component of data breach response is the data breach investigation, which aims to uncover the breach's details, assess the impact, and guide future actions based on the findings.

This section proposes a comprehensive framework that integrates behavioural profiling with Artificial Intelligence (AI) / Machine Learning (ML) technologies to improve the efficiency and accuracy of data breach investigations. This framework aims to enhance the investigation process by predicting potential breaches, understanding user behavior, and automating responses.

2.2.1 Framework Design

This proposed framework is a modified version of the data breach investigation framework by Hakim et al. (2023), with an emphasis on Behavioural Profiling and AI/ML technologies to enhance the investigation process. The steps outlined in this framework are organised into three phases:

I. **Preparation Phase**: Involves evidence categorisation and behavioural profiling, focusing on organising evidence and identifying suspicious behaviours early.

II. **Collection and Analysis Phase**: Covers systematic evidence gathering, detailed analysis, and dynamic event correlation to identify attack vectors and critical points of compromise.

III. **Reconstruction and Reporting Phase**: Includes timeline reconstruction, attack path mapping, and mapping findings to answer the 5WH questions (What, Who, When, Where, Why, How), providing a comprehensive overview of the incident to inform mitigation strategies.

Table 1: Steps of data breach investigations outlined in the proposed framework

Phase	Step	Description
Preparation	Evidence categorisation	Evidence is organised into distinct categories, such as user behaviour data, host data, network activity, and security logs, to streamline the investigation process and enhance focus on relevant information.
	Behavioural profiling	AI/ML algorithms will analyse user behavior patterns to identify deviations that may signal potential security threats or breaches, providing insights into the context of the incident.
Collection and analysis	Evidence collection	Involves gathering all relevant data from various sources, including system logs, network traffic, and user interactions, ensuring that all relevant information is available for thorough investigation.
	Evidence analysis	The collected evidence is examined in detail using AI/ML tools to extract meaningful artifacts and identify relationships between events, helping to uncover the nature and extent of the breach.
	Dynamic event correlation	Involves linking related events and artifacts in real-time to create a coherent narrative of the incident,

		enabling investigators to understand how different components of the breach are interconnected.
Reconstruction and reporting	Timeline reconstruction	The chronological order of events is established by organising artifacts based on their timestamps, allowing investigators to visualise the sequence of actions that led to the breach.
	Attack path mapping	Focuses on detailing the attackers' methods and techniques by analysing the reconstructed timeline and correlated events, providing a comprehensive view of the attack's progression.
	Mapping findings to answer 5WH questions (What, Who, When, Where, Why, How)	The final step synthesises the findings from the investigation to provide clear answers to the 5WH questions (What, Who, When, Where, Why, and How), facilitating a deeper understanding of the incident and informing future prevention strategies.

To summarise the steps above, this framework emphasises behavioural profiling to identify abnormal activities, leveraging AI/ML to enhance evidence collection, analysis, and correlation of events. By integrating dynamic event correlation, timeline reconstruction, and attack path mapping, the framework provides a comprehensive understanding of the breach. Finally, findings are mapped to answer key investigative questions, providing clear insights and guiding remediation efforts. The steps of the proposed framework are illustrated in the diagrams below for better visualisation and understanding. Figure 1 illustrates the preparation phase, Figure 2 shows the collection and analysis phase, and Figure 3 shows the reconstruction and reporting phase.

Figure 1: Preparation phase

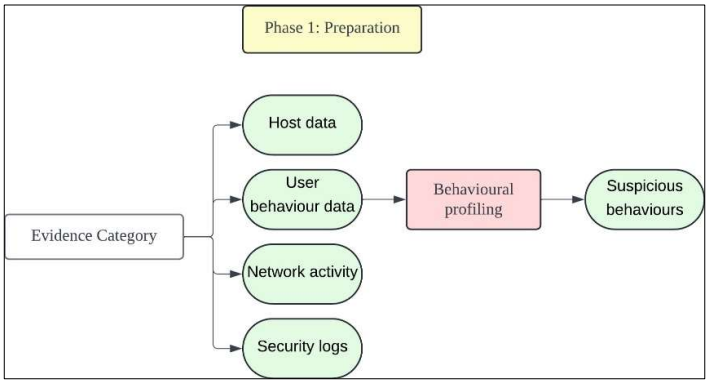


Figure 2: Collection and analysis phase

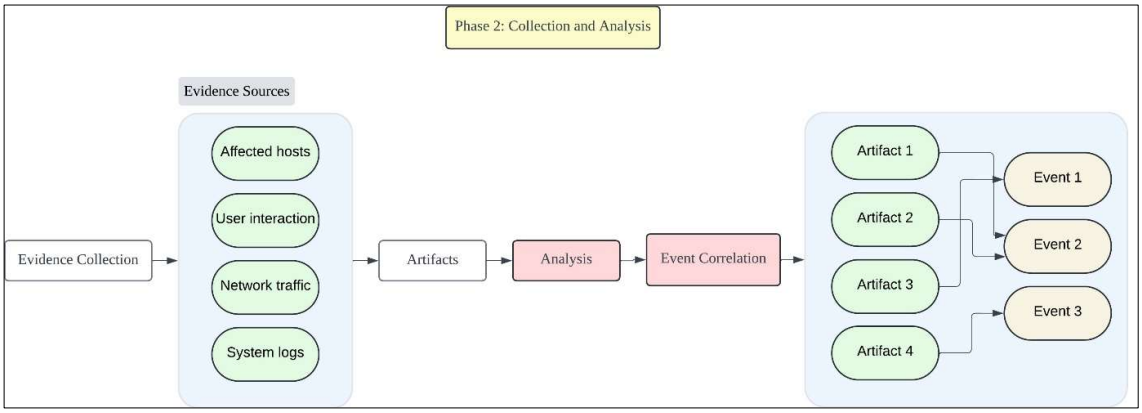
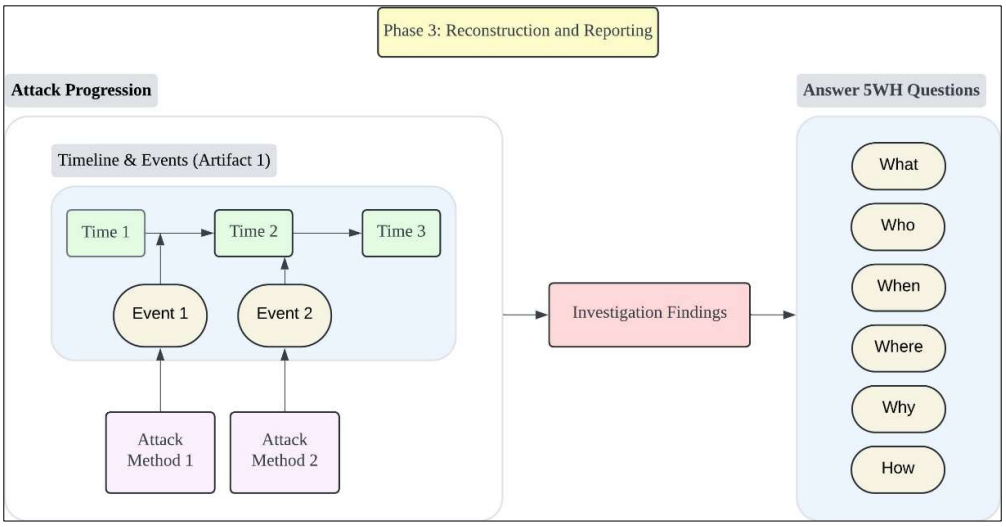


Figure 3: Reconstruction and reporting phase



2.2.2 Profiling Techniques

Criminal profiling is an essential investigative tool that helps narrow down potential suspects and assess their likelihood of committing a crime (Warikoo, 2014). A profile is

constructed from a collection of characteristics that are typically found among individuals who engage in a specific type of crime (Shinder et al., 2002).

Profiling is grounded in two main assumptions: the consistency assumption, which suggests that offenders display similar behaviours across different crimes, and the homology assumption, which states that similar crime patterns correlate with comparable offender characteristics (Kirwan & Power, 2011). Two predominant methods of criminal profiling utilised today are as follows:

- **Inductive Profiling:** Utilises a database containing extensive information about criminals associated with particular crimes. Profilers analyse this data to identify correlations and deduce the common characteristics shared by a statistically significant number of offenders for a specific crime type (Shinder et al., 2002).

- **Deductive Profiling:** Focuses on examining forensic evidence and victim profiles to infer the attacker's motive and characteristics. This method involves analysing forensic evidence, applying victimology principles, and leveraging the profiler's experience to derive insights about the criminal's attributes (Shinder et al., 2002).

In addition, Warikoo (2014) proposed a methodology that utilises a hybrid profiling model that integrates deductive processes with statistical analysis to identify common patterns in cybercriminal behavior. Key insights into the attacker's sophistication, motivations, tools, and vulnerabilities are derived from digital forensics data (Kwan et al, 2008). The following six Profile Identification Metrics are employed to assess the offender's behaviour and characteristics (Warikoo, 2014):

a. **Attack Signature**: Describes the tools utilised during the attack, distinguishing between custom code designed for zero-day exploits and commonly available tools targeting known vulnerabilities.
b. **Attack Method**: Includes the various techniques used by cybercriminals, such as social engineering, phishing, malware deployment, distributed denial of service (DDoS), and spamming.
c. **Motivation Level**: This is assessed based on the attack's complexity, where a more complex attack suggests a higher motivation level, as determined using the vulnerability tree methodology (Vidalis & Jones, 2003).

d. **Capability Factor**: This metric assesses the attacker's skills, access to resources, and proficiency with hacking tools.
e. **Attack Severity**: Categorises the impact of an attack on an organization into four levels: low, medium, major, and critical.
f. **Demographics**: This factor takes geographic location into account as an essential element for profile identification, acknowledging that certain types of cybercrimes frequently originate from specific areas (Tompsett et al., 2005).

Subsequently, the stages of the profiling model are summarised in Table 2 below (Warikoo, 2014).

Table 2: Profiling processes

Process	Description
P1: Victim Profiling	Focuses on victim profiling, which identifies the elements of individuals or organizations that attracted cybercriminals. This includes understanding the reasons behind the victim's selection and the tactics used in the attack.
P2: Motive Identification	Aims to determine the motive behind the attack, often linked to the victim. For example, an attack on government targets may indicate espionage. This process also analyses digital forensic evidence to uncover attacker characteristics and assess risks to the victim.
P3: Empirical Data Analysis	Uses statistical analysis to identify trends and behavioural patterns. Analysts compare characteristics from the previous stage with statistical data to uncover common criminal behaviours.
P4: Profile Development	Involves creating detailed profiles of cybercriminals based on identified characteristics, such as classifying a skilled attacker using zero-day exploits as a cyber spy. This profiling aids in understanding cyber threats and developing targeted prevention strategies.

2.2.2.1 Application of Profiling Techniques in the Proposed Framework Design

In the Preparation Phase, profiling aids in categorising evidence by prioritising data that aligns with known attacker signatures, while AI/ML algorithms for behavioural profiling help identify suspicious activities earlier.

During the Collection and Analysis Phase, profiling focuses evidence collection on relevant data points, such as email logs for suspected phishing attacks, and employs inductive and deductive methods to analyse evidence against known patterns. Dynamic event correlation benefits from profiling by linking seemingly unrelated events based on shared characteristics.

In the Reconstruction and Reporting Phase, profiling informs timeline reconstruction by highlighting likely attacker behaviours, enhancing attack path mapping through detailed insights into methods used. Additionally, profiling enriches the final report by providing context for the 5WH questions, particularly around the motivations and capabilities of the attackers.

This comprehensive approach not only improves immediate response strategies but also strengthens long-term prevention efforts by creating a clearer picture of the breach, making the framework more adaptive and informed by the characteristics of cybercriminals.

2.2.3 AI / ML Technologies for Data Breach Investigations

Fakiha (2023) revealed that traditional cyber forensic investigation techniques are often time and resource intensive, relying heavily on manual data collection and analysis, which can lead to errors. In contrast, the integration of AI and ML technologies significantly enhances the efficiency and effectiveness of investigations. Techniques such as clustering and anomaly detection facilitate the rapid identification of unusual data flows in network traffic patterns, effectively highlighting potential attack vectors. Furthermore, natural language processing (NLP) techniques are employed to analyse text-based communication logs, revealing atypical linguistic patterns that may indicate the extent of a breach.

The case study with J.S. Held illustrates the application of advanced AI techniques in cyber forensics, as described by Fakiha (2023). Their team of forensic experts utilised ML algorithms to analyse large volumes of data, successfully identifying patterns and anomalies that suggest malicious activity. By employing network and system analysis, they were able to

pinpoint attack vectors and assess the severity of breaches more effectively. This integration of AI and ML technologies not only expedites the identification of sophisticated attack paths but also provides a comprehensive understanding of breaches.

In addition, Support Vector Machines (SVM) and decision trees are key machine learning techniques for malware detection (Mirza et al., 2018). SVM operates by identifying the optimal hyperplane to distinguish between classes, using features like Application Program Interface (API) call statistics. Decision trees classify data through a tree-like model based on features such as file hashes, malicious IP addresses, and external calls. Together, these techniques enhance the detection and analysis of malware in cybersecurity.

Additionally, Noor (2019) compares different ML algorithms and highlights their effectiveness, particularly belief networks, in cyber forensic investigations for data breach detection. Noor (2019) explains that belief networks excel in scenarios with conflicting or missing data features, commonly encountered in recent breaches, and demonstrate resilience against irrelevant features and adversarial data manipulation.

2.2.3.1 Application of AI / ML Technologies in the Proposed Framework Design

In the Preparation Phase, ML algorithms facilitate behavioural profiling to detect unusual user behaviour patterns, categorising evidence into types like user data and security logs for focused analysis.

During the Collection and Analysis Phase, clustering and anomaly detection techniques quickly identify abnormal data flows, highlighting potential attack vectors. Machine learning tools, including Support Vector Machines (SVM) and decision trees, analyse collected evidence to classify data based on features such as file hashes and malicious IP addresses, enhancing malware detection. Additionally, dynamic event correlation creates a coherent narrative of the incident, while belief networks are employed to effectively handle scenarios with conflicting or missing data features, which are common in recent breaches.

In the Reconstruction and Reporting Phase, ML enhances timeline reconstruction and attack path mapping, establishing the chronological order of events based on timestamps. The framework synthesizes findings to address the 5WH questions (What, Who, When, Where, Why, and How), providing actionable insights for remediation.

3.0 Conclusion

In conclusion, addressing data breaches requires a multifaceted approach that combines the identification of Indicators of Compromise (IoCs) and Potential Digital Evidence (PDE) with innovative frameworks leveraging behavioural profiling and AI/ML technologies. The evaluation of IoCs highlights the importance of both low-level and high-level indicators, emphasising the need for organizations to remain vigilant and adaptive in their defense strategies against evolving threats. Furthermore, the comprehensive framework proposed in this report not only enhances the efficiency of investigations but also empowers organisations to predict potential breaches through an understanding of user behavior.

The integration of behavioural profiling techniques alongside AI and machine learning tools is critical in streamlining evidence collection, analysis, and correlation. By reconstructing timelines and mapping attack paths, investigators can develop a holistic understanding of incidents, ultimately leading to more effective mitigation strategies. Additionally, the legal considerations surrounding data collection underscore the necessity for organizations to operate within regulatory frameworks, ensuring that evidence preservation and compliance with data protection laws are prioritized.

Ultimately, this report serves as a foundation for future research and development in the realm of cybersecurity, advocating for continuous adaptation and improvement in practices to address the ever-evolving landscape of data breaches.

4.0 References

Alford, S., Turner, S. A., Crawford, G. E., Pizzey, H., Williams, M., & Mazzelli, M. G. (2020, January 3). *Data protection in investigations.* Global Investigations Review. https://globalinvestigationsreview.com/guide/the-practitioners-guide-global-investigations/2020/article/data-protection-in-investigations

American Bar Association (ABA). (2021). *Evidence Preservation: The Key to Limiting the Scope of a Breach*. https://www.americanbar.org/groups/tort_trial_insurance_practice/committees/cyber-data-privacy/evidence-preservation/

Censys. (n.d.). *What is Censys?*. https://about.censys.io/

Cloudflare. (n.d.). *What are indicators of compromise (IoC)?*. https://www.cloudflare.com/learning/security/what-are-indicators-of-compromise/

Fakiha, B. (2023). Enhancing cyber forensics with AI and machine learning: A study on automated threat analysis and classification. *International Journal of Safety and Security Engineering, 13*(4), 701-707. https://doi.org/10.18280/ijsse.130412

Forensic Science Simplified. (n.d.). *A Simplified Guide To Digital Evidence*. https://www.forensicsciencesimplified.org/digital/how.html

Glamoslija, K. (2024). *What Is Shodan? How to Use It & Stay Protected in 2024*. Safety Detectives. https://www.safetydetectives.com/blog/what-is-shodan-and-how-to-use-it-most-effectively/#:~:text=Shodan%20works%20by%20requesting%20connections,that%20are%20running%2024%2F7.

Hakim, A. R., Ramli, K., Gunawan, T. S., & Windarta, S. (2023). A novel digital forensic framework for data breach investigation. IEEE Access, 11, 42644-42659.

Harrington, C. (2013). Sharing indicators of compromise: An overview of standards and formats. *EMC Critical Incident Response Center*, *14*(5), 28-42.

Hutnik, A. Z. (2020, June 11). *Lessons learned for maintaining attorney-client privileged*

data breach investigation (and other consultant) reports. Kelley Drye. https://www.kelleydrye.com/viewpoints/blogs/ad-law-access/lessons-learned-for-maintaining-attorney-client-privileged-data-breach-investigation-and-other-consultant-reports

Iron Mountain. (2018, October 4). *What happens after a data breach? Legal ramifications and beyond*. https://www.ironmountain.com/resources/blogs-and-articles/t/the-legal-ramifications-of-a-data-breach

Kirwan, G., & Power, A. (2012). The Psychology of Cyber Crime. In *Advances in digital crime, forensics, and cyber terrorism book series*. IGI Global. https://doi.org/10.4018/978-1-61350-350-8

Kosinski, M. (2024, May 24). *What is a data breach?*. IBM. https://www.ibm.com/topics/data-breach

Kwan, L., Ray, P., & Stephens, G. (2008, January). Towards a methodology for profiling cyber criminals. In *Proceedings of the 41st Annual Hawaii International Conference on System Sciences* (HICSS 2008) (pp. 264-264). IEEE.

Maltego. (n.d.). Maltego for cyber threat intelligence. https://www.maltego.com/solutions/cyber-threat-intelligence/

Mirza, Q. K. A., Awan, I., & Younas, M. (2018). CloudIntell: An intelligent malware detection system. *Future Generation Computer Systems*, 86, 1042-1053.

MyCERT. (2024). *Cyber incident quarterly summary report: Q2 2024* (Report No. SR-027.092024). https://www.mycert.org.my/portal/advisory?id=SR-027.092024

Guttman, B., White, D. R., & Walraven, T. (2022). Digital evidence preservation: Considerations for evidence handlers (NIST Interagency Report 8387). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8387

Noor, U., Anwar, Z., Amjad, T., & Choo, K. K. R. (2019). A machine learning-based FinTech cyber threat attribution framework using high-level indicators of compromise. Future Generation Computer Systems, 96, 227-242.

Noor, U., Anwar, Z., Malik, A. W., Khan, S., & Saleem, S. (2019). A machine learning

framework for investigating data breaches based on semantic analysis of adversary's attack patterns in threat intelligence repositories. Future Generation Computer Systems, 95, 467-487.

PhishTank. (n.d.). What is phishing?. https://phishtank.org/what_is_phishing.php

Pryimenko, L. (2024, April 24). Data breach response and investigation: 8 steps for efficient remediation. Ekran. https://www.ekransystem.com/en/blog/data-breach-investigation-best-practices

SentinelOne. (2023, March 11). *What are Indicators of Compromise (IoCs)?*. https://www.sentinelone.com/cybersecurity-101/threat-intelligence/what-are-indicators-of-compromise-iocs-a-comprehensive-guide/

Shinder, D. L., & Cross, M. (2008). Scene of the Cybercrime. Elsevier.

Surfshark. (2024, July 15). *Global data breach statistics*. https://surfshark.com/research/data-breach-monitoring

Tompsett, B. C., Marshall, A. M., & Semmens, N. C. (2005). Cyberprofiling: Offender profiling and geographic profiling of crime on the Internet. In *Security and Privacy for Emerging Areas in Communication Networks, 2005. Workshop of the 1st International Conference*. IEEE. https://doi.org/10.1109/SECCMW.2005.1588290

United Nations Office on Drugs and Crime (UNODC). (n.d.). Cybercrime module 6 key issues: handling of digital evidence. https://www.unodc.org/e4j/en/cybercrime/module-6/key-issues/handling-of-digital-evidence.html

Vidalis, S., & Jones, A. (2003). Using vulnerability trees for decision making in threat assessment. University of Glamorgan, School of Computing, Tech. Rep. CS-03-2.

VirusTotal. (n.d.). How it works. https://docs.virustotal.com/docs/how-it-works

Warikoo, A. (2014). Proposed Methodology for Cyber Criminal Profiling. *Information Security Journal: A Global Perspective*, *23*(4–6), 172–178. https://doi.org/10.1080/19393555.2014.931491

Zhang, X., Yadollahi, M. M., Dadkhah, S., Isah, H., Le, D.-P., & Ghorbani, A. A. (2022). Data breach: Analysis, countermeasures, and challenges. *International Journal of Information and Computer Security*, 19(3/4), 402. https://doi.org/10.1504/IJICS.2022.127169