Cyber Threat Intelligence and IoCs and IoAs Search on the Dark Web

Martti Lehto and Timo Koskimäki
University of Jyväskylä, Finland

martti.lehto@jyu.fi
timo.a.koskimaki@jyu.fi

Abstract: Through cyber threat intelligence (CTI), information is collected and analyzed from the surface web, deep web, and dark web. Threat intelligence refers to the knowledge, context, and insight gained by analyzing a wide range of physical, geopolitical, and cyber threats. CTI specifically involves the collection, processing, and analysis of data, leading to an understanding of the motivations, targets, and attack methods of threat actors. CTI helps facilitate faster, better-informed, and data-driven security decisions. It enables a shift from reactive defense to proactive engagement against threat actors. In the context of cybersecurity, various indicators are used. The indicators that are most used are Indicators of Compromise (IoC) and Indicator of Attack (IoA). The collected observational data is used to understand the attacker's motivation for the attack and to predict their future actions. This provides the necessary perspective for decision-making to organize defense from reactive to proactive action. This study analyzes the role of the dark web as a source of IoC and IoA, as cyber threat actors primarily operate and communicate on dark web platforms. The dark web is a part of the deep web that is intentionally hidden and inaccessible through regular web browsers. Using the dark web allows for nearly complete anonymity online by encrypting data packets and routing them through several network nodes.

Keywords: Cyber threat intelligence, Dark Web, IoC, IoA

1. Introduction

Today systems are attacked more and more by single or multiple hacktivists, state sponsored hackers, cyber criminals, cyber terrorists, cyber-spies or cyber warfare fighters. The cyber security approach requires a balance of cyber threat intelligence, real time cyber-attack detection and especially the ability to cyber early warning.

The global community is facing an increase, sophistication, and successful perpetration of cyber-attacks. As the quantity and value of digital information has increased, so too have the efforts of Criminals and other Malicious actors, for whom the Internet offers the opportunity to prepare and execute anonymous attacks beyond the reach of attribution. Of primary concern is the Threat of organized cyber-attacks capable of causing debilitating disruptions to a nation's critical infrastructures, functions Vital to society, economy, or national security. So far, many proactive techniques have been proposed to deal with these threats. In order to create an effective cyber situational picture, information on various attack indicators is needed. (Lehto, 2022)

2. Cyber Threat Intelligence

Cyber threat intelligence refers to dynamic, adaptive technology that leverages large-scale threat history data to proactively block and remediate future malicious attacks on a network. CTI encompasses information derived from knowledge, skills, and experience, addressing both cyber and physical threats as well as the entities behind these threats. (Pöyhönen & Lehto, 2024) Because of evolving threats, security solutions are only as effective as the intelligence powering them. So, CTI is knowledge that allows us to prevent or mitigate cyber-attacks. The data captured by the dark web monitoring solution can be fed into automated threat intelligence systems and used to enrich that data (Lenaerts-Bergmans, 2023).

CTI can be divided into four tiers: Situational Awareness, Immediate Threats, Understanding Capabilities, and Community Awareness (Shakarian, 2017). Situational awareness includes awareness of recent attacks and their analysis. Immediate threats involve staying informed about the types of organizations that have been targeted. Understanding capabilities encompasses the assessment of the development of hackers' capabilities. Community awareness involves monitoring hacker behavior within hacker communities and tracking changes in hacker markets. (Basheer & Alkhatib, 2021)

A cyber threat intelligence solution can address each of these issues. The best solutions use machine learning to automate data collection and processing, integrate with existing solutions, take in unstructured data from disparate sources, and then connect the dots by providing context on Indicators of Compromise (IoCs) and Indicators of Attack (IoAs) and the tactics, techniques, and procedures (TTPs) of threat actors. (Koskimäki, 2024)

3. Internet Network

Table 1 briefly compares the characteristics of the surface web, deep web, and dark web according to model of Varma (2018). However, this comparison also includes the legal aspect for dark web content. In Varma's model, the dark web content was solely illegal, but according to this study, the dark web also contains legal content, such as various discussion and information-sharing platforms for dissidents and journalist. Also notice that Deep web includes Dark web, so the Contents -percentages are not visible in the Dark web sector. These layers are discussed separately by explaining the characteristics, unique features, and differences of each layer. Then we add also browsers and search engines to the table by Ghimiray and Brandefense. We also add some examples to the deep web search engines, which can search the databases of certain internal repositories on the deep web.

Table 1: The characteristics of the internet layers (Varma, 2018; Brandefense, 2022; Ghimiray, 2024)

	Surface web	**Deep web**	**Dark web**
Description	Content, that search engines can find	Content, that search engines can't find	Content, that is hidden intentionally
Known as	Visible Web, Indexed Web	Invisible network, Hidden network	
Contents	Legal	Legal + Illegal	Illegal + Legal
Information found	4 %	96 %	
Browsers	Mozilla Firefox. Google Chrome, Edge, Safari, Opera, Brave, Baidu, Yandex		Tor Browser, I2p, Freenet
Search Engines*	Google, Bing, DuckDuckGo, Brave Search, Baidu Search, Yandex Search	Google Scholar, JSTOR, JYKDOK	DuckDuckGo, Torch, Ahmia, Haystak, Not Evil, Candle, Kilos, LibreY, Toorgle, GDark. Phobos, Excavator

*Search engines and browsers that can search dark web can often be used at every level of the internet.

3.1 Surface Web

The surface web, also known as the visible web, is the part of the internet that can be accessed using regular web browsers such as Firefox or Google Chrome (Khera, 2020). When searching for information using search engines, an internet user may move from one site to another based on the search results. In this case, the user is using the surface web of the internet. (Vienažindyté, 2021) The surface web is the part of the internet that is generally accessible and open to all internet users. It is indexed by search engines and easily searchable through various search engines. (Varma, 2018)

3.2 Deep Web

Although the deep web may sound dubious, all internet users use and rely on it. When using email, private messages on social media, online banking, or reading paid content from various online newspapers intended for subscribers, the deep web is being used. (Vienažindyté, 2021) The deep web refers to a category of content on the internet that has not been indexed by search engines due to various technical reasons (Chertoff & Simon, 2015). Deep web includes databases that cannot be accessed using search engines like Google or Bing. It covers databases that can only be accessed from within an organization, content behind paywalls, pages where content is dynamically created every time they are accessed, and pages that can only be reached via the site's own search system. Additionally, emails and various discussion logs are part of the deep web. (Hatta, 2020) As early as 2000, the deep web was 1,000 to 2,000 times larger than the surface web (Bergman, 2001). In 2013, Barker and Barker concluded that the deep web was over 500 times larger than the surface web (Chertoff & Simon, 2015). Varma noted in 2018 that the deep web made up about 90% of the internet, with only 10% remaining on the surface web. Due to the vast amount of information contained on the internet, comparing or measuring the sizes of the surface and deep web is impossible (Finklea, 2017). In any case, a significant amount of the data found on the web belongs to the deep web.

3.3 Dark Web

The dark web is a part of the deep web that is intentionally hidden and inaccessible through regular web browsers. Using the dark web allows for nearly complete anonymity online by encrypting data packets and routing them through several network nodes. This network node structure is called the 'onion network,' due to its layers of encryption. (Chertoff & Simon, 2015) The anonymity provided by this technology attracts internet users to the dark web, who for one reason or another wish to operate in secret. Activities on the dark web include illegal product sales, sharing dangerous or illegal content, and other illicit or questionable actions. In addition, the Dark Web is used and accessed by, for example, dissidents or people at risk for other reasons, as well as journalists.

Based on the anonymity of the dark web, users can protect themselves and prevent digital tracking (Vienažindyté, 2021). The pattern matching techniques for dark web are related to textual data in form of logs (records). However, data can be classified as different techniques for data mining. Rajawat et.al (2022) divides Dark Web Structural Patterns into the following six categories:

1. Dark Web Click Stream Data

- This approach determines cybercriminal interest and their accomplishments in different problems like illegal trade, forums, terrorist activity, inspecting, and more.

2. News and Sentiment Analysis

- Dark web News and Dark web Sentiment data are unlabeled dark web that characterizes opinions, emotions, and attitudes defined in sources such as blogs, social media posts, online newspapers, online product reviews, and consumer support communications.

3. Dark Web Trending Volume

- Voluminous dark data can be converted to the number of jobs, and then jobs can be quickly processed using the necessary framework.

4. Dark Web Predictive Analytics

- It provides predictive scores to support in creating smart decisions and dark website behavior.

5. Dark Web Text Analytics

- This analytics is the process for originating high, prominent information from raw data, such as unstructured data and forecasting and predicting the analysis.

6. Dark Web Social Media Mining

- Through HADOOP, Facebook, Instagram and other social media discussions can use it to produce targeted real-time information.

4. Indicators

Cyber-attack detection requires the definition of the necessary indicators. Cyber threat intelligence contains Indicators of Compromise (IoC) and Indicators of Attack (IoA).

IoCs are the traditional tactical, often reactive, technical indicator commonly used for detection of threats while IoA is focused upon attribution and intent of threat actors. Another way to conceptualize this thought is to focus on WHAT (IoC) and WHY (IoA) of threat contextualization.

4.1 Indicator of Compromise

Today, the most used indicators in cybersecurity are Indicators of Compromise (IoC). IoCs are evidence that someone may have breached or is attempting to breach an organization's network. These indicators are used to detect malicious activity at an early stage and to prevent known threats. The most common IoCs include IP addresses, DNS names, and the attachment or modification of files. (Anashkin & Zhukova, 2022) IoCs focus on the method of the attack, essentially answering the question "How did the attack happen?" (Brown, n.d.).

The data provided by these indicators not only points to potential threats but can also reveal details of an attack, such as malware, compromised data, or data leaks. IoCs can be identified through event logs, extended detection and response solutions, as well as security information and event management (SIEM) systems. During an active

attack, IoCs can be used to mitigate the threat and reduce damage. After the attack, IoCs help organizations understand what happened, thus enhancing defenses and security to prevent similar attacks in the future. (Microsoft, n.d.)

However, IoCs are not a foolproof method for detecting all the threats that might target a system. They may fail to identify new or modified hacking tools used by advanced and professional attackers due to their uniqueness. IoCs might also be ineffective if an attacker sends many false indicators, filling databases with indicator noise. In this case, defenders must filter through large amounts of indicator data, increasing the risk that real indicators will be lost in the noise. This situation can also lead to a decrease in trust toward existing indicators. Moreover, IoCs may not work if the attacker does not use file-based malware techniques but instead loads malicious code through standard system features like PowerShell. IoCs also do not function proactively; they are designed to react after an attack has already occurred. For these reasons, IoCs are not always effective against modern attack methods, necessitating the use of additional indicators to monitor system security. (Anashkin & Zhukova, 2022)

Various examples of Indicators of Compromise (IoCs) are illustrated in the following list (Trend Micro, n.d.; CrowdStrike, 2022):

- Unusual incoming or outgoing network traffic in the organization's network systems.
- Unusual geographic traffic, i.e., traffic from countries where the organization does not have operations.
- Unknown applications, files, or processes in the system.
- Unusual activity from system administrators or other privileged users.
- An increase in incorrect login or access requests (Brute force attack).
- Large amounts of compressed files or data packets in incorrect locations.
- Many access requests to the same file.
- Unusual DNS requests and registry configurations.
- Unauthorized configuration changes.
- Other unusual activity, such as a significant increase in database size.

4.2 Indicator of Attack

Indicator of Attack (IoA) is digital or physical evidence of a cyber attacker's intention to launch an attack. Unlike Indicators of Compromise (IoC), IoA doesn't solely focus on the tools or methods the attacker uses, but especially on the motives behind the attack. IoA examines the environment through the "Why" question: "Why would someone want to attack us?" Early-stage detection of IoA can help prevent data breaches. (Brown, n.d.)

Using an Indicator of Attack (IoA) can reveal several critical details about a suspected attacker, such as "How did they break into the network?", "Did they exploit backdoors in the system?", or "What critical access credentials did they obtain?". Such information might help defenders detect even unknown attackers or attack methods. Since IoA focuses on the early stages of suspicious activity, it can trigger alerts before the attacker gains access to the system. (Brown, n.d.)

An Indicator of Attack (IoA) is a tool for tracking actions, essentially a rule that includes a method in which an attacker might target a system. This attack method and technique are pre-programmed into the indicator based on various theories and techniques explaining how attacks typically unfold. (Anashkin & Zhukova, 2022). If the indicator detects activity matching the patterns of these theories, it triggers an alert. These indicators can also be refined based on personal experience, making them more accurate and effective. IoA is often considered more effective than IoC (Indicator of Compromise), as attackers find it harder to change their tactics, techniques, and procedures (TTPs) than they do to alter IP addresses, DNS names, or file formats. (Anashkin & Zhukova, 2022)

Table 2: Characteristics of Indicators of Attack (SentinelOne, 2024)

Various tactics by attackers	Definition
Unauthorized Privilege Escalation	Attackers usually exploit vulnerabilities that provide a way to elevate their access to systems in order to manipulate critical systems or disable security controls.
Lateral Movement	Refers to an attacker's efforts to move through the network from one compromised system to another to find valuable data or higher privileges. This movement occurs stealthily as attackers keep quiet while increasing their foothold. IOAs encompass weird connections between internal systems or attempts to access unknown machines.

Various tactics by attackers	Definition
Exfiltration Attempts	This involves the unauthorized transfer of data out of the system. Attackers might attempt to send sensitive information such as intellectual property or personally identifiable information to external destinations. Indications of this type of attack could include large, unexpected transfers of data to unknown servers or abnormal patterns of communication that flow out of the system.
Anomalous Logins	Unusual login attempts, especially from unknown or unfamiliar locations, devices, or odd times can be an indicator of a compromised credential or brute force attacks. Take, for instance, the case of a user who was accustomed to logging in from one geographical location but suddenly exhibits logins from other parts of the world.
Command Execution	This refers to running unknown or unauthorized commands, scripts, or processes that are unrelated to normal user activity. Typically, attackers will use customized scripts when deploying malware or updating configuration settings. When a user account begins executing administrative commands it would not otherwise run, this might represent an active attack.

5. Information Collection from Dark Web

5.1 Cyber-Attack Signals

The most common IOCs of the deep and dark web are the IP addresses and domain names of companies or organizations. They often end up on various leak sites because of data breaches or other cyberattacks. On these sites, the information is shared for free or sold to other cybercriminals for further attacks. Sometimes other information about companies or organizations also ends up in dark web publications, which plan or encourage attacks against these entities. (Webs.io, n.d.)

Personal data collected from data breaches and other cyberattacks, user data for various sites, and identification data of companies or organizations are compiled into compilation lists circulating on the dark web. These compilation lists circulate on the dark web, constantly growing, as information obtained through new cyberattacks is always added to the lists, and older information is not removed from the lists. Thousands or even millions of unique personal data or identification data of organizations can be found on one list. These lists are used by a variety of cyber threat actors. By searching dark web platforms for information about an individual, company or organization, it is possible to find many threatening data leaks, where criminals have obtained critical information that can be used in future cyberattacks. When defending, it is important to know what information about the organization has been obtained by criminals. Based on this leaked information, corrective measures can be taken, whether the information includes email addresses, passwords, IP addresses or even personal data of individuals.

Events or phenomena occur in information networks that in some way indicate a possible cyber threat or the preparation of a cyber-attack. Various models have been created for cyber-attacks (e.g. LM Kill Chain and Mitre ATT&CK). These models contain the basic operating logic and patterns of various attacks, which can be used to create various signals. These signals help to detect an increase in the threat of cyber-attacks soon.

If we can collect information about the cyber-attacker's preparatory phases, we can use them as an opportunity for cyber situational picture and counter measures. For instance, the main goal of network service exploiters is to hijack as many devices as possible. Therefore, they generally target widely used network protocols such as Email, file sharing and VPN. In addition, often not skilled actors do not have the skills to develop the exploit code themselves. Therefore, they use ready-made exploit modules published by companies such as Metasploit, Cobalt Strike, other security researchers or Cybercrime-as-a-Service (CaaS) providers. CaaS includes various forms of services such as Ransomware-as-a-Service (RaaS), Malware-as-a-Service, Botnets-for-hire, Credential theft services and Distributed Denial of Service-as-a-Service (DDoSaaS). Nowadays cybercriminal no longer needs to be technically oriented, but they simply can buy different kinds of services to perform cyberattacks. These kinds of services are regularly sold in various dark web platforms.

For cyber situational awareness and early warning, Security Operation Centers (SOCs) in particular need observations of potential cyberattack preparations. Various signals can be detected from different sources and can be used to initiate the collection of additional information, increase security readiness and take countermeasures if necessary.

The following table 3 presents examples of different signals and further observations that can be made based on them.

Table 3: Possible cyber-attack signals and follow-up measures (Robindimyan, 2022)

Signal	Further observations	Remarks
A new vulnerability of a widely used network service has been discovered.	Get more information from the National Vulnerability Database (NVD). Common Vulnerabilities and Exposures (CVE).	The NVD is the U.S. government repository of standards, based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance. The NVD includes databases of security checklist references, security-related software flaws, product names, and impact metrics. CVE system provides a reference method for publicly known information-security vulnerabilities and exposures.
The exploit module for the given vulnerability has become available	Get more information from cybersecurity companies about system vulnerabilities and identification. Get information from public data resources such as Exploit-db, GitHub, Cobalt Strike, Dark Web Tools.	The Exploit Database is a CVE compliant archive of public exploits and corresponding vulnerable software. GitHub provides access control, bug tracking, software feature requests, task management, continuous integration, and wikis. Cobalt Strike is a tool that is used to replicate the tactics and techniques of long-term embedded attackers in red teaming engagements and adversary simulations.
A new exploit code has become available for a known vulnerability.	Same steps as above.	Exploit module = a part of software or tool designed to exploit vulnerability. Exploit code = code written to exploit vulnerability.
An exploit kit has begun to be advertised in crime markets.	Get more information using Dark Web Tools.	Exploit Kit = a collection of multiple exploit modules and code combined into a single package. Designed to exploit a vulnerability automatically and often containing multiple vulnerabilities in different software.
An exploit has been observed in use.	Follow information of the public and private cyber organizations, like Cybersecurity and Infrastructure Security Agency (CISA)	CISA is the operational lead for US federal cybersecurity and the national coordinator for critical infrastructure security and resilience.

5.2 Dark Web Monitoring

Dark web monitoring is a service and process offered by cyber security vendors that scans the dark web for information pertaining to an organization. These software scan and search dark web websites and forums checking for organization's information against compromised datasets being traded or sold. (Ferrill, 2024) Dark web monitoring tools are like surface web search engines) for the dark web. These tools help to find leaked or stolen information such as compromised passwords, breached credentials, intellectual property and other sensitive data that is being shared and sold among malicious actors operating on the dark web. (Lenaerts-Bergmans, 2023)

From Cyber Threat Intelligence perspective is very important to know what data these sites are offering. The dark web is a source of intelligence on the operations, tactics, and intent of cyber-criminal and state sponsored groups. There are tools and services that monitor the dark web for compromised data and provide critical information into areas of the dark web that are potentially outside our normal view. Dark web monitoring typically involves a combination of software tools tailor-built for monitoring and security researchers versed in the intricacies of potential threats and the social culture of the internet underworld. (Ferrill, 2024)

If your data have been found from the dark web, immediate and decisive actions are essential. You must evaluate the extent of the breach and take measures to contain it. This may involve shutting down some specific network segments or changing access credentials such as passwords and usernames. You also need to

understand any legal ramifications, especially concerning data protection regulations like GDPR or CCPA. Depending on the nature of the data, you might need to inform affected clients, partners, or employees about the breach and control the narrative to outside of the organisation. A swift, transparent response can help mitigate reputational damage. (Burke, 2023)

Table 4: Presents examples of companies that offer Dark Web services and tools.

Tool	Description
Brandefense	It is an AI-driven DRPS solution that scans the surface web and the dark web to glean detail on attack methods or data breaches, correlating this data and contextualizing it, and then providing alerts when an incident has relevance to your brand.
CrowdStrike Falcon Adversary OverWatch	It provides insights and visibility into dark web references to corporate data, identities, and brands, even proactively blocking threats before they become incidents.
CTM360 CyberBlindspot and ThreatCover	CTM360 offers two different solutions that monitor the dark web. It exposes indicators of warning or indicators of attack, allowing organization to identify areas of concern from network even more proactively.
Cyber Intelligence House	It delivers threat intelligence services with real-time monitoring of the dark web, deep web, malware, infostealers, hacker chatter and breaches.
CyberWatch Finland	A comprehensive situational picture of cybersecurity is created with the help of the modular service. Service extensively uses dark and deep web data.
DarkOwl Vision UI	DarkOwl Vision UI supports searching collated dark web data feeds using standard text search, Boolean logic to quickly focus in on key categories.
IBM X-Force Exchange	is primarily a data sharing platform and community, bringing threat and intelligence feeds into an interactive, searchable database.
Malware Information Sharing Platform	MISP is an open-source platform shaped around the idea of shared threat intelligence data.
Mandiant Digital Threat Monitoring	It offers visibility into intelligence pertaining to threats and leaked credentials or other corporate secrets on the open internet or the dark web.
OpenCTI	It is an open-source option for collecting, managing, and interacting with intelligence data.
Rapid7's Threat Command	It offers combined external threat intelligence, digital risk protection, indicators of compromise (IOCs) management, and remediation.
Recorded Future Intelligence Cloud Platform	It offers features constant monitoring of over 300 state actors, 3 million known criminal forum handles, billions of domains and hundreds of millions of IP addresses across the internet and dark web.
SearchLight Cyber	Spotting the earliest warning signs from dark web of an attack including leaked credentials, vulnerabilities, & chatter.
SOCRadar Advanced Dark Web Monitoring	SOCRadar offers several services and tools like insights into compromised credentials, brand impersonation, or vulnerabilities in organizations public footprint. Advanced Dark Web Monitoring offers monitoring for employee PII (personally identifiable information).
ZeroFox Dark Web Monitoring	ZeroFox Dark Web Monitoring is another software that aims to simplify the process of surfacing risks from the dark web.

6. Discussion and Conclusion

Managing situational awareness involves identifying and understanding the various threats in the operational environment. The organization must be aware of the different threats in the cyber environment, understand the risks they pose, and consider the potential consequences of these risks. The organization needs to identify the weighting factors of various threat actors to assess the severity of different threat scenarios. (Koskimäki, 2024)

Finally, this paper incorporates Dark Web information from cyberattacks according to Shakarian's (2017) four-tier Cyber Threat Intelligence model. Shakarian model can be considered a solid foundation for strategic cyber threat intelligence planning. This tiered model allows organizations to preliminarily assess and structure their cyber threat intelligence efforts in the right direction.

In the Dark Web environment at the Situational Awareness tier, it is appropriate for everyone to share this information with other actors. Information Sharing and Analysis Center (ISAC) groups can share information about observed IoA and IoC.

The purpose of Imminent Threats tier is to identify imminent threats to the organization. In practice, the simplest way to produce this situational awareness of imminent threats is to deploy web crawlers on dark web platforms

or conduct OSINT in the dark web to determine whether there has been any discussion about the organization on such platforms.

The Understanding Capabilities tier is more advanced and forward-looking. At this stage, the goal is to understand how attackers' capabilities are evolving. What programs or methods do hackers have at their disposal or what they are currently developing? Dark Web monitoring provides indications of what kinds of tools, methods, or attack vectors are being planned or have been used.

Tier of Understanding Communities involves striving to know the activities of malicious hacking communities in as broad and deep manner as possible. This includes comprehending the dynamics of dark web markets, the significance of certain key individuals within them, and the rises and falls of different community platforms. Information on these community platforms is often available only for a limited time, which is why data collection must be continuous. For example, ransomware operators may post recruitment advertisements on them. This indicates active and growing threat actors whose development should be monitored in the future.

Since most data breaches and other cyberattacks occur because an individual makes a mistake, it is crucial for organizations to ensure continuous cybersecurity hygiene and training for their employees. In cybersecurity, the importance of individual actions cannot be underestimated. Since mistakes still occur despite training, it is important to establish various indicators that monitor the organization’s systems. These indicators enable proactive or early-stage responses to emerging threats. The development and reliability of these indicators must be studied more thoroughly and extensively in the future. By creating and actively updating indicators, organizations can better monitor and protect their systems.

References

Anashkin Y. & Zhukova M. (2022). Implementation of Behavioral Indicators in Threat Detection and User Behavior Analysis, Semantic Scholar, Corpus ID: 248204962.

Basheer, R. & AlKhatib, B. (2021). Threats from the Dark: A Review over Dark Web investigation Research for Cyber Threat Intelligence, Journal of Computer Networks and Communications, Wiley Online Library, 20 December 2021 https://doi.org/10.1155/2021/1302999

Bergman, M. K. (2001). White Paper: The Deep Web: Surfacing Hidden Value. The Journal of Electronic Publishing, 7(1).

Brandefence. (2022). Top 10 Deep Web Browsers and Search Engines, May 9, 2022, https://brandefense.io/blog/dark-web/top-deep-web-browsers-and-search-engines/

Brown, S. (n.d.). Indicator of Attack (IOA) Seurity. https://www.strongdm.com/what-is/indicator-of-attack-ioa-security

Burke, T. (2023). How to Tell if Your Information is On the Dark Web, Quest, November 21, 2023.

Chertoff, M. & Simon T. (2015). The impact of the dark web on internet governance and cyber security, Centre for International Governance Innovation and the Royal Institute for International Affairs, paper series: NO. 6, Feb 2015.

Crowdstrike (2022). Indicators of Compromise (IOC) Security. Cybersecurity 101. https://www.crowdstrike.com/cybersecurity-101/indicators-of-compromise/

Ferrill T. (2024). 12 dark web monitoring tools, CSO Online, 11 Sep 2024, https://www.csoonline.com/article/574585/10-dark-web-monitoring-tools.html

Finklea K. (2017). Dark Web, Congressional Research Service, March 10, 2017.

Ghimiray D. (2024). Best search engines to search the dark web, Avast, November 26, 2024, https://www.avast.com/c-best-dark-web-search-engines#

Hatta M. (2020). Deep web, dark web, dark net: A taxonomy of “hidden” Internet. Annals of Business Administrative Science, 19(6), 277–292.

Khera, V. (2020). The Web Layers: Introduction to Surface, Deep and Darknet. https://cyberprotection-magazine.com/the-web-layers-introduction-to-surface-deep-and-darknet

Koskimäki T. (2024). Utilizing the dark web in creating and maintaining a proactive cyber situational picture, Master’s Thesis, University of Jyväskylä.

Lehto M. (2022). Cyber-attacks Against Critical Infrastructure, in Lehto M. and Neittaanmäki P. (Eds.) Cyber Security: Critical Infrastructure Protection, in series Computation Methods in Applied Sciences, Springer, pages 3-42.

Lenaerts-Bergmans B. (2023). Dark Web Monitoring, CrowdStrike blog, April 27, 2023, https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/dark-web-monitoring/

Microsoft (n.d.). What are indicators of compromise (IOC)? Microsoft Security. https://www.microsoft.com/en-us/security/business/security-101/what-are-indicators-of-compromise-ioc

Pöyhönen J. & Lehto M. (2024). Architecture framework for cyber security management, 23rd European Conference on Cyber Warfare and Security, 27 - 28 June 2024, Jyväskylä, Finland, pages 388-397.

Rajawat A, Bedi P, Goyal S., Kautish S., Xihua Z, Aljuaid H, Mohamed A (2022). Dark Web Data Classification Using Neural Network, Wiley Online Library, 28 March 2022.

Robindimyan (2023). Early Warning Intelligence — How to predict cyber attacks? Oct 9, 2022, Early Warning Intelligence — How to predict cyber attacks? | by Robindimyan | Medium

SentinelOne (2024). What are Indicators of Attack (IOA) in Cybersecurity? https://www.sentinelone.com/cybersecurity-101/threat-intelligence/indicators-of-attack-ioa/

Shakarian, P. (2017). The Enemy Has a Voice: Understanding Threats to Inform Smart Investment in Cyber Defense. New American Policy Paper, Feb. 28, 2017.

Trend Micro (n.d.). Indicators of compromise. https://www.trendmicro.com/vinfo/us/security/definition/indicators-of-compromise

Varma S. (2018). CISO Guide: Surface Web, Deep Web and Dark Web – Are they different? https://www.cisoplatform.com/profiles/blogs/surface-web-deep-web-and-dark-web-are-they-different

Vienažindyté, I. (2021). Syväverkko: mikä on deep web ja minkälaisia vaaroja siihen liittyy? NordVPN, https://nordvpn.com/fi/blog/mika-on-deep-web/

Webz.io (n.d.) All You Need to Know about IOC Monitoring on the Dark Web, https://webz.io/dwp/all-you-need-to-know-about-ioc-monitoring-on-the-dark-web/