|  |  |
| --- | --- |
| **Course code and name:** | F20DE/F21DE Digital and Knowledge Economy |
| **Type of assessment:** | ***Group*** |
| **Coursework Title:** | Creating an Innovative Startup in Digital Economy |
| **Student Name:** | Group 10 |
| **Student ID Number:** | H00415334, H00393446, H00411030, H00397506, H00323794 |

|  |
| --- |
| **Declaration of authorship. By signing this form:**   * **I declare** that the work I have submitted for individual assessment OR the work I have contributed to a group assessment, is entirely my own. I have NOT taken the ideas, writings or inventions of another person and used these as if they were my own. My submission or my contribution to a group submission is expressed in my own words. Any uses made within this work of the ideas, writings or inventions of others, or of any existing sources of information (books, journals, websites, etc.) are properly acknowledged and listed in the references and/or acknowledgements section. * I confirm that I have read, understood and followed the University’s Regulations on plagiarism as published on the [University’s website](https://www.hw.ac.uk/uk/students/studies/examinations/plagiarism.htm), and that I am aware of the penalties that I will face should I not adhere to the University Regulations. * I confirm that I have read, understood and avoided the different types of plagiarism explained in the University guidance on [Academic Integrity and Plagiarism](https://heriotwatt.sharepoint.com/sites/skillshub/SitePages/Academic-Integrity-and-Plagiarism.aspx)   **Student Signature** *(type your name): Group 10*  **Date**: *27/02/2023* |

Copy this page and insert it into your coursework file in front of your title page.

For group assessment each group member must sign a separate form and all forms must be included with the group submission.

**Your work will not be marked if a signed copy of this form is not included with your submission.**



**Coursework** **1**- **F20DE/F21DE – Digital and Knowledge Economy**

## **Topic: Creating an Innovative Startup in Digital Economy**

## **Group Members**

1. **Ansh Raj Rastogi, H00415334 (Group Leader)**
2. **Jamie Evennett, H00323794 (Group Member)**
3. **Anupam Shankar Anil Kumar, H00411030 (Group Member)**
4. **Tiasha Biswas, H00397506 (Group Member)**
5. **Mukul Kotwar, H00393446 (Group Member)**

## **Group Name: Data Defenders (Group 10)**

## **Submitted by: Ansh Raj Rastogi**

# **Peer-Assessment Form**

|  |  |
| --- | --- |
| Name | Contribution |
| Ansh Raj Rastogi | 1.1,2.1 |
| Anupam Shankar Anil Kumar | 1.2,2.2 |
| Jamie Evennett | 1.3,1.4 |
| Mukul Kotwar | 1.3 |
| Tiasha Biswas | 1.3 |
| Anant Gujrathi | None |
| Muhammad Gulfam | None |
| Iain Forrester | None |

# **Index**

|  |  |
| --- | --- |
| Topic | Page |
| 1.1 Problem Statement | 5 |
| 1.2 Executive Summary | 6 |
| 1.3 Technical Literature Survey | 7 |
| 1.4 Deployment and Impact of your company | 10 |
| 2.1Competitive Study | 11 |
| 2.2 - Business Model Canvas | 13 |
| References: | 14 |

# **1.1 - Problem Statement**

Cyber-attacks have become a significant concern in the modern digital era due to their potential to cause extensive damage to individuals, organizations, and societies. There are numerous risks, problems, and gaps caused by cyber-attacks that need to be addressed. In this response, we will outline some of the major risks, problems, and gaps caused by cyber-attacks and provide references to support these claims.

* **Financial loss**: Individuals, businesses, and governments may suffer large financial losses because of cyberattacks. For instance, ransomware attacks cost businesses more than $20 billion in losses in 2020, a 75% increase from the year before. These costs may be brought on by cyberattack-related reputational harm, downtime, productivity loss, and data theft (Cybersecurity Ventures, 2020).
* **Data breaches**: Cyber-attacks like malware, phishing, and ransomware can expose private information to unauthorised people or organisations. Identity theft, financial loss, and reputational harm to people and businesses are all possible outcomes of these breaches. The bulk of reported cyber incidents in 2020 were data breaches, with external actors responsible for 43% of all breaches (Verizon, 2021).
* **Identity theft**: Identity theft via cyber-attacks can cause financial loss, reputational harm, and emotional misery. 15% of all reported cybercrime events in the US in 2020 were related to identity theft (Federal Bureau of Investigation, 2020).
* **Vital infrastructure disruption**: Cyberattacks have the potential to seriously harm critical infrastructure, such as water supply systems, transportation networks, and power grids. These assaults may cause significant inconveniences and potentially endanger public safety (Bogdanov et al., 2020).
* **Disinformation propagation**: Cyberattacks can be used to disseminate propaganda and false information, which can have a huge negative influence on people, groups, and entire society. For instance, Russian hackers utilised social media to spread misinformation during the 2016 US presidential election, influencing voters' perceptions and potentially influencing the result of the election (House Intelligence Committee, 2018).
* **Cyberbullying** is a form of cyberattack that can have catastrophic effects on people, particularly children and teens. Cyberbullying may result in unhappiness, anxiety, and even suicide (Patchin & Hinduja, 2018).

It is imperative to address the dangers, issues, and gaps brought on by cyberattacks. These assaults have the potential to result in large monetary losses, damage to vital infrastructure, disinformation, and psychological harm to people. A multifaceted strategy, including technology solutions, political interventions, and public education, is needed to address these concerns. We can lower the dangers and lessen the effects of cyberattacks on people, societies, and communities by taking these measures.

# **1.2 - Executive Summary**

Our motive is to provide secure communication by minimising the risks of various cyber-attacks aimed at individuals and organisations. Since our target is to protect the customers’ data from being exposed to attackers, we thought that “Data Defenders” would be the best name that defines our company and the nature of our business.

Of the various kinds of cyber-attacks, DNS attacks are very prevalent and countering them is one of the main research topics now. DNS (Domain Name Service), very commonly referred to as the “Phonebook of the internet,” translates the human readable domain names (e.g., [www.google.com](http://www.google.com/)) to machine readable IP addresses (e.g., 10.101.12.34). There are several types of DNS attacks such as domain lock-up attacks, DNS hijacking, DNS spoofing, DNS Tunnelling.

Our solution relies on an Intrusion Detection System that uses Ensemble Learning methods to classify DNS traffic into genuine or malicious categories (Chijioke Ahakonye et al., 2022). Ensemble Learning is a technique that consists of a combination of various machine learning/AI models combined to determine a solution to the problem at hand. This will help to predict if a DNS communication is benign or is having a malicious intent. Our solution also considers the response time as crucial factor since these communications are real time and a delay in predicting a potential attack could lead to exploitation of vital information.

We have developed a product that offers the customers multiple levels of security. Our primary focus is on DNS attacks, but we also provide additional features such as protection from other kinds of threats like malware, trojan and phishing with the help of deep learning techniques. We offer multiple packages where each higher-level package has at least one added feature in terms of security, storage, and customisation. We also provide a trial version for 30 days with limited features, so that users can get a feel of the product and buy a full version if they like it.

The product will be available as a ready to install package from our online website. The trial version will run without a product key. The users will be asked for a product key once the trial version expires. Once the user pays for a full version, a product key will be sent to the user’s registered email address. Entering this product key would unlock the premium features and extend the term of usage.

# **1.3 - Technical Literature Survey**

**Identity theft**: - Cyberattack-related identity theft can harm individuals and businesses financially and personally. Several new technologies and methods can help prevent cyberattack-related identity theft. These work best:

* Multi-Factor Authentication (MFA): MFA requires account access with more than a password. Fingerprints, facial recognition, or phone codes can be used. MFA prevents cybercriminals from accessing sensitive data.
* Password managers: generate and store complex passwords for users. This prevents users from using weak passwords across multiple accounts, making them vulnerable to cyberattacks. Password managers can also store all passwords securely
* Biometric Authentication: Fingerprints or facial features are used to verify a user's identity. This is safer than passwords, which can be stolen or guessed.
* Identity and Access Management (IAM): IAM systems help organisations secure user access to critical resources. IAM systems enforce strict access controls and authentication policies to protect sensitive data.
* AI and ML: AI and ML can alert security teams to suspicious behaviour or activity. These technologies can also detect and stop cyber-attacks in real time, protecting systems and data.
* Blockchain technology creates secure, decentralised data storage and sharing systems. This makes it harder for hackers to steal data and prevents cyber-attacks.

Defending against cyberattack-related identity theft requires a multi-pronged approach. Using the latest security and data protection technologies and best practises can greatly reduce the risk of cyber-attacks and protect sensitive information.

Alternate solutions for identity theft protection:

Domain Name System-based Authentication of Named Entities (DANE): DANE uses DNS records to authenticate SSL/TLS certificates. Man-in-the-middle attacks, in which attackers intercept and tamper with communications, can be prevented.

Anycast DNS: Distributing DNS servers over several sites. This can increase performance, resilience, and DNS-based attack resistance.

DNS filtering stops harmful domains and webpages. This can prevent users from accidentally visiting harmful sites and becoming victims of phishing or identity theft.

Safe DNS providers: Encryption and threat intelligence assist prevent DNS-based assaults. Cloudflare, Google Public DNS, and OpenDNS offer secure DNS.

Zero Trust Network Design considers that all users and devices, inside and outside the network, are potential threats. This method verifies user and device identities, encrypts data in transit, and restricts resource access to need-to-know users.

**Data Breaches:** Protecting againstmalware, hackers and malicious intent are becoming more prominent as technology becomes more advanced and more systems become integrated online. Therefore, it is imperative that companies no matter what scale, are protected. Here are various current methods used to guard against data breaches:

* Educating the workforce and spreading awareness: One of the best ways to avoid many data breaches is simply being educated on the matter of malware and its many forms. For example, phishing e-mails are quite easy to spot for people who are educated on such matters therefore increasing awareness and educating your employees will lead to a decreased chance of people accidentally giving out confidential data and falling for scam e-mails.
* Creating back-ups and data recovery: It is good practice to back up any important data that an organisation has and being able to implement data recovery solutions can be crucial especially if the systems are vital to the organisation. An example of this being beneficial would be if a system has been under attack such as distributed denial of service, trojans and injection which would cause the system to either lose files or switch off in some way which can corrupt data, being able to have backups can keep systems functioning and being able to recover the data can mitigate damages.
* Encryption and Cryptography: In an organisation, the exchange of data is mandatory to keep the company functioning and sustainable therefore any handling of confidential data needs to be protected and one way of doing that is by encrypting the data which stops hackers from being able to comprehend what the ineligible data means and that the recipient can decrypt and read the message safely. Cryptography also has several techniques and ciphers that can be implemented to make brute force and monitoring incredibly difficult for eavesdroppers (Katz, 2019).

Currently, there is interest in developing data leak prevention and detection systems (DLPD) however many factors keep organisations from implementing them such as timeliness, scalability, and upkeep along with needing trained employees to monitor these systems. DLPD can help organisations monitor, detect, and prevent the unintentional or malicious exposure of data in an enterprise environment. DLPD becomes more desirable as big data is incredibly important in this era therefore proper systems must be designed to mitigate, prevent, and protect sensitive information. DLPD techniques can be grouped into two categories which are basic security measures and designated DLPD approaches. Basic security measures can be your anti-virus software and firewalls, but DLPD approaches specifically focus on the prevention of data leakage (Cheng, Liu and Yao, 2017).

**Financial loss**: The deployment of a DNS firewall is one alternative solution that combines intrusion detection systems (IDS) and ensemble learning to minimise financial losses in organisations caused by DNS attacks. These losses can be caused by malicious users trying to get access to a company's domain name system.

A DNS firewall is a security system that detects and prevents DNS threats in real time by combining DNS-based threat information with machine learning and artificial intelligence (AI) algorithms. It can recognise and block suspicious domain name system (DNS) queries that may signal a DNS attack. Some examples of DNS attacks include domain generation algorithms (DGA), DNS cache poisoning, and domain name system tunnelling.

The results of several different machine learning models are combined in an approach called ensemble learning, which is utilised by a DNS firewall. This helps to enhance accuracy and reduce the number of false positives. This strategy enables the system to recognise and respond to new and emerging DNS assault methods, some of which may not be identified by a single model. This is made possible by the concept of using many models.

A DNS firewall can also provide organisations with granular control over DNS traffic, giving them the ability to ban or allow specific domains or IP addresses. This control can be provided to the business in the form of granular control. This helps prevent financial losses by restricting unwanted access to financial information and other sensitive data. This also helps prevent losses of other types of sensitive data.

Other DNS-based security solutions, such as DNSSEC (DNS Security Extensions) and DANE (DNS-based Authentication of Named Entities), can be implemented by businesses in addition to a DNS firewall to protect against DNS attacks and guarantee the integrity of DNS data. These solutions are both examples of DNS-based authentication of named entities.

In general, the deployment of a DNS firewall that includes intrusion detection systems (IDS) and ensemble learning can be an efficient method for companies to protect themselves against financial losses brought on by DNS attacks. However, it is essential to keep in mind that no solitary technology can offer fool proof defence against cyberattacks. Therefore, an all-encompassing cybersecurity strategy should incorporate several different technologies, policies, and best practises in order to reduce the likelihood of potential problems.

Security in the cloud: As more and more companies shift their data and apps to the cloud; cloud security is becoming an increasingly essential topic. Cloud security technology can assist in providing protection against data breaches and other forms of cyberattacks, both of which can result in monetary losses.

The cybersecurity strategy known as "zero-trust security" operates under the presumption that each individual user and piece of hardware connected to a network contains the potential to provide a security risk. This strategy involves checking the credentials of every user and device that attempts to access a network or application and allowing access to the system only if the user or device satisfies a set of predetermined safety standards.

The term "endpoint security" refers to the process of securing the numerous computers, mobile devices, and servers that connect to a network. Examples of endpoints include laptops and mobile devices. Using anti-virus software, firewalls, and encryption software are all examples of possible measures that can be taken to protect against cyber threats.

# **1.4 - Deployment and Impact of your company**

Data Defenders will deploy various solutions into the market targeting individuals and companies through various package schemes through our online website. For example, a standard package from our online website would include the standard frameworks, plug-ins, firewalls, detectors etc. that will be used to protect companies against malicious malware and software and have the basic functionality to ensure security of private data and to reduce the probability of data breaches while also increasing the chance of detecting any unknown software allowing for preventative action.

From there, several other packages can also be bought e.g., ‘Gold Package, Diamond Package’ where each increasing package level will provide more security features, accessibility options, developer settings, better encryption, warranties, more servers, and storage etc. at a higher price.

We have decided to go with this strategy as not only does it allow for a more diverse range of products but it also satisfies the many different situations that companies or individuals are in, for example, a big corporation would benefit more with the highest level package as it contains the highest security that Data Defenders can provide at a higher cost which this corporation can afford while another situation is a start-up company that does not have as much revenue to spend therefore they can buy the standard package where they will still benefit from Data Defender’s protection at a cheap and affordable price.

We believe that everyone should be protected from the dangers of the online world and with more diverse products, the more customers we can protect in their given situation! We think it is best to allow our customers to purchase our products online as e-commerce has been steadily on the rise and being far more lucrative and popular compared to traditional methods (Rheude, 2019). Also, a website provides numerous benefits such as allowing customers to buy our products from anywhere and allowing for online transaction without the hassle of waiting for delivery and being able to learn about our company and the many products that we can offer to them (Maat and Konings, 2018).

With regards to our problem statement, our security techniques and packages will allow companies to be better equipped against data breaches and cyberattacks which can save millions and billions in financial loss, prevent numerous types of cyberattacks such as trojans, phishing and identity theft, and maintaining integrity and stability in critical systems which can potentially save lives.

# **Part 2**

# **2.1 - Competitive Study**

Comparing several methods for creating an efficient intrusion detection system using ensemble learning techniques is referred to as a competitive study for intrusion detection system systems. A machine learning technique called ensemble learning involves merging various models to enhance the system's overall performance.

Here are some advantages of ensemble learning:

* **Improved accuracy:** In comparison to individual models, ensemble learning improves accuracy and lowers error rates by combining the outputs of numerous models. This is especially helpful in intrusion detection, where precision is crucial and false positives and false negatives can have major repercussions.
* **Robustness:** Because numerous models are combined to smooth out mistakes and inconsistencies, ensemble learning can be more resistant to noisy or incomplete data. This is crucial in intrusion detection because attackers may employ strategies to hide their actions and avoid detection.
* **Adaptability:** By integrating new models or altering current ones, ensemble learning may adjust to changing conditions, such as new sorts of attacks. As a result, it is a more adaptable and scalable method of intrusion detection.
* **Diversity:** Ensemble learning mixes several models with various architectures, parameters, and training sets. By lowering the chance of overfitting and capturing various parts of the data, this variety can enhance the system's overall performance.
* **Resilience:** When faced with attacks that are intended to go undetected, ensemble learning is frequently more resistant.

It may be harder for attackers to anticipate and escape detection by combining various detection approaches and models. Comparing ensemble learning to other conventional techniques, it can offer a more reliable and effective approach to intrusion detection. However, the specific advantages will vary depending on the implementation and application.

To do a competitive analysis for a company using ensemble learning for intrusion detection, we must first identify and assess the market's current competitors. These are a few potential rivals, along with their advantages and disadvantages:

* **Darktrace**: A cybersecurity business with headquarters in the UK, Darktrace use machine learning and AI to find online threats. Their strategy is comparable to ensemble learning because it combines various AI algorithms to produce an all-encompassing picture of network activity. The sophisticated AI algorithms used by Darktrace and their capacity to recognise new and emerging threats are some of its primary advantages. However, the complexity and difficulty of configuring and maintaining their system may prevent smaller organisations from using it.
* **TrendMicro**: TrendMicro is a multinational cybersecurity firm that provides a variety of intrusion detection products, including their XDR platform that employs machine learning to identify and address threats. The XDR platform from TrendMicro is simple for organisations to use and includes several interfaces with other security solutions. False positives and missed detections, on the other hand, have been mentioned by a few users, which may have an impact on the system's efficacy.
* **Cisco**: Cisco is a top supplier of networking and cybersecurity solutions, and one of these solutions is the Stealth watch system, which employs machine learning to find risks. The networking know-how of Cisco and its products' capacity for integration with other Cisco goods are among its advantages. Yet, the cost and complexity of their system may prevent smaller businesses from using it.
* **Vectra AI**: Vectra AI is a cybersecurity firm that employs AI and machine learning to identify threats and take appropriate action. They utilise many models to examine network data and spot anomalies, which is a method akin to ensemble learning. The strengths of Vectra AI include their capability to recognise sophisticated threats and their intuitive user interface. Yet, implementing and maintaining their system could be expensive and need large resources.

Overall, there are several competitors in the market for ensemble learning-based intrusion detection, each with unique strengths and disadvantages. Our company sets itself apart in this industry through its approach to ensemble learning, user-friendly interface, and capacity to offer continuing assistance and training to its clients. To make sure we can compete with already-established competitors in the market, we would take pricing and scalability into account.

# **2.2 - Business Model Canvas**

|  |  |  |  |
| --- | --- | --- | --- |
| **Problem** | **Solution** | **Unique Value Proposition** | **Customer Segments** |
| Increasing Cyber-attacks in the digital world leading to multiple issues like Data breach, identity theft, monetary loss, and so on. | Develop an Intrusion Detection System that specializes on DNS attacks with the help of ensemble learning | 1. Protects against DNS Attacks, which is a common mechanism to steal sensitive information 2. Protects against malware. 3. Improved user experience and ready to install module. 4. Multiple package plans to increase choices for the customers, thereby increasing the chances of buying the product. | 1. Individual users, for securing their personal computers from attacks. 2. Enterprises with IT departments intending to prevent DNS or malware attacks. 3. Government organizations |
|
|
|
| **Existing Alternatives** |
| Darktrace, TrendMicro, Cisco, Vectra AI |
|
|
|
|
| **Key Activities** | **Key Resources** | **Cost Structure** | **Revenue Streams** |
| 1. Create and support Intrusion Detection System. 2. To keep track of the emerging threats, conduct research activities for new threats. 3. Marketing to attract new customers. 4. Provide good customer support and troubleshoot to existing customers. | 1. Developers having valuable experience in countering cyber security attacks. 2. Engineers specialized in Artificial Intelligence. 3. Front end engineers to develop the user interface. 4. Skilled and experienced cloud engineers for effective deployment and maintenance. 5. Marketing and sales team to promote the product. 6. Support Engineers to handle troubleshooting and customer training. | 1. Development and maintenance cost for software. 2. Hosting the software securely and effectively. 3. Marketing and sales expenses. 4. Research expenses to identify new threats. 5. Employee compensation | 1. License fees for using the software, varying according to the package plan. 2. Fees for troubleshooting or extended customer support. |
|
|
|
|
|
|
|
|
|

# **References:**

* Bogdanov, E., Ponomarev, A., Rybalchenko, A., & Voas, J. (2020). Cybersecurity of Industrial Control Systems: A Survey. IEEE Communications Surveys & Tutorials, 22(1), 489-520.
* Braue, D. (2021). *Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031*. [online] Cybercrime Magazine. Available at: <https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/>.
* Internet Crime Complaint Center (2020). *2020 Internet Crime Report*. [online] FBI. Available at: <https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf>.
* House Intelligence Committee. (2018). The Russia Investigations: Report on Russian Active Measures. Retrieved from https://www.intelligence.senate.gov/sites/default/files/documents/Report\_Volume2.pdf
* Patchin, J. W., & Hinduja, S. (2018). Cyberbullying among adolescents: A case study of its nature and effects. Journal of School Violence, 17(2), 118-133.
* Chijioke Ahakonye, L.A., Ifeanyi Nwakanma, C., Ajakwe, S.O., Min Lee, J. and Kim, D.-S. (2022). *Countering DNS Vulnerability to Attacks Using Ensemble Learning*. [online] IEEE Xplore. doi:https://doi.org/10.1109/ICAIIC54071.2022.9722641.
* Rheude, J. (2019). *The 2010s: A Decade of ECommerce Growth*. [online] Red Stag Fulfillment. Available at: <https://redstagfulfillment.com/2010s-ecommerce-growth-decade/>.
* ‌Maat, K. and Konings, R. (2018). Accessibility or Innovation? Store Shopping Trips versus Online Shopping. *Transportation Research Record: Journal of the Transportation Research Board*, [online] 2672(50), pp.1–10. doi:https://doi.org/10.1177/0361198118794044.
* Katz, J. (2019). *Introduction To Modern Cryptography.* CRC Press.
* Cheng, L., Liu, F. and Yao, D.D. (2017). Enterprise data breach: causes, challenges, prevention, and future directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, [online] 7(5), p.e1211. doi:https://doi.org/10.1002/widm.1211.
* Abraham D. Sofaer, Seymour E. Goodman, A.D.S.S.E.G. (ed.) (2020) *The Transnational Dimension of Cyber Crime and Terrorism*. Available at: <https://books.google.co.uk/books?hl=en&lr=&id=yY0nAgAAQBAJ&oi=fnd&pg=PP1&dq=technologies+to+combat+financial+loss+due+to+cyber+attacks&ots=MfuO5vk57P&sig=X2sLHPFuIS5k85miyvHqy138loo&redir_esc=y#v=onepage&q=technologies%20to%20combat%20financial%20loss%20due%20to%20cyber%20attacks&f=false> (Accessed: 2023).
* r, B. (2006) *Emerald logo*, *Developments in the global law enforcement of cyber‐crime Roderic Broadhurst* . Available at: <https://www.emerald.com/insight/content/doi/10.1108/13639510610684674/full/html#idm45716301116384> (Accessed: February 27, 2023).