Dtect Assignment 4:

Customer Value Proposition

Alan Chen, Weiyuan (Carl) Che, Or Aharoni, Rutwa Engineer, Xi Huang

Part 1: Business Model Canvas

Customer Segments: Our product provides insider threat detection which can prevent potential security incidents and save our target market, large financial firms with most workers working from home, from financial and reputational loss. It also benefits the cybersecurity engineers and directors since an efficient, well-performing tool can be essential to succeeding in their professional positions.

Value Propositions: Our solution offers two major services where value is created. The display of aggregated activity logs which provides a clear visualization of user activities and a machine learning model which has the ability to detect threats through analyzing the activity logs.

Distribution Channels: Our product offers services through a webapp where our customers will have access to services that create value such as user activity display.

Customer Relationships: We would establish customer relationships where our customers would request our services and we would be the provider of automation for the insider threat detection process and data analysis.

Revenue Streams: Our revenue will be gathered through a quarter-annually subscription service.

Key Activities: For the product to perform well, our app will first have to fulfill its function. It will have to display useful aggregates of user activities in detail and make correction predictions of anomalies to prevent security incidents. Our team will also constantly update and improve

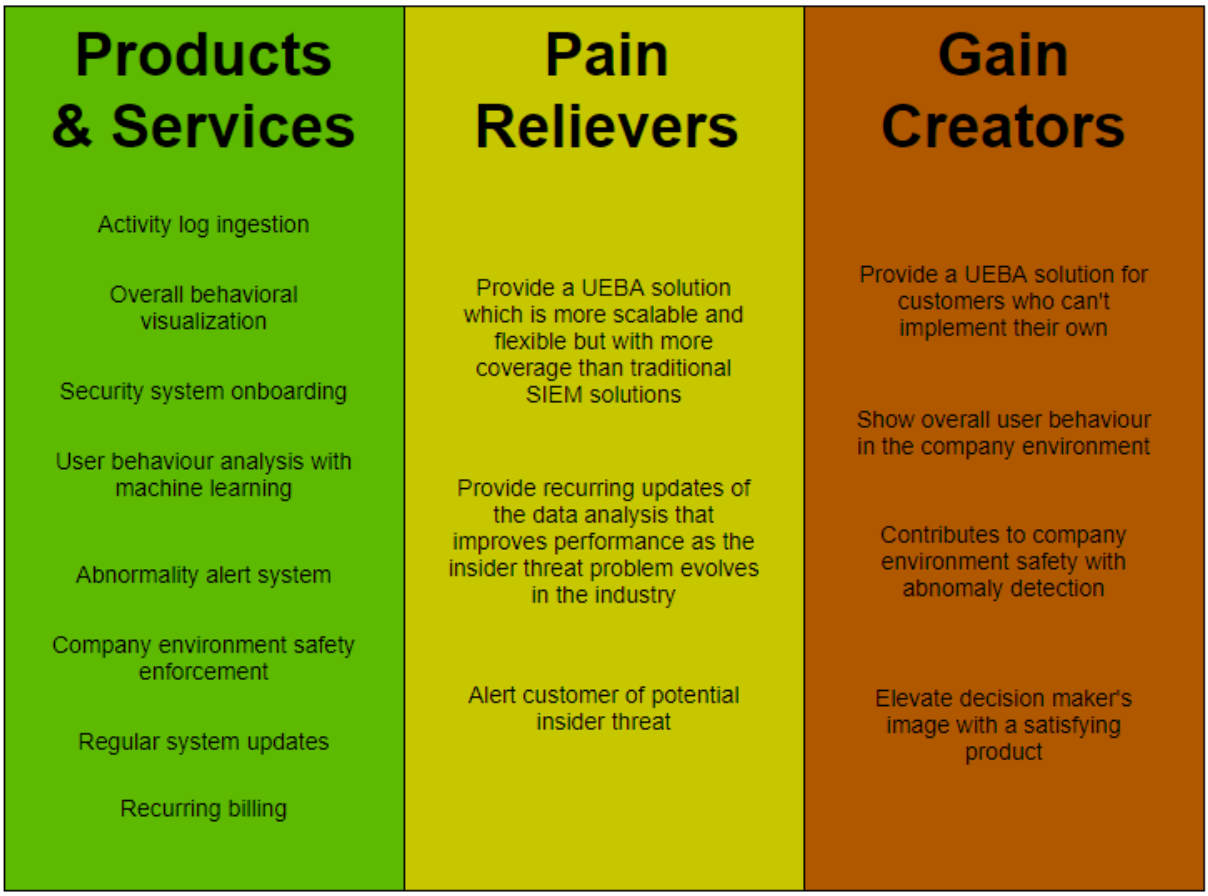
the model so that the product can maintain its performance. This will help strength the belief that our existing customers have in our product's ability and raise its reputation. Finally, with an effective marketing strategy, more customers will incorporate our product in their solution to the insider threat problem.

Key Resources: Developers and ML R&D intellectuals ensure the high quality of the product and its continuous improvement. An online platform provides a distribution channel for the product. Customer relationship managers are also needed to build trust relationships to preserve our current customers as well as to build our company's brand which is essential in pushing our product and delivering its value to a larger audience. Funding will enable our company to acquire aforementioned platforms and human resources to successfully create, deliver and capture our product's value.

Key Partners: Our investment partners are essential since their funding provide access to higher quality human resources such as skilled developers and useful technologies that build services that provide the product's value. Cybersecurity reps from our customers help validating the performance of our product and are a key part in building the relationship between our company and our customers.

Costs: The major costs could include hiring costs and research project funding, costs to run marketing campaigns and certain licensing costs that come with using third-party technologies to develop and maintain our product.

Part 2: Value Proposition Canvas



From our customer segmentation process, we identify the most important jobs of our customer profiles are finding a reliable UEBA solution for insider threat detection, as well as the resulting maintaining a controlled workplace environment and earning respect from their peers and supervisors. Other than that, some customer profiles would care more about the finances while others may stress about the performance details. Currently in the customer discovery process, we have initial designs on the technical aspects. We propose an unsupervised machine learning model that analyses time-series data. It takes user behavioural history and peer behaviours into perspective for anomaly detection. The data analysis is accompanied with a visualization of overall behaviours in a summarizing matter. This technical design can solve customers' job of monitoring digital workplace activities and spot anomaly. By using this tool, customers can more easily detect and handle insider threat. Given the recurrent invoice, the customer can try out the cost and performance of insider threat detection and handling with our product without a long-term dedication.

Our solution provides the following **pain relievers** for the customer. Our UEBA solution bases itself on machine learning and statistical analysis. Compared to traditional SIEM solutions that are based on fixed rule sets, it is capable of detecting more subtle and pattern-based behaviour anomalies. At the same time, it is more flexible and scalable to change, for example, a surge in hiring or a sudden shift from on-premise to remote working. Using UEBA eliminates the pain due to the limitations of purely using rule sets. By detecting anomaly in user behaviour, we reduce pain in customer in executive positions who worry about insider threat in their company which could lead to potential repercussions. As technology evolves, we provide recurring updates to our machine learning model, incorporating new training based on company behaviour and new training sets that improves performance to reduce pain of the customer upset by the development of the insider threat problem in the industry.

Our solution provides the following **gain creators** for the customer. As mentioned earlier, UEBA can detect more subtle behaviours and patterns and is mush more flexible to change in the workplace in comparison to implementing rule sets. This overcomes limitations of traditional SIEM and grows the coverage of monitoring within the environment. Our product and services save the trouble for customers who do not wish for or have trouble with implementing their own solutions. With the assist of our visualizations, customers are able to monitor overall user behaviour in the company. Combined with the anomaly detection running in the background without interfering with regular workflow of the company, customers are able to handle potential threats and achieve a safer workplace environment. Moreover, by choosing a satisfying product, we hope to grow sense of achievement in the decision-making roles and elevate their professional status.

Part 3: Competitive Landscape

Direct competitors

In the user behaviour analytics (UBA) market space, there are several direct competitors. Direct competitors, in our case a sell comparable products and goals to our startups (Burstein, 2012). Some of the top UBA tools are from companies like Splunk, Microsoft Advance Threat Analytics, Aruba, and Palo Alto Cortex (Harvey & Robb). All of these companies' tools understand the difference between normal user behaviour and abnormal user behaviour. As a result, they are able to create products that are versatile across different sectors like finance, health care, retail, and so forth (Guercio, 2020). This makes their customer base quite large. Moreover, companies like Palo Alto Cortex already offers both "supervised and unsupervised machine learning models" (Guercio, 2020). As well as provide alerts summaries of abnormal user behaviour. This is quite similar to our idea of a minimal viable product. Many of these companies also offer cloud-based and software-based solutions.

However, a disadvantage that these companies have is that they do not reveal the number of fake positives their tools produce – there is no disclaimer. It is usually after the customer has purchased the product; they realize this issue of fake positives. Here is an example of Splunk's discussion board. By no means is our team stating that our tool will have no false positives, but we will be transparent as to approximately how many false positives when we hand over the product to a customer. To add on, all of these companies do not modify the product when they distribute them in different sectors. For instance, the finance sector and the health sector will get the same product without any customization? So, how well do their products detect the abnormal behaviour between a receptionist at a hospital versus an IT manager at a bank.

Many of the companies above offer some sort of free trial that can range from a few days to a month. Depending upon how well the product performs. According to the Microsoft ATA website, their pricing is by far the cheapest from $160 per 2 years. Similarly, Palo Alto Cortex is about $344 per year. In comparison, Aruba at a one-time price of $13 000 because they offer a top-class hardware security solution. Splunk is quite affordable at $1800 per year. Most of them have delivery of 3 to 7 business days, with the exception of Aruba, which might take a few weeks to deliver since they distribute firewall appliances. Of course, customer service is included with all the products. And they usually try to offer quick service from discussion boards to phone calls. In terms of warranties, Spunks offers 30 days and other companies like Aruba and Palo Alto Cortex offer 1 year.

For barriers to entry our competitors pose for our product are: "access to more distribution channels" and software license agreement/patents (CSC454 lecture 6, 2020). These are barriers for us because many companies listed above have entered the market before us and their customers already know them and their product. This leads to more referrals for the products and an increase the distribution of products across different sectors. Next, software licenses and patents make it legally challenging for us to implement a machine learning algorithm or code if, by chance, we end up creating a similar one to those companies. As a result, they would disable the progress of our product.

The barriers to entry our product pose to our competitors is our pricing and quality of our product. We aim to create a UBA tool that create minimal number of false positives, and a user-friendly interface with the lowest price in market. This will allow us to build a brand for ourselves in the UBA market space.

Indirect competitors

Our indirect competitors are digital forensics companies like Magnet Forensics, iDiscovery Solutions, and Belkasoft ("Top Digital Forensics Solution Companies," 2020). The tools, products, and services these companies offer are related to our UBA solution. However, their

customer base and business models are different. Digital forensics companies cater to law firms, law enforcement agencies, and private investigators. The goal of these tools is to find evidence that shows the wrongdoings of perpetrators. Some advantages of digital forensics tools have is that they are able to process through terabytes of data! Their software shows the results in an organized manner where you have different tabs for emails, texts, etc. In addition, the search functions are able to narrow the exact evidence you might be looking for in just a few minutes.

Although the biggest disadvantage they have is that digital forensics tools require a lot of manual work to get the right results (Bennett & Hopper, 2014). This is because every criminal is different. People also need to be trained extensively to use digital forensics tools. The digital forensics industry is looking into machine learning, but a lot of it is at the research phase (Iqbal & Abed, 2020).

Digital forensics tools have a similar pricing range as UBA tools. Magnet Forensics price has a one-time fee of $1700 for their AXIOM tool. Belkasoft's evidence analyzing tool is $500 for the regular version and $10 000 for enterprise version. Both companies offer a 30-day free trial for their products. Whereas iDiscovery is different, clients have to request services they want like data collection analysis or evidence processing. They all deliver the software product within a few business days. Many of them have a 1-year warranty, and have customer support centers that provide great service 24/7.

The main barrier that the digital forensics companies pose to our product is governmental policies (Forensic Examination of Digital Evidence, n.d.). Since digital evidence is just as important as physical evidence, there are standards to evidence processing so that it can be considered valid in court proceedings. Our UBA tool is based on machine learning. As a result, many governmental policies might question if there is any bias in our tool. They usually avoid purchasing a "black box" algorithm. These factors would make it difficult for us to infiltrate the digital forensics market.

Barriers that our product poses to digital forensics company is how different our product is from theirs. Our target market will be finance. Hence, our user behaviour analytics tool will require very little manual work. Both of our products cater to very different target markets and that will make it difficult for digital forensics companies to successfully enter the UBA market.

Out of category

Replacement competitors for us are open-sourced intelligence tools (OSINT). OSINT is quite interesting because they are not really companies. Many of these tools are open-sourced, and most are free to use for the public. There are database search engines that prevent account takeovers to public data sets like Visual Genome. Some of its advantages are how easily accessible it to an average person without paying a large sum of money to access mind-boggling

information (“Advantages and disadvantages of open-source intelligence”, 2017). Many of these tools are known to be quite effective at their job.

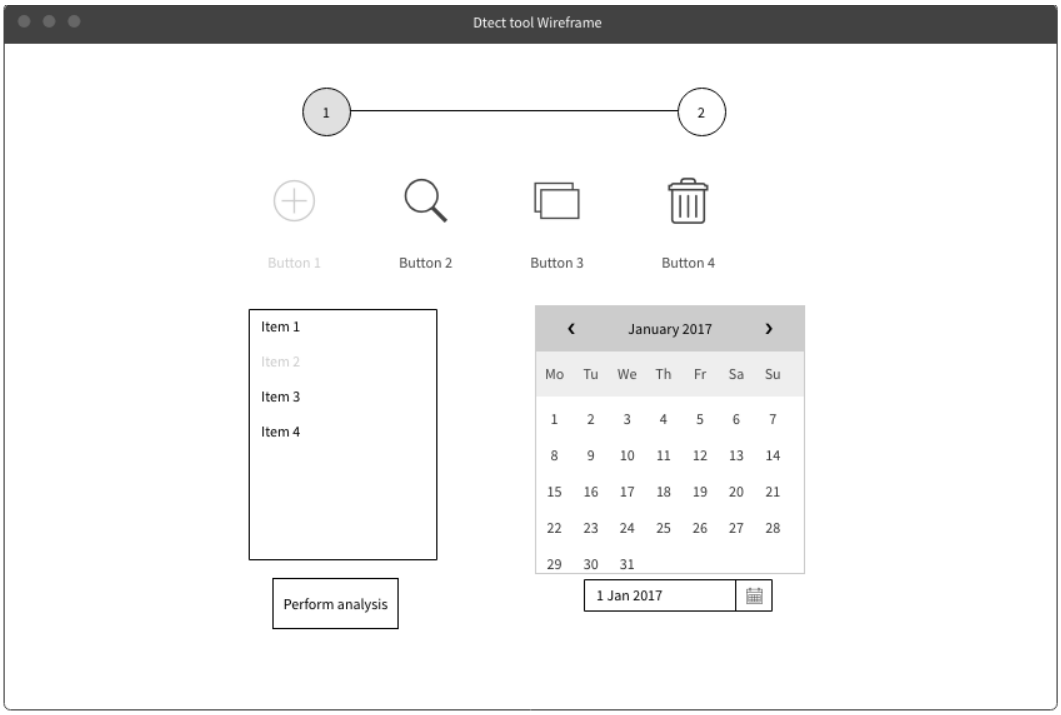
But because they are open-sourced, they might pose some legal and ethical issues due to the nature of the information they reveal like public data sets. This makes it extremely difficult for investors to capitalize on the product. Its performance is also debatable because it has a “free for all” type of model. There are no guarantees or warranties. The key point is to use OSINT tools at your own discretion.

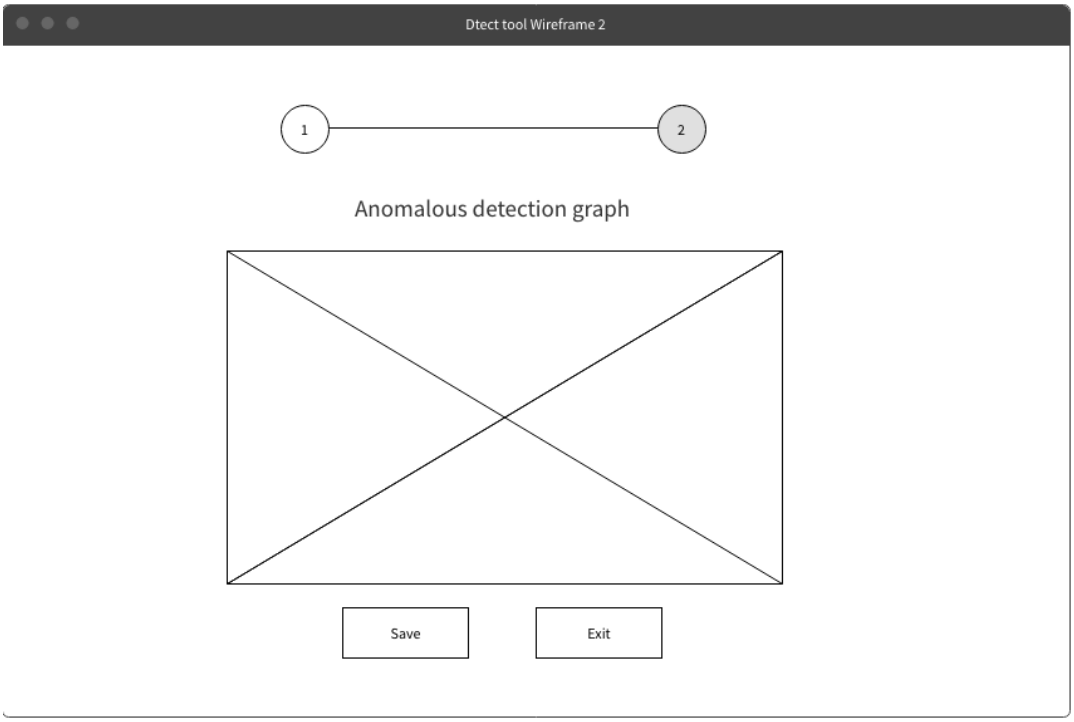
The barriers that our UBA tool poses to OSINT is the economies. Our minimal viable product will capture the essence of a UBA tool, which will have a price associated with it. Since a lot of OSINT products are free and legally questionable, those issues will act as a barrier and prevent them from entering the UBA industry. In contrast, the barriers that OSINT poses to our UBA tool is the cost advantage. Essentially, someone could create a great, functional UBA tool of their own and make it open-sourced like this one. The price point and its functionality would make it very difficult for our product to become sustainable.

Value Proposition Selection

The distinct competitive advantage we provide is the ability to ingest large amounts of information. This makes it easier for large corporations like a bank, who have gigabytes and terabytes of data, to use our tool. Furthermore, we would provide our customers with a user-friendly solution, as denoted by our wireframes. There are a lot of UBA tools that exist but often take years to use it efficiently. Our tool would ensure that the user interface is simple and pinpoint to information that our customers are interested in. Also, we plan on making our tool more customizable to cater to different sectors in the finance industry, like insurance or investment companies.

We would also ensure that we are providing our customers with a free trial so that they become accustomed to the product before they purchase it. Another competitive advantage is that we would be offering the lowest price in the UBA market. This is because, as newcomers in the UBA industry, we want people to try out our product and give feedback so that we can improve it even further.


Dtect tool Wireframe
1
2
Button 1
Button 2
Button 3
Button 4
Item 1
Item 2
Item 3
Item 4
Perform analysis
January 2017
Mo Tu We Th Fr Sa Su
1 2 3 4 5 6 7
8 9 10 11 12 13 14
15 16 17 18 19 20 21
22 23 24 25 26 27 28
29 30 31
1 Jan 2017


Dtect tool Wireframe 2
1
2
Anomalous detection graph
Save
Exit

References

Advantages and disadvantages of open source intelligence. (2017). Retrieved from https://expertsystem.com/advantages-disadvantages-open-source-intelligence/

Aruba Introspect Trial | Bridgeway. Retrieved from https://www.bridgeway.co.uk/aruba-introspect-trial

Azure Advanced Threat Protection | Microsoft 365. (2020). Retrieved from https://www.microsoft.com/en/microsoft-365/identity/advance-threat-protection

Belkasoft Offers Free Licenses to Evidence Center 2012 to Eligible Forensic and Educational Organizations. (2020). Retrieved from https://belkasoft.com/bec/en/free_evidence_center_for_le.asp#:~:text=Pricing%20and%20Availability&text=Pricing%20for%20Forensic%20IM%20Analyzer,edition%20is%20available%20from%20%249999.95.

Bennett, J., & Hopper, R. (2014). Automated and Manual Forensic Examinations. Encyclopedia Of Criminology And Criminal Justice, 100-108. doi: 10.1007/978-1-4614-5690-2_613

Burstein, D. (2012). Market Competition 101: The 3 types of competitors to keep an eye on | MarketingSherpa Blog. Retrieved 26 October 2020, from https://sherpablog.marketingsherpa.com/marketing/competition-types-to-watch/

Cortex XSOAR Community Edition. (2020). Retrieved from https://start.paloaltonetworks.com/sign-up-for-community-edition.html

Forensic Examination of Digital Evidence: A Guide for Law Enforcement (2020). Retrieved from https://www.ncjrs.gov/pdffiles1/nij/199408.pdf

Guercio, K. (2020). Best User and Entity Behavior Analytics (UEBA) Tools. Retrieved from https://www.esecurityplanet.com/products/top-ueba-vendors.html

Iqbal, S., & Abed Alharbi, S. (2020). Advancing Automation in Digital Forensic Investigations Using Machine Learning Forensics. *Digital Forensic Science*. doi: 10.5772/intechopen.90233

Magnet AXIOM Reviews and Pricing - 2020. (2020). Retrieved from https://www.capterra.com/p/149088/Magnet-IEF/

Top Digital Forensics Solution Companies. (2020). Retrieved from https://digital-forensics.enterprisesecuritymag.com/vendors/top-digital-forensics-solution-companies-2019.html

Snusbase Database Search Engine. (2020). Retrieved from https://snusbase.com/

Splunk Enterprise and Cloud | Pricing. (2020). Retrieved from https://www.splunk.com/en_us/software/pricing/enterprise-and-cloud.html