DTECT Business Plan

CSC454: Business of Software, University of Toronto

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

12-15-2020

DTECT Business Plan

Table of Contents

Executive Summary

As the number of insider threats and the cost to resolve them have grown significantly over the past few years, there is an increasing concern in data security and this is a problem that is difficult to monitor and solve as anomalous behavior is constantly evolving. Dtect aim to provide a scalable solution that is easy to use and integrate with existing systems. Our product is a web application that offers an innovated visualization component to keep track of events and a machine learning component to detect anomalous behavior. Our target market is the large financial firms who might rely on cloud-based technology and/or have employees working remotely. This market not only have vulnerabilities to insider threat, but also have data that is valuable which is very expensive to resolve if a breach were to occur. Our competitors are mainly UBA vendors, but where we stand out is the design of our visualization tools which already matches other vendors that have been around for a decade and also the ability to easily integrate into existing systems.

According to our market analysis, our target market is still looking for effective UBA products for detecting insider threat and their use case matches what we provide including activities such as activity log ingestion, visualization, alert system and a scalable UBA detection system. Dtect currently has an MVP that includes a functional web application connected to a machine learning model. Our team currently has a wide range of skillsets including full-stack development, data science, business analysis, customer outreach, and UI/UX design. In the near future, we aim to expand our engineering team to improve our visualization tools and acquire more talent on the machine learning team to strengthen our data analysis. In addition, we plan to hire a sales team to help reach our exponential increase in annual subscribers for our first five years projection. Dtect does not expect to see positive net earning for the first two years, but will break even in the third year and grow rapidly in the 4th and 5th year.

Part 1 - Business Opportunity

1. Business Idea

In recent years, companies have started adapting User Behaviour Analytics (UBA) solutions to protect and manage insider threats. According to a recent study by Ponemon Institute, "the number of insider-threat incidents increased by 47% in the last two years, and the average annual cost of insider threats has also increased by 31% to $11.45 million" (Ponemon Institute LLC, 2020)

UBA is a process of detecting and monitoring abnormal behaviour in users and systems. It has three main components. The first one is data analytic, which establishes baseline behaviour and pattern for users. Deep learning is used to build behaviour profiles comprehensively. Data integration of the system logs, network packet and other system data. Data Presentation, which presents and alert any potential threats. There are many UBA solutions today that utilize machine learning. However, there are many different approaches to detecting insider threats, each with its advantages and disadvantages.

Our solution is a web-based application. It is hosted on the cloud and uses a machine-learning algorithm to analyze system logs and detect user behaviours. Our software collects real time events and stores them in a database. Our elegant, simple to use user interface shows the employees' activities and displays a graph of all aggregated events. Our tool also provides a list of abnormal user behaviour making it easier for threat hunters to detect

2. Market Analysis

UBA provides insider threat solution for a large share of the global market. It affects the growth of the market, and it is rapidly growing. According to the Ponemon Institute study (Ponemon Institute LLC, 2018), the most affected industry by insider threat is the finance industry (Figure 1). The impact is so severe that it can lead to data leaks, fraud, and financial loss (Figure2). When the company's data is at stake, the payout is exceptionally high. The financial services sector spends about $14.5 million annually to protect themselves from insider threat. That is a 20.3% increase from 2018 (Figure3). Moreover, the 2020 Securonix insider threat report (Securonix , 2020) and BetterCloud research (Securonix, 2020) indicate that organizations that use cloud-based resources and applications are being more vulnerable to insider threats (Figure 4). It also suggests that t with the COVID-19 pandemic, insider threats have increased. Also, according to Malwarebytes' report (Malwarebytes, 2020), 45.5% of the respondents said the biggest challenge of remote operating their company was finding the right cybersecurity tools (Figure 5). The study also showed that about 47% of the respondents were aware of cybersecurity issues. Based on our research, financial companies with many remote employees are expected to grow globally in the UBA industry.

3. Competitive Landscape

Dtect has numerous direct and indirect competitors in the UBA. Splunk is a well-known competitor in the UBA space. They have a very similar product to Dtect, where they collect data from company servers and flag anomalous data. However, Splunk is more of a data visualization tool rather than a machine learning algorithm. LogRhythm uses both machine learning and data visualization to help investigators find flaws in user behaviours and any vulnerabilities in the data architecture. Splunk and LogRhythm have been in the UBA industry since 2003 and have built a stellar reputation for their products.

Our indirect competitors comprise of digital forensic companies like Magnet Forensics. Many of their digital forensic tools provide for government agencies and law enforcement so, that they can find digital evidence for the person of interest. Digital forensic tools do not narrow down on anomalous behaviour, but instead, it presents all the digital evidence. It is up to the investigator to limit the search using filters and then go on the fact-finding mission. Digital forensic tools are simple to use with a bit of training but do not provide the same compatibilities as a UBA tool.

While designing our UBA tool, Dtect took into consideration the good qualities of both our direct and indirect competitors. Our user-friendly interface shows many aspects of abnormal user behaviour, starting with activity count. We believe it's important to understand all of the activities that occurred in order to train and improve our machine learning model. We also have a section for "User threat level," which calculated "Flagged events percentage per user." This feature makes it easier for investigators to begin their search between hundreds of employees. We are a Startup, but our data visualization tool matches up to companies that have been in the UBA space for more than a decade. We provide the quality and innovative designs that make an impact on the UBA industry.

Part 2 – Product - Market Fit Analysis

1. Customer Value Proposition

Our target market segmentations are large companies with a significant number of remote workers in the finance industry. In the form of a web application towards the customer, we intend to provide them with analytics and automation in user behaviour analytics to assist with insider threat detection. We will apply a quarter-annually subscription-based pricing scheme. Our Business Model Canvas is shown in Figure 6 in the appendix.

In specific, our products & services include the following:

- Activity log ingestion
- Overall behavioral visualization
- Security system onboarding
- User behaviour analysis with machine learning
- Abnormality alert system
- Regular system updates & performance improvement

With our products & services, we are able to relieve customer pains by providing a UEBA solution displaying user behaviour which is scalable, flexible, and evolving compared to potential alternative approaches such as developing their own solutions. This creates gains for contributing to the company's environment safety with anomaly detection.

2. Product-Market Fit Analysis

According to our industry partners, financial companies are still in search of effective UBA products to assist in insider threat. Our total addressable market is about $350 million (Dtect, 2020). In addition, we are predicting low churn rate in our customers. Ever since the start we have been working with the industry partners from RBC in understanding what they are looking for in a desirable solution. Starting with a minimal viable product (MVP), we will continue to collect user feedback from the market and understand the Net Promoter Score for measuring our product-market fit. Feedback collection will also be able to guide us in applying both major and minor improvements to our product.

3. Product-Technology RoadMap

Currently we have a minimal viable product as a prototype. More basic features on the web applications shall be implemented before launch. User experience research will be done on a regular basis for each major UI update.

We acknowledge that we do not have certain machine learning expertise in related areas. As the MVP is implemented with a basic machine learning component, we wish to bring onboard talent for the data analytics part of our product.

For the first two years, we plan on putting priority in improving performance on our UEBA solution, including improving accuracy and lowering false positive rate. This will involve experimenting and research with different data analytics approaches and data representation with different training sources. In addition, user feedback will be incorporated in the performance improvement.

On the third year, we plan to expand our business by going deeper into specific fields of the industry, such as insurance or asset management. We see to tackle insider threat detection for more specific scenarios from these fields. Pricing tiers will be implemented based on the finely defined scenarios which entail a different variety of service.

We value infrastructure building in our design and planning. Throughout the years we intend to make our product's onboarding, integration, and usage process as easy as possible for the customer. In specifics, we can integrate our product with popular major platforms such as AWS and Azure.

Insider threat is an evolving field. We plan to maintain our anomaly detection development in order to preserve or improve detection performance and detection coverage. This will be an ongoing task in the roadmap plan, including the first two years as described earlier.

Part 3 – Planning & Execution

1. Outlook, Benchmarks, and Development Plans

We will have multiple benchmarks to monitor the growth of our business. Our business growth for the first five years will be dependent on subscriber count. Subscriber count can be measured with added subscriber rate and churn rate. We expect our annual added subscriber count to increase exponentially, tripling from the year before for the first five years. In 2023, when we expect to break even, we should see 1968 added subscribers and 6839 added subscribers by 2025. To reach these benchmarks, we plan on expanding the sales team to increase new subscriber count and focus on hiring engineers to improve UX and model performance to keep churn rate low. While we do not expect to get any positive earnings in the first two years, we should break even in the third year and our exponential growth trend will propel us into larger gains in the 4th and 5th year.

2. Sales Strategy and Financial Projection

We intend to build a quality software that achieves our performance requirements. To make onboarding and operating simple, we plan to integrate our solution with popular platforms such as AWS and Azure for infrastructure building. We also plan to develop specific use cases that tailor our solution towards our target customer segments where the problem of insider threat is severe and well-known. Additionally, a team of sales representatives will be hired to look for and communicate with our prospects. Our financial projection shows that we will break even in the third year. Despite no positive net earnings in the first two years, it is predicted that the revenue will increase rapidly year by year, leading to a revenue of $7.6M and an EBITDA of $5.6M in the fifth year. We also project our CAC payback period to be less than a month from 2023 onwards.

3. Financing Needs, Current Investors and Exit Strategy

Our financial projection shows a deficit in EBITDA of around $390,000 in the first year and $234,000 in the second year. We will need investments in the first two years to break even. Currently, we are looking for partners to engage in a further proof of concept before preparing to enter venture capital. Our desired investors are likely to be mostly comprised of corporations from our customer segment which are large financial firms. For our exit strategy, we will look to either merge with or be acquired by another company regardless of the future state of the business. By merging or acquisition, we can partially preserve our company's value and avoid a complete liquidation.

Startup Team

Our Startup consists of five founders each with their own areas of expertise.

Alan is a full stack developer. He constructed Dtect’s database from the Los Alamos data and implemented the webserver along with Xi. Alan has previously worked at Ritual Technologies as a software intern and brings expertise in agile methodologies and backend development.

Xi is our data analyst and picked the applicable data points from the Los Alamos data set. He also implemented the data analysis component, which helps pinpoint abnormal user behaviour. Xi currently works for both Vector institute and The Hospital for Sick Kids as a research assistant. He brings to his machine learning knowledge and software engineering knowledge to Dtect.

Rutwa is our business analyst she has contributed to building customer personas and creating surveys for potential customers. Moreover, she created the financial projections for the next 5 years and perform competitive analysis. Rutwa works for the Government of Canada as a business analyst and brings her expertise in stakeholder relations and finances.

Or is specializes in customer outreach, as she has many contacts around the globe. She sent out customer surveys and aggregated their responses. She also contributed to creating the problem statement at the beginning. Or works at SOTI as a research development intern and brings her expertise in project management.

Carl designed the user interface as well as the workflow of the web application. Furthermore, he created the customer profiles and the business canvas. Carl has worked as a Quality Insurance Analyst at Oracle Canada bring expertise in product development, testing, agile methodologies and front-end development.

Appendix

Supporting Market Analysis Data

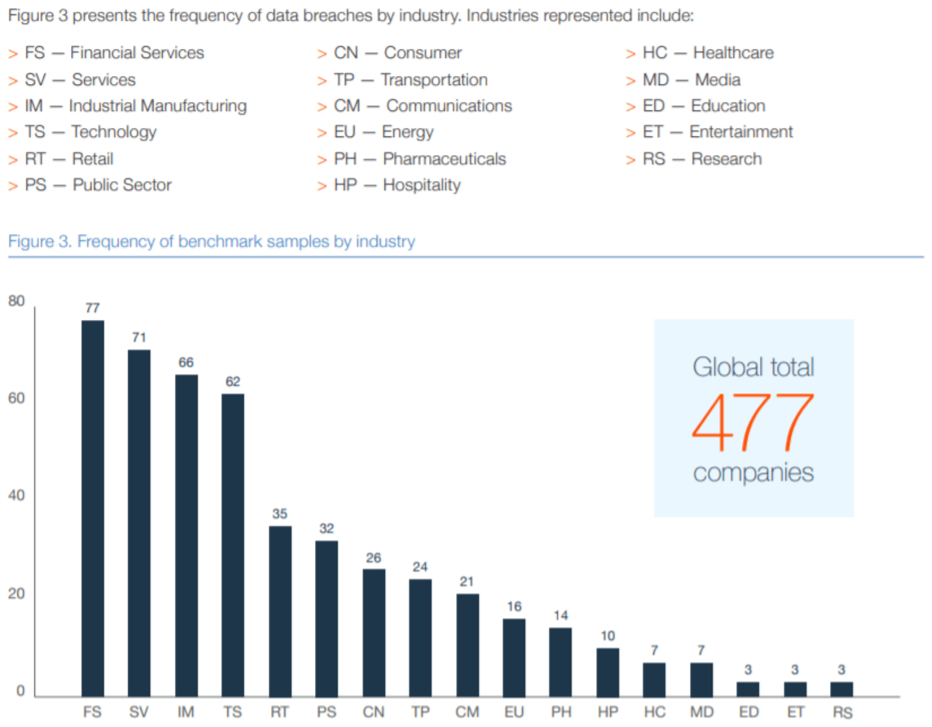


Figure 3 presents the frequency of data breaches by industry. Industries represented include:

- > FS — Financial Services
- > SV — Services
- > IM — Industrial Manufacturing
- > TS — Technology
- > RT — Retail
- > PS — Public Sector
- > CN — Consumer
- > TP — Transportation
- > CM — Communications
- > EU — Energy
- > PH — Pharmaceuticals
- > HP — Hospitality
- > HC — Healthcare
- > MD — Media
- > ED — Education
- > ET — Entertainment
- > RS — Research

Figure 3. Frequency of benchmark samples by industry

Figure 1: Frequency of data branch by industry - Ponemon Institute report.

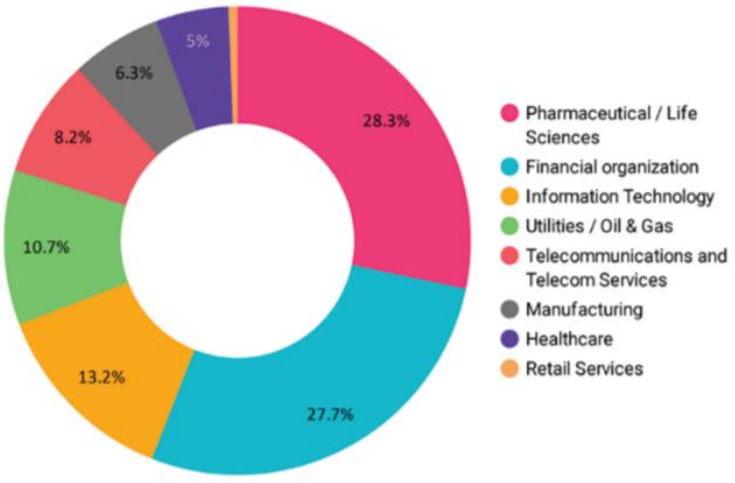


Figure 2: Threat analysis by industry. - Securonix report (2020).

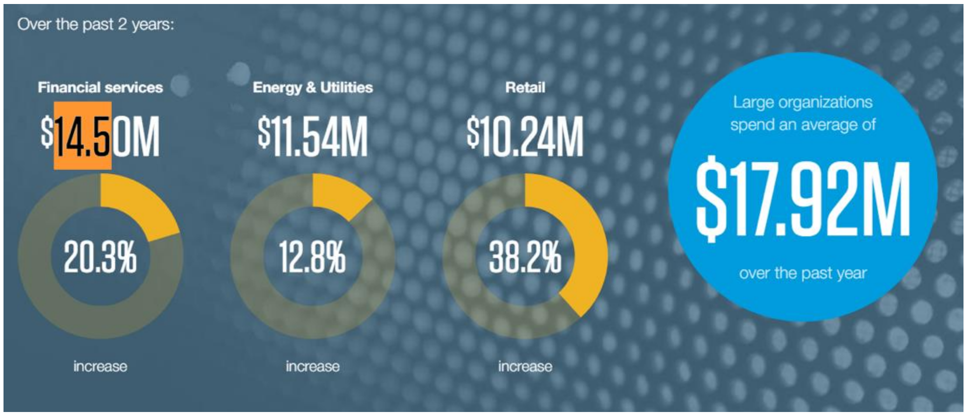


Figure 3: Spending in dealing with insider threat over the past 2 years. - Ponemon Institute report.

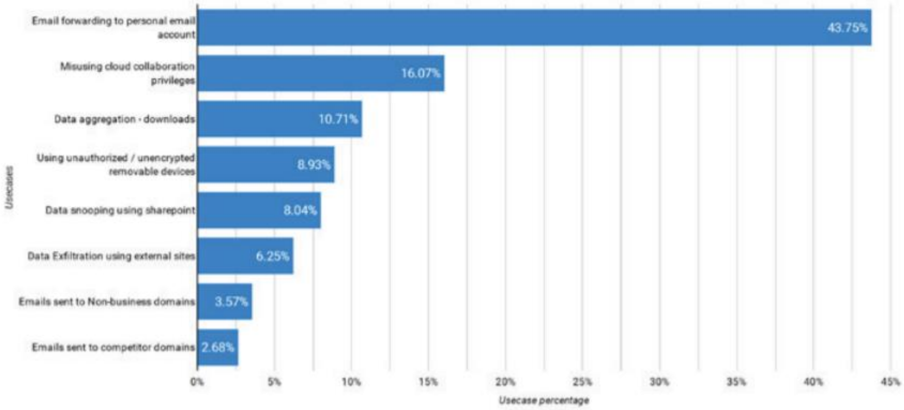


Figure 4: Common behaviors that were users extract sensitive data. - Securonix report (2020).

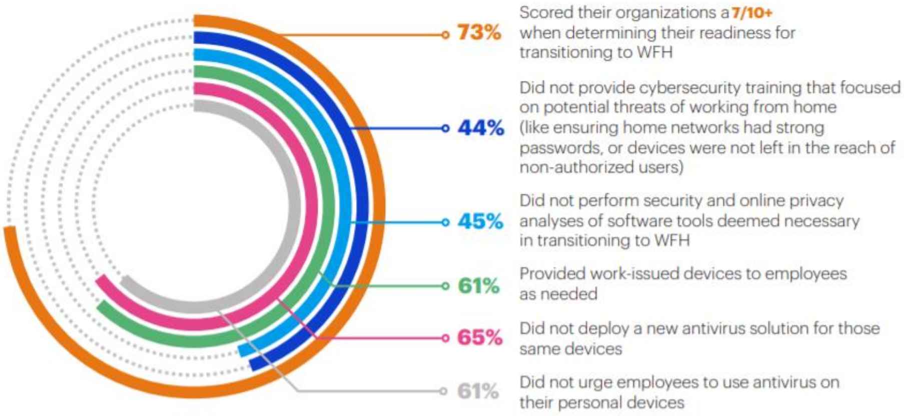
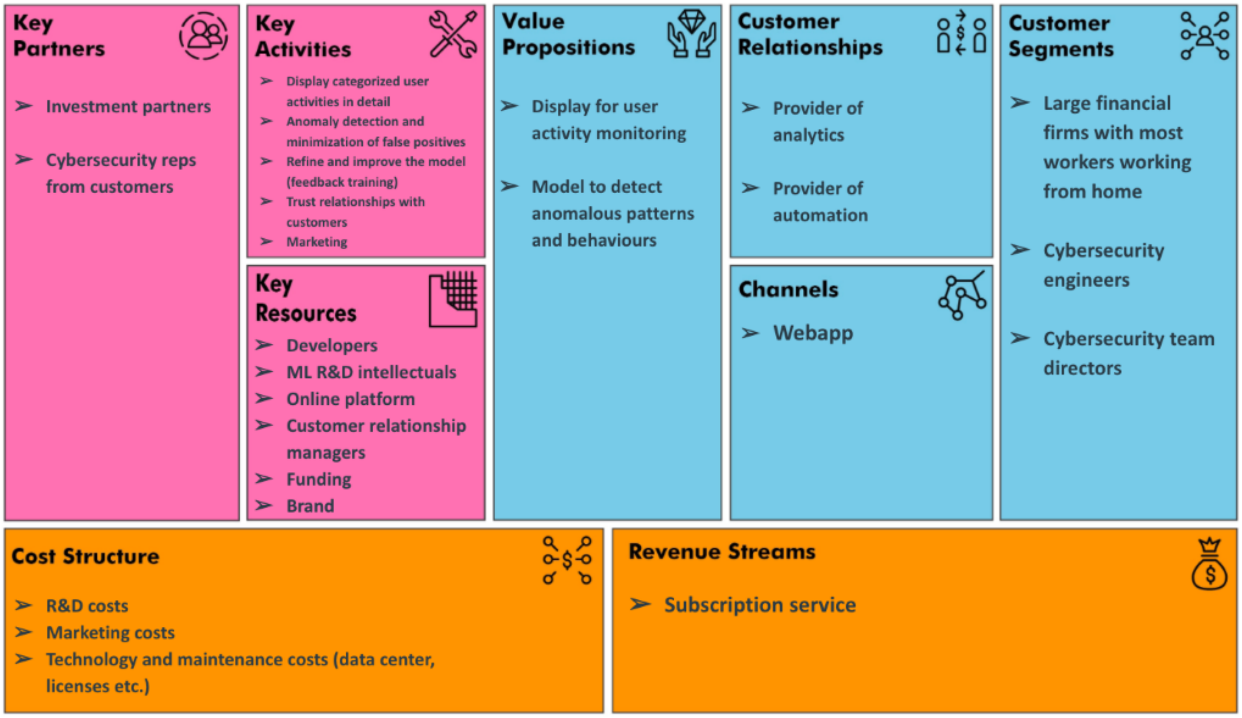


Figure 5: Organizations' biggest challenges to work from home. - Malwarebytes report (2020).

Revenue Models and Cost Estimation Calculations



Key Partners

- Investment partners
- Cybersecurity reps from customers

Key Activities

- Display categorized user activities in detail
- Anomaly detection and minimization of false positives
- Refine and improve the model (feedback training)
- Trust relationships with customers
- Marketing

Key Resources

- Developers
- ML R&D intellectuals
- Online platform
- Customer relationship managers
- Funding
- Brand

Value Propositions

- Display for user activity monitoring
- Model to detect anomalous patterns and behaviours

Customer Relationships

- Provider of analytics
- Provider of automation

Channels

- Webapp

Customer Segments

- Large financial firms with most workers working from home
- Cybersecurity engineers
- Cybersecurity team directors

Cost Structure

- R&D costs
- Marketing costs
- Technology and maintenance costs (data center, licenses etc.)

Revenue Streams

- Subscription service

Figure 6: Business Model Canvas

Financial Projection Supporting Charts

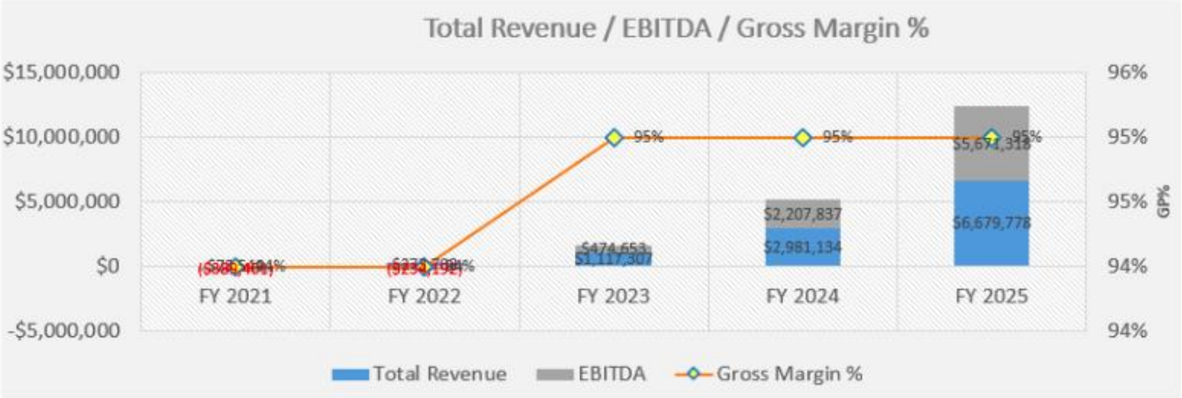


Figure 7: Total Revenue / EBITDA / Gross Margin %

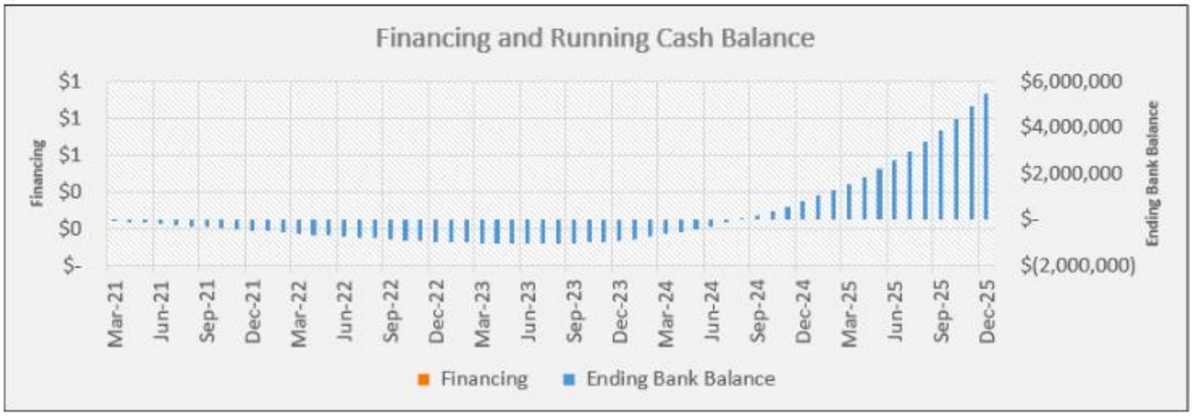


Figure 8: Financing and Running Cash Balance

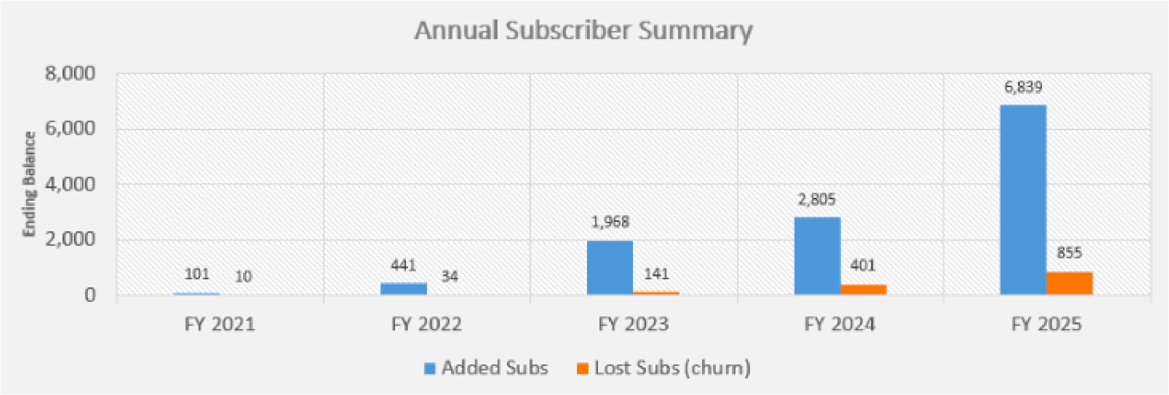


Figure 9: Annual Subscriber Summery

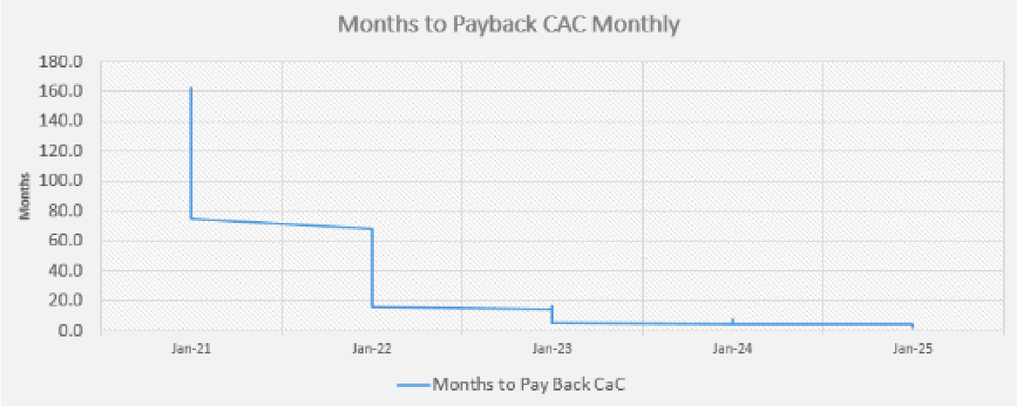


Figure 10: Months to Payback CAC monthly

References

Magnet Forensics. (2020). *Uncover Digital Evidence - Build Stronger Cases*. Retrieved from Magnet Forensics: https://www.magnetforensics.com/

Dtect. (2020). *Assignment 5: Financials Modeling and Projections*. Retrieved from Quercus: https://q.utoronto.ca/courses/181260/assignments/415396/submissions/7056?download=10745887

LogRhythm. (2020). *SIEM Platform & Security Operations Center Services*. Retrieved from LogRhythm: https://logrhythm.com/

Malwarebytes. (2020). *Enduring From Home: COVID-19's impact on business security*. Retrieved from Malwarebytes: https://resources.malwarebytes.com/files/2020/08/Malwarebytes_EnduringFromHome_Report_FINAL.pdf

Ponemon Institute LLC. (2018). *2018 Cost of a Data Breach Study: Global Overview*. Retrieved from IBM: https://www.ibm.com/downloads/cas/861MNWN2

Ponemon Institute LLC. (2020). *2020 Cost of Insider Threats Global Report*. Retrieved from Observer IT: https://www.observeit.com/cost-of-insider-threats/

Securonix . (2020). *2020 Securonix Insider Threat Report*. Retrieved from Securonix : https://pages.securonix.com/rs/179-DJP-142/images/Insider-Threat-Report-May-2020-Securonix.pdf

Securonix. (2020). *2020 Securonix Insider Threat Report*. Retrieved from Securonix: https://www.bettercloud.com/monitor/wp-content/uploads/sites/3/2019/03/BetterCloud-State-of-Insider-Threats-2019-FINAL.pdf

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