Dtect Assignment 2a: Business Opportunity, Market Analysis, and Startup Team

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

Part 1: Business Opportunity

Statement of Problem

Insider threat is a growing security risk for many organizations and has become one of their top concerns. It is defined as cybersecurity threats that come from within the company. There are three types of insider threats: Malicious, Accidental, and Negligent. These potential insider threats could show different user behavior patterns.

The severity of the insider threat issue is high. According to a recent study by Ponemon Institute, the number of insider-caused cybersecurity 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 [1]. The impact on the organization not only includes a great monetary loss but also compromises the customers' confidentiality and integrity.

A weak point in security today is recognizing and preventing an insider threat. The existing approaches are using false positive diagnostics by implementing rules into their systems (spam filters, firewalls, anti-malware software) and utilizing machine learning tools to find anomalies. However, both approaches can lead to the wrong conclusion depending on the rules or model's complexity, leaving some threats undetected or blocking legitimate, benign user actions. Unfortunately, there is no one-size fit solution for insider threat and not all organizations have the infrastructure to support a solution.

With the increasing volume of insider threats, we aim to provide a solution to a rapidly growing market that helps organizations detect threats before a potential incident. Understanding the nature of insider threats can help us form mitigation strategies and find proactive solutions that protects sensitive data from potential leaks. By defining UBA/UEBA tools, we can create a better security protection that fits each organization's needs.

The End Result

Use cases:

Figure 1 below shows a visualization of the use cases to our software solution.

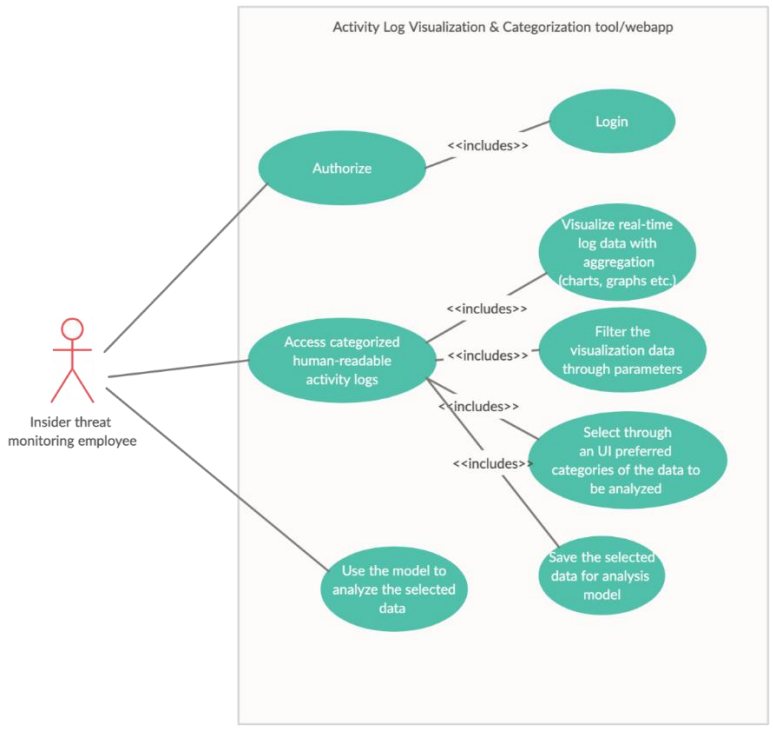

Figure 1: Visualization of the proposed software tool.

The Scope of Work

We intend to build a platform for the complex and diverse dataset of user activities in order to detect and prevent insider threats. It provides data translation, categorization, visualization and management services. The product is a tool that helps the user understand the data better and provide customization before data analysis.

As the problem is insider threat, this product is targeted towards corporations. Our product fits the market for corporations that desires data clarity in addition to existing analysis methods. Specifically, corporations that want to turn indecipherable logs into categorized records, visualize the data in the logs and extract parts that they consider useful instead of just feeding the data into a model. Corporations that look for betterment of data analysis tools would fall outside of the scope of the target market.

Part 2: Market Analysis

Industry Selection

Since cybersecurity is prominent to any kind of business that deals with sensitive data, our product can be applied to many industries. However, we have chosen the financial industry for two reasons. Firstly, the financial industry has a large amount of data breaches compared the other industries. A 2018 Ponemon Institute study [2] revealed that the financial industry had the most data breaches in 2018 (Figure 2).

Figure 2: Frequency of data breaches by industry.

Secondly, the data in the financial industry is very sensitive. Thus, the impact of an insider threat incident in finance can be quite devastating. The banking industry alone incurred the most cybercrime cost in 2017 ($16.55 million) and 2018 ($18.37 million), shown by Figure 3 [3].

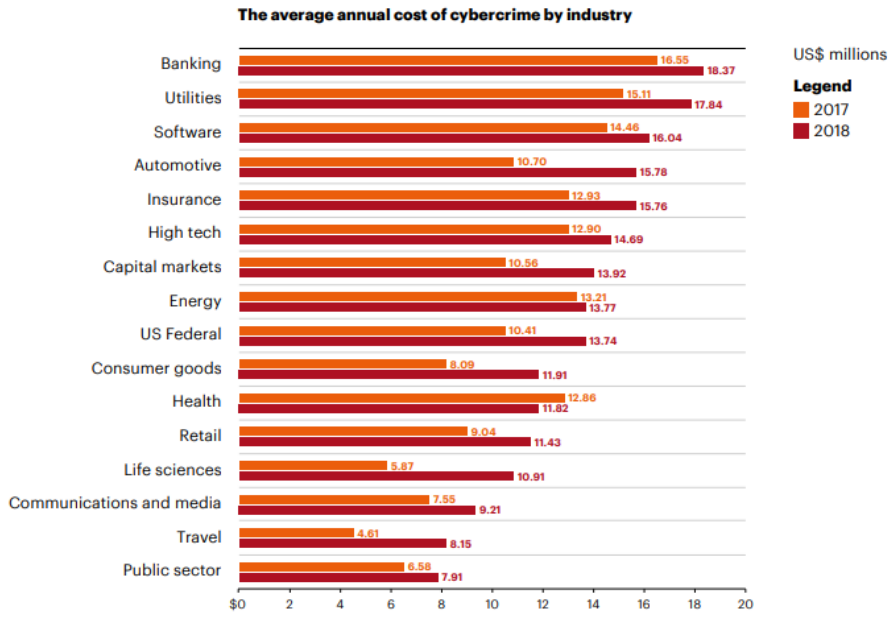

Figure 3: The average annual cost of cybercrime by industry.

Market Segmentation Options

Since insider threat poses a great risk to organizations, our approach is to use firmographic segmentation.

One option is to group the market by the number of employees in the company because insider threat becomes more complex as the number of employees increases. From the "2020 Cost of Insider Threats Global Report" [1], large companies spent more than an average of $17.92 million on insider threat incidents over the past year (Figure 4), while smaller organizations spent an average of $7.68 million. From those large organizations, financial services spent more money than other sectors at $14.50 million, a 20.3% increase over the past two years.

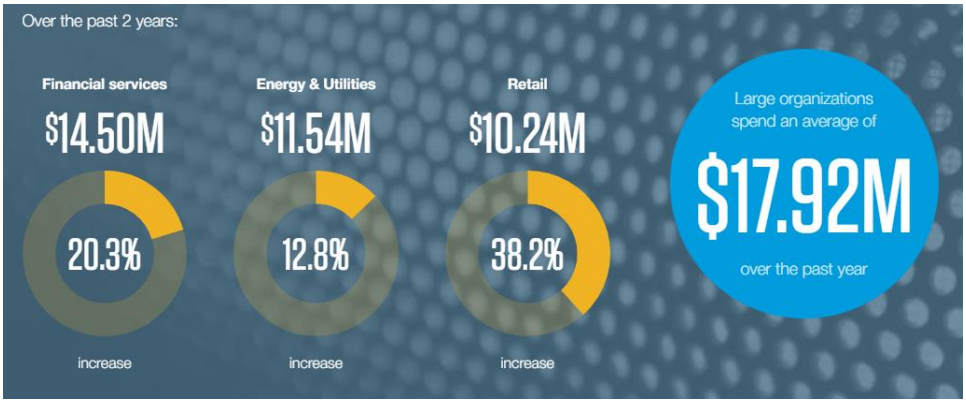

Figure 4: Spendings in dealing with insider threat over the past 2 years.

Additionally, companies with higher number of employees feel more vulnerable according to a 2019 survey conducted by BetterCloud (See Figure 5) [4]. This can potentially lead to more investment and demand in cybersecurity from larger companies.

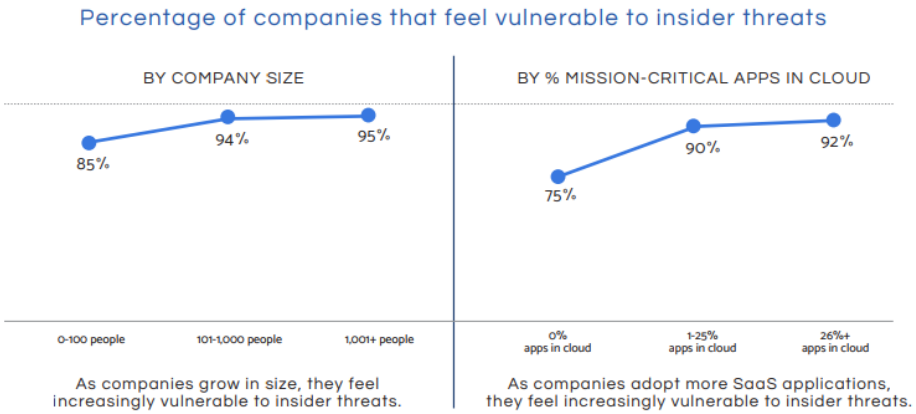

Figure 5: Vulnerability towards insider threats.

The graph to the right also shows that companies feel more vulnerable to insider threats when using more mission-critical apps in the cloud. From this, we could also form another segmentation based on a company's reliance on online tools.

A third option to do market segmentation is to categorize companies based on the number of employees working remotely. With similar reasoning as segmentation by number of employees, having people working remotely introduces more possibilities for insider threat incidents to occur. Malwarebytes conducted a research about COVID-19's impact on business security [5]. They surveyed over 200 managers, directors, and cybersecurity roles at U.S. companies of

different sizes. 24% of the respondents said they paid unexpected expenses for cybersecurity breaches and 20% said they faced a security breach as a result of a remote worker (Shown in Figure 6). In addition, 45.5% of the respondents said the biggest challenge of operating the company remotely was finding the right cybersecurity tools (Figure 7). The study also showed that 47% of the respondents indicated that employees were aware about cybersecurity issues when working remotely.

Figure 6: Insecurities regarding remote workers.

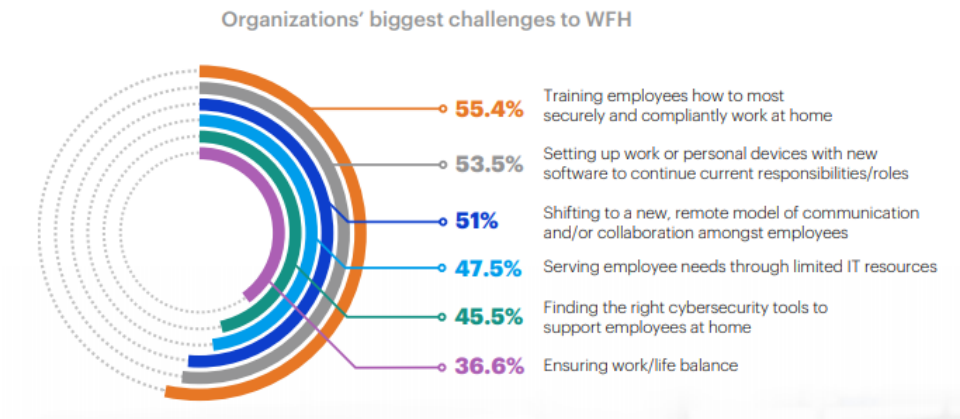

Figure 7: Organizations' biggest challenges to Working From Home.

From previous incidents and growing concerns with working remotely, companies are paying more attention to cybersecurity tools. Thus, this segmentation has potential to finding our target market.

Target Market

From the segmentation options discussed above, our target market will be large financial organizations with large number of remote workers. The size of the market is increasing from the effects of COVID-19 which is forcing employees to work from home (Figure 8). Companies will also consider the option of working remotely even after the pandemic and many have already moved to remote permanently [6].

Figure 8: Organizations' biggest challenges to Working From Home.

A major trend that is rapidly emerging into the industry is machine learning. Previously, many companies relied on SIEM with fixed rules to detect cyberthreats, but this approach does not scale well for large companies and it was not an effective way to handle insider threat. With the emergence of machine learning, UEBA is becoming the modern solution to combat insider threat and newer SIEM products are starting to integrate with UEBA as well.

Since machine learning solutions are relatively new, there is competition on creating the best performing model. Every company designs them differently and they also incorporate different features to target different markets. This gives the opportunity for new entrants to enter the scene because this area is always experimenting and evolving.

Part 3: Startup Team

Dtect consists of 5 team members each bringing their own experience and expertise into the start-up.

Alan has worked in multiple fast-paced start-ups as a full-stack software engineer. Carl is well-versed in user interface design, software quality assurance, and software development in the banking industry. Or has a master's degree in applied computing and has adequate experience as a network engineer and software developer. Rutwa's ample experience as a Business Analyst

intern, where she has designed business architecture models to convey business requirements to stakeholder. Xi's software development experience, passion in machine learning and business and his ability to see the big picture will greatly benefit the future of Dtect.

In terms of strategic roles, Alan, Carl and Xi will focus on the forefront of the software design and development while conducting their fair share of market research. Or will moderate between the technical and business side with her relevant experience in telecom and internet industry. Rutwa will be leading the business development and project management side, which will include quarrying over the user behaviour analytics market. Together we will be exploring the field, networking and negotiating with stakeholders to make Dtect into a successful start-up.

Our team is accustomed to working with people with various levels of experience and expertise. We work best under a spectrum of different ideas and opinions. We value critical thinking, adaptability, and persistence. Experiences with failures in teamwork led us to establish some ground rules for the autonomy of our start-up. Our ground rules include communicating daily to provide updates on both ongoing and upcoming tasks. We believe our past experiences working in various teams have prepared us for creating Dtect.

Our goal is to build a meaningful user behaviour analytics tool that is successfully able to help companies detect deviant employee activities. We hope to gain insights into the business world of software, build our professional experiences and explore start-up entrepreneurship under the environment of the course. We believe that with guidance and investment from our stakeholders, our skills and expertise can crack insider threat issues at large corporations.

References

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

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

[3] Accenture, Ponemon Institute LLC. (2019). *The Cost of Cybercrime.* Retrieved from Accenture: https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf

[4] BetterCloud. (2019). *State of Insider Threats in the Digital Workplace*. Retrieved from BetterCloud: https://www.bettercloud.com/monitor/wp-content/uploads/sites/3/2019/03/BetterCloud-State-of-Insider-Threats-2019-FINAL.pdf

[5] 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

[6] Loten, A. (2020). *For Many, Remote Work Is Becoming Permanent in Wake of Coronavirus*. Retrieved from Wall Street Journal: https://www.wsj.com/articles/for-many-remote-work-is-becoming-permanent-in-wake-of-coronavirus-11590100453