Dtect Assignment 3:
Customer Persona & Customer Profile

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

Below are two customer personas we introduce for our UEBA product.

DTECT

PROJECT: CSC454 PERSONA: Javier Lorenzo

NAME

Javier Lorenzo

TYPE

Recommender

Goals

- Effectively identify and mitigate internal and external security risks using machine learning
- Explore security breaches to pinpoint system weakness
- Create solid security requirements for new systems

Quote

" I enjoy challenging myself to solve problems that we don't necessarily know if there's, yet, a solution for."

Demographic

Male 30 years

Toronto, Canada

Married

Cyber security engineer at Anon Company

$92,000

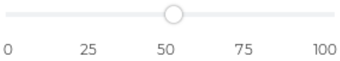
Company size: 5000 employees

Background

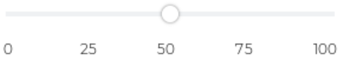
Javier has a PhD in Computer Science from the University of Waterloo, where he specialized in machine learning. He has 10 years of experience working as a DevSecOps for a mid-size company where he conducted automated security testing. In addition, he has conducted threat modelling to understand weaknesses in the infrastructure.

Skills

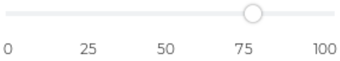
Teamwork



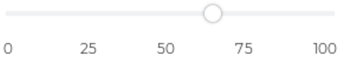
Data intuition



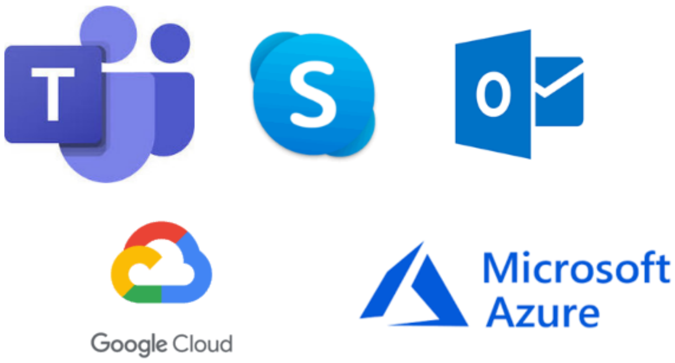
Intellectual curiosity



Data visualization



Software platforms used at work



DTECT

PROJECT: CSC454 PERSONA: Larry Powell

NAME

Larry Powell

TYPE

Decision Maker

Goals

- Accompany the Risk and Compliance team at Name company, where the primary goal is to risk monitor and manage financial exposure
- Complete and maintain multiple compliance certifications
- Proceed through audit reviews with minimum issues

Background

Larry has worked in the information security sector for more than 20 years. He is serving as a Director of Compliance and Risk at Name Company, where his main role is to risk manage the financial aspects of the company. In addition, Larry has completed 9 cybersecurity certificates including Check Point Certified Security Expert (CCSA), and Microsoft Certified Solutions Expert (MCSE). Previously, he held many roles including manager and consultant at well-known companies such as Motorola, PwC, and Grant Thronton LLP.

Demographic

Male ______ years

Toronto, Canada

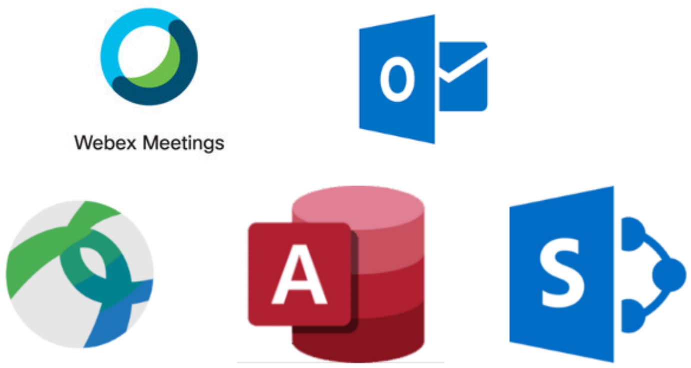
Married

Director at Name Company

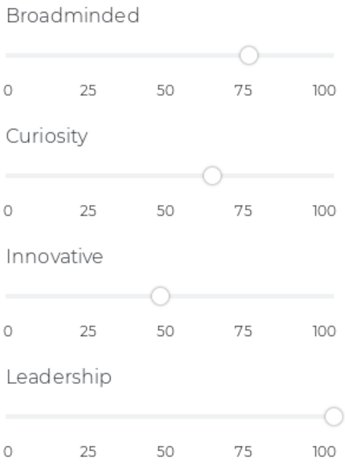
$100, 000

19, 000 employees

Software platforms used at work



Skills



For each of our proposed customer personas, we present an empathy map that covers this customer’s role and experience that associates with our product.

DTECT

Javier Lorezo

Think and Feel

1. Stressed about the amount responsibility he has over sensitive data that could cost the company a great amount of money if a breach occurs

2. Afraid that insider threat is happening undetected despite the current cybersecurity solutions implemented

3. Aspires to do a good job at ensuring data security, satisfy management and prevent any data breaches from happening

4. Worried people working from home and relying more on online resources could allow more possibilities for insider threat to occur

5. Dreams about being a key member of the company and being promoted to director of security

6. Concerned about whether current cybersecurity solutions are sufficient and thinks about how it could be improved as cybersecurity threats are constantly evolving

Hear

7. Cybersecurity professionals and researches talk about trends, new solutions, and potential hazards through conferences

8. Managers remind that the data is extremely sensitive and confidential and a data breach would be very costly to recover

9. Friends, coworkers, and colleagues are careless, negligent, or uninformed of potential cybersecurity risks while working remotely

10. News reports of increasing amount of phishing attacks throughout the past few months of people working remotely

See

11. Other companies that are in similar industries having incidents relating to cybersecurity

12. Other companies that are in similar industries using advanced cybersecurity measures

13. Recommendations from fellow professionals and advertisements on tech forums from cybersecurity service providers

14. The fact that cybersecurity risk can lead to major consequences

15. His colleagues who he trusts

16. A work environment at home

Say and Do

17. Protective when talking about his job

18. Gives reports to management about the safety of data

19. Requests coworkers regularly to take precautions to ensure security

20. Actively looking for cybersecurity solutions and new hazards

21. Monitors activity and looking out for suspicious behavior

22. Grants access to certain tools and data for the employees that need it for their job

Pain

23. Problem is complex and continuously evolving

24. Defining behavioral rules is not flexible and scalable enough

25. It requires a lot of time and effort to create and maintain their own solution to solve insider threat detection

26. It is hard to tell whether a solution is effective

27. Insider threats may already exist undetected in the company

28. Common mistakes: unintentional risky usage of data or office tools

Gain

29. Saves time and effort in attempting to detect insider threat

30. Expectations of detection and avoidance of insider threats are satisfied

31. A solution with data science analysis where regular workflow will not be influenced by threat detection

32. Life is made easier by having an AI solution to automatically learn new behavioural patterns

33. Being able to avoid worrying management about security incidents and become a valuable asset to the company

34. Stable, reliable, scalable options that analyzes behaviours instead of hard rules

35. Failure is measured in false positives and false negatives; success is measured in avoidance of breaches, incidents and handling suspicious behaviours before it escalates

The highest-ranked jobs we can help Javier solve are functional, social and emotional jobs. Functional jobs are the most important because it has direct impact towards all the other customer jobs. Our product could help Javier feel more secure as it is backed up by data science rather than unscalable fixed rules. Using AI to adapt to new trends, it would make the jobs much easier and so our product would be a suitable buy for Javier.

The biggest pains of Javier are: 27, 25, 26 (see empathy map). 27 is the most intense pain since a cybersecurity incident may occur any time. Additionally, due to the nature of the insider threat problem, it can be difficult to verify the effectivity of a solution before an incident occurs. If a solution is not effective, it could fail to detect potential threats which will lead to incidents occurring eventually.

The top gains for Javier are: 30, 29, 35. Detection and avoidance of insider threats are the end goals for him, if those expectations are met, the gain will be very substantial. A UEBA solution would provide detections of potential threats and further actions can then be taken to avoid security incidents before they escalate. Having a stable, reliable, scalable option to analyze behaviour is a major advancement and is therefore important to the end goal.

DTECT

Larry Powell

Think and Feel

1. Stressed about whether his selection of UEBA solution can be effective before purchase

2. Concerned that the current cybersecurity solutions may raise too many false positives

3. Aspires to select beneficial, easy-to-use UEBA products to minimize security risks

4. Worried that company can lose financial value and reputation if a security incident occurs

5. Concerned about whether the cost of a third-party solution is justified by the quality that the solution provides

Hear

6. Cybersecurity professionals and researches talk on online forums and groups about new solutions and their opinions on new and existing solutions

7. Other managers in the company discuss that the need for a solution on security risk monitoring and management is imminent

8. Colleagues from current or past companies spreading the news on security incidents that have happened

See

9. The benefits and limitations that other companies in similar industries obtain by using a variety of UEBA products

10. A work environment at home for all employees at the company

11. Advice and opinions from other professionals in online cybersecurity groups and forums on selecting UEBA solutions

12. Many different UEBA products are available, each having their advantages and disadvantages

13. The lack of alert investigation and validation features of many solutions can lead to false positives

Say and Do

14. Protective of company's information on how cybersecurity is handled

15. Engage in heavy market research before purchasing third-party solutions

16. Raise awareness on the insider threat problem by speaking to the employees

17. Actively looking for state-of-the-art cybersecurity solutions

18. Ensures employees are taking preventive security measures

Pain

19. Requires money and effort to purchase and integrate a third-party solution

20. Existing solution causes too many false positives

21. Lack of feature to further investigate and validate the alert raised by the product before possible counteractions

22. A security incident can potentially lead to a loss financially as well as in company's reputation

23. Unable to fully verify whether a solution is effective before purchase

24. It can be difficult to find information about certain UEBA products during market research

Gain

25. Saves money and effort in attempting to detect insider threat

26. Being able to identify anomalous patterns of behaviour which might indicate potential attacks

27. Being able to analyze and validate alerts raised by the product before taking actions

28. Makes life easier by having an automated detection process using AI

29. The success in selecting an effective UEBA product can raise the image of the decision maker in the company

30. Cost-benefit analysis can be used to measure the success and failure of the selected product

31. The detection process will not affect the regular workflow which can save time and human resources

Given the role as a director, social jobs and basic needs are crucial to Larry. Communication and leadership are his primary skills at work. His pride and confidence also play a large part in this role. As such, his job will be easier if his team does well. Our product may help the security team get good solution for insider threats which will keep Larry at ease trying to come up with effective ways to solve insider threats. These social jobs, basic needs, and emotional jobs all occur constantly for Larry as cybersecurity is a problem that is always evolving.

The top pains for Larry are: 19, 20, 21 (see empathy map). Pain 19 is intense for Larry since there is a limited budget for cybersecurity. The other two pains are annoyances that lead to extra costs from the company. More resources need to be devoted into manual work to go through flagged events in order to determine which are fake and which are real. This requires paying workers to do this additional work. Due to user behavior events coming in on a regular basis, these pains occur regularly as well. Our product could address these pains as it is providing a solution that learns from patterns over time so extra resources would not be required.

The top gains for Larry are: 25, 26, 27. These gains are significant for Larry. As a decision maker, he is primarily looking for solutions that are cost efficient and accurate. It is costly for both time and money to make his team develop a better solution from scratch. It could be more efficient to purchase a third-party solution and have his team maintain that solution. By doing so, he could save money in development and get better results sooner. Larry can gain initially from purchasing third-party solutions and regularly see smaller gains over time from reduced manual work.

Here, we discuss the bases of our profiles' hypotheses. Our industry partners from RBC has presented that insider threat is a current topic with numerous incidents happening in the industry every year (see 7,11,27 of profile 1, 8,19 of profile 2). Financial companies are often targeted and these attacks incur great consequence (Ponemon Institute LLC, 2020) (see 8,14 of profile 1, 4,22 of profile 2). Javier's role is to maintain a safe internal environment. It is a sensitive task that is deemed essential for many employers (Chuvakin, UEBA Clearly Defined, Again?, 2016) (see 1,3,5, 31,33 of profile 1). Larry is a decision maker on choosing the best solution for the company with consideration of cost and quality (see 3,19,25 of profile 2). Formerly, the most dominant security measure has been SIEM, including applying rule sets, which has limitations (Chuvakin, UEBA Shines Where SIEM Whines?, 2016) (see 2,24 of profile 1, 5,12,13,20,21,23 of profile 2). Given the situations and based on responses from our industry partners, many companies are exploring UEBA (see 12,13,32,34 of profile 1, 6,7,9,11 of profile 2). Our industry partners also have informed us of the complexity of the evolving problem, using big data and machine learning to model employee behavioural patterns and detect anomalies (see 6,20,23,25,26,29 of profile 1, 26,27,28 of profile 2). The analysis tool must catch suspicious behaviours with a manageably low false positive rate (see 30,35 of profile 1, 2 of profile 2). With the development of COVID-19 pandemic, companies have migrated its operations remotely, some maintaining similar status after the pandemic ends (Loten, 2020) (see 16 of profile 1, 10 of profile 2). This may introduce further complexity into insider threat detection (see 4,10 of profile 1). Aside malicious threats, it is also Javier's duty to prevent negligent and accidental threats from our observation of the role (see 9,19,21,22,28 of profile 1). While developing the customer profiles, we have conducted customer surveys to aid us in building these profiles. Based on our responses we have applied hypotheses towards their role-specific aspects of the empathy maps (see 15,17,18 of profile 1, 1,14,15,16,17,18,24,29, 30,31 of profile 2).

In order to verify these assumptions, we propose connecting with professionals in the field who has similar experiences with the persona. The more we interact with, the more insight we gain about their specific roles. By sending out a survey to people who are in the positions of our personas, we can learn about what it is like to be specifically in their shoes, the challenges in their job, as well as their goals and expectations (see 1,3,5,6,7,8,13,15,17,18,19,20,21,22,23,24,25,26,27,29,30,31,32,33,34,35 of profile 1, 1,3,4,14,15,16,17,18,19,21,23,24,25,29,30 of profile 2). Surveys can also be given to people in surrounding occupations whose experiences can be understandably empathized by our characters (see 2,4,9,16,28 of profile 1, 2,5,31 of profile 2). We can compare their differences to learn about similarities and assess transferrable aspects. In addition, we can verify the jobs, pains and gains of a role by conducting market research and looking for credible supporting literature (see 10,11,12,14 of profile 1, 6,7,8,9,10,11,12,13,20,22,26,27,28 of profile 2).

We have reached out to numerous professionals in roles relevant to our customer personas. In the limited time we had, we have gathered three swift responses that we discuss below. We provided them with a questionnaire that covers their background, role, company information, company's existing cybersecurity measures and their professional opinions towards UEBA. These discussions with professionals in the field not only verifies (for or against) our preliminary assumptions, it also adds perspectives into our profile building, expanding our characters.

For the first persona, we have two responses from recommender roles in the industry: A is a security solutions architect; B is a data scientist in a large bank. They think that the functional job of finding a UEBA solution is crucial. They both follow new technology in the field, research solutions usually recommended by fellow professionals and sees UEBA as the next phase of cybersecurity. Regarding social jobs, they both believe applying a good UEBA solution from us would allow the character gain respect from his superiors. For emotional jobs, they are proud of what they do and believe applying a UEBA solution would make the character feel secure. Both A and B agree about the pains that insider threat may already exist undetected, coming up with an original solution may be costly and it's hard to measure a solution's effectiveness. For gains, they agree that it is essential to have low false positives with good true positives. However, A, who provides security solutions to companies of different sizes and industries, notes that many companies are satisfied and would not pursue UEBA solutions. It does not apply to our exact segmentations, but it reminds us that our assumption of the importance of UEBA needs to be grounded on its affordability vs. performance.

For the second persona, we have received response from a Director of Compliance and Risk at a financial firm. He agrees that our solution can solve the character's social jobs and emotional jobs, but he believes functional jobs are as important. He agrees that non-UEBA solutions has limitations and security incidents incur serious repercussions to the company. At the same time, he thinks that due to the nature of AI, it is likely UEBA would give more false positives. As for the gains, he agrees that purchasing our UEBA solution can save money and effort and allow them to be able to identify anomalous patterns which might indicate threat and take actions to assess and prevent ahead of time.

References

Chuvakin, A. (2016). *UEBA Clearly Defined, Again?* Retrieved from Gartner: https://blogs.gartner.com/anton-chuvakin/2016/12/12/ueba-clearly-defined-again/

Chuvakin, A. (2016). *UEBA Shines Where SIEM Whines?* Retrieved from Gartner: https://blogs.gartner.com/anton-chuvakin/2016/11/14/ueba-shines-where-siem-whines/

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

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