User Profile for Cyberity

We are trying to solve the problem of insider threats, focusing on inadvertent/negligent, malicious threats, and credential theft. Some malicious threats include sabotage, IP theft, espionage, fraud. Some inadvertent/negligent threats include human error, phishing, malware, stolen credentials. We are creating a product/service that would help solve this issue in financial institutions

What is your Job Title?

Senior Manager Data Science

What is your background?

PhD Physics, 4 years at bank, data science and cybersecurity

Who is the decision-maker for purchasing enterprise software?

VP - Chief Information Security Officer

If the company were to buy our product, who is the one to request it (Team or individual or both)? Who would be the end-user for our product?

It could be the end user, via their management to the VP.

The remaining questions ask about the end-users who would buy our product/service. If you are not the end-user, please try to answer the questions with the best of your abilities. If you don't know the answer just skip it.

What are the job responsibilities of the end-user?

Investigate, triage and report incidents

What is the goal of the end-user that would purchase our product?

Reduce time spent, capture more true positive events, have better insights into why an alert was generated (context, history etc)

What are the challenges of the end-users?

What barriers would keep the end-users from purchasing our product?

Cost. Scalability. Efficacy. Support. Existing solutions. Integration.

What jobs are the end-users trying to get done?

I’m going to assume by “you”, you mean end user. I don’t know how to answer this still! I think i answered it in the goal question above?

What social or emotional jobs could our product get help done? (ex. feeling good, sense of security, trying to look good etc.)

I don’t understand.

What will be the biggest frustrations for the end-users of our product?

Again assuming end user. Probably too many alerts.

What obstacles stand between the end-users and what they want to achieve

Not enough time.

Which risks might the end-users fear take?

Assuming end user. Misclassifying an alert and allowing data loss to occur.

What do the end-users truly want or need to achieve?

..

How do you/end-users measure success?

data loss prevented.

What are some strategies you/end-users might use to achieve your goals?

...

To better help our study - Please forward this survey to someone who can also help answer these questions :)

This content is neither created nor endorsed by Google.

Google Forms

User Profile for Cyberity

We are trying to solve the problem of insider threats, focusing on inadvertent/negligent, malicious threats, and credential theft. Some malicious threats include sabotage, IP theft, espionage, fraud. Some inadvertent/negligent threats include human error, phishing, malware, stolen credentials. We are creating a product/service that would help solve this issue in financial institutions

What is your Job Title?

Senior manager, academic relationships

What is your background?

HR

Who is the decision-maker for purchasing enterprise software?

We have a centralized team

If the company were to buy our product, who is the one to request it (Team or individual or both)? Who would be the end-user for our product?

Likely a security team

The remaining questions ask about the end-users who would buy our product/service. If you are not the end-user, please try to answer the questions with the best of your abilities. If you don't know the answer just skip it.

What are the job responsibilities of the end-user?

What is the goal of the end-user that would purchase our product?

What are the challenges of the end-users?

What barriers would keep the end-users from purchasing our product?

What jobs are the end-users trying to get done?

What social or emotional jobs could our product get help done? (ex. feeling good, sense of security, trying to look good etc.)

What will be the biggest frustrations for the end-users of our product?

What obstacles stand between the end-users and what they want to achieve

Which risks might the end-users fear take?

What do the end-users truly want or need to achieve?

How do you/end-users measure success?

What are some strategies you/end-users might use to achieve your goals?

Sorry that I can’t give you more information on this! I am the HR person :)

To better help our study - Please forward this survey to someone who can also help answer these questions :)

User Profile for Cyberity

We are trying to solve the problem of insider threats, focusing on inadvertent/negligent, malicious threats, and credential theft. Some malicious threats include sabotage, IP theft, espionage, fraud. Some inadvertent/negligent threats include human error, phishing, malware, stolen credentials. We are creating a product/service that would help solve this issue in financial institutions

What is your Job Title?

Director of JSOC Analytics, Global Cyber Security at RBC

What is your background?

Phd in Astrophysics

Who is the decision-maker for purchasing enterprise software?

It depends on the solution; if it has to do with data visualization and blotting , then it's the Security Operation Centre. If it has to do with ML/AI then it's Global Cyber Security Team (Insider threats)

If the company were to buy our product, who is the one to request it (Team or individual or both)? Who would be the end-user for our product?

It's combined. The normal process is you present your POC to multiple teams depending on the offerings of the solution as stated in the previous question. If the team(s) show see that it could be a viable solution and they show interest, then you go through the procurement process, which includes negotiation, going through a standard security protocol, then purchase of the solution. The senior manager of the team interested in the solution is the one who will have to locate the funds.

The remaining questions ask about the end-users who would buy our product/service. If you are not the end-user, please try to answer the questions with the best of your abilities. If you don't know the answer just skip it.

What are the job responsibilities of the end-user?

The end-user is the data protection team.

(How big is this team?)
Eighteen individuals currently but will expand next year. The head of the team is a sound data analyst with a particular focus on UBA

What is the goal of the end-user that would purchase our product?

Prevent internal threats

What are the challenges of the end-users?

(Where is the pain in status-quo?)
(Why are the current solutions not working, and hence you need a new solution)

There are multiple solutions currently addressing different angles of the threat, as it is not realistic to assume that one solution will do it all.

Solutions are currently working fine, but we need to be proactive as threats are ever-changing, so we have to cope with new thread methods and be proactive before they even occur. We need a robust tool that is safe and proactive.

Examples of solutions available in the market are IMB product QRadar.

(Is this something you're currently using at RBC?)
I can't disclose that.

Current challenges include too many false alerts, so the data analyst will have to go through these alerts and filter them, which is painful. For example, my work schedule is typically 9-6, but today I started work at noon, so I finished at 8 pm. So the system should somehow figure out anomaly versus malicious activity.

(Do you have a specific work schedule published ahead so the system can compare against that schedule?)

Employees on the branch levels do have a set schedule, but not management.

(Do you think it will be a good idea to create a customized user behaviour for each employee based on historical trends and compare against this normal behaviour to determine possible threats?)

Yes, this will be a good idea. Normal behaviour could be built on an individual's behaviour; peer's behaviour...etc managers, for example, have expected user behaviour. The biggest challenge in using UBA is how to customize it, so you don't get many false alerts.

(What is another angle to capture malicious activity?)
Transmission of data; the malicious user will have to transfer the server's data to his/her local computer.

(You mentioned in the lecture that printing is a standard method of transferring data. Does the Data Security Team get a notification if an employee print something remotely?)

Yes.

What barriers would keep the end-users from purchasing our product?

If the product is not addressing the team's needs and is not intuitive to use.

What jobs are the end-users trying to get done?

Proactively prevent insider threats.

What social or emotional jobs could our product get help done? (ex. feeling good, sense of security, trying to look good etc.)

All! However, it's not realistic to achieve all! So one or two of the above goals!

What will be the biggest frustrations for the end-users of our product?

Slow/Bad UI design

What obstacles stand between the end-users and what they want to achieve

If the solution is not able to coop with the continuous nature of the internal threats

Which risks might the end-users fear take?

None! the solution must be safe 100%

What do the end-users truly want or need to achieve?

See previous answers

How do you/end-users measure success?

Simulation attacks or actual incidents

What are some strategies you/end-users might use to achieve your goals?

Try to think about how malicious people work? The psychology behind what they do and the technology they use. Look in the market for available solutions? Why are they working/failing?

(Do malicious users know how data protection team capture malicious activities?)

Yes, they do, that's why they are always changing their methodology.

(What strategies are currently used at RBC to address these threats?)
I cannot discuss that.

(If I'm to ask you for a wish list in the proposed solution, what would you say)
1- Good and fast data handling
2- Good UI design, nice graphics, easy to determine where the threat is and why is it a threat
3- Perfect detection rate (low false +ve)
The reality that you can't achieve all of these aspects to the full extent in one solution, so do one aspect really well and the other aspects to a good extent.

To better help our study - Please forward this survey to someone who can also help answer these questions :)