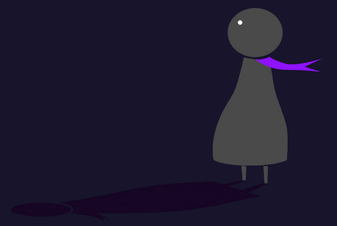
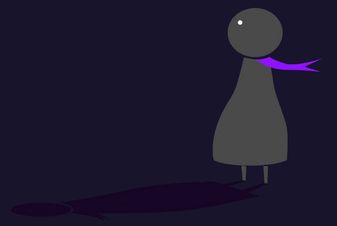
Portfolio shorts

Short stories from projects I’ve worked on

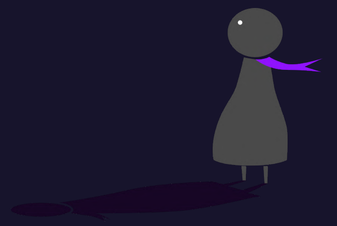


Please note. The linear and brief nature of these presentations inevitably puts a skew on reality. I have tried my best to stay true to what happened but for brevity have removed some details.



digital shadows_

In this episode I’ll be showing you a project I worked on whilst at Digital shadows



Digital shadows helps you find and remedy digital risks.

Constantly monitoring the deep, dark and open web for things that might be a risk.

If it finds something it **raises an alert.**

The problem is the automated monitoring Digital shadows does only finds half the risks.

Early research from the product team looked at everything we weren’t raising automatically.

What they found was that nearly 50% of risks were ‘Custom’ to each business.

An example of what automation can’t help you with...

“My company is running a public event next month.

How can I monitor mentions of my company, VIP’s and locations in the run up to and during this event?”

Project goal

How might we protect companies from the ~50% of risks that are ‘custom’ for each client?

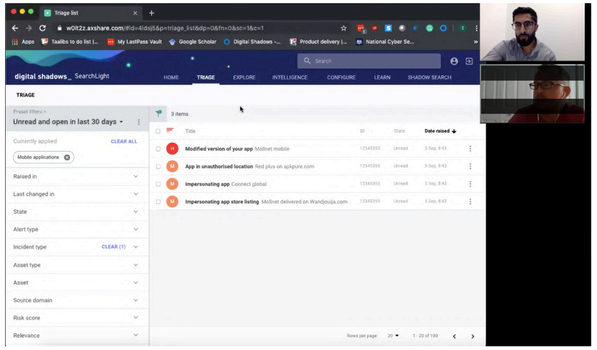
Who was on the team?

UX Design Lead / Researcher
Cyber security SME
Product manager
CTO
UI Designer

Process

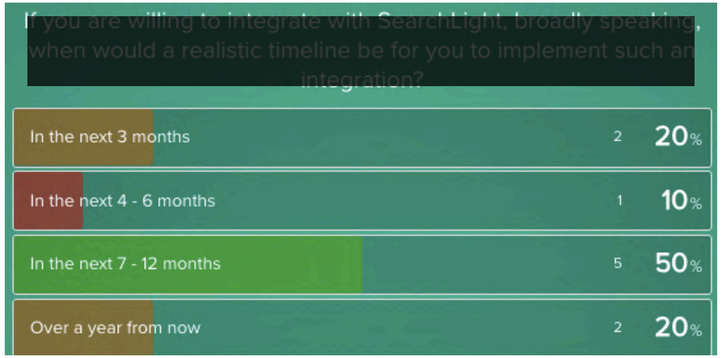
Discovery research
Analysis and synthesis
Concept definition
Concept testing
UI design
Beta testing
Go live behavioural analytics

Discovery research



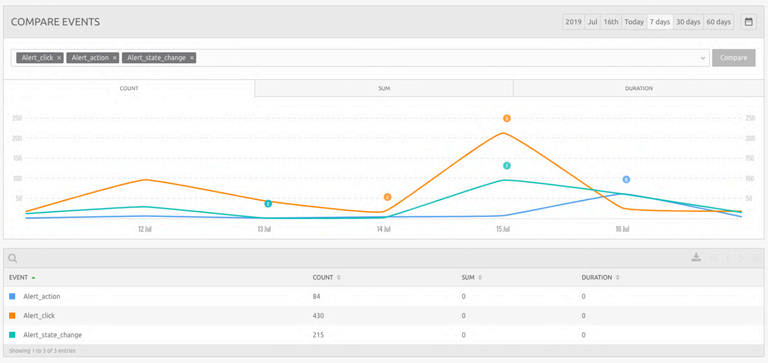
1

User interviews



2

Surveys

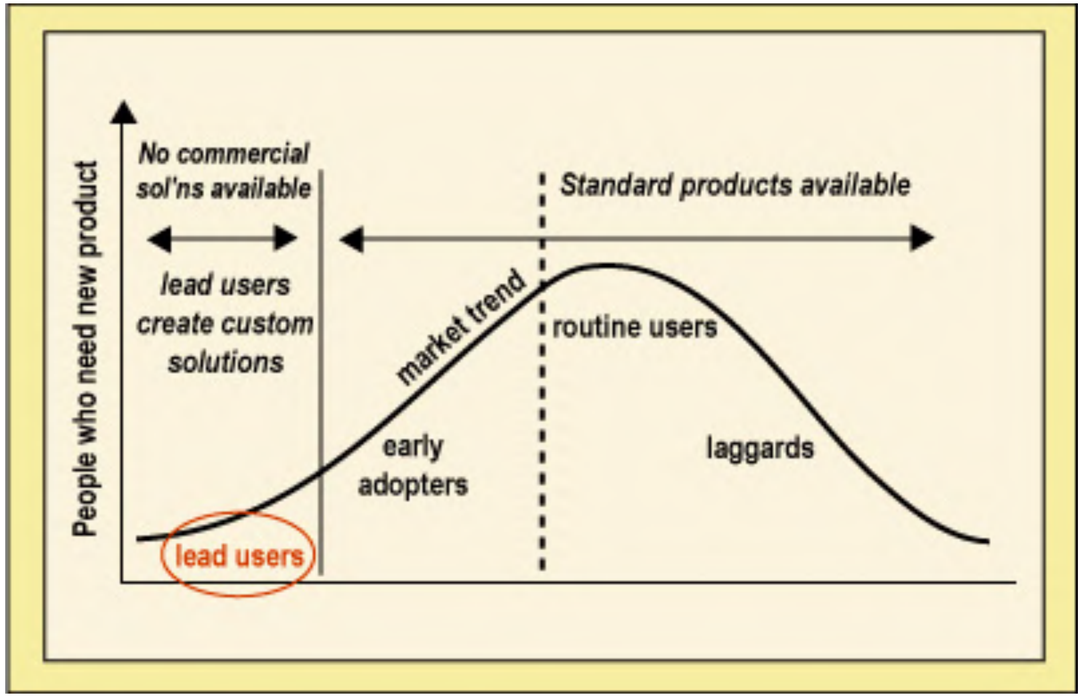


3

Tracking relevant events

Key insight | Some of our customers were meeting this need with a feature not intended for this purpose.

A ‘Saved search’ feature that was developed with different use cases in mind was actually being used to monitor for these ‘Custom’ risks.

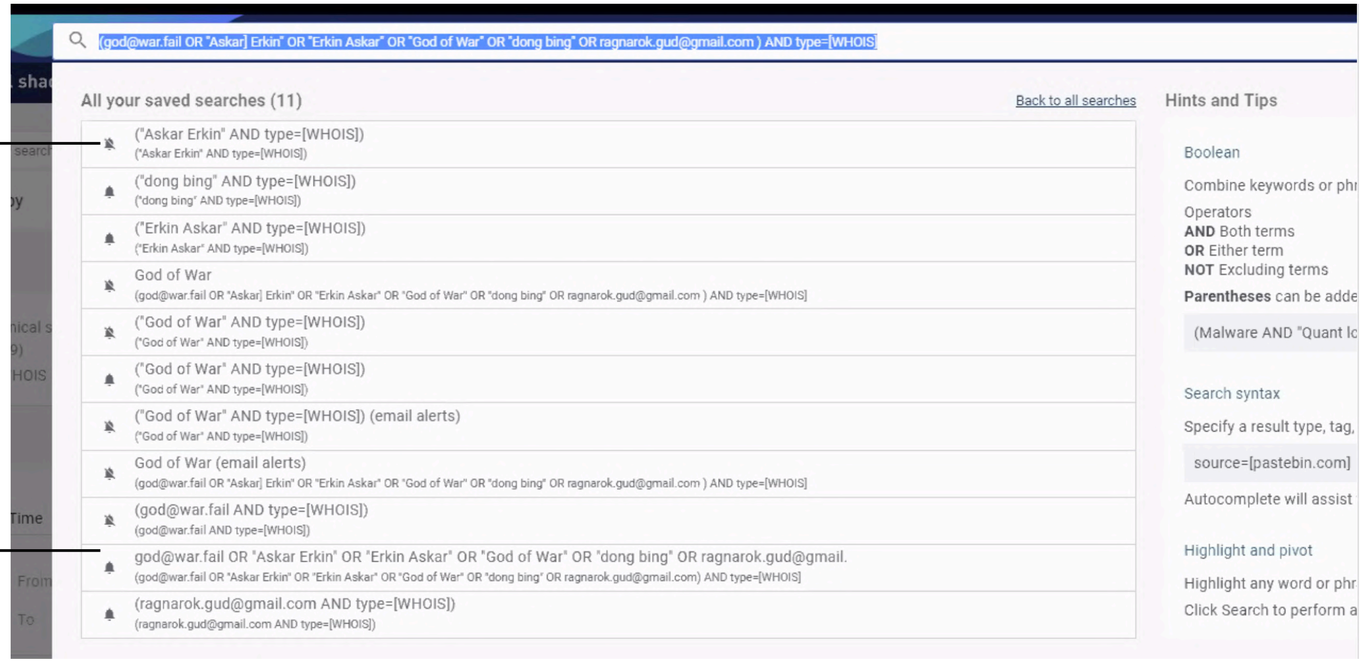


How was this need being met?

Seeing how the Lead users were making the system work for them

Start trying out some searches to see if they understood the query language and to see what results they might get.

Adding more to the search as they grew more confident writing the query



How was this need being met?

What were the main problems they had?

Users didn’t understand the query language

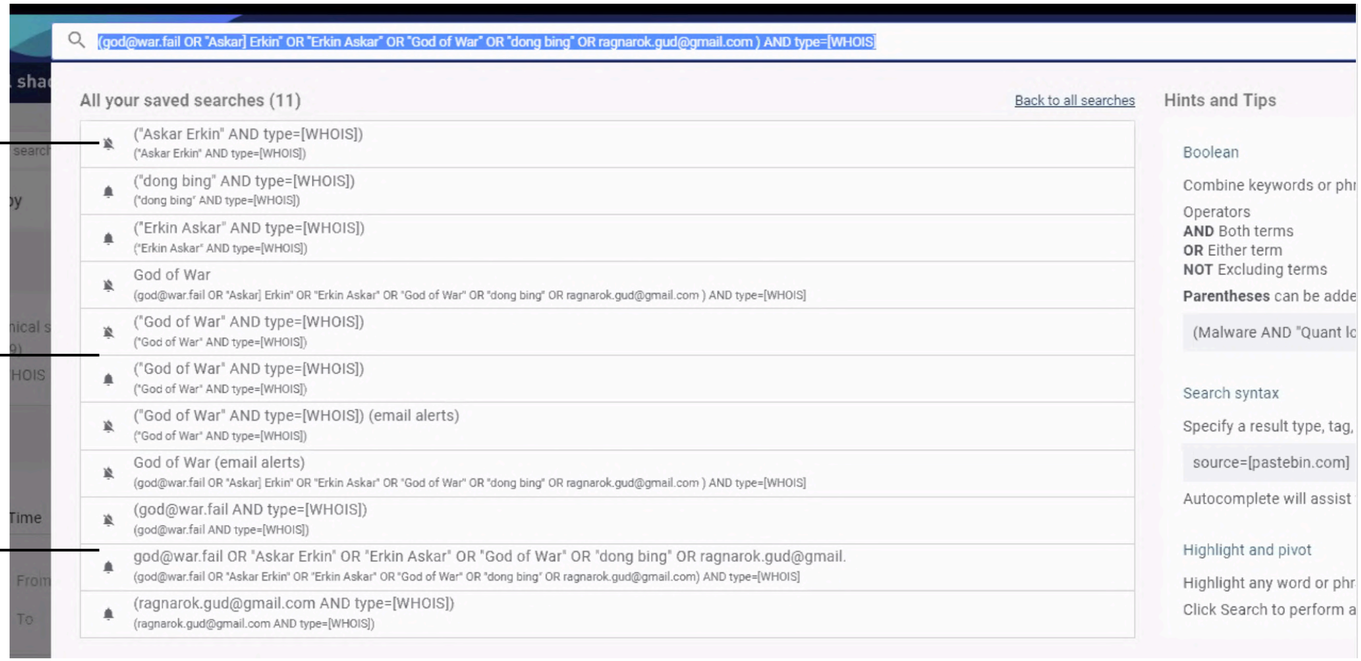
1

The queries were so broad, too much noise in the results

2

Logical operators and query relationships were confusing

3



Understanding the journey

Synthesising research themes into a task flow that describes what they are:

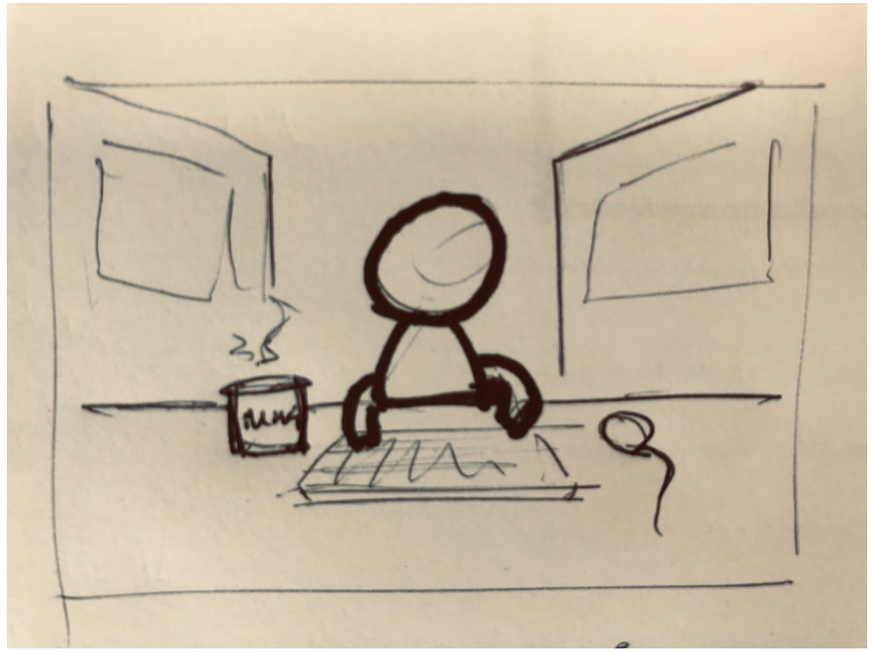
Doing
Thinking
Feeling

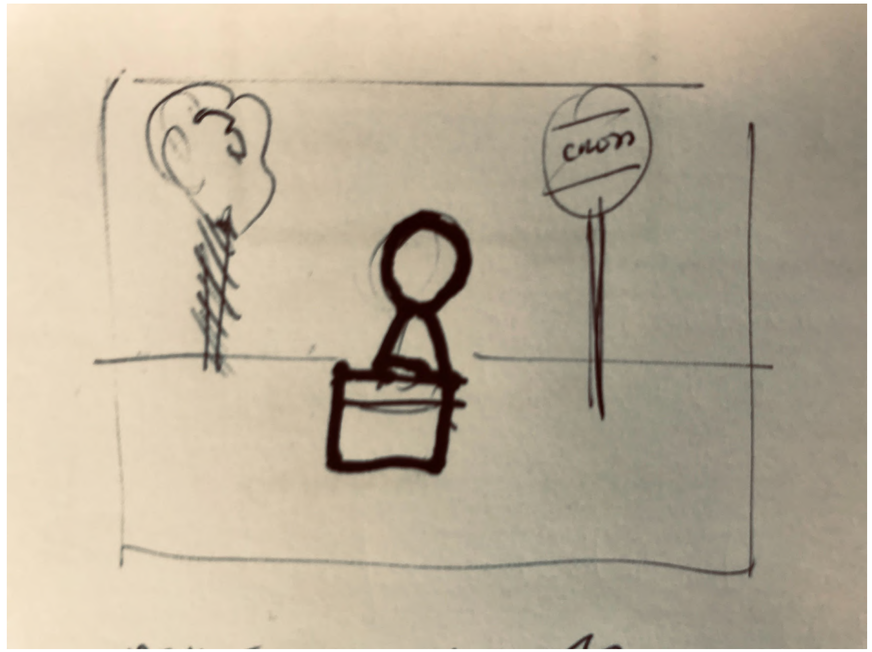
Throughout the process of creating a query and managing it.

Information without emotion is not well retained.

Stories helped communicate what our users were doing and why to the rest of the team.

Telling stories about how our users were meeting this need, why and how was crucial to getting alignment from everyone involved.





Framing the problem

How might we help a non technical user write custom queries to protect their company without generating too much noise?

How might we help a non technical user manage queries they have created, ensuring they become more accurate over time?

Concept creation

Who was involved?

UX Design Lead / Researcher
Cyber security SME
Product manager
CTO
VP Engineering
UI Designer
Customer success manager

Breaking down complexity

```
(source=[Twitter])

AND

([Asset.company = Digital Shadows] or [Asset.domain = digitalshadows.co]
or [Asset.domain = digitalshadows.co.de] or [Asset.domain =
digitalshadows.com] or [Asset.domain = digitalshadows.co.uk])

AND

([Keyword.group = Hacktivist_keywords])

AND

(source=[Twitter])

AND

([Asset.company = Digital Shadows] or [Asset.domain = digitalshadows.co]
or [Asset.domain = digitalshadows.co.de] or [Asset.domain =
```

1

Query content

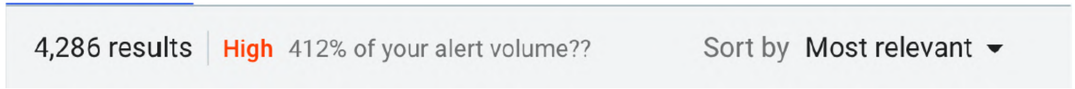
This is what they want to be in their query

2

Query relationships

This is how they want things to be related

Breaking down complexity



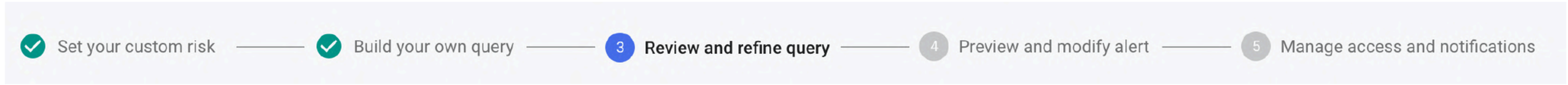
3

Query results

If I ran this query how many results would I have over time?

It’s extremely important I don’t write something that is broad or I will overload my team mates with alerts.

Breaking down complexity



4

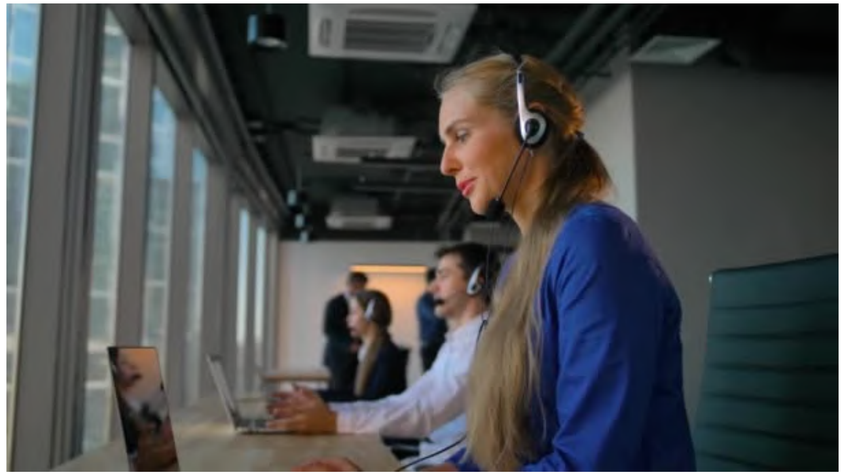
Query building, management & hygiene

How long will this query run for?
Is there any information I want to write about the query on the alert we get so other team mates know what it’s about etc...

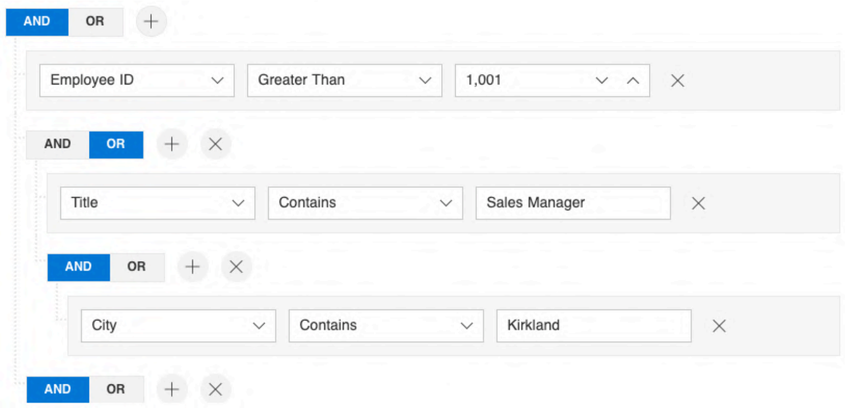
What are the behaviours we want? Where else in the world can we find them?

This is a useful question to ask when looking for inspiration.

On this project we ended up looking at structured conversations. This was our metaphor.



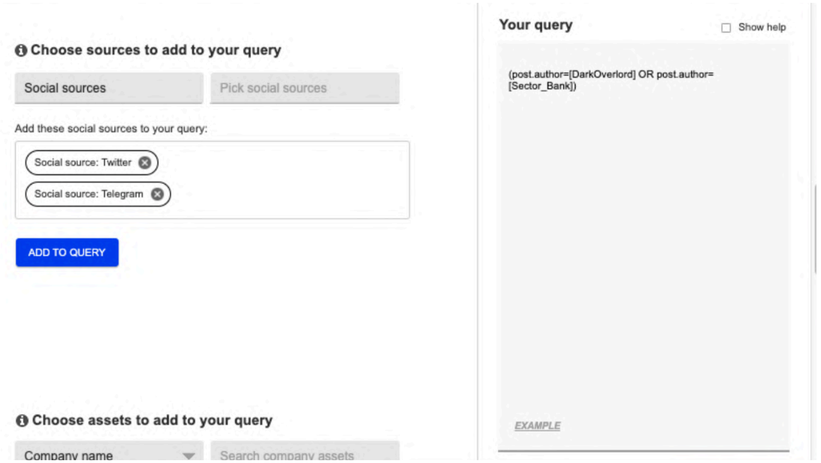
Two distinct approaches



1

Approach 1

Logic trees | tried and tested, put to use by other tools including our leading competitor.



2

Approach 2

Talk to me | Turning query creation into a conversation.

Design technique | Scaffolding

Describe what you want in plain English

1

Design technique | Scaffolding

Describe what you want in plain English

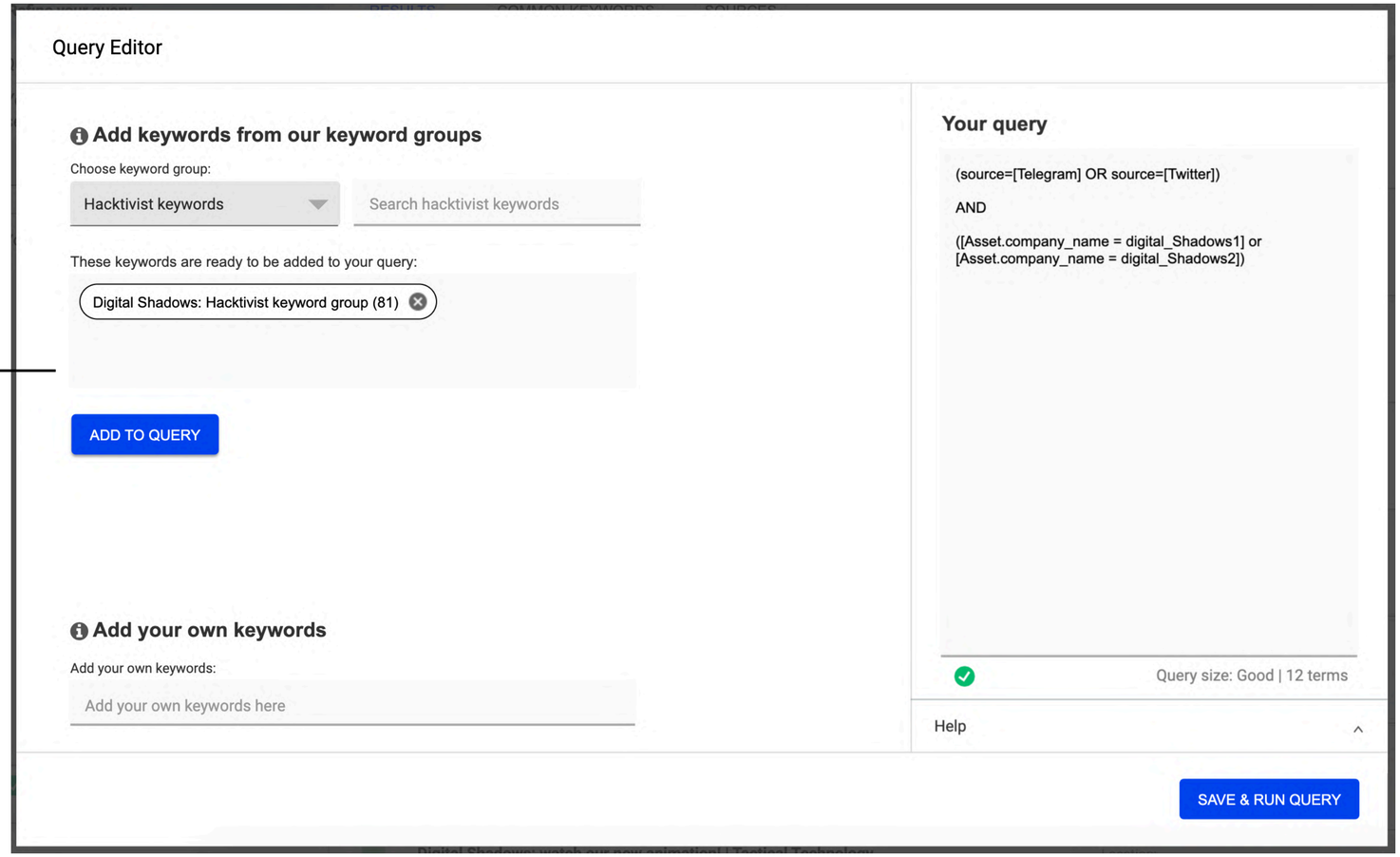
Design technique | Forcing function

Making you press start primes you to act out how the tool will be used in the next step

Design technique | Chunking

Getting you to ‘Add content’ to your query first

3



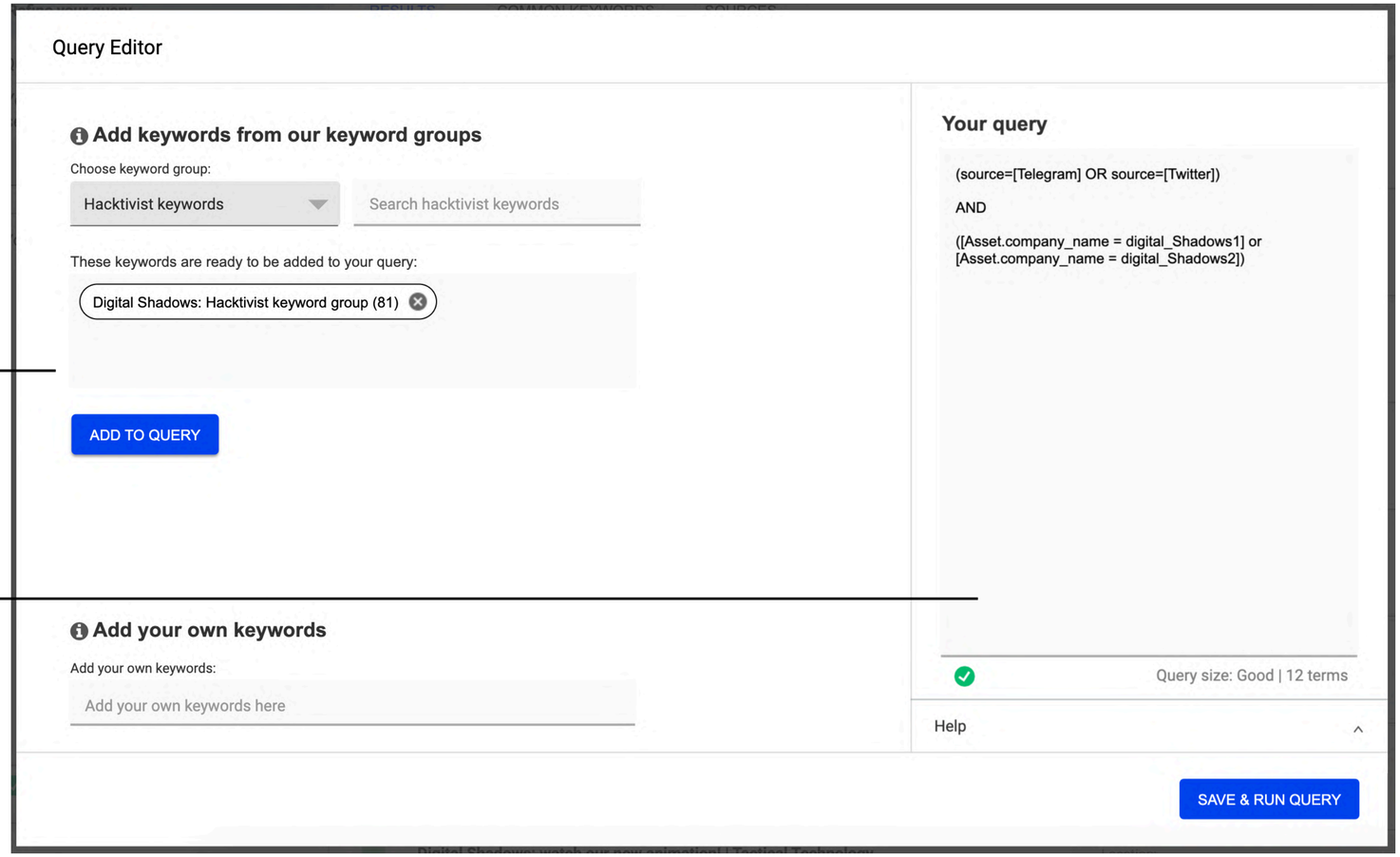
Design technique | Chunking

Getting you to ‘Add content’ to your query first

Design technique | Progressive disclosure

As you add the content to your query, you learn how the query language is structured

You also get to understand relationships much more easily because of how the query is broken down on multiple lines.



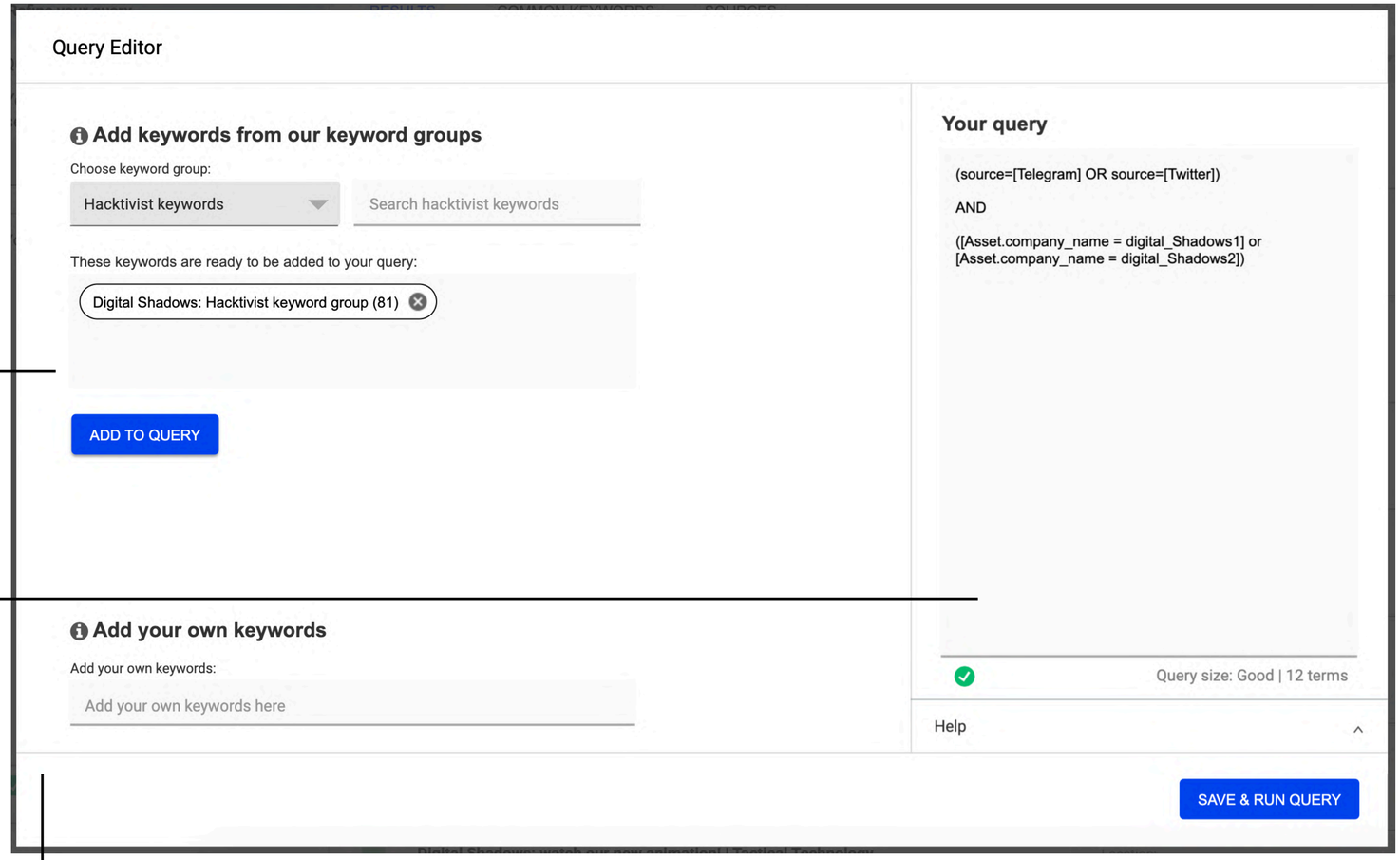
Design technique | Chunking

Getting you to ‘Add content’ to your query first

Design technique | Progressive disclosure

As you add the content to your query, you learn how the query language is structured

You also get to understand relationships much more easily because of how the query is broken down on multiple lines.



3

4

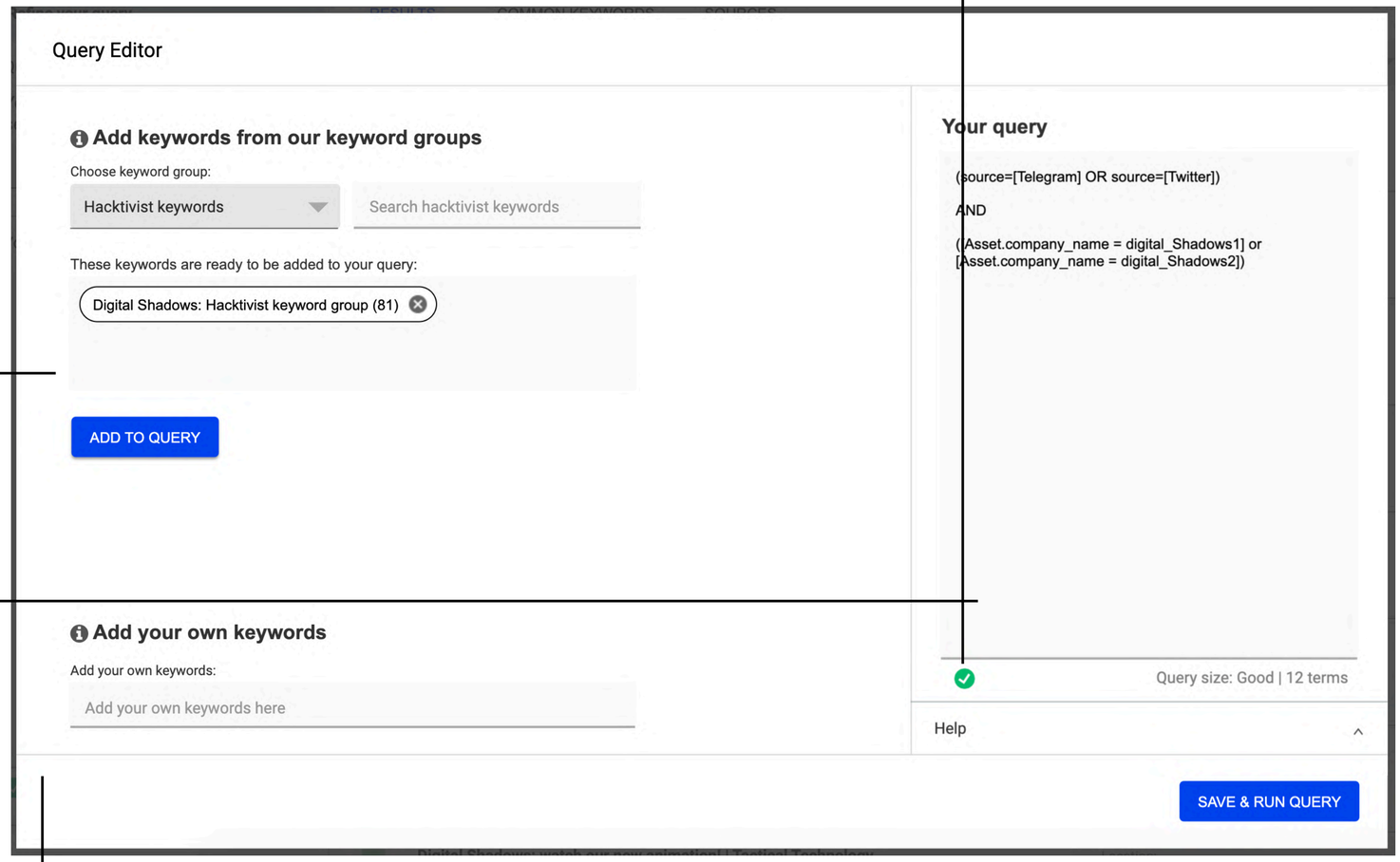
5

Design technique | Adaptive difficulty

Works for first time users and power users who want to just write the query out directly.

6

Immediate feedback if the query won't run



3

Design technique | Chunking

Getting you to 'Add content' to your query first

4

Design technique | Progressive disclosure

As you add the content to your query, you learn how the query language is structured

You also get to understand relationships much more easily because of how the query is broken down on multiple lines.

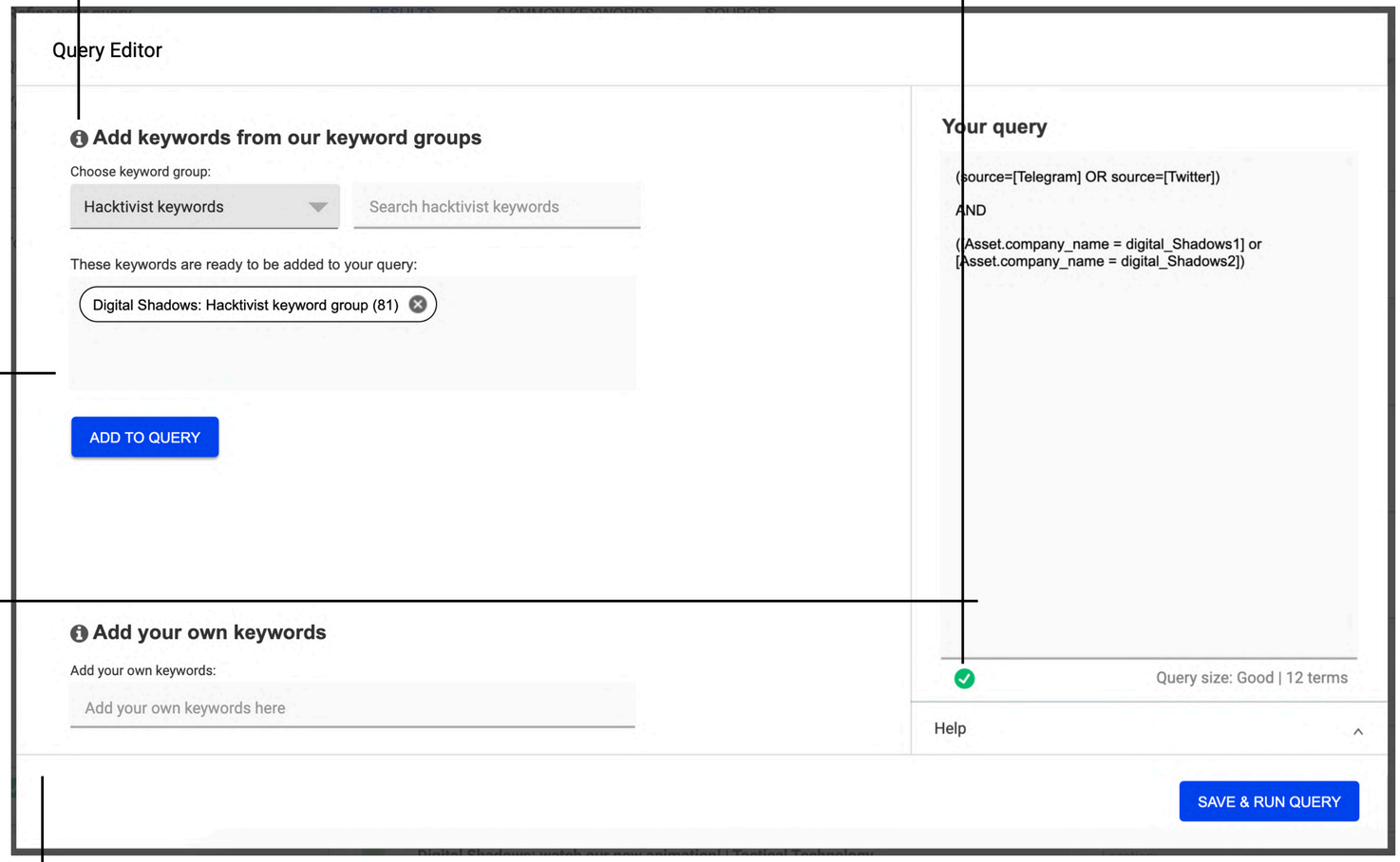
5

Design technique | Adaptive difficulty

Works for first time users and power users who want to just write the query out directly.

7 In context help

6 Immediate feedback if the query won't run



Design technique | Chunking

Getting you to 'Add content' to your query first

3

Design technique | Progressive disclosure

4

As you add the content to your query, you learn how the query language is structured

You also get to understand relationships much more easily because of how the query is broken down on multiple lines.

5

Design technique | Adaptive difficulty

Works for first time users and power users who want to just write the query out directly.

Design evaluation (Internal)

Heuristic evaluation

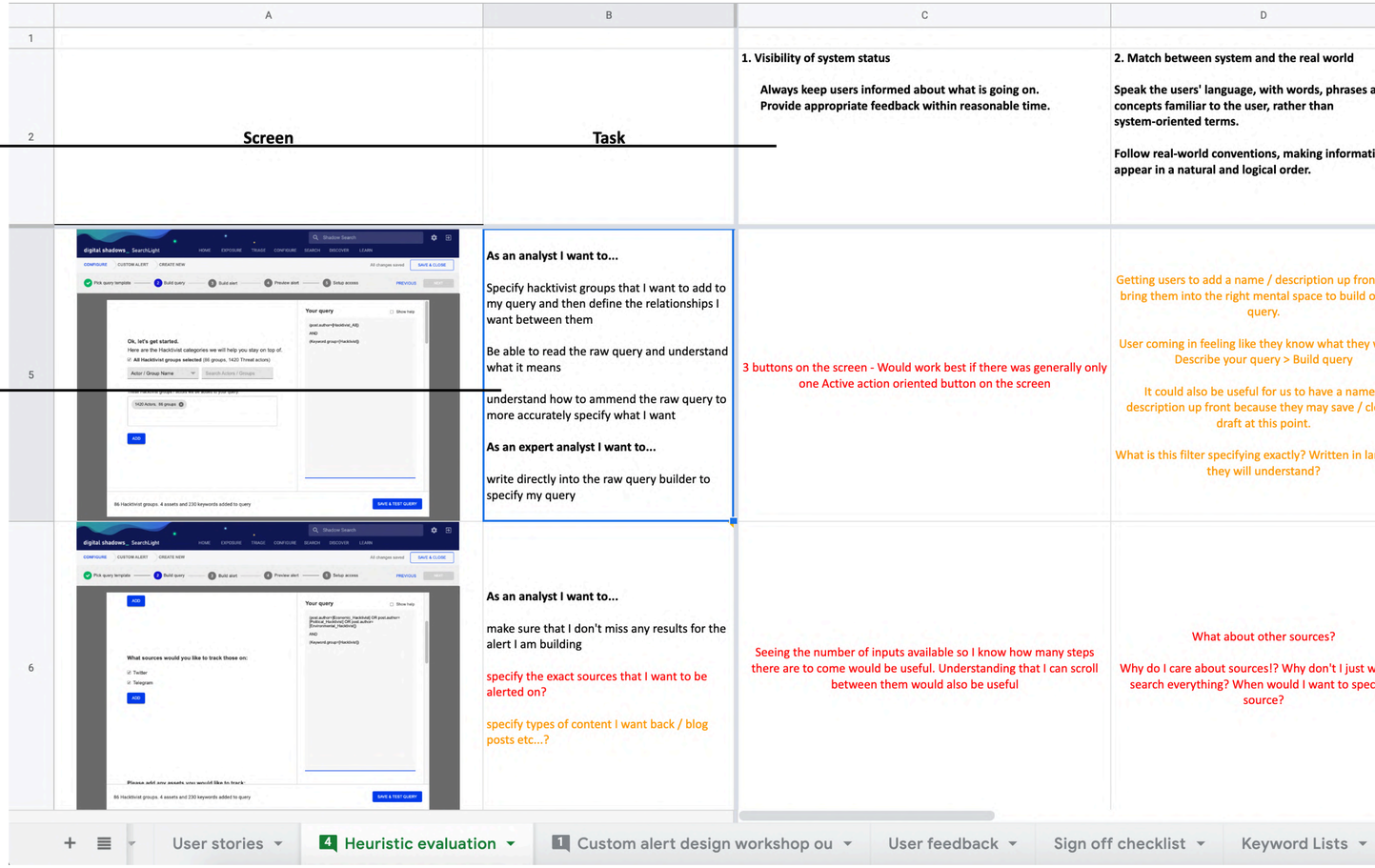
1

Broad rules of thumb that ensure the basics are covered

Task based evaluation

2

Otherwise known as ‘Cognitive walk throughs’ this method of testing involves going through the design with each task the user may want to complete and seeing if it is possible or could be improved.



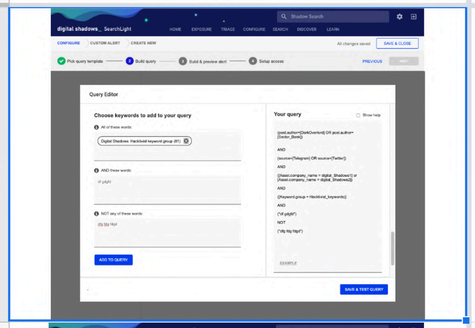
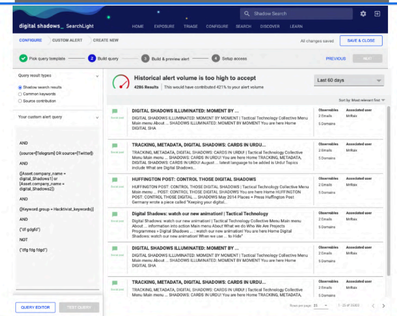
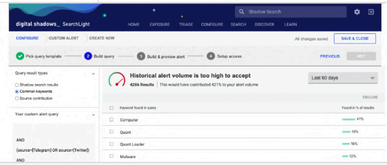
	A	B	C	D
1				
2	**Screen**	**Task**	**1. Visibility of system status** **Always keep users informed about what is going on. Provide appropriate feedback within reasonable time.**	**2. Match between system and the real world** **Speak the users' language, with words, phrases a concepts familiar to the user, rather than system-oriented terms.** **Follow real-world conventions, making informati appear in a natural and logical order.**
5		**As an analyst I want to...** Specify hacktivist groups that I want to add to my query and then define the relationships I want between them Be able to read the raw query and understand what it means understand how to ammend the raw query to more accurately specify what I want **As an expert analyst I want to...** write directly into the raw query builder to specify my query	3 buttons on the screen - Would work best if there was generally only one Active action oriented button on the screen	Getting users to add a name / description up fron bring them into the right mental space to build o query. User coming in feeling like they know what they Describe your query > Build query It could also be useful for us to have a name description up front because they may save / cl draft at this point. What is this filter specifying exactly? Written in la they will understand?
6		**As an analyst I want to...** make sure that I don't miss any results for the alert I am building specify the exact sources that I want to be alerted on? specify types of content I want back / blog posts etc...?	Seeing the number of inputs available so I know how many steps there are to come would be useful. Understanding that I can scroll between them would also be useful	What about other sources? Why do I care about sources!? Why don't I just w search everything? When would I want to spec source?

User stories | 4 Heuristic evaluation | 1 Custom alert design workshop ou | User feedback | Sign off checklist | Keyword Lists

Design evaluation (With users)

Scenario based testing

Your company has an AGM in 2 weeks and you are interested in monitoring social media mentions of your company and VIP’s by known threat actors.

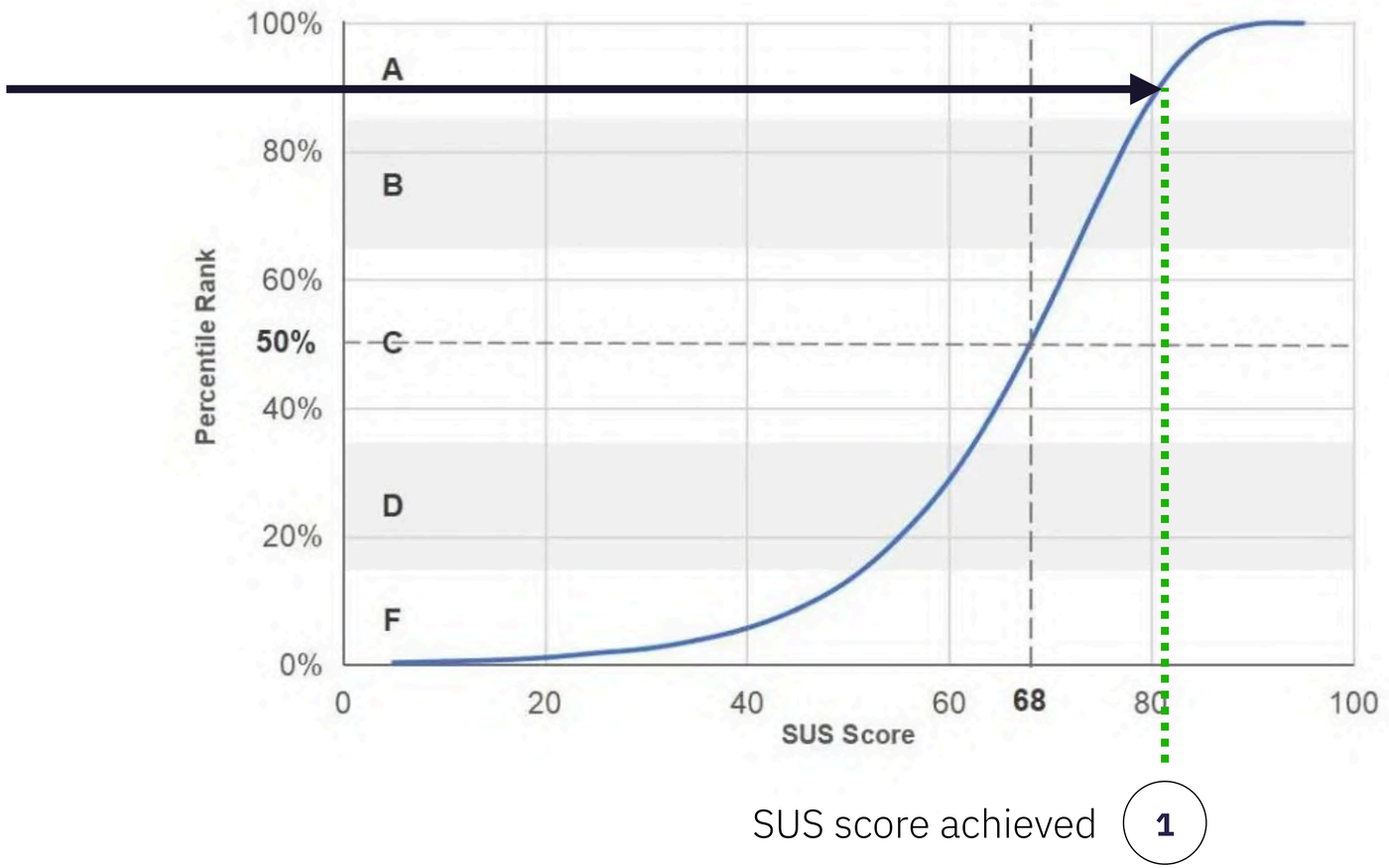
	A	B	C
1			
2	Screen	Mike Rennie - MEDIUM TECHNICAL PROFICIENCY	Gaurav Mukherjee - TECHNICALLY PROFICIE
10		**Keyword group: I would think this is a list of keywords that DS has designtated to being useful in doing keyword searches on hacktivists.** **I would love to be able to see what that is - to see if the word I’m looking for is in that list.** **If from this page you could see the keywords, how would you want to: I see the problem here is that there are 81 here - but it would be good to remove them one by one with the pebble ‘x’, but if that’s not possible I’m not sure how you would allow that functinality.** Next - save and test query I’d then want to see what my results are.	**Keywords: Would like to see the keywords in group. Clicked details. Manually excluded a keyword from the list by addi clause** **“This is good”** More help in adding the keywords - suggesting similar wor **Found save and test quickly.**
11		Historical volume too high - does that mean I have to tighten my query. If this was added to my alerts it would add 400%, why do I care about that? So if I want to reduce I might go to less then 60 days. Clarification: this page is helping you understand and reduce volume of the alert. What would help: Dates, filter and organise by fields. I would assume that these would be the alerts I would recieve when I turn it on. Do you feel comfortable editing the query in this format? **Yes, very. I can see all the reulsts and amend appropriately. Re-edit, and test again - awesome.**	This is saying that if you have this as an alert you would ha Found ‘common keywords’ really quickly
12		Would you ever want to bring back the builder? Only if I forgot what I had as options How would you go back to the previous screen? Previous button in top right I wouldn’t think this was a breadcrumb scenario Top left options: talk through the other options Common keywords	

Design evaluation (With users)

Testing results

Using the SUS (System usability survey) questionnaire after getting users* to complete this scenario we were able to benchmark the design which got an

SUS Score: A



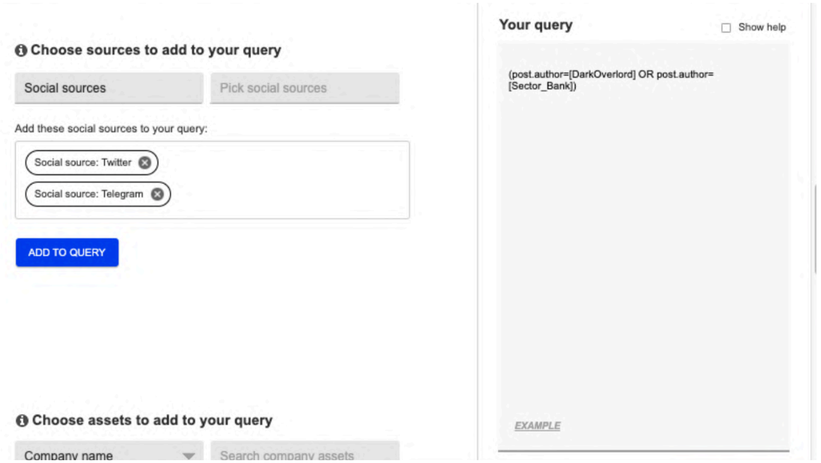
*We tested the design with 6 users

The winning approach

1

Approach 1

Logic trees | tried and tested, put to use by other tools including our leading competitor.



2

Approach 2

Talk to me | Turning query creation into a conversation.

Moving into UI design & thinking of edge cases

Asking two questions:

Do we have a design pattern that already serves this use case?

How could this go wrong?

Design spec

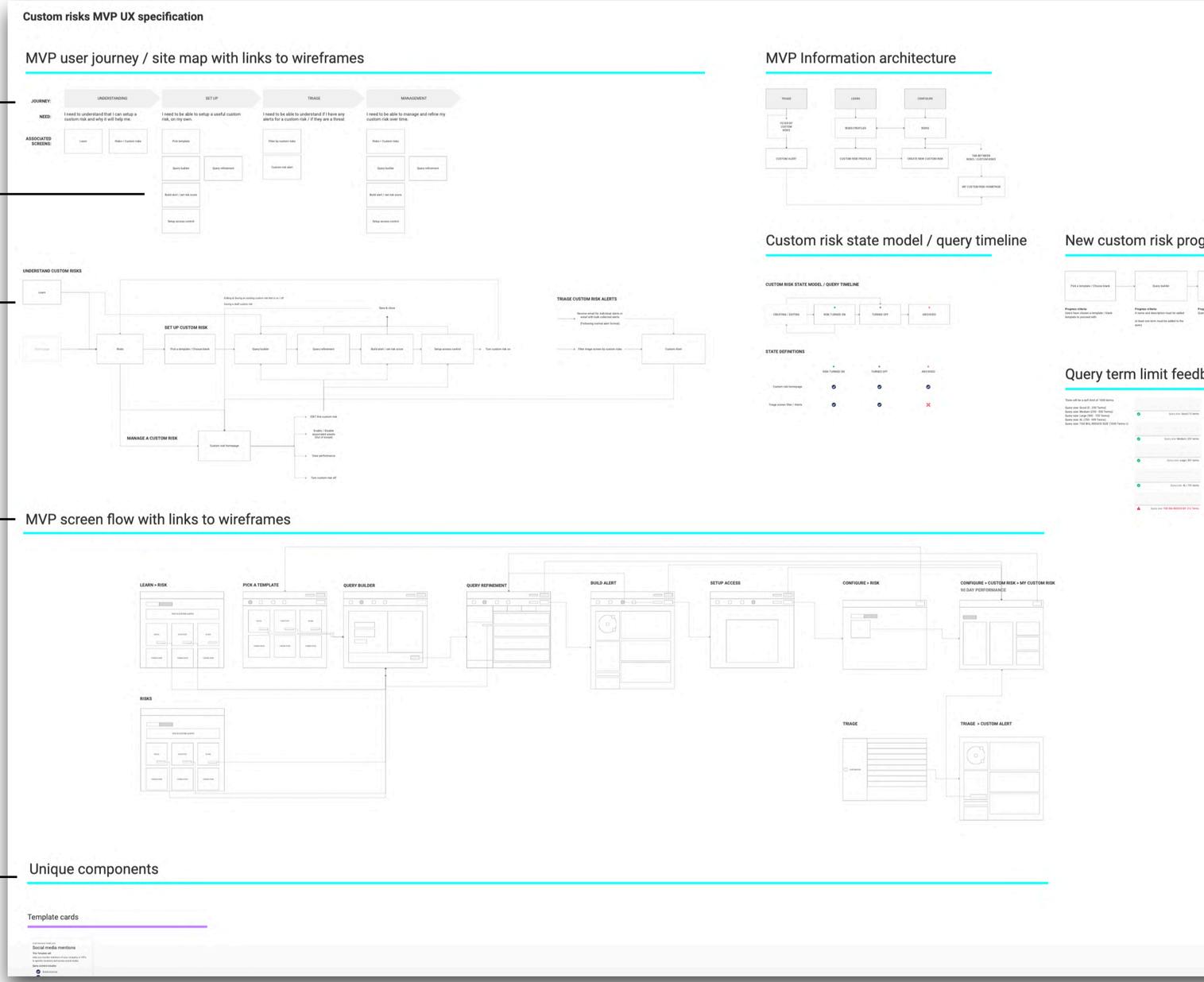
User journey 1

Associated screens 2

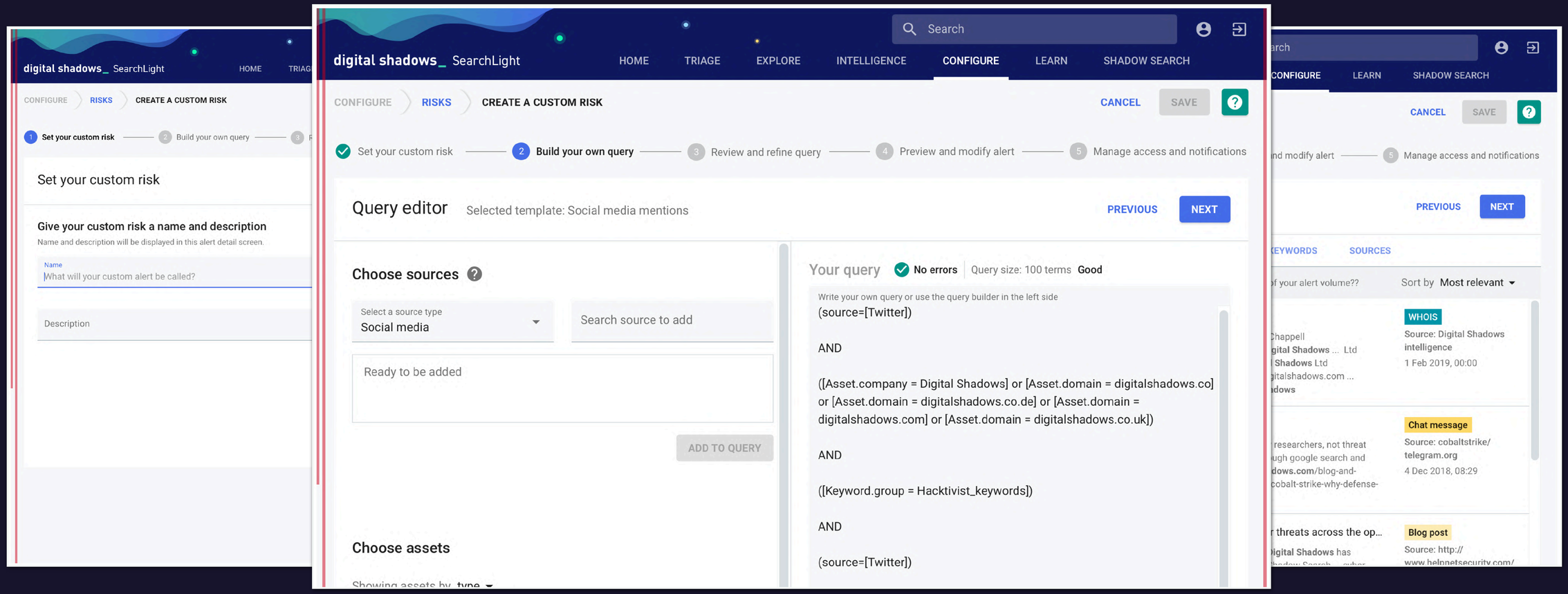
Site map 3

High level screen flow diagram 4

Component level permutations 5



Final UI design (Miya)



Behaviour tracking

Events to track 1

What is the trigger for this event 2

	A	B	C	
1		**Event name**	**Trigger**	**Attrib**
2				
3	**Risk**			
4		customRisk_Tab	Users clicking on the custom risk tab	
5		customRIsk_CreateNew	Users clicking on the create new custom risk button	
6				
7	**Risk/CreateNew/pickTemplate**			
8		customRisk_CreateNew_TemplateChoice	When users select to configure a template, which do they choose?	
9		customRisk_CreateNew_templatePickingFinished	what is the time between each time the user presses 'NEXT' in the custom risk building process	
10				
11	**Risk/CreateNew/queryBuilder**			
12		customRisk_CreateNew_contentTypeAdded	when the 'add to query' button is pressed, what type of information is added	
13		customRisk_CreateNew_contentAmountAdded	when the 'add to query' button is pressed, how much information of a type is added	
14		customRisk_CreateNew_helpSelected	when the users view 'Help'	
15		customRisk_CreateNew_totalQueryTerms	when the user runs the query how many terms do they have?	
16		customRisk_CreateNew_contentSelectAll	When the user selects all for a particular type of content, can we track that along with the type of content they have selected all on. EG(They selected all - on hacktivist threat actors related to banks)	

Our beta measures of success

Can a non technical user write custom queries to protect their company without generating too much noise?

Can a non technical user manage queries they have created, ensuring they become more accurate over time?

Feedback so far

This is a new feature that is currently in Beta. It is too early to say for sure we have been successful, but every beta client has at least 1 custom risk up and running.

Can a non technical user write custom queries to protect their company without generating too much noise?

Can a non technical user manage queries they have created, ensuring they become more accurate over time?

That’s all folks

Thanks for reading