

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?

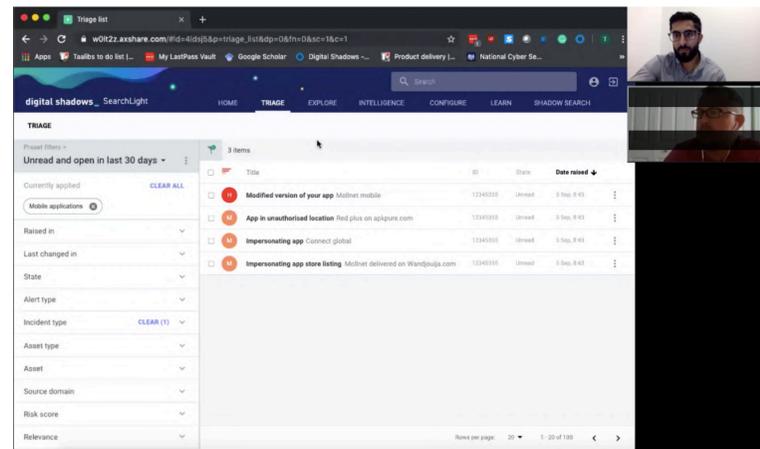
Who was on the team?

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



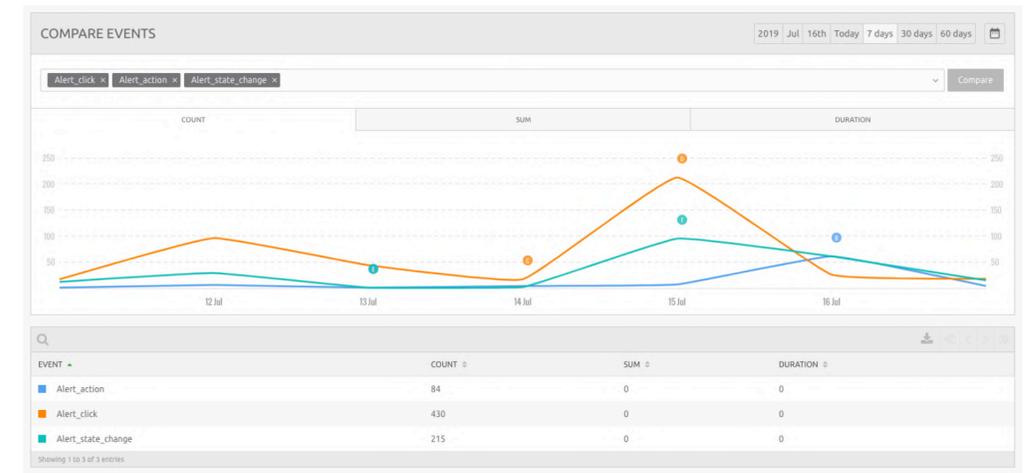
1

User interviews



2

Surveys

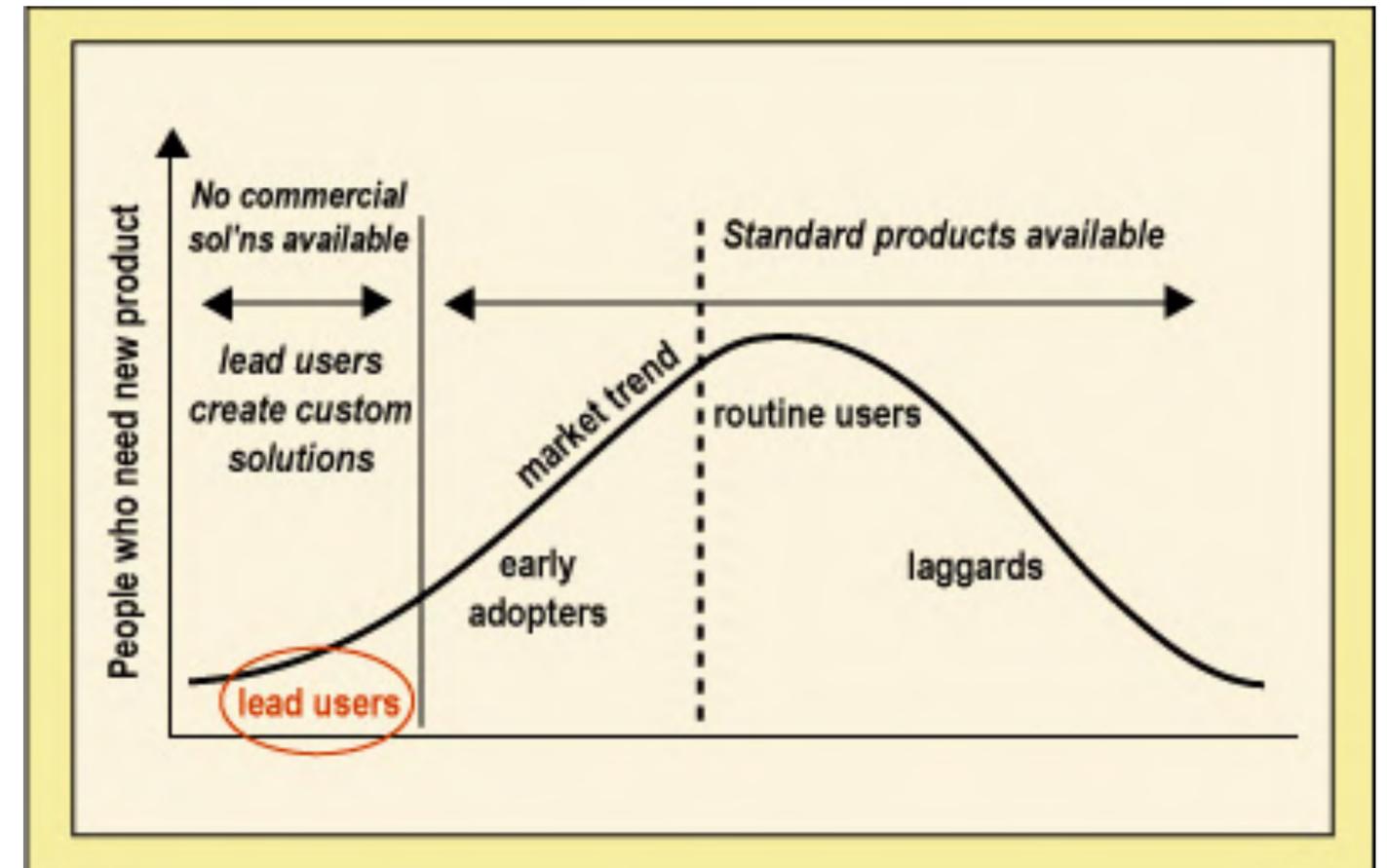


3

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

The screenshot shows a search interface with a search bar at the top containing the query: `(god@war.fail OR "Askar" Erkin OR "Erkin Askar" OR "God of War" OR "dong bing" OR ragnarok.gud@gmail.com) AND type=[WHOIS]`. Below the search bar is a section titled "All your saved searches (11)" with a "Back to all searches" link. The list of saved searches includes:

- 1. ("Askar Erkin" AND type=[WHOIS])
- 2. ("dong bing" AND type=[WHOIS])
- 3. ("Erkin Askar" AND type=[WHOIS])
- 4. God of War (god@war.fail OR "Askar" Erkin OR "Erkin Askar" OR "God of War" OR "dong bing" OR ragnarok.gud@gmail.com) AND type=[WHOIS]
- 5. ("God of War" AND type=[WHOIS])
- 6. ("God of War" AND type=[WHOIS])
- 7. ("God of War" AND type=[WHOIS]) (email alerts)
- 8. God of War (email alerts) (god@war.fail OR "Askar" Erkin OR "Erkin Askar" OR "God of War" OR "dong bing" OR ragnarok.gud@gmail.com) AND type=[WHOIS]
- 9. (god@war.fail AND type=[WHOIS])
- 10. god@war.fail OR "Askar" Erkin OR "Erkin Askar" OR "God of War" OR "dong bing" OR ragnarok.gud@gmail.com (god@war.fail OR "Askar" Erkin OR "Erkin Askar" OR "God of War" OR "dong bing" OR ragnarok.gud@gmail.com) AND type=[WHOIS]
- 11. (ragnarok.gud@gmail.com AND type=[WHOIS])

On the right side, there is a "Hints and Tips" sidebar with the following content:

- Boolean
- Combine keywords or phrases
- Operators
- AND Both terms
- OR Either term
- NOT Excluding terms
- Parentheses can be added to group terms
- (Malware AND "Quantum Leap")
- Search syntax
- Specify a result type, tag, or field
- source=[pastebin.com]
- Autocomplete will assist
- Highlight and pivot
- Highlight any word or phrase
- Click Search to perform a search

Two callout boxes are present: a circle with the number "1" pointing to the first saved search, and a circle with the number "2" pointing to the eighth saved search.

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

The screenshot shows a search engine interface with a search bar at the top containing the query: `(god@war.fail OR "Askar] Erkin" OR "Erkin Askar" OR "God of War" OR "dong bing" OR ragnarok.gud@gmail.com) AND type=[WHOIS]`. Below the search bar is a section titled "All your saved searches (11)" with a link to "Back to all searches". The list of saved searches includes:

- ("Askar Erkin" AND type=[WHOIS])
- ("dong bing" AND type=[WHOIS])
- ("Erkin Askar" AND type=[WHOIS])
- God of War
(god@war.fail OR "Askar] Erkin" OR "Erkin Askar" OR "God of War" OR "dong bing" OR ragnarok.gud@gmail.com) AND type=[WHOIS]
- ("God of War" AND type=[WHOIS])
- ("God of War" AND type=[WHOIS])
- ("God of War" AND type=[WHOIS]) (email alerts)
- God of War (email alerts)
(god@war.fail OR "Askar] Erkin" OR "Erkin Askar" OR "God of War" OR "dong bing" OR ragnarok.gud@gmail.com) AND type=[WHOIS]
- (god@war.fail AND type=[WHOIS])
- god@war.fail OR "Askar Erkin" OR "Erkin Askar" OR "God of War" OR "dong bing" OR ragnarok.gud@gmail.
(god@war.fail OR "Askar Erkin" OR "Erkin Askar" OR "God of War" OR "dong bing" OR ragnarok.gud@gmail.com) AND type=[WHOIS]
- (ragnarok.gud@gmail.com AND type=[WHOIS])

On the right side, there is a "Hints and Tips" section with the following content:

- Boolean
- Combine keywords or phrases
- Operators
- AND** Both terms
- OR** Either term
- NOT** Excluding terms
- Parentheses** can be added to group terms
- (Malware AND "Quantum Leap")
- Search syntax
- Specify a result type, tag, or field
- source=[pastebin.com]
- Autocomplete will assist you
- Highlight and pivot
- Highlight any word or phrase
- Click Search to perform a search

Understanding the journey

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

Doing
Thinking
Feeling

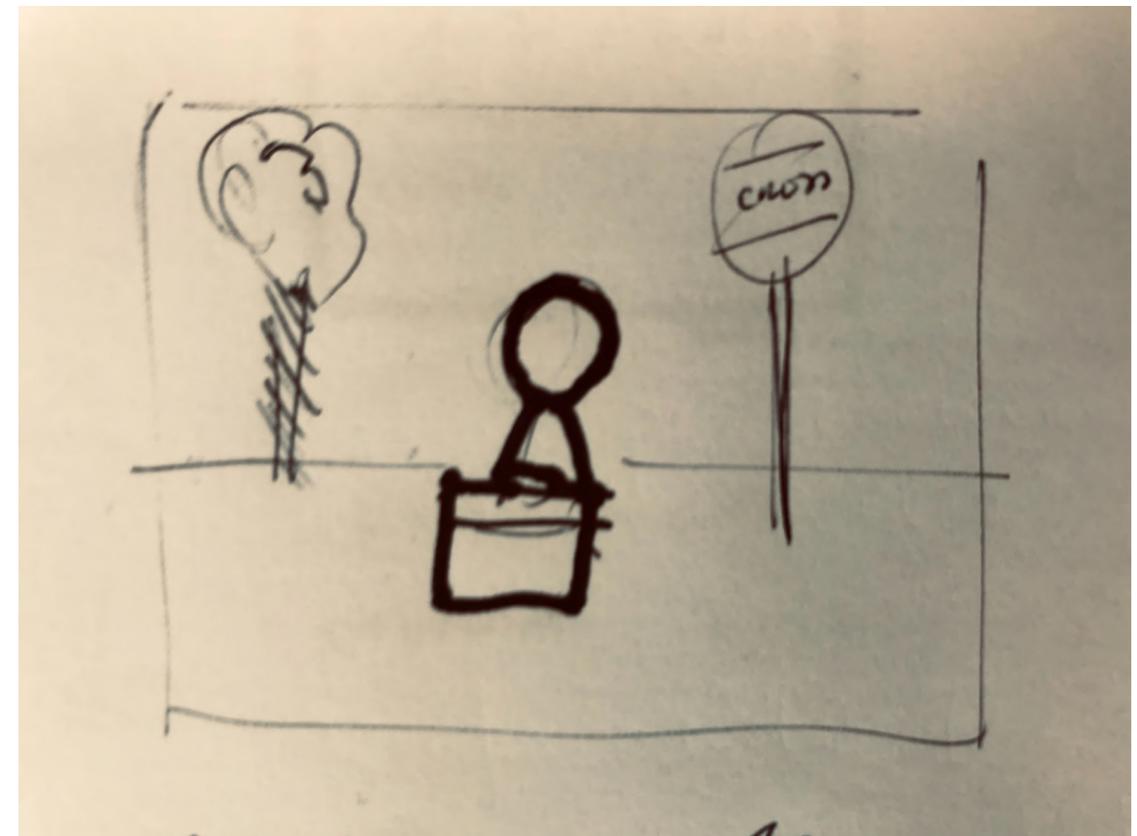
Throughout the process of creating a query and managing it.



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 = Hactivist_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

4,286 results | **High** 412% of your alert volume??

Sort by Most relevant ▼

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

✓ Set your custom risk ——— ✓ Build your own query ——— 3 Review and refine query ——— 4 Preview and modify alert ——— 5 Manage access and notifications

4

Query building, management & hygiene

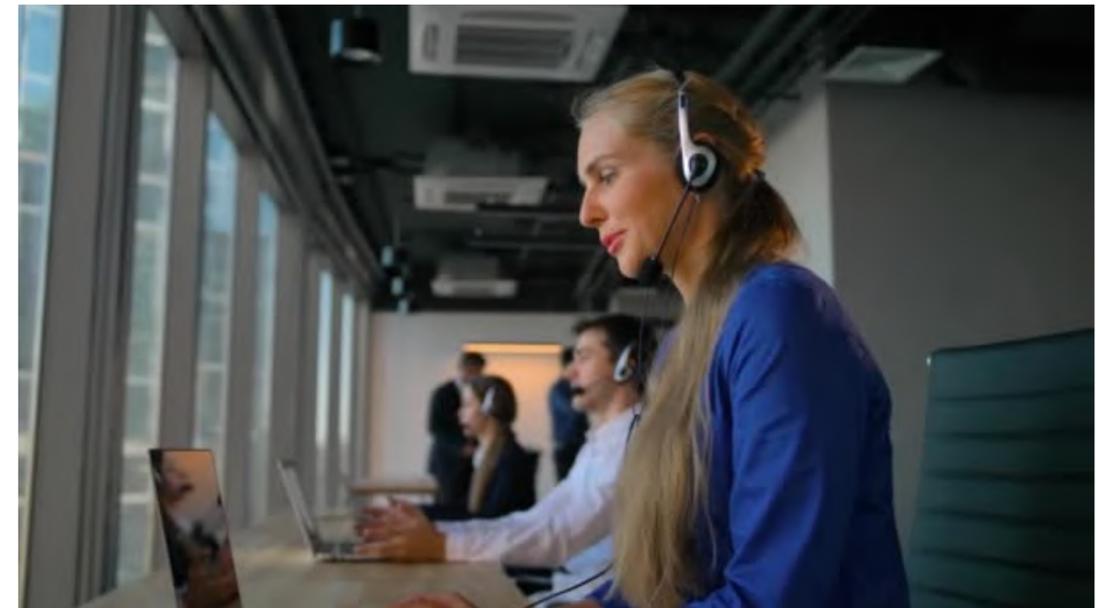
How long will this query run for?

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

A screenshot of a query builder interface. It features a vertical stack of four filter clauses, each with its own AND/OR logic selector and add/remove buttons. The clauses are: 1. Employee ID Greater Than 1,001. 2. Title Contains Sales Manager. 3. City Contains Kirkland. 4. (The fourth clause is partially obscured but follows the same pattern). The interface uses a clean, modern design with light gray backgrounds and blue accents for the logic buttons.

1

Approach 1

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

A screenshot of a query builder interface with a conversational approach. It is divided into three main sections: 1. 'Choose sources to add to your query' with a 'Pick social sources' button and a list of selected sources (Twitter, Telegram). 2. 'Choose assets to add to your query' with a 'Search company assets' input field. 3. 'Your query' which displays the resulting query: `(post.author=[DarkOverlord] OR post.author=[Sector_Bank])`. The interface is clean and uses a light gray color scheme.

2

Approach 2

Talk to me | Turning query creation into a conversation.

Design technique / Scaffolding

Describe what you want
in plain English

1

Query Editor

Give your custom alert a name & description:

Name:

What will your custom alert be called? 0 / 40

Description:

What will this custom alert do? 0 / 200

This description will show up on alerts raised

START BUILDING QUERY

SAVE & RUN QUERY

Design technique / Scaffolding

Describe what you want
in plain English

1

Design technique / Forcing function

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

2

The screenshot shows a 'Query Editor' interface. At the top, there are navigation links for 'RESULTS', 'COMMON KEYWORDS', and 'SOURCES'. Below these is a large empty text area. A section titled 'Give your custom alert a name & description:' contains two input fields. The first is labeled 'Name:' and has the placeholder text 'What will your custom alert be called?' with a character count of '0 / 40'. The second is labeled 'Description:' and has the placeholder text 'What will this custom alert do?' with a character count of '0 / 200'. Below the description field, a note states 'This description will show up on alerts raised'. A 'START BUILDING QUERY' button is positioned below the description field. At the bottom right of the interface is a 'SAVE & RUN QUERY' button. A footer at the very bottom contains the text 'Digital Shadows: watch our new animation! | Tactical Technology'.

Design technique / Chunking
Getting you to 'Add content' to
your query first

3

The screenshot shows a 'Query Editor' interface with two main sections. The left section is titled 'Add keywords from our keyword groups' and includes a dropdown menu for 'Hactivist keywords' and a search input field. Below this, a list of keywords is shown, with 'Digital Shadows: Hactivist keyword group (81)' selected. A blue 'ADD TO QUERY' button is positioned below the list. The right section, titled 'Your query', displays the resulting query: '(source=[Telegram] OR source=[Twitter]) AND ([Asset.company_name = digital_Shadows1] or [Asset.company_name = digital_Shadows2])'. A green checkmark and the text 'Query size: Good | 12 terms' are visible at the bottom of this section. A 'Help' link is located at the bottom right of the right section. A large blue 'SAVE & RUN QUERY' button is positioned at the bottom right of the entire interface.

Query Editor

ⓘ Add keywords from our keyword groups

Choose keyword group:

Hactivist keywords Search hactivist keywords

These keywords are ready to be added to your query:

Digital Shadows: Hactivist keyword group (81) ✕

ADD TO QUERY

ⓘ Add your own keywords

Add your own keywords:

Add your own keywords here

Your query

(source=[Telegram] OR source=[Twitter])
AND
([Asset.company_name = digital_Shadows1] or
[Asset.company_name = digital_Shadows2])

Query size: Good | 12 terms

Help ^

SAVE & RUN QUERY

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.

The screenshot shows a 'Query Editor' interface. It is divided into two main sections: 'Add keywords from our keyword groups' and 'Add your own keywords'. The 'Add keywords from our keyword groups' section includes a dropdown menu for 'Hactivist keywords', a search input field, and a list of available keyword groups. One group, 'Digital Shadows: Hactivist keyword group (81)', is highlighted with a blue button labeled 'ADD TO QUERY'. The 'Add your own keywords' section has a text input field with the placeholder 'Add your own keywords here'. On the right side, the 'Your query' section displays the current query: '(source=[Telegram] OR source=[Twitter]) AND ([Asset.company_name = digital_Shadows1] or [Asset.company_name = digital_Shadows2])'. Below the query, there is a green checkmark and the text 'Query size: Good | 12 terms'. At the bottom right, there is a blue button labeled 'SAVE & RUN QUERY'. Two annotations are present: a circle with the number '3' pointing to the 'ADD TO QUERY' button, and a circle with the number '4' pointing to the 'Add your own keywords' section.

Design technique / Chunking
Getting you to 'Add content' to your query first

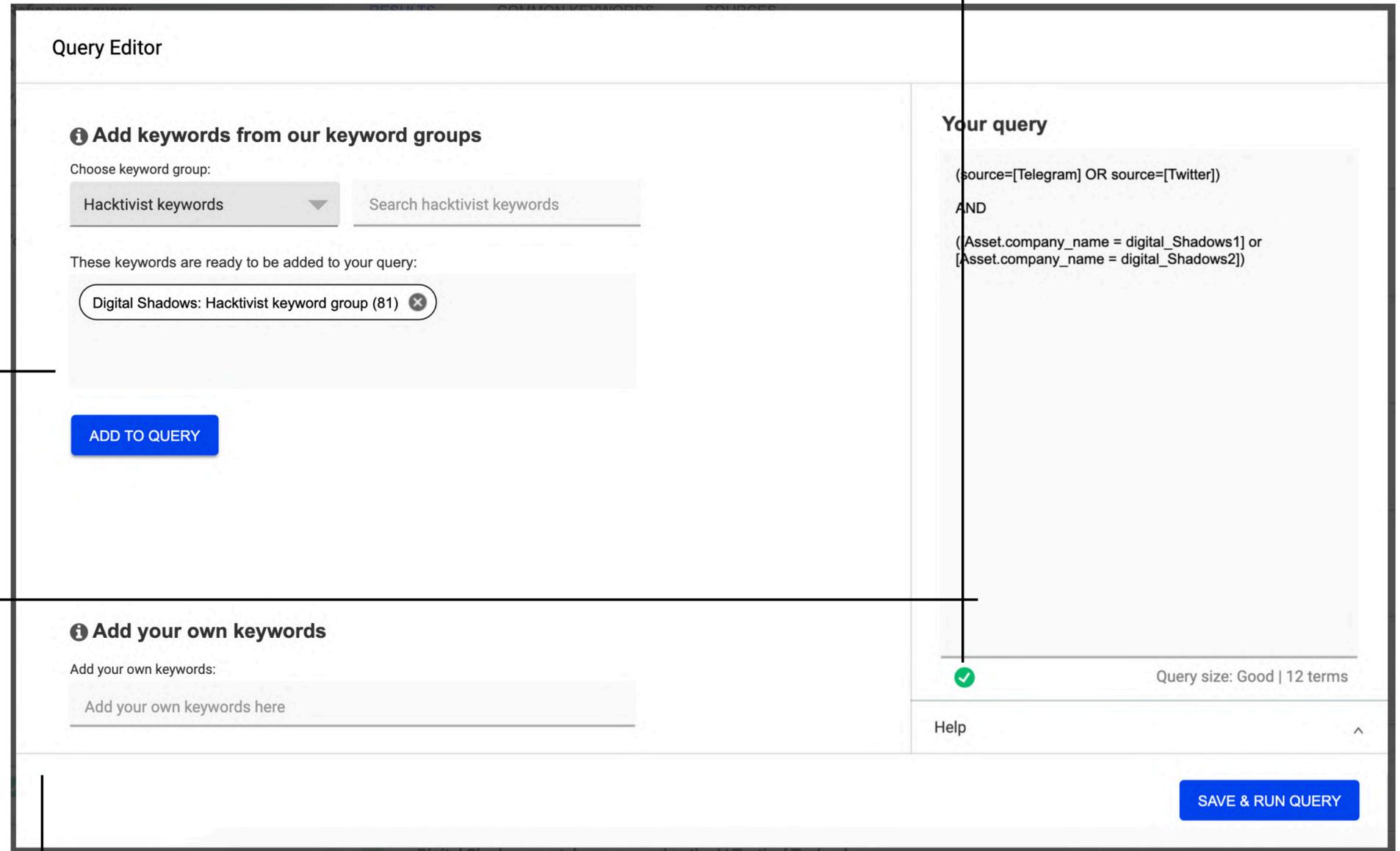
Design technique / Progressive disclosure
As you add the content to your query, you learn how the query language is structured

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

The screenshot shows a 'Query Editor' interface. It is divided into two main sections: 'Add keywords from our keyword groups' and 'Add your own keywords'. The 'Add keywords from our keyword groups' section includes a dropdown menu for 'Choose keyword group' (currently set to 'Hactivist keywords') and a search input field 'Search hactivist keywords'. Below this, a list of keywords is shown, with one selected: 'Digital Shadows: Hactivist keyword group (81)'. A blue 'ADD TO QUERY' button is positioned below the list. The 'Add your own keywords' section features a text input field labeled 'Add your own keywords here'. On the right side, the 'Your query' section displays the generated query: '(source=[Telegram] OR source=[Twitter]) AND ([Asset.company_name = digital_Shadows1] or [Asset.company_name = digital_Shadows2])'. Below the query, a green checkmark and the text 'Query size: Good | 12 terms' are visible. At the bottom right, there is a blue 'SAVE & RUN QUERY' button. Three annotations are present: '3' points to the 'ADD TO QUERY' button, '4' points to the 'Add your own keywords' section, and '5' points to the 'SAVE & RUN QUERY' button.

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



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

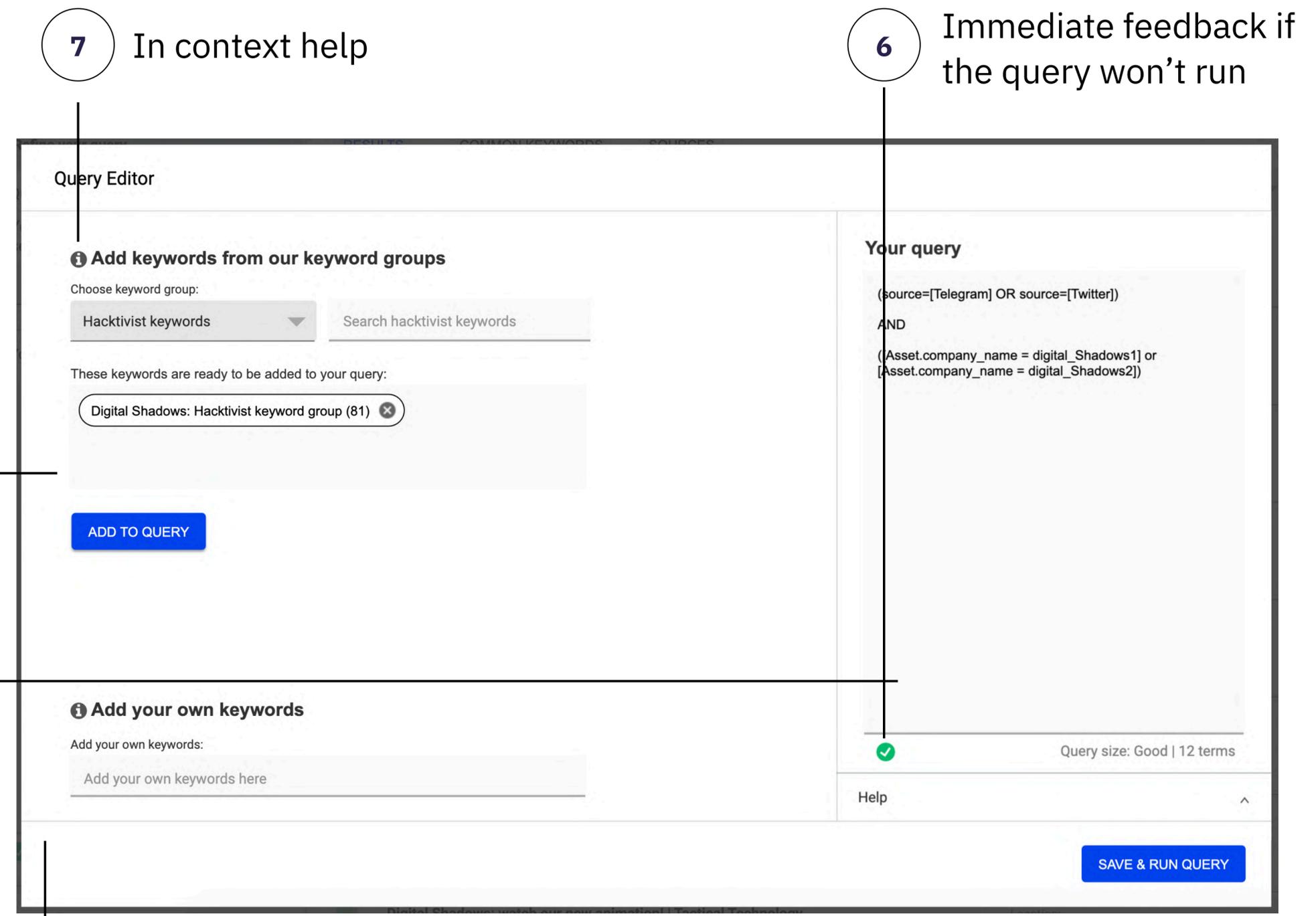
Design technique / Adaptive difficulty

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

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

7

6

In context help

Immediate feedback if the query won't run

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

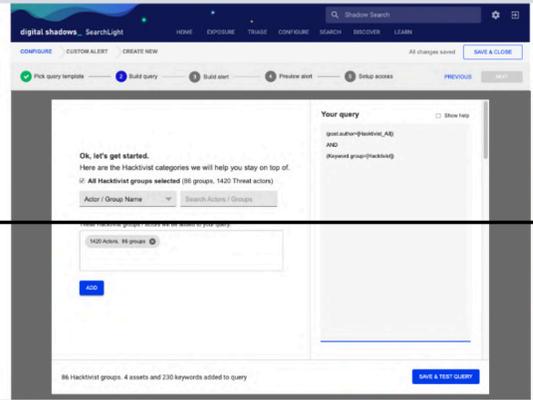
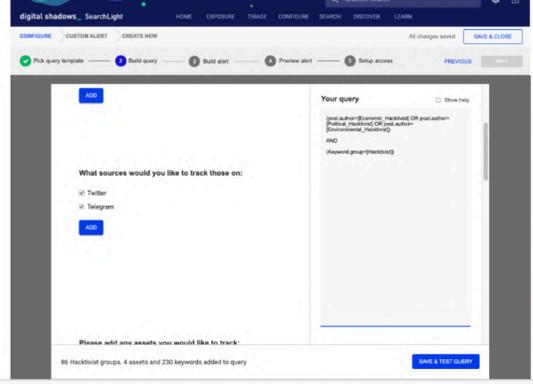
Broad rules of thumb that ensure the basics are covered

Task based evaluation

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.

1

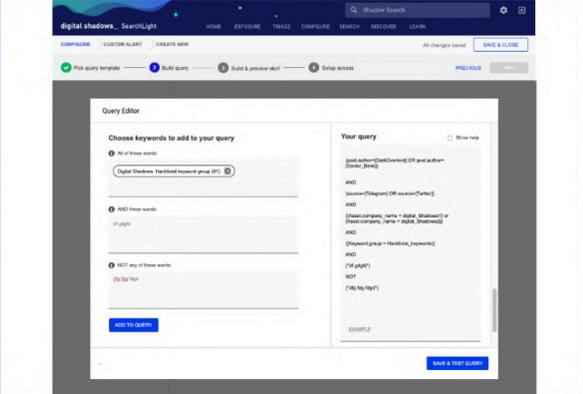
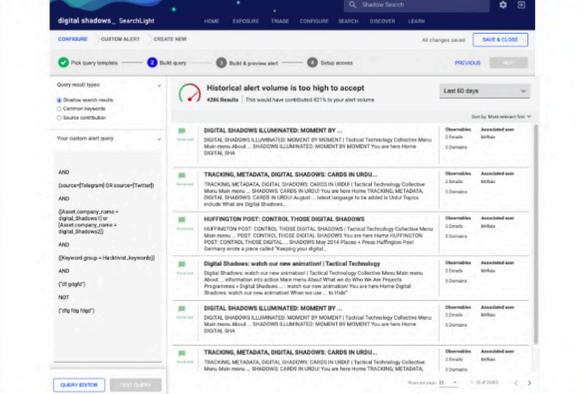
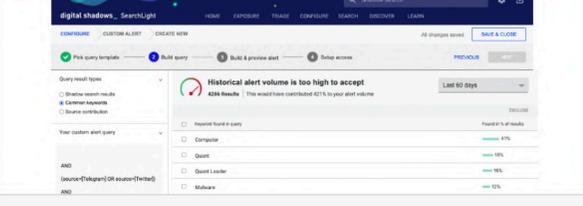
2

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

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.

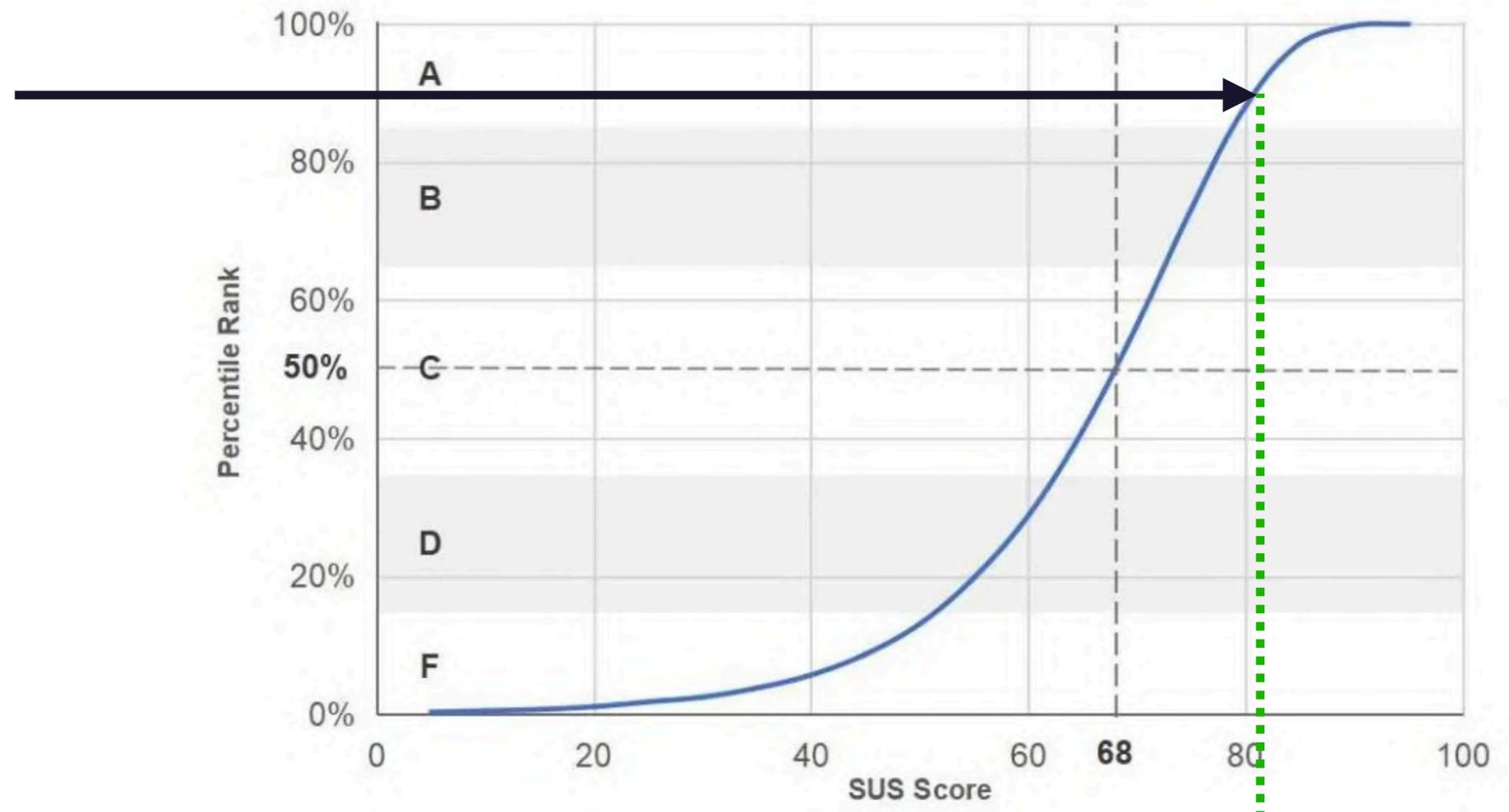
| | A | B | C |
|----|---|---|--|
| 1 | | | |
| 2 | Screen | Mike Rennie - MEDIUM TECHNICAL PROFICIENCY | Gaurav Mukherjee - TECHNICALLY PROFICIENT |
| 10 |  | <p>Keyword group: I would think this is a list of keywords that DS has designated to being useful in doing keyword searches on hackers.</p> <p>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 functionality.</p> <p>Next - save and test query I'd then want to see what my results are.</p> | <p>Keywords: Would like to see the keywords in group. Clicked details. Manually excluded a keyword from the list by adding a clause</p> <p>"This is good"</p> <p>More help in adding the keywords - suggesting similar words</p> <p>Found save and test quickly.</p> |
| 11 |  | <p>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 than 60 days.</p> <p>Clarification: this page is helping you understand and reduce volume of the alert.</p> <p>What would help: Dates, filter and organise by fields.</p> <p>I would assume that these would be the alerts I would receive when I turn it on.</p> <p>Do you feel comfortable editing the query in this format? Yes, very. I can see all the results and amend appropriately. Re-edit, and test again - awesome.</p> | <p>This is saying that if you have this as an alert you would have found 'common keywords' really quickly</p> |
| 12 |  | <p>Would you ever want to bring back the builder? Only if I forgot what I had as options</p> <p>How would you go back to the previous screen? Previous button in top right I wouldn't think this was a breadcrumb scenario</p> <p>Top left options: talk through the other options Common keywords</p> | |

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



SUS score achieved **1**

*We tested the design with 6 users

The winning approach

A screenshot of a logic tree query builder interface. It features four stacked filter clauses, each with its own 'AND/OR' and '+/x' controls. The first clause is 'Employee ID' with a 'Greater Than' operator and the value '1,001'. The second clause is 'Title' with a 'Contains' operator and the value 'Sales Manager'. The third clause is 'City' with a 'Contains' operator and the value 'Kirkland'. The fourth clause is partially visible.

1

Approach 1

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

A screenshot of a conversational query builder interface. It is divided into two main sections: 'Choose sources to add to your query' and 'Choose assets to add to your query'. The first section has a 'Social sources' dropdown and a 'Pick social sources' button. Below it, a list shows 'Social source: Twitter' and 'Social source: Telegram' with 'x' icons to remove them. An 'ADD TO QUERY' button is present. The second section has a 'Company name' dropdown and a 'Search company assets' button. To the right, a 'Your query' panel displays the generated query: '(post.author=[DarkOverlord] OR post.author=[Sector_Bank])' and includes a 'Show help' link and an 'EXAMPLE' label.

2

Approach 2

Talk to me | Turning query creation into a conversation.

Design spec

User journey

1

Associated screens

2

Site map

3

High level screen flow diagram

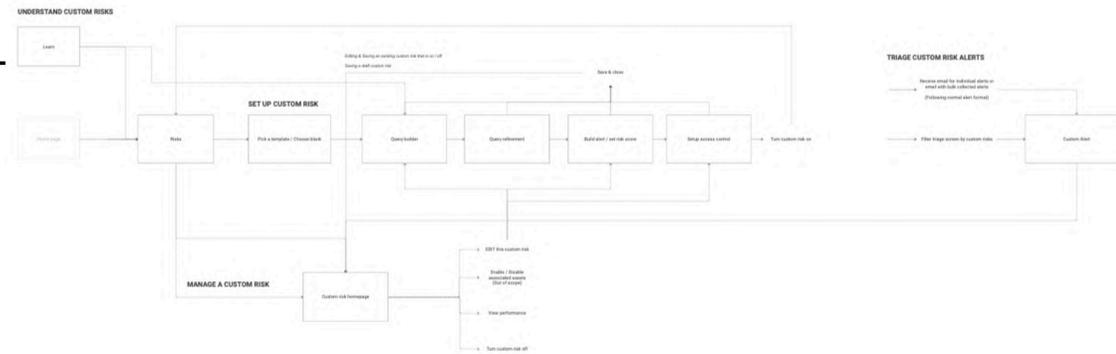
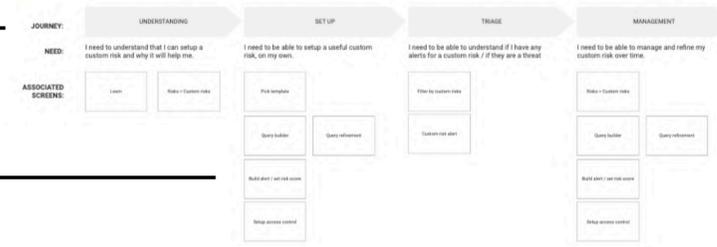
4

Component level permutations

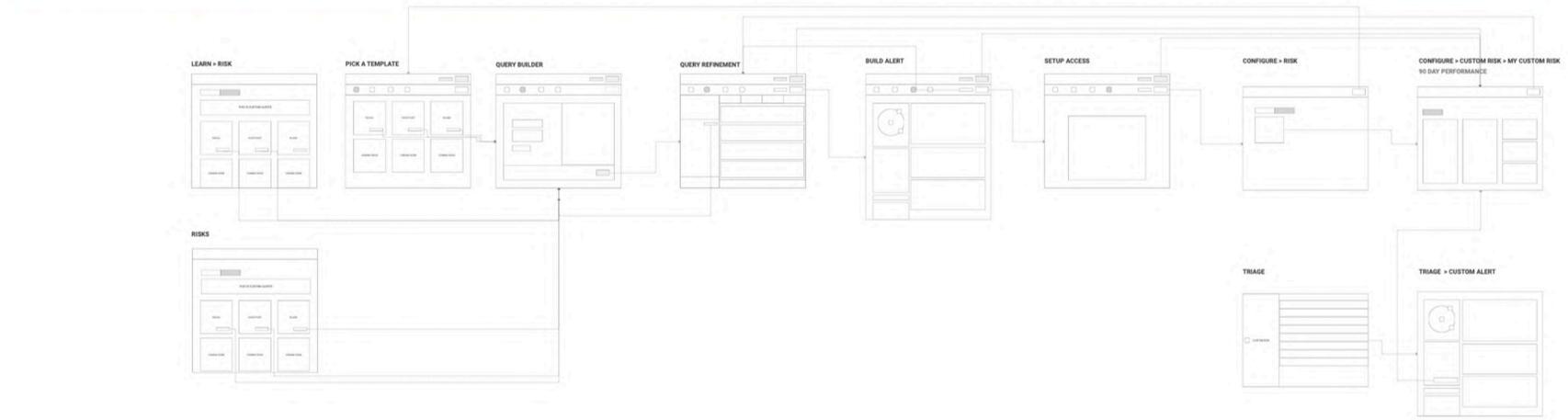
5

Custom risks MVP UX specification

MVP user journey / site map with links to wireframes



MVP screen flow with links to wireframes

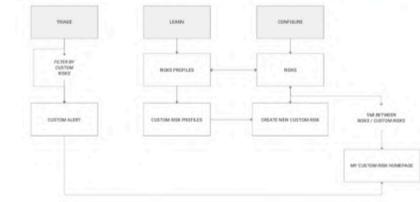


Unique components

Template cards



MVP Information architecture



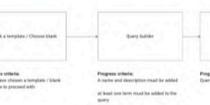
Custom risk state model / query timeline



STATE DEFINITIONS



New custom risk prog



Query term limit feed



Final UI design (Miya)

digital shadows SearchLight | HOME | TRIAGE | EXPLORE | INTELLIGENCE | **CONFIGURE** | LEARN | SHADOW SEARCH

CONFIGURE > RISKS > CREATE A CUSTOM RISK

1 Set your custom risk — 2 Build your own query — 3 Review and refine query — 4 Preview and modify alert — 5 Manage access and notifications

Set your custom risk

Give your custom risk a name and description
Name and description will be displayed in this alert detail screen.

Name: What will your custom alert be called?

Description:

Query editor | Selected template: Social media mentions | PREVIOUS | NEXT

Choose sources ?

Select a source type: Social media | Search source to add

Ready to be added

ADD TO QUERY

Your query ✓ No errors | Query size: 100 terms | Good

Write your own query or use the query builder in the left side

(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 = Hactivist_keywords])

AND

(source=[Twitter])

KEYWORDS | **SOURCES**

Sort by: Most relevant

| | |
|--|---|
| Chappell igital Shadows ... Ltd Shadows Ltd igitalshadows.com ... adows | WHOIS Source: Digital Shadows intelligence 1 Feb 2019, 00:00 |
| researchers, not threat ugh google search and dows.com/blog-and- cobalt-strike-why-defense- | Chat message Source: cobaltstrike/ telegram.org 4 Dec 2018, 08:29 |
| r threats across the op... | Blog post Source: http:// www.helnetsecurity.com/ |

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

