RSAConference2020
San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: IDY3-R07

The Value of Human-Centered Research in Identity and Access Management

Keita Wangari
Senior UX Researcher
Google Cloud

Charlotte Massey
UX Researcher
Google Cloud

Juliette Hainline
UX Researcher
Google Cloud

Agenda

1 | Human-Centered Research

2 | Case Study: Security Center

3 | Case Study: Alert Center

4 | Apply & Resources

RSAConference2020

1 | Human-Centered Research

Is it **software testing**?

Is it **usability testing**?

Is it about **making users happy**?

Old World

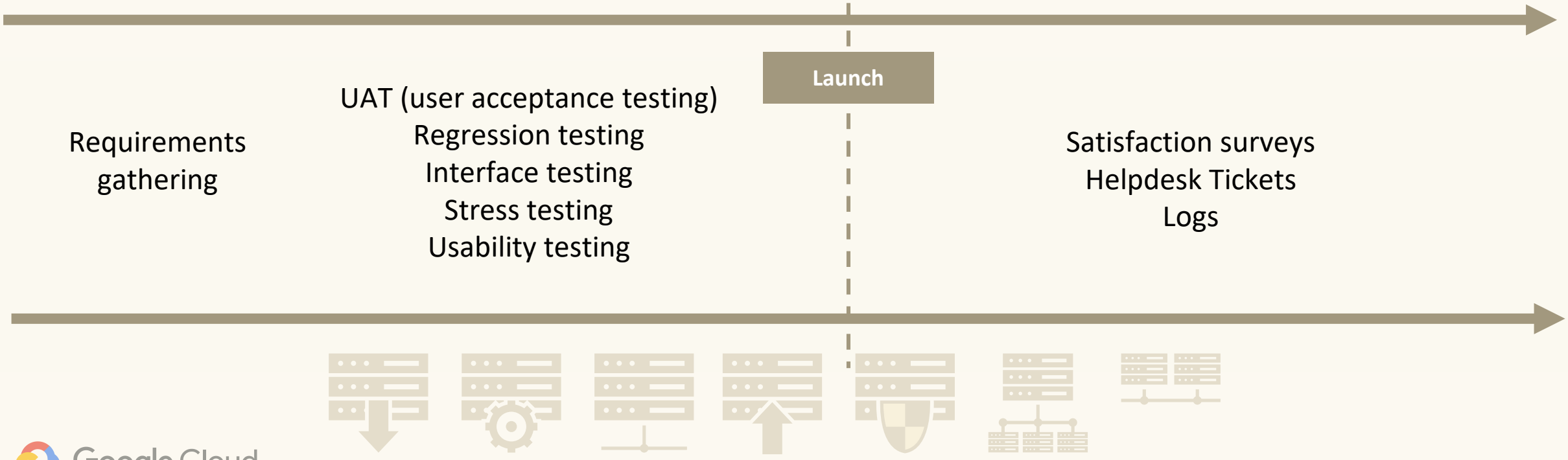
Deployment Environment

On-premise | Corporate desktop-based | VPN only access | Employee-only access

Old World

Deployment Environment

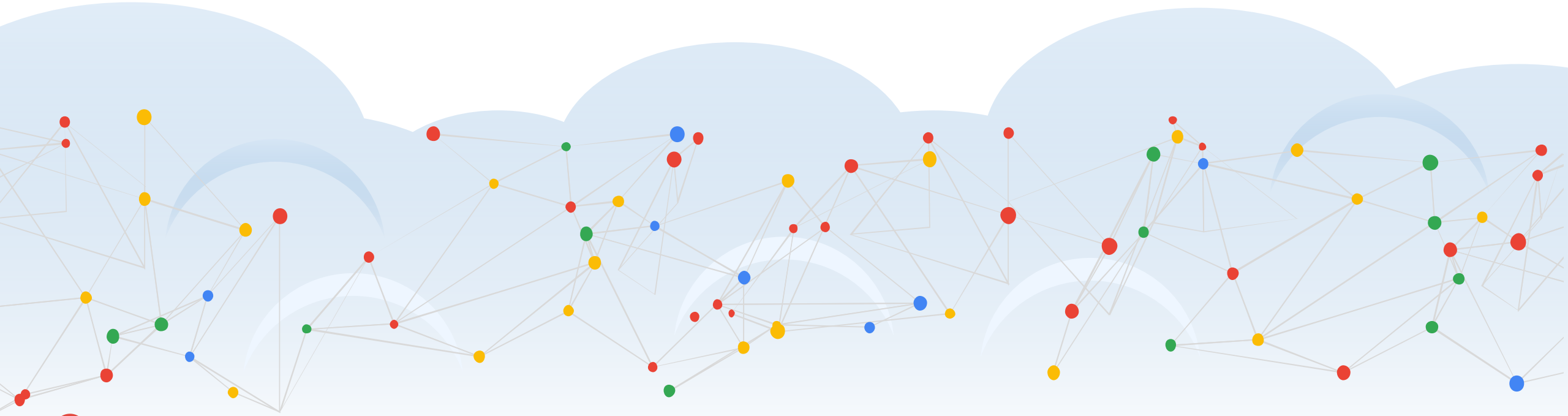
On-premise | Corporate desktop-based | VPN only access | Employee-only access



New World

Deployment Environment

Cloud first | Anytime, Anywhere access | Many apps & devices



Technology is just one dimension.

The other is people.

Their behaviors, preferences, & goals in response to technology.

IAM Policy

Mandated by CEO, regulators, security, compliance, etc.

IT team

Business Outcome

Desired gains & behavior as a result of the policy.

IAM Policy

Mandated by CEO, regulators, security, compliance, etc.

IT team

Business Outcome

Human Behaviors, Goals, Preferences Have Impact

IAM Policy

Mandated by CEO, regulators, security, compliance, etc.

IT team

Unintended Business Outcome

IAM Policy

Mandated by CEO, regulators, security, compliance, etc.

IT team


Human-centered research
starts here.


Who are the users?
What's the context?
What are their behaviors, mental models, & goals?

IAM Success Factors Heard at Gartner IAM Summit

Recognizing data quality challenges from the beginning, enabling painless migration, understanding how the business works, and **putting employees in control** are core zero-trust principles.

~Large Tech Company

Experience should be **user-centric** rather than IT-centric.

~Large Health Insurance Company

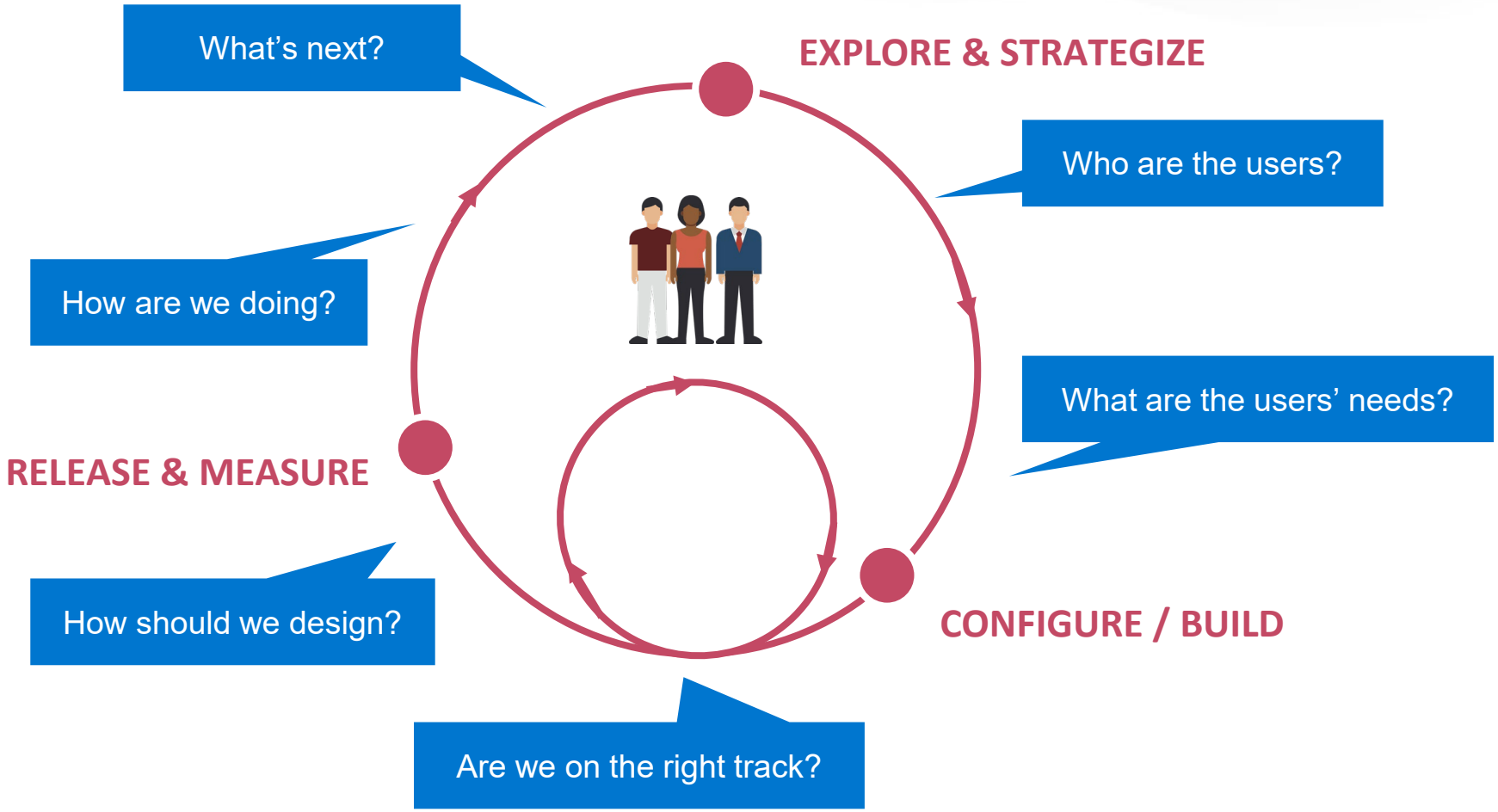
Hyperfocus on **usability**, both external & internal.

~Large Coffee Company

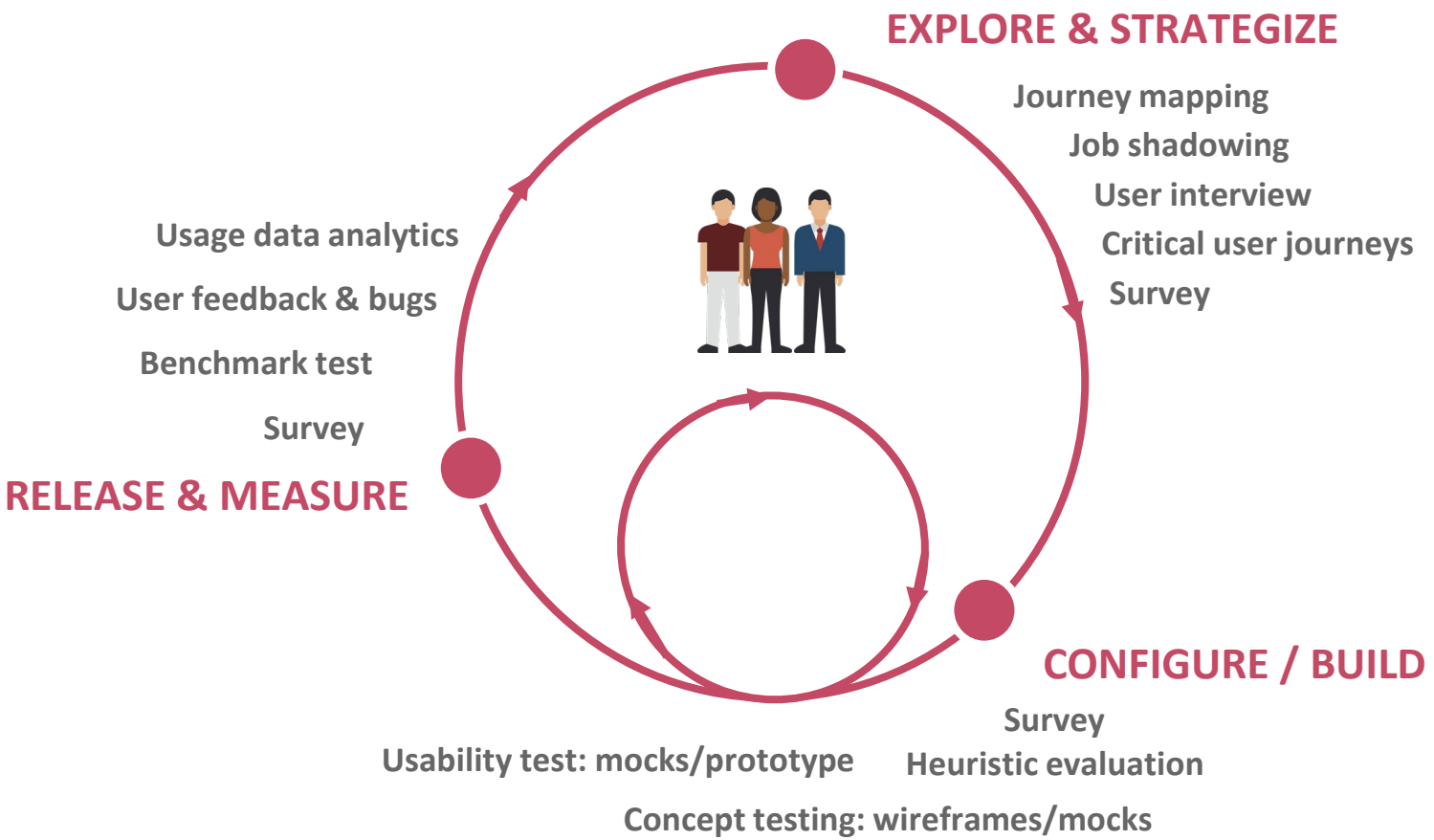
We can't control the interface but can control the **metadata, what they review, what's on the screen**.

~Large Home Improvement Retail Company

This is Human-Centered Research



Fitting Human-Centered Research into Development



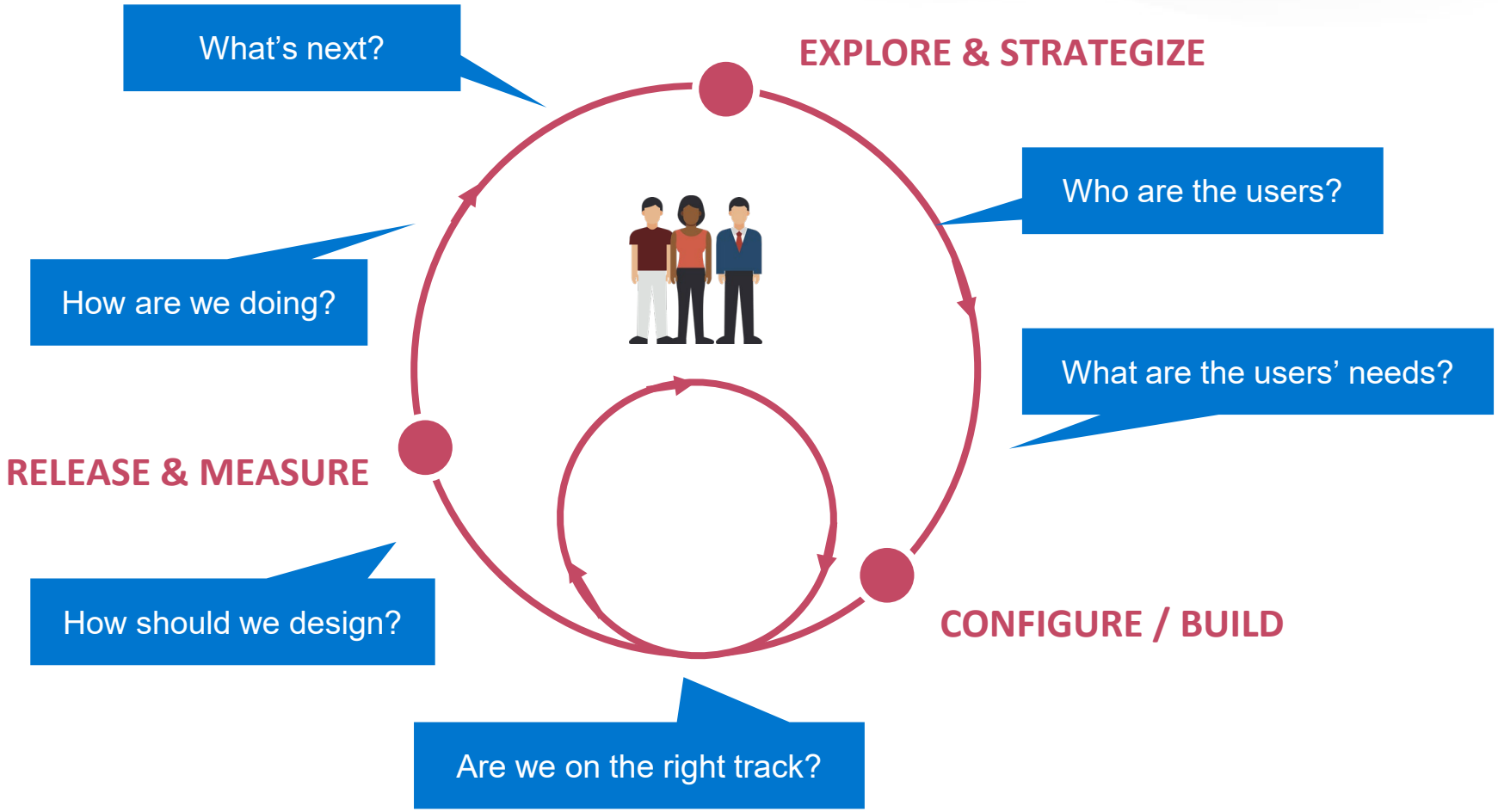
RSAConference2020

2 | Case Study - Security Center

The importance of exploratory research

Google Team: Tony Mallier (Lead researcher), Zach Mesa, Chad Tyler, Don Kalar

Fitting Human-Centered Research into Development

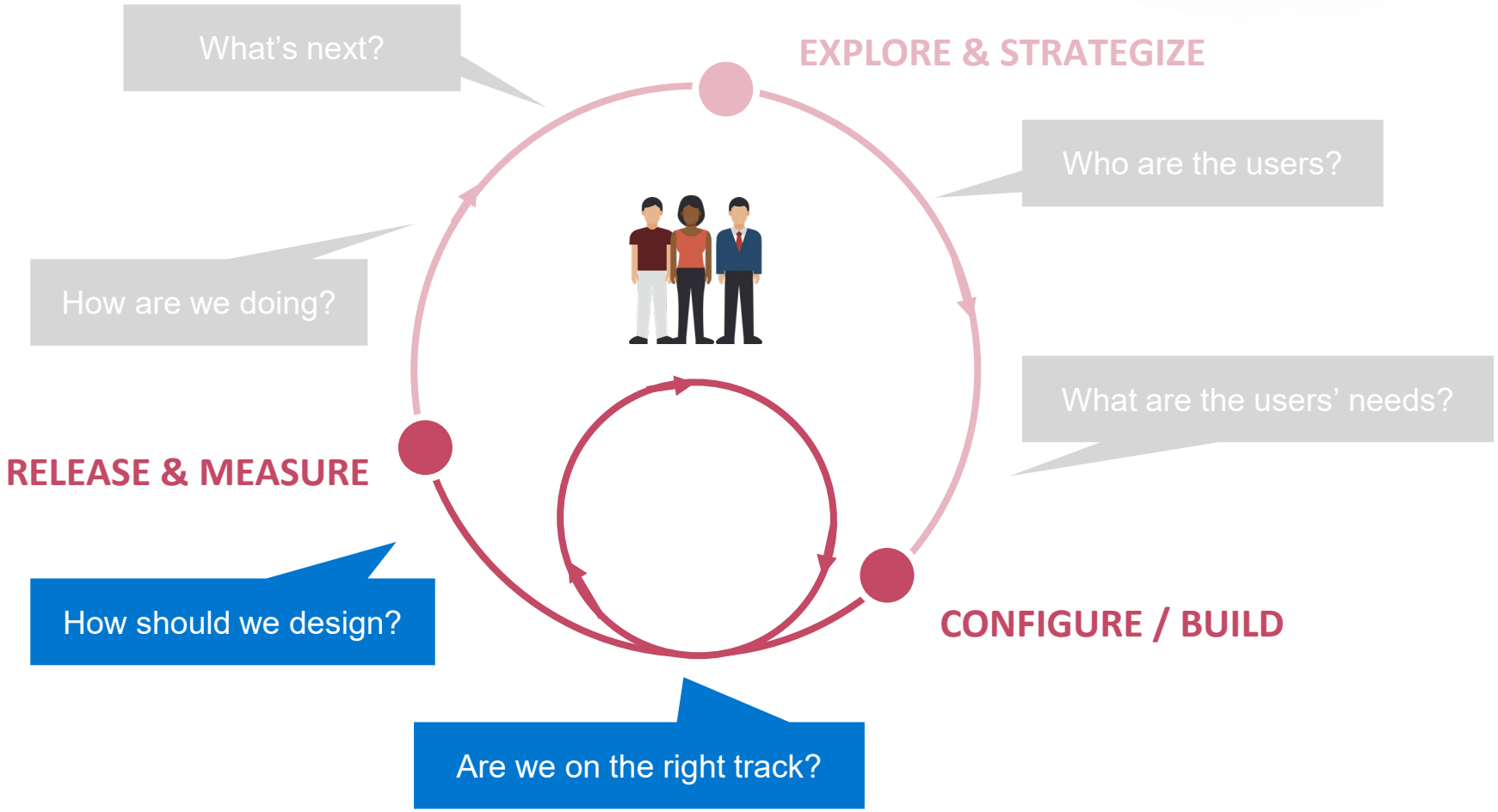


Challenge

Users needed help managing security in G Suite.

The team developed a dashboard concept, but user validation was required.

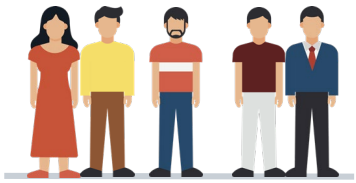
Fitting Human-Centered Research into Development



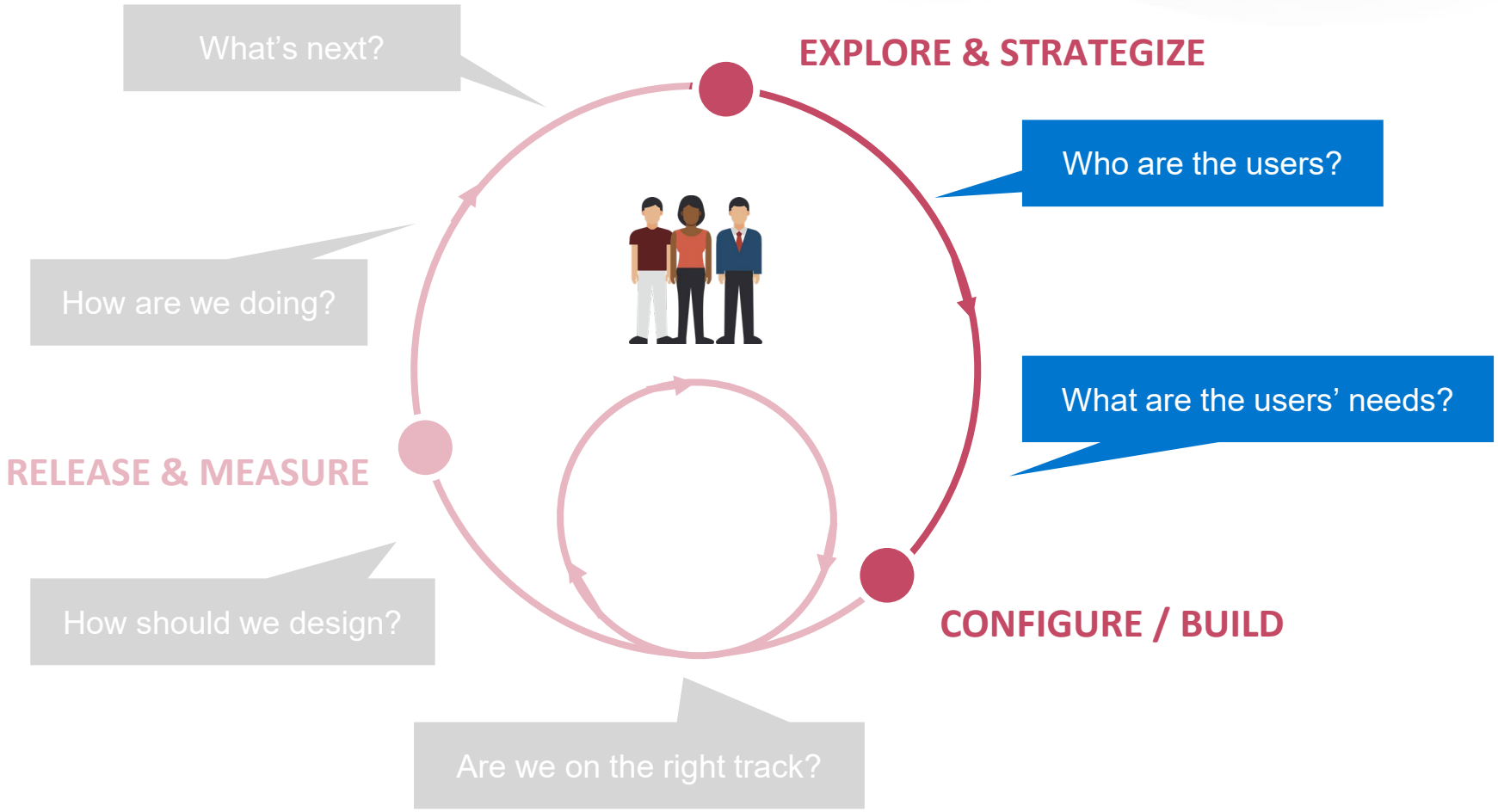
Challenge

Dashboards did not really help users manage their security.

"I don't think this is actionable, to me it seems like this is a lot of information... I have 97,000 unauthorised unauthenticated messages … **What would I do with that**?"



Fitting Human-Centered Research into Development



Research Method: Journey Mapping

Journey Focus

If someone within a company gets a phishing email, how can a security admin get rid of it?

The Journey Before

DISCOVER

1

End user sends admin an email that she suspects is phishing.

TRIAGE

2

Admin searches in cPanel > Reports > Email log search to find other recipients.

3

Admin uses Vault to search for emails with similar content or subject lines.

4

Admin exports the results from Vault.

5

Admin uses Vault metadata to find affected users and messages

RESOLVE

6

Admin changes passwords of affected users as a precaution.

7

Admin uses GAM to remove phishing emails from users' inboxes.

TRIAGE

8

Admin searches in cPanel > Reports > Login activity to find potential phished users.

9

Admin creates a list of potentially compromised accounts.

10

Admin searches in cPanel audit logs to look for suspicious user activity for affected users.

11

Admin searches in Vault for emails that may have been sent by affected users.

RESOLVE

12

Admin uses GAM to remove phishing emails from affected users

13

Admin changes affected users passwords as a precaution.

PREVENT & REPORT

14

Admin removes the IP from the whitelist.

15

Admin contacts affected parties: managers, users, vendor.

16

Enforce 2-factor authentication for phished users and high-value users.

17

Create and execute user education about phishing attacks.

18

Create content compliance rules in Gmail settings to catch similar messages.

19

Admin changes affected users passwords as a precaution.

The Journey After

1. DISCOVER

Admin receives an alert when an end user marks a message as phishing in her inbox. The alert contains an action button to “Investigate Alert”. All messages with the same message ID are quarantined automatically.

2. TRIAGE

The alert action takes the user to a powerful investigation tool that populates a filter that renders the alert event with detailed context. The context should help the admin identify groups of affected users and objects (files, messages, etc…)

3. RESOLVE

Admin uses the same investigation tool to commit bulk actions on groups of users and objects (files, messages, users). Actions could include ACL changes for files, suspending users, deleting / quarantine emails.

4. PREVENT & REPORT

Admin creates a report for stakeholders with information from the Security Center.

Admin works through additional items in the Security Health Checkup page to mitigate future risk.

Outcome

- **Drastically reduced resolution time for users**
  - Exploratory research uncovered core journeys & challenges

> "The ability to remove [a phishing email] immediately saves us HOURS."

- **Developed a more comprehensive solution**
  - Exploratory research led to G Suite Security Center (Security Investigation Tool, Security Health & Alert Center) instead of just a dashboard

Outcome

- **Increased collaboration**
  - The co-design process made users feel like a part of the design process

> "It's pretty crazy that your roadmap is directly in line with the feedback."

- **Better alignment**
  - Internally, PMs, designers, and Eng were on the same page

> "Diversity of thought will lead to a more refined outcome."

Explore and Strategize: things to keep in mind

- **Who should you talk to?**
  - Try to keep your sample representative
- **What kind of feedback are you looking for?**
  - Decide what to focus on based on technical constraints but be open to the possibilities uncovered during research
- **When should you do it?**
  - Exploratory research should be conducted as early as possible to inform product design

Explore & Strategize is relevant to IT practitioners

- **Identify people** that may be affected by policy / system changes (identifying segments)
- **Observe or journey map** their work process
- **Simplify and/or automate** with configuration & data decisions

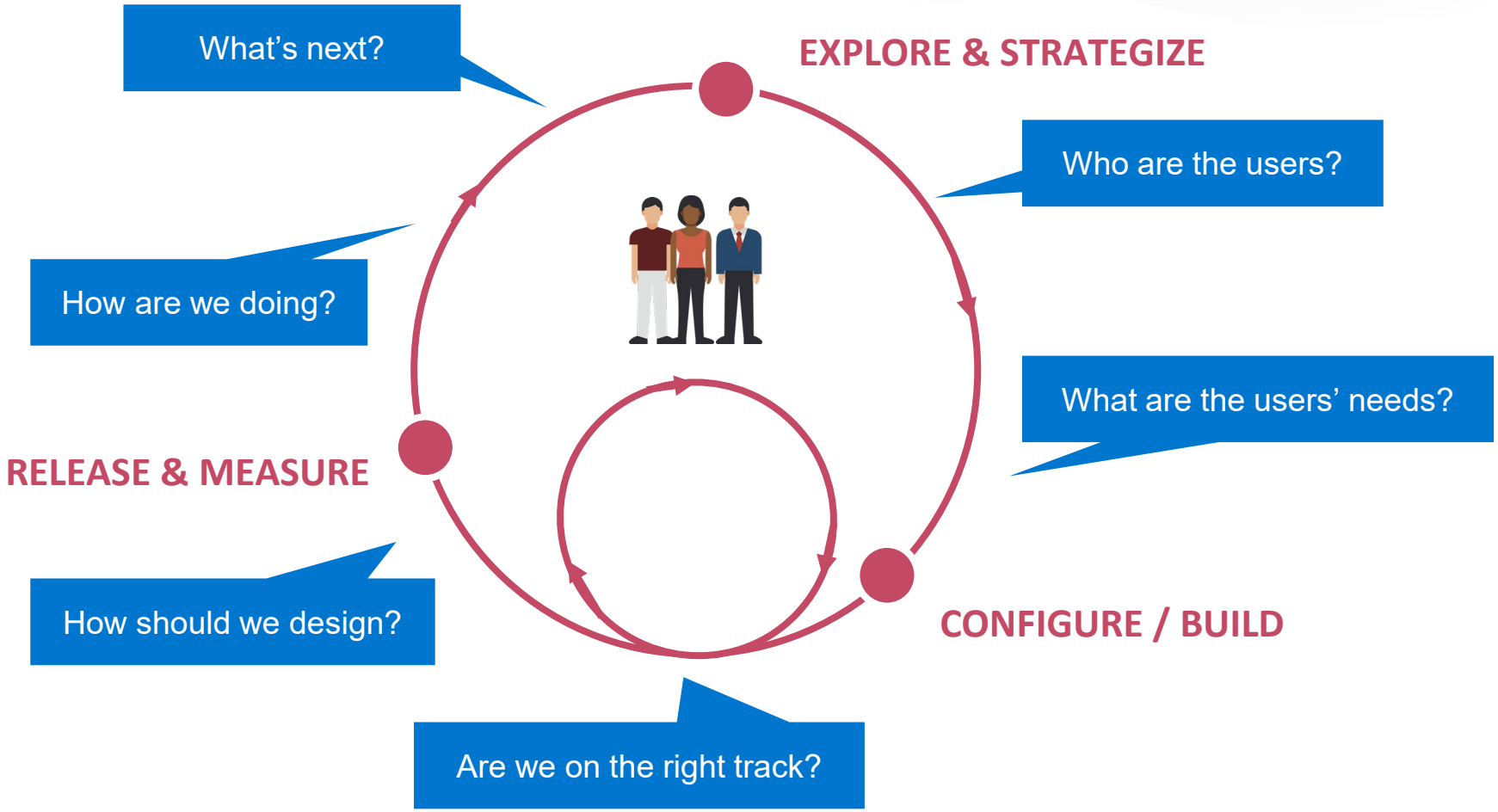
RSAConference2020

3 | Case Study - Alert Center

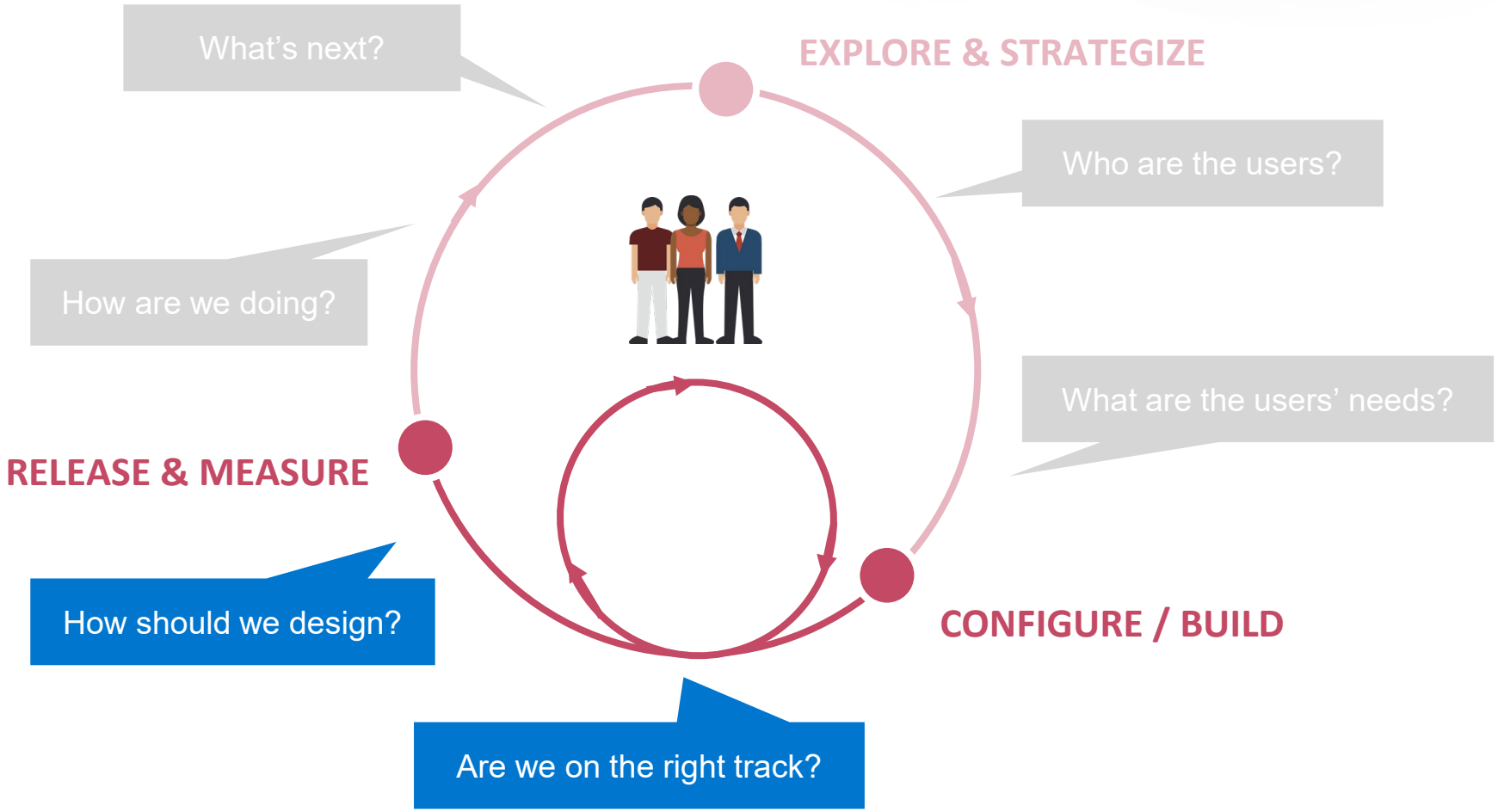
The importance of iterative research

Google Team: Noelle Easterday (Lead Researcher), Jessica Staddon, Alicia Korn, Darshan Patel

Fitting Human-Centered Research into Development



Fitting Human-Centered Research into Development

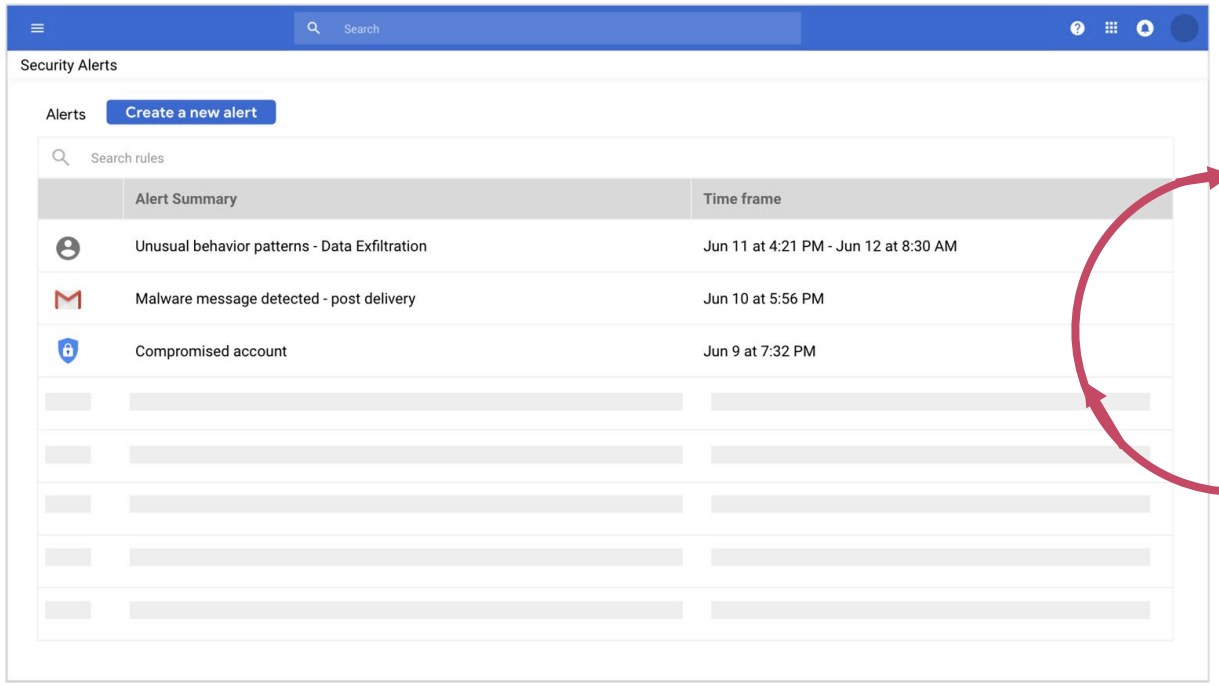


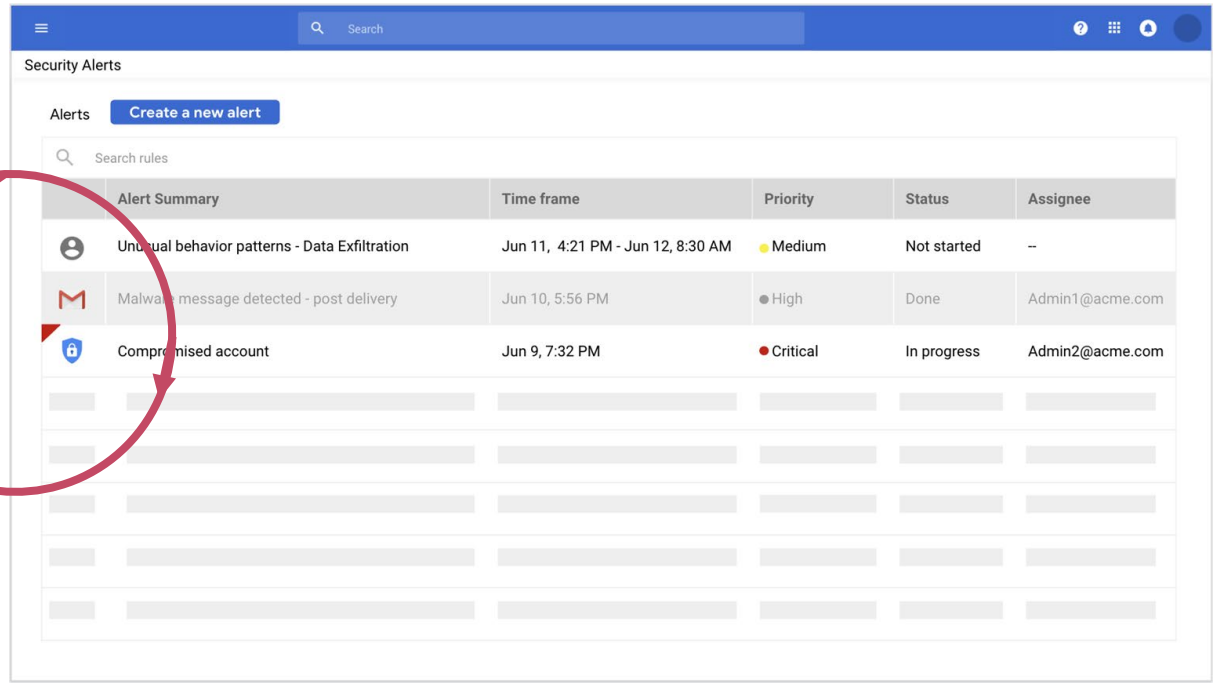
Challenges

- **IT and Info Sec teams get LOTS of alerts**
- **How can we design a list page that helps them manage this volume?**
- **What is the minimum information needed?**

"I have 2,300 sitting in my spam folder right now...We have a lot of false positives."
IT Manager, Manufacturing company (3,000+ employees)

Test initial designs and iterate!





Planning Iterative Research Questions

Start with open ended questions…

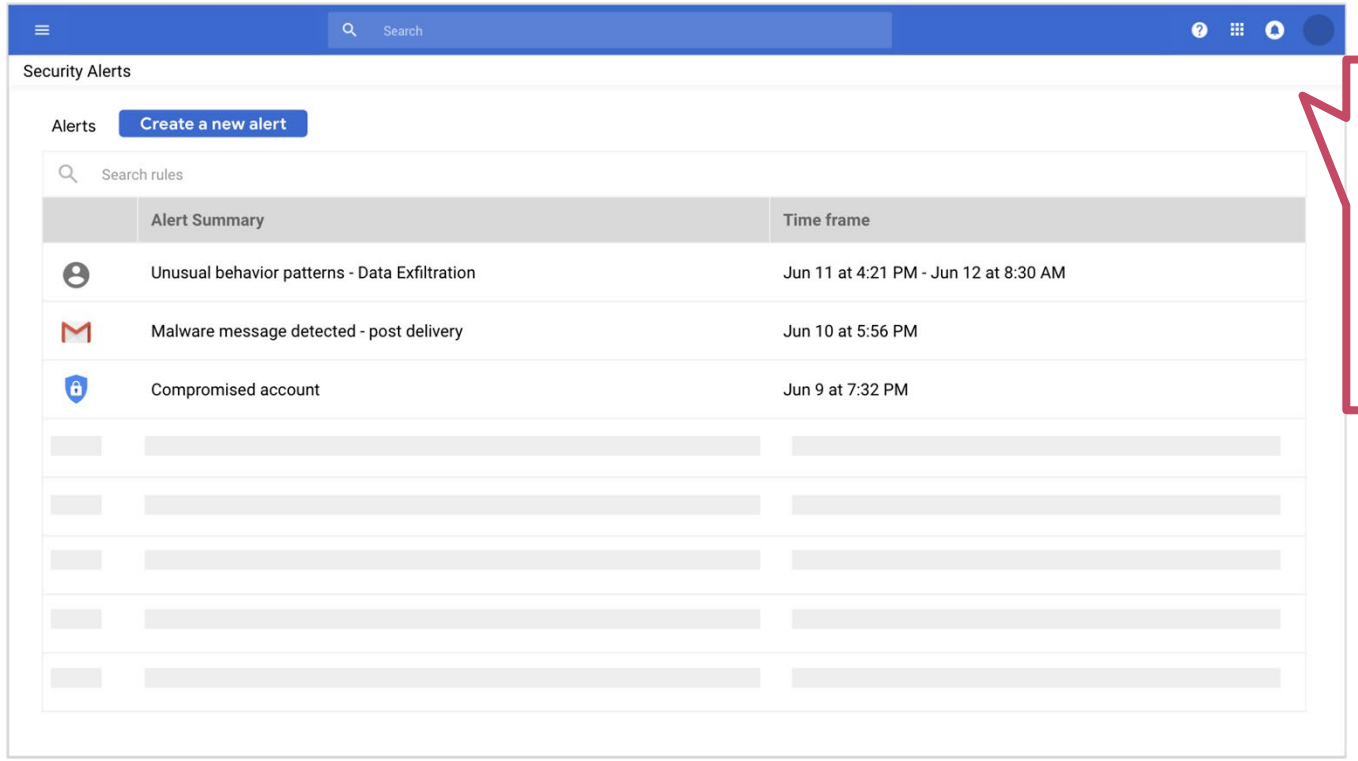
- What do you think?
- Talk me through what you see here.
- What are your thoughts?

Open ended follow-ups…

- Why?
- What does that mean to you?
- What would you want to do next?

Be selective with targeted questions as they can introduce bias into your feedback...

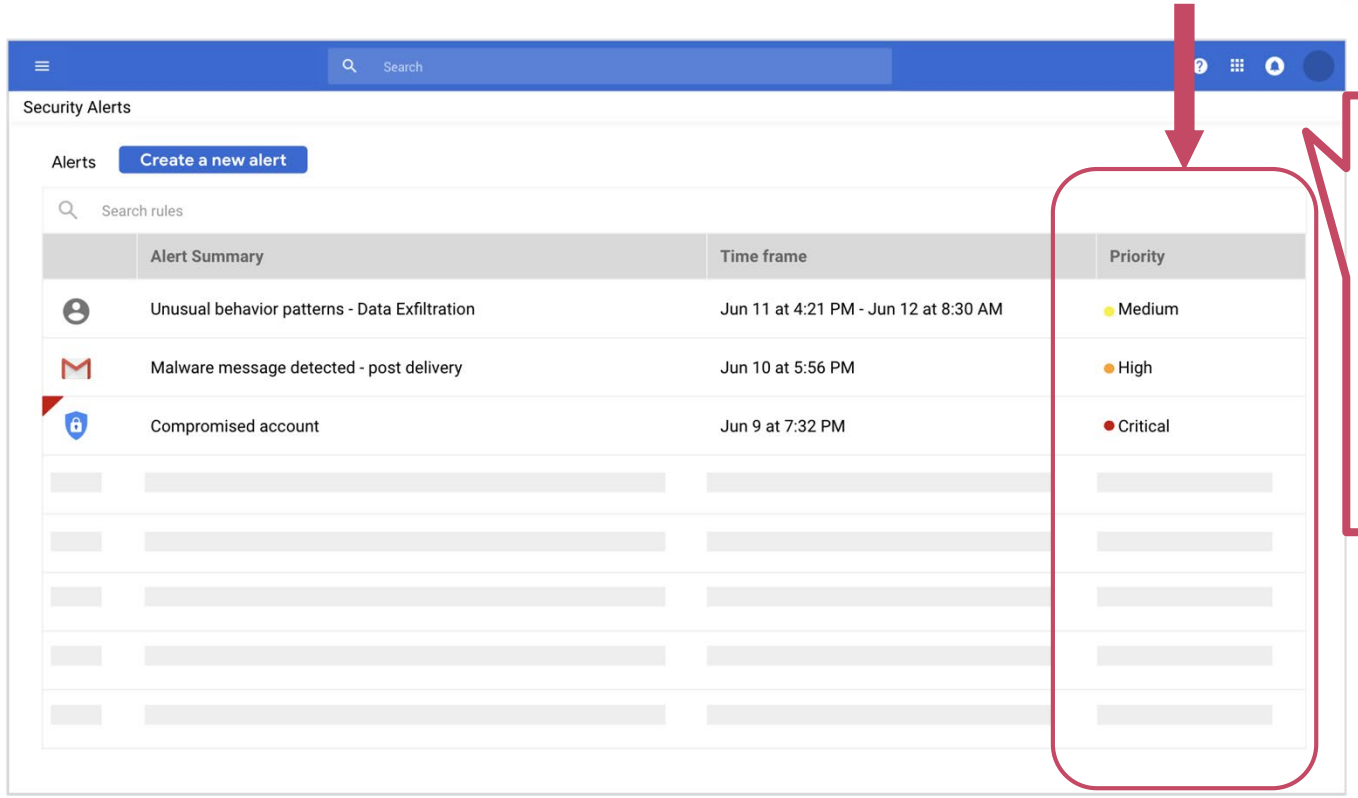
Findings: Help me know where to start



User feedback

This list isn't very helpful because they can't easily triage which alerts pose the highest risk and should be addressed first

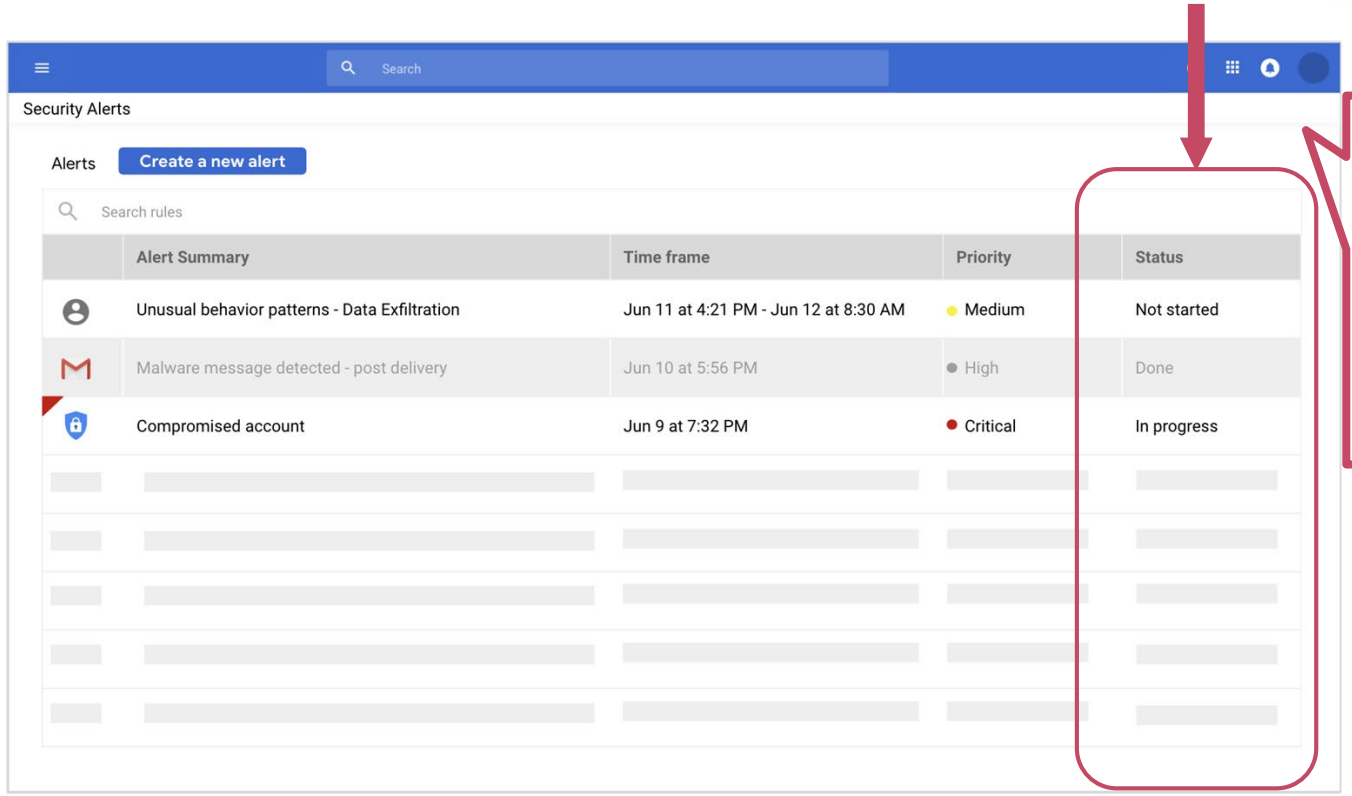
Findings: Is it already being worked on?



User feedback

This helps users know what to address first… But they also need to know if another analyst is already working on it so they don't duplicate efforts

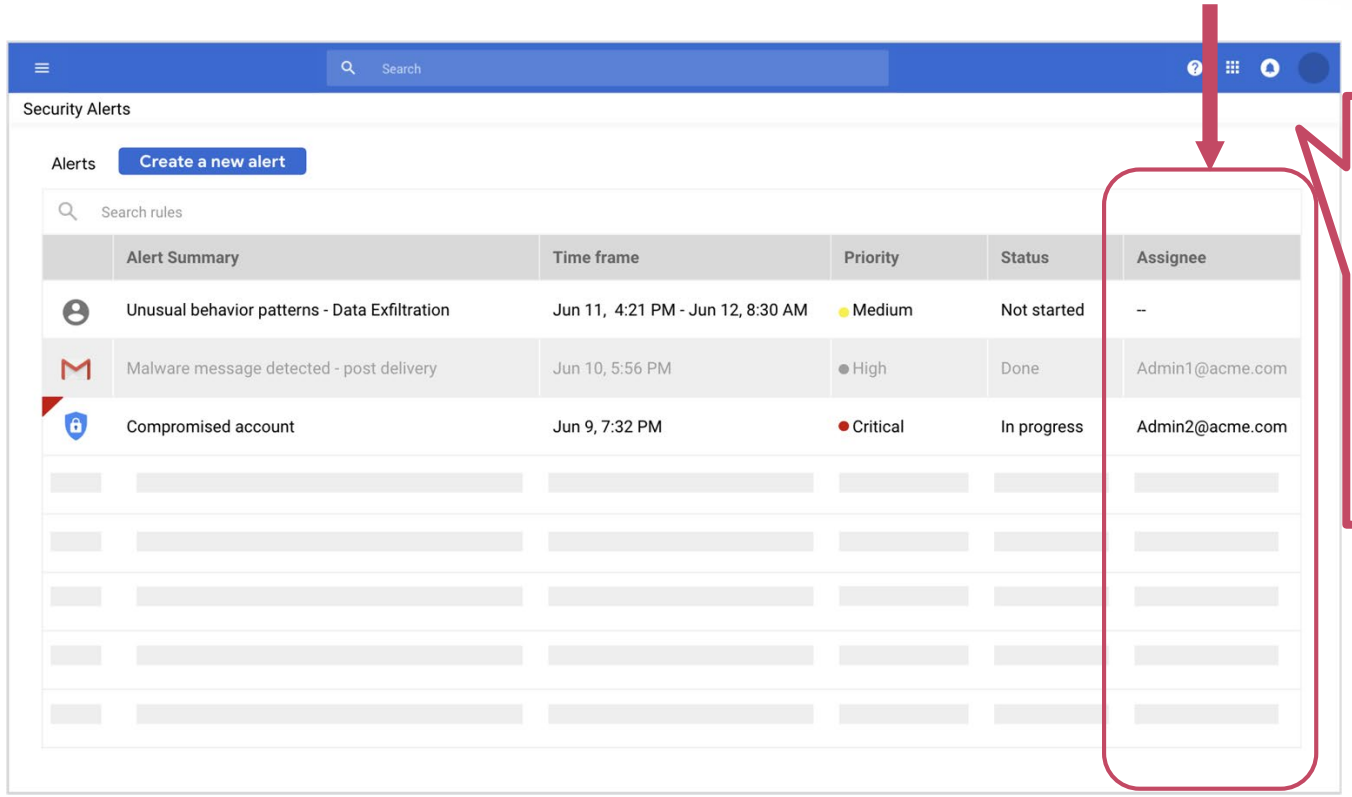
Findings: Who's responsible for it?



User feedback

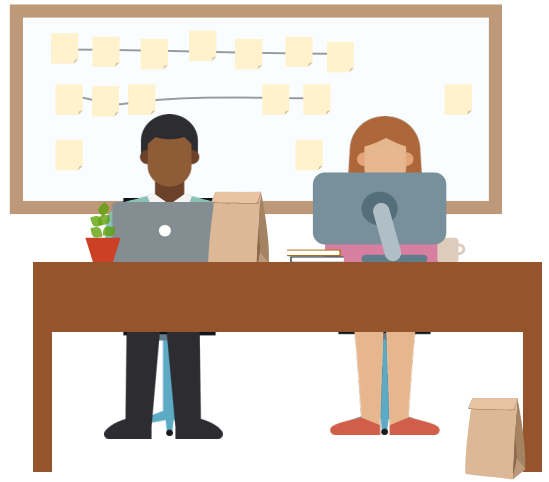
Knowing the status is helpful, but they also need to know who is working on it. That tells them who is responsible for closing it out.

Findings: Let me customize priority

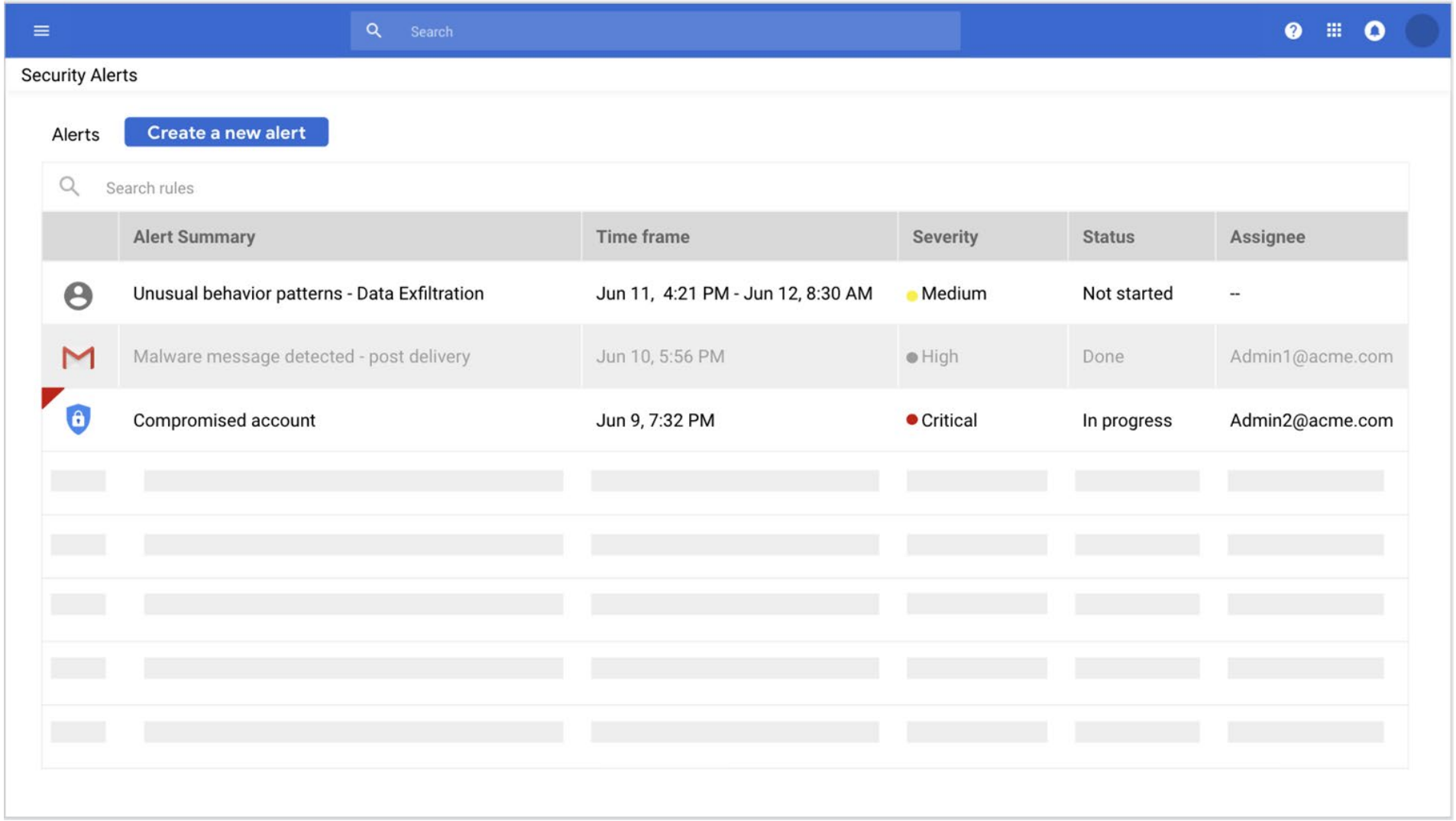


User feedback

It's helpful to give a first pass at ranking alerts, but they are ultimately the owners of their data and need to be able to determine which alerts to prioritize



Final Outcome



Outcome

- **Designs help users accomplish goals more easily**
- **Re-usable guiding principles**
  - Informed high-level design principles
  - Inspired a large-scale survey and paper published in IEEE conference on privacy & security

Configure and Build: things to keep in mind

- **Who should you talk to?**
  - Keep your sample representative
  - Do they need to have specialized knowledge? Or, should your tools work for everyone?
- **What kind of feedback are you looking for?**
  - High level concept and workflow → less polished, wireframes
  - Detailed design feedback → polished or even click-thru mocks
- **Knowing when you're done**
  - Define success metrics early
  - Can be subjective and is sometimes guided by product team constraints

IT practitioners need to be user-centric too

"We have to think like an end user and not like an IT person. Sometimes I'll ask our end users how something is done. If I've got other trusted colleagues I'll get them to test things out."
VP IT, Marketing & Advertising company (1,000+ employees)

"My boss always says we're bad testers. -- there's a lot of unknowns - we probably need to do a better job of coming to a business user when we need to test."
Sr IT Manager, Consumer Goods company (30,000+ employees)

RSAConference2020

4 | **Apply**

Getting Started with Research

- **Immediately** | Start building the case
  - Identify deployment failures
  - Assess cost of not doing research
- **3 months** | Identify resources
  - Can you borrow, contract, or hire?
  - Is a team member interested in learning?
- **9-12 months** | Identify pilot & execute
  - Identify impact & metrics
  - Consider the stage, the questions, & resources

Resources

Externally Published IEEE Paper

"It's a generally exhausting field: A large scale study of security incident management workflows and pain points"

Learning about research

Usability.gov

RSAConference2020

5 | Q & A