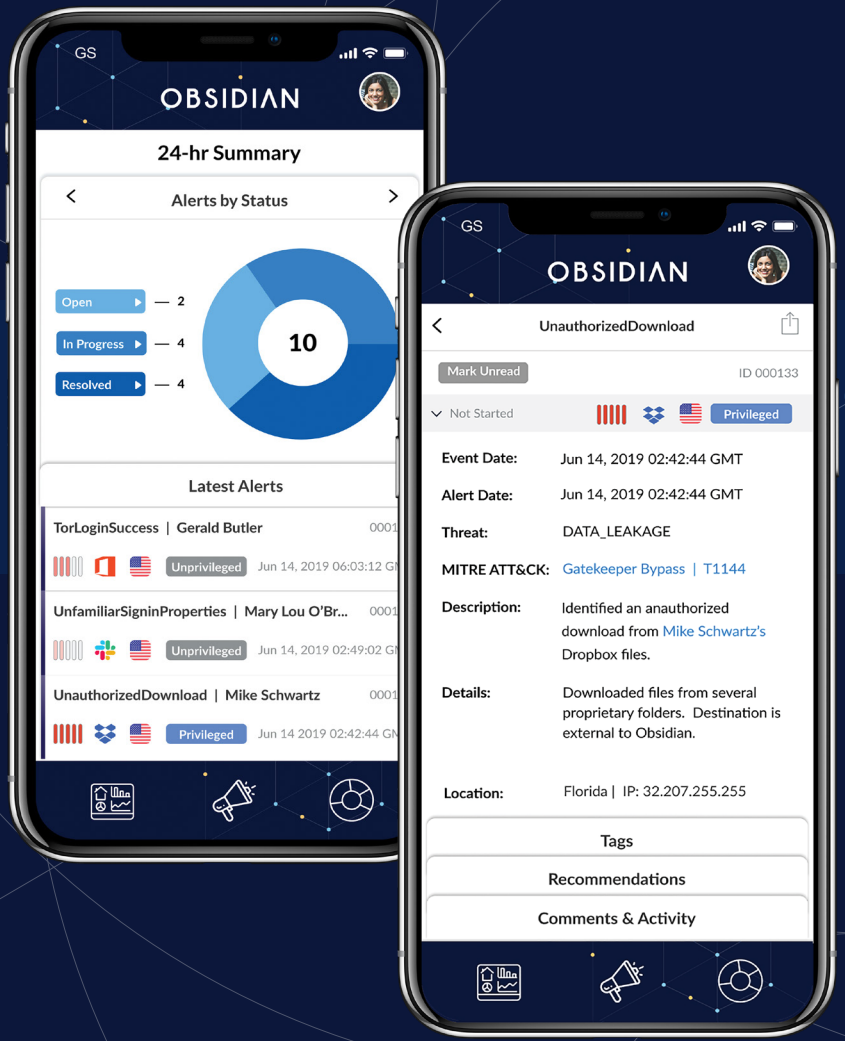
CASE STUDY

Christine Benedict, Cassandra Hoo, & Gregory Puett



Security Never Sleeps

Alert Monitoring - 24/7

OBSIDIAN

Dedicated to all the loved ones that put up with our crazy for a year.

TABLE OF CONTENTS

OVERVIEW

OBSIDIAN

MEET THE TEAM

Obsidian Security

Sean Borman
Product Manager

Alfonzo Martinez
UX Designer

Team Obsidian Bleu

Christine Benedict
Product Manager

Cassandra Hoo
UX Designer

Gregory Puett
Researcher

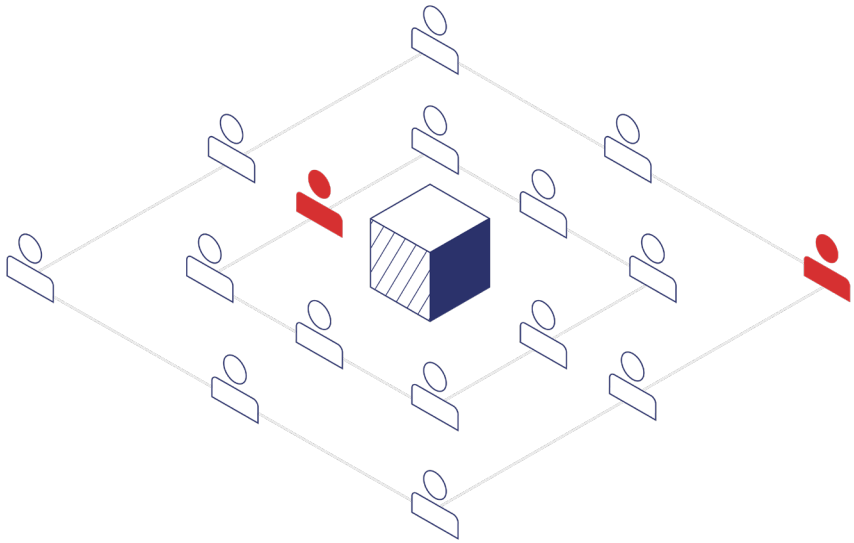
Mark Baldwin
Mentor

EXECUTIVE SUMMARY

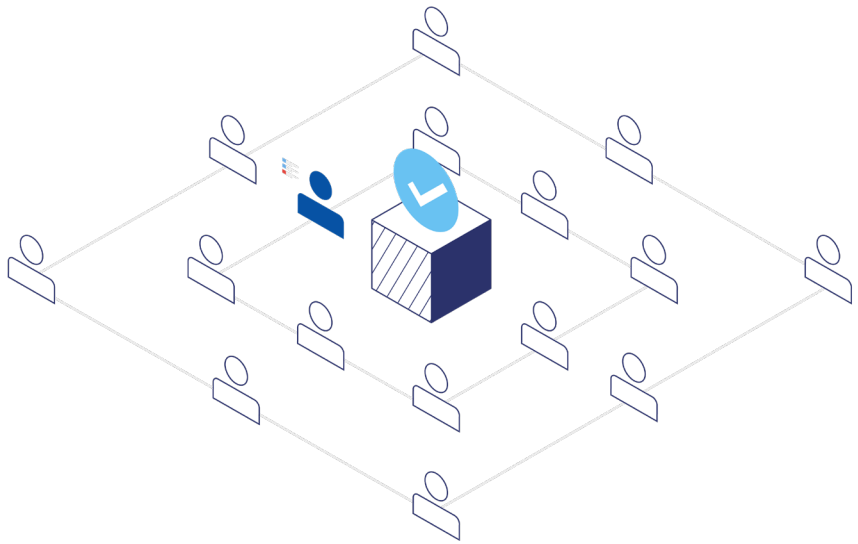
The Platform

Many companies are now using cloud-based services (i.e. G Suite, Dropbox, Salesforce, etc.) and storing information outside the traditional firewall structure. Because of this shift, hackers have found a new way to infiltrate and steal information undetected. They are now increasing attacks on users of cloud-based systems rather than directly attacking the systems themselves... by simply logging in.

Powered by machine learning, Obsidian Security's platform provides tools to identify potential security compromises based on abnormal user activity.



Unprotected System



System Protected by Obsidian

EXECUTIVE SUMMARY

The Need

Security is a 24/7 job.

Obsidian tasked our team to create a native mobile app that can alert their users of potential security threats. The users will be able to take appropriate action anytime and anywhere.

The Process

Research & Discovery: Our team conducted interviews with stakeholders and potential users to understand the cybersecurity space. This included their needs and work processes.

Product Requirements Document: Our Product Manager created a list of design and development specifications based on what we learned from our research & discovery phase.

Design and User Testing: We went through two phases of design and user testing. For the first phase, we designed a clickable, mid-fidelity, grayscale prototype. After analyzing the results and feedback from our user testing, we created a clickable high-fidelity prototype. After testing this prototype, we produced a list of recommendations and next steps for Obsidian Security.

WHAT IS CYBERSECURITY?

Intro - Security Never Sleeps

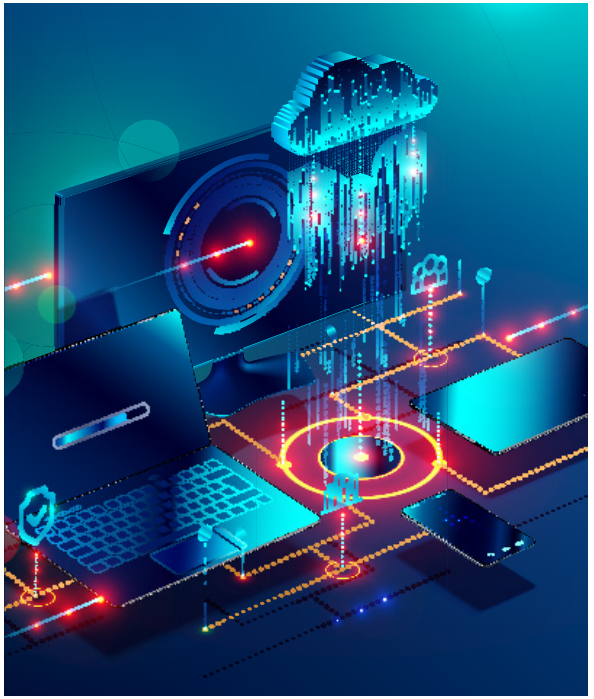
Data breaches for small and enterprise companies can cause huge losses, both financially and reputation-wise. Juniper Research's forecast suggests that the global annual cost of data breaches will be over $2.1 trillion by 2019. This is due to rapid digitization of consumer lives and enterprise records.[1] Obsidian Security's platform protects more than just identity and access. It provides analysts with critical forensic tools to isolate who and what was compromised in the event of a security breach. This increases the efficacy of damage control and provides a company with prompt, pertinent information so that they can pursue immediate remedial action.

In this day and age, cybersecurity professionals need to be accessible 24/7 in order to navigate potentially disastrous scenarios. Based on this notion, Obsidian Security has hypothesized a solution to compliment their current product -- an accompanying mobile application, which provides notifications/alerts for security professionals, even when they're not at their computers.

Obsidian requested our team to research and test this hypothesis. We then designed a clickable, high-fidelity prototype based on our results.

1 Cheng, Long, et al. "Enterprise Data Breach: Causes, Challenges, Prevention, and Future Directions: Enterprise Data Breach." Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, vol. 7, no. 5, Sept. 2017, p. e1211. Crossref, doi:10.1002/widm.1211.

WHAT IS CYBERSECURITY?



Cybersecurity can be abstract, almost so invisible that it's hard to define. Our group's first challenge was to understanding this topic as a whole. Specifically, what does Obsidian focus on?

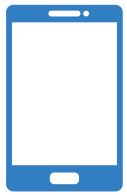
At its core, security professionals deal with the protection of computer systems -- hardware, software, and electronic data -- from all incidents including theft, negligence, and damage.

These trained specialists are the first line of digital defense for companies and their employees.

WHAT IS CYBERSECURITY?

Cybersecurity Professionals Protect:

Company owned hardware (i.e. servers, databases, computers)



Personal employee hardware (i.e. laptops, tablets, phones)

The employees themselves

Hackers don’t break in. They login.

- Chief Information Security Officer, Cisco

WHAT IS CYBERSECURITY?

Breaking and Entering in Plain Sight

Imagine you're a security guard at a major corporation. And you're at the main entrance.

It's your job to make sure that every employee swipes in correctly with their unique identification. But what if there's an impostor in a convincing professional disguise? And they're using a stolen ID.

Would you know? Be honest.

Compromising an employee's identity is one of the easiest ways for a hacker gain access to cloud-based services utilized by a company. Once they have this employee's credentials, hackers can login as a legitimate user, blending in seamlessly with other users of the system. In order to combat this, security professionals need to track every employee's unique digital habits, movements, and privileges, then flag anything that seems suspicious and out of character.

If they find an impostor, the account is shut down, and user privileges are suspended until the issue at hand is resolved.

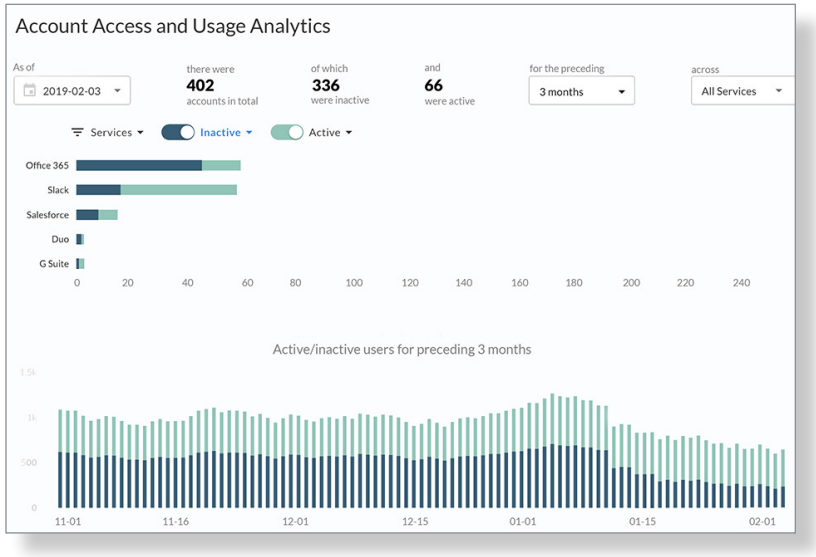
WHAT IS CYBERSECURITY?

Obsidian Security's Solution to Protecting the Cloud

Obsidian's cybersecurity platform protects its customers by flagging abnormal employee activity within cloud-based services used by their company. This innovative technology logs and tracks every user's movements on a granular level. If any activity seems out of character for a specific user, Obsidian creates an alert. These alerts give security professionals immediate notification on potential attacks and provide detailed data (i.e. the severity level, the time the event occurred, the affected user, the location, etc.) to give a full picture of the situation. This allows analysts to know exactly who and what was compromised, in addition to any sensitive information accessed.

What makes Obsidian Security unique is its ability to visualize security data in a detailed yet easy to understand way. Obsidian has created a full suite of intricate maps, tables, and charts to help professionals assess the health and safety of an organization in real time. This includes monitoring trends and abnormalities within given time frames.

The platform is also highly customizable. Security professionals can easily modify their settings to view and organize data in a way that works for their needs. Obsidian's alerting system also provides professionals with recommended steps for resolving the issue so they can take action quickly.



www.obsidiansecurity.com/platform/

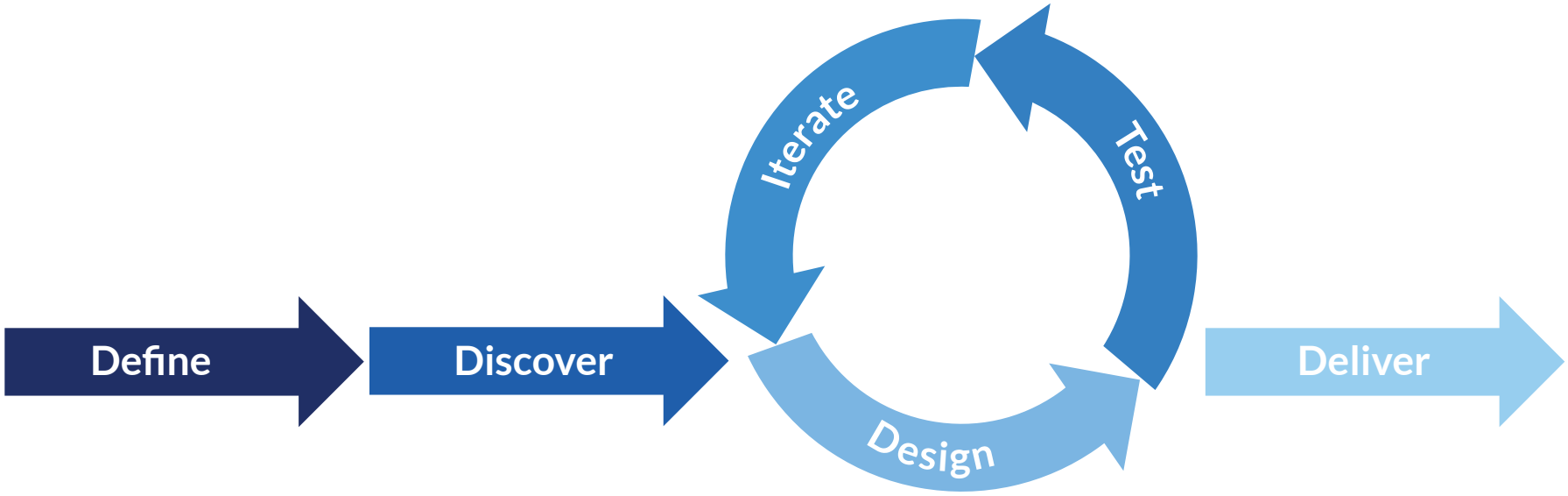
THE CHALLENGE

Do’s and Don’ts

Working alongside a security company came with its own challenges. Our team had to:

- Understand the complicated and clandestine world of cybersecurity.
- Be respectful of sensitive information.
- Read between the lines when we didn’t have access to proprietary data.
- Decide what information and features from Obsidian’s platform we wanted to carry into the mobile app, and what new features we were designing from the ground up.

PROCESS, TIMELINE & STRATEGY OVERVIEW



Over the course of our six-month project, our team engaged in several rounds of research, design, and user testing. Our final deliverables included a clickable high-fidelity prototype, a product requirements document, a research report, and recommendations for the next phase.

RESEARCH PARTICIPANTS

In the course of our project, we spoke with seven cybersecurity professionals. These professionals were either actual Obsidian Security customers, or Obsidian employees viewing our project from a customer standpoint.

Participant	Research Contribution	Role	Security Industry Experience
Customer 1	• Semi-Structured Interview • Phase I User Testing	• Security Engineer, CSO • Advisor for Obsidian	20 years
Customer 2	• Semi-Structured Interview • Phase I User Testing	• Security Engineer, Research • Researcher for Obsidian	8 years
Customer 3	• Semi-Structured Interview • Phase I User Testing • Phase II User Testing	• Security Engineer, SOC • Researcher for Obsidian	12 years
Customer 4	• Semi-Structured Interview • Phase I User Testing • Phase II User Testing	• Professional Services	19 years
Customer 5	• Semi-Structured Interview • Phase I User Testing • Phase II User Testing	• Head of Security	16 years
Customer 6	• Phase I User Testing	• Senior Security Researcher at Obsidian Security	7 years
Customer 7	• Phase I User Testing • Phase II User Testing	• Senior Director of Technology	10 years

PHASE I

Research & Discovery

OBSIDIAN

My procedure is:
show up to work,
check some emails,
get shit done.

- Customer #5

PHASE I - RESEARCH & DISCOVERY

Goals

- Familiarize ourselves with the cybersecurity industry.
- Explore the lives of cybersecurity professionals, both in and out of the workplace. This includes daily processes, job challenges, and likes/dislikes.
- Uncover the unique needs of various security professionals.
- Conclude what mobile app features would make the job easier for our target demographic.

Testing Methods

1. Semi-structured Interviews

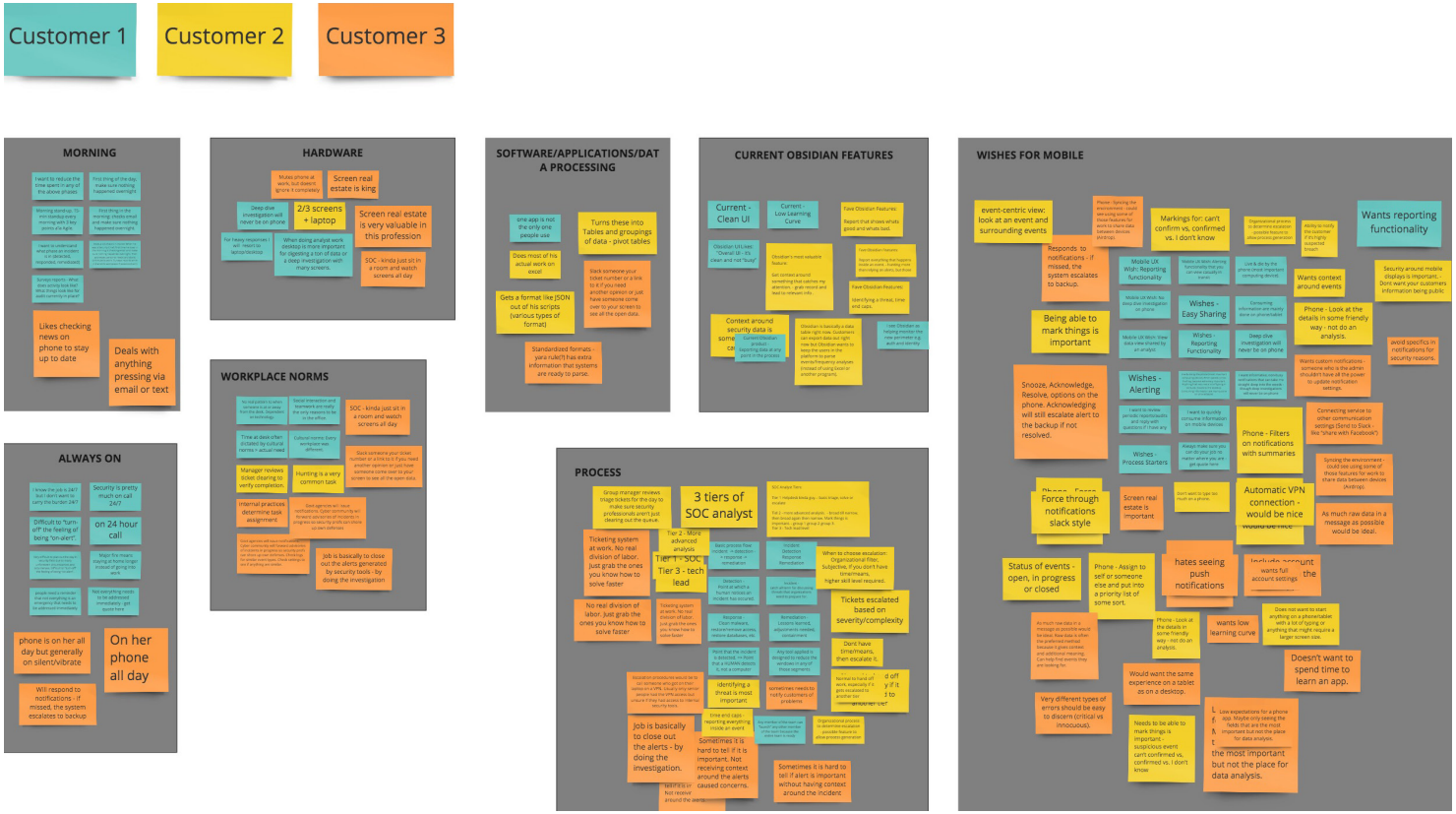
- Interviewed Customers 1, 2, 3, 4, and 5.
- Asked each participant the same base set of questions, over a 1-hour period.
- Interviews were flexible and allowed for unique follow-up questions.

2. Unstructured Interviews

- Held individual hour long interviews relating to the cybersecurity industry with two professionals from our personal places of work.

PHASE I - RESEARCH & DISCOVERY

Affinity Diagram & Data Analysis



Since our team members all worked remotely, we aggregated our data using the collaboration software Miro. For each semi-structured interview, each team member created their own sticky notes, containing key findings. We then organized these notes collectively, based on theme and similarity. Due to interview timing, our last two participants (Customers 4 and 5), were not included in our affinity diagram. Their feedback was taken into account for our initial designs.

PHASE I - RESEARCH & DISCOVERY

Key Findings

After analyzing our data, we found eight key findings/patterns amongst our three participants:

Morning Processes: Every interviewee stated that one of the first things they do every morning is to check their phone for overnight alerts.

"Always On:" Security is a 24/7 job. Professionals need to be on call at all times, even when not at their desks. Their phones are always on them, so they can be ready to take action at a moment's notice.

Workplace Norms: Security professionals may have varied experiences in the workplace. Some arrive every morning in a suit, while others show up whenever in a hoodie. This doesn't change the fact that they are always on (see above).

How Work Gets Done (Physical Resources): Security professionals have to review different sources of data simultaneously. They prefer multiple monitors at their work stations. As Customer 3 aptly put it, "Screen real estate is king."

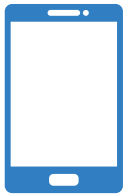
PHASE I - RESEARCH & DISCOVERY

Key Findings

How Work Gets Done (Software Resources): Professionals also depend on the simultaneous aid of multiple software applications for their workspace.

Analyst Tiers: There are three tiers for security analysts: Tier 1 (front line of defense, first to notice problems), Tier 2 (more advanced and detailed analysis), and Tier 3 (tech leads/managers).

Current Reasons for Using Obsidian Security: Obsidian's platform has a very clean UI that is visually oriented and easy to understand.



Obsidian Mobile App Wish List: Mobile alert notifications (push, text, call, etc.), alert overview listing page, alert details page, visualization of data for events and reporting, and the ability to filter information.

PHASE I - RESEARCH & DISCOVERY

Proto-Personas & User Flow Diagrams

Our team crafted three “proto-personas” based off data derived from our interviews.

We used these proto-personas to help us visualize and empathize with potential customers, so that we could design a mobile application that would best fit their needs.

Chief Security Officer

Pgs. 21-23

Manager

Pgs. 24-26

Security Analyst

Pgs. 27-29

PHASE I - RESEARCH & DISCOVERY

Chief Security Officer (CSO) Proto-Persona

"One of the reasons that people in this space burn out so quickly is because it truly never shuts off. I wake up with it, I go to sleep with it. There are constant emails and alerts coming in. It's hard to explain, but that's the life."

"When it comes to consuming information, my phone and my tablet are usually my best friend."

Security

Generating Reports

Triage

Analysis

Task Management

Company Management

Device Use

Cellphone

Tablet

Computer

Work Habits

Time at Desk/Computer

Not at Desk/Mobile

Characteristics

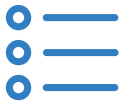
- Analytical
- Hard Worker
- Problem Solver
- Leader
- Driven
- Engaged

PHASE I - RESEARCH & DISCOVERY

Work Style

- Does analytical work at a computer and reviews info on many screens
- "Always on" and ready to tackle the day
- Uses mobile device on-the-go and tablets for meetings
- Often more responsive than strategic

Frequent Tasks



- Checks phone/email immediately in morning
- Surveys reports during commute to plan out day
- Attends project planning and governance meetings
- Reports analysis and research

Goals

- Stay up-to-date with the latest security trends and threats
- Stop problems before they happen
- Keep team on task and focused

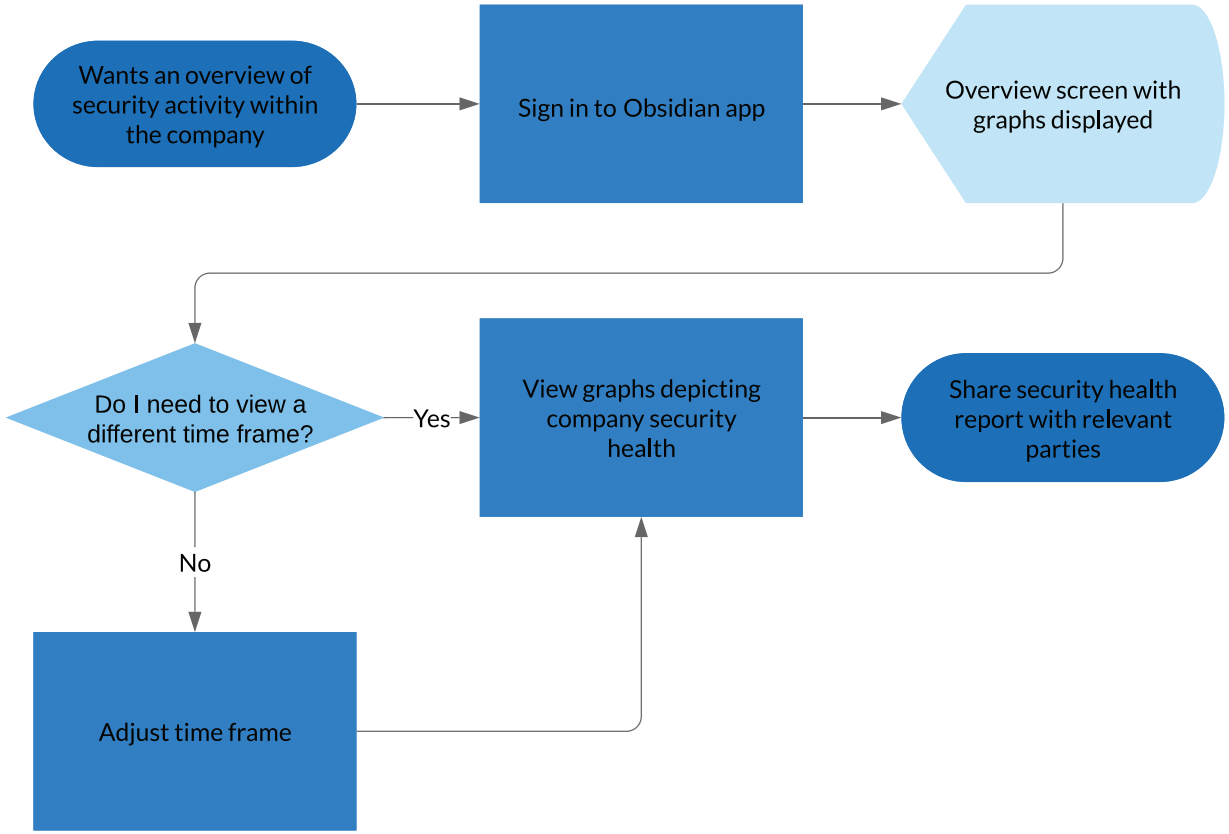
Frustrations

- Wishes there was more time in the day to focus on research and strategy
- Being "On" all the time is exhausting
- Too many push notifications can be distracting

PHASE I - RESEARCH & DISCOVERY

Chief Security Officer (CSO) User Flow Box Diagram

Figure - 1A



PHASE I - RESEARCH & DISCOVERY

Manager Proto-Persona

"Group managers review triage tickets for the day to make sure security professionals aren't just clearing out the queue."

"I'm less in the product and more about putting contextual pieces together. This can include talking to the customers who are having the problems, or understanding where or why attacks are occurring."

Security

Generating Reports

Triage

Analysis

Task Management

Company Management

Device Use

Cellphone

Tablet

Computer

Work Habits

Time at Desk/Computer

Not at Desk/Mobile

Characteristics

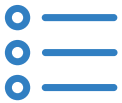
- Analytical
- Organized
- Resourceful
- Leader
- Delegator
- Strategic

PHASE I - RESEARCH & DISCOVERY

Work Style

- Interfaces with clients to keep them informed of security alert statuses
- Organizes team's on-call scheduling
- "Always on" and ready to take action
- Advances company security initiatives

Frequent Tasks



- Generates reports to show company security health
- Manages personnel schedules to ensure coverage
- Reviews tickets to confirm tasks were completed

Goals

- Ensure high quality, rapid solutions to security alerts
- Keep team on task and focused
- Operational stability - make sure the company can always do its job

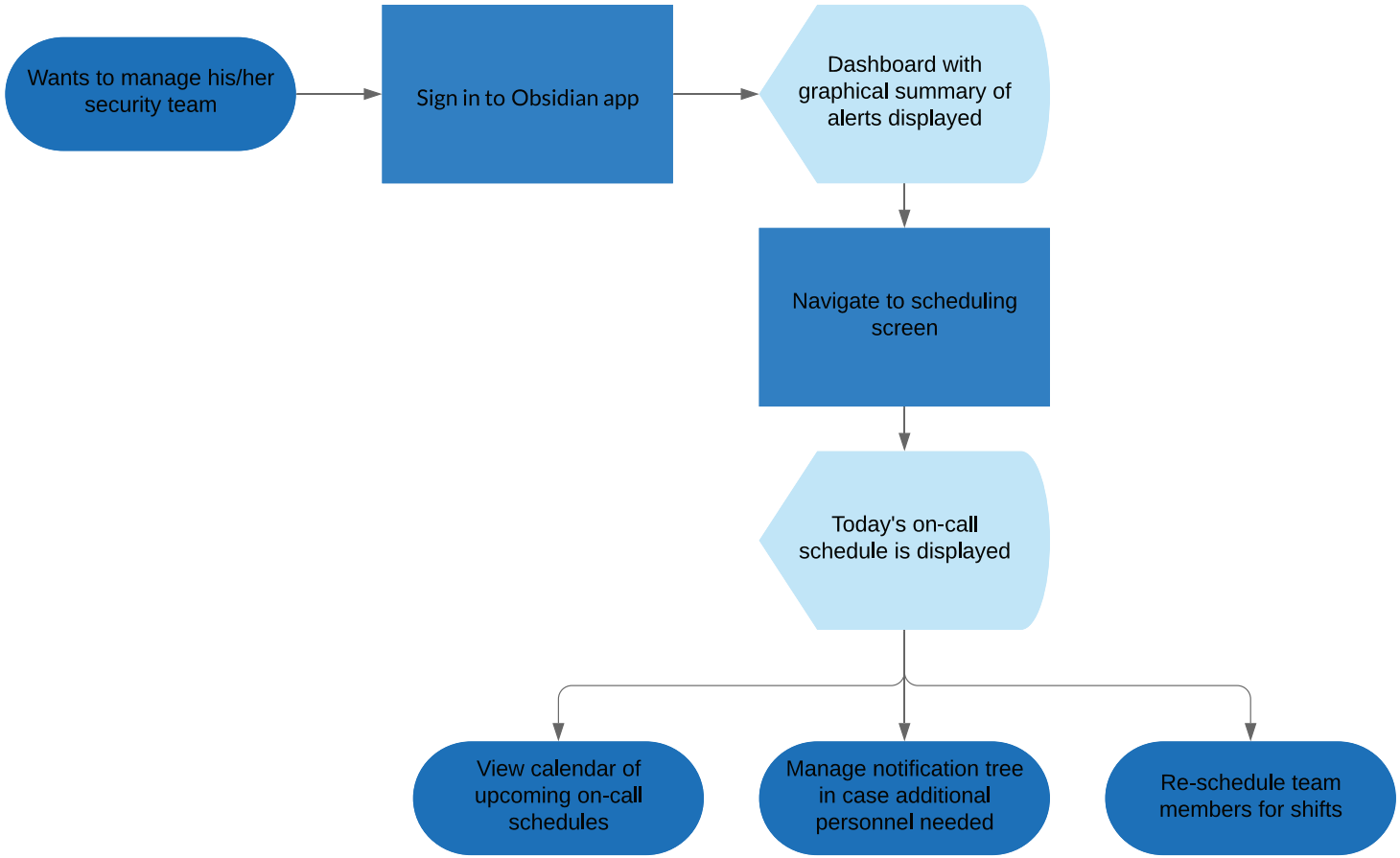
Frustrations

- Too many emails, tickets, and notifications to review
- Difficult to coordinate individual schedules with task assignments
- Raising employee security awareness and proper practices is challenging

PHASE I - RESEARCH & DISCOVERY

Manager User Flow Box Diagram

Figure - 1B



PHASE I - RESEARCH & DISCOVERY

Security Analyst Proto-Persona

"I do deep dives in data to gather contextual insights, find patterns, and piece everything together."

"You have to be really comfortable with your work set-up so you can quickly move through different thoughts without being caught up. It would be hard to navigate through a broad-to-deep cycle on a mobile device."

Security

Generating Reports

Triage

Analysis

Task Management

Company Management

Device Use

Cellphone

Tablet

Computer

Work Habits

Time at Desk/Computer

Not at Desk/Mobile

Characteristics

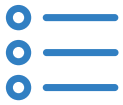
- Analytical
- Detail Oriented
- Problem Solver
- Patient
- Organized
- Multitasker

PHASE I - RESEARCH & DISCOVERY

Work Style

- Constantly checks to see if there are any important alerts to attend to
- "Always on" and accessible 24/7
- Triages work to others depending on the level of severity and best business practices

Frequent Tasks



- Organizes data into tables and groups to discover patterns
- Hunts and does deep dives
- Creates reports

Goals

- Clear the alert and incident queues
- Find the needle in the haystack
- Keep the company protected

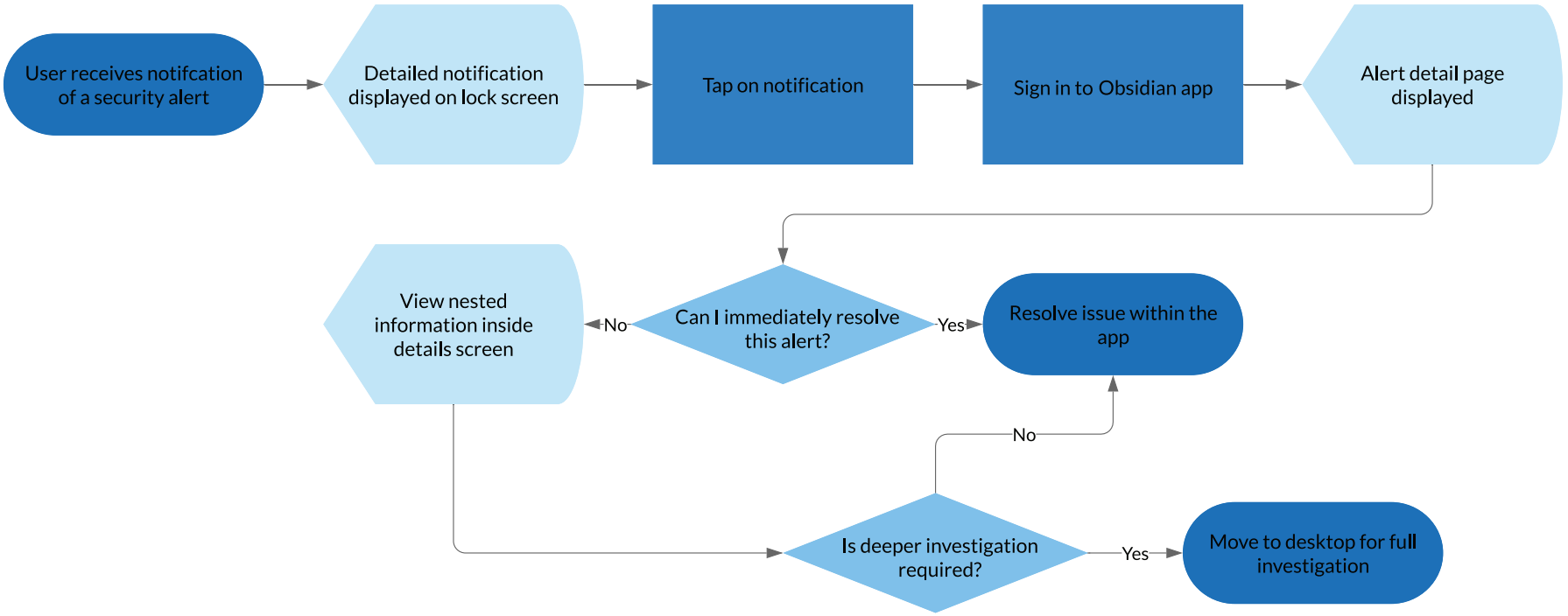
Frustrations

- Not enough context around alerts in some programs
- Getting too many push notifications
- Being tethered to a device 24/7

PHASE I - RESEARCH & DISCOVERY

Security Analyst User Flow Box Diagram

Figure - 1C



PHASE I
Design

OBSIDIAN

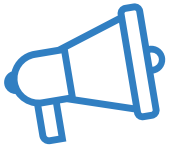
PHASE I - DESIGN

Product Requirements Document (PRD)

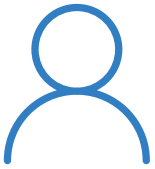
A PRD provides a holistic picture of all the specifications and components needed for each phase of design/development. This document was explicitly requested by Obsidian in order to outline the scope and specificity of the mobile app.

The PRD focused on the following specifications:

Secure Login and Logout



Alert Triage



User Profile

Notification Setting Customization

Reports

Scheduling & Personnel Management

PHASE I - DESIGN

The preliminary PRD was based on our research, proto-personas, and user flows. We also included wish list items discussed with Obsidian in meetings.

Our specification aligned with the primary goals of each proto-persona. As the product and the scope of the project matured -- due to feedback, interviews, and discussions -- the PRD was updated to reflect the current state of work.

During the discovery phase, the Security Analyst emerged as the primary target user for the mobile platform. With this realization, we reprioritized the scheduling system design for Managers and updated the PRD accordingly to reflect. Reporting was also scaled back.

For Phase I, we focused on two main user flows:

1. **Being Notified -** The process of viewing a notification and deciding what steps to take next.

2. **Hunting -** Browsing the app to view reports and alerts.

Primary Target User

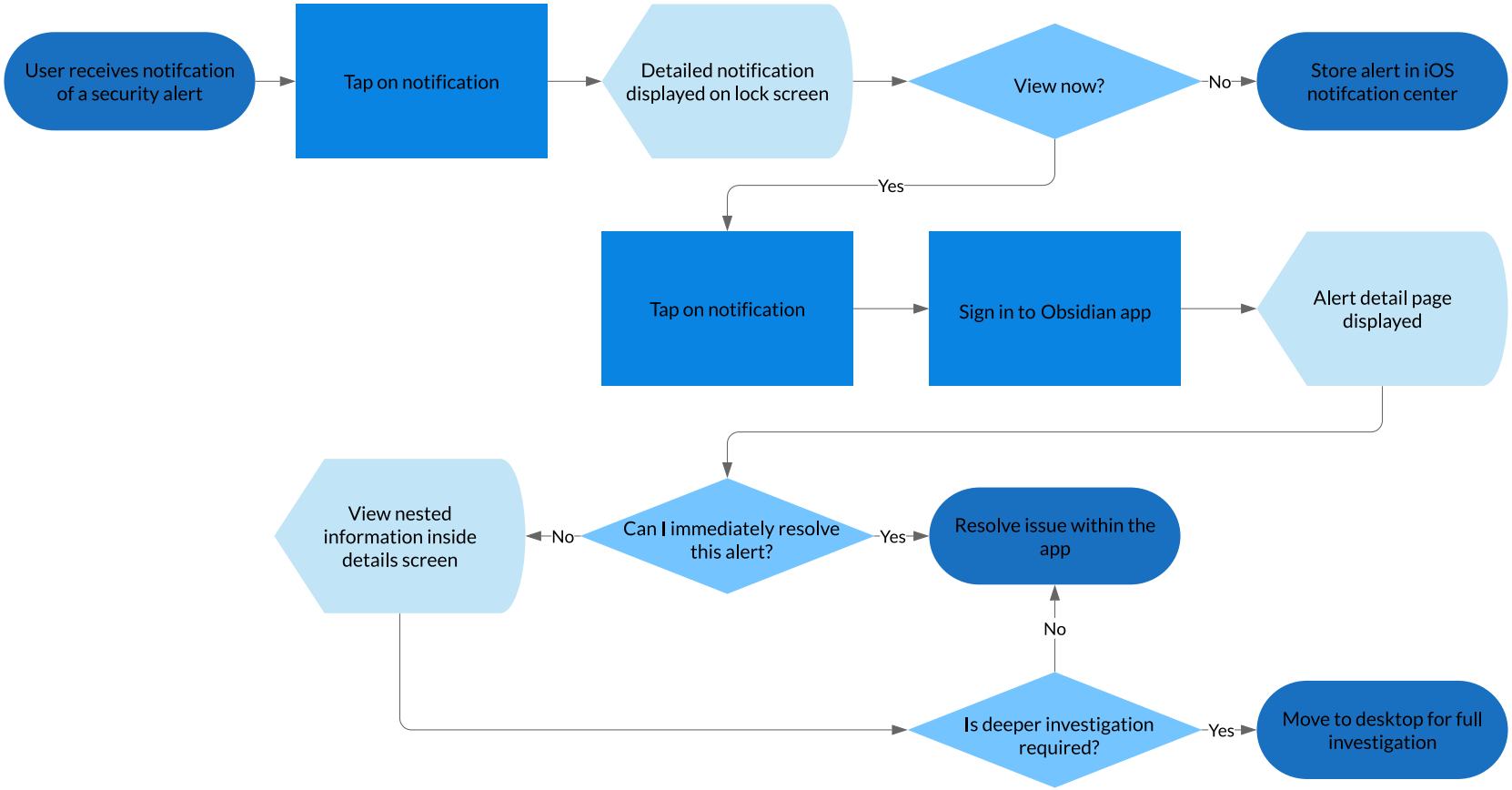
Security Analyst

Pgs. 27-29

PHASE I - DESIGN

“Being Notified” User Flow Diagram

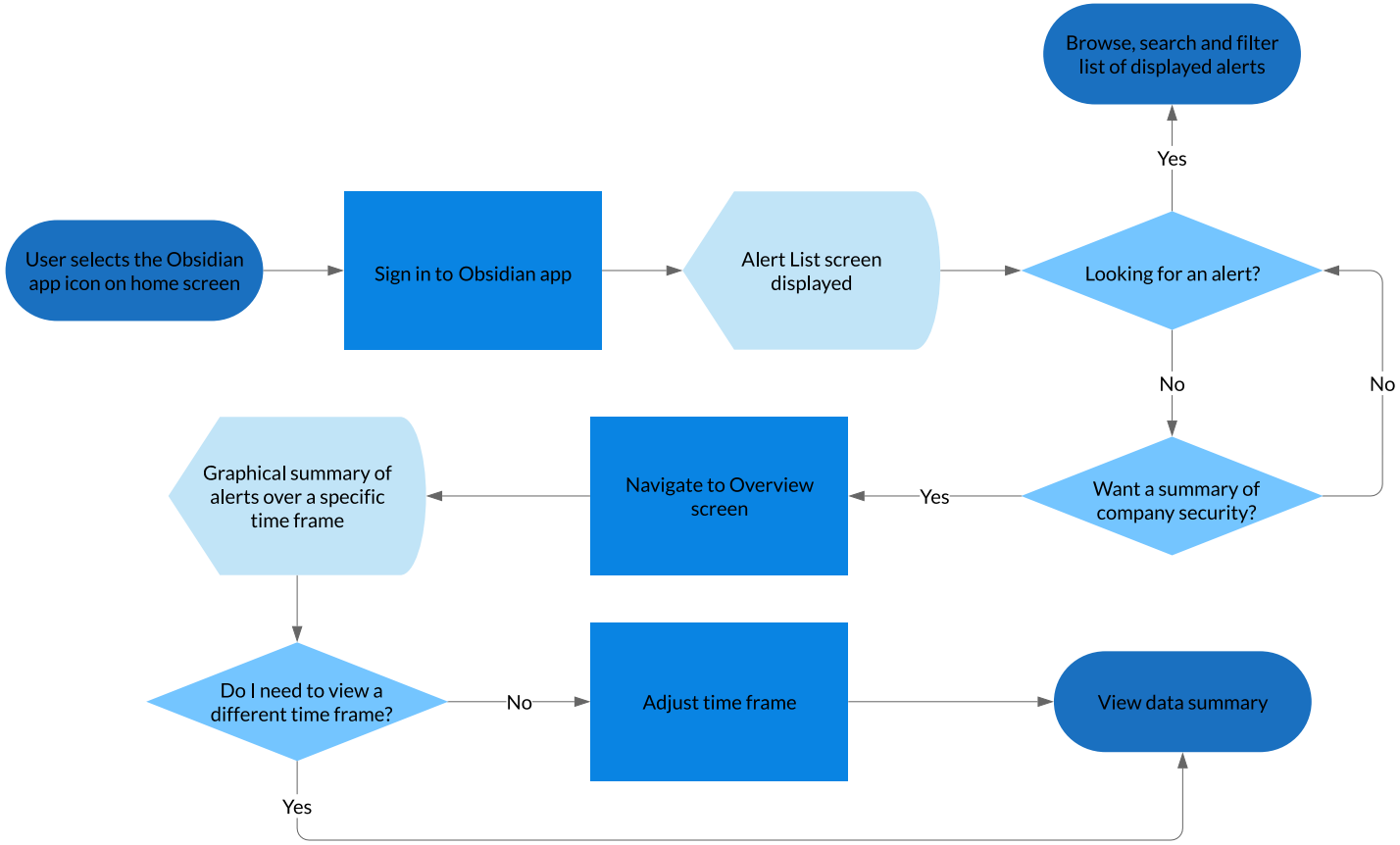
Figure - 2A



PHASE I - DESIGN

“Hunting” User Flow Diagram

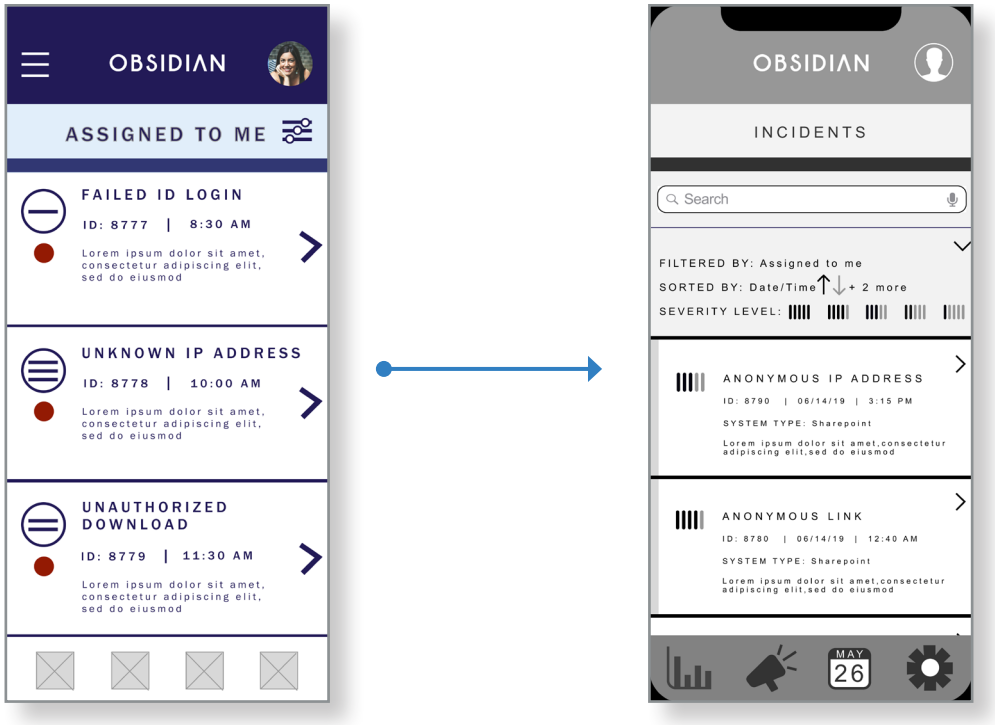
Figure - 2B



PHASE I - DESIGN

Wireframes

Our initial wireframes were originally designed in full color. To alleviate bias during user testing, we reduced to grayscale, so that both our team and testers would not be influenced by color.



PHASE I
User Testing

OBSIDIAN

PHASE I - USER TESTING

Goals

- Understand what features, design elements, and user flows were working.
- Verify if our login system was secure enough for our user's standards.
- Discover what users expected to see on the main screen/landing page.
- Validate if we provided the correct information to security professionals.
- Observe if the information was visually presented in a user friendly way.
- Find out if our users needed a reporting screen. If so, what should go on it?
- Learn if our alert notification settings and filter options were customizable enough and easy to use.
- Ascertain what information users wanted to have and be able to update in their profile.

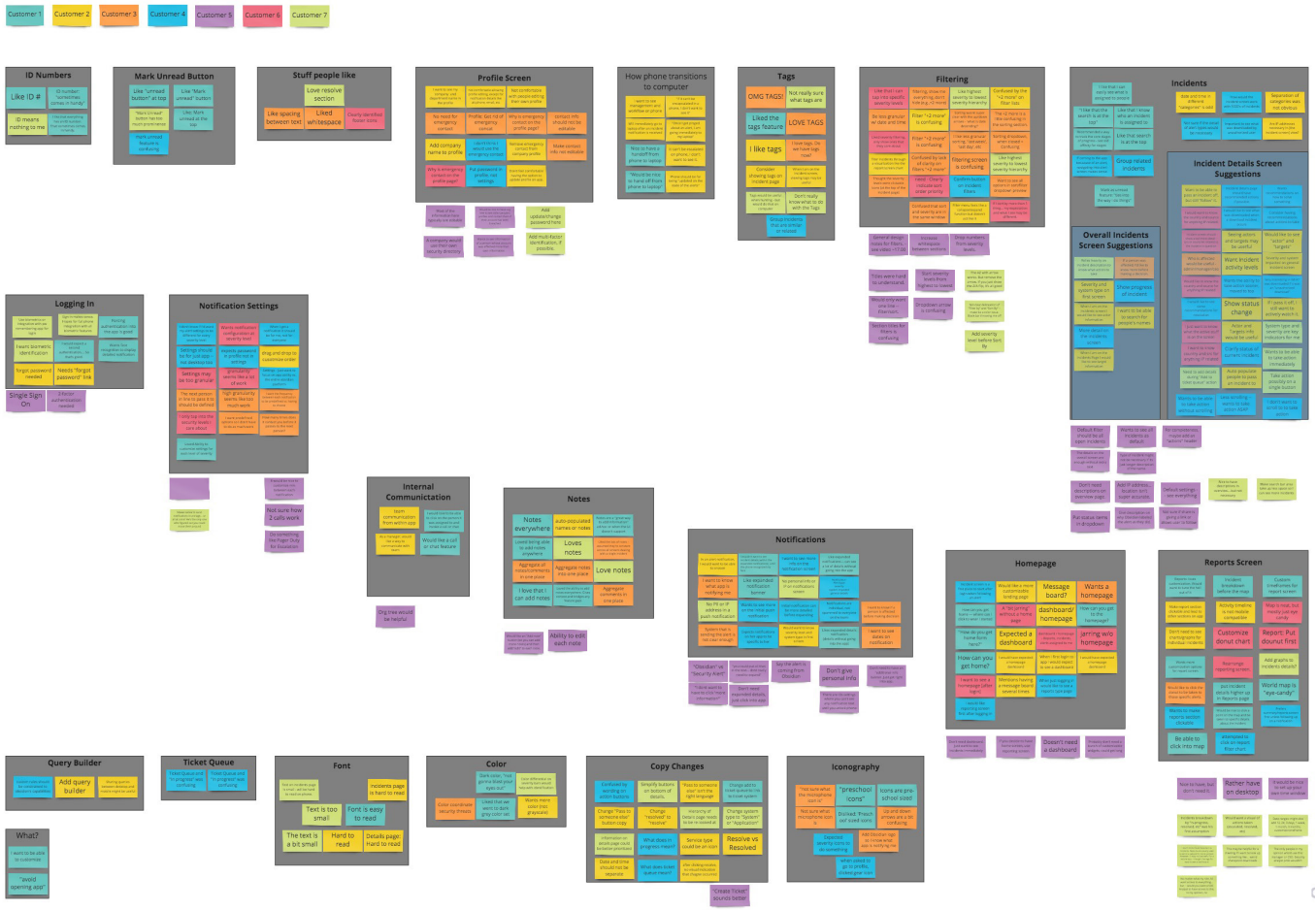
PHASE I - USER TESTING

User Testing Details and Protocols

- All customers participated.
- Usability tests were conducted over the video conferencing software, Zoom.
- Each of our participants shared their screens with us. We were able to view their movements and actions while using our prototype.
- We video recorded all of our tests in addition to taking notes.
- Users followed a “think aloud” protocol - they were instructed to talk through their thoughts/actions as they progressed. They also gave feedback.
- We took our users through our Security Analyst’s two user flows (“Being Notified” and “Hunting”).
- We measured our design and usability success/failures based on our users’ ability to complete each of our tasks.
- Completion time was initially considered. However, due to lengthy feedback by several customers, we felt it was more important to hear their comments than focus on the time it took them to complete the task.

PHASE I - USER TESTING

Affinity Diagram & Data Analysis



Our team members once again used Miro to aggregate the findings from each of the user tests. These tests provided us with significant qualitative feedback for our final phase.

PHASE I - USER TESTING

Universal Design Feedback

1. Pick colors that won't draw attention of people passing by a user when said user is on their phone.

2. It would also be helpful to pick darker colors that aren't harsh to the eye in case a user needs to check their phone in the middle of the night.

3. Use a larger, more readable font.

4. Make the icons in the footer smaller.

PHASE I - USER TESTING

Profile and Setting Screens Feedback

1. Remove the emergency contact feature.
2. Limit what users can edit. Users expressed that they could not edit their profile without admin privileges.
3. Move notification settings into profile screen instead of displaying on footer navigation menu.
4. Remove “Vibrate” and “Ring.” This is an iOS setting.
5. Simplify the settings and create a default. Users were confused by the notification order, frequency, and time.
6. Create accordion menu to showcase all severity level setting options before the fold.
7. Create “Sync” option so users don’t have to tediously set up each severity level. Set one and be done.

PHASE I - USER TESTING

Push Notification to Login Screen

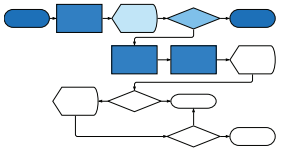
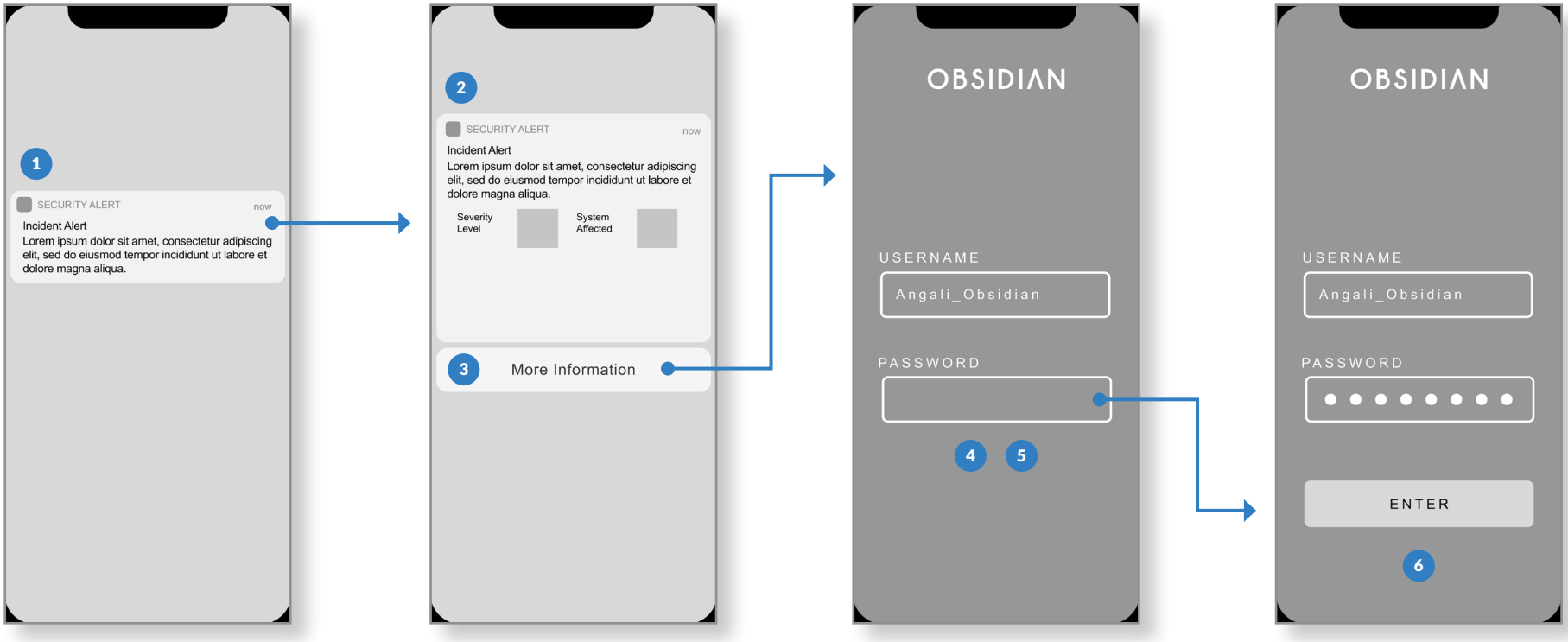


Figure 2A



1. Add company logo to push notification so users know Obsidian is sending said notification.
2. Provide pertinent information without giving away anything secure/private for a passerby to see.
3. Direct user to “Alert Details” screen after initial push notification. The expanded push notification with more info is not necessary.
4. Add biometrics as a sign-in option to speed up login.
5. Implement a “Forgot Password” feature.
6. Users voiced annoyance with authenticating for every sign in, but understood it from a security standpoint.

PHASE I - USER TESTING

Alert Details Screen Feedback

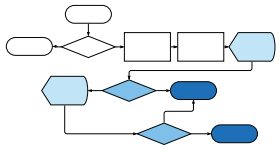
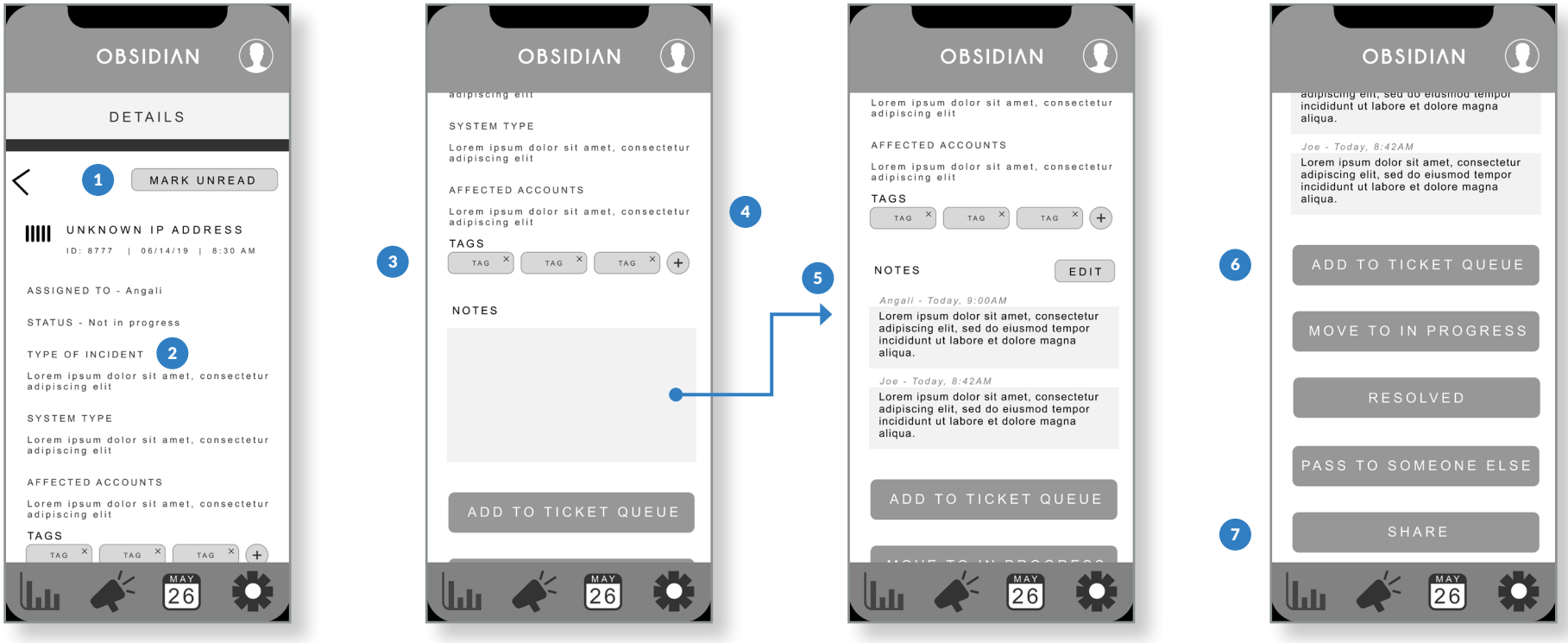


Figure 2A



1. Make the “Mark Unread” button smaller so it has less visual hierarchy on the screen.

2. Add the “Rule” so security professionals understand why Obsidian thought the alert was valid.

3. Keep “Tags” feature in next iteration. Users responded positively to it and thought it could be useful.

4. Include Obsidian’s recommended steps.

5. Modify “Notes” feature so users can edit their own notes and track comments by action and event time line.

6. Remove ticketing feature. Most users already use a ticketing software, like Jira and Zendesk.

7. Make actionable buttons viewable before the fold.

PHASE I - USER TESTING

Alert Overview and Filter/Sort Screen Feedback

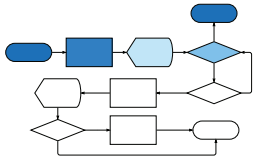
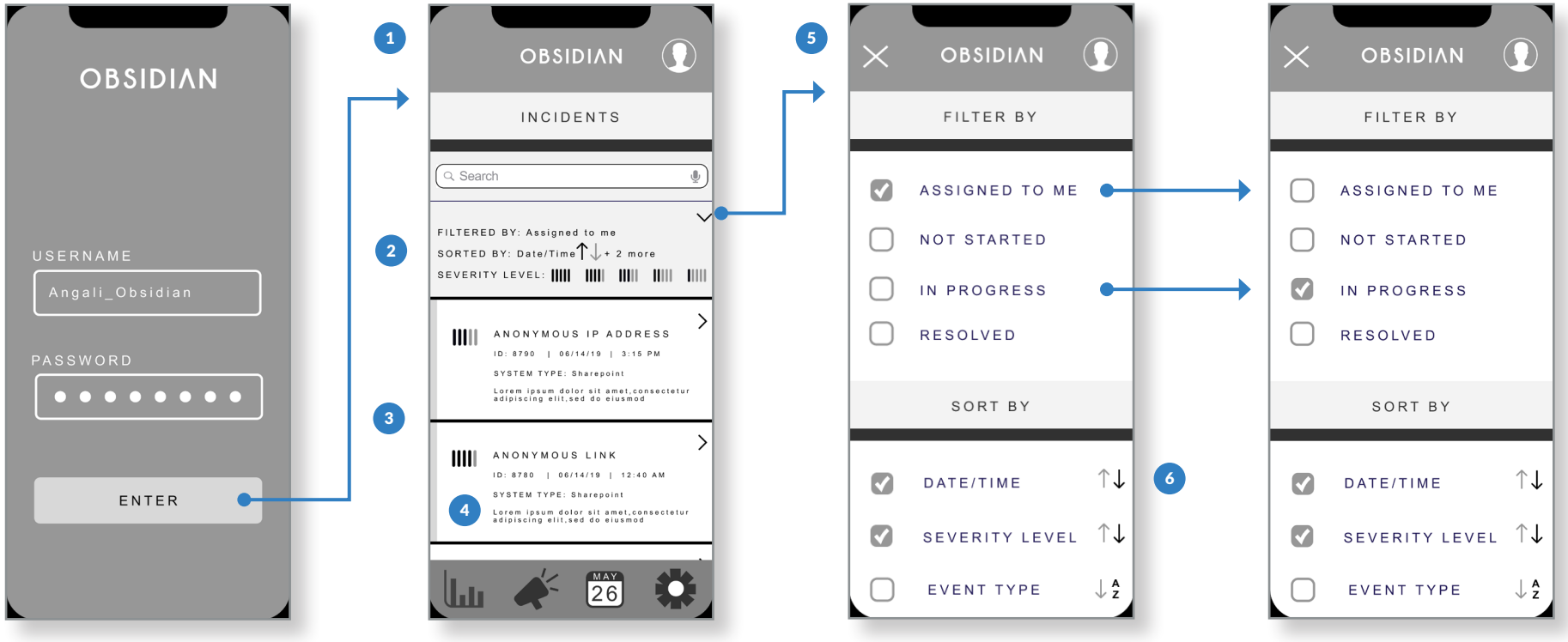


Figure 2B



1. Create a different “Landing Page.” Some users expected to see a “Reports” or “Overview” screen instead.
2. Simplify and make the “Search/Filter/Sort/Severity” section at the top take up less room.
3. Show more “Alerts” on the screen before the fold.
4. Display which user’s account was affected.
5. Users liked that they could customize their view of alerts via sorting and filtering.
6. Make directional icons less ambiguous.

PHASE I - USER TESTING

Report Overview Screens Feedback

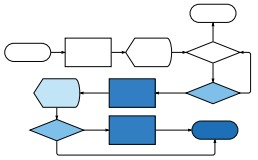


Figure 2B

1. The “Reports” screen had mixed reviews. High level security executives and managers thought it was a nifty feature for meetings. Analysts thought it wasn’t useful.

   Some users suggested to make this the “Home/Landing” screen if they’re opening the app from “iOS Home.”

2. Make graphs and maps interactive. Some users tried clicking on them and wished they led somewhere.

PHASE II
Design

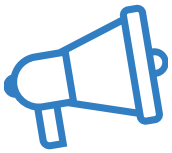
OBSIDIAN

PHASE II - DESIGN

Design Focus

Our team considered all user testing feedback for the design of our high fidelity prototype and adjusted our user flow diagrams accordingly. In addition to fine-tuning our UI, we integrated Obsidian's colors, icons, typography, and branding.

We concentrated on implementing the following features:



Alerts

As discussed, Security Analysts emerged as the primary users of our mobile platform. Therefore, "Alerts" became the most important section within the application.

Security Analysts evaluate multiple sources of information when determining if an alert represents a legitimate security incident. The smallest detail could tip key decisions or connect a series of related alerts. Because of this, we conducted a comprehensive analysis of all information that we planned to display on each screen.

One of the more challenging design aspects we encountered was identifying the most important information to display on push notifications and the alert overview lists. In order to determine the most helpful hierarchy and information structure, we asked targeted follow-up questions to multiple users and implemented features accordingly.

PHASE II - DESIGN

Reports

The “Reports” section was renamed to “Overview,” as we removed the option to create a printed/shared document that could be available outside the application.

We designed a series of graphical representations that illustrate the current state of a company’s security health. We decided to make the graphs/charts interactive, as many of our users tried to tap on the them during the last phase of user testing. For example, our “Alerts by Status” donut chart allows users to view pre-filtered alert lists by status.

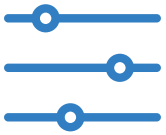
In addition, we created a “Service Connection Status” feature to show that the Obsidian platform is actively receiving expected data from all connected services.

Settings

Users expressed desire for customizable push notification within the mobile app. Our initial design gave users control over the frequency, number, and method of notifications for each of the five security alert levels. However, our initial feedback indicated that this was too complex. Users needed something simpler.

We streamlined the interface for our current iteration. We also added a sync setting so users could set one security alert level and synchronize it for the rest.

PHASE II - DESIGN



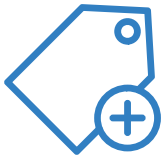
Filtering and Sorting

Our initial filtering and sorting feature left some users a bit overwhelmed. The current iteration displays a cleaner, catalogued, hierarchical menu for selecting sort and filter criteria. It also enables security professionals to hunt for patterns within data categories that might indicate a larger imminent threat.

Secure Login and Logout

In our first iteration, logging into the mobile application required only a username and password. User feedback indicated a desire to include biometric and password manager options as well. We decided on a form of two-factor authentication, which would include either an authenticator app or a biometric feature, in addition to traditional login criteria.

We decided to omit the following features:



Ticketing

Previous research indicated a mixed desire for a ticketing system within the mobile app. Some companies wanted integration with outside ticketing platforms such as Jira, Zendesk, and ServiceNow. Since Obsidian's current platform does not integrate with any of these systems, we determined that this topic would be out of scope.

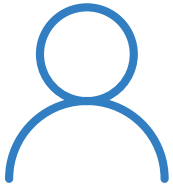
PHASE II - DESIGN

Passing Alerts

In our original wireframes, we included a button to pass alerts between colleagues. In our final design, we chose to provide simple native link sharing until a messaging and ticketing system could be developed.

Scheduling

We originally believed that the ability to manage teams/assign on-call times would be important for larger companies. As we learned more about the daily routines of our users, we realized that many of the current users of the Obsidian platform do not work with large teams or already utilize independent scheduling systems.



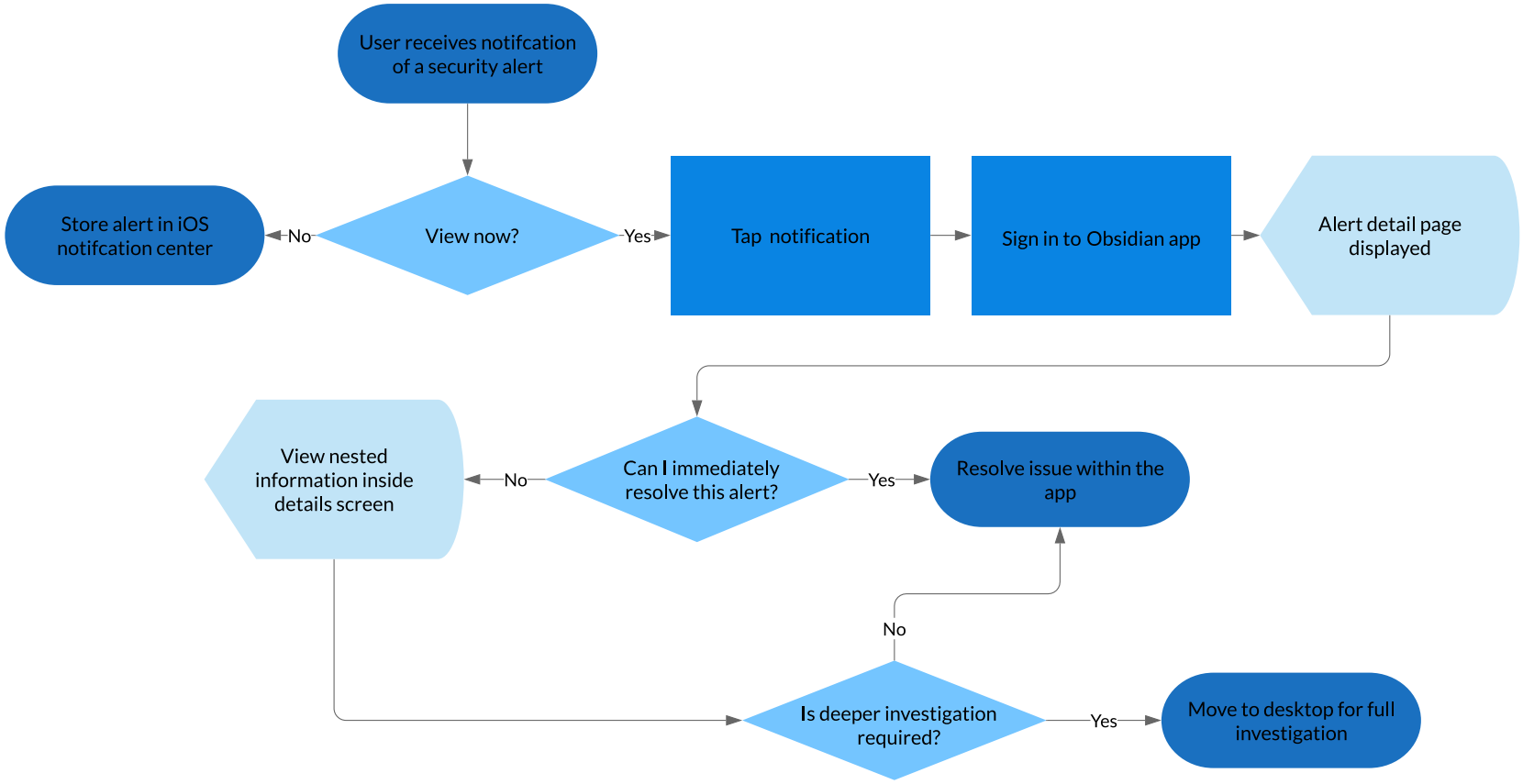
Profile Editing

Based on responses from users during wireframe testing, we learned that many companies use a global directory and restrict their employees from updating their personal information. Other companies use Single Sign-On (SSO) and likewise want to limit the user's ability to edit their own data. For that reason, we removed the capability to edit personal information within the mobile app.

PHASE II - DESIGN

“Being Notified” User Flow Diagram - Final

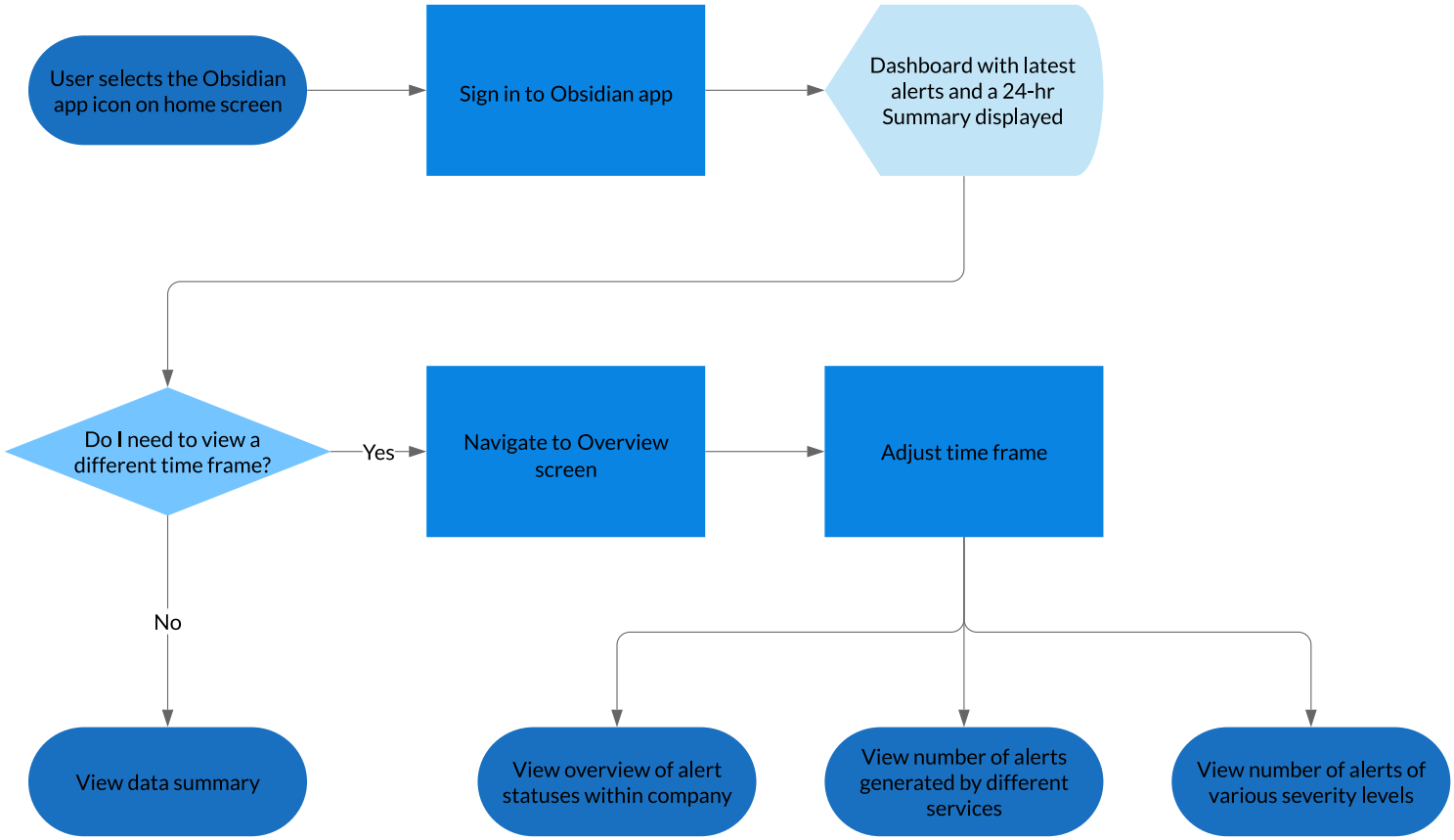
Figure 3A



PHASE II - DESIGN

“Hunting” User Flow Diagram - Final

Figure - 3B




PHASE II
User Testing
OBSIDIAN

PHASE II - USER TESTING

Goals

- Locate primary usability pain points
- Validate content on alert details screen
- Verify extent of a user's ability to edit their profile
- Gauge reactions/gather feedback for the notification system
- Further understand use cases for "Overview" screen
- Solicit user feedback on the "Landing/Home" screen

PHASE II - USER TESTING

User Testing Details and Protocols

- Due to scheduling constraints, only Customers 3, 5, and 7 participated.
- Usability tests were conducted over Zoom.
- Each of our participants shared their screens with us. We were able to view their movements and actions while using our prototype.
- We video recorded all of our tests, in addition to taking notes.
- Users followed a “think aloud” protocol - they were instructed to talk through their thoughts/actions as they progressed and give feedback.
- We measured our design and usability success/failures on our users’ ability to complete each of our tasks. Time to complete tasks was tracked and analyzed.

PHASE 2 - USER TESTING

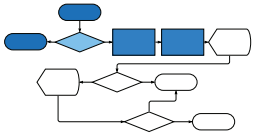
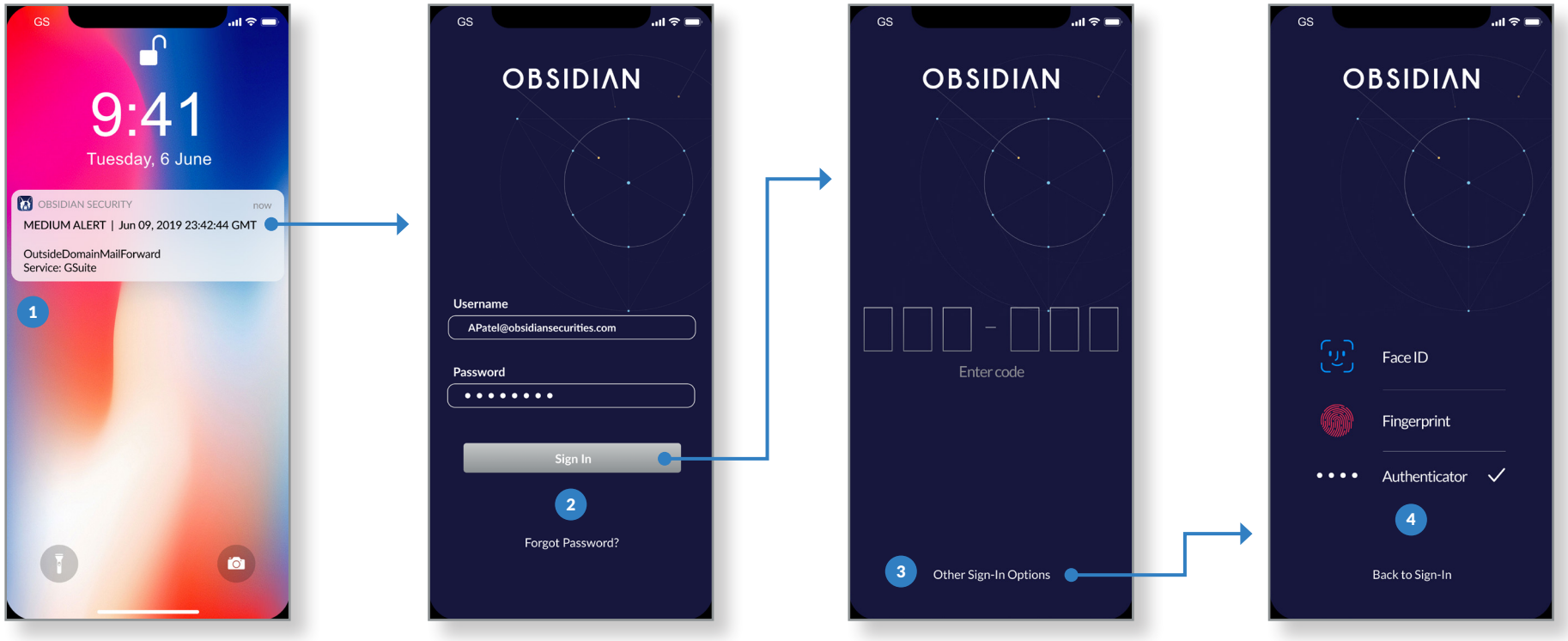


Figure 3A

Push Notification to Login Screen Feedback



1. Users liked the simplified push notification.

2. Users were again annoyed that they needed to authenticate every time they entered the application, but understood the benefits of enhanced security.

3. Some users found it difficult to modify their login options unless instructed to do so from the login screen.

4. Users appreciated the two-factor authentication and biometric verification options.

PHASE 2 - USER TESTING

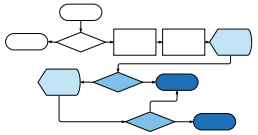
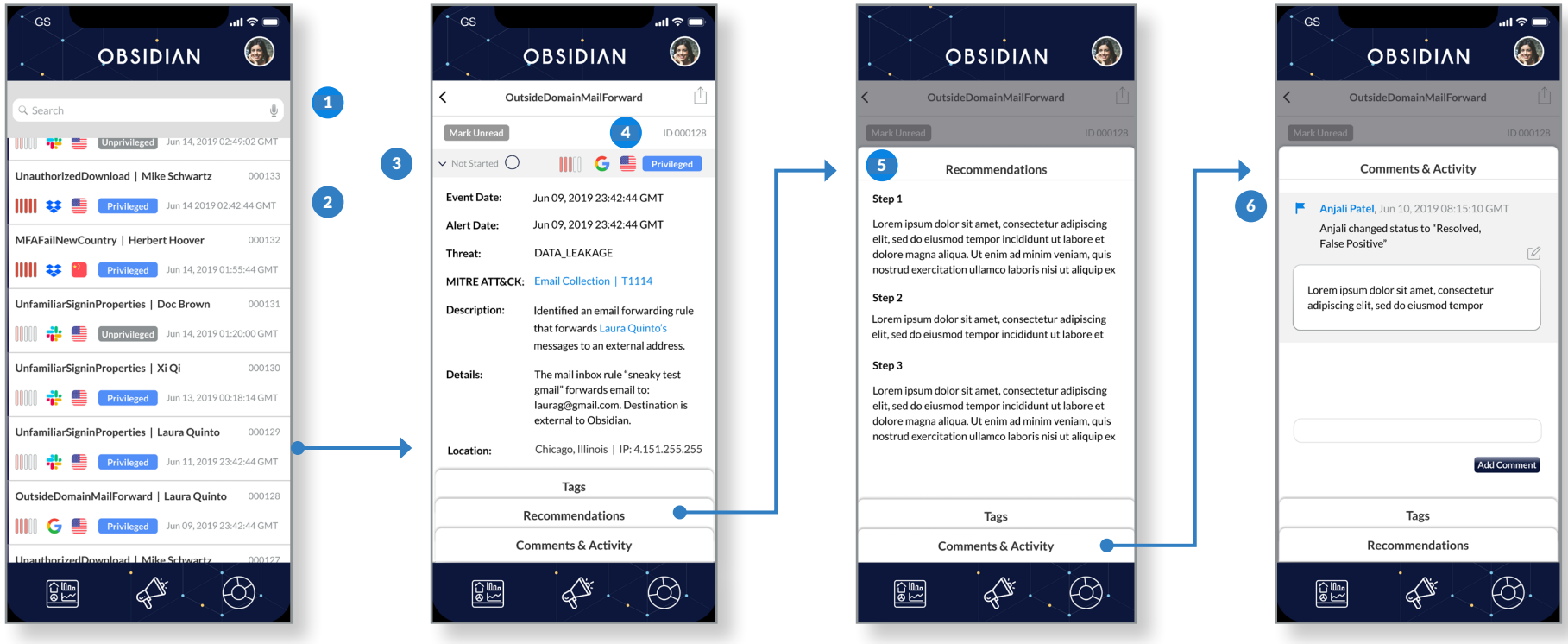


Figure 3A

Alerts Overview and Details Screen Feedback



1. Users liked the search function.
2. Per client request, timezone was default set to GMT. Users were unaware they could change it.
3. Changing the status was not intuitive, as there are no obvious affordances.
4. Confusion whether the flag icon was indicating attack origin or destination.
5. Users appreciated the tabbed cards but had difficulty closing out of them. They kept clicking on the gray area.
6. Users liked the "Comments and Activity" card. However, a corresponding inbox/messaging system would be ideal.

PHASE 2 - USER TESTING

iOS Screen to Login Screen Feedback

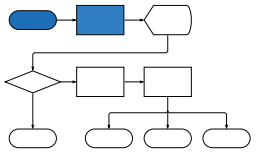
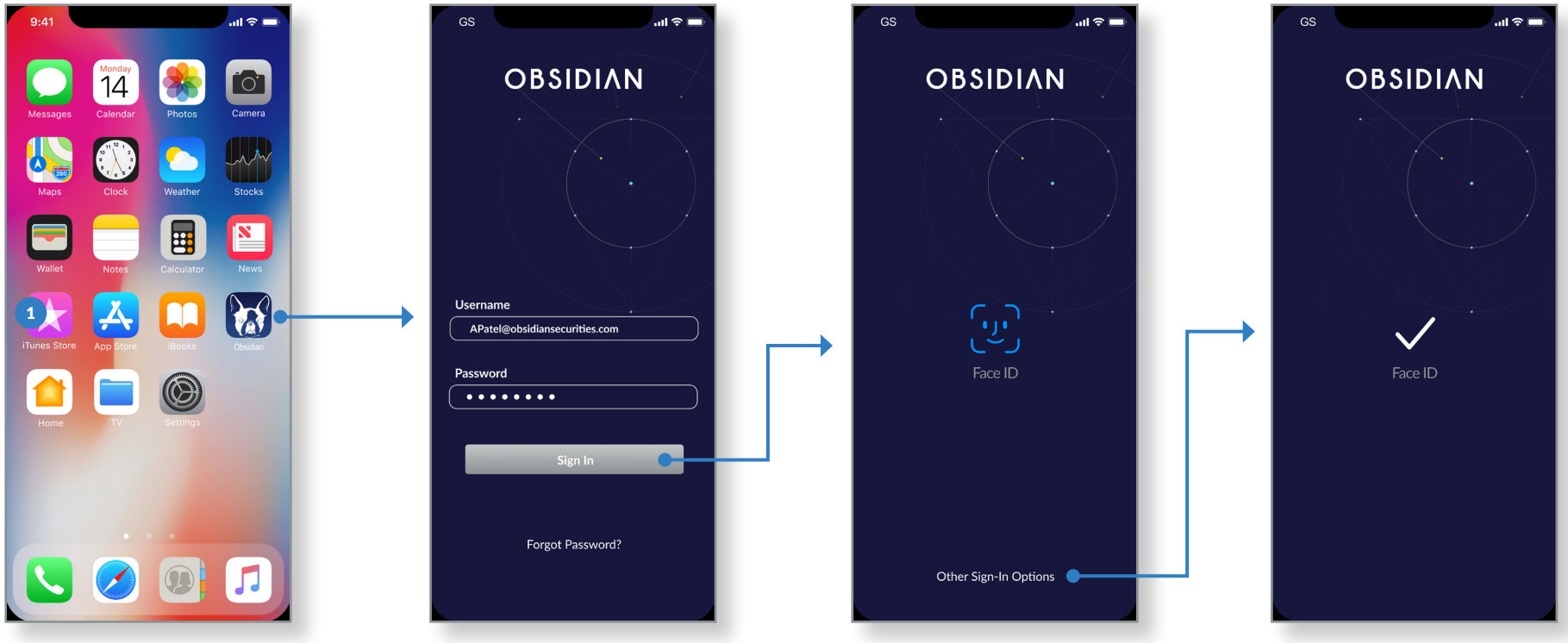


Figure 3B



User flow from iOS screen to login received the same feedback as mentioned on page 57.

PHASE 2 - USER TESTING

24-Hour Summary Landing Screen Feedback

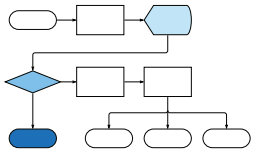


Figure 3B

1. Although our users requested a landing screen that displayed 24-hour reports and the most recent alerts, most did not find it useful once they saw it in play.

2. Our users liked that the three charts (severity, status, and service) were interactive and went to pre-filtered/ sorted alert lists.

3. It was not intuitive that the "Latest Alerts" card expanded for some of our users.

PHASE 2 - USER TESTING

Overview Screen Feedback

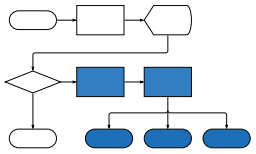


Figure 3B

1. Users were confused about the usefulness of this screen when compared to the screen for “24-Hour Summary.” Some users suggested that we should combine the two.

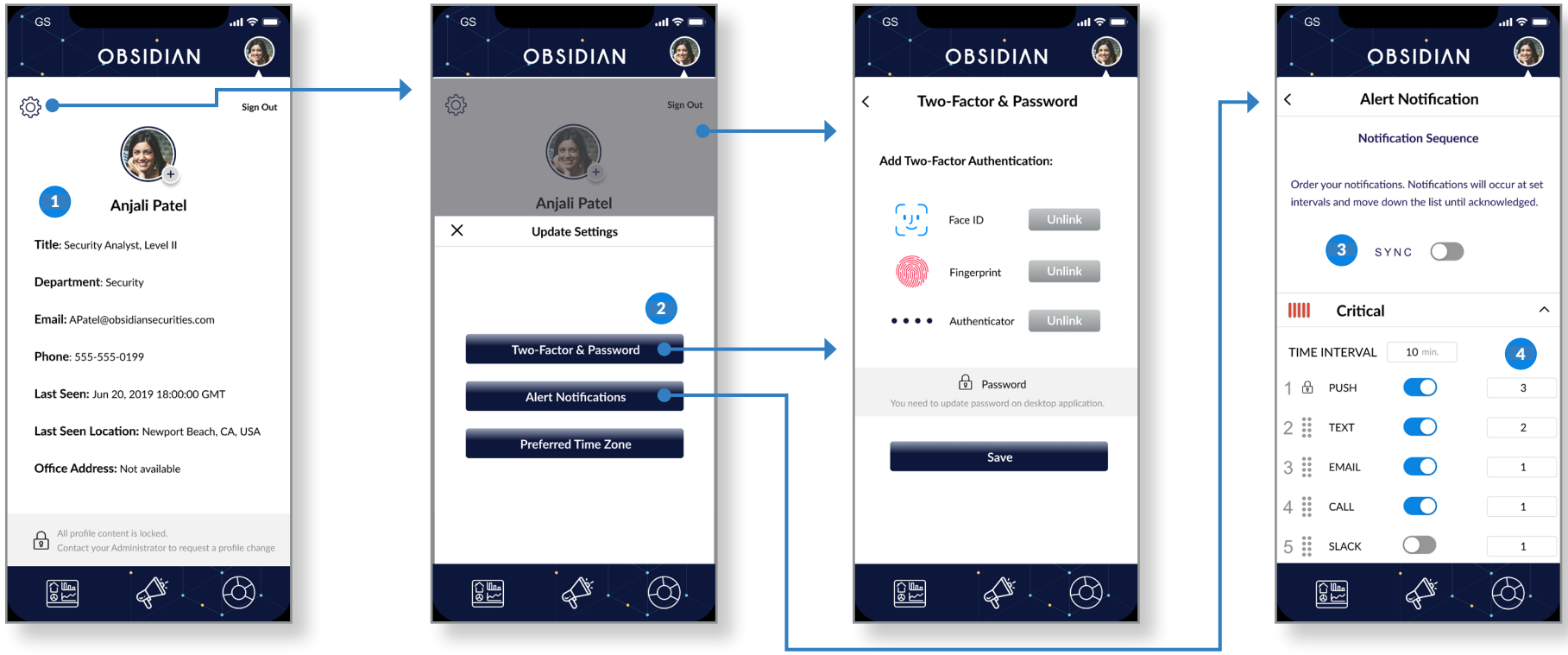
2. Just like the “24-Hour Summary page, users liked that the three charts (severity, status, and service) were interactive and went to pre-filtered/sorted alert lists.

3. No user understood that the footer icon for this section referred to a graph oriented dashboard page.

4. Users liked that they could customize their date range.

PHASE 2 - USER TESTING

Profile and Settings Screen Feedback



1. The information contained in the profile screen wasn't relevant to users. However, they did feel that the info would be helpful if it was a part of a company directory.

2. Users had a hard time trying to find where they could change their two-factor authentication and password. It may make more sense to have these accessible on the login screen(s).

3. None of the users expected the "Sync" button to behave the way we designed it.

4. Users were impeded by the complexity of the notification system. Some noted that they would likely never utilize this feature if they were using the actual mobile application.

PHASE II
Recommendations

OBSIDIAN

PHASE II - RECOMMENDATIONS

Our team analyzed our findings in order to formulate solutions for future iterations of Obsidian's product design. These recommendations relate to potential mobile and platform features, as well as usability improvements uncovered from our final round of testing.

Alert Routing

An alert routing structure could be used to notify users who only need to receive specific alerts. For instance, a security team may have individuals or groups assigned to watch over certain services, who would only want to be notified of alerts within their area of responsibility.

Users in higher management positions may not want to receive alert notifications, but would still want to use the mobile application to keep tabs on company health.

Alert routing could also be used in conjunction with a personnel management system, to notify team members who are only on-call at a scheduled time. Interview research indicated that security professionals believed that burnout was due to being, "Always on, 24-7." Only notifying on-call personnel is one way to try to fight that burnout and give security team members a reprieve from constant notifications.

PHASE II - RECOMMENDATIONS

Alert Watch Lists

Chief Security Officers may not need to be notified of every single alert. They may however, be very interested in the ever changing status of one or two high priority alerts. One thing that kept coming up in user interviews/tests was the notion of 'following' an alert which the user found important. Having a "Watch List" would allow users to follow certain alerts for individualized monitoring.

Alert Status

The option to change alert status is displayed in a drop-down menu on the "Alert Details" page. Users did not realize that this menu was an interactive component. If it had either stood out as an obvious drop-down menu or had been in the form of a button, it might have had better visibility as an interactive component.

Alert Naming Convention

When listing out alerts, there needs to be a more consistent shortened alert title for mobile displays. In order to be unique and informative, this version would need to take into consideration the prioritization of the alert's rule, event, and type.

PHASE II - RECOMMENDATIONS & NEXT STEPS

Notification Settings

More rounds of design iteration are needed in regards to the notification settings. Users were confused about what these settings would actually do, even with simplification and brief directions. While some users had expressed the desire for more sophisticated notification options, our current settings may have been too complicated for the actual practical needs of the users.

Connection Visibility

In the high-fidelity prototype, application connection status is shown at the top of the “Overview” screen. Currently, there is no similar feature on the desktop platform.

Discussion with the Obsidian team informed us that in the future, broken service connections may be handled as critical-severity security alerts. Corresponding alerts would show up in the “Alert Overview” screen. Users would then receive notification.

We feel it’s important to graphically highlight these statuses. Users need to know immediately if there is a problem with a service connection. It may also be helpful to add names of associated services, as users might not recognize them by logo alone.

PHASE II - RECOMMENDATIONS & NEXT STEPS

Messaging

A consolidated list of comments regarding an alert was created within the “Alert Details” page. Users expressed interest in communicating this with their teams.

An inbox messaging system would allow users to securely disseminate information, or forward alerts to fellow team members for verification. This feature would need to be weighed against the option of Slack integration. Creating the ability to open Slack links within the Obsidian mobile or desktop application might also be viable.

Custom Comment Requirements

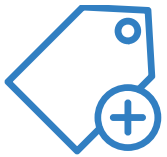
There was varying feedback on how the mobile application forced a user to input a comment before they could resolve an alert. Some users liked this requirement, because it added context to why the alert was resolved and also prevented colleagues from closing it out before taking proper time to verify the action.

Other users looked for the fastest possible way to resolve an alert (especially low severity ones), so that they could move on to the more important triage tasks.

PHASE II - RECOMMENDATIONS

Intuitive Menu Closing

We discovered that many users struggled to close some of the menus. In the card structure of the “Alert Details” screen, users had difficulty discerning how to shift between cards and how to close them out entirely. Every user tried to click the shadowed space on the outside of the card. In the “Filter/Sort” screen, clicking on the filter icon in the upper right of the page to close the menu was also not intuitive. Users voiced that they were looking for a confirmation button to save their filter preferences and take them back to their newly filtered list of alerts.



Third Party Ticketing Integration

As Obsidian markets to larger corporations, the likelihood of encountering a ticketing system already in place increases. Services such as Jira, ServiceNow, or Zendesk provide robust features that can be utilized across multiple company verticals.

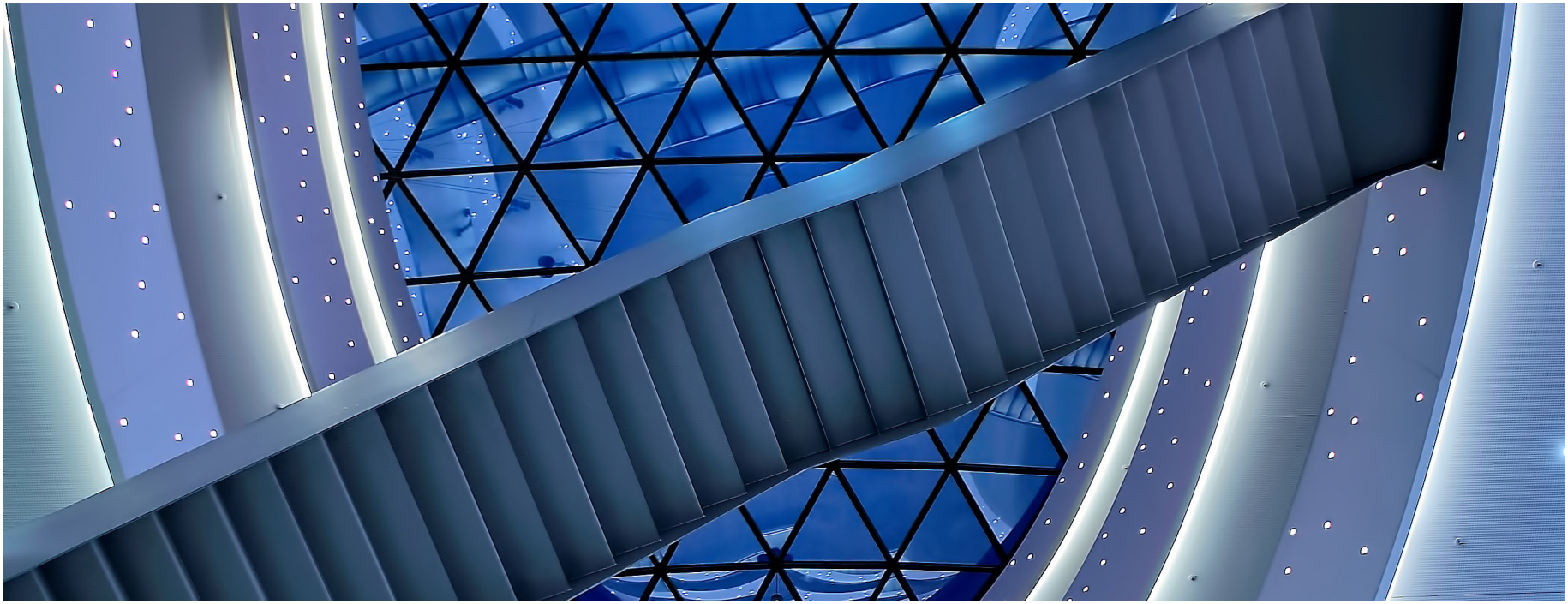
Obsidian research suggests that companies already integrated with these systems would prefer to link them to Obsidian’s platform, opposed to switching entirely.

From a mobile perspective, this would mean implementing the ability to send alerts to a linked ticketing system and support continued third-party monitoring/tracking.

PHASE II - RECOMMENDATIONS

Personnel Management System

Originally, the Manager proto-persona was identified as one of our three main user types. A personnel management system would allow these Managers to organize their on-call schedules for their team. Team members would be notified when their shifts start and end. These members could also request shift changes from their Managers and conduct all scheduling related communication within the platform.



PHASE II - RECOMMENDATIONS

Conclusion

This project started with a simple request, “Make me a mobile app. Please.” What was at first a seemingly innocuous query has been developed over the past six months into an actual high-fidelity prototype. The contents of this mobile application are extensively backed by research, user testing, and hours of professional design.

Creating a mobile extension to Obsidian Security’s desktop platform is a solid step towards a more flexible and customizable user environment. Companies and their Security Analysts can elect to use the mobile application to augment their preferred workflows as much they want.

During this project, we discovered that customizable solutions are imperative for security professionals, so that they may respond to potential threats in a timely and efficient manner.

Our recommendations provide key points to consider moving forward in regards to additional iterations and development of the mobile app. As Obsidian Security continues to develop the holistic experience of their platform, we look forward to seeing how they will integrate our research discoveries, mobile designs, and recommendations into their future product.

It has been a pleasure working with the Obsidian team and we wish them all the best as their product continues to evolve!

Thank you

OBSIDIAN