Shawn Kenney

IBM

SOC Reservation System

◉ Research ○ Strategy ◉ Design ○ Leadership

Introduction

In addition to threat monitoring services the “Managed” portion of IBM Managed Security Services means that IBM employees have responsibility for the maintenance of their customers network security devices such as firewalls and intrusion detection systems. These teams work out of a network of Security Operations Centers (SOC) located around the world. When a change such as a firmware update is needed to these devices it needs to be scheduled during a “maintenance window” that doesn't impact business operations for the customer. Historically, these windows were scheduled through e-mail and appointments entered in a shared Lotus Notes calendar. Tracking team member availability across time zones and continents was also done with this shared calendar.

SOC managers reached out to our team to discuss how we might be able to design a bespoke system to help them manage their work and availability. It was clear that the tools they needed to manage their operations did not match the level of sophistication their tools to monitor networks around the globe had.

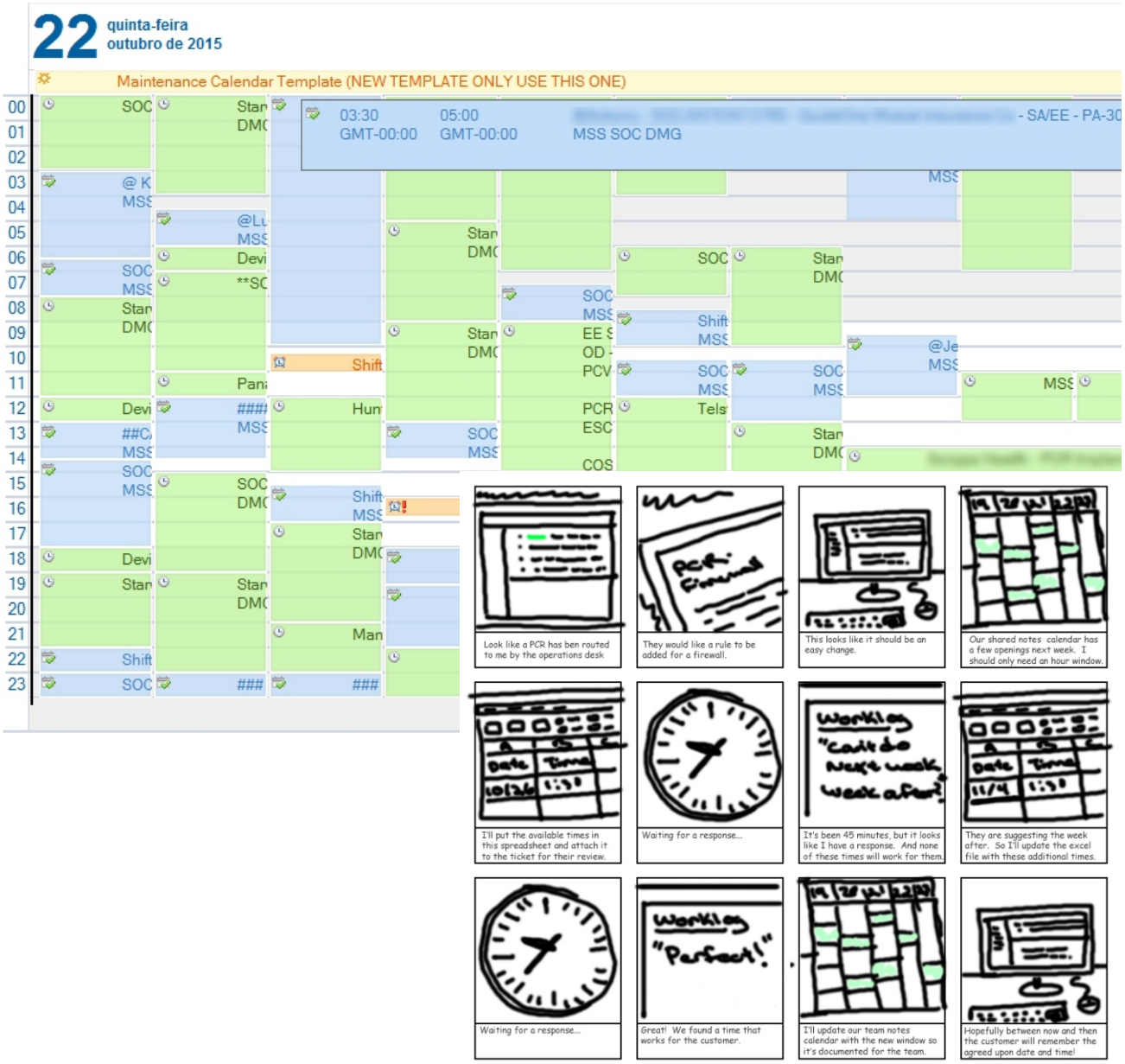
https://www.ibm.com/services/managed-security

Process

We started by holding learning sessions with leaders of our Security Operations Centers to understand the day-in-the-life experience of our teams and their work. We learned how support requests come into the system, how those tasks get assigned, the time policies that were in place to accommodate the work being performed, plus post-appointment administrative work, what managers/shift leaders need to know as work is being performed, along with the impact of contractual agreements with clients that dictate when work can be performed. We also learned how work moves between shifts and how teams work together across time zones.

It was clear from these discussions that we needed a view tailored for our team members, as well as a view for shift managers that could look across team members to see work scheduled when starting or transferring a shift to another leader.

Once we had a good feel for the needs of our SOC teams, we leveraged IBM's Design Thinking Methodology to begin working through the problem. As a team, we first iterated through creating "Hills," which are essentially opportunity statements in the form of "Who, What, and WOW." These Hills covered a few unique needs of our teams, allowing us to break the larger problem down into smaller chunks that we could then pull back together into concepting. Once we had our Hills, we created some storyboards of as-is scenarios and to-be scenarios for how we'd like the flow for each to go moving forward.

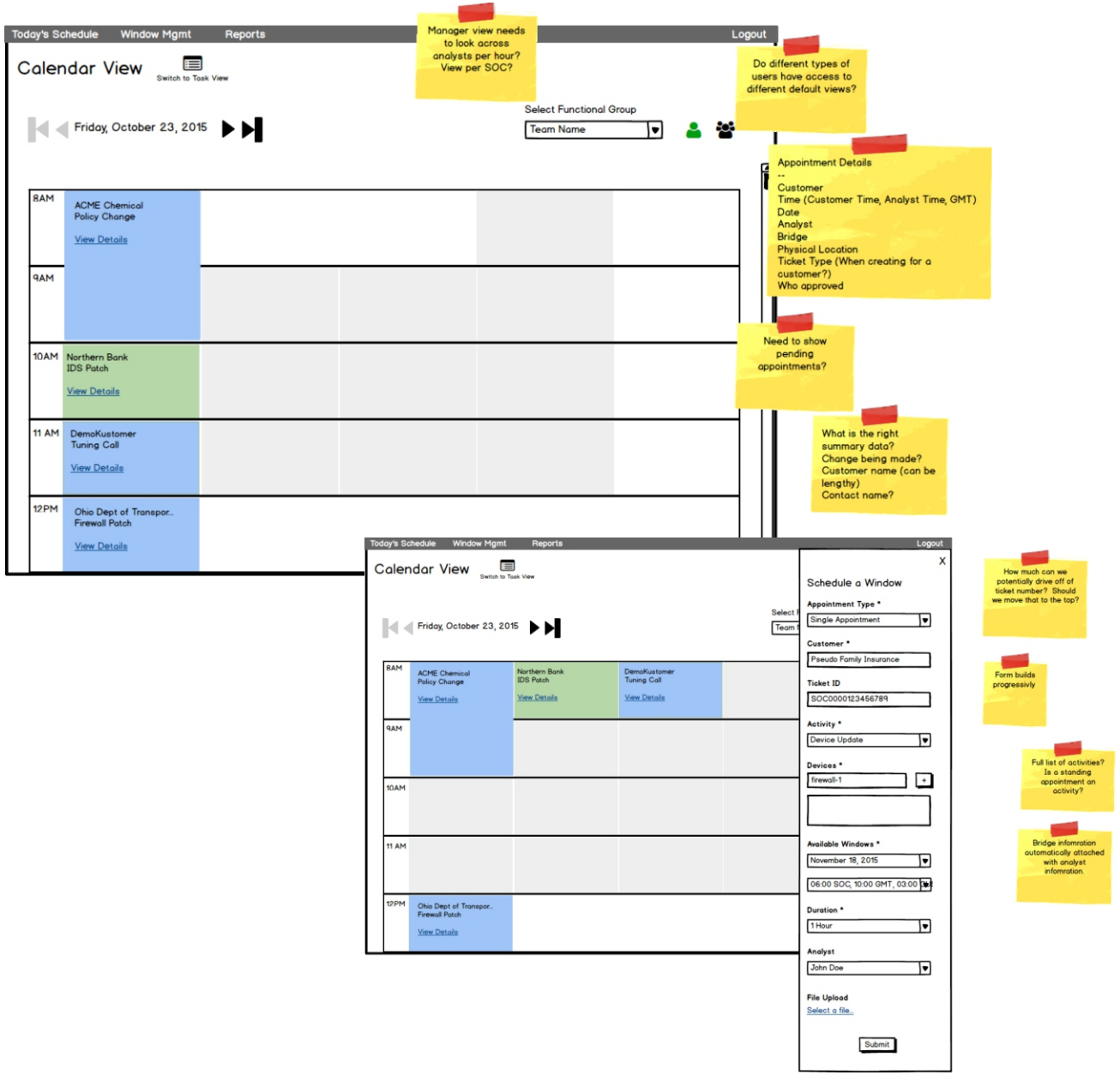


Early Iterations

In early design concepts, we explored how to lay out different views of appointments in the system and how those might change between what an individual team member would see, what a shift lead would see, and how these views could be customized using filters.

Non-English names were an early concern from a screen utilization perspective, along with the display of long client names. We worked with managers to understand how they shorthand names and did an analysis of our team members' names to see what the “worst-case scenario” length was. These discussions ultimately led to the how we prioritized information display for an appointment block.

We also spent time exploring how much of the experience could be data-driven off data stored in the support tickets, with the intent of streamlining the effort needed by analysts to get an appointment in the system. These concepts were initially created as wireframes in Balsamiq, our team's wireframing tool at the time. Once we went through a few cycles of design revisions, we moved into creating higher fidelity designs in Photoshop, eventually leading to a click-through prototype that we could get feedback on from team members.

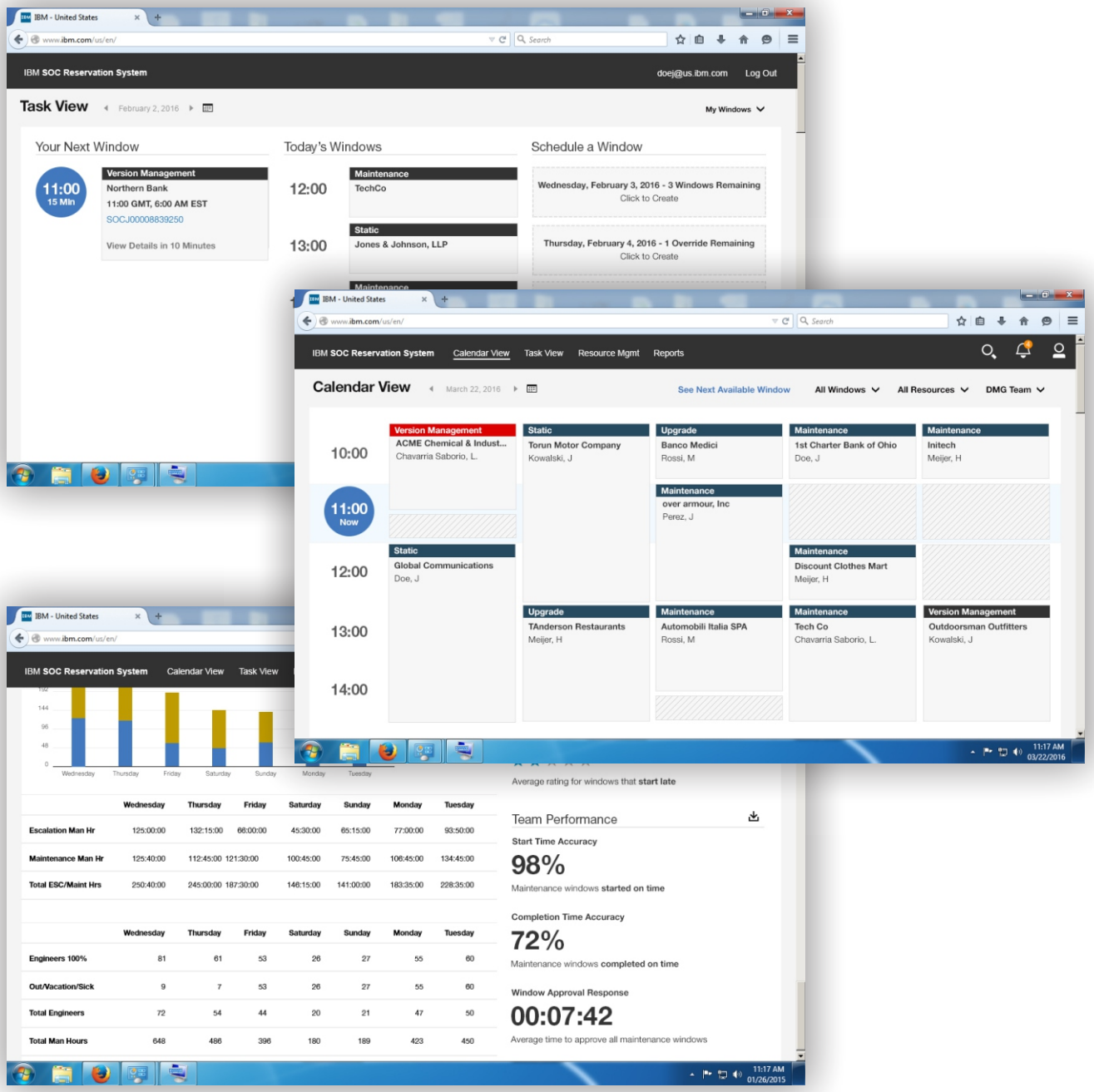


Final Design

For MVP instead of just designing views for those performing the work and SOC shift leads, we revised our approach to account for the Operations Desk staff responsible for creating windows, and updated the designs to allow managers the ability to create, approve, and assign windows to team members. The view for team members performing the work, allowing them to see only the work assigned to them for a day and the details for the work being performed, remained consistent with earlier concepts.

The view for individual team members was task-focused. The screen highlighted their next maintenance window, the type of task to be performed, and a link to the ticket so they could prepare in advance. To the right of that were additional windows that were coming up in their shift. All times were in GMT, which SOCs used to keep their operations centers around the globe aligned. The final section of their view allowed them to schedule time slots for future work that aligned with their personal availability.

The view for shift leads allowed them to see tasks across each hour. In addition to seeing who was performing the work and for which client, the shift lead could also see which tasks had run over their allotted time. This allowed them to reach out and provide support to the team member if needed. They could also receive notifications for any pending requests and approve them from here as well. Finally, we also designed a report they could sue to see overall team performance on for the week.



Project Summary

The team was excited to begin using this new tool and, during the development phase, described it as “the nicest tool we've had built for us.” Our development team was also excited to build it, and due to the level of thought and planning during the design process, the team was able to review the designs and begin building it immediately. They had demonstrable code to demo to our SOC partners after just a few sprints.

Unfortunately, I accepted an offer for a new position before development was completed on this project, so I never had the opportunity to see this project in action in person. I don’t have any for this project and even if I had stayed, I’m not sure that success would have been measured by “reduced time by ‘X’ percent”. .

Sometimes we in the UX community put too much focus on quantifiable metrics to validate our design decisions after the fact. For this project success simply would have been measured by stepping foot in a Security Operations Center and seeing the team operating as better versions of themselves. In those terms, the “thank you’s” I received before I left IBM was quantifiable enough.