Shawn Kenney

IBM

SOC Mobile Ticketing System

● Research ○ Strategy ● Design ○ Leadership

Introduction

IBM's global network of Security Operations Centers (SOCs) and their customers had been using the same web-based tools for over a decade, inherited through an acquisition.

This tool's success was critical to IBM's value proposition. When monitoring potential threats for a client, IBM analysts play a forensic role: they gather evidence, package it, and then escalate it to the client. Ultimately, the client's Chief Security Officer makes the final call on how to proceed with any potential threat.

Over time, the aging platform (see right) suffered from a lack of developers familiar with the underlying framework or willing to learn it, as well as inadequate support for mobile devices and accessibility compliance. This provided our window to review how effective the tool was at escalating events to clients for them to prioritize and act on.

Project Date

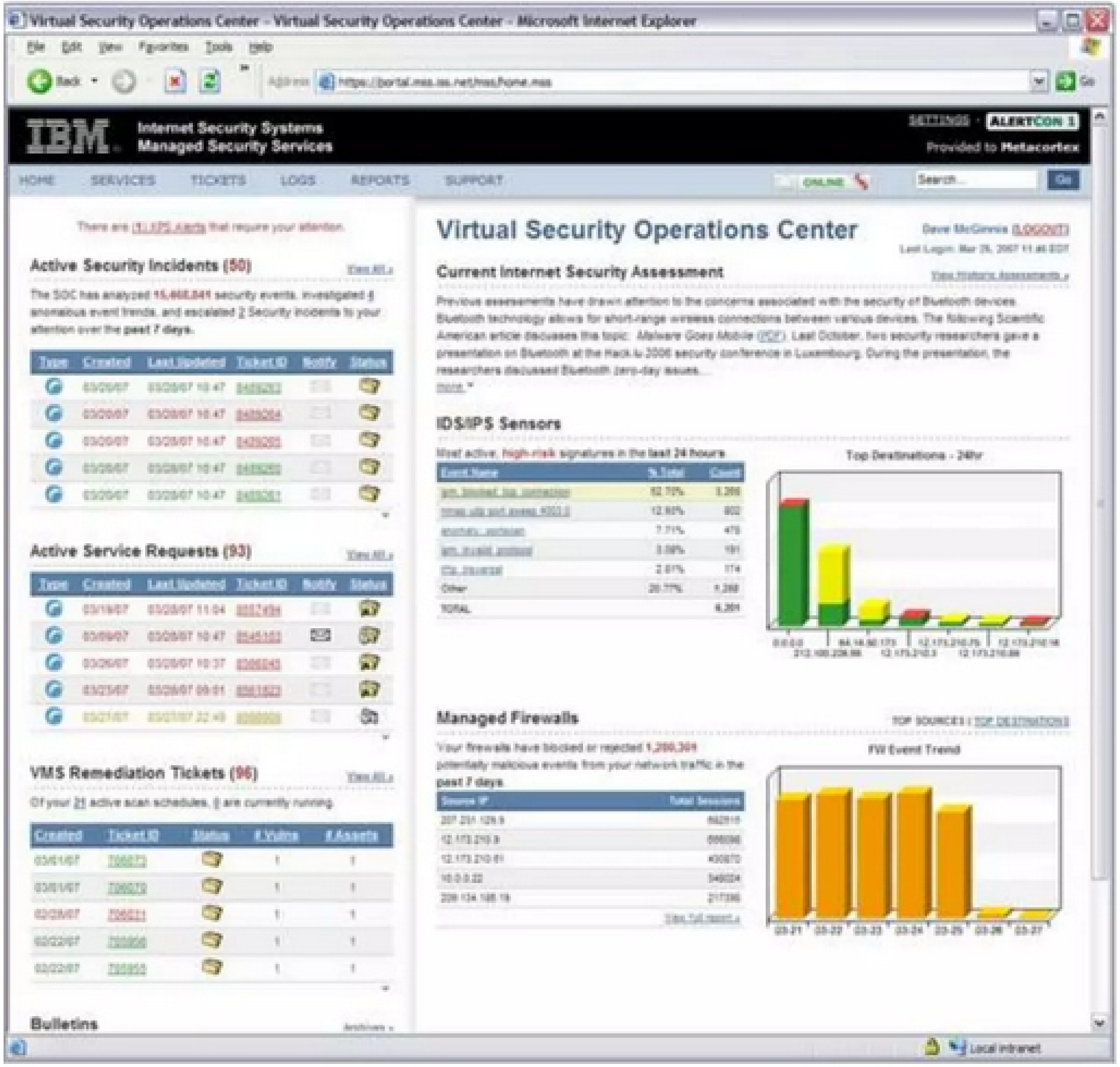
Fall, 2015

Tools Used

Balsamiq Mockups, Adobe Photoshop, IBM Design Thinking

Additional Team Members

Brian Anderson, Maciej Forc



Virtual Security Operations Center - Virtual Security Operations Center - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://portal.mss.iss.net/mss/home.mss
Go
Internet Security Systems
Managed Security Services
SETTINGS
ALERTCON 1
Provided to Metacortex
HOME SERVICES TICKETS LOGS REPORTS SUPPORT
ONLINE
Search...
Go
Local intranet

There are (1) IPS Alerts that require your attention.

Active Security Incidents (50) View All

The SOC has analyzed 15,468,041 security events, investigated 4 anomalous event trends, and escalated 2 Security incidents to your attention over the past 7 days.

Type	Created	Last Updated	Ticket ID	Notify	Status
	03/20/07	03/28/07 10:47	8459263		
	03/20/07	03/28/07 10:47	8459264		
	03/20/07	03/28/07 10:47	8459265		
	03/20/07	03/28/07 10:47	8459262		
	03/20/07	03/28/07 10:47	8459261		

Active Service Requests (93) View All

Type	Created	Last Updated	Ticket ID	Notify	Status
	03/19/07	03/28/07 11:04	8557494		
	03/09/07	03/28/07 10:47	8545183	✉	
	03/26/07	03/28/07 10:37	8566243		
	03/23/07	03/28/07 09:01	8561823		
	03/21/07	03/27/07 22:49	[illegible]		

VMS Remediation Tickets (96) View All

Of your 21 active scan schedules, 0 are currently running.

Created	Ticket ID	Status	# Vulns	# Assets
03/01/07	706673		1	1
03/01/07	706672		1	1
02/28/07	706621		1	1
02/22/07	705956		1	1
02/22/07	705955		1	1

Bulletins Archives

Virtual Security Operations Center

Dave McGinnis (LOGOUT)
Last Login: Mar 28, 2007 11:46 EDT

Current Internet Security Assessment View Historic Assessments

Previous assessments have drawn attention to the concerns associated with the security of Bluetooth devices. Bluetooth technology allows for short-range wireless connections between various devices. The following Scientific American article discusses the topic: Malware Goes Mobile (PDF). Last October, two security researchers gave a presentation on Bluetooth at the Hack.lu 2006 security conference in Luxembourg. During the presentation, the researchers discussed Bluetooth zero-day issues...
more

IDS/IPS Sensors

Most active, high-risk signatures in the last 24 hours

Event Name	% Total	Count
[illegible]	52.70%	3,269
[illegible]	12.93%	802
[illegible]	7.71%	478
[illegible]	3.08%	191
[illegible]	2.81%	174
Other	20.77%	1,288
TOTAL		6,201

Top Destinations - 24hr

Managed Firewalls TOP SOURCES | TOP DESTINATIONS

Your firewalls have blocked or rejected 1,288,369 potentially malicious events from your network traffic in the past 7 days.

Source IP	Total Sessions
207.231.129.9	662519
12.173.210.9	658098
12.173.210.81	430870
10.0.0.22	349024
209.134.198.19	217398

View full report

FW Event Trend

Process

Why was the lack of mobile support a problem? We conducted interviews with several of our clients' Chief Security Officers (CSOs) to understand their process when investigating a threat. I also went on-site to shadow a CSO for a day in their environment.

A common complaint was that the existing system required them to be tethered to their desks in order to review an alert, meaning they wouldn't see it if they were away from their desk or would have to stop what they were doing to return to their desk to determine if it's worth investigating.

Our new approach needed to allow a CSO to triage on their mobile device when a threat was escalated. Through our conversations, we identified the essential details a CSO would need in order to make a decision: whether to continue what they are doing or pause their current task to begin an investigation. Since threats can arise at any time during the day, their current task might be attending a meeting, commuting to the office, or having dinner with their family.

Once we completed our research, the second phase was to build out functionality for IBM analysts to create tickets. We were asked to maintain parity with the existing functionality as much as possible. A normalization effort was made to clean up inconsistencies between screens and align the look and feel with the new IBM design language.

Once that was done, we began work on our mobile concepts.

Is there a device outage? If there is, that's a priority.
Is there an attack under way? How long has it been active?
What's the IP address? Is it internal to my organization?
Where can I review the research that has been done so far?

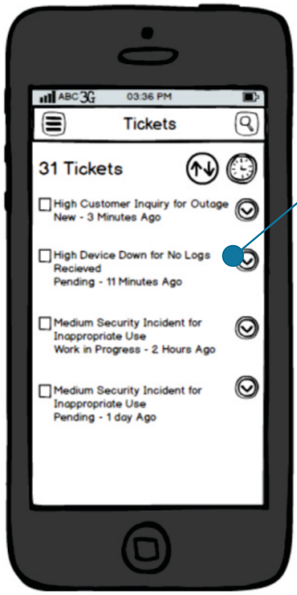
Generated by Microsoft Designer

Early Iterations

Our early iterations focused on the display of tickets within a native mobile app. The details for each ticket could be expanded or collapsed and sorted either by severity or by a specific timeframe. Summary-level details for each ticket included the event title, perceived severity, recency, and a brief description. The CSO could tap into the event to view more detailed information. They would also be able to search for past tickets, allowing them to compare current events to similar past incidents.

Wireframes were validated through additional research sessions with our initial participants. During these calls, we identified additional details a CSO would need to prioritize their time. The ability for the client to create a support ticket in response to an incident - such as quickly blocking an IP - was identified as being helpful along with seeing the ticket number in the event they needed to follow up with us. Additionally, access to the raw log data was identified as important. This can be quite a large data set so it didn't need to be in the app, but needed to be accessible from the app.

Additionally, our internal stakeholders suggested we verify their contact information in the app and that a rating system be included to encourage clients to provide more detailed information about issues, helping to improve our services.



31 Tickets

□ High Customer Inquiry for Outage
New - 3 Minutes Ago

□ High Device Down for No Logs Recieved
Pending - 11 Minutes Ago

□ Medium Security Incident for Inappropriate Use
Work in Progress - 2 Hours Ago

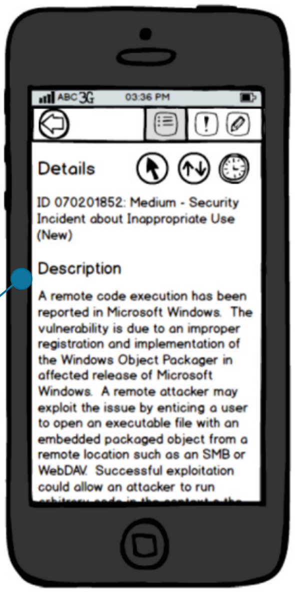
□ Medium Security Incident for Inappropriate Use
Pending - 1 day Ago

Summary Data

Focus placed on the bare minimum needed to understand the potential situation, and if this is worth a deeper review.

Detailed Data

Detailed data on the event could be accessed from the summary view, including standard definitions of the attack.

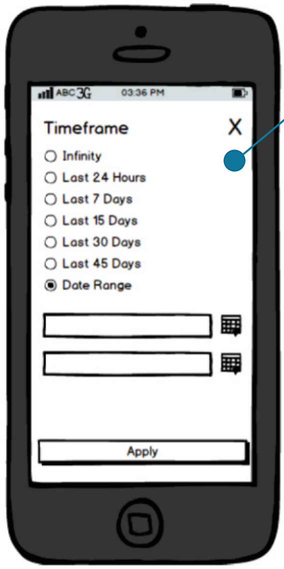


Details

ID 070201852: Medium - Security Incident about Inappropriate Use (New)

Description

A remote code execution has been reported in Microsoft Windows. The vulnerability is due to an improper registration and implementation of the Windows Object Packager in affected release of Microsoft Windows. A remote attacker may exploit the issue by enticing a user to open an executable file with an embedded packaged object from a remote location such as an SMB or WebDAV. Successful exploitation could allow an attacker to run



Timeframe

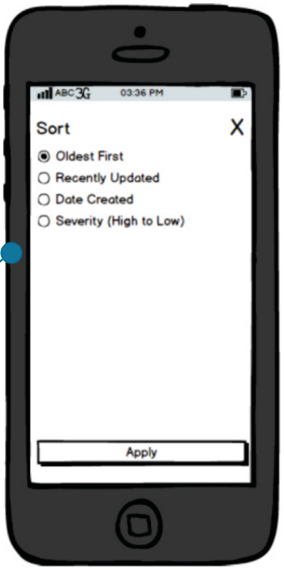
○ Infinity
○ Last 24 Hours
○ Last 7 Days
○ Last 15 Days
○ Last 30 Days
○ Last 45 Days
● Date Range

Timeframe

A coordinated attack can last for several hours, and come from multiple IP's. Being able to filter by timeframe would allow the CSO to focus on this.

Sorting

By using tabs in this way, the value proposition for the product was being obscured from the user and devalued.



Sort

● Oldest First
○ Recently Updated
○ Date Created
○ Severity (High to Low)

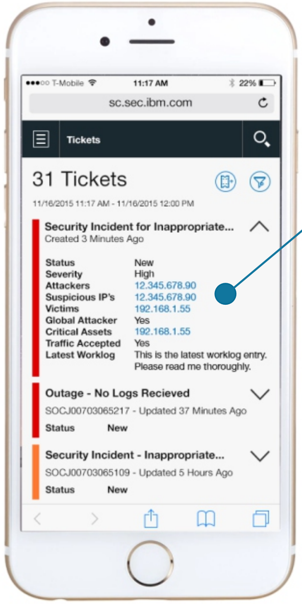
Final Version

Our final designs incorporated the IBM design language and included far more robust data for each event. The summary data displayed was tailored to the specific type of event. Where available, IP addresses were linked to IBM X-Force Exchange to provide more information about the traffic source. Any relevant blacklist information was also included.

Color was used to reinforce the severity indicated in the event details, following the client's established best practices. For example, an outage is always a high priority, while a security incident may turn out to be a false positive.

When creating a ticket, clients could select the type of incident or request, add notes, verify their identity, and provide a 1-5 star rating.

The final technology approach was to build this as a mobile-responsive web app to accelerate time to market and maintain a single codebase that could also support desktop use. To bring the project full circle, we integrated many of our mobile design concepts into the updated desktop designs and provided guidance to our development team on how the interface should respond across desktop, tablet, and mobile devices.



31 Tickets

11/16/2015 11:17 AM - 11/16/2015 12:00 PM

Security Incident for Inappropriate...
Created 3 Minutes Ago

Status	New
Severity	High
Attackers	12.345.678.90
Suspicious IP's	12.345.678.90
Victims	192.168.1.55
Global Attacker	Yes
Critical Assets	192.168.1.55
Traffic Accepted	Yes
Latest Worklog	This is the latest worklog entry. Please read me thoroughly.

Outage - No Logs Recieved
SOCJ00703065217 - Updated 37 Minutes Ago
Status New

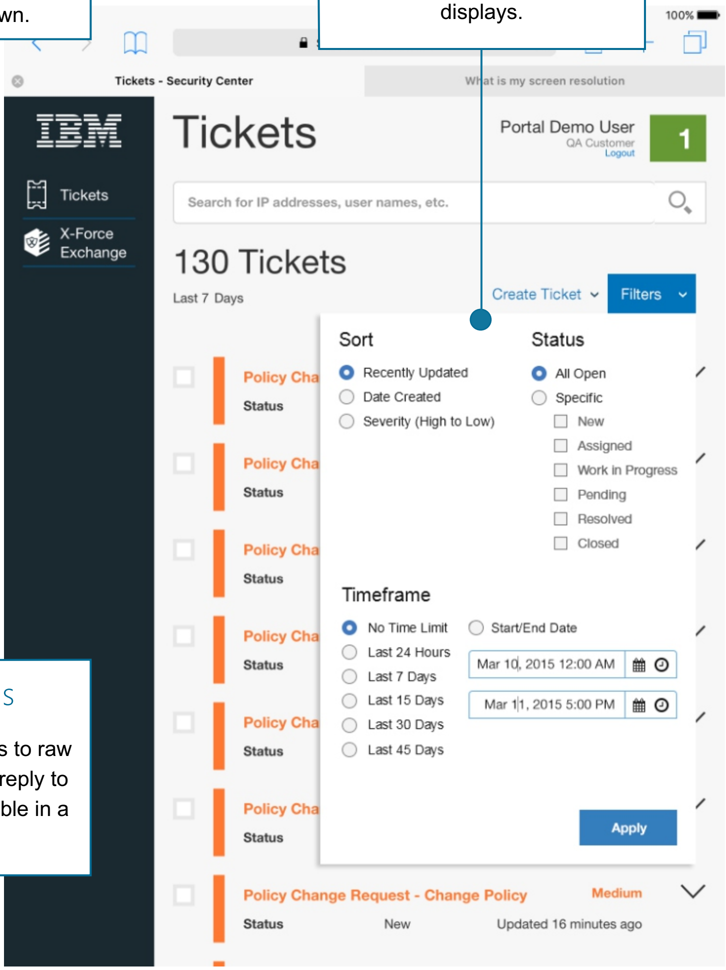
Security Incident - Inappropriate...
SOCJ00703065109 - Updated 5 Hours Ago
Status New

Ticket Summary

Unique summary details were defined based on the type of security event shown.

Streamlined Actions

Sorting and Filtering by timeframe were combined into a single feature across responsive displays.


100%
Tickets - Security Center
What is my screen resolution
IBM
Tickets
X-Force Exchange
Portal Demo User
QA Customer
Logout
1
Search for IP addresses, user names, etc.
Create Ticket
Filters
Apply

Tickets

130 Tickets

Last 7 Days

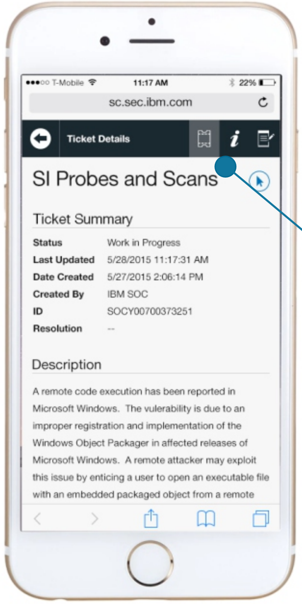
Sort
● Recently Updated
○ Date Created
○ Severity (High to Low)

Status
● All Open
○ Specific
□ New
□ Assigned
□ Work in Progress
□ Pending
□ Resolved
□ Closed

Timeframe
● No Time Limit
○ Last 24 Hours
○ Last 7 Days
○ Last 15 Days
○ Last 30 Days
○ Last 45 Days
○ Start/End Date
Mar 10, 2015 12:00 AM
Mar 11, 2015 5:00 PM

Policy Cha
Status

Policy Change Request - Change Policy Medium
Status New Updated 16 minutes ago



SI Probes and Scans

Ticket Summary

Status	Work in Progress
Last Updated	5/28/2015 11:17:31 AM
Date Created	5/27/2015 2:06:14 PM
Created By	IBM SOC
ID	SOCY00700373251
Resolution	--

Description

A remote code execution has been reported in Microsoft Windows. The vulerability is due to an improper registration and implementation of the Windows Object Packager in affected releases of Microsoft Windows. A remote attacker may exploit this issue by enticing a user to open an executable file with an embedded packaged object from a remote

Ticket Details

General Details, access to raw logs, and the ability to reply to the ticket were accessible in a revised header.

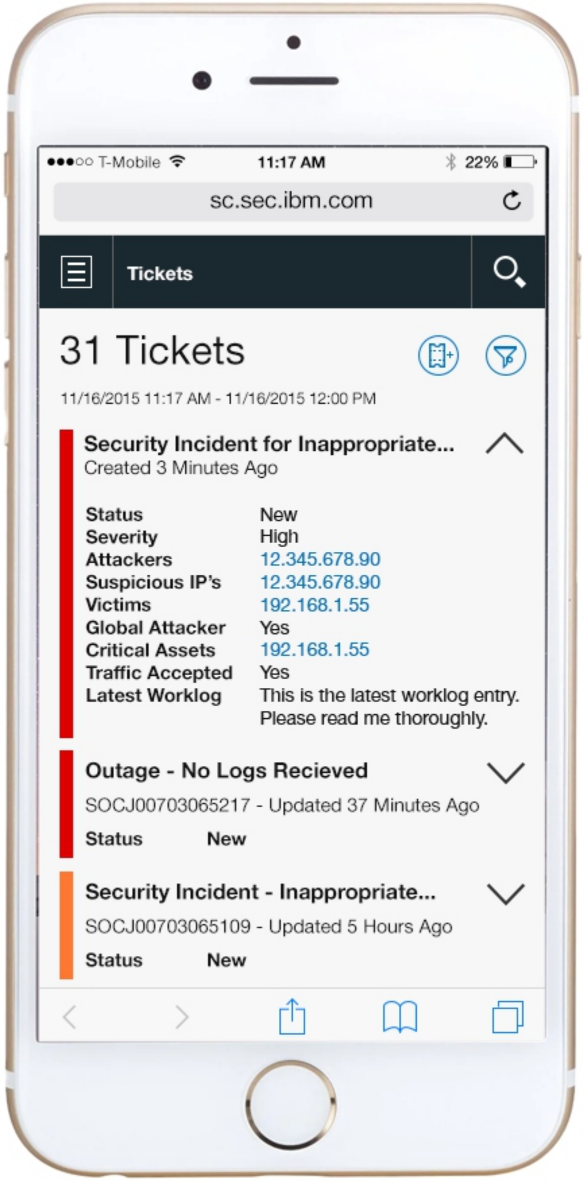
Summary

The MVP tickets app was delivered on schedule and built to spec. High marks were given by users for the ability to use the app on mobile devices, and with helping to prioritize their work.

As it relates to mobile design in the enterprise space, I am a firm believer that a mobile device does not replace a desktop, but rather is a tool that reflects a moment in time along the users journey. This project is a great example of that.

The ability to complete a threat investigation on a phone *could* be done. However, the research and behavior showed that it's more convenient to conduct deep analysis with multiple large screens and browser tabs which a phone, or even a tablet in 2015 was not going to support well.

Conversely. while we can bring laptops with us from meeting to meeting, carrying a full desktop around with us is just not practical. The ability to use the small form factor as a triage device, that can be used to prioritize their next steps is a great use of a portable, small form factor. I've continued to take this approach to mobile design projects in my career.



31 Tickets

11/16/2015 11:17 AM - 11/16/2015 12:00 PM

Security Incident for Inappropriate...
Created 3 Minutes Ago

Status	New
Severity	High
Attackers	12.345.678.90
Suspicious IP's	12.345.678.90
Victims	192.168.1.55
Global Attacker	Yes
Critical Assets	192.168.1.55
Traffic Accepted	Yes
Latest Worklog	This is the latest worklog entry. Please read me thoroughly.

Outage - No Logs Recieved
SOCJ00703065217 - Updated 37 Minutes Ago
Status New

Security Incident - Inappropriate...
SOCJ00703065109 - Updated 5 Hours Ago
Status New