

Unlocking User-Centered Design Methods for Building Cyber Security Visualizations

Sean McKenna^{1,2}, Diane Staheli², Miriah Meyer¹

¹ *University of Utah*

² *MIT Lincoln Laboratory*

motivation

user-centered design:

- incorporate user needs

for **cyber security**:

- user-centered design methods have been used

 - e.g. cyber command gauge cluster *[Erbacher 2012]*

- significant **challenges** for cyber security

**design methods can
overcome limited time
and access to users**

**qualitative
coding**

personas

**data
sketches**

redesign

dashboard

redesign of a software tool

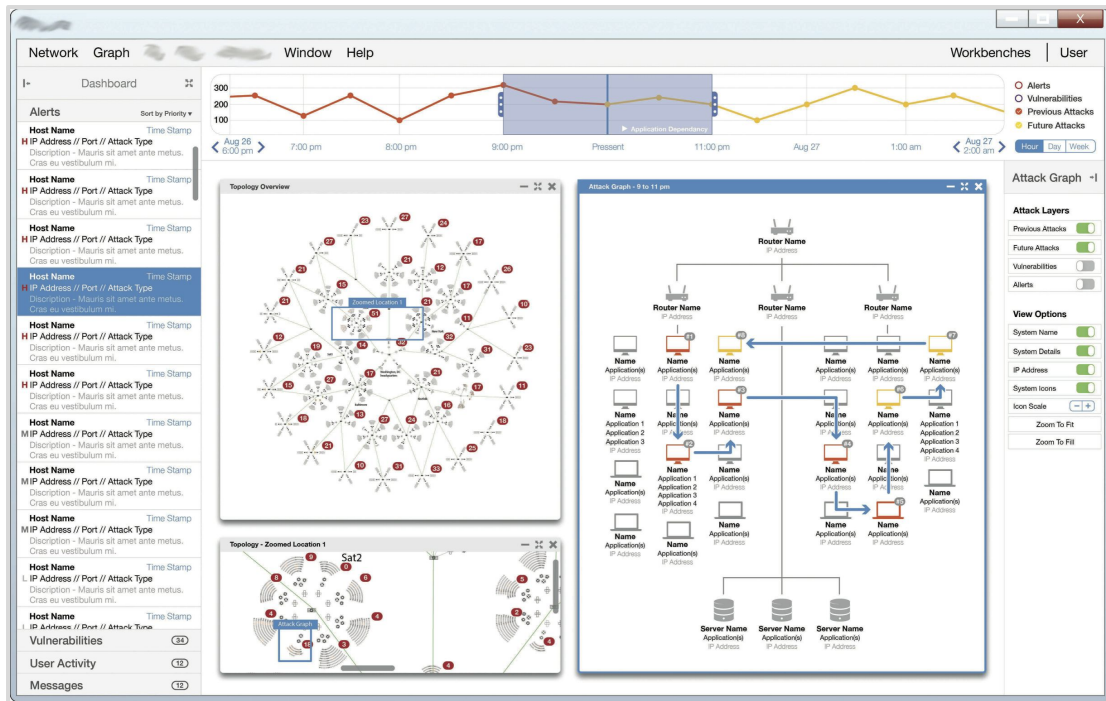
cyber security firm hired our team:

evaluate usability

find right visualizations

team was new to cyber security
and limited access to users

performed literature review to
begin to understand this space



cyber security dashboard

facilitate communication
of cyber information

different goals:

identify users

compare options

previous work focused
on analysts as users



qualitative coding



we had **too much** information!

detailed analysis of 3 papers:

cognitive task analysis (CTA)

key focus on users

qualitative coding:

structure, organizing and consolidating information [*Strauss & Corbin 1990*]

process:

find quotes, assign codes, meet to agree, and adapt codes

results of qualitative coding:

category	sub-category	sub-sub-category	evidence	author	pages
communities	attackers		"... increasingly sophisticated technical and social attacks from organized criminal operations"	D'Amico	19
data	external	website	"information published on hacker websites"	D'Amico	29
data	processed	report	"incident report, intrusion set, problem set from other organizations, information about the source and or sponsor of attack" & "incident reports are [often] textual documents"	D'Amico	35
data	raw	packets (data, netflow)	"network packet traffic, netflow data or host-based log data"	D'Amico	25
design guidelines	tutorial		"tutorial on how to get started; not just the user's manual certification process so people can become certified"	Erbacher	212
design guidelines	uncertainty visualization		"visualization should have a weight based on the accuracy of info" & "force-directed graphs where trust is the primary spring force"	Erbacher	210,212
other	metaphor		"Cyber security is essentially a human-on-human adversarial game played out by automated avatars."	Fink	46
phases	situational awareness	perception	"During the first stage, a CND analyst acquires data about the monitored environment, which is typical of the perceptual stage of situation awareness."	D'Amico	32
responsibilities	communication		"importance of analyst communication in the data transformation"	D'Amico	30
roles	managers		"most were active analysts; a few were managers"	D'Amico	23
roles	network analyst		"computer network defense (CND) analysts"	D'Amico	19
			"If a vulnerability scan returned a suspect IP address, he would then have to go through several different tools in different windows to get information about the IP, such as the host name, its location in the network or building,		

synthesized codes into **design opportunities:**

e.g. temporal visualization

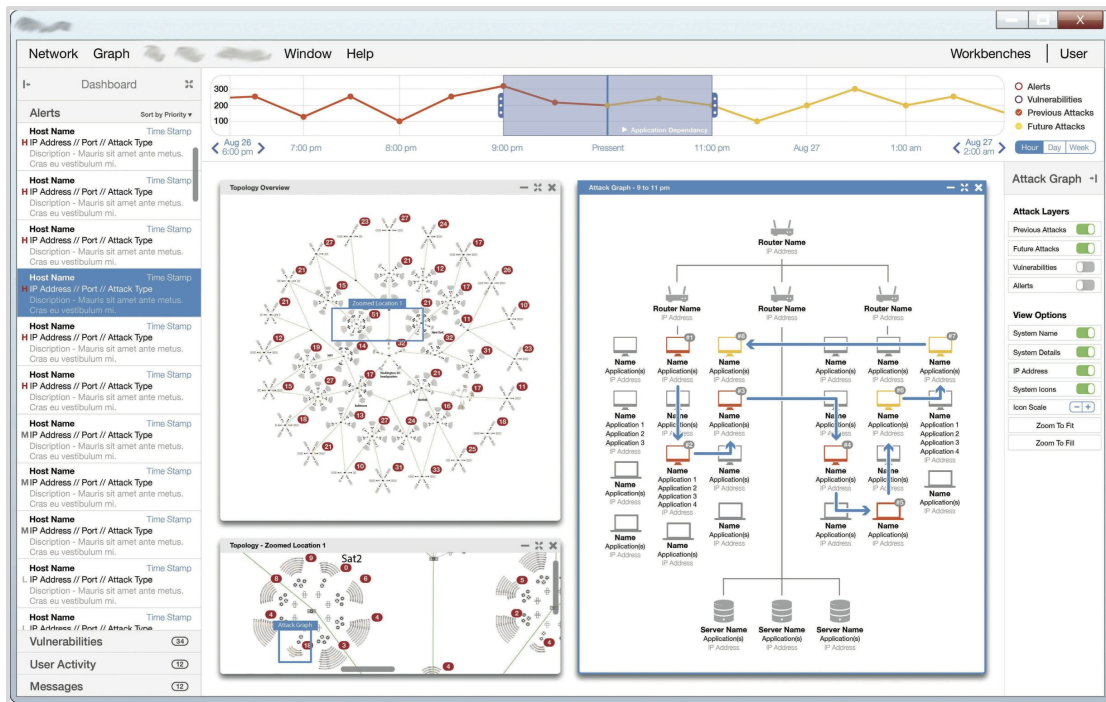
prioritized opportunities and
iterated into a mockup interface

cyber security firm:

developer made changes

evaluation (A/B testing)

deployed new version



reflections:

found user needs with limited access to users

effective method since resulted in a deployed tool

cannot replace access to real users

usage recommendation:

start small, expand your scope & code papers from appropriate venues:

e.g. VizSec, VIS, CHI, HFES, Behavior & Information Technology, Computers & Security, FIRST, HST, AMCIS, SAM, CyCon, FloCon, CogSIMA, DHS CATCH, HCI HAS, CTS SECOTS



what is a **persona**?

archetypes of users *[Martin & Hanington 2012]*

to build personas:

conducted **interviews** across various stakeholders

identified **four types** of personas:

analyst, manager, director of IT, and a CEO

specific to a cyber security dashboard



Cyber Analyst (information-gathering)

Goals	Identify anomalous network behavior		
Knowledge	Operations ●○○○○	Cyber ●●●●●	
Cyber SA	Attention ●●●●○	Temporal Window ←————→	
Key Questions	<ul style="list-style-type: none"> • What does my network look like? • What happened on the network last night? What's different? • Is something bad happening? • How was my network attacked? • Who is attacking my network? • Does this attack matter? • What did the bad guys do? 		



NOC Manager (information-synthesis)

Goals	Communicate impact on operations		
Knowledge	Operations ●●○○○	Cyber ●○○○○	
Cyber SA	Attention ●●●○○	Temporal Window ←———→	
Key Questions	<ul style="list-style-type: none"> • Does this attack matter? • How serious is the attack? • What do I do about the attack? • Are there any negative effects? • How successful was the attack? • What did the bad guys do? • What did the bad guys take? 		



Director of IT (decision-making)

Goals	Maintain cyber situational awareness		
Knowledge	Operations ●●●○○	Cyber ●●●○○	
Cyber SA	Attention ●●○○○	Temporal Window ←———→	
Key Questions	<ul style="list-style-type: none"> • Does this attack matter? • How serious is the attack? • What do I do about the attack? • Are there any negative effects? • What did the bad guys do/take? • Is it a good day on the network? • How is my network different from last week? 		



CEO (decision-making)

Goals	Coordinate personnel and operations		
Knowledge	Operations ●●●●●	Cyber ●○○○○	
Cyber SA	Attention ●○○○○	Temporal Window ←———→	
Key Questions	<ul style="list-style-type: none"> • How can we maintain ongoing operations? • What could happen if a critical system is impacted? • What are the most critical systems at risk of attack? • What cyber resources will be needed in the future? 		

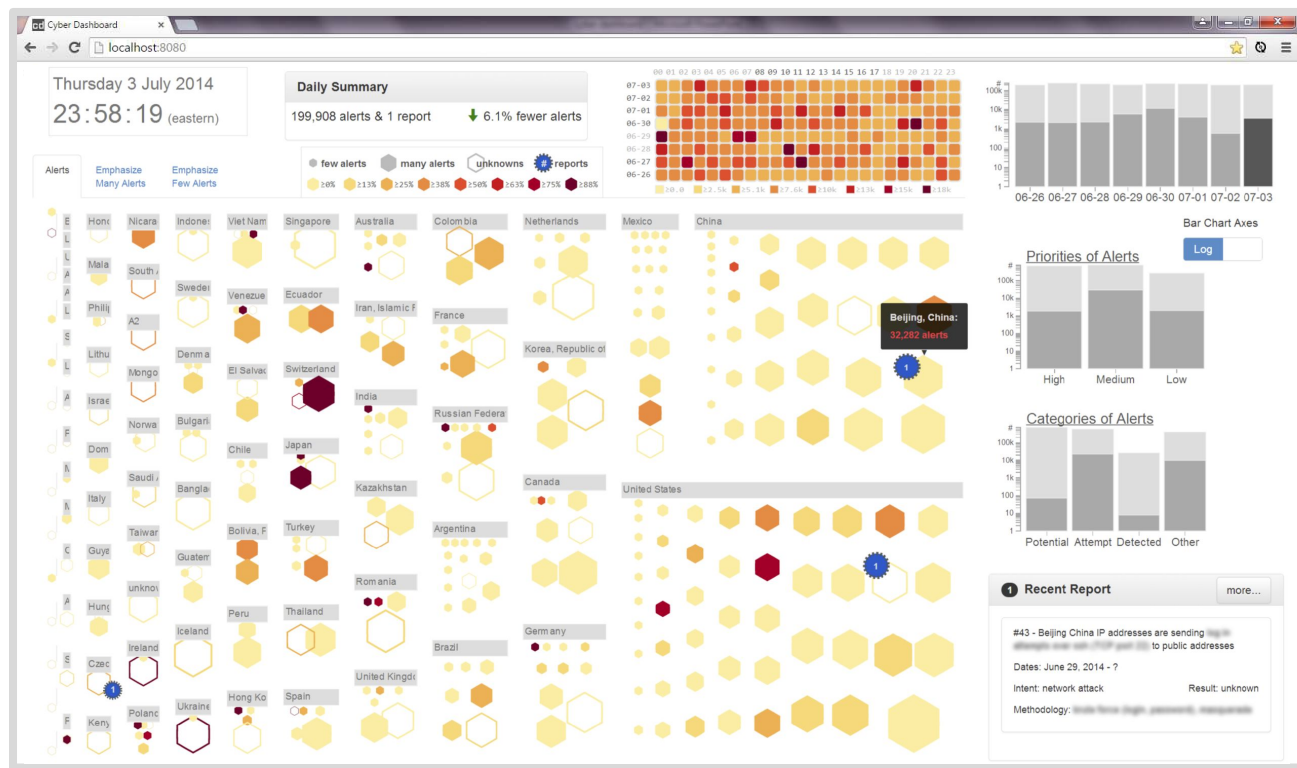
used personas to target users: analysts and managers

focus saved time

crafted ideas for a dashboard, prioritized against personas

first prototype produced

not deployed yet though



reflections:

limited our design focus to certain users

personas could be used in future projects

usage recommendation:

talk with real users, if possible, to build personas

otherwise, use existing research, like qualitative coding



<https://www.flickr.com/photos/nnova/2081056587/in/photostream/>

data sketches

what is a **data sketch**?

a quick and dirty visualization *[Lloyd & Dykes 2011]*

acquire data:

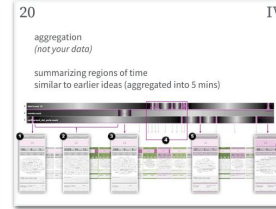
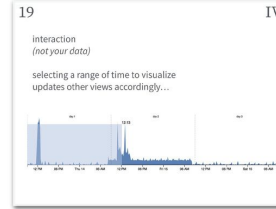
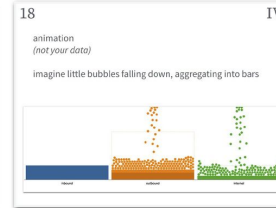
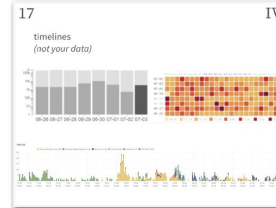
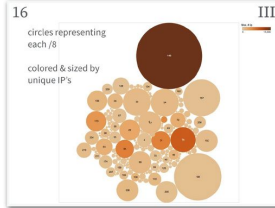
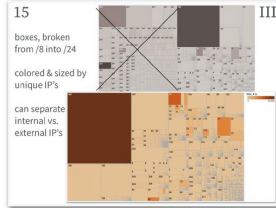
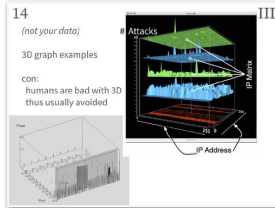
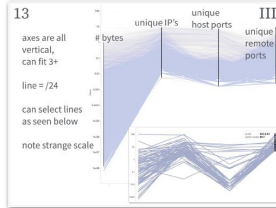
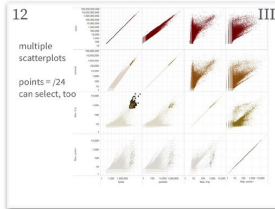
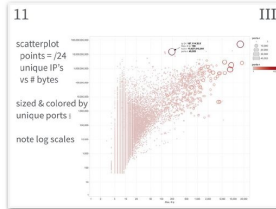
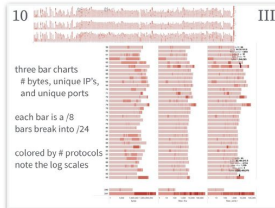
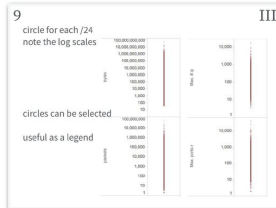
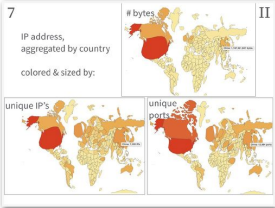
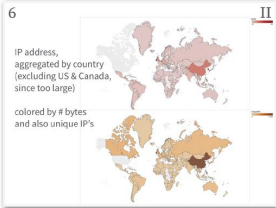
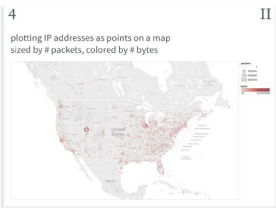
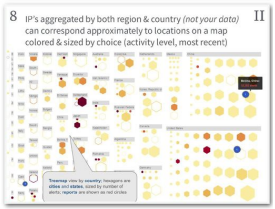
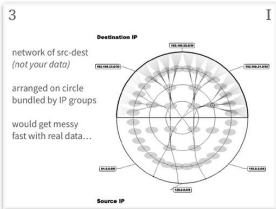
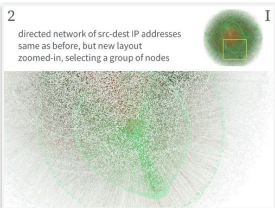
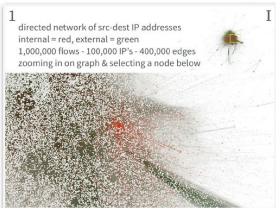
obtained a **network flow** dataset from an analyst at our university

visualize data:

brainstorm various ways to encode

what is the best way to represent data on a dashboard?

produced 20 data sketches using Python, Tableau, Gephi, and D3.js



feedback with analyst:

avoid complex
visualizations

clear aggregation

iterated on the design

evaluation:

tested usability

deployed to users



reflections:

effective for comparing multiple encodings

worked well for a use-case of a dashboard

complex visualizations may be useful for analysis

usage recommendation:

repurpose the tools you know and experiment with new ones:

e.g. Python, Tableau, Gephi, D3.js, Processing,
Excel, Spotfire, Arcsight, Splunk

design methods can overcome limited time and access to users

qualitative
coding


personas

data
sketches

redesign

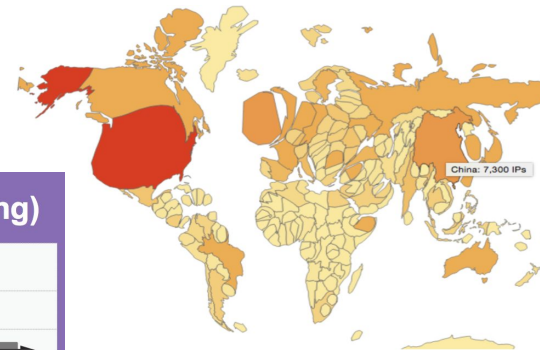
dashboard

category	sub-category	sub-sub-category	evidence
communities	attackers		"... increasingly sophisticated technical and social attacks from organized criminal operations"
data	external	website	"information published on hacker websites"
data	processed	report	"incident report, intrusion set, problem set from other organizations, information about the source and or sponsor of attack" & "incident reports are [often] textual documents"
data	raw	packets (data, netflow)	"network packet traffic, netflow data or host-based log data"
design guidelines	tutorial		"tutorial on how to get started; not just the user's manual ... certification process so people can become certified"
design guidelines	uncertainty visualization		"Visualization should have a weight based on the directed graphs where trust is the primary spring"
other	metaphor		"Cyber security is essentially a human-on-human out by automated avatars"
phases	situational awareness	perception	"During the first stage, a CND analyst acquires the environment, which is typical of the perceptual stage of awareness."
responsibilities	communication		"importance of analyst communication in the data"
roles	managers		"most were active analysts; a few were managers"
roles	network analyst		"computer network defense (CND) analysts"
workflows	investigate		"If a vulnerability scan returned a suspect IP address go through several different tools in different ways about the IP, such as the host name, its location, its OS version and update status, its owner, and its number."



Cyber Analyst (information-gathering)

Goals	Identify anomalous network behavior	
Knowledge	Operations ●○○○○	Cyber ●●●●●
Cyber SA	Attention ●●●●○	Temporal Window ←————→
Key Questions	<ul style="list-style-type: none"> • What does my network look like? • What happened on the network last night? What's different? • Is something bad happening? • How was my network attacked? • Who is attacking my network? • Does this attack matter? • What did the bad guys do? 	



to find out more:

sean@cs.utah.edu

<http://mckennapsean.com/vizsec-design-methods/>

acknowledgements: Jonzy, Dan Bowden, Tamara Denning, staff members at MIT Lincoln Laboratory, Dominika Mazur, Matthew Parkin, and James Agutter