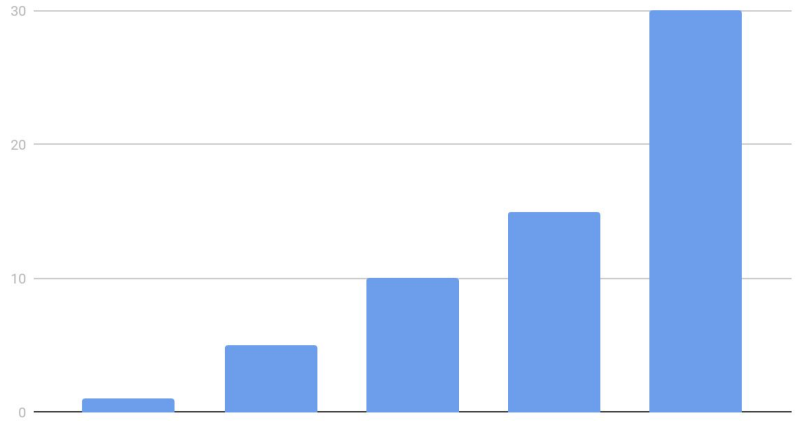
# User experience design

Or, “How to love your users without being all weird about it”

# What is user experience?

# Let’s talk about defects first

Cost to fix software defects



| Design and architecture | Implementation | Integration testing | Customer beta test | Postproduct release |
|---|---|---|---|---|
| 1X* | 5X | 10X | 15X | 30X |

*X is a normalized unit of cost and can be expressed in terms of person-hours, dollars, etc.
Source: National Institute of Standards and Technology (NIST)†

*By catching defects as early as possible in the development cycle, you can significantly reduce your development costs.*

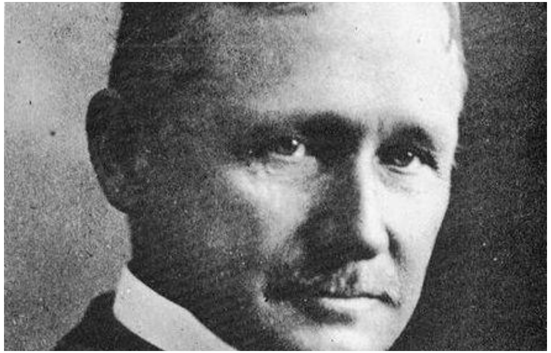
Developers have a technical understanding of “bugs”: implementations that do not match the specification.

End users aren’t so technical though, and don’t know what the software *should* be doing.

End users simply know that “this software doesn’t do what I want.”

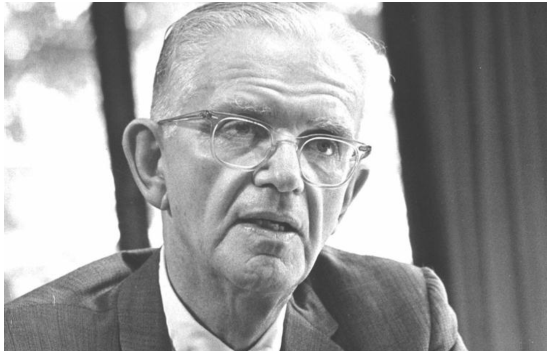
**How can we better understand what a user wants before delivering software?**

# Heros that have come before us



**Frederick Winslow Taylor**

Author of *The Principles of Scientific Management*, 1911



**Henry Dreyfuss**

Author of *Designing for People*, 1955

**Don Norman**

Author of *The Design of Everyday Things*, 1988

# Systems in service of their users

The common thread of these individuals isn’t software.

It’s in their focus on humans over systems.

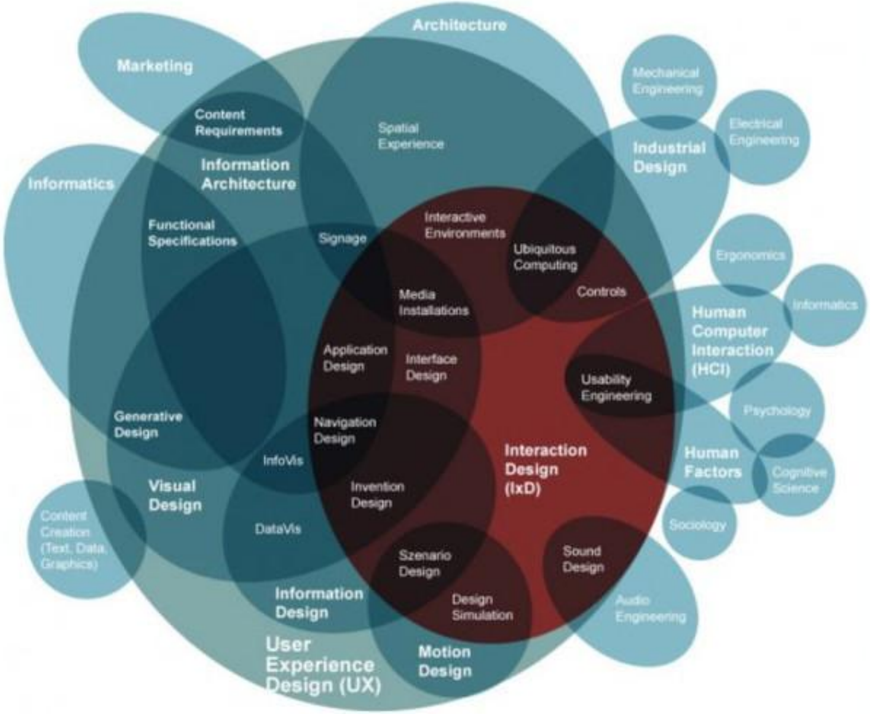
User experience design is about building systems that focus on the problems that people have.

# “I thought it was just about making things pretty”

The field of UX covers a broad range of topics, including visual design.

Appearance is an important factor of usability, but must be considered alongside many other objectives.

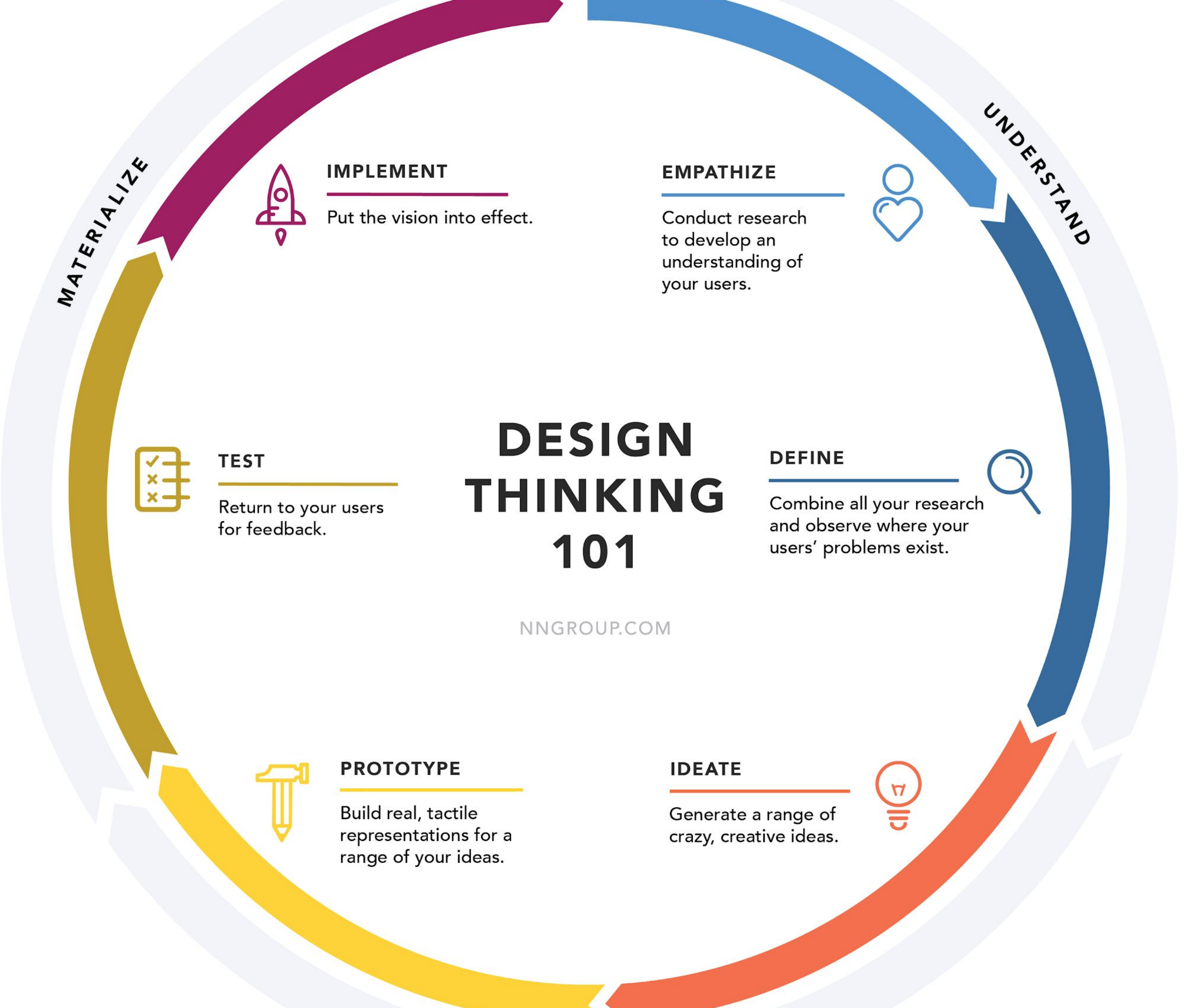
Remember Flash websites? That’s what you get when you focus on appearance instead of experience.



# User-centered design process

# A way of thinking

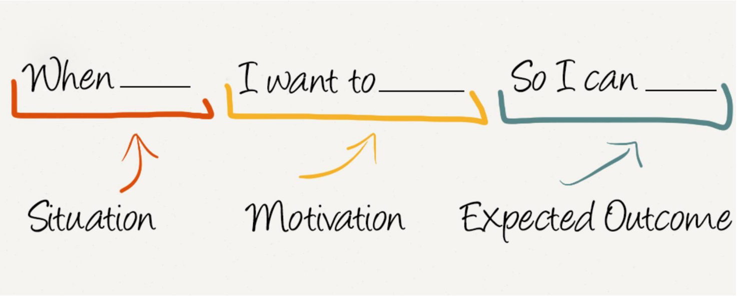
# A way of life



MATERIALIZE
UNDERSTAND
IMPLEMENT
Put the vision into effect.
EMPATHIZE
Conduct research to develop an understanding of your users.
TEST
Return to your users for feedback.
DESIGN THINKING 101
DEFINE
Combine all your research and observe where your users' problems exist.
NNGROUP.COM
PROTOTYPE
Build real, tactile representations for a range of your ideas.
IDEATE
Generate a range of crazy, creative ideas.

# Discovery phase

Talk to users to find and understand their needs. Learn who they are, how they work, what they like and dislike. Focus solely on the users' needs, not on solutions.



**Tools**

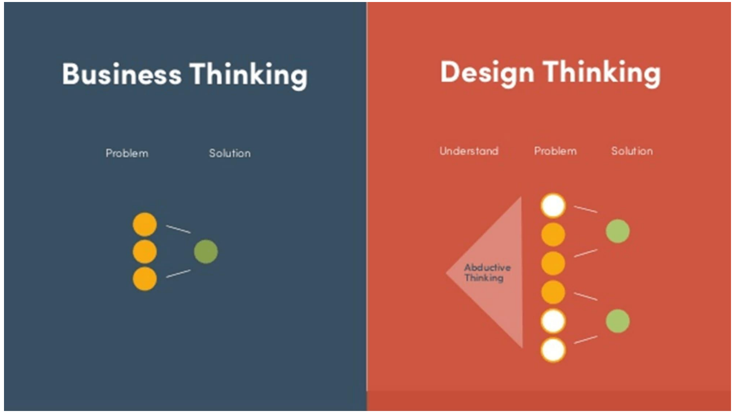
- Empathy
- User interviews
- Diary studies
- Surveys
- Journey mapping
- User analytics

**Output**

- Personas
- User stories

# Exploration phase

Look at the user problems from multiple angles. Try lots of ideas, especially crazy ones. Don't settle on any solution too early. Build hypotheses and prototypes.



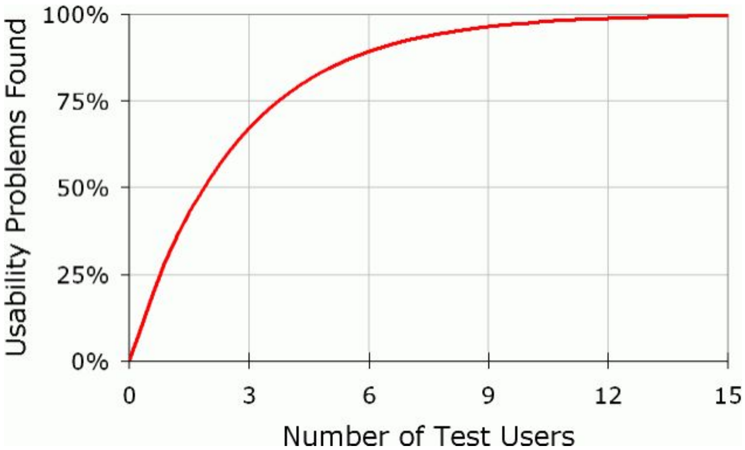
**Tools**

- Sketching
- Diagramming
- Competitive analysis
- Design reviews

**Output**

- Flows
- Wireframes
- Hi-fi comps
- Interactive prototypes

Conduct experiments with real users to confirm or reject your design hypotheses. Continue to watch for new, unseen issues!



**Tools**

- Usability study
- Wizard of Oz study
- Card sort study
- Expert (of usability) review
- A/B tests

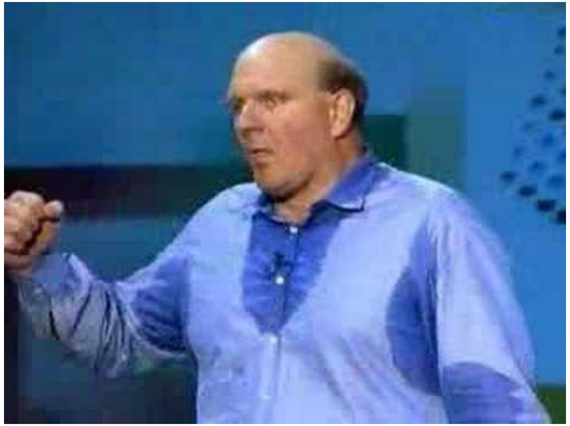
**Output**

- Confirmed or rejected hypothesis
- New problems to address — either for design under test or system as a whole

# Validation phase

# Delivery phase

Take the verified designs and create real software from them. Apply good software practices and make something we can build upon. Get the software into users' hands.



**Tools**

- Developers, developers, developers!
- Design systems

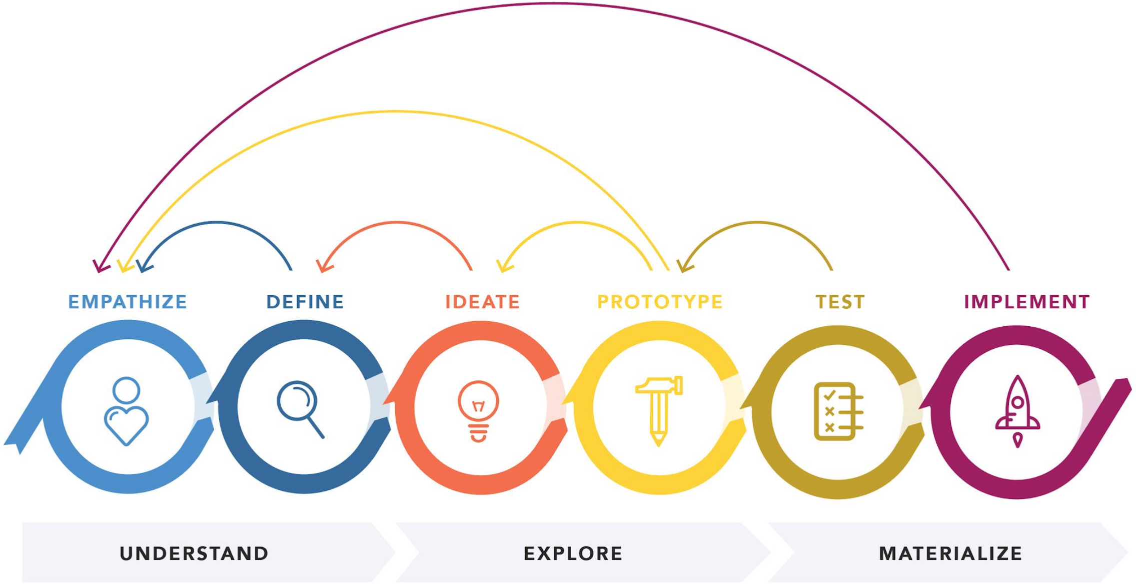
**Output**

- Production-grade software
- Happy users 😍

# Lather, rinse, repeat

This process gives you ample chances to step back and reevaluate.

Even once you've reached the "end", you can always go back to listening to your users.



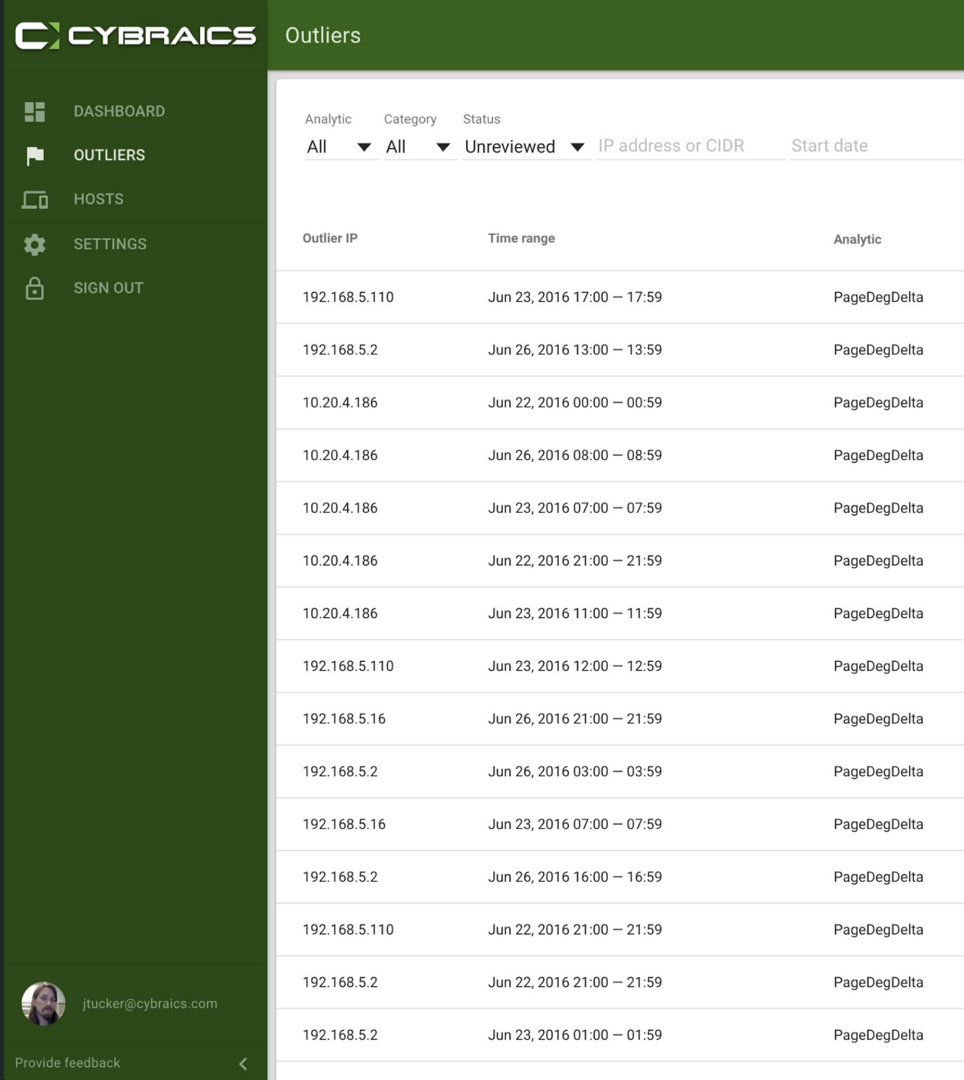
# “Case” study

# nLighten 0.5

The only fully-developed concept in the UI was “Outliers”.

Customer presentations were created by gathering links to outliers and publishing them in a PPT with some explanatory copy.

Strategically, this sucked.



Outliers

Analytic: All
Category: All
Status: Unreviewed
IP address or CIDR
Start date

| Outlier IP | Time range | Analytic |
|---|---|---|
| 192.168.5.110 | Jun 23, 2016 17:00 — 17:59 | PageDegDelta |
| 192.168.5.2 | Jun 26, 2016 13:00 — 13:59 | PageDegDelta |
| 10.20.4.186 | Jun 22, 2016 00:00 — 00:59 | PageDegDelta |
| 10.20.4.186 | Jun 26, 2016 08:00 — 08:59 | PageDegDelta |
| 10.20.4.186 | Jun 23, 2016 07:00 — 07:59 | PageDegDelta |
| 10.20.4.186 | Jun 22, 2016 21:00 — 21:59 | PageDegDelta |
| 10.20.4.186 | Jun 23, 2016 11:00 — 11:59 | PageDegDelta |
| 192.168.5.110 | Jun 23, 2016 12:00 — 12:59 | PageDegDelta |
| 192.168.5.16 | Jun 26, 2016 21:00 — 21:59 | PageDegDelta |
| 192.168.5.2 | Jun 26, 2016 03:00 — 03:59 | PageDegDelta |
| 192.168.5.16 | Jun 23, 2016 07:00 — 07:59 | PageDegDelta |
| 192.168.5.2 | Jun 26, 2016 16:00 — 16:59 | PageDegDelta |
| 192.168.5.110 | Jun 22, 2016 21:00 — 21:59 | PageDegDelta |
| 192.168.5.2 | Jun 22, 2016 21:00 — 21:59 | PageDegDelta |
| 192.168.5.2 | Jun 23, 2016 01:00 — 01:59 | PageDegDelta |

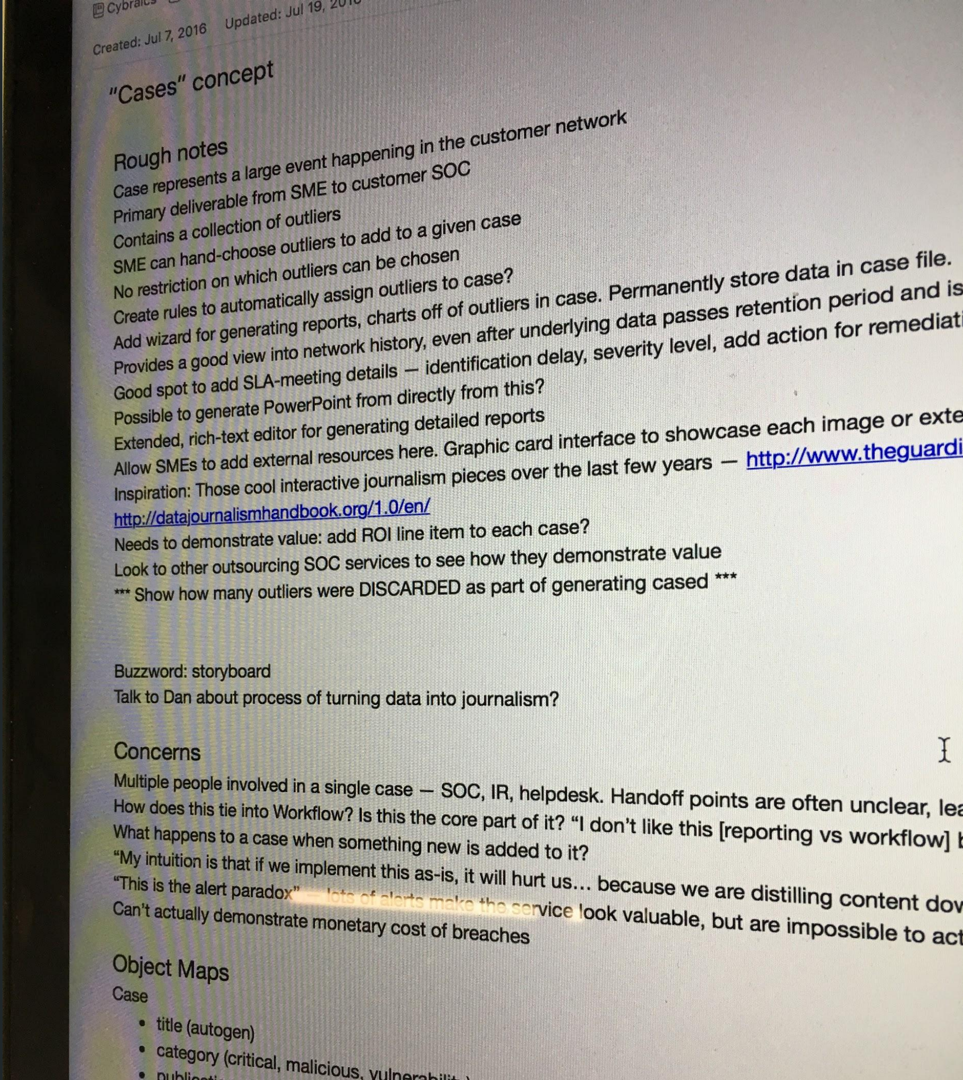
# A new concept

“How can we engage the customer directly within the product?”

Explored the problem space and generated lots of new ideas.

Some became foundation of nLighten’s Cases concept.

Many never saw the light of day.



Cybraics

Created: Jul 7, 2016 Updated: Jul 19, 201

"Cases" concept

Rough notes

Case represents a large event happening in the customer network
Primary deliverable from SME to customer SOC
Contains a collection of outliers
SME can hand-choose outliers to add to a given case
No restriction on which outliers can be chosen
Create rules to automatically assign outliers to case?
Add wizard for generating reports, charts off of outliers in case. Permanently store data in case file.
Provides a good view into network history, even after underlying data passes retention period and is
Good spot to add SLA-meeting details — identification delay, severity level, add action for remediat
Possible to generate PowerPoint from directly from this?
Extended, rich-text editor for generating detailed reports
Allow SMEs to add external resources here. Graphic card interface to showcase each image or exte
Inspiration: Those cool interactive journalism pieces over the last few years — http://www.theguardi
http://datajournalismhandbook.org/1.0/en/
Needs to demonstrate value: add ROI line item to each case?
Look to other outsourcing SOC services to see how they demonstrate value
*** Show how many outliers were DISCARDED as part of generating cased ***

Buzzword: storyboard
Talk to Dan about process of turning data into journalism?

Concerns

Multiple people involved in a single case — SOC, IR, helpdesk. Handoff points are often unclear, lea
How does this tie into Workflow? Is this the core part of it? “I don’t like this [reporting vs workflow] b
What happens to a case when something new is added to it?
“My intuition is that if we implement this as-is, it will hurt us… because we are distilling content dov
“This is the alert paradox” — lots of alerts make the service look valuable, but are impossible to act
Can’t actually demonstrate monetary cost of breaches

Object Maps

Case

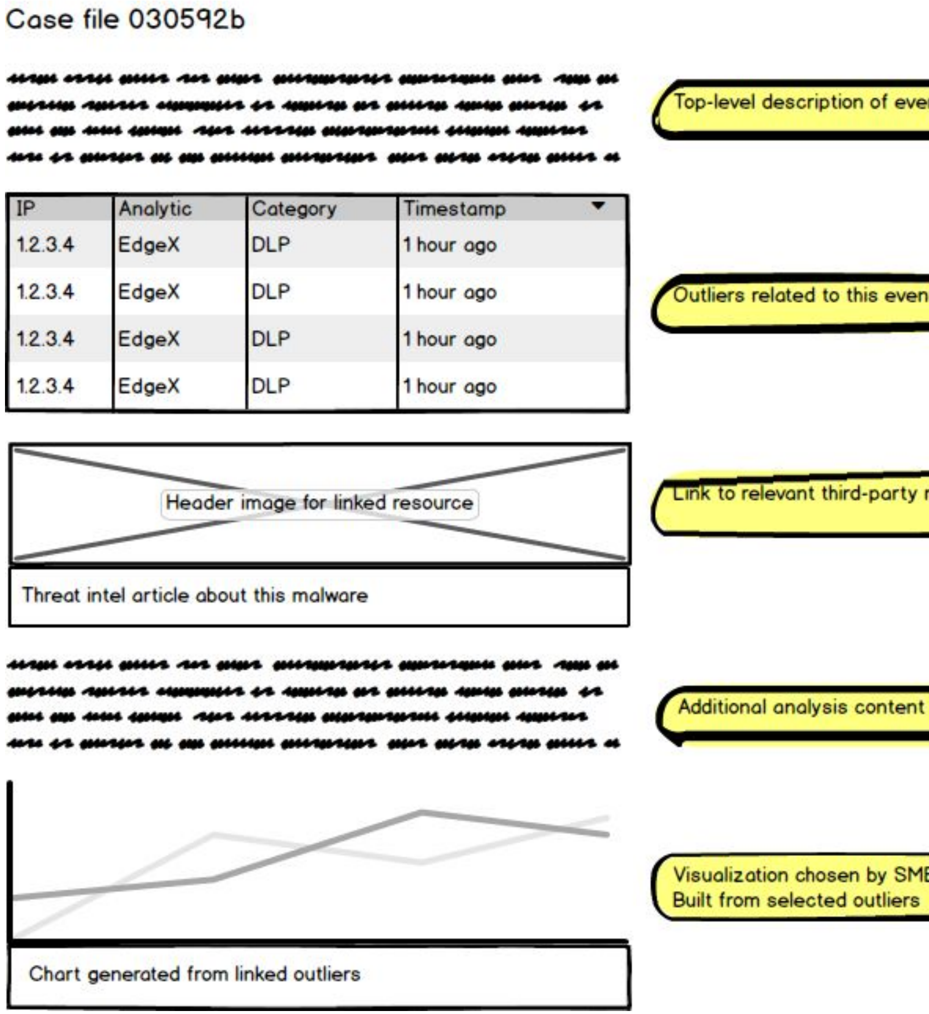
- title (autogen)
- category (critical, malicious, vulnerabilit
- publicati

# Building an experiment

Want to validate the concept (“Cases will help us communicate with customers”) and the prototype (a system for working with Cases).

Test goals

1. Navigating to “Cases”
2. Creating a new case
3. Adding a link to a third-party article
4. Uploading an attachment
5. Linking outliers
6. Publishing a case



Case file 030592b

| IP | Analytic | Category | Timestamp ▼ |
|---|---|---|---|
| 1.2.3.4 | EdgeX | DLP | 1 hour ago |
| 1.2.3.4 | EdgeX | DLP | 1 hour ago |
| 1.2.3.4 | EdgeX | DLP | 1 hour ago |
| 1.2.3.4 | EdgeX | DLP | 1 hour ago |

Header image for linked resource

Threat intel article about this malware

Chart generated from linked outliers

Top-level description of eve

Outliers related to this even

Link to relevant third-party r

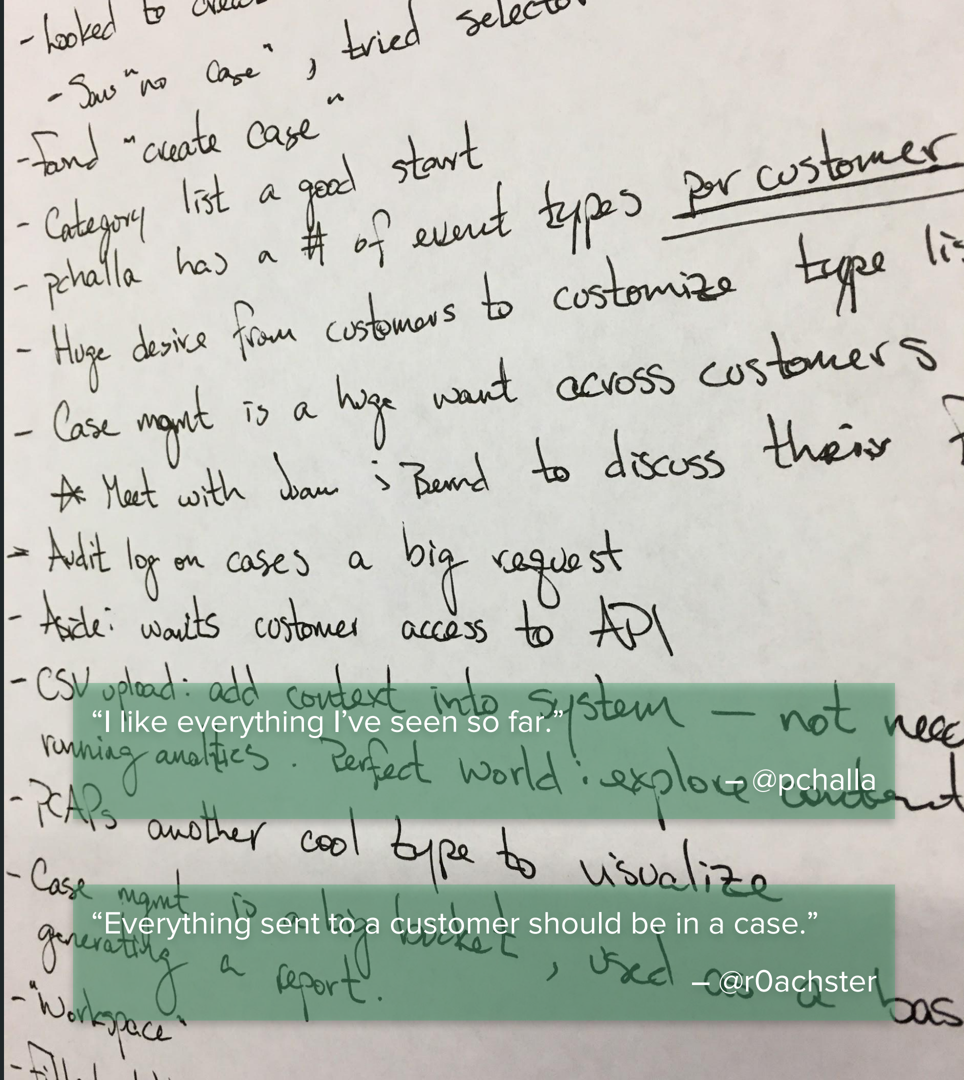
Additional analysis content

Visualization chosen by SME
Built from selected outliers

# Hypothesis confirmed!

Conducted user interviews with our existing SOC staff. The idea resonated well and the prototype worked.

| Task | Failed | Assisted | Succeeded |
|---|---|---|---|
| Creating a case | 0 | 1 | 2 |
| Adding link to third-party article | 0 | 0 | 3 |
| Uploading an attachment | 0 | 0 | 3 |
| Linking outliers to case | 0 | 1 | 2 |
| Publishing a case | 0 | 0 | 3 |



- looked to creat… tried selecto…
 - Saw "no case",
- Found "create case"
- Category list a good start
- pchalla has a # of event types per customer
- Huge desire from customers to customize type li…
- Case mgmt is a huge want across customers
 ✱ Meet with Juan & Bernd to discuss their …
→ Audit log on cases a big request
- Aside: wants customer access to API
- CSV upload: add context into system — not nece…
 running analytics. Perfect world: explore content
- PCAPs another cool type to visualize
- Case mgmt is a big bucket, used as a bas…
 generating a report.
- "Workspace"
- Fill…

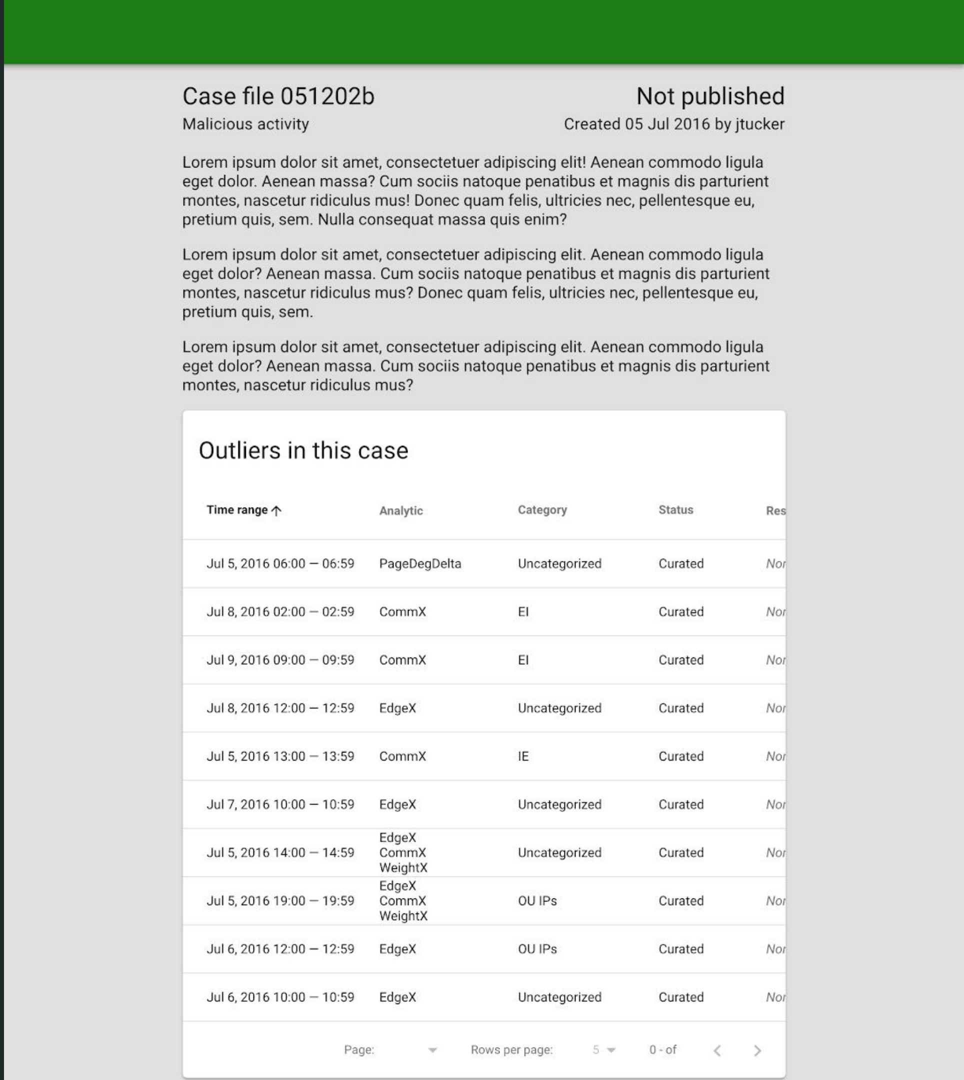
> "I like everything I've seen so far."
>
> – @pchalla

> "Everything sent to a customer should be in a case."
>
> – @r0achster

# Cases v1.0

Now validated, we built the Cases concept into nLighten v1.1.0. It became a central part of the UI and our service offering.

Everyone lived happily ever after.



Case file 051202b

Malicious activity

Not published

Created 05 Jul 2016 by jtucker

Lorem ipsum dolor sit amet, consectetuer adipiscing elit! Aenean commodo ligula eget dolor. Aenean massa? Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus! Donec quam felis, ultricies nec, pellentesque eu, pretium quis, sem. Nulla consequat massa quis enim?

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Aenean commodo ligula eget dolor? Aenean massa. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus? Donec quam felis, ultricies nec, pellentesque eu, pretium quis, sem.

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Aenean commodo ligula eget dolor? Aenean massa. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus?

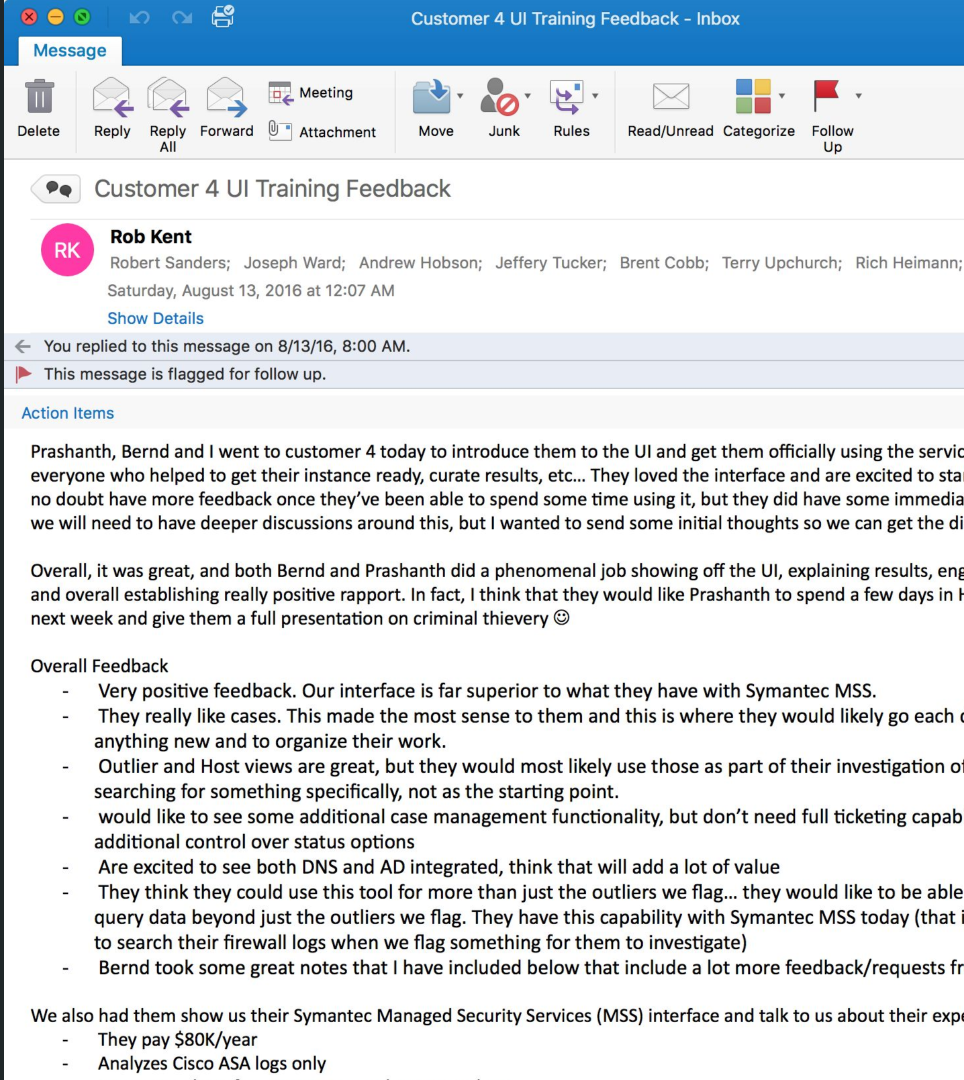
Outliers in this case

| Time range ↑ | Analytic | Category | Status | Res |
|---|---|---|---|---|
| Jul 5, 2016 06:00 – 06:59 | PageDegDelta | Uncategorized | Curated | Nor |
| Jul 8, 2016 02:00 – 02:59 | CommX | EI | Curated | Nor |
| Jul 9, 2016 09:00 – 09:59 | CommX | EI | Curated | Nor |
| Jul 8, 2016 12:00 – 12:59 | EdgeX | Uncategorized | Curated | Nor |
| Jul 5, 2016 13:00 – 13:59 | CommX | IE | Curated | Nor |
| Jul 7, 2016 10:00 – 10:59 | EdgeX | Uncategorized | Curated | Nor |
| Jul 5, 2016 14:00 – 14:59 | EdgeX<br>CommX<br>WeightX | Uncategorized | Curated | Nor |
| Jul 5, 2016 19:00 – 19:59 | EdgeX<br>CommX<br>WeightX | OU IPs | Curated | Nor |
| Jul 6, 2016 12:00 – 12:59 | EdgeX | OU IPs | Curated | Nor |
| Jul 6, 2016 10:00 – 10:59 | EdgeX | Uncategorized | Curated | Nor |

# A new challenger approaches!

After a few months, new feedback from sales, customers, and SOC staff starts coming in:

- Case presentation is messy and inconsistent
- Hard to standardize and surface common data
- No obvious way to integrate into workflow



Customer 4 UI Training Feedback

Rob Kent

Robert Sanders; Joseph Ward; Andrew Hobson; Jeffery Tucker; Brent Cobb; Terry Upchurch; Rich Heimann;

Saturday, August 13, 2016 at 12:07 AM

Show Details

You replied to this message on 8/13/16, 8:00 AM.

This message is flagged for follow up.

Action Items

Prashanth, Bernd and I went to customer 4 today to introduce them to the UI and get them officially using the servic
everyone who helped to get their instance ready, curate results, etc… They loved the interface and are excited to sta
no doubt have more feedback once they've been able to spend some time using it, but they did have some immedia
we will need to have deeper discussions around this, but I wanted to send some initial thoughts so we can get the di

Overall, it was great, and both Bernd and Prashanth did a phenomenal job showing off the UI, explaining results, eng
and overall establishing really positive rapport. In fact, I think that they would like Prashanth to spend a few days in h
next week and give them a full presentation on criminal thievery ☺

Overall Feedback

- Very positive feedback. Our interface is far superior to what they have with Symantec MSS.
- They really like cases. This made the most sense to them and this is where they would likely go each anything new and to organize their work.
- Outlier and Host views are great, but they would most likely use those as part of their investigation o searching for something specifically, not as the starting point.
- would like to see some additional case management functionality, but don't need full ticketing capab additional control over status options
- Are excited to see both DNS and AD integrated, think that will add a lot of value
- They think they could use this tool for more than just the outliers we flag… they would like to be able query data beyond just the outliers we flag. They have this capability with Symantec MSS today (that i to search their firewall logs when we flag something for them to investigate)
- Bernd took some great notes that I have included below that include a lot more feedback/requests fr

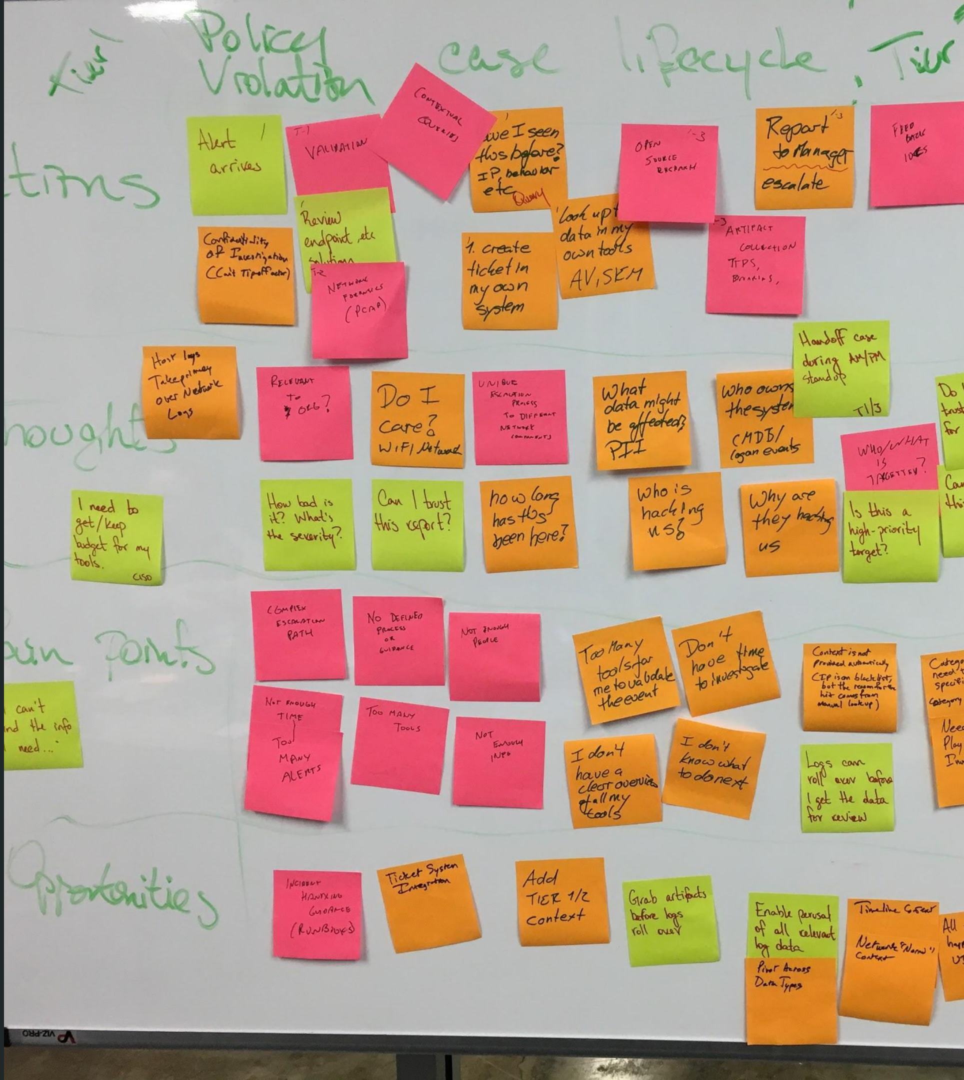
We also had them show us their Symantec Managed Security Services (MSS) interface and talk to us about their expe

- They pay $80K/year
- Analyzes Cisco ASA logs only

# Back to research

Hosted a Journey Mapping session with our SOC to understand what a typical SOC incident lifecycle looks like.

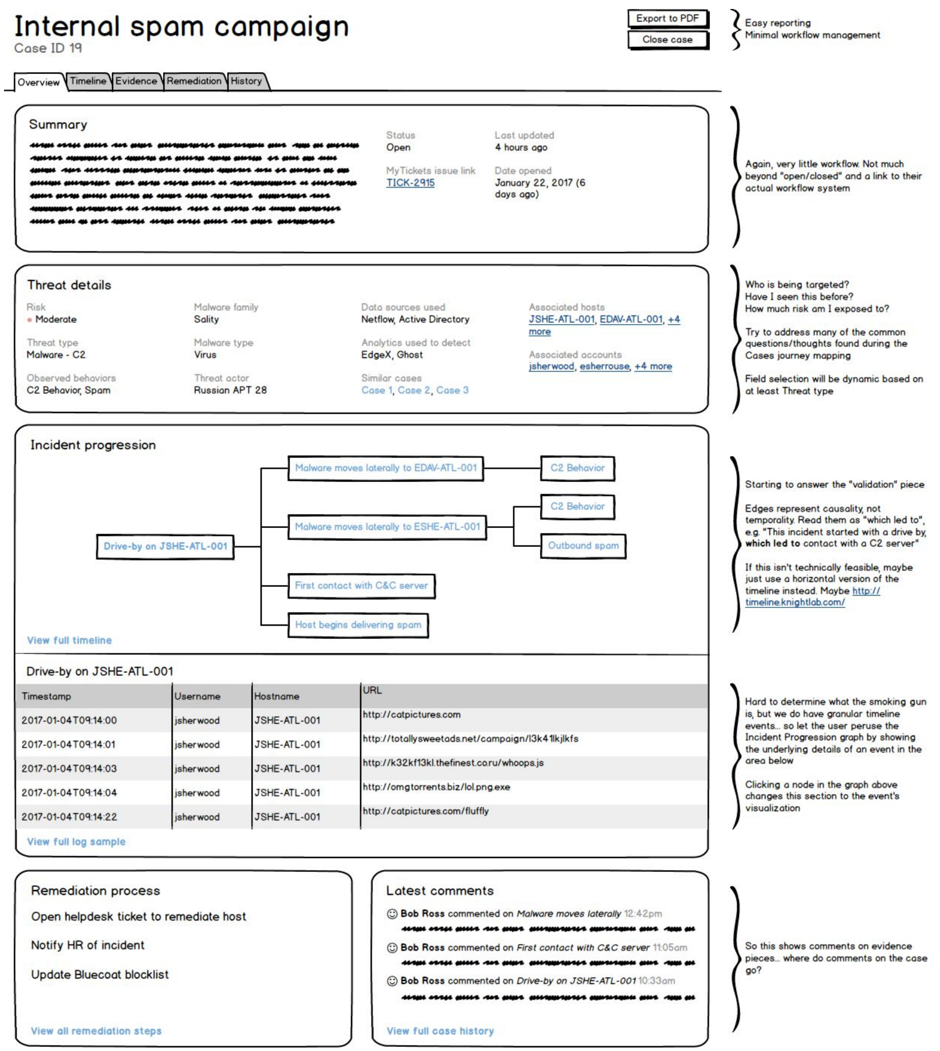
It revealed many opportunities we had to extend "Cases" in a way that made them more actionable to our customers.



Policy Violation
case lifecycle
Tier
Actions
Thoughts
Pain Points
Opportunities
Alert arrives
Validation
Contextual Queries
Have I seen this before? IP, behavior etc Query
Open Source Research
Report to Manager escalate
Feed back loops
Review endpoint etc solutions
Confidentiality of Investigation (Can't Tip off actor)
Network Forensics (PCAP)
1. create ticket in my own system
Look up data in my own tools AV, SIEM
Artifact Collection TTPs, Binaries,
Handoff case during AM/PM standup
Hour logs Take primary over Network Logs
Relevant to org?
Do I care? WiFi Network
Unique Escalation Process to different network components
What data might be affected? PII
Who owns the system CMDB/logon events
Who/what is targeted?
I need to get/keep budget for my tools. CISO
How bad is it? What's the severity?
Can I trust this report?
how long has this been here?
who is hacking us?
Why are they hacking us
Is this a high-priority target?
Complex Escalation Path
No Defined Process or Guidance
Not enough people
Too many tools for me to validate the event
Don't have time to investigate
Context is not provided automatically (IP is on blacklist, but the reason for the hit comes from manual lookup)
can't find the info need...
Not enough time
Too many alerts
Too many tools
Not enough info
I don't have a clear overview of all my tools
I don't know what to do next
Logs can roll over before I get the data for review
Incident Handling Guidance (Runbooks)
Ticket System Integration
Add Tier 1/2 context
Grab artifacts before logs roll over
Enable perusal of all relevant log data
Pivot Across Data Types
Timeline Context
Network "Normal" Context
VIZ-PRO

# Another experiment

Iterated on design significantly. Went through 3-4 concept iterations before settling on a likely winner.



Export to PDF
Close case
Overview
Timeline
Evidence
Remediation
History
Malware moves laterally to EDAV-ATL-001
C2 Behavior
C2 Behavior
Malware moves laterally to ESHE-ATL-001
Outbound spam
Drive-by on JSHE-ATL-001
First contact with C&C server
Host begins delivering spam

## Internal spam campaign

Case ID 19

Easy reporting
Minimal workflow management

### Summary

Status
Open

Last updated
4 hours ago

MyTickets issue link
TICK-2915

Date opened
January 22, 2017 (6 days ago)

Again, very little workflow. Not much beyond "open/closed" and a link to their actual workflow system

### Threat details

Risk
● Moderate

Threat type
Malware - C2

Observed behaviors
C2 Behavior, Spam

Malware family
Sality

Malware type
Virus

Threat actor
Russian APT 28

Data sources used
Netflow, Active Directory

Analytics used to detect
EdgeX, Ghost

Similar cases
Case 1, Case 2, Case 3

Associated hosts
JSHE-ATL-001, EDAV-ATL-001, +4 more

Associated accounts
jsherwood, esherrouse, +4 more

Who is being targeted?
Have I seen this before?
How much risk am I exposed to?

Try to address many of the common questions/thoughts found during the Cases journey mapping

Field selection will be dynamic based on at least Threat type

### Incident progression

View full timeline

Starting to answer the "validation" piece

Edges represent causality, not temporality. Read them as "which led to", e.g. "This incident started with a drive by, **which led to** contact with a C2 server"

If this isn't technically feasible, maybe just use a horizontal version of the timeline instead. Maybe http://timeline.knightlab.com/

Drive-by on JSHE-ATL-001

| Timestamp | Username | Hostname | URL |
|---|---|---|---|
| 2017-01-04T09:14:00 | jsherwood | JSHE-ATL-001 | http://catpictures.com |
| 2017-01-04T09:14:01 | jsherwood | JSHE-ATL-001 | http://totallysweetads.net/campaign/l3k41lkjlkfs |
| 2017-01-04T09:14:03 | jsherwood | JSHE-ATL-001 | http://k32kf13kl.thefinest.co.ru/whoops.js |
| 2017-01-04T09:14:04 | jsherwood | JSHE-ATL-001 | http://omgtorrents.biz/lol.png.exe |
| 2017-01-04T09:14:22 | jsherwood | JSHE-ATL-001 | http://catpictures.com/fluffly |

View full log sample

Hard to determine what the smoking gun is, but we do have granular timeline events... so let the user peruse the Incident Progression graph by showing the underlying details of an event in the area below

Clicking a node in the graph above changes this section to the event's visualization

### Remediation process

Open helpdesk ticket to remediate host

Notify HR of incident

Update Bluecoat blocklist

View all remediation steps

### Latest comments

☺ **Bob Ross** commented on *Malware moves laterally* 12:42pm

☺ **Bob Ross** commented on *First contact with C&C server* 11:05am

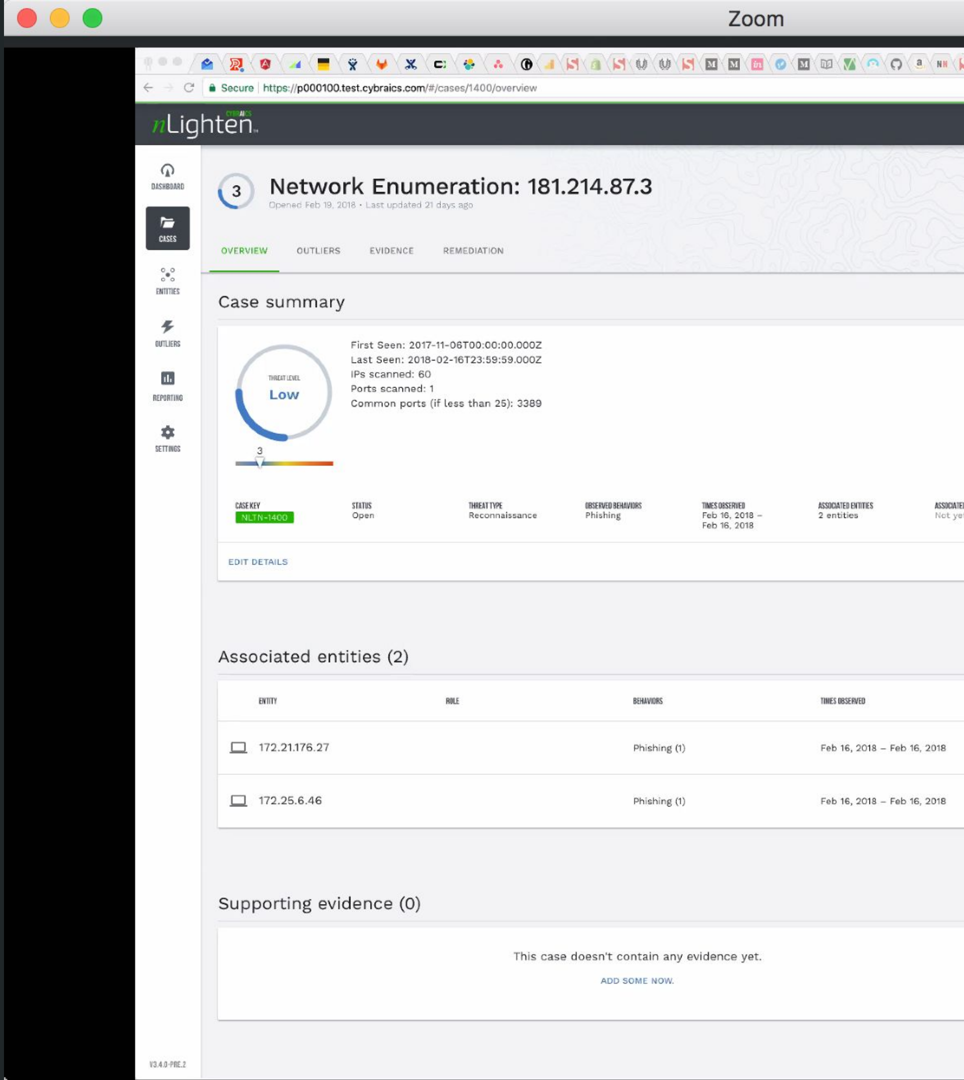
☺ **Bob Ross** commented on *Drive-by on JSHE-ATL-001* 10:33am

View full case history

So this shows comments on evidence pieces... where do comments on the case go?

# Expert approved!

Conducted user interviews with SOC and industry professionals.



## Network Enumeration: 181.214.87.3

Opened Feb 19, 2018 • Last updated 21 days ago

### Case summary

First Seen: 2017-11-06T00:00:00.000Z
Last Seen: 2018-02-16T23:59:59.000Z
IPs scanned: 60
Ports scanned: 1
Common ports (if less than 25): 3389

| CASE KEY | STATUS | THREAT TYPE | OBSERVED BEHAVIORS | TIMES OBSERVED | ASSOCIATED ENTITIES | ASSOCIATE |
|---|---|---|---|---|---|---|
| NLTN-1400 | Open | Reconnaissance | Phishing | Feb 16, 2018 – Feb 16, 2018 | 2 entities | Not ye |

### Associated entities (2)

| ENTITY | ROLE | BEHAVIORS | TIMES OBSERVED |
|---|---|---|---|
| 172.21.176.27 | | Phishing (1) | Feb 16, 2018 – Feb 16, 2018 |
| 172.25.6.46 | | Phishing (1) | Feb 16, 2018 – Feb 16, 2018 |

### Supporting evidence (0)

This case doesn't contain any evidence yet.

# Cases v2.0

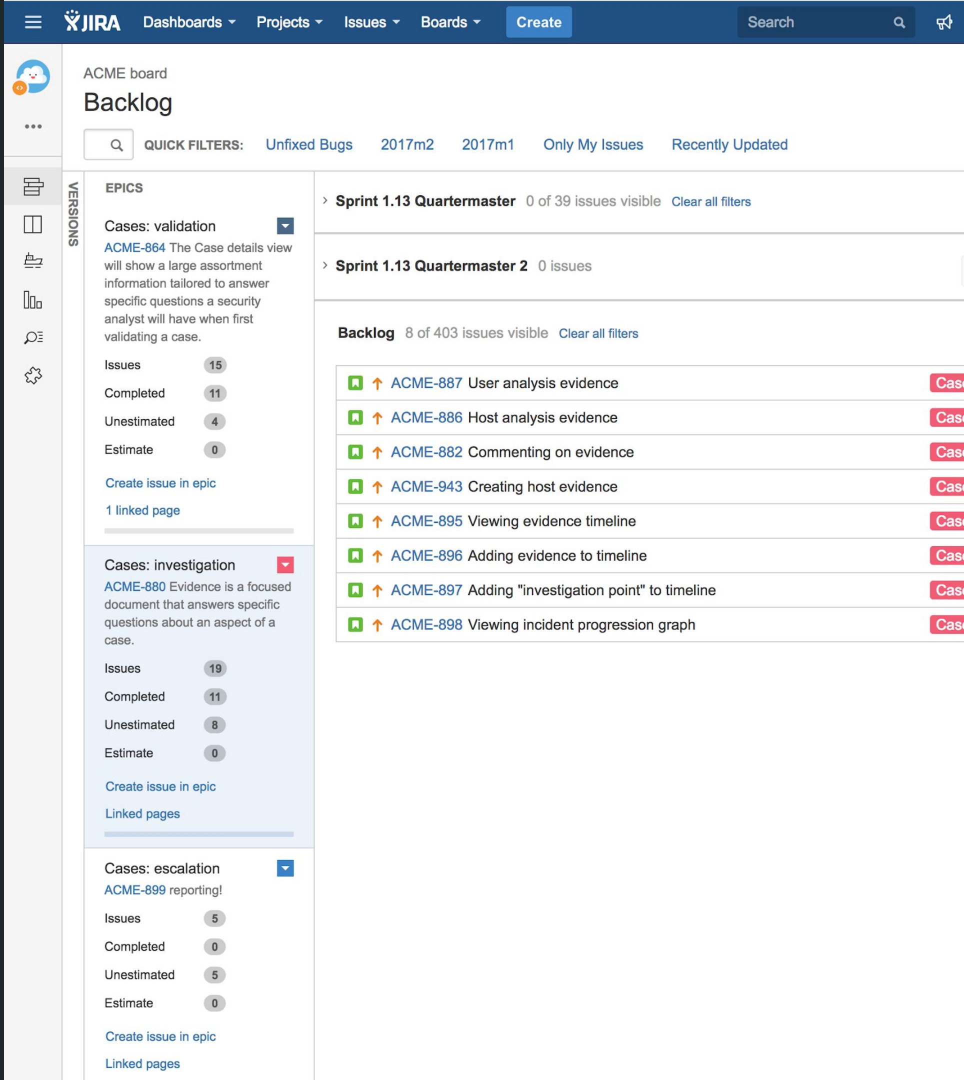
Broke designs down into **61** JIRA tickets. Prioritized, scoped, and planned implementation sprints.

Case overhaul – v2.0

Janus evidence – v2.2

Remediation guidance – v3.1

Even now, Cases continue to evolve. In v3.2 we revamped the Overview to focus more on the entities involved.



ACME board

Backlog

QUICK FILTERS: Unfixed Bugs 2017m2 2017m1 Only My Issues Recently Updated

EPICS

Cases: validation

ACME-864 The Case details view will show a large assortment information tailored to answer specific questions a security analyst will have when first validating a case.

| | |
|---|---|
| Issues | 15 |
| Completed | 11 |
| Unestimated | 4 |
| Estimate | 0 |

Create issue in epic

1 linked page

Cases: investigation

ACME-880 Evidence is a focused document that answers specific questions about an aspect of a case.

| | |
|---|---|
| Issues | 19 |
| Completed | 11 |
| Unestimated | 8 |
| Estimate | 0 |

Create issue in epic

Linked pages

Cases: escalation

ACME-899 reporting!

| | |
|---|---|
| Issues | 5 |
| Completed | 0 |
| Unestimated | 5 |
| Estimate | 0 |

Create issue in epic

Linked pages

Sprint 1.13 Quartermaster 0 of 39 issues visible Clear all filters

Sprint 1.13 Quartermaster 2 0 issues

Backlog 8 of 403 issues visible Clear all filters

- ACME-887 User analysis evidence Cas
- ACME-886 Host analysis evidence Cas
- ACME-882 Commenting on evidence Cas
- ACME-943 Creating host evidence Cas
- ACME-895 Viewing evidence timeline Cas
- ACME-896 Adding evidence to timeline Cas
- ACME-897 Adding "investigation point" to timeline Cas
- ACME-898 Viewing incident progression graph Cas

# Cases v.next?

“I want to understand more about the events that led up to this case.”

“I need more fine details in this case to cross-check against my own logging systems.”

“I want help communicating these findings with security management and executives.”

# But wait there's more!

This is not a secretive process — it's happening organically throughout Cybraics.

- **@jticknor** and **@mike_c** build analytics by observing our SOC's process
- **@amatteson** and **@aris** are making tools to raise operational data to our customer ops team
- **@ggross**, **@mrs.robinson**, and **@nhardy** working and reworking and reworking our business processes to better suit the needs of our staff

# This is where the magic happens ✨

Designers often talk about “delighting” the user. It’s not just about pretty graphics and fancy animations.

It’s about solving the problems they have in ways they couldn’t imagine.

This is a core part of building an “innovative” product. You don’t set out to build one, it’s a label that comes after being used in the market.

# How can we focus more on this?

Continue placing user needs at the center of our product design process. Features aren’t about “ticking a box”, they’re about solving a problem people are having.

Avoid immediately jumping to solutions. Spend time understanding the problems at hand and how they relate to one another. Explore alternatives before committing. Expect to throw ideas away.

Focus on building and validating hypotheses. Think about how you can cheaply validate concepts with users.

Acknowledge that you don’t get to opt out of “providing a UX.” Devote time and attention to this process. It will pay rewards.

# Summary

User experience design is about putting your users at the center of your process and your product.

You don’t get to opt out of “providing a UX.” Users will evaluate you on this regardless of the time you invest.

Being deliberate about this process will lead to a more innovative, successful product.

# Fin.

# Sources

- https://www.nngroup.com/articles/design-thinking/
- http://alistapart.com/article/discovery-on-a-budget-part-i
- https://www.smashingmagazine.com/2018/03/guide-user-testing/
- https://www.smashingmagazine.com/2018/01/comprehensive-guide-product-design/
- https://medium.com/@marcintreder/the-history-of-user-experience-design-5d87d1f81f5a
- https://www.linkedin.com/pulse/tips-how-learn-uiux-design-beginners-grace-jia
- https://www.nngroup.com/articles/why-you-only-need-to-test-with-5-users/
- https://www.nngroup.com/articles/usability-roi-declining-but-still-strong/
- https://www.nngroup.com/articles/aesthetic-usability-effect/
- https://wiki.int.cybraics.com/display/UX/Cases