UX / UI / PRODUCT DESIGN PORTFOLIO

Tomasz (Tomek) Zemla
www.pixelbox.com
tomek@pixelbox.com

INTRODUCTION

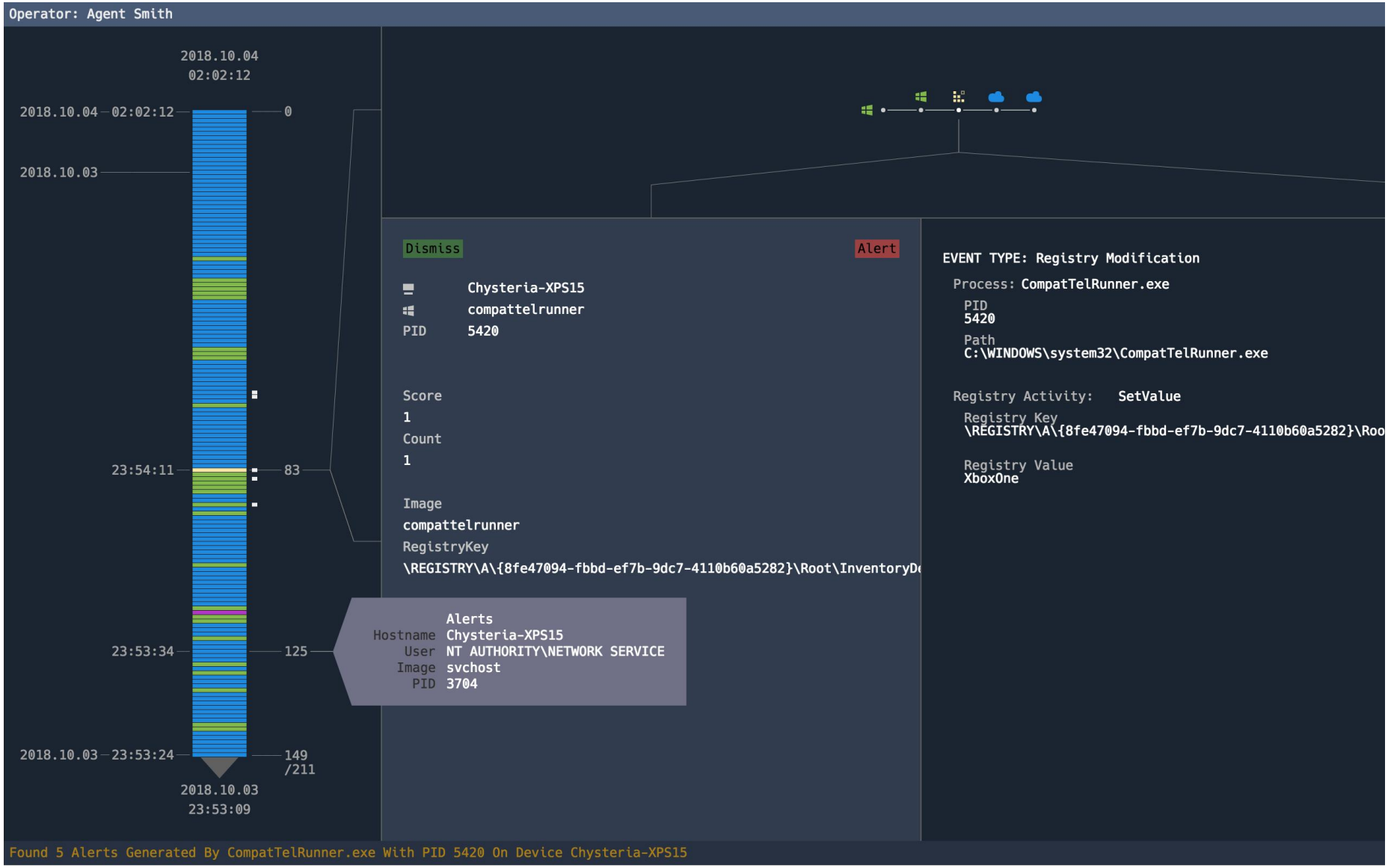
The following pages contain samples of my work selected from a few recent projects. For the sake of brevity, only short descriptions and a few images are presented. Please reach out to tomek@pixelbox.com for more information.

TABLE OF CONTENTS

01 SMART Monitor Prototype [CYDEF]

I designed and developed an early poof-of-concept prototype for a cybersecurity application called SMART Monitor. It was later granted a US patent. The goal of this early exploratory work was to test the ideas for the design of a highly interactive UI supporting cybersecurity analysts in their threat-hunting work.

My background in computer science and extensive experience as a software developer helps me create sophisticated, functional prototypes. In this instance, the prototype was built using the Electron / Node framework and Canvas API using TypeScript with sample data loaded from JSON files. The prototype went through many iterations to refine its design based on testing with industry insiders.


Operator: Agent Smith
2018.10.04
02:02:12
2018.10.04 02:02:12 0
2018.10.03
23:54:11 83
23:53:34 125
2018.10.03 23:53:24 149 /211
2018.10.03
23:53:09
Dismiss
Alert
Chysteria-XPS15
compattelrunner
PID 5420
Score
1
Count
1
Image
compattelrunner
RegistryKey
\REGISTRY\A\{8fe47094-fbbd-ef7b-9dc7-4110b60a5282}\Root\InventoryD
Alerts
Hostname Chysteria-XPS15
User NT AUTHORITY\NETWORK SERVICE
Image svchost
PID 3704
EVENT TYPE: Registry Modification
Process: CompatTelRunner.exe
PID
5420
Path
C:\WINDOWS\system32\CompatTelRunner.exe
Registry Activity: SetValue
Registry Key
\REGISTRY\A\{8fe47094-fbbd-ef7b-9dc7-4110b60a5282}\Roo
Registry Value
XboxOne
Found 5 Alerts Generated By CompatTelRunner.exe With PID 5420 On Device Chysteria-XPS15

02 Flamethrower [Delve]

I collaborated closely with the lead data scientist at Delve to design visualization for the product's AI black box. It is a system for context scoring of cybersecurity vulnerabilities and exposures. The goal of the project was to explain the internal workings of the system to gain the trust of our customers and help the sales and marketing team demo the product.

The created data visualization allowed interactive exploration of the whole ML processing pipeline of the cybersecurity vulnerabilities to understand how various contextual factors affected the score calculation. Shown here is a high fidelity wireframe from the late stages of the design. It was created using the Sketch tool. The project was jokingly codenamed Flamethrower by the team because of how it looked.

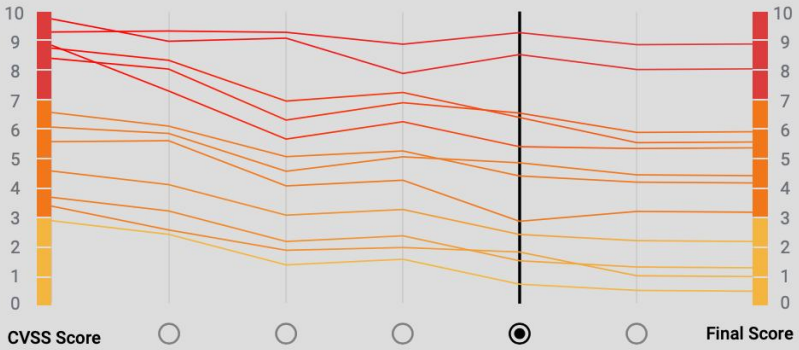
DASHBOARD VULNERABILITIES REMEDIATION WEBSITES SERVERS AUTO DISCOVERY ALL TEAMS

SUMMARY DELVE AI FEED

Modifier Groups

- Vulnerability Properties
  - Base Score
  - Payload Analysis
  - Exploitation Ease
  - Detection Reliability
- Asset Context
  - Exposure
  - Software & Services
  - Behavioral Analytics
  - Availability Requirements
  - Website Content
  - Scan Frequency
- Network Context
  - Network Attack Surface
  - Pivoting Potential
  - Outstanding Asset Detection
- Organization Context
  - Behavioral Analytics
  - Remediation Time
- External Context
  - Public Exploit Availability
  - Threat Intel

Vulnerability Prioritization **Organization Context**



Changes across selected modifier for all vulnerabilities in the system

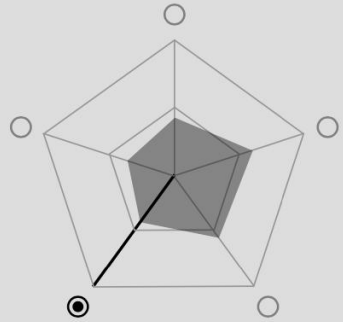
21% ↑ Increase	13% — No Change	66% ↓ Decrease	−45% ↓ Delta	−0.3 ↓ Average

Space for additional explanatory text discussing current modifier group selection above or overview if no selection in the initial state.

Explanations for individual factors (like Behavioral Analytics, Remediation Time, Exploitation Ease, etc) can be discussed here.

Possibly more data/statistics/graphs in the future if available...

Modifier Groups Average Influence



In the right column we could provide list of reference links to our white papers, blog posts or other supporting documentation...

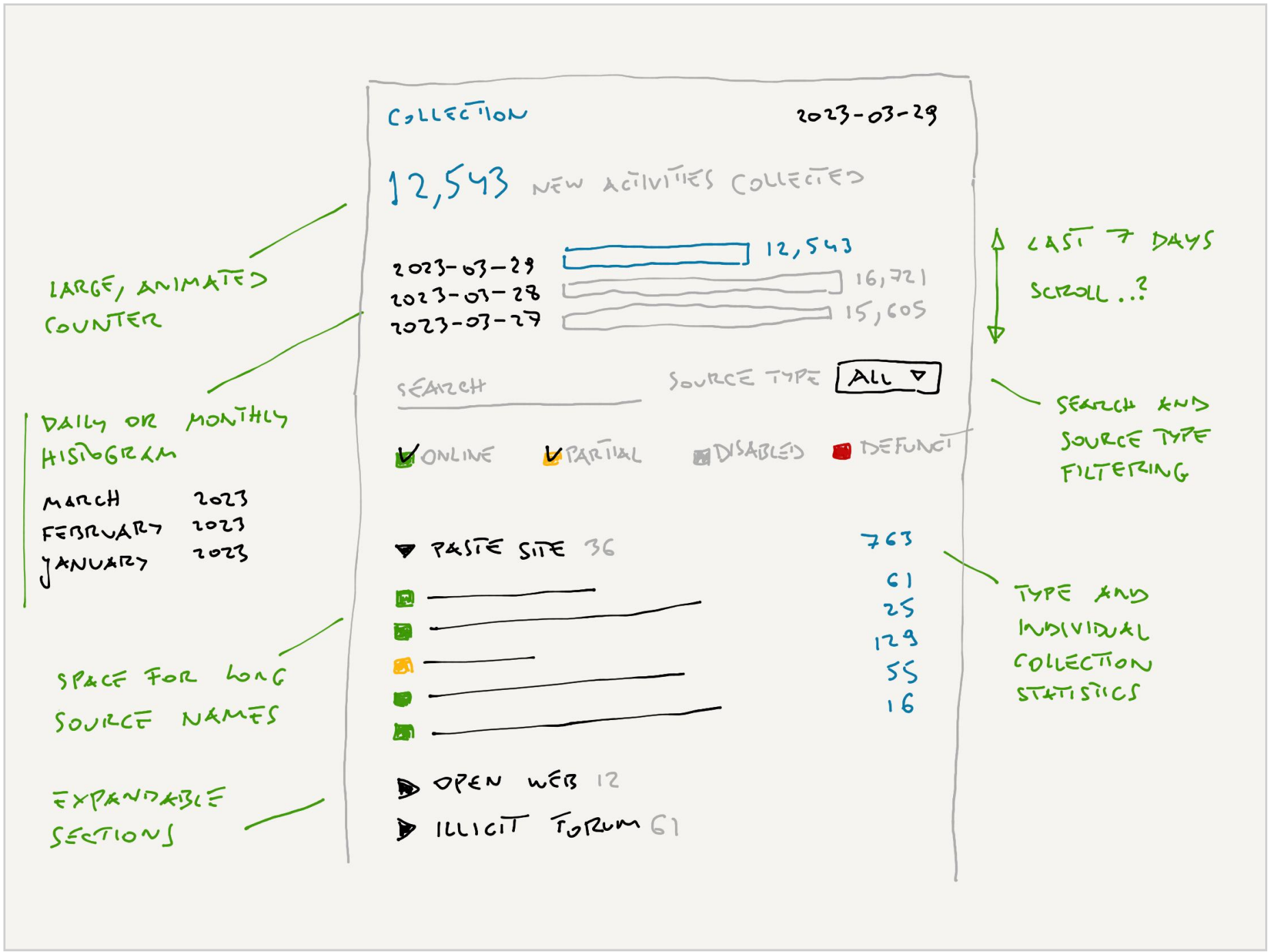
Reference Link One
Reference Link Two
Reference Link Three

03 Discussion Sketch [Flare]

This is an example of a very quick sketch produced in the context of the engineering and product team discussions. Creating *live* sketches on a physical whiteboard (or virtual one in the context of remote work) is a very effective way to bring the team on the same page of understanding the product interface design.

I strive to produce such supporting work during (or shortly after) the meetings to facilitate quick iteration and discussions of the product design ideas.

This specific sketch was used in the context of discussions for the design of a page showing statistics and the status of threat intelligence data collection. The primary goal was to let users understand what are the specific sources of data. The secondary goal was to impress potential customers with the scope of the collection system.

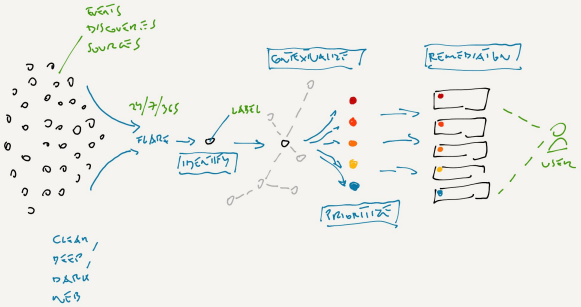

COLLECTION
2023-03-29
12,543 NEW ACTIVITIES COLLECTED
2023-03-29 12,543
2023-03-28 16,721
2023-03-27 15,605
LAST 7 DAYS
SCROLL ..?
LARGE, ANIMATED COUNTER
DAILY OR MONTHLY HISTOGRAM
MARCH 2023
FEBRUARY 2023
JANUARY 2023
SEARCH
SOURCE TYPE
ALL
SEARCH AND SOURCE TYPE FILTERING
ONLINE
PARTIAL
DISABLED
DEFUNCT
PASTE SITE 36
763
61
25
129
55
16
TYPE AND INDIVIDUAL COLLECTION STATISTICS
SPACE FOR LONG SOURCE NAMES
EXPANDABLE SECTIONS
OPEN WEB 12
ILLICIT FORUM 61

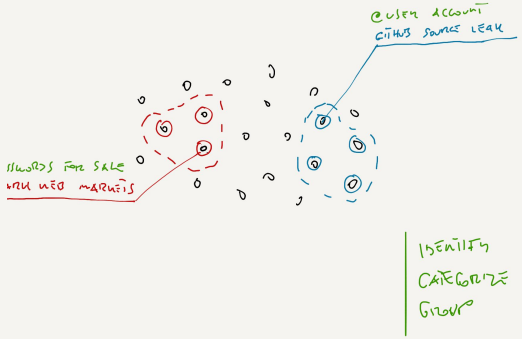
04 Data Visualization Concept Sketch [Flare]

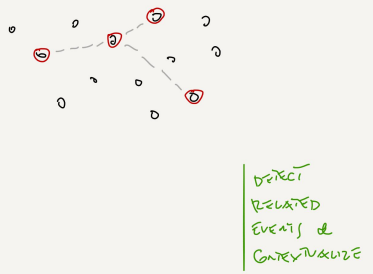
I created a series of sketches for an animated data visualization storyboard explaining the system of cybersecurity threat intelligence data collection and processing software. The sketches served as a mental model for designing various marketing materials and creating easier-to-understand interface workflows for users.

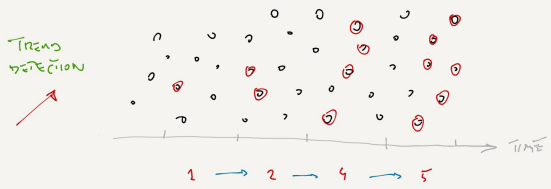
Creating such mental model drawings to bridge the gap between data engineering, product design and user experience is very helpful in designing the interfaces. These concept sketches create common understanding between all stakeholders.

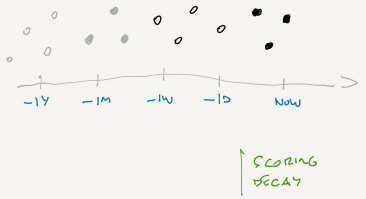
I try to always make them as part of my product design work process to support communication with the whole team.

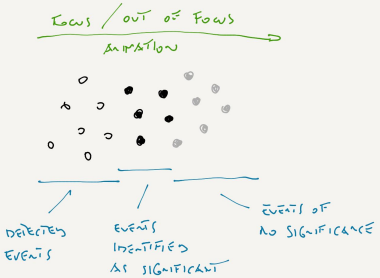

EVENTS
DISCOVERIES
SOURCES
24/7/365
FLARE
LABEL
IDENTIFY
CONTEXTUALIZE
PRIORITIZE
REMEDIATION
USER
CLEAN
DEEP
DARK
WEB

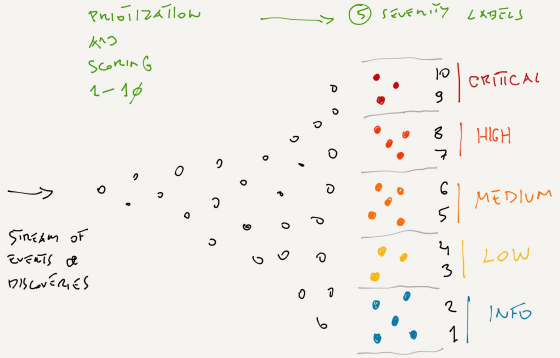

CUSTOMER ACCOUNT
CITIUS SOURCE LEAK
KEYWORDS FOR SALE
DARK WEB MARKETS
IDENTIFY
CATEGORIZE
GROUP

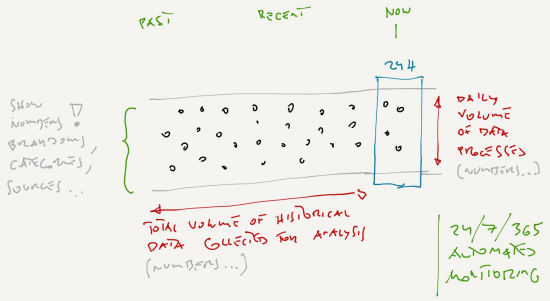

DETECT
RELATED
EVENTS &
CONTEXTUALIZE

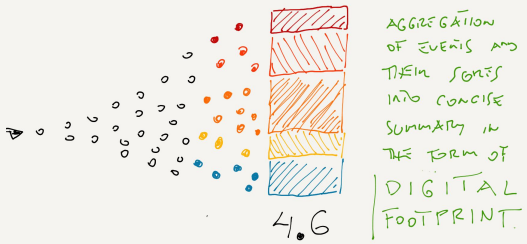

TREND
DETECTION
TIME
1
2
4
5


-1Y
-1M
-1W
-1D
NOW
SCORING
DECAY


FOCUS / OUT OF FOCUS
ANIMATION
DETECTED
EVENTS
EVENTS
IDENTIFIED
AS SIGNIFICANT
EVENTS OF
NO SIGNIFICANCE


PRIORITIZATION
AND
SCORING
1-10
5 SEVERITY LABELS
STREAM OF
EVENTS &
DISCOVERIES
10
9
CRITICAL
8
7
HIGH
6
5
MEDIUM
4
3
LOW
2
1
INFO


PAST
RECENT
NOW
24H
SHOW
NUMBERS
BREAKDOWNS
CATEGORIES
SOURCES
DAILY
VOLUME
OF DATA
PROCESSED
(NUMBERS...)
TOTAL VOLUME OF HISTORICAL
DATA COLLECTED FOR ANALYSIS
(NUMBERS...)
24/7/365
AUTOMATED
MONITORING


AGGREGATION
OF EVENTS AND
THEIR SCORES
INTO CONCISE
SUMMARY IN
THE FORM OF
DIGITAL
FOOTPRINT
4.6

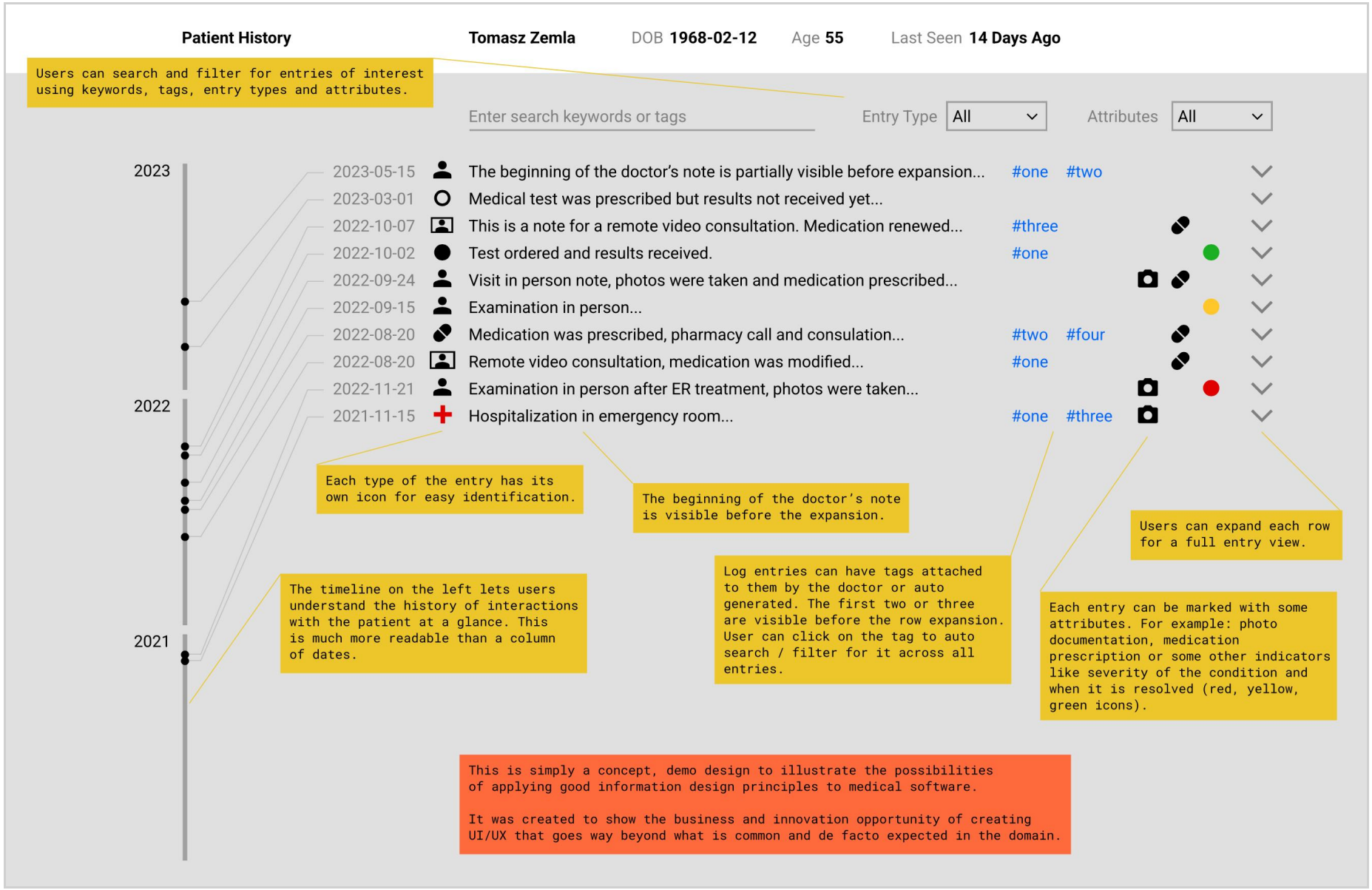
05 Medical Record Concept [Symba]

I designed a concept screen (as a high-definition wireframe) for a new startup in the medical technology space. The planned application was an electronic patient records system.

The key proposed innovation was the integration of the timeline of patient-doctor interactions with a very concise (one line per entry) log summarizing these events. Each line in the log represents one event (like in-person or video consultation, medication prescription, etc). Icons are used to indicate the type of the event. Each log entry is mapped to the timeline on the left of the screen.

This very compact information design allows doctors to see the patient's history at one glance. It makes it instantly visible how many doctor-patient interactions occurred, how often and when.

The concept wireframe is augmented with explanatory annotations - the yellow/orange callouts. I often use this style of presentation to highlight the most important parts of the design when communicating with various stakeholders.


Patient History
Tomasz Zemla
DOB 1968-02-12
Age 55
Last Seen 14 Days Ago
Users can search and filter for entries of interest using keywords, tags, entry types and attributes.
Enter search keywords or tags
Entry Type All
Attributes All
2023
2022
2021
2023-05-15 The beginning of the doctor's note is partially visible before expansion... #one #two
2023-03-01 Medical test was prescribed but results not received yet...
2022-10-07 This is a note for a remote video consultation. Medication renewed... #three
2022-10-02 Test ordered and results received. #one
2022-09-24 Visit in person note, photos were taken and medication prescribed...
2022-09-15 Examination in person...
2022-08-20 Medication was prescribed, pharmacy call and consulation... #two #four
2022-08-20 Remote video consultation, medication was modified... #one
2022-11-21 Examination in person after ER treatment, photos were taken...
2021-11-15 Hospitalization in emergency room... #one #three
Each type of the entry has its own icon for easy identification.
The beginning of the doctor's note is visible before the expansion.
Users can expand each row for a full entry view.
The timeline on the left lets users understand the history of interactions with the patient at a glance. This is much more readable than a column of dates.
Log entries can have tags attached to them by the doctor or auto generated. The first two or three are visible before the row expansion. User can click on the tag to auto search / filter for it across all entries.
Each entry can be marked with some attributes. For example: photo documentation, medication prescription or some other indicators like severity of the condition and when it is resolved (red, yellow, green icons).
This is simply a concept, demo design to illustrate the possibilities of applying good information design principles to medical software.
It was created to show the business and innovation opportunity of creating UI/UX that goes way beyond what is common and de facto expected in the domain.

06 Gen.AI.z Concept Wireframe [UNI3T]

I worked with a multidisciplinary group of scientists and AI researchers on the concept of an innovative application for collaborative research in biosciences. The overall idea was to create a social media-like application supporting pharmaceutical research.

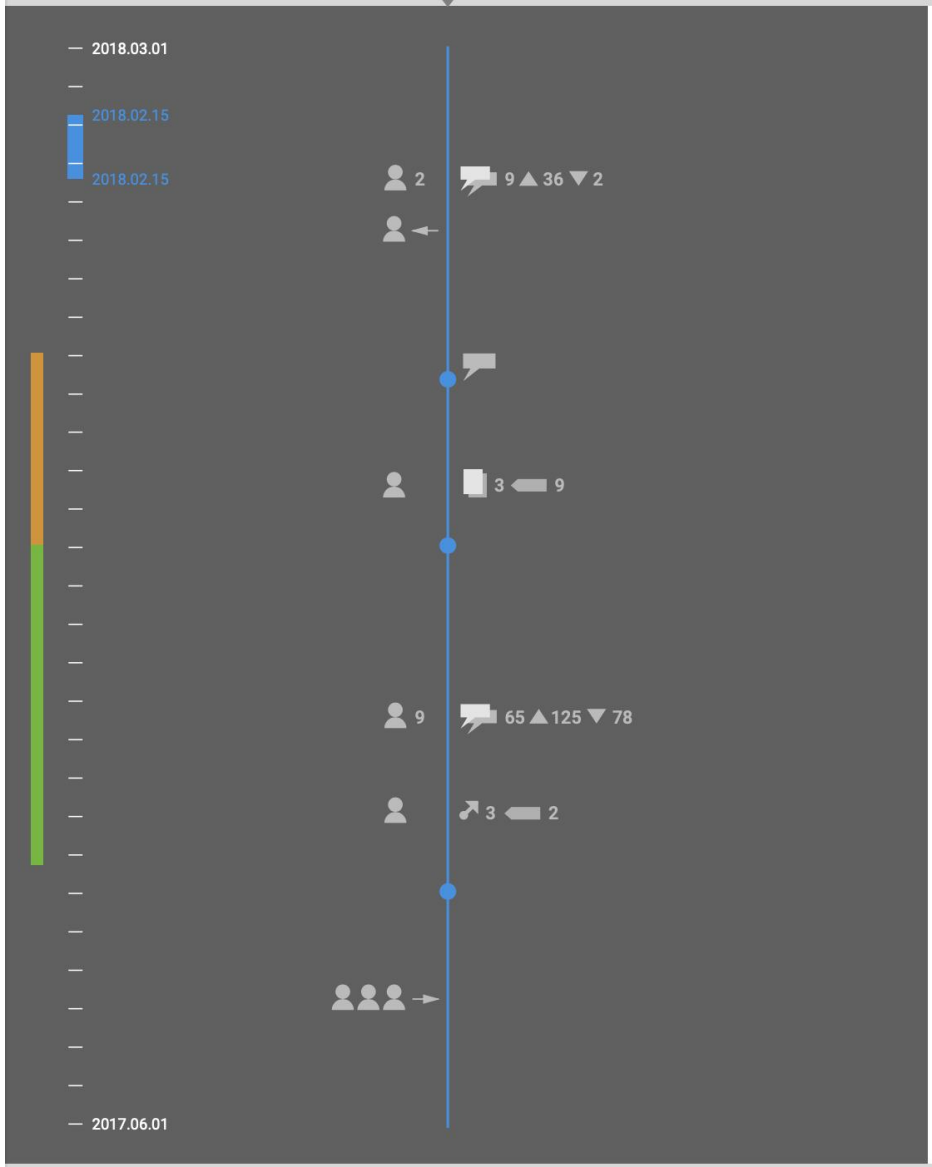
The application would be augmented by behind-the-scenes AI processes that attempt to *connect the dots* between various research activities and discoveries.

The concept screen shown here was a proposal for a visual display of conversations around the research topics. Extensive storyboards were developed to showcase the proposed ideas to possible investors.

Gen.AI.z Home Dashboard Framework **Token** Management Report 2461

Pippeting Variability Issue

Filter: None



Exchange Touch

2018.03.01 17:00:05 Pippeting Variability Issue

Users @Eddie @Leo @Phil @Sylvain have completed their contribution on the touch Pippeting Variability Issue. Commenting and voting may continue until the token owner @Patrice has marked the scoring system as complete.

User	Suggestion	Comments	Votes	Decison
@Philippe	Use different pipette tips with different adhesive properties more...	Most upvoted comment more...	25	■
@Leo	Hyphothesis two short description more...	Most upvoted comment more...	12	■
@Sylvain	Hyphothesis three short description more...	Most upvoted comment more...	4	□
@Eddie	Hyphothesis four short description more...	Most upvoted comment more...	3	□

2018.03.01 17:00:05 Pippeting Variability Issue

Users @Eddie @Leo @Phil @Sylvain have acknowledged the request for contribution on the touch Pippeting Variability Issue

2018.03.01 17:00:05 Pippeting Variability Issue

@Patrice: Request for support on **Hypothesis Formulation** and initiated a scoring system touch.

276 Days 27 Members 76 Annotations 1256 Conversations Documents 65 Tags 167 Links

06

07 Interface Concept Diagram [Flare]

I was asked to imagine the future evolution of the software application in the context of the company's long-term strategy.

The proposal I created was based on the idea of adopting a proven model of Integrated Development Environments used in software development to meet the needs of cybersecurity analysts.

In order to explain the proposed vision I created two drawings. The first one to explain the key elements of the information architecture of the design. The second one was the actual high-fidelity concept screen - see the following pages.

These drawings served as the materials for executive team discussions about the future of the software application and the company.

Flare Future UX/UI Concept : IME - Integrated Monitoring Environment

Dashboard

Contains visualizations
of digital footprint, its history,
recommendations and summary
reports

Findings
(Formerly Home/Events/Alerts)

Contains lists of alerts but also
various entities depending on the
context. Lists of employees, hosts,
IPs, emails, actors.

Also displays search results as lists.

Findings panel can be searched,
filtered and sorted in multiple ways
(always depending on the current
context)

Identifiers

Management of identifiers, lists
of current and recommended ones.

Also policies on automatic adding
of discovered identifiers based on
the level of confidence.

Collection

Management, listing and status
of sources.

Main Menu

Note the logical
ordering of key sections:

Collection (sources) is
at the bottom.

Identifiers (searched
against sources) are next
above.

Findings are the 'raw'
results of the identifiers
cross referenced against
the collection.

Dashboard with executive
reports and summaries of
cybersecurity intelligence
is at the very top.

Listing

This panel always contains listing of some entities.
The type of entities depends on the current selection
of the main menu and context.

This can be list of alerts/events (Findings), list of
available visualizations (Dashboard), list of identifiers
(Identifiers) or list of sources (Collection).

Many other listings can appear here depending on the
current context - for example search results.

Main Information Space

Displays all details for the currently selected item
in the list on the left side. Information is grouped
into tabs. In addition, individual tokens of information
(emails, IPs, actors, etc) can be interacted with.

Auxiliary Information Panel

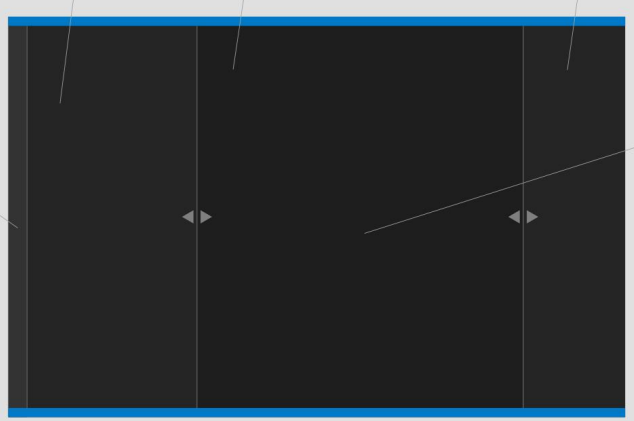
Automatically loads with secondary information
whenever something is selected in a list on the
left and details are displayed in the main panel.

Some information is provided using generative AI.

The categories of information shown:

AI Assist
Help (built-in documentation)
See Also
Related

The auxiliary panel allows for quick pivoting and
following information paths through connecting
the dots.



Information Token Pivoting

Any type of structured information (email, person name,
IP address, threat actor, port number, etc) can be selected
and pivoted on using a drop down menu that offers
various selections to follow.

Many of these operations would result in a list that
loads into the left panel and is ready for further
processing. (Step 1 in secondary workflow sequence)

This 'select and follow' pivoting actions enable following
freely the logical paths across the web of information.

Primary Workflow

1. Select the main section from the main menu on the far left.
2. Work through the list of items.

   Each module can have multiple lists. They can be searched, filtered and sorted.
3. Access details of the currently selected item in the main area.
4. Use auxiliary panel on the right to access AI and standard assist information, built-in help, 'see also' information and various lists for pivoting through data.

Secondary Workflow

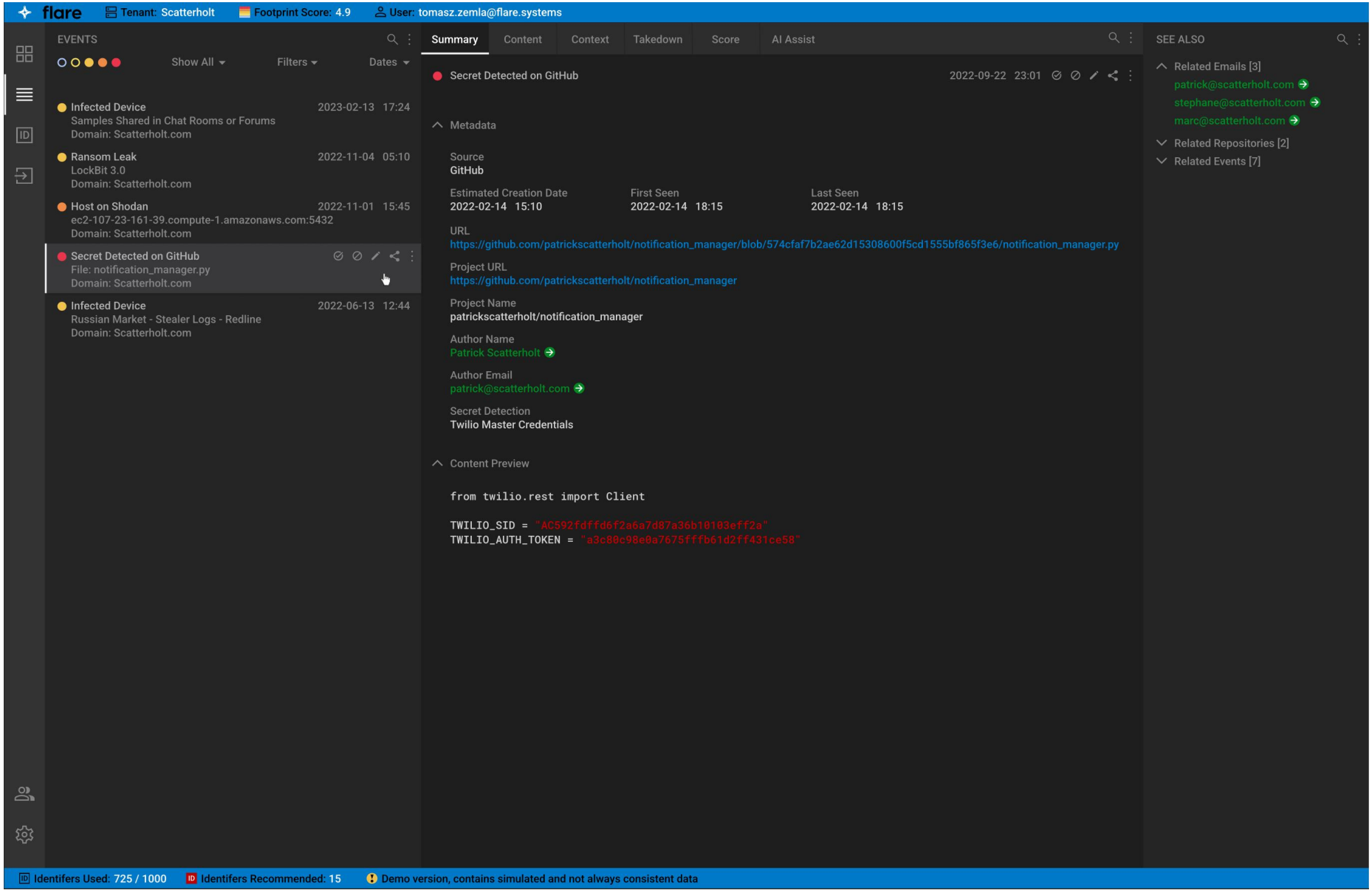
1. Secondary or alternative workflow starts with users loading some specific list of items into the left panel. This can be a result of search, pivoting on some data item (anywhere in the interface), requesting related items or suggestions from AI assist.

2 3 4 Like the steps above

08 Interface Concept Screen [Flare]

The high-fidelity concept drawing imagines a future version of the software as the Integrated Monitoring Environment. This is the second part of the exploratory project - see previous pages for the overview.

This concept mockup was inspired heavily by the design of Visual Studio Code, adapting it to the needs of cybersecurity analysts.


flare
Tenant: Scatterholt
Footprint Score: 4.9
User: tomasz.zemla@flare.systems
EVENTS
Show All
Filters
Dates
Infected Device 2023-02-13 17:24
Samples Shared in Chat Rooms or Forums
Domain: Scatterholt.com
Ransom Leak 2022-11-04 05:10
LockBit 3.0
Domain: Scatterholt.com
Host on Shodan 2022-11-01 15:45
ec2-107-23-161-39.compute-1.amazonaws.com:5432
Domain: Scatterholt.com
Secret Detected on GitHub
File: notification_manager.py
Domain: Scatterholt.com
Infected Device 2022-06-13 12:44
Russian Market - Stealer Logs - Redline
Domain: Scatterholt.com
Summary
Content
Context
Takedown
Score
AI Assist
Secret Detected on GitHub 2022-09-22 23:01
Metadata
Source
GitHub
Estimated Creation Date
2022-02-14 15:10
First Seen
2022-02-14 18:15
Last Seen
2022-02-14 18:15
URL
https://github.com/patrickscatterholt/notification_manager/blob/574cfaf7b2ae62d15308600f5cd1555bf865f3e6/notification_manager.py
Project URL
https://github.com/patrickscatterholt/notification_manager
Project Name
patrickscatterholt/notification_manager
Author Name
Patrick Scatterholt
Author Email
patrick@scatterholt.com
Secret Detection
Twilio Master Credentials
Content Preview
from twilio.rest import Client
TWILIO_SID = "AC592fdffd6f2a6a7d87a36b10103eff2a"
TWILIO_AUTH_TOKEN = "a3c80c98e0a7675fffb61d2ff431ce58"
SEE ALSO
Related Emails [3]
patrick@scatterholt.com
stephane@scatterholt.com
marc@scatterholt.com
Related Repositories [2]
Related Events [7]
Identifers Used: 725 / 1000
Identifers Recommended: 15
Demo version, contains simulated and not always consistent data

09 NorthSec Conference Generative Animation [Pixelbox]

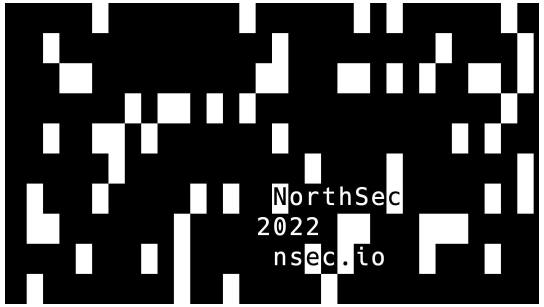
I was commissioned to design projections for the annual NorthSec cybersecurity conference. I created a program to generate an ever-evolving stream of black-and-white screens of graphic compositions with industry buzzwords and glitchy animated transitions.

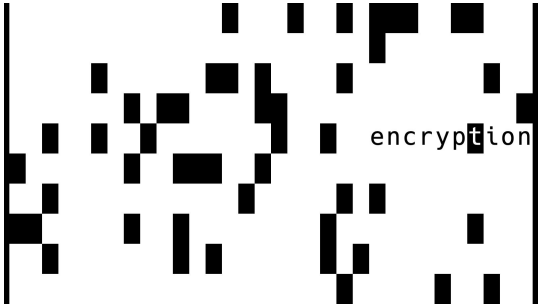
The visual concept aimed to evoke the theme of hacking.

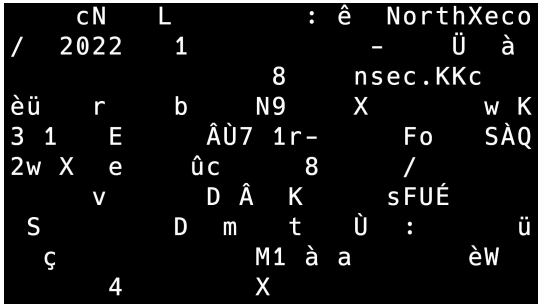
Here is the long list of keywords that were my inspiration: code, data, memory, terminal, console, protocol, transmission, encryption, decryption, corruption, error, binary, on, off, true, false, 0, 1.

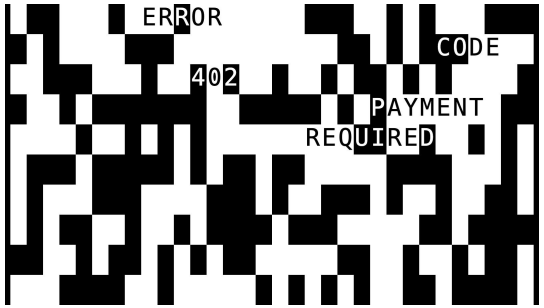
The resulting program was also used to display a practical conference information like presentation scheduling, wifi access, etc. It was developed using TypeScript and Canvas API.

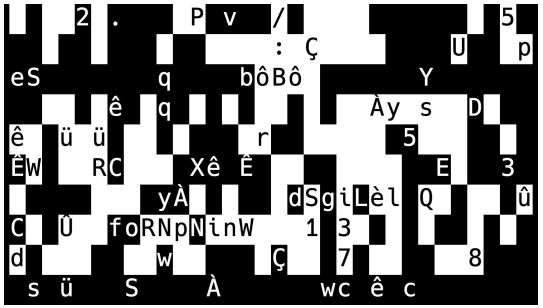
You can see the forever-evolving animation on my website: www.pixelbox.com/nsec.


NorthSec
2022
nsec.io


encryption

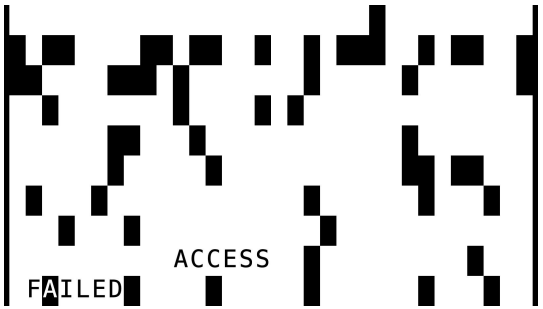

cN L : ê NorthXeco
/ 2022 1 - Ü à
8 nsec.KKc
èü r b N9 X w K
3 1 E ÂÙ7 1r- Fo SÀQ
2w X e ûc 8 /
v D Â K sFUÉ
S D m t Ù : ü
ç M1 à a èW
4 X

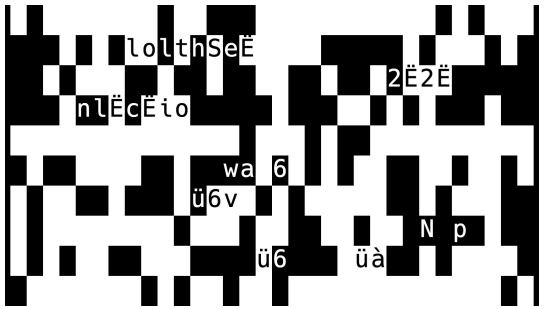

ERROR
CODE
402
PAYMENT
REQUIRED

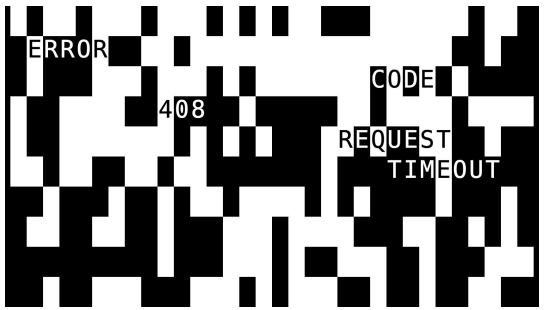

2 . P v / 5
: Ç U p
eS q bôBô Y
ê q Ày s D
ê ü ü r 5
ÊW RC XêË E 3
yÀ dSgiLèl Q û
C Û foRNpNinW 1 3
d w Ç 7 8
s ü S À wc ê c

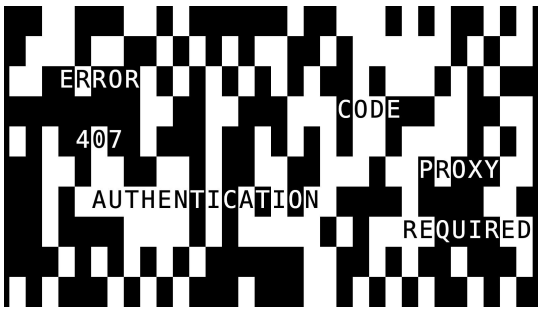

distributed
denial
of
service
attack

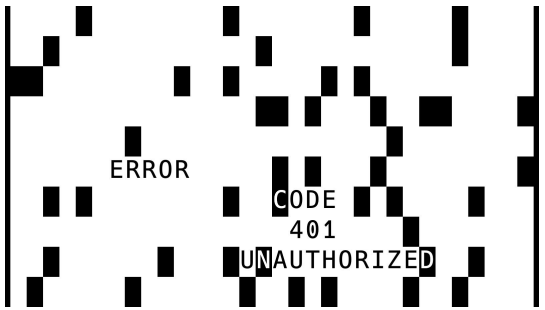

fÜ 4ü Ïâ Èx V Hr-wakC
B 8y ü5 Ê â AS u 8R
dT EKç . H x bÜ3 v NfU2O
çyçp hV7 Dmeô L RHÏÊk/Tâ a
q1V RB h S s0 6HorBhSÜc v
. g iS W E Gp7 5m022 w
C 1 U z nsYCwmi- TâNf cX W
7o0 FkëÛ1Q 1N9ué Yàw6X
/ üê b 2 : ï P Ô ù2
4T ù : hlè aQ u7 0û S EV


ACCESS
FAILED


lolthSeË
2Ë2Ë
nlËcËio
wa 6
ü6v
N p
ü6 üà


ERROR
CODE
408
REQUEST
TIMEOUT


ERROR
CODE
407
PROXY
AUTHENTICATION
REQUIRED


ERROR
CODE
401
UNAUTHORIZED

10 Corporate Branding T-Shirt [Flare]

Being a generalist and working with small R&D organizations and startups I often get asked to create various graphic design materials to support the teams and their work. I was asked to design a t-shirt for the company retreat.

The design made playful reference to bad passwords and command line prompt familiar to all cybersecurity hackers who were the target audience for this swag. It was aligned with the company’s mission of helping businesses improve their security posture.


GET
> $#!T
FIXED
flare