Czech Technical University in Prague

Faculty of Electrical Engineering

Department of Computer Graphic and Interaction

Prototype of Application for Rapid Security Incident Investigation

Master thesis

Bc. Pavla Kohákova

Master programme: Open informatics

Branch of study: Human computer interaction

Supervisor: Ing. Ondřej Vaněk, Ph.D.

Prague, May 2019

MASTER'S THESIS ASSIGNMENT

I. Personal and study details

Student's name: **Kohákova Pavla** Personal ID number: **420310**

Faculty / Institute: **Faculty of Electrical Engineering**

Department / Institute: **Department of Computer Graphics and Interaction**

Study program: **Open Informatics**

Branch of study: **Human-Computer Interaction**

II. Master's thesis details

Master's thesis title in English:

Prototype of Application for Rapid Security Incident Investigation

Master's thesis title in Czech:

Prototyp aplikace pro rychlé vyšetřování bezpečnostních incidentů

Guidelines:

Discuss design and functionality of a user interface, which would allow to the target group of the cybersecurity incidents analysts (threat hunters) to explore the data collected by SIEM and third-parties with less effort (both cognitive and temporal). Study and understand the domain and analysts' needs and extract the main features of tool sections and create scenarios. Design the main environment, workflow, and components in the form of paper mock-up and collect feedback. Create a low-fidelity prototype which should demonstrate the potential of the tool in its breadth, i.e., integrate all features described by the domain experts as their needs. The goal is to understand the visual aspect of the application as well as the structure/positioning the primary application components, without necessarily specifying the detailed interaction with and between the components. Evaluate the low-fidelity prototype with at least five persons from the target group. Based on the output of low-fidelity testing, create a high-fidelity prototype with a subset of features to validate with target group participants. The subset of features will be selected based on the feedback from the target group.

Bibliography / sources:

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide. NIST Special Publication, 800(61), 1-147.
Chuvakin, A., Barros, A. (28. 2. 2018). Preparing Your Security Operations for Orchestration and Automation Tools. Gartner.com [online]. Available at: https://www.gartner.com/doc/3860563
MacKenzie, I. S. (2012). Human-computer interaction: An empirical research perspective. Newnes.

Name and workplace of master's thesis supervisor:

Ing. Ondřej Vaněk, Ph.D., Blindspot Solutions, U Nikolajky 5, Praha 5

Name and workplace of second master's thesis supervisor or consultant:

Date of master's thesis assignment: **22.01.2019** Deadline for master's thesis submission: _____

Assignment valid until: **20.09.2020**

Ing. Ondřej Vaněk, Ph.D. Supervisor's signature	Head of department's signature	prof. Ing. Pavel Ripka, CSc. Dean's signature

© ČVUT v Praze, Design: ČVUT v Praze, VIC

III. Assignment receipt

The student acknowledges that the master's thesis is an individual work. The student must produce her thesis without the assistance of others, with the exception of provided consultations. Within the master's thesis, the author must state the names of consultants and include a list of references.

2.5.2019
Date of assignment receipt

Student's signature

© ČVUT v Praze, Design: ČVUT v Praze, VIC

Declaration

I hereby declare that I have written this master thesis independently and I quoted all the sources of information used in accordance with Methodological instructions on ethical principles for writing an academic thesis.

In Prague, May 2019

_____

Acknowledgment

Firstly, I would like to thank a lot to my thesis supervisor, Ing. Ondřej Vaněk, Ph.D. for the continuous support, time he dedicated to our sessions and aspiring guidance during all stages of the project.

Secondly, I want to express sincere gratitude to all cybersecurity experts, their valuable advices and opinions and the kind approach to collaboration.

Last but not least, I am very grateful to my family for their huge support during throughout all my years of study.

Abstract

Cybersecurity analysts face a great challenge when investigating security incidents which happened within their corporate computer network. A vast amount of data is typically being collected into SIEM (Security Information and Event Management) platforms and another huge set of data is available from third parties. There is a need of a system, which would make the investigation of incidents easier, as the human resources of security teams are very limited, and the amount of information is too huge to be handled manually. Current commercial solutions may be tied to a specific software stack, they require normalization of input data and they are too expensive for a certain segment of analysts.

We conducted a qualitative research with five analysts specialized on incident investigation and found out their needs. Based on those, we defined use-cases and scenarios. Focus was on the unification of needed functions under a single solution, as well as providing knowledge from more sources in one place. Moreover, we discussed features allowing collaboration and knowledge sharing. Those were projected into paper mock-ups and we collected feedback.

Based on the analysis, we designed a low-fidelity prototype and presented it to five analysts. Their evaluation was reflected in the next stage, where we transformed a subset of selected features into a high-fidelity prototype. We collected feedback on the high-fidelity prototype from six analysts. Finally, we wrote down ideas how the prototype could be improved in the future.

Keywords: cyber security incident, incident investigation, SIEM, threat intelligence, security tools, User-Centred Design, user research, prototyping

Abstrakt

Analytici kybernetické bezpečnosti čelí velké výzvě, když vyšetřují bezpečnostní incidenty, ke kterým došlo v jejich podnikové síti. Velké množství dat je shromažďováno do platforem SIEM (software pro management bezpečnostních informací a událostí) a další značné sady dat jsou dostupné od třetích stran. Protože jsou lidské zdroje velmi limitované a informací je příliš mnoho na to, aby byly zpracovány manuálně, je zapotřebí mít systém, který by usnadnil vyšetřování incidentů. Současná komerční řešení mohou být vázána na konkrétní softwarové nástroje, požadují normalizaci vstupních dat, a navíc jsou pro jistou část analytiků cenově nedostupná.

Provedli jsme kvalitativní výzkum s pěti analytiky, kteří se specializují na vyšetřování incidentů, a zjistili jsme, jaké jsou jejich potřeby. Na tomto základě jsme definovali případy použití a scénáře. Důraz byl kladen na sjednocení potřebných funkcí do jednotného řešení, a také na dostupnost znalostí z více zdrojů na jednom místě. Zaobírali jsme se i funkcemi, které umožňují spolupráci a sdílení znalostí. Vše jsme zohlednili v časném papírovém modelu, na který jsme sebrali zpětnou vazbu.

Na základě analýzy jsme navrhli low-fidelity prototyp, který jsme předvedli pěti analytikům. Jejich hodnocení jsme promítli do další fáze, ve které jsme převedli vybrané prvky do high-fidelity prototypu. High-fidelity prototyp jsme nechali ohodnotit šesti analytiky. Na závěr jsme sepsali nápady, jak bychom vylepšili prototyp v budoucích krocích.

Klíčová slova: incident kybernetické bezpečnosti, vyšetřování incidentů, SIEM, threat intelligence, nástroje pro bezpečnost, User-Centred Design, uživatelský výzkum, prototypování

Content

List of Figures

List of Tables

1. Introduction

Cybersecurity analysts face a great challenge when investigating security incidents which happened (or which are happening) within their corporate computer network. A vast amount of data is typically being collected into SIEM (Security Information and Event Management) platforms and another huge set of data is available from third parties. Those are typically merged together to provide a comprehensive view on the network. However, this view is presented only in the data and the analyst's challenge is to dive into the data and find the incident needle in a data haystack.

The motivation for this project is a real need of a system, which would make the investigation of incidents easier, as the human resources of security teams are very limited, and the amount of information is too huge to be handled manually.

Commercial solutions may be tied to a specific software stack, they require normalization of input data and they are too expensive for a certain segment of analysts. The ambition of this thesis is the exploration of needs of cybersecurity incident analysts and design a tool which will unite required functionality under a single platform, which would make the investigation easier. Apart, starting from scratch and freedom of design (which doesn't have to correspond to available commercial tools) might generate new ideas. The workname of this investigation tool, which we will prototype, is RSI^3.

This thesis is divided into six chapters: Introduction, Domain analysis, Design analysis, Low-fidelity prototype, High-fidelity prototype and finally Conclusion and future work.

In the Domain analysis part we will define a target group and a platform and introduce the cooperation of security tools. We will define user-centred design techniques used for the analysis. Subsequently, we will present information gained from interviews with analysts. We will analyse State of the Art and take a look on existing tools, logs sources and threat intelligence platforms. Finally, we introduce challenges to be solved and define which to focus on.

In the Design analysis chapter we will define two personas, sum-up current workflow and based on these define scenarios and storyboard, two main use cases and other required functions. We present paper mock-ups and their early usability evaluation.

The next chapter is dedicated to the process of creation and evaluation of the low-fidelity prototype. We describe the design of the low-fidelity prototype and afterwards the set-up and results of the usability test.

In the high-fidelity prototype chapter we follow-up the findings resulting from the low-fidelity prototype testing and describe the designing of the high-fidelity prototype with a subset of features, and the process of their evaluation.

In the final chapter we summarize done work and mention future work on this topic, both from user design and algorithmic point of view.

1.1 Assignment

Discuss design and functionality of a user interface, which would allow the target group of the cybersecurity incidents analysts (threat hunters) to explore the data collected by a SIEM and third-parties with less effort (both cognitive and temporal).

Study and understand the domain and analysts' needs (see section 2 Domain analysis) and extract main features of tool sections (see section 3.5 Use cases and functions) and create scenarios (see section 3.3 Scenarios).

Design the main environment, workflow, and components in the form of a paper mock-up and collect a feedback (see section 3.6 Paper mock-ups).

Create a low-fidelity prototype which should demonstrate the potential of the tool in its breadth, i.e., integrate all features described by the domain experts as their needs. The goal is to understand the visual aspect of the application as well as the structure/positioning the primary application components, without necessarily specifying the detailed interaction with and between the components. (see section 4.1 Design) Evaluate the low-fidelity prototype with at least five persons from the target group (see section 4.2 Evaluation).

Based on the output of low-fidelity testing, create a high-fidelity prototype (see section 5.1.2 Implementation) with a subset of features to validate with target group participants (see section 5.2 Evaluation). The subset of features will be selected based on the feedback from the target group (see section 5.1.1 Selection of features).

1.2 Dictionary

This is a list of abbreviations and terms, which will be used in this thesis. Some of the terms are widely used, some are used for clarity of this thesis (e.g. RSI^3 for name of whole project, Analyst for the target user).

RSI^3	Rapid Security Incident Investigation Interface (this project). Investigation tool.
Analyst	Cybersecurity expert who is specialist in cyber threat analysis and investigation of cybersecurity incidents.
SOC	Security operations centre. A team of cybersecurity analysts, which monitors and evaluates enterprise information systems and cares about their cybersecurity.
SIEM/LM system	Security Information and Event Management / Log Management system.
SOAR system	SOAR stays for Security Orchestration, Automation and Response. SOAR systems are technologies enabling collecting security data from various sources, their reporting and automated evaluation. Orchestration means connecting and integrating various security applications and processes together. Automation means that the software takes actions on its own – e.g. calculates some statistics, executes machine learning processes based on big data gained from other systems etc. Incident response is an organized approach to addressing and managing the aftermath of a security breach or cyberattack, also known as an IT incident, computer incident or security incident. [s3]
Triage, priority	Important aspect of investigation tools is prioritization of security incidents. The priority given to the incidents is called triage. The triage calculating process takes many factors into consideration, e.g. type of the incident, participated entities, relevant CTI sources etc.
Maliciousness	A property of entities (e.g. IP addresses, subjects), calculated based on orchestrated resources and considering such aspects as credibility, relevance and severity.
(C)TI	(Cyber) Threat Intelligence. Concept of a science which collects intelligence from dark web with a mission to research and analyse trends and technical development in areas of cybercrime, hacking activism and cyber spying.
Enrichment sources	Open and often crowd-sourced computer-security sources for threat information sharing. Examples can be CTI tools as VirusTotal, AlienVault OTX (open-threat exchange), MISP, whois etc.
Indicator of compromise (IOC)	Indicators of compromise point out potentially malicious activities on a system or network and artefacts that with high confidence indicate a computer intrusion. Digital artefacts comprise suspicious IP addresses and host names, URLs and domain names of botnets, MD5 hashes of malware files, virus signatures, Windows registry entries, network processes and services. [s4]

Log	One small file or packet describing a part of an event, a row in the network communication.
Event	Group of logs which creates together an event. Event can be “log in,” “download” etc.
Alert	Alert on potential threat, based on trigger rules and consisting of suspicious events and logs.
Incident	A group of alerts or suspicious events diagnosed as a security incident. Example of suspicious events is a sequence of login, send in, download and log out in interaction with a potentially malicious domain.
Device	Hardware device – e.g. personal computer, tablet, smartphone, camera, router.
IP address	An Internet Protocol address (IP address) is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. [s5] IP address can be translated by using a decentralized naming system Domain Name System (DNS)
URL	Uniform Resource Locator, contains the protocol to be used (i.e. HTTP, FTP), the domain name or IP address, the path, and optional fragment identifier.
Subject	An owner of IP address – it can be a physical user who possesses device connected to the internet, it can be a server, it can be a web page – anything what can be IP address related to.

Table 1 Dictionary

2. Domain analysis

The aim of the analysis is to understand the domain of cybersecurity and to get an insight into the needs of cybersecurity analysts. We have studied some existing SIEM systems (see State of Art Analysis) and papers about security incidents investigation ([s1],[s2]) and based on these, we got a brief idea what could be the topics related to the problem we are trying to solve. Afterwards, we have prepared questions to be answered by experts in SIEM branch and made a user research.

After that we made a recherche about SIEM and SOAR tools and sources of logs and CTI tools. We specified the challenges to be solved and defined what problems we will focus on. In this chapter we sum up these collected materials, based on which we were creating our prototypes.

2.1 Target group

RSI^3 should be an investigation tool, which would help the cybersecurity analysts to investigate suspicious events and incidents in the network and uncover real threats. These specialists are also called “threat hunters”. Users of RSI^3 will be specialists, who care for cybersecurity in companies with thousands of devices. Analysts are usually part of the SOC (Security operation centre) team.

2.2 Target platform

RSI^3 is meant to be an online service, which will be used by the experts on their computers. Therefore, by designing the interface, we will consider a screen size of an average monitor, which could be around 15 to 27 inches.

2.3 Security tools cooperation

In this section, we would like to introduce the difference between a SIEM and an investigation tool and their cooperation.

SOC analysts are often working with multiple tools. They are looking at the SIEM console for new alerts, TI service portals for information about the entities involved, and endpoint detection and response (EDR) for context on what is happening on the affected endpoint. They may even be using workflow tools to control the triage and investigation process. [s1]

There are two functions of the SOC team:

The first one is to set up security monitoring tools to receive raw security-relevant data (e.g. login/logoff events, persistent outbound data transfers, firewall allows/denies, etc.). This includes making sure that critical cloud and on-premises infrastructure (firewall, database server, file server, domain controller, DNS, email, web, active directory, etc.) are all sending their logs to log management, log analytics, or SIEM tool.

The second function is to use these tools to find suspicious or malicious activity by analysing alerts; investigating indicators of compromise (IOCs like file hashes, IP addresses, domains, etc.); reviewing and editing event correlation rules; performing triage on these alerts by determining their criticality and scope of impact; evaluating attribution and adversary details; sharing findings with the threat intelligence community; etc. [s6]

RSI^3 should be a tool to support the second function. Therefore, the purpose of RSI^3 is not information and alert collection, but taking those as input and evaluate them, enrich them by CTI sources and help with the investigation. RSI^3 should be an investigation system.

2.4 User-centred design and used tools

User-Centred Design (UCD) is a user interface design process that focuses on usability goals, user characteristics, environment, tasks, and workflow in the design of an interface. UCD follows a series of well-defined methods and techniques for analysis, design, and evaluation of mainstream hardware, software, and web interfaces. The UCD process is an iterative process, where design and evaluation steps are built in from the first stage of projects, through implementation. [u1]

The major advantage of user-centred design is that it makes possible a deeper understanding of the psychological, organizational, social, and ergonomic factors that affect the use of computer technology. The involvement of users assures that the product will be suitable for its intended purpose in the environment in which it will be used. This approach leads to the development of products that are more effective, efficient, and safer. [u2]

For the analysis phase, we decided to use a qualitative approach. Reason for this is that the branch of cybersecurity is very large and for non-professionals would be hard to formulate relevant quantitative questions. Quantitative research gains limited information, as it is bounded by the fantasy of the question's author.

We decided to use a contextual inquiry method, which is one of the qualitative Context of Use methods.

Contextual inquiry is a semi-structured interview method to obtain information about the context of use, where users are first asked a set of standard questions and then observed and questioned while they work in their own environments. Because users are interviewed in their own environments, the analysis data is more realistic than laboratory data. This technique is good for getting rich information about work practices, the social, technical, and physical environments, and user tools. [u3]

For participant recruiting we used a snow-ball sampling strategy. The process consists of finding a few representatives of the target group and these representatives give recommendations for next people. Researchers have championed the use of snowball sampling in social computing research, where a global directory of all users is usually unavailable and snowball sampling can be viewed as a form of convenience sample. [u4] This is also a case of cybersecurity analysts, as it is not very common job position and there are no contacts for such experts, as they are part of big companies. It is difficult to recruit several participants who would be specialized in incident analysis and at the same time would be willing to help with the research, therefore the personal recommendation system seemed to be the most effective way of recruiting.

Based on the results of user interviews and State of the Art analysis, we could specify requirements. UCD offers a lot of techniques to be used. We have decided to create personas to clarify who is a target user. We introduced typical scenarios and a storyboard. We decomposed current analyst's workflow into a hierarchical task analysis graph. Arising from current workflow and needed functions, we defined main use-cases and other required functions. As we realized that there are many parallel tasks in main use-cases, we decomposed those in form of Concur Task Trees.

A persona is a representation of a fictitious user that includes a concise summary of the characteristics of the user, their experience, goals and tasks, pain points, and environmental conditions. [u3]

Scenarios of use are descriptions of one or more users interacting with a system, device, or process to achieve a goal under specified conditions and constraints. They provide information about the context in which a system has to operate, in a user- and task-oriented way. [u3]

A storyboard is a technique for illustrating an interaction between a person and a product (or multiple people and multiple products) in narrative format, which includes a series of drawings, sketches, or pictures and sometimes words that tell a story. [u3]

Hierarchical task analysis (HTA) is a widely used type of task analysis, where a high-level task is decomposed into a hierarchy of subtasks. [u3]

Concur Task Trees is a notation which focuses on activities that users aim to perform. Main features are hierarchical structure of subtasks, graphical syntax which is easier to interpret and reflects the logical structure in tree-like form and rich set of temporal operators. Examples of the temporal operators are [] for choice, []>> for enabling with information passing, ||| for concurrent tasks and |[]| for concurrent communicating tasks. [u8]

Afterwards we started an interactive process of design creation and evaluation. We decided that this process will have three phases. The first one should be a paper mock-up study, where the basic idea is discussed with the analysts. Second phase introduces a low-fidelity prototype and is tested by target users, as well as the third phase regarding a high-fidelity prototype.

2.5 Users interview

For gaining the qualitative data, we selected a contextual inquiry method and we recruited seven participants, based on a snow-ball sampling technique.

We have prepared a session guide for the interviews. Firstly, we introduced the basic idea of the project we would like to realise. Afterwards, we put some questions about the cybersecurity analysis domain. Than we asked the participants to show us some of the cases they are currently working on to see their workflow. In the last part, we made a short brainstorming with the participants, what kind of tool they would like to have.

Each interview was taken on the participant's workplace. The reason was to have access to participant's computer and see the tools they use. Sessions took between 40 and 85 minutes.

We made a private audio record with the permission of the participants to be able to listen to the interview again, to gain more information, and to be able to concentrate during the interview on speech and not on making notes.

In this chapter we will sum up the results of interviews, which will introduce the domain of cybersecurity analysis. The spectrum of use cases in cybersecurity analysis is very large and depending on the use case and the question, which the analyst wants to solve, the collected data, used tools and used approach may differ very much. During the interviews there were mentioned a lot of diverse tools, possible input data, use cases and practical examples.

Note that word "user" refers to users in company network the analyst are working with. Our target users are called "analysts".

2.5.1 Participants

This section describes recruited participants and their background.

Participant ID	**Time in security job**	**Job description**
P1	10 years	Threat analyst in a networking company
P2	20 years	Threat analyst in a networking company
P3	14 years	Cyber threat scientist in a networking company
P4	4 years	Threat analyst in an antivirus software company

P5	1 year	Threat analyst in an antivirus software company
P6	2 months	Developer of commercial investigation tool with an experience with cybersecurity issues
P7	2 months	Developer of commercial investigation tool

Table 2 User interviews participants

Interviews helped us to get a basic insight into the cybersecurity, analysis of threats and suspicious incidents. We gained also awareness of the domain of the SIEM system and investigation tool development.

Interviews with experts on cybersecurity analysis (P1, P2, P3, P4, P5) clarified the approaches used in analysis and introduced to us the commonly used tools, as well as the biggest challenges the analysts must face.

P1 and P2 work as cybersecurity analyst for a very long time and have a great overview about possible cases of security threats and know plenty of tools and approaches how to analyse them. They could describe closely the process of investigating suspicious incidents.

P3 specializes rather in machine learning and threat identification. “I am processing logs of any type and I am trying to search for threats in them. I try not to search for threats manually, but I rather look for machine learning algorithms to find the threats automatically.”

P4 deals with analysis of files and binaries, which are marked as possible malware and harmful files.

P5 is working as scientist, developer, analyst and investigator at once, therefore he has a big overview and knows about simulating and solving the threats. He is in the domain for shorter time, therefore he focuses just on some use cases of analysis, mainly the botnet problem.

Another story were the insights coming out of interviews with the developers. These participants work on backend for a newly developing investigation tool, which should be an enriching component of an existing SIEM system. Developers introduced to us their proof-of-concept, which was made rather for proving the functionality of the system, not a perfect design. P6 and P7 explained us the function of their backend and the cooperation of the SIEM system and the investigation tool.

2.5.2 Data, enrichment sources, used tools

The size of data, the way how analysts filter it, and the ways how they prepare them before visualisation depends on the problem to be solved.

“It depends on what we are doing the analysis for. If I want to detect the people behind the event, or the relationship between two users, I use different datasets. In one analysis I may need to see the evolution of the protocol in the histogram, to find out if it is an attack, which is related to ransomware or to port scanning. In another one I need to know a social relationship or the countries of the users. So, the selected visualisation tool depends on the graph method, which depends on the data, and those depend on what I am looking for.” [P2]

“There are many questions which must be answered by doing the analysis. There are many tools, each suitable for another task. There are programs for searching, analysing, isolating and filtering data, writing data etc.” [P1]

Generally, millions of logs flow daily through the network and in one second there are collected thousands of logs. Therefore, the analyst must filter out just suspicious and interesting data and ignore

most of the traffic. The need of filtering out the majority of data and working just with relevant subsample was mentioned by all participants.

Analysts filter out the data by using SIEM systems, commands in command line, queries, machine learning and some custom systems. E.g. in case of P4, the antivirus client collects data and he gets already detected suspicious data to analyse. P1 and P2 use sometimes the Splunk SIEM system. P2 finds Splunk sometimes too slow, therefore he uses nmapfe tool to make an nmap scan, and uses often command line and some grep-based commands for filtering. P1 works as well very often with command line and some internally developed machine-learning tools.

The logs from the network can be collected on more levels (on router, firewall, proxy, domain controller…) and they also depend on the permitted access to the data. If a company gives the data for external analytics, they deliver logs from network, company servers, but not from machines of the employees. On the contrary, if the analyst is inside the company, he could have the possibility to go to check the machine of his colleague.

"I, as an analyst in networking company, see connections and can decide if it is an attack or not, but I cannot check the behaviour of the attack in the victim device, as I have only the access to the network logs." [P1]

"If I am working with data in local network, I can use DNS to translate IP addresses to the names of the domains I am resolving. I can see web connections and get exact information. I use bro (currently Zeek, open-source network analysis framework) to enrich my data. But I can do these just when I have access to the network. If I don't, I have e.g. some web logs from my customers, which I should investigate. When I focus on HTTP weblogs, I use ManaTI. I also use MISP to find the relations. But I don't need to analyse all malware in the world – there are other tools for it. For example, MISP shares all malware in the world, it has a graph showing who shared what, and with these I can filter out what is appropriate to my problem." [P2] ManaTI is also used by P1.

Some analysts may collect just information about network flow, some others also the binaries. Based on this, the structure of the logs may differ. But mostly the logs contain IP addresses of sender and receivers, the port, information about content, time of the connection and duration, information of connection type (SSH, SSL…), some information about device, sometimes about the domain etc.

"I collect the packets from router and get a linearly stored sequence of packets. The packet contains always a five tuple with Source IP address, Source Port, Destination IP address, Destination Port, Protocol, plus some useful statuses. We get millions of such packets and we cluster them to bigger aggregations, called netflows, which is a communication file between two devices." [P5]

Based on collected logs, the analysts search for more information. E.g. P4 and P5 use antivirus database of blocked URL. P3 search for the domain and namespace of the user binary and afterwards explores the domain, which relates to the address of autonomous system and servers.

Analysts gain more information about suspicious addresses on shared systems, as VirusTotal [P1, P2, P4, P5], Open threat exchange OTX [P2], whois database [P2, P3], RiskIQ PassiveTotal Threat Investigation Platform [P2, P1 for DNS], walrusway [P1], MISP [P1, P2] and programs, which translate IP addresses to domain names.

These enrichment sources show for example the reputation of IP addresses and share information about files (e.g. which antivirus software would detect the file as malicious). They can also show some relations and connections between addresses and threats.

"I work with some entities so often, that I know them by heart. For example, I know some Google and Dropbox addresses, so I don't have to check VirusTotal every time. However, some cloud services as

Amazon generate a lot of its addresses, and therefore I must check them, as the reputation may change." [P1]

"MISP is a platform for sharing threat intelligence events between the community. There are some graphs, and this is probably the most used tool for sharing and analysing threat intelligence events. In this case we are focusing on attacks like 'I am being attacked' or 'One of my computers in the network is being infected' or 'Our CEO lost the data'. From events, traffic and flow, MISP generates more data. E.g. from IP address we can get countries, the reputation and other parameters." [P2]

When analysing emails and other kinds of data than web logs, the strategy would differ.

"I have seen who visited injurious server, and I searched, if there was also another user registered from similar company, if someone received the same email…" [P3]

"In case of email, you have all the headers with information as who is it coming from, who received it, and the computer, which received the email. If you have access to an email server computer and somebody sends you this suspicious email, maybe you know the journey of the email. If you don't have the access to the server, you have just the email itself and then it is harder to investigate, and you must use different tools. Reputation is not so relevant by email addresses, as it is very easy to generate a new one and to misuse someone's address" [P2]

2.5.3 Analyst workflows and needs

As we already mentioned, the area of cybersecurity is very large and there are many different job positions and approaches how to analyse threats and malwares.

For example, P4 works with data files detected as malicious and investigates, if it is really a malware.

"In my company, there are mostly people doing scientific research, people developing the software part and our third team is into threat investigating. I prefer machine learning – the team of investigators finds one incident, delivers it to us and we learn our algorithms on this incident and find thousands more based on this. Therefore, I find machine learning more effective, but I need the one who investigates this one incident I can build on.

The algorithms for machine learning are learned again on logs of any types. Most machine learning methods don't work just how it is, so I try to adjust them for the security domain. I train them on datasets with a few of positive samples (positive means malicious). Or I use particularity of the JSON data. I also break into anomaly detection methods. Learning comes in case we don't have labels on the data levels we get. I work mostly with text, not with graphical tools. It suits more to my scientific research.

Firstly, I use some easy detectors – that filters out 95% of traffic, and I use the expensive and complicated detectors on the rest. But it is very difficult to find general threats. Cognitive threat analysis has a lot of anomaly detectors (40-50), where one part is general and answers to questions related to non-typical behaviour of user. Another part of detectors is specialized – it knows how the particular malware behaves and identifies behaviour typical for this malware, like some hash in data etc.

Another approach is to focus on the monetization of malware. Does is show adds? Mines it bitcoins or another cryptocurrency? Is it ransomware – that one is hardly catchable from network, we must already know where it came from, because it has hidden network traffic. Or sending of spam, which has big traffic on non-authenticated email serves. It is also hard to detect Denial of Service attack – botnet strike from a lot of places and every infected computer sends a few requests." [P3]

Machine learning is used hugely in the domain of cybersecurity. P5's company uses machine learning for dividing found malwares into about five thousand of clusters, and in each cluster they train a local model for quicker analysis and categorization.

P5 also tries to simulate some threats to create better protection: "Firstly we have to define the threat and then find a way how to simulate it, to check the efficiency of our protection. The threat may have more phases. For example, if some of IoT (Internet of Things) devices is infected, it may correlate to virtual events, but also to some physical events. E.g. when the device is connected to network, it must be identified, which is both the physical and software event. We must consider both of them, when preparing the simulation. While simulating, on our router we measure the communication in the whole network and then we perform a manual analysis. We have to define some bigger units, called 'events' for making the analysis quicker." [P5]

P1 mentioned problems related with the type of network attack and the possibility of seeing proper logs. Attack may be intrusion, of infection.

"In case of intrusion, which is an unauthorized activity on a computer network, the attacker is trying to get privileges and break into the network. Once he is in the network, he can get into the computer and do a lot of evil stuff, but I may not see it, as I may not have access to the logs from the attacked device. Therefore, intrusion is harder to find, as there may be just one connection to see. I must focus on connecting events, which contain access logs, process logs etc.

In case of an infection with malware, network logs are more reach. The victim got infected somehow and the attacker wants to control the malware and uses the connection to command the malware what to do. As malware needs constant communication, it is easier to find it than in case of intrusion. I find all IPs the device is communicating with. I get some statistic, as how much communication went to which destination, if the communication was opened repeatedly and so one. Afterwards, I check the details of the communication between suspicious IP addresses." [P1]

P1 described nicely the process of the investigation and talked about the time demands for the investigation.

"Let say that our case would be, that we would focus on ten users and the question would be 'Are these users infected, or not?' And if we found them as infected, we would like to know with what.

Just the first question, if 10 users are infected or not, takes about 3-8 hours to clarify, according to the experience of the analyst and to the complexity of case. I personally would be able to analyse 10-50 users per day only for answering this simple question. The question 'What they are infected with' takes much more time.

If I know one user is infected, I make deeper analysis to find what he was infected with. This may take hours or even days – that depends on if the infection is something known, if the binaries include some indicators of compromise. If I find nothing, I must go even deeper, especially if the malware is new or somehow weird. For the known threats, it takes about 4 hours to identify them.

I use command line to filter out important logs. I separate them by users and make a manual, text-based hunting. Any tool, which helps text processing, is useful. I also used Splunk a lot.

After manual hunting analysis, there are more possibilities what to do, according to what I found. And if I found nothing suspicious, there would be always things to try. For example, I may not focus just on the network logs, but also on inconsistencies. If the user uses Windows, he has a sort of profile, which corresponds to some user agency. I can check the Windows parameter, whether there is something weird, which wouldn't fit the windows picture – e.g. iPhone-like request sent from Windows. I search

for anomalies and for doing this, I need an experience and I need to have comparison to stuff which I know.

E.g. if the outgoing communication from victim device went to thousand outside addresses, I check them, check their reputation, what should be their content and then I have just a few addresses left and I may dive into logs between victim and this few outside addresses." [P1]

Most of the participants lifted out the communication, as a key need for analysing. It is very important to communicate between the teams and with colleagues, so that they don't analyse the same data twice.

"For communication we use Slack and Google docs for sharing and collaborating. We use also a great collaboration tool called Realtime board. There you can create a graph of the attack, add info from Linux, various files, pictures, it allows to put data in different formats - sometimes ports opening computer, screenshots of attack, maps, timelines, Google files… It is a customizable tool and usually about ten to twenty people put their content into it at the same time." [P2]

2.5.4 Analysis goals and use cases

In this section we will list some possible security problems and analysis question, as well as mentioned cases, which we collected during the interviews.

Privacy leaks detection

"A case of privacy leaks may be, when a security camera streams a video and is connected to an IP address, which changes. This change may mean that an attacker got into the camera and started to send the video to attacker's address. Therefore, the analyst wants to know what everything happened before?

However, the change of IP address (or other entity, e.g. web), must not always be wrong. For example, the owner of the camera may monitor his house and when he goes on vacation, he starts to send video to the hotel instead of default location. There are also some higher operations – e.g. when the device wants to download updates, and therefore connects to another IP address than the default one.

For such changes, there are more approaches to react, as the change may be malicious as well as safe. In case of Antivirus and malware chasing, the change must be blocked immediately. In case of security cameras, there could be used an approach to contact the owner with the message, that something changed, and leave the decision on him." [P5]

P5 also mentioned the importance of the content. It is a big difference, if the leaked video would be a video of someone's garage, or from a bank counter, where some very confidential information might be seen.

Same issue was mentioned by P2, who prioritizes the cases to analyse according to the status of the victim. Even a less-harmful attack may become critical, once the victim would be a CEO of the company, or a confidential company server.

Another case may be when some sensitive data were sent to an IP address, where they shouldn't be sent to, e.g. somewhere out of the company network. Analyst wants to explore how the traffic to the IP address was. He needs to know, it there was just this one leak of sensitive data, or if there were more data sent to that IP address.

Intrusion problems

"Let's imagine an IoT device, which has not an ideal protection, and is connected to the network, e.g. an outdated IP security camera. Camera logs to router and forwards its opened port (by using protocol

UPNP – universal plug and play) to port 23, to be accessible from outside. Router accepts and camera shows on port 23 its telnet protocol. Telnet running is a mistake, but it is still very popular. There comes an attacker from outside, searches for opened ports and tries port 23. Router asks the attacker for username and password. Attacker uses a dictionary attack, guesses the passwords and gains access. It notifies the command and control server, which sends a telnet command to download the botnet binary (via wget or tftp command) [s7]. This binary starts botnet processes. Binary may be caught and analysed, reconstructed and shared on VirusTotal. The file is not encrypted, as it went through telnet.

Anyway, once the botnet binary is on camera, it starts to run and make an nmap scan of whole network (i.e. mass scan) and searches for more opened ports. Once the attacker makes a successful intrusion into network, he may enslave more devices and make huge damages. For example, the attacker may enslave a speaker, which is not critical device by itself, but it may be close to the computer, which listens to Alexa device. Attacker enslaves Alexa with voice commands from the speaker and therewith takes over the control over the computer." [P5]

How to identify malware? Is the file malicious or not?

"I manually create rules how to identify malware. Half of my task is to find what could be wrong and think up the rules. I develop a lot of small programs in Python or Scala to help me with identification. I search for strange URLs, which tries to look like other domains – for example 'googleplay.info'. I search for sequences in malicious files to define a rule like 'Whenever this sequence occurs, block the file.' I use heuristic detection a bit, but it is rather inaccurate. I analyse web threats, as html and JavaScript or other scripts which try to do something evil." [P4]

Do my rules work properly?

With malware identification is also connected the task to control, whether the rules work properly. P4 must check that the application runs properly and how many messages about catching suspicious files are in queue. If the rules would be wrong defined, system would catch too much healthy files as suspicious, or by contrary, won't catch enough threats. P4 must check, that the detection isn't active too much.

Is this file / behaviour / email a threat?

"I search online for similar email, indicates of compromise, and maybe I find some malware which is sending these emails. I get all the emails in the company, which were going through the same servers. Or I have text in email and make a natural language processing, isolate some features and cluster emails with similar texts, because I search for an anomaly, which could be a threat." [P2]

Which computers were receiving and moving the malicious email up to the point we caught it?

"If I have IP addresses, I can check who is it, its reputation. I can check which receiving headers are fake, because someone can inject a false header – you can simulate a route through some count of computers, although it is not true. I check who sent the email? Is it a real email address?" [P2]

Is the obfuscated file a malware?

"Obfuscated files are unreadable as plain text. Often malware is obfuscated for not being recognized. However, obfuscation is used also for safe files, because some of them want to walk around ad blockers, some others do it for making the file shorter. I must decrypt files to be able to identify if the file is dangerous. There are many tools for decrypting obfuscated texts, however, it makes the job harder." [P4]

Who attacked my device?

"I go to see who was logged in which time – so maybe I need the timeline. I watch the addresses and which country they were connected from. Then I manage these pieces of information until I finish." [P2]

"Computer is infected, because the user visited a concrete domain. I try to uncover the infrastructure behind. I have seen who was on the server, if there were some similar users registered etc. Then I use whois database and search for relations and connections." [P3]

Which was the attack?

"I don't care who attacked me, I care what happened, so I go to the log of application, or to the content of the packets, or to files, which somebody left in the computer. I search for specific hash or content, which would identify the treat. I create a correlation graph or correlation table to investigate." [P2]

"The computer is infected, but there is a vast number of domains, it would be a very large graph. Therefore, I firstly search for domains, which was visited only by the infected user. Or I check if the user behaved somewhere differently than in other domains." [P3]

Am I being attacked? Are there attacks in flow, or not?

"I use Stratosphere tool for controlling the flow of information – are there attacks or not? We collect too much data, it is continuous infinite flow of network data, like two to three gigabytes in one minute, therefore it is impossible to make a graph. I need some detectors to find the incidents automatically." [P2]

Policy monitoring

"Organizations have some policies. In the policy we prohibit and monitor some actions, as a visit of any porn side, using peer-to-peer, watching movies on Netflix, some corporate employees cannot access to social sites in work hours… We have some constraints as part of the policy and we put own policy in the tool.

Then we are monitoring the network flow in real time. We want to alert once the policy is broken, and take an action, which is related to threat intelligence. For this use case, I need real time, I don't care about the timeline. But sometimes I may need to check history.

However, policy is usually not very interesting for us, as there the policy and security issues are others. There are just a few cases, in which was the security threat related to policy breaking." [P2]

2.5.5 Example investigation

Participants mentioned some procedures, from which we build two examples of investigation.

Investigating malware

One user in company was attacked by malware. Firstly, analyst analyses whether the attack was successful or not. Once it was not successful, he changes the priority to much lower.

Once the attack was successful, he is analysing the infected user. The main task is to find out what happened by this one user.

When he knows everything about what happened by one user, and he has enough time, he analyses other users. There are two use cases. The time of the infection is known. One use-case is to care about presence and future – what happens to the victim and what is the behaviour of the attacker. Second use-case is past. What happened by the victim in the last week? Was the attack repeated before?

There are many ways how the concrete analysis may look like. For example, the malware came from injurious URL. With CTI sources analyst finds all URLs, which may have something in common with the malware. Analyst searches for other victims by indicators of compromise. He analyses the behaviour of the infected user, e.g. if the victim spreads the malware. Analyst wants to see the communication of the user in the past.

Unauthorised access

One user has connected or tried to connect somewhere in the company (to a private address), where he shouldn't have access. Analyst wants to find out if it is an attack which depreciates authentication rules, or just an error in access configuration. For investigating this, it could be helpful to know how many times connected the user to the address and which other users connected to the address (are there more users, which shouldn't have access rights?).

If someone unauthorised has connected to one of sensitive confidential company servers, the analyst needs to know, if it happened just in case of one server, or if some others are in danger. Therefore, he should search also for traffic to other servers.

Another case to solve is when there are too many connections blocked, e.g. by firewall. There may be more reasons for that: either there is an attack, or the firewall is wrongly configured. Analyst dives into collected logs and explores them, if they were caught correctly or not.

Some incidents can be focused on repeated actions, as changing a password for many times in a short time frame or repeated tries to log in somewhere. Analyst may explore these events and find what happened, whether these tries were done by the real user, trying to recall his password, or if it is an attack.

2.5.6 Wanted qualities of investigation tool

We discussed with the participants, what functions an investigation tool should have, what are the disadvantages of current tools and what are the key properties of tools for cybersecurity analysis.

Key quality of the tool is to make processes quicker than before.

"Visualisation for security is super artistic nowadays. It is hard to guess 'what if…' It is hard to put everything at one place. Therefore, it is important to put in as many constraints as possible. It shouldn't be a global tool to answer all questions and solve all malware in the world. But essential is to be quicker in solving a particular task by using the tool." [P2]

Hand in hand with the effectiveness and lack of time goes a need to have a good overview, sum up of the incidents and a possibility to prioritize.

"First page must show enough to decide what to analyse first. We analysts would like to review everything and make sure there is nothing dangerous, but there is never enough time and human resources to do so. Therefore, we need to discover normal and suspicious behaviour as soon as possible. The first page should highlight what to look at and show priorities. I want to see aggregation of what happened and if the attack was successful. How many attempts to attack were there? And I don't have much time to read through, therefore the text should be as short and apposite, as possible. I would also appreciate to see time estimation for analysis. Which can, of course, change – e.g. when the time press enables me to check two users and then I must move to another incident when nothing found." [P1]

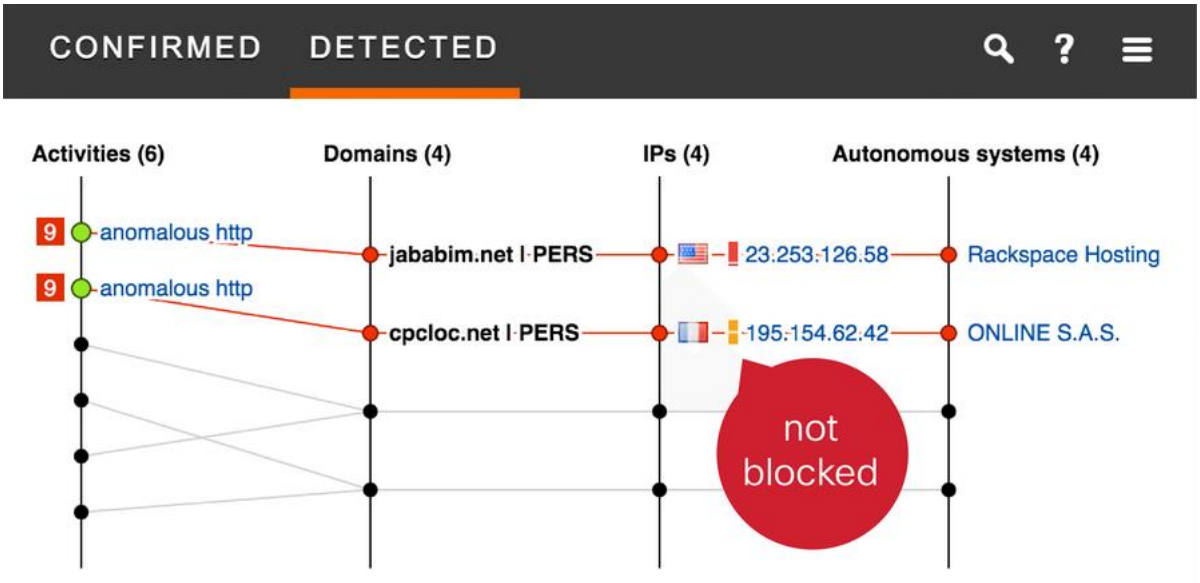
"I want to have a possibility to create high-level views. Create from packet flows sequences bigger aggregations. I want to see descriptions as: 'Someone is scanning 100000 IP addresses and he is doing it for 20 minutes.' Or 'Someone is doing a dictionary attack on port 23.'" [P5]

“I must see a sum up in the introduction menu. I want to see prioritization and some quick statistics, as the number of victims, the attacker, how many times the event occurred and some proportions. A common case could be 1000 attacker from e.g. China to one victim as company server for 1000 times – those attackers are virtual bot computers and they are trying to get in the victim’s device. I want to know who the victim is. Is it a human, as my colleague, or a device, as server or printer? Is it the CEO (Chief executive officer), or someone less important? I want to slide quickly down the menu and know what happened and where to start.” [P2]

“There are so many tasks, that I must prioritize it. When something shows not to be as important, I need to postpone it or discard it, once there is something more important to do.” [P3]

P1 liked the visualization of a sample reports on cognitive.cisco.com, as it has an interesting level of aggregation and prioritization.

1 [i1] Sample threat findings, Overview of identified threat categories.



2 [i1] Sample threat findings, Banking trojan

Another important quality of the tool is to enable communication within the team. In the menu the analyst should check who works on the incident.

“I want to comment on the task on the main screen. I want some functions from issues tracking products as JIRA – who is working on the task, what is the priority, assign the task to someone, write

quick notes. The notes help to hand over the task to a colleague, if he is specialist, or if it is urgent. Or I want to catch gained information, so that I can follow up the next day and jump quickly to the problematic. Analyst have sometimes too much to remember, so I need to write down my ideas." [P2]

The tool should be very customisable. P2 mentioned, that the configuration of the interface should be able to help the experts and newcomers to see different levels of detail. P1 said, that every analyst in team uses different dashboard and different statistics. Also, P5 wants a possibility to scale up and define own events and incidents.

When exploring the details, P2 wants to highlight what triggered the attack. P5 wants to see some graphs, subgraphs, tables and dashboards like from Grafana. P1 would welcome enriching from online sources, as it is exhausting to go to VirusTotal every time and check everything manually.

P2 discussed use of timeline graph, that he searches for daily patterns. He rather compares traffic with same time another day than with time around the event. He wants to see, whether the victim was attacked before that week, etc.

P1 also talked about the pros and cons of Splunk, which is one of the leading tools. "Splunk is paid, mostly for amount of data. Therefore, it is very expensive solution, as we have traffic of millions of users, which means gigabytes per day. We must decide what to use and what not to optimize the expenses. Input is usually a big JSON, which is interpreted by columns and axes. Input must be well structured, which takes a long time. We must prepare the input, there must be no empty values, the values must be used properly, we cannot mix numerical, text and categorical inputs. And the logs don't always have the same structure and we must map some properties on the adequate one.

But what is good, in Splunk we can make great dashboards. The tool consumes data, gives timestamps to it and sorts it. We can than make some queries, as 'show me the top 10 destination IPs', we can compare traffic with previous period of time, it can generate nice tables with predefined functions. We can get all users visiting a given server. But we have to define own statistic, dashboards, configuration and visualizations." [P1]

2.5.7 Investigation tool development

As mentioned in the introduction, participants P6 and P7 work on backend for an investigation tool, which will be an extension component for an existing SIEM system. Firstly, they explained to us the cooperation between SIEM system and investigation tool.

SIEM system is a collector of many information. Some datasets can flow into SIEM in real time (as network logs), some can be inserted, as in-company catalogues (e.g. factory statistics, data about sold products etc.). SIEM system recognizes potential threats, e.g. by machine learning, sophisticated definitions (overtaken e.g. from antivirus systems) and custom definitions of rules for filtering out the incident. Example custom definition may be 'Filter out, when someone fails to log in to one URL for more than 100 times in 10 minutes.' Based on definitions, SIEM queries the database with stored information and therewith identifies incidents and related dataset.

List of triggered incidents and associated logs is delivered by the SIEM system to the investigation tool, which groups small logs into events, makes aggregations and extends data by information gained from enrichment sources, as reputation.

SIEM system itself has a lot of components, cares about real time reports and helps to solve other analysis tasks than the investigation tool. Other SIEM components are not important for the investigation tool creation and the developers don't know much about its function.

P6 and P7 talked about the technologies they use and about problems they considered while doing this choice. We discussed used libraries, graph creation, data storage and mechanics working on backend, however, this information is not important for the RSI[3] design, as the technical solution for backend may vary.

Investigation tool, as presented, was not suitable for laymen, because there were some complicated components which the analyst will learn to work with. Developers were searching for a compromise between user control, usability and intuition.

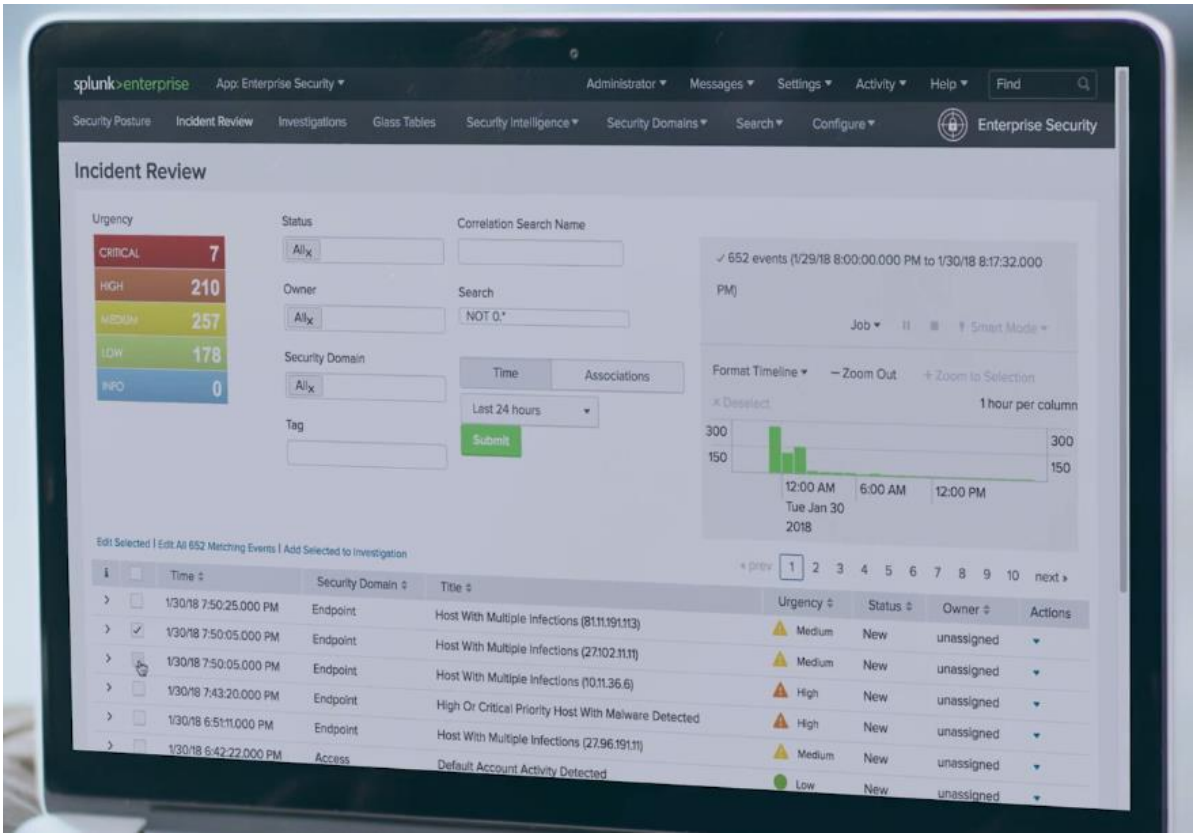
2.6 State of the Art Analysis

In this chapter we will describe technical background of the problematics. Firstly, we will point out some SIEM systems and SOAR or graphical tools. Afterwards we will make an introduction into types of logs and their structure. We will describe enrichment sources, mentioned by interview participants.

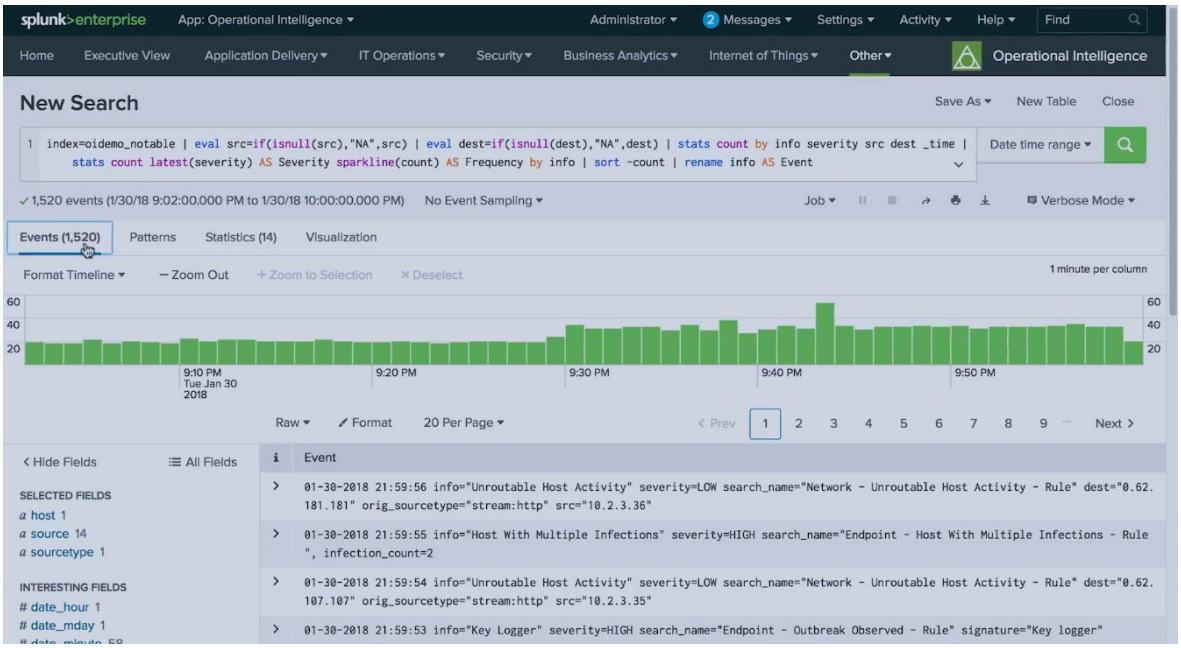
2.6.1 Existing tools

Splunk

Splunk is a company providing more products for different solutions, as application delivery, business analytics, cloud solutions, IoT & Industrial Data, IT Operations, Log Management and Security & Fraud. Log management enables Splunk users to index machine data, search, correlate and investigate, make drill-down analysis, monitor and alert and create reports and dashboards [s8]. Splunk also has components for Incident Investigation and Forensics: Analyse and confirm high-priority incidents to determine the circumstances and scope of an incident while appropriately handling incident investigation and response [s9]. Splunk is a robust solution, however, it is commercial, and therefore very pricey for big amount of data.



3 [i2] Splunk: Incident investigation forensics



4 [i2] Splunk: Incident investigation forensics

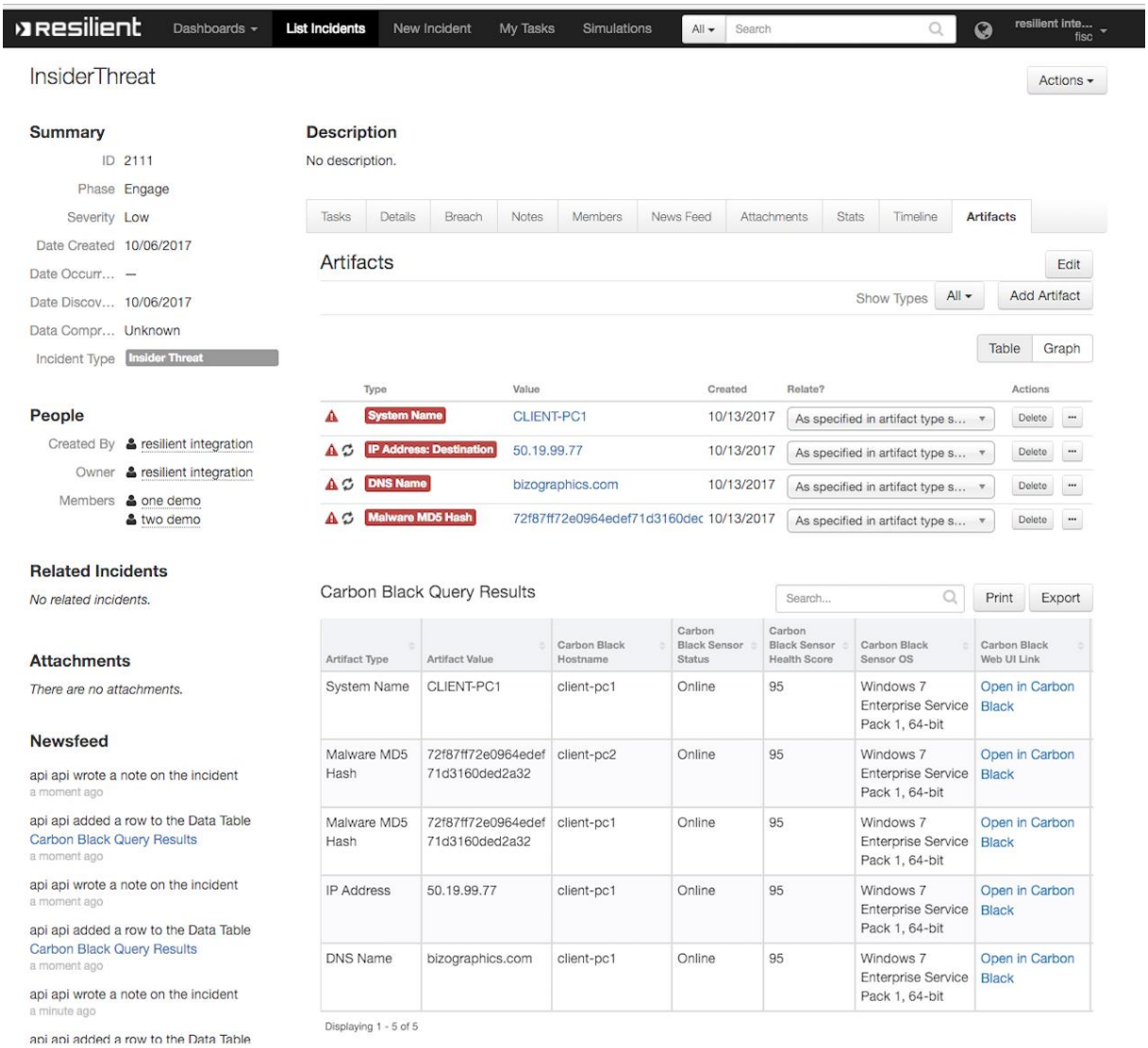
IBM solutions

IBM is dedicated to the development of security software. Among their solutions, QRadar is a SIEM system, which can be combined with case management system Resilient and Analyst's notebook i2. These solutions cover many use-cases of incident investigation. However, the solutions were developed by different divisions and therefore contain overlapping in data organization and don't have united design and data loading processes.

IBM i2 Analyze is an enterprise intelligence analysis environment that enables information sharing and intelligence production with the flexibility of both web-based and rich desktop clients. It facilitates analysis of large volumes of data through an extensible, service-oriented environment designed to integrate into existing enterprise infrastructure. [s10]

IBM QRadar SIEM helps security teams accurately detect and prioritize threats across the enterprise, and it provides intelligent insights that enable teams to respond quickly to reduce the impact of incidents. By consolidating log events and network flow data from thousands of devices, endpoints and applications distributed throughout your network, QRadar correlates all this different information and aggregates related events into single alerts to accelerate incident analysis and remediation. [s11]

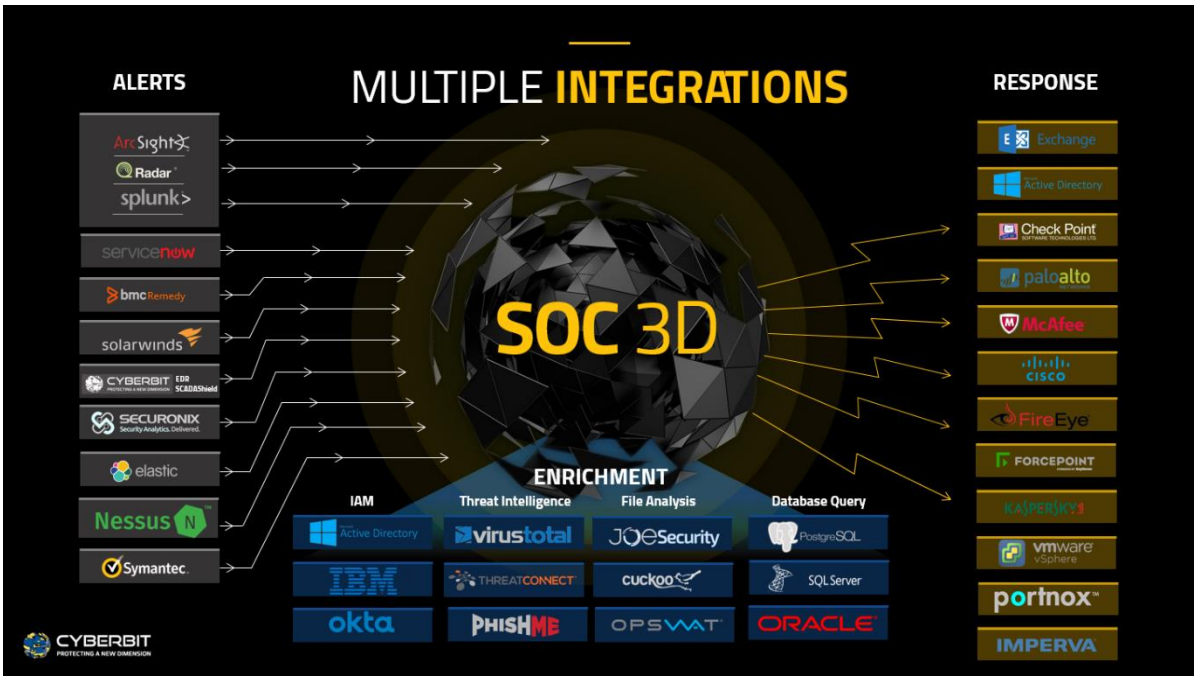
IBM Resilient Incident Response Platform cares for orchestrating and automating incident response processes. It makes security alerts instantly actionable, provides intelligence and incident context, and enables adaptive response to complex cyber threats. Dynamic Playbooks provides the agility, intelligence, and sophistication needed to contend with complex attacks. [s12]



5 [i3] IBM Resillient: Query results

SOC 3D

SOC 3D is a SOAR solution developed by company Cyberbit, who is also concentrating on other security solutions, as Endpoint Detection and Response, ISC/SCADAShield and Cyber Range for security training and simulation platform. SOC 3D is SOAR platform combining automation, orchestration, and big-data powered investigation into a single and comprehensive incident response platform that triples SOC efficiency, provides unprecedented visibility and reduces time-to-respond by 90%. [s13]



6 [i4] SOC 3D: Integrations

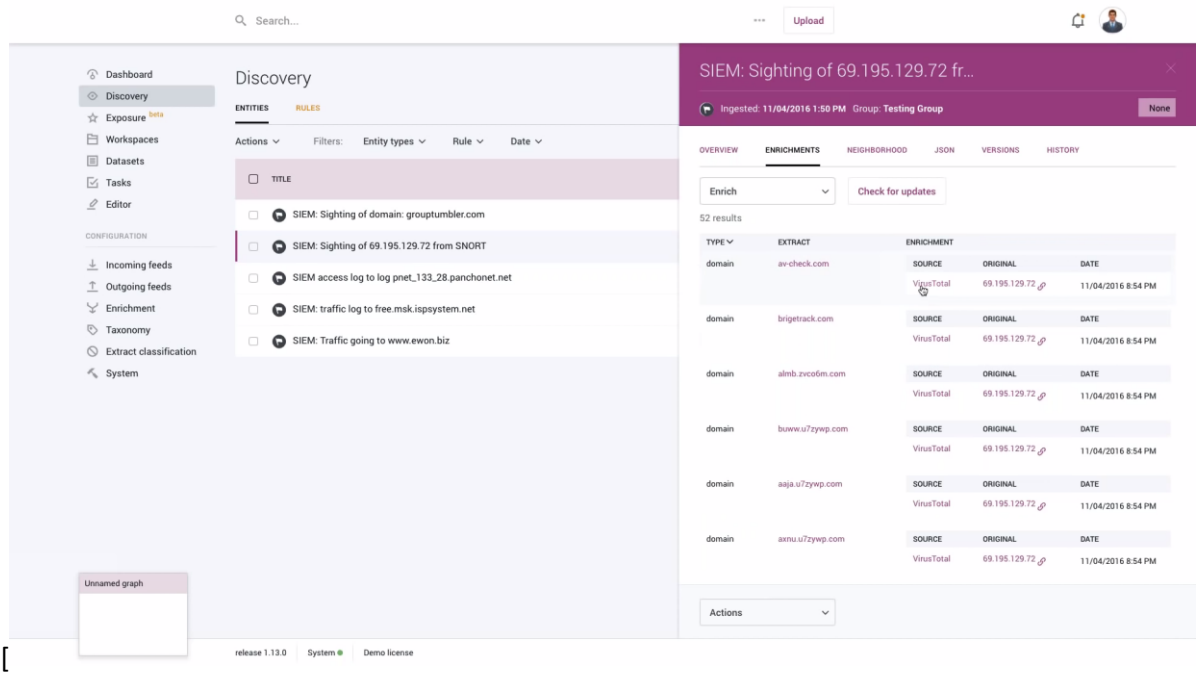
ManaTI

ManaTI is a tool created by The Stratosphere IPS project, which was born in the CTU University of Prague in Czech Republic. The goal of the ManaTI project is to develop machine learning techniques to assist an intuitive threat analyst to speed the discovery of new security problems. The machine learning will contribute to the analysis by finding new relationships and inferences. The project will include the development of a web interface for the analyst to interact with the data and the machine learning output [s14]. ManaTI works rather with the text form of logs than with dashboards visualization.

7 [i5] ManaTI: Home table

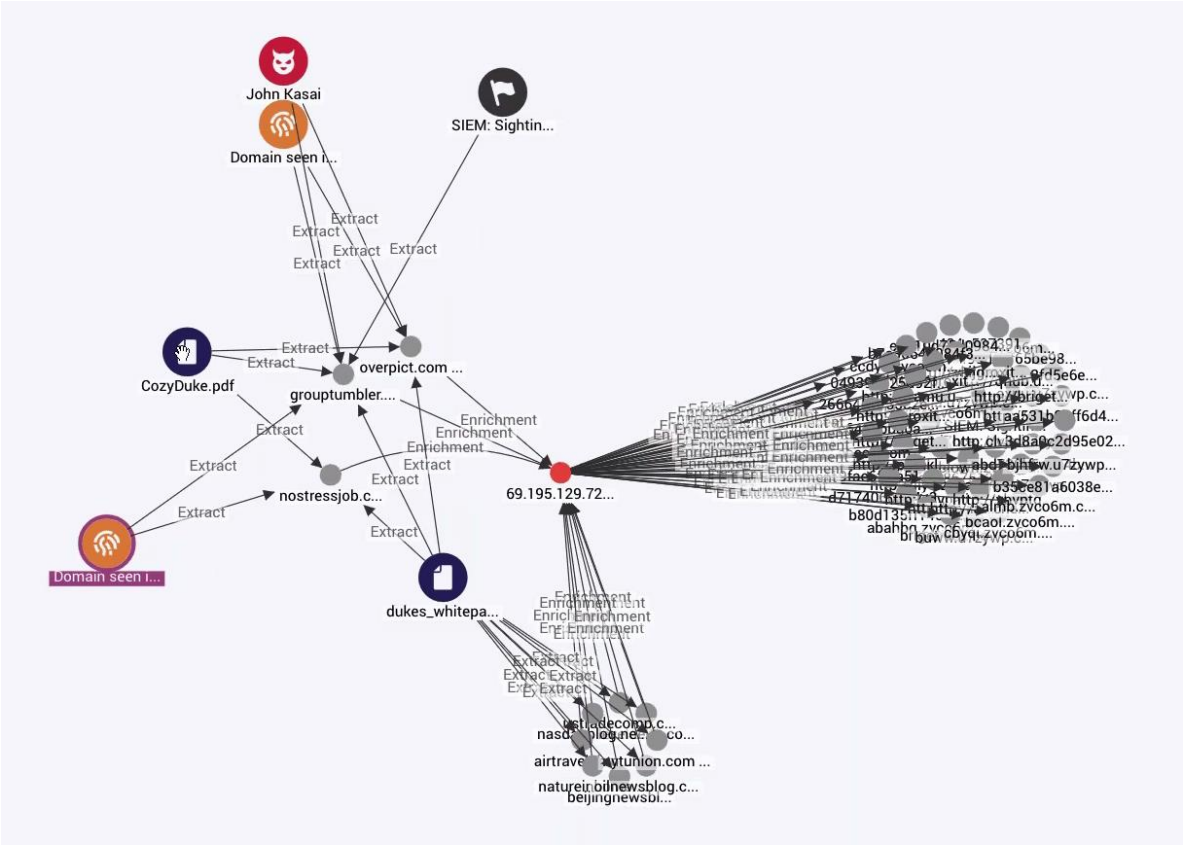
Keylines

Keylines is a commercial tool for building powerful custom network visualization applications. It has features such as customization, compatibility with browsers, automatic layouts, node combining and grouping, network filtering, social network analysis, time bar and geospatial networks. [s15]



[

8 [i6] Keylines: Incident page



9 [i7] Keylines: Graph expansion after three steps

Grafana

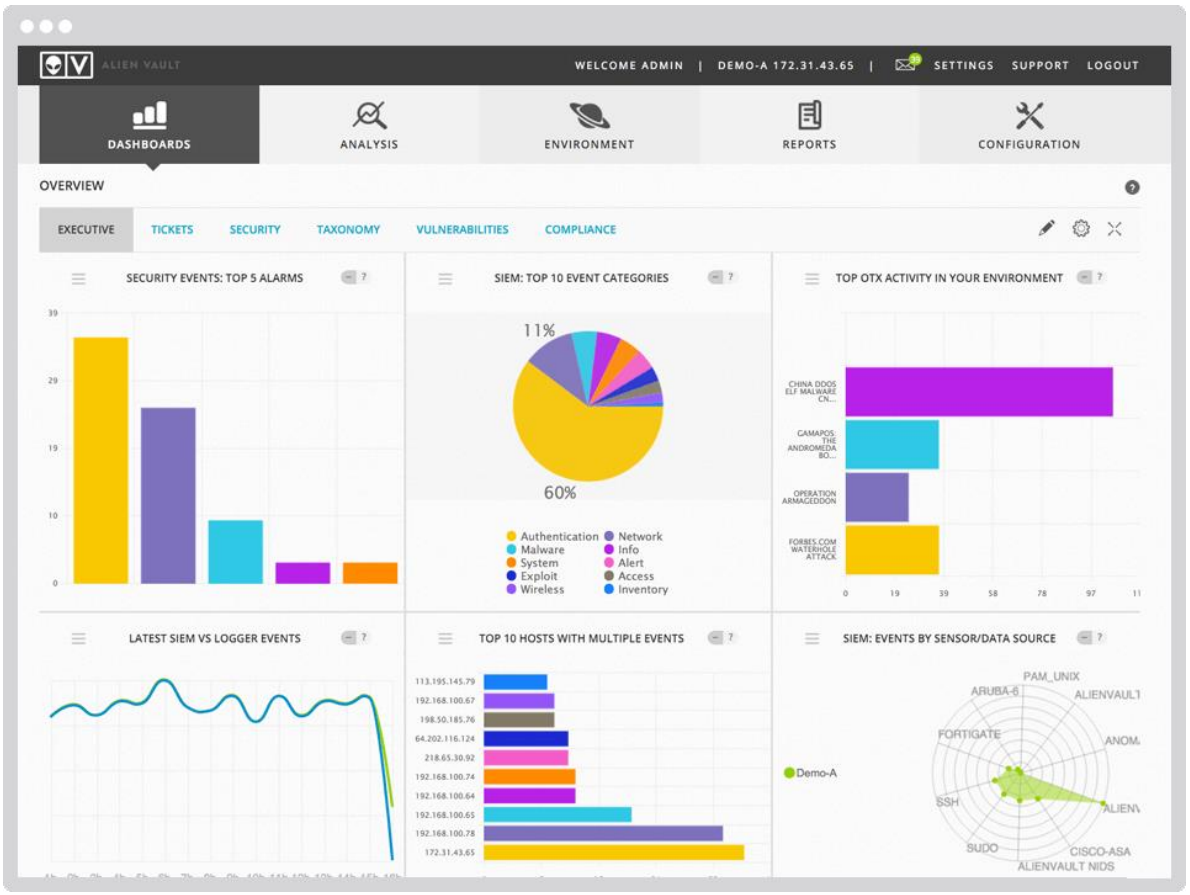
Grafana is an open platform for analytics and monitoring. It allows to query, visualize, alert on and understand metrics no matter where they are stored. Create, explore, and share dashboards with your team and foster a data driven culture [s16]. It is a tool rather for nice visualization and custom dashboard creation than for concrete analysis.

Linkurious

Linkurious is an on-premise graph visualization and analysis software that helps uncover hidden threats and opportunities from anti-money laundering to cyber-security [s17]. Linkurious focuses on general data analysis, not on security incidents investigation.

AlienVault

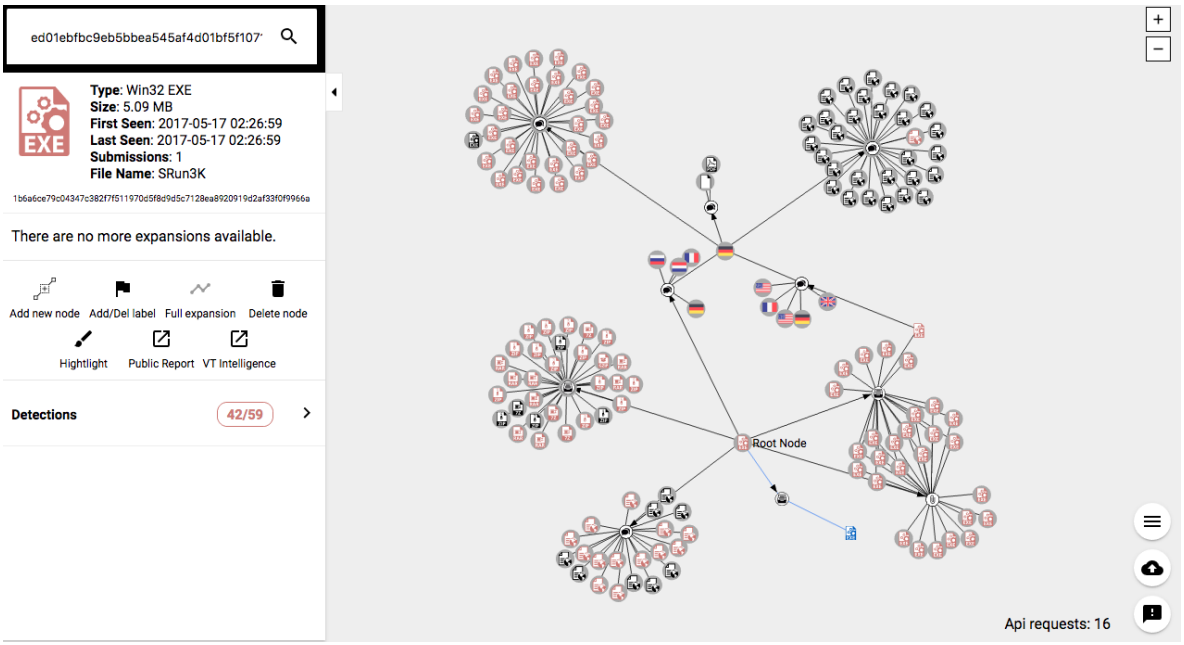
AlienVault offers a commercial solution, as well as an open source SIEM. The open source version provides capabilities as asset discovery, vulnerability assessment, intrusion detection, behavioural monitoring and SIEM event correlation [s18]. The commercial version USM Anywhere provides some more features, as log management or threat intelligence.



10 [i8] AlienVault: Dashboards

VirusTotal

VirusTotal Graph is a visualization tool built on top of VirusTotal's data set. It understands the relationship between files, URLs, domains and IP addresses and it provides an easy interface to pivot and navigate over them [s19]. The tool helps the analyst to watch the circumstances around malicious issues, however, it doesn't help to analyse concrete incidents, as it doesn't focus on events.



11 [i9] VirusTotal Graph example

Other solutions

We have mentioned just some of current solutions. There are many commercial products, which differs in pricing, use cases, investigation covering etc. Another examples of SOAR can be Phantom Cyber, Demisto, ServiceNow SecOps and Swimlane. Regarding SIEM, there could be mentioned some leading companies, according to "Magic Quadrant" evaluated by Gartner [s20], a research and advisory company – LogRhythm, Dell Technologies (RSA), Exabeam, MacAffee, Securonix etc.

2.6.2 Logs sources and description

There are plenty of systems which generate logs. Logs can be collected in firewalls, active directory, router, database, syslogs from applications, Microsoft exchange data, emails, device logs etc.

According to Chichonski et al. [s2], we could divide the logs into three groups:

Logs from operating systems, services, and applications (particularly audit-related data) are frequently of great value when an incident occurs, such as recording which accounts were accessed and what actions were performed. Organizations should require a baseline level of logging on all systems and a higher baseline level on critical systems. Logs can be used for analysis by correlating event information. Depending on the event information, an alert can be generated to indicate an incident.

Logs from network devices such as firewalls and routers are not typically a primary source of precursors or indicators. Although these devices are usually configured to log blocked connection attempts, they provide little information about the nature of the activity. Still, they can be valuable in identifying network trends and in correlating events detected by other devices.

A network flow is a particular communication session occurring between hosts. Routers and other networking devices can provide network flow information, which can be used to find anomalous network activity caused by malware, data exfiltration, and other malicious acts.

Difference in the sources is the reason, why the structure of logs always differs and contains a lot of heterogeneous parameters.

For making the design process more concrete, we will focus on network logs with following structure:

- Date, start time and duration
- Sender IP address and port
- Destination IP address and port
- Content of the data – number of packets, number of bytes and description.

2.6.3 Threat Intelligence

Threat Intelligence enrichment sources are an important source of data, which are shared across the community. Community data may be more reliable than some official sources, as there are many experts on cybersecurity. In this section, we will describe some enrichment sources, which were mentioned by the interviewed participants, as there are many possible sources.

VirusTotal is a free online service that analyses files and URLs enabling the identification of viruses, worms, trojans and other kinds of malicious content detected by antivirus engines and website scanners. At the same time, it may be used to detect false positives, i.e. innocuous resources detected as malicious by one or more scanners. [s21]

RiskIQ PassiveTotal expedites investigations by connecting internal activity, event, and incident Indicator of Compromise (IoC) artefacts to what is happening outside the firewall—external threats, attackers, and their related infrastructure. PassiveTotal simplifies the event investigation process and provides analysts access to a consolidated platform of data necessary to accurately understand, triage, and address security events. [s22]

Cisco Talos Reputation center is a real-time threat detection network. The data is made up of daily security intelligence across millions of deployed web, email, firewall and IPS appliances. Talos detects and correlates threats in real time using the largest threat detection network in the world spanning web requests, emails, malware samples, open-source data sets, endpoint intelligence, and network intrusions. [s23]

The **MISP** threat sharing platform is a free and open source software helping information sharing of threat intelligence including cyber security indicators. It is a threat intelligence platform for gathering, sharing, storing and correlating Indicators of Compromise of targeted attacks, threat intelligence, financial fraud information, vulnerability information or even counter-terrorism information. [s24]

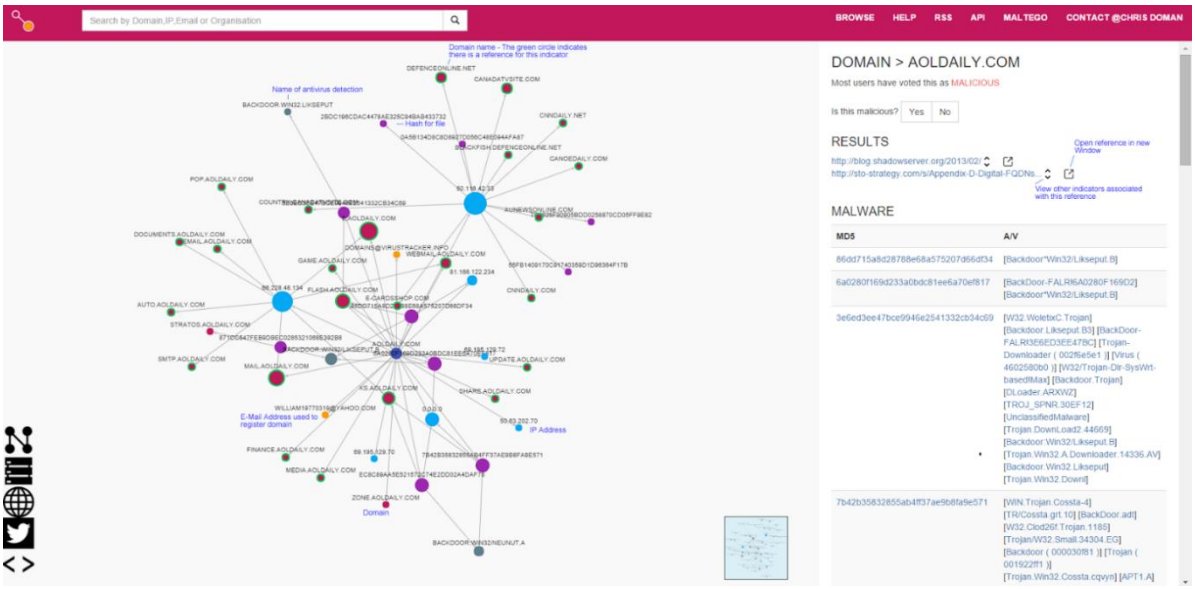
urlscan.io is a service to scan and analyse websites. It queries external services to determine whether a page is malicious. [s25]

WHOIS is a query and response protocol that is widely used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block, or an autonomous system, but is also used for a wider range of other information. The protocol stores and delivers database content in a human-readable format. [s26]

AlienVault OTX - Open Threat Exchange is the neighbourhood watch of the global intelligence community. It enables private companies, independent security researchers, and government

agencies to openly collaborate and share the latest information about emerging threats, attack methods, and malicious actors, promoting greater security across the entire community. [s27]

OTX powers also a **ThreatCrowd** search engine for threats.



12 [i10] ThreatCrowd

2.7 Challenges to be solved

Many challenges come to consideration when developing an investigation tool. We identified nine of them:

2.7.1 Be quicker

The tool must make the process quicker than the current solution, otherwise the analysts will not use it. This implies many developer challenges – e.g. quick rendering, big data processing, queries on historical data, quick data fetching from external sources, automation of some workflow processes, scalable deployment infrastructure, and others.

However, there are many front-end challenges as well – e.g. placement of control panels on intuitive areas, small number of user actions needed to gain results (e.g. quick filtering for overview as well as few steps for detail view - the graph should be extendable in a few clicks and at the same time it should be still transparent, etc.).

2.7.2 Be practical

Today's trend is to create a lot of nice visualization and dashboards for showing the results. Analysis by using graphs and tables can be trendy and effective, but it must be combined with the quickness, as the analyst has no time for waiting on a nice graph to be drawn. All participants said that they prefer "quick results over nice pictures." The gamification respect, which is often considered in UX design, has to step aside.

2.7.3 Overview and prioritization

RSI[3] has to give an effective approach to information. There should be a transparent sum-up and overview on frontend, which shows everything important at once with a minimum of text (as reading is time consuming).

Big challenge at the server side is the interpretation of data fetched from SIEMs and other sources. This includes incidents identification (e.g. merging repeated SIEM alerts into one incident, rejection of false-positive alerts) and prioritization of the incidents.

2.7.4 Collaboration

RSI^3 should enable communication, knowledge sharing, and collaboration within the team. There must be a possibility to assign tasks, to comment, and to make sufficient documentation (share pictures, comments, links, maybe even documents). The tool should also catch the investigation processes (e.g. in form of replays), so that the team members can learn from each other.

2.7.5 Customization

The investigation process is not united as each analyst has different needs, experience and specialization, and the incidents are unique, as well as the categories of them. It is hard to define global workflow scenarios, as each investigation is specific and there are many exceptions. Therefore, there has to be a possibility to customize items. Customization should be done on two levels. Each company or a SOC team should have a possibility to create own list of important devices, customize form of input data, data resources and influence the calculation of automated algorithms. Second level is the customization for each user - specialists and newcomers need to see different levels of detail and therefore they must have a possibility to edit their dashboards and overview of incidents etc.

2.7.6 Data enrichment

The data should be automatically enriched by all available information from various enrichment sources on backend. Searching for data on more places is time-consuming and therefore bringing the data to one place, where the analyst can compare and select data according to his actual need will help to make the process of investigation quicker.

2.7.7 Detail

RSI^3 should enable the analysis in more detailed levels, starting from the overview, ending by detail of one log. RSI^3 should work in compliance with Shneiderman's visual information-seeking mantra: "Overview first, zoom and filter, then details-on-demand." [u5] There should be a possibility to filter out and show the results in more forms – table, graph, timeline etc.

2.7.8 Persisting intermediate findings and results

There should be a possibility to export the data and to preserve the state of the analysis. The work done by the analysts should be recorded. This can be used afterwards for continuing in investigation, replays, reports (e.g. the data could be sent to SIEM or project management systems for detailed reporting), and also as data for tool automation.

2.7.9 Automation

The tool should automate as many steps of the analyst's workflow as possible. An example of the possible automation processes on the backend can be the prioritization, enrichment, automated investigation etc. Automated processes on the frontend could be demonstrated by alerts showing, replay of automated investigation, pop-ups of most critical incidents etc.

Another automation problem could be creation of so-called playbooks, which requires significant effort. [s1]

2.8 Focus

Resulting from previous sections, the creation of investigation tools brings a huge field of tasks and problems to be solved. The objective of this project is to examine graphical possibilities of the tool, primarily in breath. Therefore, we won't focus on problems which will be solved mainly by algorithms at the backend. E.g. the evaluation of alerts and their clustering under a single incident will be shown as a list of incidents, which will be accessible from the user interface. Backend will also solve such tasks as connection of data gained from SIEM, CTI tools and other sources. The prioritization and incident category will be solved on backend as well, based on previous data and intelligent algorithms, just as the subsequent automatization of investigation.

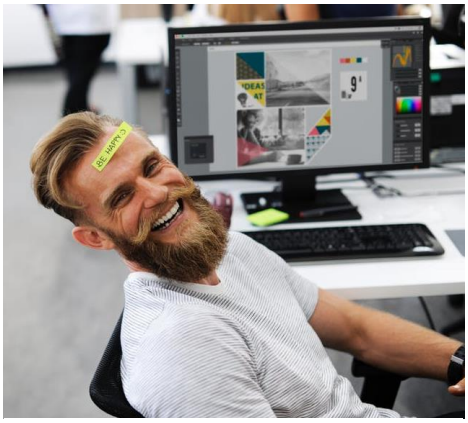
Our main focus is therefore orchestration – unification of functions provided by more tools into one, so that the analyst doesn't have to distract attention, transfer data from one tool to another etc. We will focus on overview and the path from dashboard to details, possibilities of collaboration and knowledge sharing and finally possibility to edit overviews according to analyst's personal needs.

3. Design analysis

In this chapter we will describe the process of RSI[3] designing. Firstly, we identified personas and current workflow. We introduced four scenarios and a storyboard, and consequently we described workflow within RSI[3] on two use cases and pointed out other functions, which need to be supported. Afterwards we presented and evaluated paper mock-ups, which capture main design ideas.

3.1 Personas

3.1.1 Eda



13 [i11] Persona Eda.

Eda is 44 years old. He studied Informatics at Saarland University in Germany and in the last year of his bachelor study he found the CISPA Institute and started to focus on computer security. He found his raison d'être in security and became an expert on threats investigation. As he is very communicative, he shares his knowledge with colleagues and helps them to get overview and he also partially supervises new colleagues.

Eda is very relaxed and optimistic person. He doesn't mind investing his time in something which he found helpful for others. However, he hates to spend his precious time with any bureaucracy issues. He uses Linux operating system and prefers work with two big screens, as he must work on more project parallelly.

3.1.2 Julia

14 [i12] Persona Julia

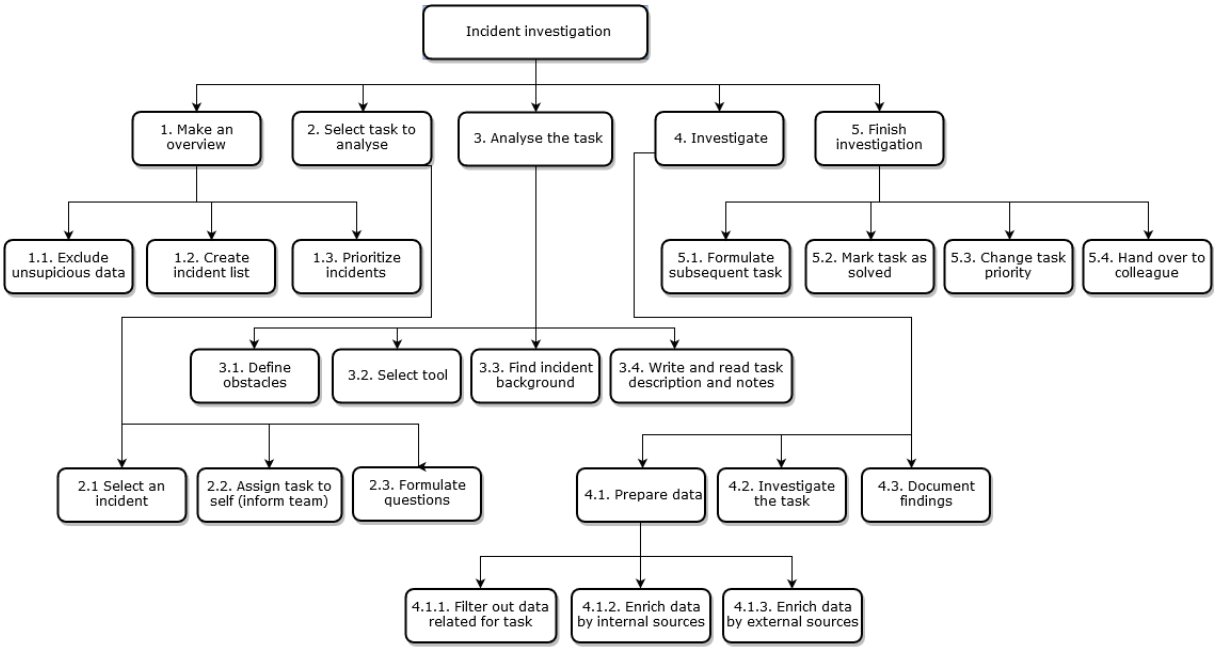
Julia is 24 and finished her master study in Information Management at the University of Economics in Prague, with having previous knowledge of Informatics gained by bachelor study at Czech Technical University. She was looking for her first job and was attracted by a position of junior security manager. She has just a few experiences with computer security, but she is a strong analytical thinker. She likes to have things sorted and clear. Once she gets a good defined assignment, she can organize her time and workflow very well and create quickly nice results. She is friendly and therefore her colleagues take care to help her to dive into her new job.

Julia is used to meet with a lot of people and she organized some university projects. She is a Windows user. She has a well-organized structure of her data folders. She travels a lot and therefore she likes to work on her laptop.

3.2 Current Workflow

Based on the information we got from the interviews, we sum up the process of the security incidents investigation. There is no general workflow, as there are many challenges and tasks to be solved and

each task demands an individual approach. Nevertheless, we summed up the abstract processes into a hierarchical task analysis diagram and we described the nodes.



15 Current Workflow Hierarchical Task Analysis

Hierarchical Task Analysis describes individual steps which might be taken. There are many ways, where the analyst may choose another way, there are many iterative steps and the realization of particular steps differs.

One of the iterative steps, which are present for the whole time of investigation, are the communication activities (2.2., 3.4., 4.3., 5.2., 5.3., 5.4.). Analyst makes notes for himself or for colleagues. The team should have an overview which task is assigned to who.

Analyst may jump back to some processes. For example, when he solves an incident, he may first search for an answer on the question “Was the attack successful?” Once he realizes it was (in step 5), analyst formulates new question as “Who is responsible?” (5.1.) and jumps to step 2 with analysing new task. In other cases, he may hand over the task to a colleague (e.g. specialist for attack category, machine learning researcher who finds patterns based on the incident, colleague who has a next shift…) and the colleague starts from step 3.4. – reads notes from previous task owner and continues in investigation.

1. Make an overview	The analyst goes through the process of evaluating SIEM data and alerts, making a list of incidents and assigning triage to them according to the available properties and description.
2. Select task to analyse	Based on own specialization and triage, analyst selects an incident to be investigated. He formulates the questions to investigate. E.g. Are the attacks successful? Who was attacked? Who is the attacker? What was the route of the attack? Did this happen before?
3. Analyse the task	There are some obstacles which should be identified (e.g. What are our data? Do we have access to data from device, or just network data?). Analyst chooses a tool for the investigation according to data and goal – whether he wants to work with a plaintext in the command line, with a graph in visualisation tools, whether he works with past data or real-time dashboard etc. He chooses the type of

	visualisation. Analyst sums up the known background, e.g. if he previously worked on a similar case and knows something. Analyst writes down collected knowledge to later recall and to share it with colleagues.
4. Investigate	Analyst does the investigation. He repeatedly prepares data, investigates it and writes down his findings, as long as he does not finish with the task. Data are enriched by internal sources (e.g. assigning the name of an employee to device), as well as external sources (CTI reputation, circumstances etc.)
5. Finish investigation	When the analyst is ready with the investigation, he may mark the task as solved. He may also change a triage, once he finds the attack is not essential and postpones the investigation, as there may be more crucial tasks. He may hand over the task to a colleague.

Table 3 Notes to HTA – Incident investigations subtasks

RSI^3 should replace some parts of the workflow done manually (e.g. part 1 – making an overview, omits task 3.2. as the functions will be part of RSI^3, help with incident background finding (3.3) and data preparation and enriching (4.1.). Therefore, the workflow with RSI^3 will differ.

3.3 Scenarios

We introduced typical scenarios how the RSI^3 could be used.

3.3.1 Making an overview

Eda comes to his job on the morning, greets his colleagues, makes a coffee and goes to his computer. He turns on RSI^3 and checks notification to see what happened in the time he was absent. He checks the chat and reads the messages from his colleagues. Eda looks on the overview of incidents. He walks through the incidents to see what happened, which incidents are already under the analysis of his colleagues, and which are suitable for him to investigate.

Eda decides what incidents he is going to work on today – he may continue in the previous analysis, or he may start a new investigation. To make this obvious, Eda prioritizes the incidents and considers also the automatic prioritization. Eda also assigns some incidents to his colleagues, when he knows he will not have enough time to solving them in contrary to his colleagues, or when he knows that some of the colleagues have a better knowledge for given type of incidents. Afterwards Eda starts to investigate incidents assigned to him one after another.

3.3.2 Investigation of a single incident

Eda decides to dive into an incident, which was classified as a malware attack with a high triage. Eda assigns this incident to himself and goes through incident statistics. He sees on timeline, that the activity on logs was first small and then it started to increase. He also sees that there are many data coming out of the internal network. Eda controls included IP addresses and guesses what might happen – probably someone from the company downloaded a malware which is now trying to steal some data from the company.

With this hypothesis, Eda goes to details of investigation and controls the relationships between the involved entities. He notes down his findings, so that he can sort out his ideas. He finds out the victim in the company and also public IP addresses, from where the malware was downloaded and where the data was sent to. Eda checks the reputation of the IP addresses based on connected CTI tools. He makes sure that the attack is over and checks what happened. He marks the malicious IP addresses to

be observed, so that he may check easily that the attack isn't continuing or repeating. After that, he marks the incident as solved and may take a break.

3.3.3 Learning and collaboration

Julia just finished her initial procedures and today she wants to investigate her first incident. She was assigned one incident with smaller priority for not being forced to rush. She wants to look at incidents from her colleagues with same category and learn how they proceed by solving it. She filters out similar solved incidents from the past and replays how the colleagues led the investigation. She reads through the notes regarding those incidents, and also reads the instructions shared in the team board. After doing this, she has an inspiration how to move ahead, and can start her first own investigation.

3.3.4 Personal configuration

When Julia started to work as an analyst, she wanted to see all available statistics about the incident, because she needed more clues to formulate the hypothesis. Meanwhile Eda has such a high experience, that he wants to see mainly graphs showing some incident patterns, because that is sufficient for him. That is why Eda and Julia need to configure their dashboards to see different information. Julia gets an inspiration by Eda's graphs and she adds some of them to her dashboard, but then she adds tables with more basic information. After doing such configuration, she opens overview of the incident she is going to work on, and sees tables with basic information and graphs, which help her to efficiently use her knowledge and formulate a hypothesis.

3.4 Storyboard

To demonstrate the usage of RSI[3], we created following storyboard.

16 Storyboard: Incident investigation. Created in storyboardthat.com

3.5 Use cases and functions

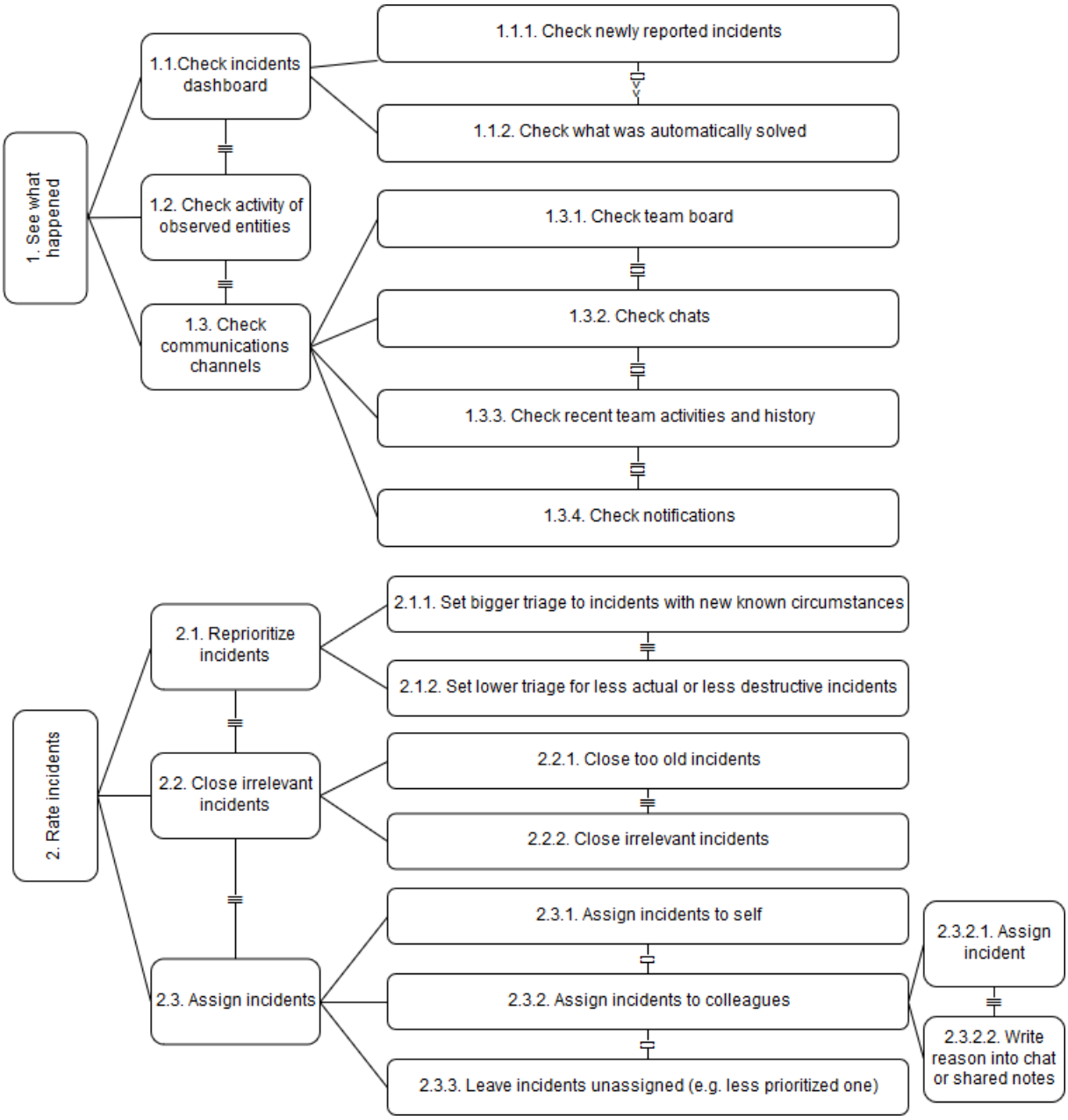
In this section we will focus on the main use cases of RSI[3]: Making an overview with the prioritization and investigation process. We also introduce three important functions, which support the use of RSI[3] and both main use cases: collaboration support, user management and tool setting.

3.5.1 Use Case: Making overview of incidents

Following Concur Task Tree breaks down tasks, which should be done to get an overview of incidents which happened previously (e.g. on the beginning of the work shift).

First the analyst sees what happened – the order of steps is interchangeable, but he checks incident dashboard to see newly reported incidents (once on the screen, he may also control which incidents were automatically solved), he controls Observed entities and he also reads through communication channels (that can be done also in various sequence, and information from one channel can be duplicated or extended in other one).

After analyst gets an overview, he rates incidents – he may change triage of the incidents, close irrelevant incidents (e.g. those which are already outdated, or those which were false-positives or are far from suspect alerts) and assign incidents – either to self, or to someone else in the team, or leave the incidents unassigned.



17 Concur Task Tree: Making an overview of incidents

3.5.2 Use Case: Incident investigation

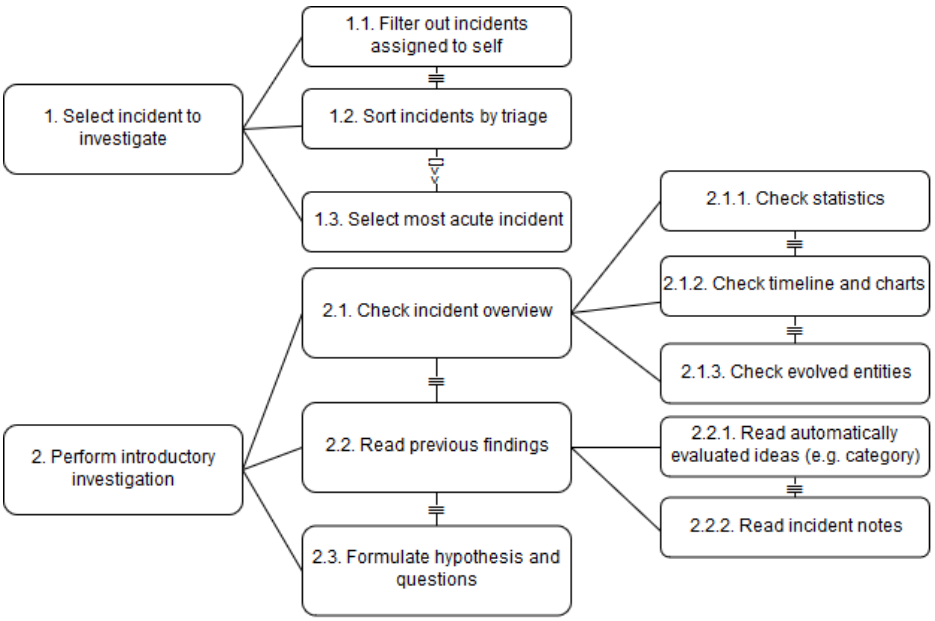
Following Concur Task Tree breaks down tasks, which should be done while investigating a concrete incident.

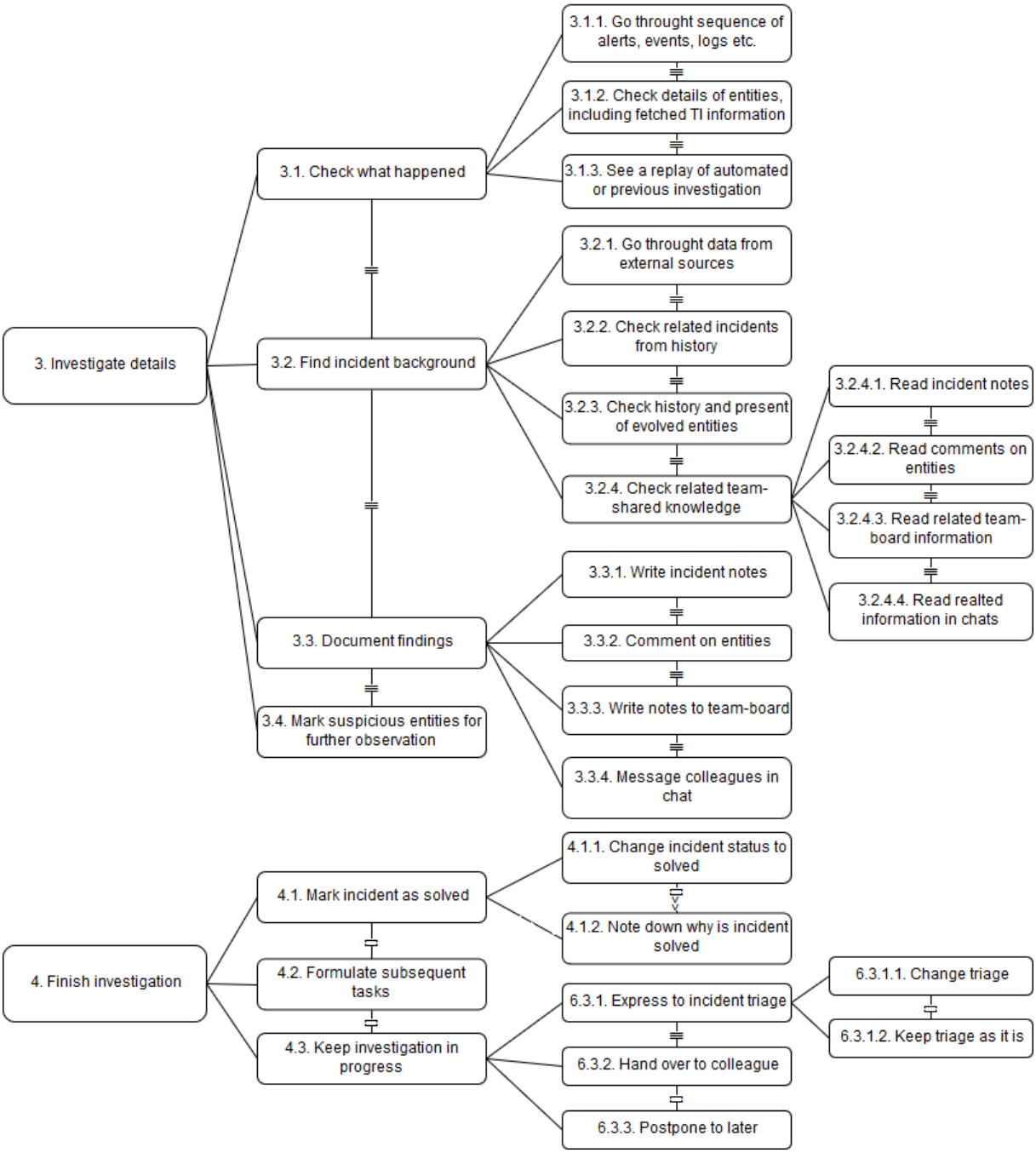
Firstly, analyst chooses an incident to investigate, based on triage and seriousness of the incident.

After that performs analyst an introductory investigation – he needs to check overview statistics, timelines etc., and data which were automatically evaluated. In case there was an automatic investigation performed, or if analyst takes over incident from someone, or continues in something he was solving previously, there might be documentation about previous findings, which is good to read to get a clue. While doing this, analyst formulates a hypothesis what might have happened and formulates questions he is going to answer in the investigation (e.g. "Who attacked us, does the threat last, what happened in the communication between attacker and victim," etc.)

When analyst knows what to concentrate on, he dives into details. He walks through the sequence of logs, searches for relationships, causes and consequences, he uses the third-party data as CTI information to get more knowledge. All the time he documents his findings and marks suspicious entities for further observations.

There are more ways to finish the investigation. One possibility is that the analyst finds what he was looking for and may close the incident as solved. Another one is, that he formulates subsequent tasks and then performs the investigation again with different focus. The third possibility is to continue in the investigation later – e.g. in case when there is no more time on the day to investigate the incident, or when analyst needs to hand it over to a colleague. There might be a need to change the incident triage.





18 Concur Task Tree: Incidents investigation

3.5.3 Function: Team collaboration

Team collaboration is present in all phases of investigation and therefore in both use-cases. The tasks related to team collaboration are following:

- Possibility to chat
- Team board for knowledge persisting over all projects
- Shared notes to single incidents on level of the incident, as well as comments to entities itself. Comments to entities should be propagated across all incidents.
- Possibility to assign incidents to colleagues
- Notifications about incidents assignment, progress etc.

3.5.4 Function: User management

RSI[3] should behave independently for each team (or company). Each team should have an administrator, who will have rights to add or remove a member of the team – RSI[3] user. Administrators have the right to make normal user an administrator.

Each user should be able to login and logout. Also, each user should be able to manage his account – e.g. change password or change profile photo.

3.5.5 Function: Tool configuration

We have identified five areas of tool configuration: personification of dashboards, configuration of entities as devices and subjects, configuration of automation algorithms, connection to CTI sources, connection to SIEM.

Some lists and calculations should be unified throughout the team (e.g. connection to SIEM and automation algorithms) and therefore configurable only by admin, but readable by all users, so that they can check the structure of system. Other configuration (e.g. personification of dashboards, overview of single incident) should be configurable by all users.

Configuration of Incident overview

Each analyst should be able to define overview of incident as he wants to. He should be able to define tables, select which entities should be mapped on rows or columns, define chart, define timeline. Also, he should be able to arrange those elements as it suits him – i.e. have possibility to change its placing, size etc.

Configuration of entities

Analysts should be able to mark devices in network (e.g. list names and IPs in the network), mark down known subject (e.g. big companies such as Google, who have given range of IPs) and blacklist some dangerous entities, which could influence the automation.

Configuration of incident classification

The team should be able to control automated algorithms. E.g., they should have a possibility to edit factors of the triage calculation, possibly to downgrade triage for older incidents. Team should be able to define possible incident states, as well as the categories of resolution (e.g. as “false positive,” or “malware,” which can help with the overview as well as future learning of the automated algorithms. Last but not least, there should be a place where to define playbooks for automated investigation.

Configuration of connection to CTI

Admin should define for each CTI source technical parameters needed to connect, such as an API key. Then he should choose which information should be fetched from the source, and whether this should be done automatically for each entity, or if the analyst should do this manually (e.g. in case of less used CTI sources)

Configuration of connection to SIEM

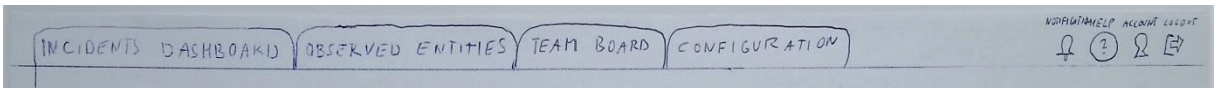
Admin should define all technical parameters which are needed to connect to SIEM – e.g. access data for SIEM account, format of input data, mapping on RSI[3] data format or vice versa.

3.6 Paper mock-ups

In this stage we have designed paper mock-ups with main accent on arrangement of RSI[3] sections and design of the mainframe. We concentrated on understanding of the workflow of overview making and incident investigation, therefore we just wrote down content of other sections. Our mock-ups are not clickable, as that is solved in the next stage, namely low-fidelity prototyping.

3.6.1 Mock-up creation

We sketched the main frame and proposed the sections. To the top line we placed notifications, help, account and logout to the right. On the left side we placed tabs for most important sections – Incident overview, Observed entities, Team board and Configuration. We have also prepared subsections of those sections to test whether the arrangement is intuitive.



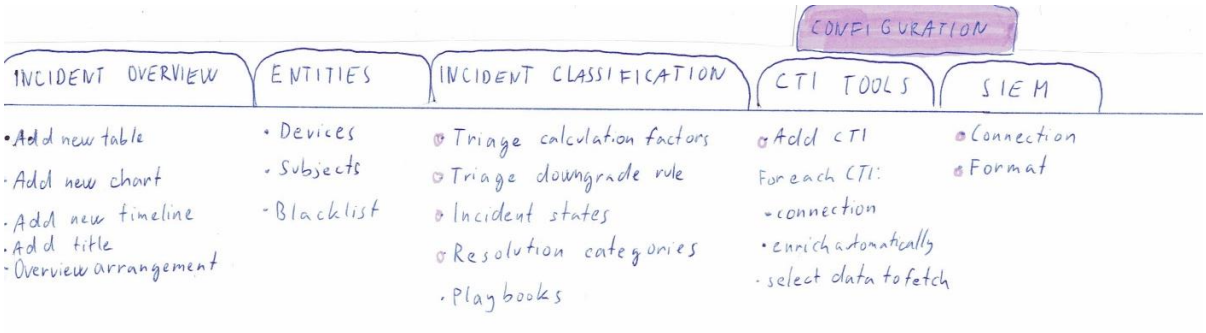
19 Mock-up: top line of main frame

The figure shows placement of main sections of RSI[3] – Incidents dashboard, Observed entities, Team board and Configuration, followed by notifications, help, account and logout on the left.

We placed the chat to the right down corner, which is a position chosen by the vast majority of software solutions.

We also sketched an overview of incidents in form of a filterable, sortable and editable table, as this solution should be transparent, show a lot in one screen and allow analysts to assign and reprioritize incidents.

We also prepared sketches for investigation of one concrete incident, namely an example Incident overview with statistics, example graph and incident notes. We also prepared two more graphs for other cases. Therewith we wanted to assure the workflow of investigation and define entities with main role, so that we can take them into consideration in the Configuration section.



20 Mock-up: proposed content of Configuration section

We decided to place the tabs with open incidents on the left toolbar, as the upper and left toolbar are commonly used for tool control tabs. With placements of incident tabs to the left, the analyst can switch between overview sections and individual incidents without much steps.

3.6.2 Evaluation process

We proceeded according to G. J. Kim's [u7] advice in chapter *Focus Interview/Enactment/Observation study*, where he writes (shortened): „One of the easiest and most straightforward evaluation methods is to simply interview the actual/potential users and observe their interaction behaviour, either with

the finished product or through a simulated run. Depending on the stage of the development at which the evaluation takes place, the application or interface may not be ready for a full-fledged test drive. Thus, a simple paper mock-up may be used so that a particular usage scenario may be enacted for use during a subsequent interview. While mock-ups provide a tangible product and thus improved feel for the system/interface at an early stage of development, important interactive features may not have been implemented as yet."

We have presented the paper mock-ups to four analysts to collect their feedback on the ideas behind. We asked same analyst as in the interview phase (P1, P2, P4, P5) to make sure we understood their needs correctly.

We presented them the arrangement of the components and discussed with them the process of overview making and investigation. We wanted to know whether the workflow would be intuitive enough and whether would RSI^3 make the investigation easier. We wanted to gain new ideas about the design and details of the components as well, therefore we encouraged the analysts to brainstorming. Each session took between 20 and 30 minutes.

3.6.3 Results

We have collected ideas to the components, which are reflected in the low-fidelity prototype design. We also collected following recommendations on improvement of mock-up ideas:

1. Analysts approved the idea of RSI^3, as it could make their work easier. The arrangement of the main sections was as they would be expecting, aside from the user management section, which should be moved out of the team board section.
2. Analysts commented a lot on the Incident overview table, which they see as the most important part of RSI^3. Each of them emphasised another information which should be shown. We should project this in next phases in form of customizable incident table. Analysts also find important to show some statistics immediately in the incident list, e.g. number of victims and attackers, or which type of device was the likely victim. Analysts wanted to have checkboxes in menu for making operations on more incidents at once.
3. Analysts approved basic idea behind the graph and added more factors to be considerate. They also pointed out the need of grouping and filtering, as there will be thousands of logs.
4. Analysts commented also on names. They proposed to rename "Team Board" subsection with notes in Team Board section to "Team Notes". One participant was confused by the example title in Incident overview "incident info" and wanted to rename it to "basic info."
5. Analysts wanted to highlight the triage in the incident dashboard, so that they can quickly define what to concentrate on. We have decided to indicate this by colour.
6. We dealt with the situation when analysts wanted to discuss rather the processes on backend, as incident prioritization and evaluation, than the related design. Therefore, we tried to introduce the aim clearer in next sessions.

4. Low-fidelity prototype

In this chapter we will describe the process of low-fidelity prototype creation and evaluation.

4.1 Design

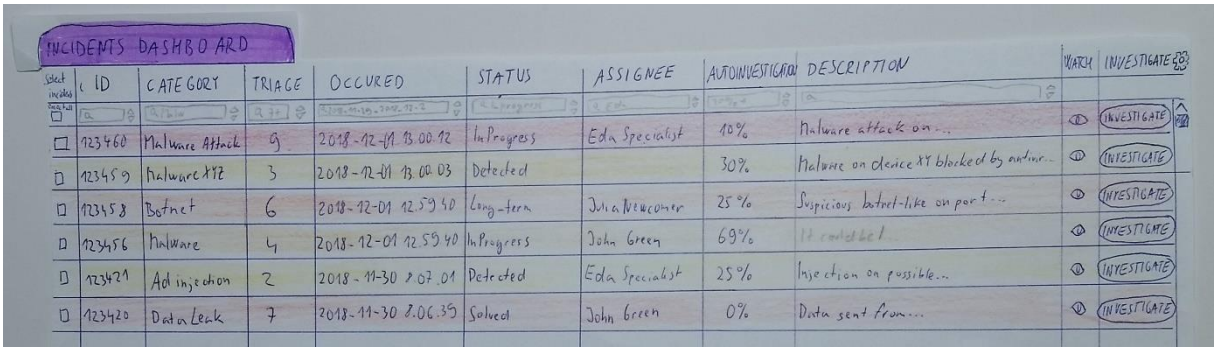
We have decided to create low-fidelity prototype from paper, as this approach is quick, we could make more ideas and re-draw them easily, when we found some improvements during the designing process. Paper prototypes also enables to correct some minor issues immediately during the evaluation (e.g. placement of a forgotten button).

We created wireframes of the RSI[3] sections, as well as some pop-ups and forms. Therewith we wanted to communicate the structure of RSI[3] (sections), the content of the section pages and the functionality (what the content will represent, the interaction with pages etc.). The interaction between the parts of the RSI[3] were simulated by adapting the Wizard of Oz technique.

The Wizard of Oz technique is an efficient way to examine user interaction with computers and facilitate rapid iterative development of dialog wording and logic. The technique requires two machines linked together, one for the user and one for the experimenter. The experimenter (the "wizard"), pretending to be a computer, responds to user queries either directly or by pressing function keys to which common messages have been assigned. [u6]

The process of low-fidelity prototype creation started from the main frame, verified by the mock-ups testing. We expanded on the ideas behind individual tabs. We prepared some example incidents, IPs, devices and users, which go through whole prototype, so that the users can imagine the case and cooperation of the sections. Based on the user interviews and recommendations from mock-ups feedback, we also presented properties of incidents and their example values (e.g. states of incident), which will be later editable.

4.1.1 Incidents Dashboard



21 Low-fidelity prototype: design of Incidents dashboard section

Visualization of example incidents – important properties as incident ID, category, triage, occurrence, status, assignee, level of auto-investigation and description are shown in columns. Columns are sortable and filterable. User can edit in the settings which columns should be shown or hidden. User can become a watcher of each incident or continue to the investigation tab of single selected incident.

Data in the table with incidents stayed as in the mock-up. We suggested some more possible columns and we have reflected this in the setting possibilities of incident dashboard. Each incident has some auto-generated properties (as time of the incident – when it occurred, finished and its duration; the time when it was discovered, triage, description based on automated investigation, level of this investigation in percentage, category of incident, estimation of the time needed for investigation, trigger overtaken from input data, statistics counts of involved entities – logs, public IPs, private IPs,

devices and subjects), and properties completed by the analysts (assignee, watchers, status, resolution category, comment). All properties, except unique ID, can be edited by clicking directly in the table. The columns may be sorted and shown as the analyst needs to, the breath of column is also configurable. Under the header of table, we placed a space to filter out shown incidents, and to stable-sort them. Based on the feedback to mock-ups, we added a column with checkboxes and one extra line under the table, to do the action for all selected incidents at once.

4.1.2 Observed entities

We suggested a parallel coordinates graph, which should warn about activities of observed entities and also the graph of activities of observed entities under each coordinate. We added a settings section where can the user add or delete observed entity.

Reason for entity observing might be when an IP is malicious, its behaviour was stopped and now the analyst wants to ensure it is not problematical anymore.

4.1.3 Team board

In this section we captured knowledge sharing. In the team notes subsection, team members can share their knowledge to some sets of incidents or workflow know how, they can share their ideas, notes to work distribution etc.

In the history subsection, there should be reflected bigger actions in RSI^3, as changes in configuration, adding of new users or big steps in incident investigation, e.g. change of status (not the smaller steps in investigation process). RSI^3 could cooperate with the SIEM and send data about actions there for more detailed reporting about the team activity.

4.1.4 Configuration

In the Configuration section, the user can personalize the tool, specify connection with other tools, edit entities etc.

Incident overview tab enables analyst to adapt the Incident overview statistic according to his needs. He can add titles, tables, charts and timelines, change their proportions and positioning. We also sketched ideas for the process of titles, tables, charts and timelines adding.

Entities section enables to name devices in the private network for quicker identification. It should be possible to load this information from a file, not only manually. There are listed also known subjects, so that the analyst doesn't have to remember known providers. It is also a place for blacklist defining, which will point out the most suspicious IP addresses.

Incident classification section outlines some possibilities to edit the automated processes. From this section, the analyst could influence the triage calculation algorithm, degrade triage of outdated incidents, edit possible incident states and resolution categories – this all should be readable by all users, but editable only by admin, so that the team works with consistent information. Creation of playbooks for automated investigation belongs to this section, however, we didn't go to details as the playbook investigation is rather a backend part of the solution.

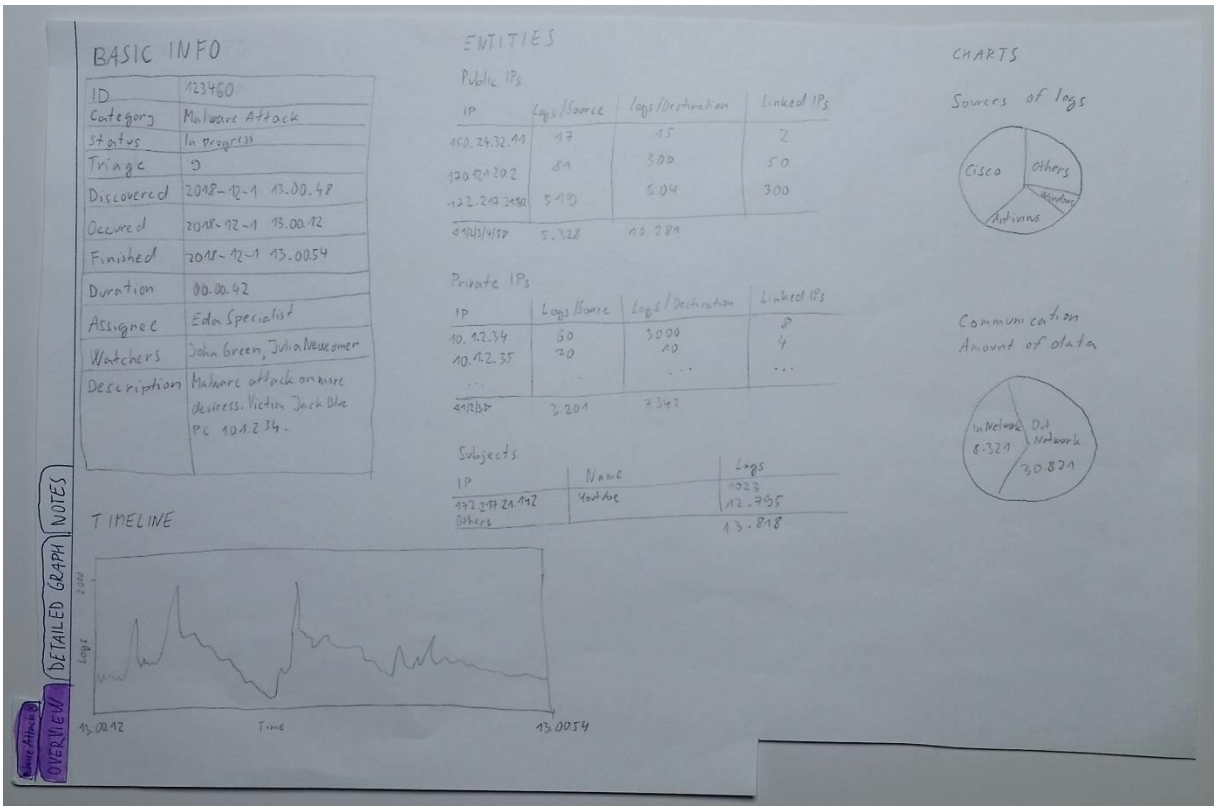
In the CTI tools section, user should define the connection to CTI tools and what data should be fetched. Next section, SIEM, should define the connection to SIEM systems, data structure, etc. – however, we didn't go to details, as this should be part of the development process.

The last section, Users, will be shown only to admins. Admin will be able to add new users to the team or remove inactive ones. There will be a possibility to make a normal user to an admin.

4.1.5 Incident

We presented one incident simulation. In the Incident overview we simulated basic information about the incident, then added statistics about entities related to this incident, added two pie charts (one with sources of the SIEM logs, other one with data shifted in scope of the incident), and an example timeline with number of incident logs in time of incident.

In incident notes section, analysts will have a space to keep their knowledge, comment on their findings, add images, links, files related to the particular investigation.



22 Low-fidelity prototype: design of Incident overview

Incidents which were selected for investigation will be opened as side tabs. There will be three sections – incident overview, detailed graph and notes. This figure shows the Incident overview section, where the analyst can see configurable statistics about the incidents (in this case table with basic information, timeline, tables with entities – public and private IP addresses and subjects, and also two charts with sources of logs and amount of data in the communication). The analyst should be able to formulate a hypothesis based on these statistics and continue with investigation of details in the Detailed graph tab.

4.1.6 Incident Graph

In this phase we have decided not to dive into a detailed interaction with the incident graph, visualization of details and analysis of the graph structure. There would be many problems and challenges to solve and doing a proper analysis of those problems would be too extensive task to fit in the scope of this thesis and it would need an extra research.

Some of the first questions were how to visualise what is happening in the network – which type of graph to use (e.g. force-directed graph), what type of layout to use (e.g. the Fuchterman-Reingold multiscale algorithm), if the tree graph-structure would be suitable, if the graph should be unidirectional and how the cycles should be handled.

Secondly, there is an outline of the graph elements – nodes and edges. How the entities should look like? What entities should be captured there and how to make entities configurable for needs of each user?

Thirdly, we were asking us what should change as the graph will grow big. Should we accent the most important nodes, should we use a fish-eye zoom technique or fade out the previously used nodes?

Finally, there is the information detail to be taken into consideration. For filtered information detail, or for showing subset of smaller amount of data, we could consider such techniques, as parallel coordinates or interactive cluster grams and heat markers. For showing relations between two entities, we could use a matrix-based visualisation.

After we broke down what would be needed to analyse to make a good design of detailed graph, it was clear that it is out of scope of this thesis.

4.1.7 Next parts

The notifications should include such information, as when someone makes important changes on watched incident, mentions user in some notes or assigns and incident to him.

The help section should have a wiki-based user manual with searchable information – we didn't prototype this one, as this should be a standard help system.

In account section the user should be able to edit his account, i.e. change password and profile photo.

The logout button helps to log out of the system, the login screen purposes to log in.

RSI^3 includes small chat in the right corner, so that the analysts can communicate directly without switching to other tools.

4.2 Evaluation

4.2.1 Goals

The goal of the low-fidelity prototype testing is to find out possible problems soon. We want to make sure that the work with RSI^3 is intuitive and change processes which wouldn't be intuitive enough. We also want to get feedback on our mainly focused tasks, and thus that RSI^3 helps with incident investigation, team cooperation and that the analysts would profit from using RSI^3 for their job.

4.2.2 Test set-up

Procedure

The testing session with each participant took about 45 – 75 minutes. Firstly, we introduced to the participants the key ideas behind RSI^3 and explained the reason for testing. Then we asked them about their experience with computer security and incident analysing. After that, we let them to perform the tasks in interaction with the paper low-fidelity prototype by using the Wizard of Oz technique. Afterwards, we asked them six questions to summarize the evaluation process. Finally, we asked on their feeling from the testing process.

Location

The sessions took place in quiet places with big desk available, as in café or consultation rooms in the buildings of participant's company.

Participants

Participant ID	Time in security job	Job description
P1	7 months	Cybersecurity analyst in a consulting company
P2	2 years	Threat analyst in an antivirus software company
P3	3 years	Threat analyst in an antivirus software company
P4	3 months	Threat analyst in an antivirus software company
P5	10 months	Cybersecurity analyst in a consulting company

Table 4 Low-fidelity prototype testing participants

4.2.3 Test scenarios and questions

We prepared following tasks to evaluate the RSI[3]. Going through these tasks with participants should give us feedback on all sections of the prototype, and on the workflow.

Task 1: Check what recently happened in RSI[3] – notifications, chat, team activities, check new incidents.

1. The analyst reads through the notifications.
2. The analyst checks chat and reads new messages.
3. The analyst goes to Team board section.
4. The analyst reads team notes, checks what tasks he was asked to do.
5. The analyst checks team history and checks relevant tasks his colleagues solved.
6. The analyst goes to incident table screen and checks new incidents and their info.

Task 2: Readthrough the incidents in Incidents dashboard, reprioritize them and assign some incidents to yourself

1. The analyst finds incidents extra mentioned in Task 1 and gives them bigger priority and assigns them to self.
2. The analyst checks the table of incidents and filters out new ones.
3. The analyst sorts incidents by triage.
4. The analyst assigns most relevant incidents to self.
5. The analyst may look what more possible columns can be displayed.

Task 3: Check observed entities, remove observing of the non-actual ones.

1. The analyst goes to Observed entities section.
2. The analyst sees the relations graph and timeline of activities.
3. The analyst decides what entities he doesn't want to observe anymore.
4. The analyst edits the list of observed entities by removing the non-actual one.

Task 4: Investigate incident. Select from Incident overview incident with biggest triage. Read through the statistics and make a hypothesis. Check the detailed graph and make notes. Make incident as solved.

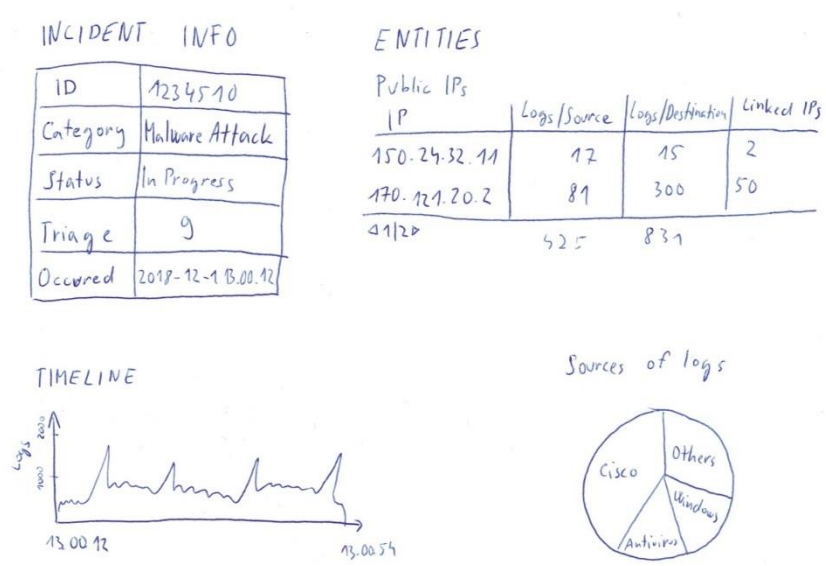
1. The analyst goes to incident table and selects new incident with biggest triage assigned to self.
2. The analyst clicks on "Investigate" button. Therewith is he redirected to the Incident overview.
3. The analyst reads through the statistics and makes a hypothesis what might have happened.
4. The analyst goes to detailed graph.
5. The analyst sees the replay of automated investigation and watches the elements of graph investigation.
6. The analyst makes a printscreen of the graph.

7. The analyst goes to incident notes and adds a comment.
8. The analyst adds to incident notes the printscreen of the graph.
9. The analyst marks incident as solved and fills in the reasoning form.

Task 5: As admin, add new user, make him admin, log out and log in as the new user.

1. The admin goes to the Configuration section and subsection Users.
2. The admin fills in the form with name, email address and password for the new user.
3. The admin creates new user profile.
4. The admin logs out.
5. The new user logs in by using the login form.

Task 6: Create own Incident overview according to the template. Add tables, charts, timeline and titles and sort it in the order of template.



23 Low-fidelity prototype: Incident overview template

1. Go to the “configuration” – “Incident overview” section.
2. The analyst clicks on button “Add new table”.
3. The analyst selects Incident as entity to map.
4. The analyst selects to map properties on row.
5. The analyst clicks on continue button.
6. The analyst selects properties to be shown.
7. The analyst sorts the selected properties.
8. The analyst clicks on create button.
9. The analyst clicks on button “Add new table”.
10. The analyst selects Public IPs as entity to map.
11. The analyst selects to map properties on column.
12. The analyst clicks on continue button.
13. The analyst selects properties to be shown.
14. The analyst sorts the selected properties.
15. The analyst clicks on create button.
16. The analyst clicks on button “Add new chart”.
17. The analyst selects “logs” as an entity to map.

18. The analyst selects “piechart” as type of chart.
19. The analyst clicks on continue button.
20. The analyst selects “Source” as property to be shown.
21. The analyst clicks on continue button.
22. The analyst selects “Number of logs” as a metric.
23. The analyst clicks on create button.
24. The analyst clicks on button “Add new timeline”.
25. The analyst selects entity and time range to be mapped.
26. The analyst clicks on create button.
27. The analyst clicks on “Add new title”.
28. The analyst fills in the title text.
29. The analyst clicks on create button.
30. The analyst arranges the inserted tables, chart and timeline in the overview frame.

Task 7: Check configuration of entities. Remove one entity of list of devices. Remove one subject. Edit one entity on blacklist.

1. The analyst goes to configuration – entities section.
2. The analyst watches what is written in the list of devices, subjects, and on the blacklist.
3. The analyst removes one new entity from list of devices.
4. The analyst removes one subject from the list.
5. The analyst edits one of the IPs on blacklist, or its suspiciousness.

Task 8: Check and read through configuration of incident classification. Give feedback to resolution categories and incident states, and to the other elements in section.

1. The analyst reads the lists in configuration – incident classification section.
2. The analyst gives verbal feedback on the elements in section.

Task 9: Check the CTI source section.

1. The analyst goes to configuration – CTI tools section and sees what tools are connected and what data are fetched.

After going through the tasks, we asked the participants following six questions, to get a summarizing feedback on RSI^3:

1. Was the solving of tasks intuitive?
2. What did cause you problems?
3. Does RSI^3 help with the investigation?
4. Does RSI^3 help with the communication within the team?
5. Where did you see the biggest advantage of RSI^3?
6. Is there something you are missing?

4.2.4 Results and findings

All participants fulfilled the tasks without any bigger complications in a short time, except task 3, where we identified problems with the observed entities graph interpretation. However, at some sections the participants had some questions or recommendations regarding the function.

Incident dashboard section

P3 was confused by the button “investigate.” He thought that clicking on this button should be followed by an action, e.g. assigning the incident automatically to him. Therefore, he would prefer to

rename the button to “show,” so that the action is only showing the data and assigning comes separately. P5 asked about the button “watch,” as it was not clear to him, that it makes him watcher as in a ticketing system.

P4 was confused by the word “triage” and she didn’t know what the scale is. Therefore, she would like to see an explanation of the heading, e.g. by hovering over the heading. P3 didn’t know the word “triage” as well, he is used to the term “priority.” P5 also asked about range of scale.

P5 would like to see all incidents if he were team leader, otherwise he would like to see by default just incidents assigned to him or without assignee.

P5 didn’t know where to close more incidents at once, it took him a while to find it.

Observed entities

This section was confusing for all participants.

P1 doesn’t think an incident is an entity to observe, as the malicious behaviour should be blocked by that time. He would rather observe the malware.

P2 would rather see a real-time dashboard with the amount of communication. He would need more description to the graphs. He didn’t like the idea behind the columns, as the relations visualisation would be too complicated. The parallel coordinates evoked him rather a timeline, which he didn’t want to see. P2 was slightly confused by the term “Subject,” as that evokes him “Suspect.”

P3 would imagine rather timeline graphs based on concrete incidents and more heuristics. He thinks linear graph doesn’t have a place there, as it is hard to connect e.g. columns of subjects and public IPs without creating too many lines.

P4 was missing description of the graphs in lower part and thinks activity of each observed entity should be shown separately. P4 would like to see the details about activity on demand, e.g. the logs.

P5 didn’t understand the branching, and how the graphs depict intensity of entities actions. He didn’t like the idea of deleting entities in another window – he would like to do it directly in the graph.

Team board

P4 commented on the team notes sections. She thinks it would be better either to separate it to a wiki and issue tracking section, or rather remove all the job tracking notes and leave it for other tools. RSI^3 should be a tool only for analysts, therefore notes should be a place to keep knowledge about investigation processes, but not to share done work, as that should be seen also by company managers who don’t have access to RSI^3.

P2 and P3 commented on team history. They find important to have different levels of logging. They want to see difference between bigger actions (e.g. solving more patterns at once) and smaller actions (one incident status change). This could be done by tree structure, or by colour difference.

Configuration

There were some comments on the ordering of the configured elements. P1 was missing a possibility to change the order of CTI tools. He also mentioned that he would like to be able to sort everything alphabetically (e.g. the entities in list, but also the columns in Incidents dashboard setting sections, in the table-adding form etc.). Problem with alphabetical sorting was also reported by P5. P3 didn’t like using of the arrows for reordering, he would prefer the drag and drop principle.

P4 commented on the lists in the entities section. She would like to have packages of devices (e.g. for each floor of the company building one package), subjects (whitelist for generally known services, internal, customers, suppliers…) and also packages of blacklisted IPs. She missed comments to

blacklisted entities, as she needs to note down why is an IP address on a blacklist and what incident is it linked to.

P1 and P5 would make from the Incident overview configuration section rather a setting section directly at the Incident overview tab.

P2 didn't like the scroll scale at the incident classification section, for him it is annoying way to change the proportions.

P2 would add the state "Verified by," or "Accepted" to the example states, so that the prototype catches the process of verifying of incidents evaluated automatically or by junior analysts.

P3 would like to configure a possibility of automatically assigning incidents of given category to concrete analysts.

P3 was considering the levels of RSI^3 users, distinguished as normal users or admin. He would add one level for senior analysts with more permissions than normal users, so that the administration of RSI^3 doesn't depend only on admin users.

Incident

Participants liked the Incident overview section, but they wanted some more statistics specific for their specialization. P2 suggested graphs with file entropy and peano curves, as senior analysts can guess the type of incident from that. He suggested also a preview of the malware binary file. P2 likes how VirusTotal compares opinions on file from more possible antivirus software, so he wants something similar, e.g. various CTI tools ideas about the incident. P4 wanted more concrete timelines – she would like to see timelines for logs of different types, e.g. connecting, sending, encrypting etc. P5 also commented on timelines – he would like to see separate timelines for public and private IPs, or even filter out one concrete IP address to see its traffic directly in overview.

We also discussed moving the configuration of Incident overview directly to the overview section. P2 thinks there should be a default setting, so that junior users don't have to create this dashboard by themselves. P3 imagined incident template, which could be changed for each incident – at least by wrapping the tables.

P3 mentioned that it would be nice to have something like SQL querying for the statistic, because of the possibility to configure conditions. However, it could be only SQL selecting and only for advanced users, as the querying could potentially make some errors in the system.

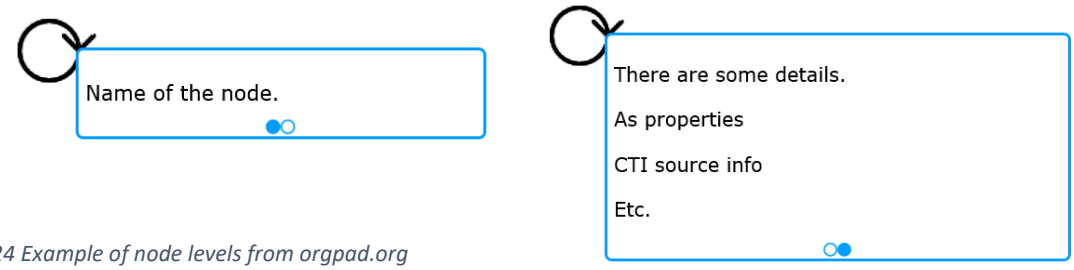
P1 and P3 liked the possibility to make notes directly to each incident. P2 probably wouldn't use this function, because he would prefer internal wiki of the company, where he can share with non-analytics colleagues. For the sharing reasons, he would add exporting possibility to the notes section.

P4 mentioned, that it would be hard for her to have a lot of notes apart from the overview and graph investigation, she would like to have a small place for to-do list, which would be seen both in overview and graph.

P1 would like to add a "graphshot" to notes, i.e. openable screenshot of the graph. P4 had similar idea, when she mentioned she would like to create a snapshot of a graph.

Participants didn't comment much on the graph part, as this is not covered in this thesis. Nevertheless, they liked some ideas, as replay and the possibility to comment directly on the nodes.

P3 raised an idea of more levels of node, where the details could be shown directly in node after clicking, and he referred to project orgpad.org.



24 Example of node levels from orgpad.org

P1 wished to have an extra button to incident status change in all tabs of the incident. In contrary, P4 thinks the status change shouldn't be in the graph tab at all and only in overview. P5 had problems with incident closing, as he went back to close it in the Incidents dashboard section, not directly at the investigated incident.

P5 would like to have arrows on node connection, so that he remembers how he expanded.

Regarding the investigation flow, P2 was missing a place to write down the complexity of done analysis, which should be also projected into team history.

P3 missed a possibility to link manually two incidents which are related, as one attack case with two forms of execution – e.g. and incident where spam downloads a virus, and an incident with botnet, where the attacker is the same person who sent virus before.

Notification, Help, Chat, Account, Logout, Login

There were no ambiguity or recommendations on these sections.

Summarizing feedback

In next part, we present the answers of questions given in an interview after tasks execution.

1) Was the solving of tasks intuitive?
   All participants answered that the solving of tasks and the tool was intuitive for them.
2) What did cause you problems?
   For P1 was strange the placement of single incidents tabs on the left side, but he got used to it.
   P2, P3, P4 and P5 had problems with the observed entities section. P4 also mentioned the missing captions in incident overview heading.
3) Does RSI^3 help with the investigation?
   P1: "Yes, I think it could be very helpful."
   P2: "Yes, I would especially emphasise the analytical part, as the incidents dashboard and incident investigation. The "scrum" part could be left for other tools."
   P3: "I think it could be helpful, I see it as an improved ticketing system."
   P4: "Yes, I like especially the incident dashboard, that table could help to make decisions."
   P5: "Yes, I see potential."
4) Does RSI^3 help with the cooperation within team?
   P1: "Yes, it does."
   P2: "Yes, but maybe that part wouldn't be necessary for me."
   P3: "Yes, I think it helps rather in documentation than communication. It depends on the company policy how they use the potential of the tool."
   P4: "I think so, especially the assigning and the wiki part for single incidents."
   P5: "Yes, I had there what I needed – especially chat and dashboard."
5) Where did you see the biggest advantage of RSI^3?
   P1: "That ideas, which could be find under more tools, would be united under one design."

P2: “I liked the idea of the graph, and the details as the blacklist.”
P3: “That it unifies many systems under one.”
P4: “All available pieces of information are at one place.”
P5: “I liked the incidents dashboard.”

6) Are there any sections you are missing?
P1: “A tab with tasks assigned to me, so that I don’t have to filter it out.”
P2: “No.”
P3: “Not really. But a console or a scripting interface would be nice to have.”
P4: “Yes, I was missing a section in configuration, where would be such staff as application version, copyright, click for automatic update of the software etc.”
P5: “Now I don’t have any idea what to add.”

5. High-fidelity prototype

5.1 Design

5.1.1 Selection of features

Based on the results and findings, which we gained by the low-fidelity prototype testing, we decided to choose features to be realized in the high-fidelity prototype.

The weakest part of the low-fidelity prototype was the Observed entities section. Designed graphs were controversial and there would be a need of redesigning this section. We would need to get a deeper understanding and for this, take a step back and do more research, ideally in the form of a focus group (which is a session with a diverse group of people with discussion about a product), where we could collect requirements and find trade-off between contradictory ideas. After this, we would start again with sketches and low-fidelity prototyping of this section.

The participants also received the cooperation functions in different ways – some participants emphasized those sections, which were helping with communication and documentation, other ones would skip those functions in sake of incident investigation itself.

Therefore, we decided to point out in the high-fidelity prototype the feature of Incidents dashboard and the single incident investigation, especially the Incident overview, which were the most emphasized features of RSI[3] and seemed to have the biggest potential.

We will also keep the other sections in the menu, but the content will be only described in a text, where we also sum-up improvement ideas gained in the low-fidelity prototype feedback.

5.1.2 Implementation

We have decided to create the high-fidelity prototype in a UX prototyping tool Axure. With this tool we were able to create the menu control, interactive Incident overview and notes section. For the Incidents dashboard table, we decided to include Google Spreadsheet, as the response of a dynamical table with all designed elements in Axure might be too slow and the Spreadsheet offers all needed functions as sorting and filtering.

By using the Google Spreadsheet, we could quickly prototype wished design, including colour scheme, allowed values, lock of changes on given columns, sorting and filtering. Only difference between our vision and the functions provided in Google Spreadsheet is, that we cannot disable the “delete column” function (by using the protected data range function) without disabling the function or column sort and hide.

For generating of some mock-up data we used the functionality of a web mockaroo.com, together with Excel functions.

We changed the colour design of the tool to look more attractive. We made the decisions according to the recommendations of Material Design system [u9] and we applied a material design palette [u10] on all pages, to have the colours unified and balanced. We unified used fonts to the sans-serif font Roboto, and we unified letters case and style within all widget as buttons, texts and titles.

We prepared interaction for a schemed walk through the incident investigation and generated tables and graphs with the mock-up data.

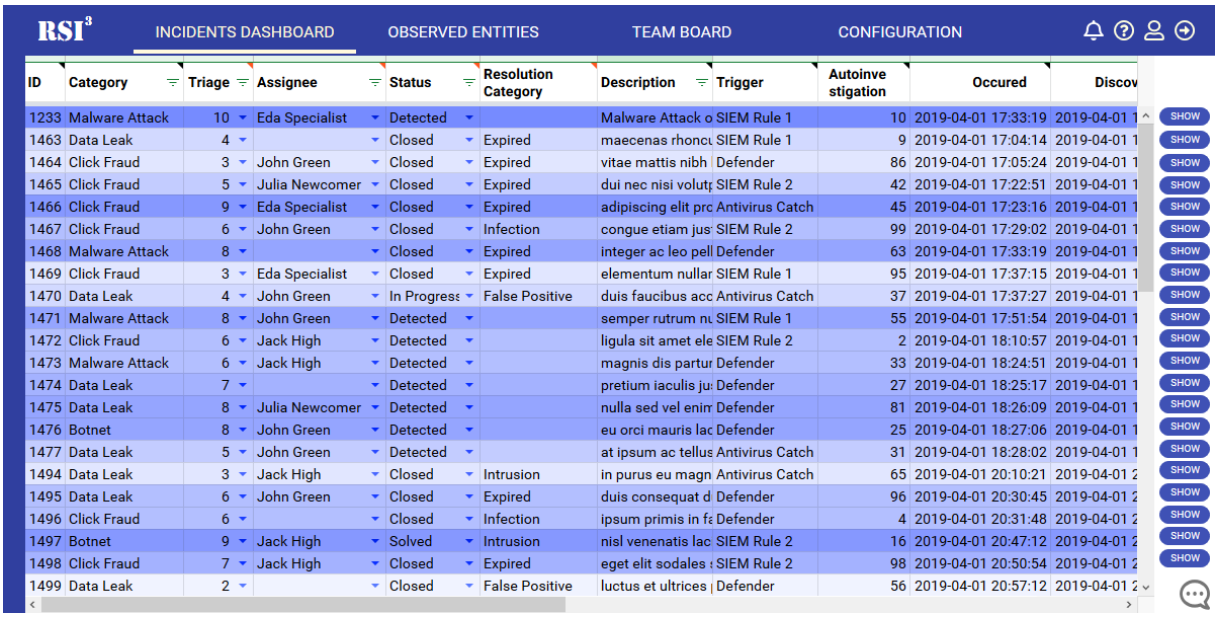
Based on the idea of P2, we added an example file entropy to the Incident overview by using the data downloaded from redcanary.com [s28]. We generated some of the calculated graphs in different sheets and inserted just images to the demo, as the calculation caused leaks in page loading.

Results from previous testing were reflected in the prototype. As for the Incidents dashboard, we added tooltips to the header. We changed the colour scale to fit into the new design and to show more distinctly what is the range of triages. We added mock-up data for all possible columns and it is up to the user which columns he wants to hide and how he wants to sort them. User can change editable properties at once just by pasting the wished value. We renamed the button, which is showing a single incident, to "show".

We introduced slightly different elements in the Incident overview page. We show the Basic info table with subset of incident properties, which are intended to be configured. This is a place, where the user can change the status of the incident. It reflects the possibility to change the status in the Incidents dashboard, and it reacts on the proposal of P4 to enable status change only in the Incident overview. We added an example file entropy, which was mentioned by P2. We kept the tables of private and public IPs, as well as the timeline. In case of the timeline, we added a filter for all, public or private IP addresses logs, which reflects the wish of P5. We reflected the wish of P2 and added a sample table with CTI information. We added one pie-chart, which can be exchanged for a different one, to simulate an interaction with the settings section.

We moved the settings from Configuration section directly to the Incident overview. We followed an idea of P2 to have a default template, and of P3 to wrap or hide elements not needed for given incident. There will be a default template same for all new users of RSI^3. It will be configurable – the user can add or remove elements. User can also remove or add elements at level of current incident – therewith he can hide components, which he doesn't want to look at for actual investigation. In the settings the user should be able to add new elements and configure its properties, including applied filters.

For settings simulation, we prepared a scenario when the user exchanges two charts. All elements in page should be moveable, so that the analyst may change their position as it suits him. We demonstrated this on the second chart.

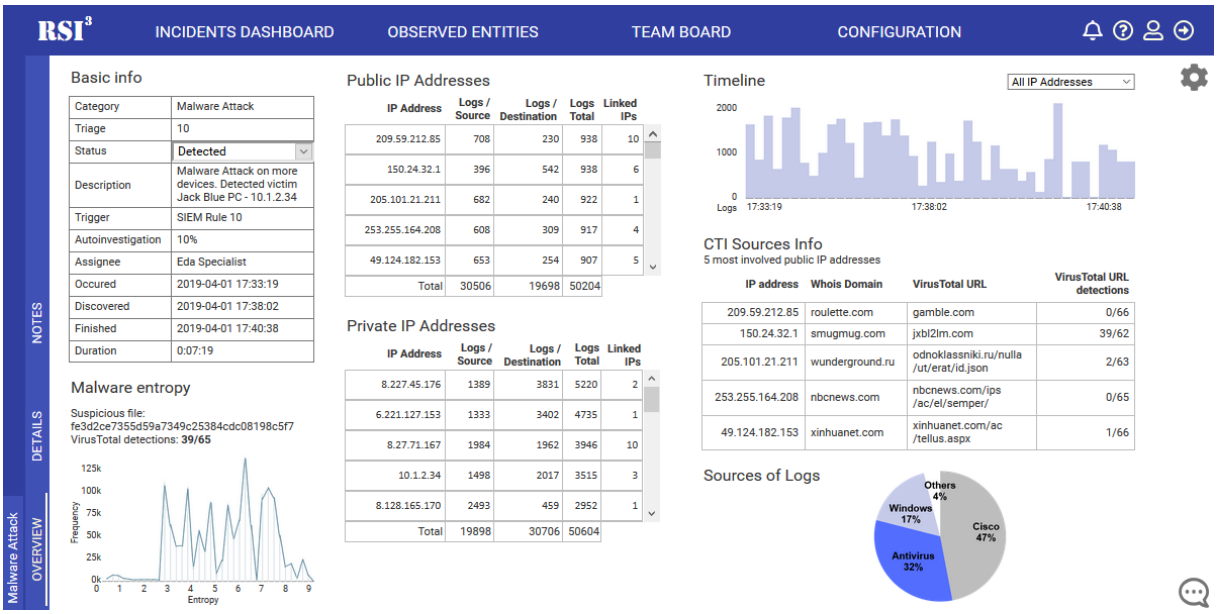


ID	Category	Triage	Assignee	Status	Resolution Category	Description	Trigger	Autoinvestigation	Occured	Discov	
1233	Malware Attack	10	Eda Specialist	Detected		Malware Attack o	SIEM Rule 1	10	2019-04-01 17:33:19	2019-04-01 1	SHOW
1463	Data Leak	4		Closed	Expired	maecenas rhoncu	SIEM Rule 1	9	2019-04-01 17:04:14	2019-04-01 1	SHOW
1464	Click Fraud	3	John Green	Closed	Expired	vitae mattis nibh	Defender	86	2019-04-01 17:05:24	2019-04-01 1	SHOW
1465	Click Fraud	5	Julia Newcomer	Closed	Expired	dui nec nisi volut	SIEM Rule 2	42	2019-04-01 17:22:51	2019-04-01 1	SHOW
1466	Click Fraud	9	Eda Specialist	Closed	Expired	adipiscing elit prc	Antivirus Catch	45	2019-04-01 17:23:16	2019-04-01 1	SHOW
1467	Click Fraud	6	John Green	Closed	Infection	congue etiam jus	SIEM Rule 2	99	2019-04-01 17:29:02	2019-04-01 1	SHOW
1468	Malware Attack	8		Closed	Expired	integer ac leo pell	Defender	63	2019-04-01 17:33:19	2019-04-01 1	SHOW
1469	Click Fraud	3	Eda Specialist	Closed	Expired	elementum nullar	SIEM Rule 1	95	2019-04-01 17:37:15	2019-04-01 1	SHOW
1470	Data Leak	4	John Green	In Progress	False Positive	duis faucibus acc	Antivirus Catch	37	2019-04-01 17:37:27	2019-04-01 1	SHOW
1471	Malware Attack	8	John Green	Detected		semper rutrum nu	SIEM Rule 1	55	2019-04-01 17:51:54	2019-04-01 1	SHOW
1472	Click Fraud	6	Jack High	Detected		ligula sit amet ele	SIEM Rule 2	2	2019-04-01 18:10:57	2019-04-01 1	SHOW
1473	Malware Attack	6	Jack High	Detected		magnis dis partur	Defender	33	2019-04-01 18:24:51	2019-04-01 1	SHOW
1474	Data Leak	7		Detected		pretium iaculis ju	Defender	27	2019-04-01 18:25:17	2019-04-01 1	SHOW
1475	Data Leak	8	Julia Newcomer	Detected		nulla sed vel enim	Defender	81	2019-04-01 18:26:09	2019-04-01 1	SHOW
1476	Botnet	8	John Green	Detected		eu orci mauris lac	Defender	25	2019-04-01 18:27:06	2019-04-01 1	SHOW
1477	Data Leak	5	John Green	Detected		at ipsum ac tellus	Antivirus Catch	31	2019-04-01 18:28:02	2019-04-01 1	SHOW
1494	Data Leak	3	Jack High	Closed	Intrusion	in purus eu magn	Antivirus Catch	65	2019-04-01 20:10:21	2019-04-01 2	SHOW
1495	Data Leak	6	John Green	Closed	Expired	duis consequat d	Defender	96	2019-04-01 20:30:45	2019-04-01 2	SHOW
1496	Click Fraud	6		Closed	Infection	ipsum primis in fa	Defender	4	2019-04-01 20:31:48	2019-04-01 2	SHOW
1497	Botnet	9	Jack High	Solved	Intrusion	nisl venenatis lac	SIEM Rule 2	16	2019-04-01 20:47:12	2019-04-01 2	SHOW
1498	Click Fraud	7	Jack High	Closed	Expired	eget elit sodales	SIEM Rule 2	98	2019-04-01 20:50:54	2019-04-01 2	SHOW
1499	Data Leak	2		Closed	False Positive	luctus et ultrices	Defender	56	2019-04-01 20:57:12	2019-04-01 2	

25 High-fidelity prototype: Incidents dashboard

Incidents dashboard is an important section, where the analyst can see sortable and filterable list of detected incidents. The colour of column is shown according to the priority of the incident. Each column shows a property of incident and the analyst

can change the order of columns, hide or show the columns according to his needs. The dashboard provides to the analyst basic information about the incidents and based on these they can prioritize, estimate what is going on and assign the incidents to members of the team. Single incident investigation can be opened from there.



26 High-fidelity prototype: Incident overview

Incident overview provides to the analyst configurable statistics about the incident, based on which he should be able to formulate a hypothesis and questions to be investigated. This incident overview shows table with basic properties of the incident, malware entropy, list of public and private IP addresses which participated in the incident, filterable timeline of logs, table with information from CTI sources about most involved IP addresses and chart with sources of logs.

5.2 Evaluation

5.2.1 Goals

Main goal of the high-fidelity prototype testing is to evaluate the usability of the Incidents dashboard and the Incident overview section in the context of the RSI^{3}system. We want to know, whether named sections help analysts to explore collected data with less effort and help with the incident investigation. We want to test if the proposed design is pleasant for the analysts and if the positioning of components is intuitive.

5.2.2 Test set-up

Procedure

We tested the prototype with five participants (P1-P5) at once. A team of analysts agreed to give us feedback and wanted to hear more about the project so far. Therefore, we firstly hold a one-hour session, where we presented to the participants the problematic of the investigation of cybersecurity incidents and how we approach it. We summed up the procedure of the user-centred design and which tools and techniques we used. Afterwards we shortly referred to the low-fidelity prototype and explained to the participants how we have chosen features to be implemented in the high-fidelity prototype, and their connection to other features, which were not transferred to the high-fidelity prototype. Finally, we gave them a context of the prototype data – e.g. that there are four example members of a SOC team (Eda Specialist, Julia Newcomer, Jack High and John Green), some predefined states of incident, resolution categories etc.

After this introduction session we advanced to the testing procedure. Each participant received testing instructions, own copy of the prototype and an online sheet for collection of written feedback. For the

whole time we were present and available to answer any questions, clear up any ambiguities and we could also see the reactions of participants on the prototype.

Participants tested the prototype and wrote the feedback for 40-70 minutes. We had a summarizing talk with each participant after s/he finished.

We had a different section with P6, where we just went through the testing part and collected the feedback in spoken form. There was less need to explain the context, as P6 took part already in the low-fidelity prototype testing and therefore he knew what to expect.

Location

First sessions took place in the office of the team of analysts. Second session took place in a quiet café.

Participants

As mentioned above, participants P1-P5 were members of the same team in the same company. P1 and P2 helped us for the second time, as they gave as the initial interview (also as P1 and P2). Session with P6 was arranged individually and he was the only expert who helped us across the whole project (P5 in user interviews, P2 in low-fidelity testing).

Participant ID	Time in security job	Job description
P1	7 years	Threat analyst in a networking company
P2	20 years	Threat analyst in a networking company
P3	5 years	Machine learning and security researcher in a networking company
P4	3 years	Cybersecurity tools developer
P5	2 years	Data analyst and machine learning developer in a networking company
P6	2 years	Threat analyst in an antivirus software company

Table 5 High-fidelity prototype testing participants

5.2.3 Test scenarios and questions

We prepared following tasks and steps to evaluate the RSI^3 high-fidelity prototype.

Task 1: Making an overview of incidents - Incidents dashboard section

1. Look at the properties of given incident.
2. If you don't understand the title, read the tooltips.
3. Hide those columns which you don't find useful.
4. Sort the columns (properties) as it suits you.
5. Filter the most important incidents, corresponding with time availability of your SOC team and assign the incidents to you and your colleagues (your imaginary name is Eda Specialist).
6. Check quickly the less important incidents, if there is nothing which would seem more suspicious than as it was automatically evaluated by the system.
7. Pick up an incident which you want to investigate and go to Task 2.

Task 2: Incident investigation - single incident tab (Incident overview)

1. Open incident from the Incidents dashboard.

2. Read through basic info.
3. Look at the public and private IP addresses which participated in the incident. You can sort each of the columns.
4. Look at the timeline. You can filter out logs sent from public, private or all IP addresses.
5. Look at the malware entropy.
6. Look at the table with data from CTI sources about the most involved IP addresses.
7. Open settings. Remove the pie chart with logs sources for this incident.
8. Add a pie chart for transferred megabytes.
9. Add this pie chart to the template of all incidents (default).
10. Edit the position of pie chart (the application should later enable moving and resizing of all elements).
11. Formulate a hypothesis about what might have happened, and questions which you will try to answer in a deeper investigation.

Task 3: Deeper investigation and knowledge saving options

1. Go to incident details, look at proposed functions.
2. Make a graphshot.
3. Go to the Incident notes section. Insert the graphshot.
4. Add a comment to it.
5. Mark incident as Solved.
6. Fill in the form for solved incidents.
7. Close the incident in a side tab.

We prepared questions to evaluate the prototype:

General questions:

- Where do you see the biggest advantage of RSI^3?
- How would RSI^3 make the investigation easier or quicker?
- What did cause you problems?
- Name 3 things which you liked on the design.
- Name 3 things which you would improve on the design.

Incidents dashboard sheet:

- What did you like in the Incidents dashboard? What information was useful to make an overview and prioritize incidents? What helped you to get a clue what the incident is about?
- What did you miss in the Incidents dashboard? What more properties would help you to make a quick decision about the priority?

Single incident investigation:

- What datasets in the Incident overview did you find useful?
- What clues would you read in the overview components (tables, graphs)?
    - Basic info
    - Malware entropy
    - Public IP addresses
    - Private IP addresses
    - Timeline
    - CTI sources info
- How would you personalize the overview? What statistic would you add?

Deeper investigation:

- How would you like the graph-like form of investigation, with detailed information (tables with logs, specific CTI info etc.) on demand?
- What knowledge would you keep in the notes section? What knowledge would you keep directly in the details section (e.g. in comments on nodes)?

5.2.4 Results and findings

We will sum up the results of the high-fidelity prototype testing, which should be factored into the next iteration of the high-fidelity prototype.

General feedback

All participants agreed on the opinion, that combining different data sources to one place is the biggest advantage of RSI^3. RSI^3 could make the investigation easier or quicker, but some participants were restrained to say how much – for example P1 mentioned that there would be a learning curve, which will have to be evaluated to estimate the improvement of current processes.

P6 also raised up the configurability and the fact, that the tool is domain specific and therefore has bigger potential than some other visualization tools, and he liked the communication possibility within RSI^3.

The perception of most useful features differed among the participants – e.g. P3 liked the dashboard, as she saw it quite comprehensive and flexible at the same time, meanwhile P4 raised the single Incident overview and details. P6 told us he likes the layout and how it is connected, and pointed out the Team board and assignees, although the main focus was not on these collaboration features.

When I was asking about things the participants liked about the design, there were also some smaller features mentioned: P3 liked the idea of graphshot (as it was not just a static screenshot), P5 liked the notes, to keep a track of findings.

Participants spoke well about the concept of tabs and possibility to examine several incidents simultaneously. However, P4 was not sure about the vertical position. P1 noted that it would be better to name the tabs by a name or an ID to avoid duplicities of category names.

There was some confusion about the terminology, e.g. about *public* and *private* IPs or *incident category* versus *resolution category*. We realized that the tooltips are not solving the terminology problem completely, there would be a need of a research to find proper self-explaining names for all properties, such that the names are understandable for all analyst from different backgrounds. Also, the example resolution category values made some confusion, as the analysts wouldn't name the resolution categories as proposed.

In general, it would be very helpful to cooperate with some analysts to get into the prototype real, or more real-looking data, as it is hard to guess the example values without a deep domain knowledge.

P1 asked us a lot of questions about how the system should evaluate incidents, and she would like to have that explained in the design. Her questions were general (How the logs are ingested and combined together?) as well as concrete, for example in the case of the CTI sources info table in the Incident overview:

"It is helpful, but I am not sure how this data is obtained or if its accurate. If this is not clear I would not trust what I see there. How a whois delivered to the system a domain, if you searched for IP? Where did you get the URL, is that all, or are more URLs? Partial information is more damaging than lack of information and can lead to bad conclusions."

Similar feedback was given by P2 – he would like to know how the priority was assigned, also with taking account of the category. He was unsure about the defining of subject, whether that feature could be useful to him, and how would be the subjects counted in the incident. He would welcome better explanation of relationship between number of devices and amount of IP addresses (as hardware devices can have more than one IP address). P6 also required better explanation of the devices.

P6 thinks that the time when incident was finished might be misleading, at least until the automated processes are very accurate.

P1 wants to have more dense design, for her there was a lot of space that was not used.

P4 would like to introduce keyboard shortcuts to reduce the number of clicks.

P2 and P4 commented on the format of the dates, as it was hard to read. Possible solution for this is to divide the date and time into two columns, and potentially introduce filtering on hidden columns, which would enable them to filter out given date, but don't show this date and only times. P2 would also change some of the times to relative ones, which would enable him to hide more columns.

In general, number should have spacings in triplets.

P6 also mentioned that prototype doesn't demonstrate a unique URL of single incident, which is very important for him for sharing the incident with someone quickly. He mentioned the need of having a stable interface, with memory, all URL parameters etc., which helps to keep the consistent state when the user interacts with more sections.

Incidents Dashboard

On the beginning of testing process, there was some confusion about how to filter in columns, change their position and hide them. This was captured in P1's observation: "The sorting and filtering is a must, and I am not sure if a Google spreadsheet is ideal for that." We should make the system of position changing more obvious, and we could add a hide icon to each column, to make this function more obvious. On the contrary, P3 had a positive approach: "It was easy to filter out incidents based on different criteria and easy to hide data that are not that interesting at the moment." P6 thought Google sheet was a good approach, as he thinks that having the excel-like functions should be almost standard.

We also received various comments on the colours. P1 was not sure about giving different colours to the incidents. P2 would link the colour also with status. P4 would show colourful categories or add icons to categories for quicker perception. He didn't like the colour of system. Meanwhile P6 liked the colouring of incidents and he was glad that there is no red colour, as he finds red components in software too aggressive.

P1 would like to filter by triage such incidents, which are not expired – we should capture this in prototype data.

P3 didn't like the individual "show" button per line. P4 would like to have clickable rows to see more information and add a link for details on demand. P6 had also problems with opening the incident from the button.

We also observed how the participants would personalise their dashboards. P1 would add a column with hash, which helps to resolve things quickly. She needs to see a confidence level of the categorization. P2 liked the category column. He would hide the ID column and also some of the timing columns (and replace it with relative timings), as mentioned above. He changed the position of the assignee column, as he was looking too much on it and it is not so important to have it on top position. P4 liked the category property but would postpone it to later position. He missed an incident name

column. He hid the description, as it is not important in the overview for him. P5 liked timings and alert sources columns. P6 switched positions of the status and the assignee column and hid the private IPs column as unnecessary.

Single incident investigation

Participants liked the Incident overview in general. They found useful the basic info table (directly mentioned were the timing properties, category and triage), tables with IP addresses, timeline and CTI sources info. Public IPs table and CTI sources info were the most popular. On the contrary, none of the participants understood the malware entropy part. The malware entropy was confusing and therefore it shouldn't be part of the default template. P6 explained to us what kind of graph he had in mind when suggesting the entropy in the low-fidelity prototype testing. This case is the next example of a feature, which will be better to prototype in direct cooperation with the analysts. P2 found the sources of log chart needless, meanwhile P5 liked it.

Participants also liked the possibility to configure the overview, add and remove components. Only negative feedback to the configuration part was by P2 and P6 – we should better explain the terms "default" vs. "current" for showing or hiding of components in all or just current view. P6 would like to have templates on the level of categories – e.g. the transferred megabytes chart would be useful for network incidents, but not for other types.

We did not sufficiently cover the demonstration of possibility to resize and change the positioning of the elements, therefore we got in the feedback some wishes for a better manipulation with elements and their resizing.

P4 missed the possibility to export the tables to paste them on some reports.

Some participants were also creative in describing what components they would add to their personalised dashboard. P2 would like a timeline graph showing how the connections were seen in time in the sense of sequence of actions. This could be similar to the current timeline but focused on single IPs. P5 would like to filter out individual IP addresses in the timeline as well. As similar thing was mentioned already in the low-fidelity prototype testing by P5, this would be good to add, or factor it into configuration of own filters. P2 described another component: "I would like to have information from the network, like destination ports. And also the amount of data transferred on each connection." P4 would add an IoC summary to the overview.

Tables with IP addresses were found as useful. P1 didn't like the division on public and private, she would either show both in one table, or put them side by side to compare. P1 and P4 didn't like the scroll of tables, it should be replaced by pagination. P4 missed the filtering possibilities in those tables. P2 would need to see the connection between the private IP addresses and the users (devices), to get helpful information.

Regarding CTI sources info table, P1 would like to bring more info (like couple of antivirus signature names), P2 would also like to see more and P1 and P5 would add directly a link to the corresponding VirusTotal (or other CTI) page for more info. P5 would also like to see the sources better to decide the importance of the alert accordingly.

Deeper investigation

The walk-through the task 3 was mostly without problems, but P4 was missing a cancel button at the incident status change (the cross was too hidden for him) and P6 had complications when closing the tab.

The answers on the question "How would you like the graph-like form of investigation with detailed information on demand?" showed that the graph would be a good way to go. Only P1 was careful

about the graph-like form – it would have to be really well done and she would need the ability to copy and paste nodes, select them, fix points and drag and drop nodes to rearrange.

Participants also liked the possibilities to keep notes for future reference or for a direct investigation. P1 missed timestamps at the notes (this was shown in the low-fidelity prototype, but we forgot to include it into the high-fidelity one). P4 would write down the assumptions and a hypothesis about the incident and would keep a to-do list. P5 would write down the steps of the attacker and a potential way of spreading.

5.2.5 Collection of ideas for improvement

While testing the high-fidelity prototype, we also prepared a few optional questions, which could help us for future redesigning of parts, which stayed on the stage of the low-fidelity prototype.

- Try to think about 3 different types of investigation (e.g. botnets, DoS, malware). How would differ the information you would be looking for? How would differ the questions and the statistics you would like to see?
- How important would you find the continuous monitoring of those entities, which played a role in some incidents?
- How far do you want to collaborate with the team in the investigation tool and what would you rather leave for other tools? (e.g. chat, wiki, knowledge share, ticketing)

Answers to different types of investigation proved us again how much the investigation procedure can differ.

Three experts commented on Denial of Service (DoS) case. P1 said that DoS must be handled immediately, meanwhile botnet investigation can wait. If it would be a traditional DoS, she would see heavy traffic spikes. If it were a distributed DoS (DDoS), she would expect to see some correlation between different clients infected. P5 would also check a timeline and would search who is the attacker. In contrary, P2 sees no point in finding who is the attacker and would concentrate on the largeness of the incident.

In case of a botnet incident, P1 expects to see the periodicity and a timeline would be a must. P2 would search for the purpose of the botnet and what data is it trying to steal, and also if it is active and working, or not anymore. P5 would search for wider image and similarities in other incidents, as well as for a pattern in botnet behaviour.

For malware incidents, P1 would firstly examine if it is really a malware. P2 would check what is it doing. P5 finds the information about the start of the attack important.

P3 described what questions would she examine in case of data leak: Which internal machines were involved in the incident? Which external IPs were associated with the leak? Are there more than one internal IPs or users that might have been victims of the leak? Are the external IPs involved in other incidents in the past? Then she would search what type of data was leaked from each involved user.

Analysts find continuous monitoring of entities important, especially monitoring of internal IPs. It would also help with investigation of botnet incidents and longer analysis of the behaviour.

Finally, we got a feedback on the need of collaboration. P1 does most investigations alone, as it saves time. She would use own team tools, but she admits that it can be useful to younger analysts to see older incidents of experienced colleagues. P2 would also use different tools, except for comments. P5 finds useful the feature of assigning tasks, as it is helpful for larger teams.

6. Conclusions and future work

6.1 Conclusion

The goal of this thesis was to explore the needs of cybersecurity analysts specialized on incident investigation, and prototype a tool, which would make the investigation easier, both in the cognitive as well as temporal aspects.

We conducted a qualitative research with five analysts and found out their needs. We went to several information sources and we investigated similar solutions, to get better insight into the current situation of incident analysis tools. Based on the needs mentioned in the qualitative research, we defined use-cases and scenarios. We focused on the need of orchestration, i.e. unification of functions which analysts need under one solution, as well as providing knowledge from more sources on one place. We also worked in solutions for collaboration and knowledge sharing.

Subsequently, we designed paper mock-ups, where we caught the main environment and the sections of the tool. We discussed this idea with four participants and based on the feedback and previous knowledge, we designed a paper low-fidelity prototype, where we simulated the workflow and the content of each section. We needed to redesign the sections many times during the process of creation, as we were trying to capture all collected requirements and we had to carefully think through the collaboration of all sections to give a complex solution. The paper prototype allowed us to iterate very quickly, therefore, we believe it was the best approach for the early stages of the product design.

We thought out a story behind the prototype and filled in some values which should be configured by the user (as incident states and categories), created imaginary members of a SOC team and example incidents data. We evaluated the low-fidelity prototype with five analysts and walked through the investigation processes – overview gaining, team collaboration, single incident investigation and tool configuration. The cooperation with participants was pleasant, as they were interested in the prototype and as they know the domain of information technologies, they could imagine the logic behind the prototype.

We identified some unclear places and new wishes in the low-fidelity prototype and we tried to fix them in the next stage. The perception of the level of usefulness of the features differed, and therefore we picked up the Incidents dashboard and single Incident overview as two functions, which were praised unitedly by all participants and we transferred those features into the high-fidelity prototype.

We created an interactive high-fidelity prototype by using Axure and Google Spreadsheet tools and improved the design based on the Material design recommendations. We prepared testing scenarios and collected feedback on the high-fidelity prototype from six participants.

In the beginning it was difficult to recruit enough participants, as it was not easy to get to the right person in the organization. Sometimes it took a few weeks to arrange the meeting, as the analysts are usually very busy. We collaborated with 12 different cybersecurity experts and two developers of real incident investigation tools. We got a helping hand by employees of such companies, as Czech Cisco, Avast, Japanese IBM and others.

The motivation for this project was a real need of a tool, which would make the investigation of cybersecurity incidents easier, as the human resources of security teams are very limited. Therefore, we had a great cooperation experience with the analysts, as they were very friendly and helpful and seemed to be interested in the solution and the creation process.

6.2 Future work

There are many problems waiting to be solved in the incident investigation field. We summed up challenges for the backend of investigation tools, design challenges which were out of scope of this thesis, and finally next steps which should be done with the RSI^3 prototype.

We found following algorithmization challenges:

- Data collection and merge – how the tool will cooperate with other tools to get data from them, e.g. the connection on multiple SIEM systems and CTI tools, removing of duplicated data and merge of corresponding data under one entity.
- Evaluation of incidents – how the tool will group logs, events and SIEM alerts under an incident, how the category of incident will be classified.
- Threats detection based on patterns and classification – how should the system automatically determine what the threat was, which entity was the attacker and the victim, how to highlight the important data in the incident.
- Incident prioritization – what factors should influence the priority, how to account CTI sources, how to learn from previous patterns.
- Creation and configuration of own entities and their relationship – how should the tool map the data on custom entities, how to specify the relationship of this entities and project their properties into the relationship, how the configuration system should look like and what should be its limitations.
- Creation of playbooks and automatization of investigation – how to define playbooks with steps, which will the tool follow to investigate the incidents automatically, how should the system automatically determine next investigation steps based on previous investigations.
- Quick processing of huge amount of data – how to store and process huge amount of data and how to optimize the create, update and delete operations and querying over the data.
- Text processing – how to parse input data, e.g. from CTI sources, and find useful information in the input texts.
- Linking of entities - e.g. linking an IP address of attacker with a real person behind, merge of available information about this person as various SNS accounts, linking of IP addresses and domains in time of the incident.

We also found next user-centred design challenges. In first line is creating of a useful investigation graph. During our research, we touched following topics:

- Entities structure and modularization – each company may have different input data and different needs which entities should be used (e.g. IP addresses, logs, devices, users etc.), therefore it would be good to have the entities configurable. Consequently, there will be a need to find out how should be the entities and their relationships projected into a graph and other sections of the tool.
- Graphical comparison of incidents – how to compare incident with related ones, comparing of the behaviour e.g. with same hour another day, as well as with traffic around the incident time, how to visualise behaviour pattern e.g. in last week.
- Graph layout and highlighting of the attack activators – how to lead the attention of analyst to the most important entities in the incident, how to deal with huge number of nodes, e.g. with less relevant ones.
- Filtering and adding of nodes – how to filter in shown entities, how to search for information, how to add nodes, entities and relationship into the graph.
- Visualisation of history – how to show past data and how to interact with them.

- Form of automated investigation and replays – how to show the results of automated investigation, how to replay previous investigation.

There is also a potential to continue with work on those aspects, which we caught in the low and the high-fidelity prototype. For the Observed entities, Team board and Configuration section, we would like to iterate the ideas and make more qualitative interview sessions with the analysts, where we could clear the requirements and definition of wished functions. We would like to combine it with quantitative research, where we could ask bigger number of analysts about potential usage of some controversial features, as it was proven, that the needs differ company by company. We could prioritize the features based on the extended research, work them in the low-fidelity prototype, again collect a feedback and project it into next iteration of the high-fidelity prototype.

The perception of the prototype could be improved by further research on terminology, where we would find self-explaining terms for the provided features.

We would also work in the high-fidelity prototype the correction and improvements of features, which were commented at the feedback. We would like to expand the interaction with the components to more scenarios. The results of next testing session could be also positively influenced by cooperation with an analyst, who would provide us some real incident data and helped us to work them in.

Finally, by repeating the prototyping and testing phases, we could go to depth and provide a prototype, which could be used as a design and requirements template for an implementation.

References

UX References

[u1] HENRY, Shawn Lawton. *Just ask: integrating accessibility throughout design*. Lawton, 2007.

[u2] BAINBRIDGE, William Sims. *Berkshire encyclopedia of human-computer interaction Vol 2*. Berkshire Publishing Group LLC, 2004.

[u3] UPA International. Usability Body of Knowledge [online]. Accessed 2019-03-30. Available at: www.usabilitybok.org

[u4] BERNSTEIN, Michael S., et al. The trouble with social computing systems research. In: *CHI'11 Extended Abstracts on Human Factors in Computing Systems*. ACM, 2011. p. 389-398.

[u5] SHNEIDERMAN, Ben. The eyes have it: A task by data type taxonomy for information visualizations. In: *The Craft of Information Visualization*. Morgan Kaufmann, 2003. p. 364-371.

[u6] GREEN, Paul; WEI-HAAS, Lisa. The rapid development of user interfaces: Experience with the Wizard of Oz method. In: *Proceedings of the Human Factors Society Annual Meeting*. Sage CA: Los Angeles, CA: SAGE Publications, 1985. p. 470-474.

[u7] KIM, Gerard Jounghyun. *Human–Computer Interaction: Fundamentals and Practice*. Auerbach Publications, 2015.

[u8] PATERNO, Fabio; SANTORO Carmen; SPANO Lucio Davide. Concur Task Trees (CTT). *W3C* [online]. 2012-02-02. Accessed 2019-03-30. Available at: https://www.w3.org/2012/02/ctt/

[u9] Google. Material Design. *Material.io* [online]. Accessed 2019-03-30. Available at: http://materialdesign.io/

[u10] Google. Material Design Color Palette Generator - Material Palette. *Materialpalette.com* [online]. https://www.materialpalette.com/indigo/indigo

Security References

[s1] CHUVAKIN, Anton; BARROS, Augusto. Preparing Your Security Operations for Orchestration and Automation Tools. *Gartner* [online]. 2018-02-28. Accessed 2019-03-30. Available at: https://www.gartner.com/doc/3860563

[s2] CICHONSKI, Paul, et al. Computer security incident handling guide. *NIST Special Publication*, 2012, 800.61: 1-147.

[s3] ROUSE, Margaret. What is incident response?. *WhatIs.com* [online]. 2017-10. Accessed 2019-03-30. Available at: https://searchsecurity.techtarget.com/definition/incident-response

[s4] TCHESNOKOV, Serguei. Indicators of Compromise: Their Role in a Company's Information Security. *ScienceSoft* [online]. 2017-11-02. Accessed 2019-03-30. Available at: https://www.scnsoft.com/blog/indicators-of-compromise-their-role-in-a-companys-information-security

[s5] POSTEL, Jon. *Internet protocol* (No. RFC 791). 1981.

[s6] AlienVault. The SOC Team: Roles and Responsibilities. *AlienVault* [online]. Accessed 2019-03-30. Available at: https://www.alienvault.com/resource-center/ebook/building-a-soc/soc-team

[s7] ROUSE, Margaret. What is command-and-control server (C&C server)?. *WhatIs.com* [online]. 2017-01. Accessed 2019-03-30. Available at: https://whatis.techtarget.com/definition/command-and-control-server-CC-server

[s8] Splunk. Log Management. *Splunk* [online]. Accessed 2019-03-30. Available at: https://www.splunk.com/en_us/solutions/solution-areas/log-management.html
[s9] Splunk. Incident Investigation and Forensics. *Splunk* [online]. Accessed 2019-03-30. Available at: https://www.splunk.com/en_us/cyber-security/incident-investigation-forensics.html
[s10] IBM. IBM i2 Analyze. *IBM* [online]. Accessed 2019-03-30. Available at: https://www.ibm.com/us-en/marketplace/enterprise-intelligence-analysis
[s11] IBM. IBM QRadar SIEM. *IBM* [online]. Accessed 2019-03-30. Available at: https://www.ibm.com/cz-en/marketplace/ibm-qradar-siem
[s12] IBM. IBM Resilient Incident Response Platform. *IBM* [online]. Accessed 2019-03-30. Available at: https://www.ibm.com/us-en/marketplace/resilient-incident-response-platform
[s13] Cyberbit. Security Orchestration and Automation and Response (SOAR). *Cyberbit* [online]. Accessed 2019-03-30. Available at: https://www.cyberbit.com/solutions/security-operations-automation-orchestration/
[s14] Stratosphere IPS. ManaTI. *Stratosphere Lab* [online]. Accessed 2019-03-30. Available at: https://www.stratosphereips.org/projects-manati/
[s15] Cambridge Intelligence. KeyLines' features. *Cambridge Intelligence* [online]. Accessed 2019-03-30. Available at: https://cambridge-intelligence.com/keylines/features/
[s16] Grafana Labs. Grafana Features. *Grafana Labs* [online]. Accessed 2019-03-30. Available at: https://grafana.com/grafana
[s17] Linkurious. Graph visualization software - Linkurious. *Linkurious* [online]. Accessed 2019-03-30. Available at: https://linkurio.us/product/
[s18] AT&T. OSSIM: The Open Source SIEM. *AlienVault* [online]. Accessed 2019-03-30. Available at: https://www.alienvault.com/products/ossim
[s19] INFANTES, Juan. VirusTotal Blog: VirusTotal Graph. *VirusTotal* [online]. 2018-01-08. Accessed 2019-03-30. Available at: https://blog.virustotal.com/2018/01/virustotal-graph.html
[s20] KAVANAGH, Kelly; BUSSA, Toby; SADOWSKI, Gorka. 2018 SIEM Gartner Magic Quadrant. *Logrhythm* [online]. 2018-12-03. Accessed 2019-03-30. Available at: https://logrhythm.com/gartner-magic-quadrant-siem-report-2018/
[s21] VirusTotal. About us - VirusTotal. *VirusTotal* [online]. Accessed 2019-03-30. Available at: https://support.virustotal.com/hc/en-us/sections/115000720829-About-us
[s22] RiskIQ. RiskIQ PassiveTotal Threat Investigation Platform. *RiskIQ* [online]. Accessed 2019-03-30. Available at: https://www.riskiq.com/products/passivetotal/
[s23] Cisco Talos Intelligence Group. Reputation Center. *Cisco Talos Intelligence* [online]. Accessed 2019-03-30. Available at: https://www.talosintelligence.com/reputation
[s24] MISP. MISP - Malware Information Sharing Platform and Threat Sharing - The Open Source Threat Intelligence Platform. *MISP* [online]. Accessed 2019-03-30. Available at: https://www.misp-project.org/
[s25] URLScan. About - urlscan.io. *URLScan* [online]. Accessed 2019-03-30. Available at: https://urlscan.io/about/
[s26] DAIGLE, L. Rfc 3912: Whois protocol specification, September 2014. *Status: DRAFT STANDARD*, 2004.
[s27] AlienVault. AlienVault - Open Threat Exchange. *AlienVault* [online]. Accessed 2019-03-30. Available at: https://otx.alienvault.com/?utm_medium=InProduct&utm_source=ThreatCrowd
[s28] DOWNING, Ben. Using Entropy in Threat Hunting: a Mathematical Search for the Unknown. *RedCanary* [online]. 2018-02-20. Accessed 2019-03-30. Available at: https://redcanary.com/blog/threat-hunting-entropy/

Image Sources

[i1] https://cognitive.cisco.com/preview/l

[i2] https://www.splunk.com/en_us/cyber-security/incident-investigation-forensics.html

[i3] https://exchange.xforce.ibmcloud.com/api/hub/extensionsNew/e7f820b6cb6f4fcba0092f61768061dc/resillient_query_results.png

[i4] https://s3-eu-central-1.amazonaws.com/cyberbit/wp-content/uploads/2018/10/29145929/Slider-SOC-product-page.png

[i5] https://youtu.be/5-g0YhGKQ28?t=29

[i6] https://youtu.be/14OPKlBIt5s?t=1250

[i7] https://youtu.be/14OPKlBIt5s?t=1403

[i8] https://cdn.alienvault.com/images/uploads/product/tour/slide-3.png

[i9] https://lh5.googleusercontent.com/_9Gbzjw1V7mPkeWi-LXQ0aWwcLRvIdBfdhLUrGUvekgv1Lm0RvL5ImIo4kgtYKnQOrfd0kuqy2uO0U2Srqg7wlyketX43CYUPd5CprncM8EfnVCP6lpOIDbwZCeC9ZTuRTP4oan3

[i10] https://1.bp.blogspot.com/-k7CQUS6t3nY/VtOJQzCErpI/AAAAAAAAANo/maNxj1K4S8Q/s640/Overall.png

[i11] https://www.pexels.com/photo/adult-chill-computer-connection-450271/

[i12] https://www.pexels.com/photo/woman-in-blue-floral-top-sitting-while-using-laptop-806835/

Appendix: Content of attached CD

Attached CD contains following files:

- This master thesis as PDF file
- Folder “Mockup” with photos of mock-ups
- Folder “Low-fidelity” with photos of low-fidelity prototype
- Folder “High-fidelity” with main Axure project, Excel file with example incidents from Incidents dashboard, file with instructions how to connect those, two print screens of the prototype and supportive Axure project and images of graphs (loading those was slowing down the main project, therefore we linked the graphs as images).