

# **Sharing cyber threat intelligence in cyber exercise**

**Does controlled sharing of threat intelligence improve situation  
awareness?**

Pasi Hyytiäinen

Master's Thesis

June 2018

School of Technology, communication and transport

Master's Degree Program in Information Technology  
Cyber Security

Author(s) Hyytiäinen, Pasi	Type of publication Master's thesis	Date June 2018
		Language of publication: English
	Number of pages 114	Permission for web publication: x
Title of publication <b>Sharing cyber threat intelligence in cyber exercise</b> Does controlled sharing of threat intelligence improve situation awareness?		
Degree programme Master's Degree Program in Information Technology, Cyber Security		
Supervisor(s) Saharinen, Karo Huotari, Jouni		
Assigned by JAMK University of Applied Sciences, JYVSECTEC Lötjönen, Jarno		
Abstract  <p>The first idea for this research started to evolve during on the cyber security exercise course at JAMK University of Applied Sciences in spring 2017, when it was noticed that the existing exercise tools were not good enough for keeping up the situation awareness of the exercise a decent level regardless of the team where one is a participant. It was difficult follow what was going on in each team.</p> <p>The research focused on two different themes: to understand how current tools in the realistic global cyber environment RGCE were used by defender teams for situation awareness during cyber security exercise. The second research theme focused on how defender teams collected, analyzed and shared cyber threat intelligence during the cyber security exercise.</p> <p>The research was conducted as empirical study containing both qualitative and quantitative approaches. Cyber security exercise course was used as a case study and two different surveys were sent to the members of the defender teams in the cyber security exercise.</p> <p>As a result, it was found out what the most used tools for the situation awareness were during a cyber security exercise. It was possible to identify which were the most important situation awareness tools and methods at individual level and at the team level as well.</p> <p>It was not possible to identify if the controlled sharing of cyber security threat intelligence in cyber exercise improve the situation awareness, as the defender teams failed to collect relevant cyber security threat intelligence. There is a need for further research how defender teams handle the cyber threat intelligence in cyber exercises to understand what issues needs to be considered when planning cyber exercises.</p>		
Keywords/tags ( <a href="#">subjects</a> ) Cyber threat intelligence, Situational awareness, Cyber Exercise, Cyber Security		

Tekijä(t) Hyytiäinen, Pasi	Julkaisun laji Opinnäytetyö, ylempi AMK	Päivämäärä Kesäkuu 2018
		Julkaisun kieli Englanti
	Sivumäärä 114	Verkojulkaisulupa myönnetty: x
Työn nimi <b>Kyberturvallisuushkatietojen jakaminen kyberturvallisuusharjoituksessa</b> Parantaako kontrolloitu kyberturvallisuushkatietojen jakaminen tilannetietoisuutta?		
Tutkinto-ohjelma Master's Degree Program in Information Technology, Cyber Security		
Työn ohjaaja(t) Karo Saharinen Jouni Huotari		
Toimeksiantaja(t) Jyväskylän ammattikorkeakoulu, JYVSECTEC Jarno Lötjönen		
Tiivistelmä <p>Ensimmäinen idea tälle tutkimukselle syntyi Jyväskylän ammattikoreakoulun kyberturvallisuusharjoituskurssilla keväällä 2017, kun huomattiin, että käytössä olevat harjoituksen työkalut eivät olleet riittävät ylläpitämään harjoituksen tilannetietoisuutta riippumatta siitä, missä tiimissä olit. Oli vaikeata seurata, mitä missäkin tiimissä tapahtui.</p> <p>Tutkimus keskittyi kahteen teemaan: yritettiin ymmärtää mitä nykyisiä työkaluja globaalissa kyberympäristössä RGCE:ssä puolustava tiimi käyttää tilannetietoisuuden ylläpitämiseksi kyberharjoituksen aikana. Toinen tutkimusteema keskittyi, siihen miten puolustavat tiimit keräävät, analysoivat ja jakavat kyberturvallisuushkatietoja kyberturvallisuusharjoituksen aikana.</p> <p>Tutkimus oli luonteeltaan empiirinen, jossa käytettiin kvalitatiivisia ja kvantitatiivisia menetelmiä. Kyberturvallisuusharjoituskurssia käytettiin kokeellisen tutkimuksen ympäristönä ja kaksi eri kyselyä lähetettiin puolustavien tiimien jäsenille.</p> <p>Tulokseksi saatiin selvitettyä, mitkä ovat tärkeimmät työkalut tilannetietoisuuden ylläpitämiseksi kyberturvallisuusharjoituksessa. Oli mahdollista tunnistaa, mitkä olivat tärkeimmät työkalut ja menetelmät niin yksilön kuin tiimin näkökulmasta.</p> <p>Ei kuitenkaan saatu selvitettyä, parantaako kyberturvallisuushkatietojen jakaminen kyberturvallisuusharjoituksessa tilannetietoisuutta, sillä puolustavat tiimit epäonnistuivat keräämään merkityksellistä kyberturvallisuushkatietoja. Onkin tarve jatkotutkimukselle, miten puolustavat joukkueet käsittelevät kyberturvallisuushkatietoja kyberturvallisuusharjoituksissa, jotta ymmärrettäisiin mitä pitää ottaa huomioon kyberturvallisuusharjoituksia suunniteltaessa.</p>		
Avainsanat ( <a href="#">asiasanat</a> ) Kyberturvallisuushkatiedot, tilannetietoisuus, kyberturvallisuusharjoitus, kyberturvallisuus		

## Contents

<b>Acronyms.....</b>	<b>8</b>
<b>1 Introduction.....</b>	<b>9</b>
<b>2 Knowledge in cyber defence .....</b>	<b>12</b>
2.1 Cyber threat intelligence .....	12
2.2 Managing the cyber threat intelligence as knowledge.....	15
2.3 Sharing cyber threat intelligence and knowledge .....	18
2.4 Situation awareness and cyber security .....	19
2.5 Research in human behavior and cyber security exercises .....	23
<b>3 Research .....</b>	<b>25</b>
3.1 Research methodology .....	25
3.2 Collecting and sharing cyber threat intelligence .....	25
3.3 Research questions .....	28
3.3.1 Situation awareness .....	28
3.3.2 Cyber threat intelligence .....	28
3.4 Risks.....	29
<b>4 Technical cyber security exercise setup .....</b>	<b>31</b>
4.1 Technical Cyber Security Exercise Course .....	31
4.2 Game controlling teams .....	32
4.2.1 White Team.....	32
4.2.2 Red Team .....	33
4.3 Blue Teams .....	34
4.4 Exercise environment .....	38
4.5 MISP – Open Source Threat Intelligence Platform .....	39
4.6 Exercise events .....	42
4.7 Processes and tools in the exercise .....	44
<b>5 Research results.....</b>	<b>45</b>
5.1 Survey information .....	45
5.2 Event detection.....	46
5.3 Situation awareness.....	47
5.4 Cyber threat intelligence .....	50
5.4.1 Collecting cyber threat intelligence .....	52
5.4.2 Analyzing cyber threat intelligence .....	54
5.4.3 Sharing cyber threat intelligence .....	55
5.4.4 Receiving cyber threat intelligence .....	57
5.4.5 Sharing and receiving cyber threat intelligence with MISP.....	59
5.4.6 Mitigation of threats .....	61
5.4.7 Quality of cyber threat intelligence .....	63
5.5 Analysis of created MISP events.....	66

<b>6</b>	<b>Discussion on results .....</b>	<b>71</b>
6.1	Analyzing the Goal 1 .....	71
6.2	Analyzing the Goal 2 .....	72
6.3	Analyzing the Goal 3 .....	74
6.4	Analyzing the Goal 4 .....	74
6.5	Analyzing the Goal 5 .....	75
6.6	Analyzing MISP as a tool .....	76
6.7	Analyzing the situation awareness .....	79
<b>7</b>	<b>Conclusions.....</b>	<b>83</b>
	<b>References.....</b>	<b>85</b>
	<b>Appendices.....</b>	<b>89</b>
	Appendix 1. Survey: Situation Awareness and Cyber threat intelligence in WINE 2018 .....	89
	Appendix 2. Survey : MISP and Cyber threat intelligence.....	94
	Appendix 3. YSOC incident handling process .....	98
	Appendix 4. Malicious IPv4 address lists in RGCE.....	99
	Appendix 5. Malicious domain names in RGCE .....	100
	Appendix 6. Malware information 1 .....	101
	Appendix 7. Malware information 2 .....	102
	Appendix 8. Malware information 3 .....	103
	Appendix 9. False user accounts.....	104
	Appendix 10. MISP Suspicious person : manilapikes.....	105
	Appendix 11. MISP event containing malware info and malicious ip's .....	106
	Appendix 12. FINESTONIA threat actor information .....	107
	Appendix 13. CNN CVE news .....	108
	Appendix 14. Telia OSINT emails .....	109
	Appendix 15. pastebin dataleaks .....	110
	Appendix 16. Christmas Tree malicious code in GitLab (Wood 2013).....	111
	Appendix 17. Suspicious user markek00310 posts in imgr.com .....	112
	Appendix 18. Suspicious twitter accounts .....	113
	Appendix 19. Suspicious bank account : manilapikes.....	114

## Figures

Figure 1. Situational awareness system .....	10
Figure 2. Cyber Threat Intelligence Model .....	12
Figure 3. Cyber resilience context .....	14
Figure 4. The conventional view on the knowledge hierarchy .....	16
Figure 5. OODA-loop in cyber defense .....	17
Figure 6. Autopoiesis at project-based company .....	18
Figure 7. OODA loop with vigilant information systems.....	20
Figure 8. The situation awareness model .....	21
Figure 9. Team situational awareness.....	23
Figure 10. White Team organization structure .....	32
Figure 11. RT organization structure.....	34
Figure 12. Exercise company relationships .....	35
Figure 13. Cyber threat intelligence sharing community.....	35
Figure 14. YSHOP organization structure .....	36
Figure 15. YSTORE organization with main communication flow .....	38
Figure 16. Small set of MISP object categories .....	41
Figure 17. MISP DDOS object template .....	41
Figure 18. Appendix 2, question 13 results .....	51
Figure 19. How difficult was it to collect cyber threat intelligence during the exercise? .....	53
Figure 20. YSTORE detected malicious IPv4 address .....	53
Figure 21. How difficult was it to analyze the collected cyber threat intelligence during the exercise? .....	54
Figure 22. CNN news hint that something is going on.....	59
Figure 23. How easy was it to collect and store cyber threat intelligence with following tools?.....	61
Figure 24. YSOC malware analysis .....	62
Figure 25. Quality of collected and received cyber threat intelligence .....	63
Figure 26. Quality of received MISP IOCs.....	64
Figure 27. YBANK detected malicious scanning .....	67
Figure 28. MISP event relationships related to detected malicious IPv4 address .....	67
Figure 29. Blacklist created based on Telia IPv4 address list .....	72
Figure 30. YSOC fails to detect their own IPv4 address .....	73
Figure 31. YBANK detected attack pattern and tools .....	73
Figure 32. YSOC detected FINESTONIA .....	74
Figure 33. YSHOP detection of malicious plugin for CSE311.....	75
Figure 34. YSHOP reported CSE311 to MISP .....	76
Figure 35. Cyber Security information consumers and providers .....	79
Figure 36. Most important situation awareness tool: MISP users vs non MISP users	81

## Tables

Table 1. Exercise team setup .....	31
Table 2. Exercise events .....	43
Table 3. Survey 1 respond rate .....	45
Table 4. Survey 2 respond rate .....	45
Table 5. Events in the exercise split by exercise day .....	46
Table 6. Detected events.....	47
Table 7. Did you collect cyber threat intelligence during the exercise? .....	47
Table 8. What tools did you use for maintaining your situation awareness? .....	47
Table 9. Tickets in incident management systems .....	48
Table 10. Weighted situation awareness tools used by BT.....	49
Table 11. Phone call statistics from the exercise .....	50
Table 12. Did you collect cyber threat intelligence during exercise? .....	52
Table 13. Did your company collect cyber threat intelligence during exercise? .....	52
Table 14. Survey 2, data of questions 4 and 5.....	54
Table 15. Survey 2, data of questions 6 and 7.....	55
Table 16. Did you share cyber threat intelligence during exercise in your company to your co-workers? .....	55
Table 17. Did you share cyber threat intelligence during exercise to other companies? .....	56
Table 18. Did your company shared cyber threat intelligence during exercise to other companies? .....	56
Table 19. What tools you or your company used to share cyber threat intelligence to other companies? .....	56
Table 20. Did your company receive any cyber threat intelligence from other companies during the exercise? .....	57
Table 21. What tools did your company use to receive cyber threat intelligence from other companies? .....	58
Table 22. Did your company share IOC data using MISP? .....	59
Table 23. Did your company receive IOC data using MISP?.....	59
Table 24. Shared MISP events .....	60
Table 25. Did you use the collected or shared cyber threat intelligence to mitigate threats? .....	62
Table 26. Did your company use the collected or shared cyber threat intelligence to mitigate threats?.....	63
Table 27. Overall quality of collected, shared and received cyber threat intelligence	64
Table 28. Trusting the cyber threat intelligence.....	65
Table 29. Quality of the received cyber threat intelligence from different sources...	66
Table 30. BTs and their incidents and events.....	66
Table 31. Expected IOCs vs analyzed MISP attributes .....	68
Table 32. Correct MISP attributes reported for detected RT events.....	69
Table 33. Expected and reported correct MISP attributes for WT events.....	69
Table 34. Summary of exercise events, containing expected MISP attributes vs reported MISP attributes .....	70
Table 35. Atomic indicators detected on wiki pages or in the incident management systems.....	71

## Acronyms

ENISA	Europe European Union Agency for Network and Information Security
CSIRT	Computer Security Information Response Team
JYVSECTEC	Jyväskylä Security Technology
RGCE	Realistic global cyber environment
TTP	Tactics, techniques and procedures
IOC	Indicator of compromise
ATP	Advanced persistent threats
CVE	Common Vulnerabilities and Exposures
OSINT	Open Source Intelligence
RT	Red Team
WT	White Team
BT	Blue Team
SOC	Security Operation Center
CSC	Cyber Security Center
MISP	Malware Information Sharing Platform
CIRCL	Computer Incident Response Center Luxembourg



# 1 Introduction

Sharing cyber threat intelligence is seen as one of the major issues when fighting against cyber crime. In Europe, the European Union Agency for Network and Information Security (ENISA) has started to improve co-operation between national and governmental Computer Security Information Response Teams (CSIRT) (Directive (EU) 2016/1148). In the United States, similar co-operation between private security organizations is improved by the Department of Homeland Security (Executive Order No. 13691).

Sharkov (2016, 1) points out in his keynote speech in 23rd ACM Conference on Computer and Communications Security that in future the challenge is to have cyber resilience, which means that nations and organizations should be prepared for unforeseeable and unpredictable unknowns i.e. “unknown unknowns” threats in cyberspace. “Unknown unknowns” are the risks or threats which have not yet been identified by anyone (Sharkov 2016, 2). It is the unknown, for example software vulnerabilities that no-one has not yet found out.

When handling cyber security incidents, collaboration is seen as an effective way to mitigate threats (Directive (EU) 2016/1148). Even if there is not trust between involved organizations, the collaboration network and sharing the information can help to handle the cyber incidents or mitigate the threats (Garrido-Pelaz, González-Manzano & Pastrana 2016, 9; Kokkonen 2016, 130).

Cyber exercises are one way to train organizations to handle cyber incidents. Cyber exercises are arranged in isolated closed cyber ranges so that organizations can train in practice how to mitigate different kinds of threats affecting their critical assets.

By definition in cyber exercise the cyber security incident is a reported and managed event, which is seen and identified by an organization, as defender team, to be something which needs to be reacted to and investigated further (Lötjönen 2017, 43).

In a cyber exercise multiple organizations can train co-operation. They might have mutual interests to mitigate cyber security incidents because the organizations might have business relations e.g. organization 1 providing software as service, platform as

service or security as service to organization 2. Collaboration is needed when organizations and their information systems depend on each other. Service level agreements are defined to ensure that each involved organization knows their own responsibilities to ensure the confidentiality, integrity and availability of the agreed assets.

Since 2011, JAMK University of Applied Sciences, the Institute of Information Technology has been a driving force to create JYVSECTEC (Jyväskylä Security Technology) as an independent cyber security research, training and development center. The technical environment for cyber security exercises is called RGCE, realistic global cyber environment. (Vatanen et al 2017, 2) )

Lötjönen, in his master thesis (Lötjönen, 2017) has defined a set of requirements for a cyber security situational awareness system for the defender in cyber security exercises held in RGCE. The defined system should help the defender to resolve cyber security incidents fast and effectively. When organizations participate in a cyber security exercise, threat intelligence is needed in order to be able to understand the ongoing situation (Lötjönen 2017, 41-42). The situation awareness system contains several components as defined in Figure 1.

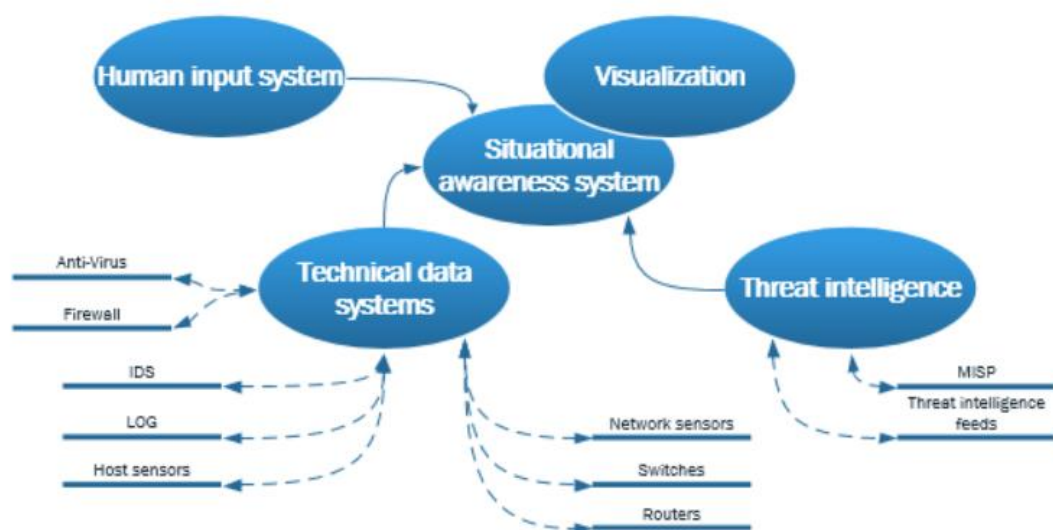


Figure 1. Situational awareness system (Lötjönen 2017, 42)

The proposed system contains a database, where cyber threat intelligence is collected during the exercise (Lötjönen 2017, 58-60), however it is not a mandatory requirement to use an additional threat intelligence sharing platform to collect and share the cyber threat intelligence between defender teams.

This thesis is assigned by JYVSECTEC, as it is currently planning the new situation awareness system based the requirement specification. There is a need to understand how current tools are used for situation awareness, not only at individual level, but also at team level as well.

The aim of this thesis is to understand what kind of threat intelligence is gathered, how it is shared between defender teams and how the shared information is used to mitigate cyber security threats. The outcome of this thesis should help JYVSECTEC to plan cyber security exercises in future.

## 2 Knowledge in cyber defence

### 2.1 Cyber threat intelligence

Figure 2 is a cyber threat intelligence model (Mavroeidis & Bromander 2017, 2), which presents what kind of information can be collected when investigating cyber security incident or what kind of information can be collected from multiple sources to gain cyber threat intelligence. The collected cyber threat intelligence should help organisations to manage cyber threats and help them to enhance cyber defence (Borum, et al. 2015).

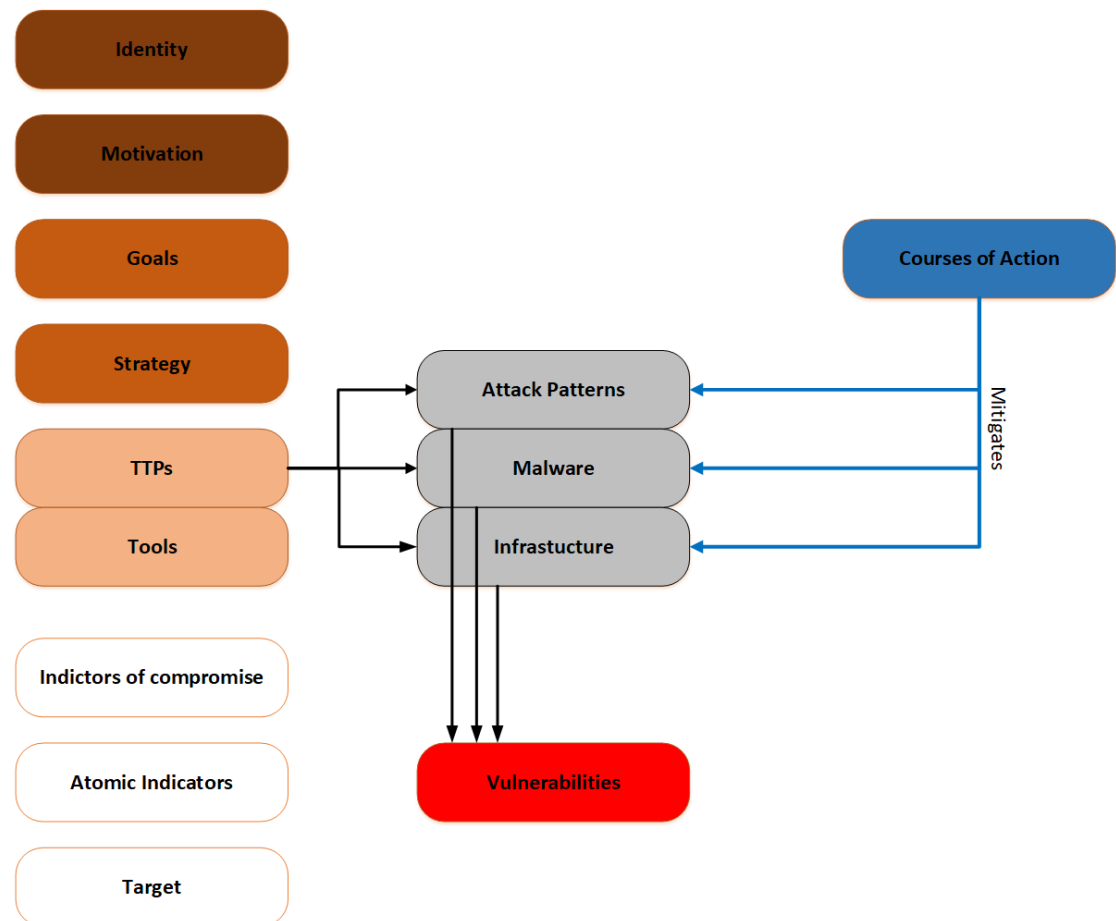


Figure 2. Cyber Threat Intelligence Model (Mavroeidis & Bromander 2017, 2)

When collecting cyber threat intelligence, the goal is to identify the threat actor, what motivates the threat actor and what goals the actor has as there cannot be strategy without goals. (Mavroeidis & Bromander 2017, 3).

TTPs i.e tactics, techniques and procedures are the technical knowledge that threat actor uses to achieve the goals (Mavroeidis & Bromander 2017, 3). Attack patterns are a way to group known attack types together, for example denial of service (DoS) or phishing emails.

Malware is usually a piece of software, which needs to be inserted into the target system for future use. Tools are used by threat actors to perform the actual attacks or to carry out technical reconnaissance to find out about possible vulnerabilities of the target.

Atomic indicator is the smallest piece of information to be used to detect and defend against cyber security threat, e.g. cryptographic hash value of a malware executable or an email address of a known spam bot. (Mavroeidis & Bromander 2017, 3; Johnson, et al 2016, 2).

The indicators of compromise (IOC) are a well documented set of atomic indicators defining a campaign grouping all relevant gathered information related to it: TTPs, atomic indicators, tools, threat actors, malware, etc. (Mavroeidis & Bromander, 2017, 3).

Course of actions are the techniques and procedures of the target to mitigate the threat actor to achieve their goals (Mavroeidis & Bromander 2017, 3). One way to mitigate the threats is to follow up different kind of security alerts such as Common Vulnerabilities and Exposures (CVE®) List (MITRE) or National Vulnerability Database (National Institute of Standards and Technology), which often contains information how to mitigate the vulnerability. Threat intelligence reports are also a good way to improve the situational awareness of an organization (Johnson et al. 2016). Often, these are related together with the CVEs.

The quality of the collected threat intelligence is an increasing problem, when organisations and individual security analysts start to collaborate to create, share,

improve and use it as organisations needs it to improve their cyber defence (Al-Ibrahim et al. 2017; Borum, et al. 2015; Sillaber, et al. 2016).

Organisations needs to have strategic cyber security intelligence to decrease the risk of cyber security incident (Borum et al. 2015). Sharkov (2016, 4) defines that organisations needs to have cyber security resilience. Cyber security resilience context is shown in Figure 3.

Sharkov defines the “known knowns” as the known threats against the confidentiality, integrity and availability of information. For example critical systems have duplicated network connections to ensure that systems can be accessed when needed. Virus scanners are another example how to be prepared for the known threats. (Sharkov 2016, 2.)

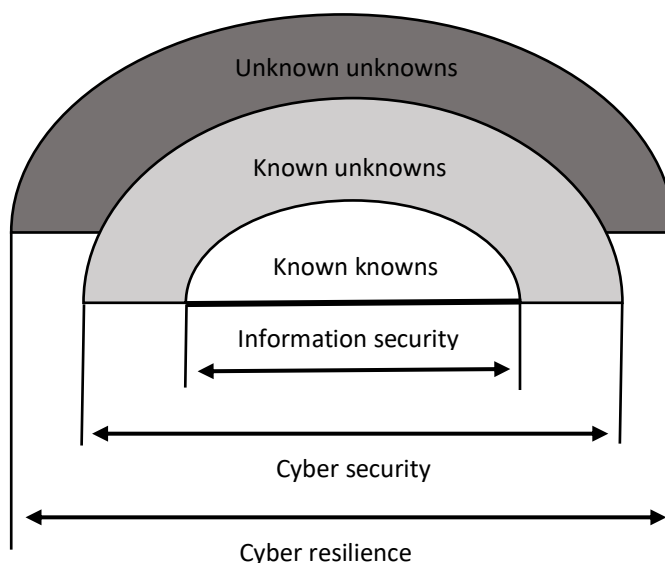


Figure 3. Cyber resilience context (Sharkov 2016, 2)

Sharkov (2016, 2) defines “known unknowns” as the way to handle the advanced persistent threats (APTs) in complicated cyber space where handling the threats requires co-operation between one or more organizations.

“Unknown unknowns” are the risks or threats which have not yet been identified by anyone (Sharkov 2016, 2). It is the unknown, for example any operating system or

used software might have vulnerabilities that no-one has not yet found out. When organisations are improving the cyber defence, the key is to be prepared to any kind of incident.

It can be considered that when an organization is going to have a cyber security exercise, it prepares to handle a set of “unknown unknown” attack patterns. If the organization gains valuable and accurate information e.g. about a new vulnerability in their used software while preparing for the cyber security exercise, it is no longer an “unknown unknown”. It can be assumed that when new vulnerability is found, there will be or already exists e.g. unknown unknown tool, malware or attack pattern which can be used by the threat actor in the cyber security exercise.

When atomic indicators of the tools or malware are found and identified, they are known knowns and security controls can be configured to detect the malware. The threat can be mitigated, for example, by updating the vulnerable software when a patch is available.

## 2.2 Managing the cyber threat intelligence as knowledge

The cyber threat intelligence can also be seen as piece of information, knowledge or data. IOCs are a well documented set of atomic indicators i.e data. Cyber security incident is a set of information and data describing what happened and when. It might also contain the data about what IOC's were seen and the information on how the incident was resolved. The cyber security incident will evolve to be knowledge when individual organisation members reuses the gathered information when resolving similar kind of cyber security incidents.

It is a philosophical question how to define data, information and knowledge, however, the most common interpretation is that data is a simple isolated fact. When several facts are grouped, combined or structured in a context, data can be called a piece of information. (Tuomi, 1999, 105.)

Cognitive and autopoietic epistemologies are philosophies, which consist of views of interpreting knowledge. Cognitive epistemology equates knowledge only with explicit knowledge, i.e. knowledge is transferable, universal and objective. Autopoietic epistemology has different views about the input that comes from

outside to receiver. This input is not seen as knowledge but as data, which has to be interpreted and it is the main reason why knowledge cannot be directly conveyed from one individual to another. This means that knowledge can only be produced, and the only way to acquire new knowledge is to observe data and combine it with existing knowledge. (Koskinen 2010, 157)

Figure 4 presentation of knowledge hierarchy. The aim is to present the fact that it takes time and effort to process enough data to get valuable information which then can be used as knowledge. The knowledge is then needed to be able to make intelligent choices when needed. (Tuomi, 1990, 106-107)

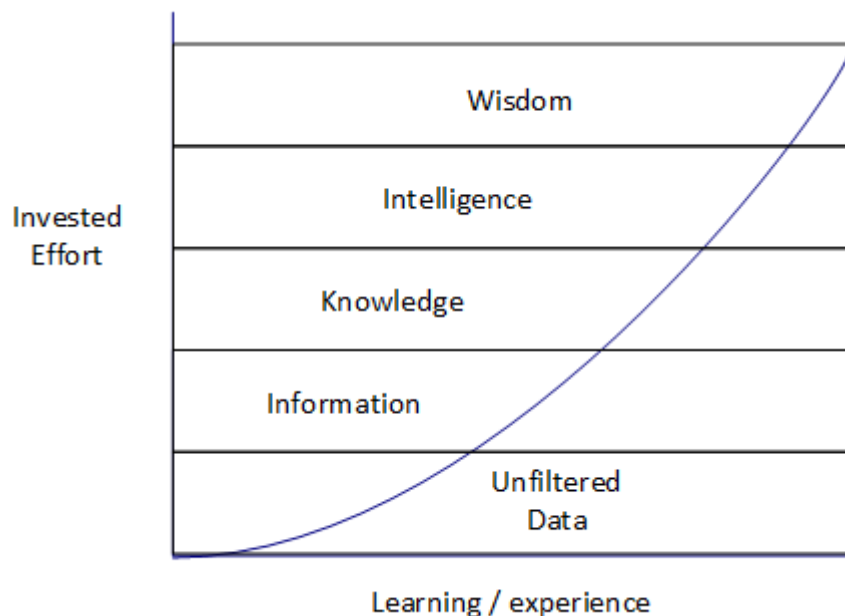


Figure 4. The conventional view on the knowledge hierarchy (Tuomi, 1999, 106)

To be able to do fast decisions or intelligent choices, the process is often referenced and simplified to OODA-loop by Boyd (Brehmer, 2005, 2-4; Fusano et al., 2011, 131). The phases are Observation-Orientations-Decision-Action and can be defined as in Figure 5, where Kokkonen (2016, 60) has adapted it to define decision making for cyber defense.



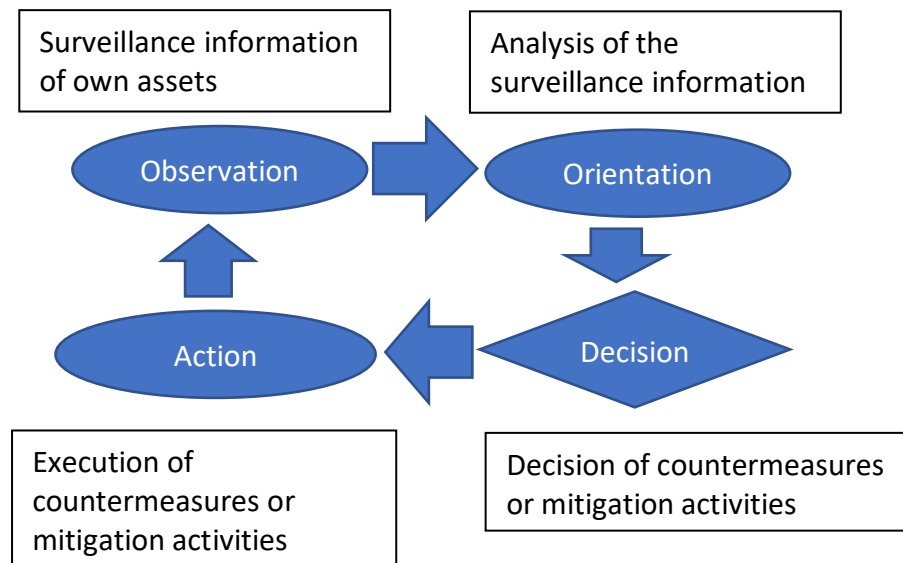


Figure 5. OODA-loop in cyber defense (Kokkonen, 2016, 60)

The observation of known-known threats should be quite trivial as the cyber threat intelligence has been made available by cyber threat intelligence sharing communities and in most cases, there is well written documentation of how to mitigate the threat. In some cases correctly configured mitigation tools can detect and even mitigate the threat automatically.

As Kokkonen (2016, 60) points out the OODA loop requires that own assets generate raw data that can be collected and analysed as surveillance information. To be able to identify and make decisions with unknown knowns or unknown unknowns cyber security threats happens, it is required that the individual person has enough information, intelligence or even wisdom.

In this context a company resolving cyber security incidents is an autopoietic system as shown in Figure 6. Handling a cyber security incident will create a small project, which is a new autopoietic system and these autopoietic systems develop their own lives and become self-referencing in their own ways as the incidents are handled by the defined incident handling process and personnel.

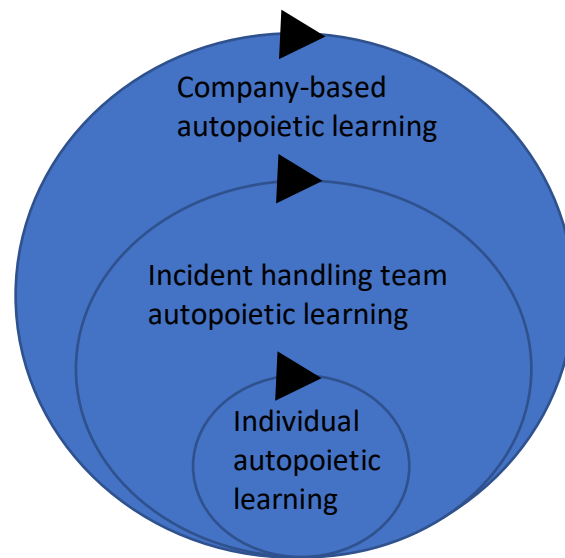


Figure 6. Autopoiesis at project-based company (Koskinen, 2010)

When cyber security incidents are linked to each other they interact mutually. Incidents generate the knowledge structures of a company, and the company itself provides the conditions and constraints for handling the incidents. The knowledge production takes place at various organizational levels: at individual, incident handling team and company level. Producing knowledge is a recursive process, where there cannot be clear breaks between past, present and future. The previous incidents have left their traces on the later incidents, which is result of producing new knowledge, which is a prerequisite for an autopoietic system (Koskinen 2010, 156).

As knowledge management point of view, the OODA-loop forces the individual cyber security incident handler to gain knowledge and intelligence as cyber threat intelligence, which he/she can then use to observe new phenomena.

### 2.3 Sharing cyber threat intelligence and knowledge

Autopoietic epistemology defines that the only way to acquire new knowledge is to observe data and combine it with the existing knowledge (Koskinen 2010, 157). This will affect how to share cyber threat intelligence data and how to observe it so that it will generate new knowledge. This issue affects when two or more people who are involved in when handling a cyber security incident as knowledge cannot be directly conveyed from one individual to another.

Several authors have pointed out that the quality of the collected threat intelligence is an increasing problem (Al-Ibrahim et al. 2017; Borum, et al. 2015; Sillaber, et al.

2016). It can be seen as a learning problem as it takes time and effort to gain intelligence, as shown in Figure 4.

Cyber threat intelligence model (Mavroeidis & Bromander 2017, 2) is trying to define different aspects of the cyber security threat or incident. Collecting data as targets, IOC's and TTP's is carried out by all cyber security incident handlers and it might be shared as cyber threat intelligence e.g. as Open Source Intelligence (OSINT).

Several authors have pointed out that there are some issues when sharing cyber threat intelligence. The main issue is the privacy i.e. can private data be shared as cyber threat intelligence when handling cyber security incidents, where laws might restrict what can be shared (Fisk et al. 2015; Johnson et al. 2016, 12; Moihassen et al. 2017, 5). The cyber threat intelligence should be an information asset and part of the risk management and cyber security management system as well.

The problem of high quality threat intelligence needs to be solved by cyber security information sharing communities where trust and maturity can be evolved (Al-Ibrahim et al. 2017; Borum et al. 2015; Sillaber et al. 2016; Zhao & White 2014). The trust and risks can be handled in cyber security information sharing communities as Kokkonen has defined (2016, 61-63).

As knowledge sharing and learning point of view the cyber security information sharing community is an autopoiesis system where new knowledge is produced whenever a person, incident handling teams or companies receive new cyber threat intelligence. The quality of the threat intelligence can be improved if the received data is enriched by the receiver, and the receiver is willing to share his own observations back.

## 2.4 Situation awareness and cyber security

The OODA loop requires that the individual person is aware of the current situation. Even though the OODA loop has been used already for long time, Endsley (1995) was one of first to create theoretical foundations for situational awareness.

In his article, Endsley (1995, 52) points out that stress, workload, complexity and automation affect the situation awareness, which will eventually affect the effectiveness of OODA loop on individual level.

Endsley (1995, 53-54) considered that in the worst case when automation fails, the users understanding how the data is processed and shown by automated systems, can quickly orientate to a new situation and keep up their situation awareness. The users passively waiting for automated alarms, might have problems to understand the root cause of the alarms and will make wrong decisions.

In cyber threat intelligence context, this means that even if it is possible to automate log management and analysis of logs to generate automated alarms, the persons handling the alarms should understand what kind of alarms the security controls are providing and what kind of anomalies they cannot detect.

A decent amount of automation to lower the complexity will affect positively the individual level to workload and stress (Endsley, 1995, 52-53). The balance between situation awareness and workload needs to be optimized so that high situation awareness can be kept without increasing workload.

El Sawy and Majchrzak in their article (2004) point out that when OODA loop is almost real time, there is a need for vigilant information systems to support decision making (Figure 7). While comparing definition of vigilant information systems (El Sawy & Majchrzak 2014, 25) to requirement specification for the situation awareness tools for blue teams (Lötjönen, 2017), the requirements for handling information from many sources i.e. data aggregation, can be considered to be the same.

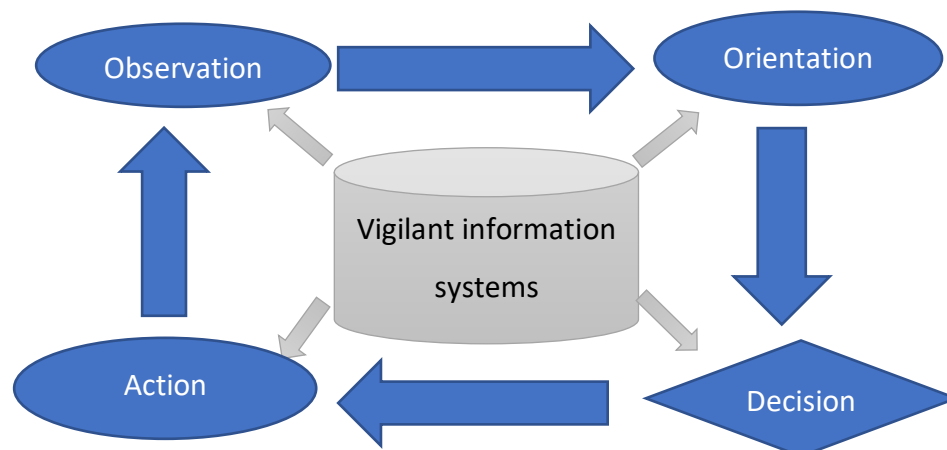


Figure 7. OODA loop with vigilant information systems

It can be understood so that when a user observes data, it takes time to process it based on autopoietic epistemology: when the first set of data is processed, the next set of data might be available before the user has managed to create a decision based on the first set of data.

In the worst case if it takes long time to solve first cyber security incident, there needs to be a system to alert the user when a more critical incident has happened, so that the user is forced to decide which of the alerts is more critical to be solved first.

Or on the other hand as Lötjönen (2017, 31) points out: when action is executed, it will change the state of the whole environment, it will not only affect the current situation awareness, but it might alter the system so that the projection of future is changed as well.

The projection of future status according to Endsley (1995, 39) is the 3<sup>rd</sup> level of situation awareness. In his work he has defined that the situation awareness can be divided into three levels as illustrated in Figure 8.

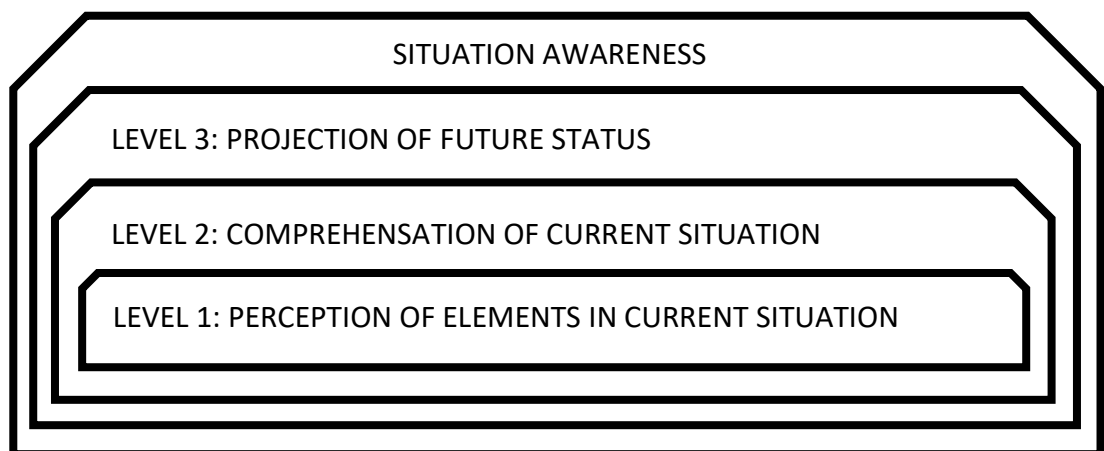


Figure 8. The situation awareness model (Endsley 1995, 35)

The perception of elements at level 1 is where correct data needs to be identified and observed from the surrounding environment (Endsley 1995, 36-37), it is the first steps to create knowledge where unfiltered data is transformed to information (see Figure 4).

Based on Koskinen (2010, 15), to gain new knowledge the observed data needs to be handled and combined with existing knowledge. In Endsley model (1995, 37), it is the

process at level 2 where the elements of the identified at level 1 are combined to create groups of identifiable patterns of information. It can be considered, that when a security control gives an alarm, the verification of the alarm's correctness will be based on the comparison of the existing cyber threat intelligence and comparison of previous alarms to the new collected information.

As Tuomi (1990, 106-107) points out knowledge is needed to be able to make intelligent choices. To be able to make intelligent choices, in OODA loop decision phase, it is required to understand what impacts the decision will have on the future. To understand what the state of the system is after each decision option, it might be important to understand before the decision is made what the wanted state is (Brehmer, 2005, 5).

For example if it is suspected that one computer might be infected by unknown malware, what is the correct way to mitigate it? Or rather, what are the steps to find, clean and verify the infected computers and harden the whole environment so that the malware will not spread and will not infect computers again. Eventually each small change is a state change in the environment as well.

When considering the malware example, it is obvious that solving that kind of case might require teamwork. In learning context teamwork is an autopoietic system, where new knowledge is produced at individual and team level.

The situation awareness at team level could be described that it is a perception of elements on level 1 and 2 at individual level and sharing it to the whole team or another team member at situation awareness level 2. At level 2, it can be assumed that both the team members or the whole team needs to have enough cyber threat intelligence to be able to handle the shared information of others to gain agreement on the current situation (Endsley, 1995, 37). The comprehension of the current situation is needed when decisions needs to be made and the projection of future status is defined.

According to Endsley (1995, 39), the team work requires that situation awareness overlaps, which is illustrated in Figure 9. The team can only work together, if there is enough information sharing until the whole team has gained comprehension of the current situation.

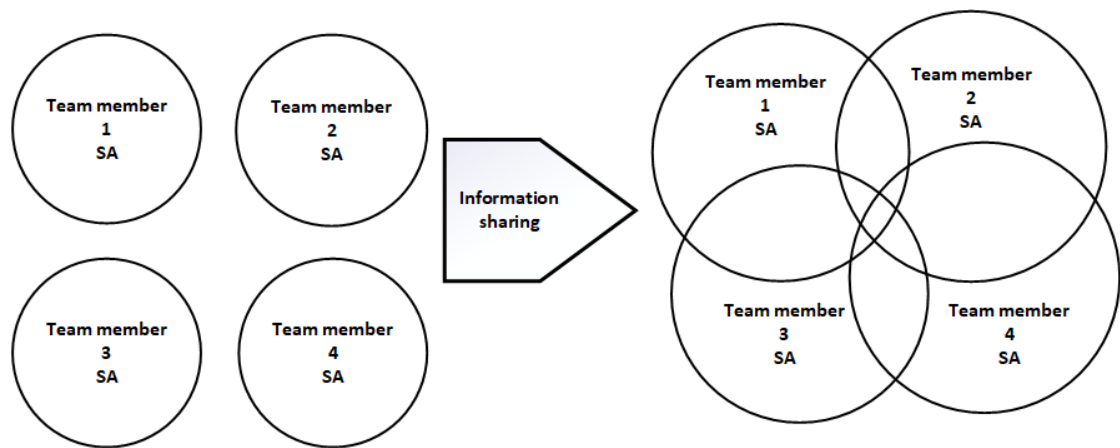


Figure 9. Team situational awareness

## 2.5 Research in human behavior and cyber security exercises

Looking up the research conducted in cyber situation awareness field, there are not so many empirical studies done (Franke & Brynielsson, 2014) and even fewer research during cyber security exercises, even though cyber security exercises should be used more to collect empirical data of cyber security phenomena (Sommestad & Hallberg, 2012).

While going through the list of articles reviewed by Franke and Brynielsson (2014) it was found out that there were not so many researches related to human behavior either.

Although it was suspected that there might have been research on how security operation centers manage cyber threat intelligence (knowledge management), how they solve cyber security incidents in distributed teams (process, human or people management) or how situation awareness is organized (processes and tools). The only conclusion is that if that kind of research is carried out, it contains only such business-critical information, which cannot be published.

One found research investigated work practices of network security professionals (Adnan et al. 2014). The authors pointed out, that even if the results look promising, but as they aimed to get respondents who work with security related tasks more than 50% of their daily work, the goal of the research was not reached. Outcome of

the research was a generic process description where incident detection, incident analysis and incident mitigation were verified to be common step by step process.

Another interesting research found was a Ph.D. Thesis by Sørensen (2012). It was an experimental study where the shared situation awareness was compared to distributed situation awareness of command and control teams. The aim was to identify how different organization structures affects communication, situation awareness and performance of the organization. In the context of cyber security exercise, Sørensen's thesis could be used to create different kinds of organization and team setups for the exercises.



### 3 Research

In the thesis, the cyber threat intelligence sharing in full live cyber security exercise between defender teams aka blue teams (BT) is studied. The aim is to understand what kind of cyber threat intelligence is collected and how it is used and shared between BTs to mitigate cyber security threats and handle the cyber security incidents. The research also focuses onto gaining insights on the tools used and how the tools are used for situation awareness during the exercise.

#### 3.1 Research methodology

As stated by Franke and Brynielsson (2014) and Sommestad and Hallberg (2012) empirical research is a suitable research method to be used in cyber security exercises. As noted in previous chapter, the cyber security exercises have not been used as a basis for academic research, hence, a multi-method approach was selected.

A case study approach was selected, due to the aim to describe what was observed in exercise context and explain cause-and-effect phenomena in the exercise (Weerakkody & Niranjala, 2015, 253).

For this purpose, cyber security exercise course at JAMK University of Applied sciences is appropriate as a case study topic, as the environment and situation of the exercise is and can be controlled by White Team (WT).

On the other hand, to get more detailed knowledge of situation awareness and cyber threat intelligence, survey research was selected as the second method to get quantitative and qualitative information on the use of different tools for situation awareness and for handling and sharing cyber threat intelligence.

#### 3.2 Collecting and sharing cyber threat intelligence

To be able to analyze the collected and shared cyber threat intelligence defined goals need to defined goals for the phenomenon in cyber security exercise context. These goals can be defined using examples based on the WT and Red Team (RT) attack blueprints.

**Goal 1:** for each cyber security incident BTs should collect source and destination information as atomic indicators

For each RT attack scenario, there was always a defined target and, in most cases, some identifiable source information as well. For example, the RT attack blueprint CSE111 (Simola & Koskinen 2018), contains detailed information that the attack target is the web application of one BT, and source is a spoofed IPv4 address from another BT IPv4 public address space.

The goal 1 for the cyber security exercise is that all BTs should try to collect correct source and target information to all detected events as detailed atomic indicators as possible. As in sharing community the quality of atomic indicators is in important role (Al-Ibrahim et al. 2017).

**Goal 2:** BTs should try to collect any tool, malware, vulnerability or attack pattern information

If the security controls are correctly configured, they can in some cases detect the used tool for the RT attack. For example, in CSE312 (Ruusupiha, 2018), the RT attack uses SQLMAP to open SQL shell used to create a new administrator account. The creation of an unknown process should be able to be detected, in this case the attack pattern including the vulnerable component and what was done can be detected.

On the other hand, Appendix 13 contains an example of CVE news. The handling of this kind information requires that BT has detected, analyzed and defined if it needs some actions or not by the BT. The CVE might or might not reveal some valid information which might be used by RT in some of their attack blueprints.

Goal 2 is to verify how well members of BTs understand the basic terminology of cyber threat intelligence focusing on what kind of cyber threat intelligence is collected by the teams.

**Goal 3:** BTs should try to identify threat actors

The WT801 scenario (Hyytiäinen, 2018) contains a definition for an imaginary threat actor. BTs need to collect the information related to all identified threat actors. They might be able to verify if the defined threat actor in WT801 (Hyytiäinen, 2018) is played by WT or RT.

In the planned scenario context, BTs should try to identify at least some information related to threat actors, their identity, motivation or goals. There is a risk that the BTs does not have either enough resources to gather and handle the cyber threat intelligence or it does not have an efficient process to do it.

**Goal 4:** BTs should share cyber threat intelligence in controlled manner

To be able to effectively mitigate cyber security incidents, the BTs should share the collected cyber threat intelligence to another BT. The aim is to detect if the members of BTs will create cyber security sharing communities as expected by Kokkonen (2016, 64) and Zhao and White (2014).

**Goal 5:** BTs should try to mitigate any threat using collected or received cyber threat intelligence

The goal is to investigate if one BT uses cyber threat intelligence received from another BT to mitigate a threat. This goal affects the planning of the time table so that there is enough time for BTs to collect, analyze and share the cyber threat intelligence. If the BTs are able to collect high quality IOCs (Goals 1 and 2) and are able to create sharing communities (Goal 4), it should be possible to verify if the shared cyber threat intelligence is used to mitigate a threat.

It will depend on the individual level how fast a BT member can process and identify the new data to get valuable information. The autopoietic epistemology defines that it is a learning process to handle the gathered data which then can be used as knowledge to make decisions when to mitigate cyber security threats. At individual level identifying and mitigating a threat requires that the OODA loop is efficient, however, if it takes a long time to process the gathered unfiltered data into meaningful information, it might not be possible to identify the atomic indicators that might be needed to make the decision on how to mitigate the threat.

In knowledge hierarchy point of view, Figure 4, the aim of goal 1, goal 2 and goal 3 is that the BT member understands the unfiltered data and managed to create a meaningful information from it e.g. IPv4 address, which then can be shared as knowledge, e.g. malicious IPv4 address, to another team member or another team.

The aim of the cyber security exercise is to train participants to detect and analyze cyber attacks, which means that participants gain valuable experience, knowledge how to detect malicious activity and intelligence how to mitigate the threat. In knowledge hierarchy point of view, Figure 4, wisdom is gained when participants can make use of knowledge and intelligence to detect unknown threat and mitigate it in an intelligent way.

### 3.3 Research questions

#### 3.3.1 Situation awareness

In this thesis, the aim is to gain information on the use of different tools of current exercise environment during cyber security exercise as situational awareness tools. The aim is to understand how an individual BT member uses different tools for situational awareness, which is a research question also identified by Lötjönen in his thesis (2017, 64).

#### 3.3.2 Cyber threat intelligence

In cyber threat intelligence context, the aim is to find out answers to following topics

Q1: How are the BTs organizing the collection, analysis and handling of cyber threat intelligence?

The aim is to have insights in what kind of organization structures and processes BTs have, to be able to design better exercises in future.

Q2: What kind of cyber threat intelligence sharing groups will be created and seen during the exercise?

As described in goal 4, there should be cyber threat intelligence sharing groups.

Q3: Does the controlled sharing of cyber threat intelligence with provided tools improve the situation awareness?

As this is one of the first empirical researches on this phenomenon area, the aim is to verify if the planned research setup works in the

research field i.e. did the planned research setup improved the situation awareness if the cyber threat intelligence was shared with provided tools?

Q4: Was the cyber threat intelligence enriched by sharing community?

As Al-Ibrahim (et al. 2017) points out, the quality of the threat intelligence is an increasing problem and if there is a need for cyber threat intelligence sharing community, it is expected that all members of the community are working towards same goal, i.e. to enrich and improve the quality of shared cyber threat intelligence.

### 3.4 Risks

To be able to get enough research data, BTs will have total freedom e.g. to organize their team structure and their processes; because of this, following risks have been identified:

R1: BTs does not have dedicated resources for handling cyber threat intelligence

BTs will get information that it is required for them to organize the collecting, handling and sharing cyber threat intelligence as a part of exercise. They will be told that all collected and shared cyber threat intelligence can be used for hardening the environments.

R2: The persons who work with cyber threat intelligence does not have enough knowledge of it

It can be assumed that all participants of the course have at least some basic understanding of cyber threat intelligence. In this case how the team handles the problem is one research question itself.

R3: There is not enough time to do collect, analyze, share and enrich the cyber threat intelligence

As the WT is controlling the game, it can be assumed that the WT will control the speed of the game so that there is enough time for cyber threat intelligence.

However, it is also a valid research result that in a live cyber security exercise BTs might not have enough resources, knowledge or time to collect, analyze and share cyber threat intelligence. The research results will affect and give hints how to organize cyber security exercises in future.

## 4 Technical cyber security exercise setup

### 4.1 Techical Cyber Security Exercise Course

The research was conducted during a cyber security exercise course in spring 2018 (Cyber Security Exercise YIIP3400, 2018; Implementation of a Cyber Exercise TTKW0320, 2018), with 80 participants divided into six teams as described in Table 1. Each team contains Master's and Bachelor's degree students. 4 master degree students were from Jyväskylä University, rest were from JAMK University of Applied Sciences. All Master's degree students are specializing to cyber security. Bachelor's degree students were from JAMK and they specialized in cyber security. Roughly 10 JAMK teachers and IT personnel were used during exercise as advisors or as members of green team (GT), to help with the technical RGCE environment.

Table 1. Exercise team setup

Team	Master degree students	Bachelor degree students	Total
White Team (WT)	8	8	16
Red Team (RT)	8	7	15
YBANK	5	8	13
YSOC	4	8	12
YSTORE	4	8	12
YSHOP	4	8	12
<b>Total</b>	<b>33</b>	<b>47</b>	<b>80</b>

Most of the Master's degree students had a long work history from different kind of information technology companies containing work history related to cyber security as well. The Bachelor's degree students were selected to this course only if they had already passed a selected set of cyber security courses.

The technical cyber security exercise has several course objectives. The aim was to train students to (Lötjönen et al. 2018)

- Participate and contribute in planning, execution and review phases of Cyber Security Exercise
- Detect and analyze a subset of cyber attacks in a partially unknown ICT-environment and assess the risk levels of the threats for business
- Analyze technical functions of the different attack vectors, identify the different threat actors and their effect on business continuity
- Handle cyber security incident using planned processes and procedures

- Plan a remediation plan and preventative measures (Assess, countermeasure and mitigation of those cyber attacks)
- Recognize, plan and execute threats, attack vectors and methods in fictional scenario
- Conduct teamwork

## 4.2 Game controlling teams

The game was controlled by the WT and the RT was the cyber conflict generation organisation. WT together with the RT created the fictional background story for the exercise. RT designed the cyber security events and the detailed technical attack blueprints based on the background scenario.

WT had the main responsibility for creating overall plans and time schedules for the exercise. WT also controlled every aspect of the exercise such as timings when and where something will happen, where as RT was the team to execute the technical cyber security attacks when requested by WT.

### 4.2.1 White Team

Figure 10 shows WT organisation structure where the numbers present the amount of persons. The aim of the organisation was to create clear communication flow between exercise management and between needed functionalities.

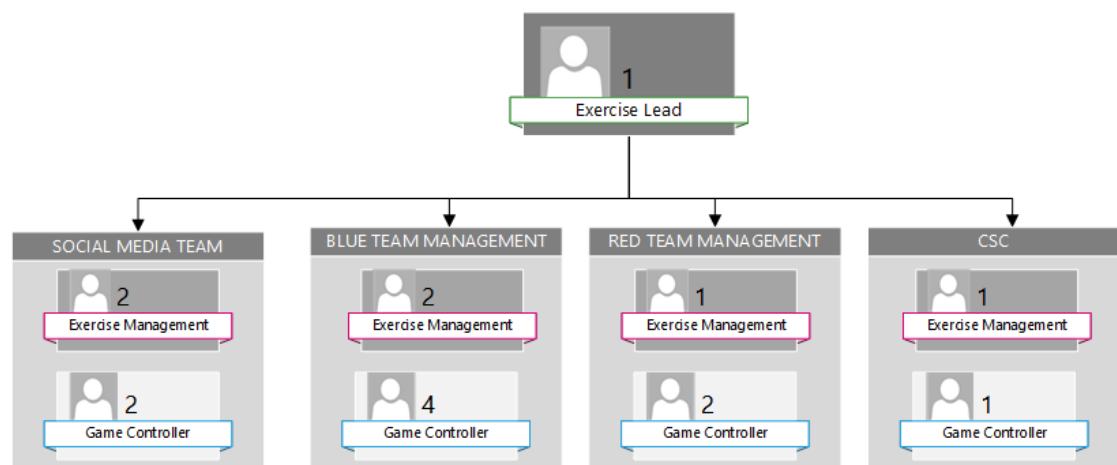


Figure 10. White Team organization structure

The role of the social media team was to handle and control the social media events of the WT and follow up different social media platforms in the exercise. During the exercise they published news and their social media topics related to the RT attack blueprints.



The role of the blue team management was to handle and control all issues related to the BTs. For example the blue team game controllers followed up how BTs reacted to the RT technical attacks. One of the main tasks was to be an employee or an customer of the BT, to verify that the technical business environment of BT was working through out the exercise. If problems were detected, they contacted BT helpdesk as an employee or the issues were discussed in social media as a customer.

RT management was to controll the exercise with the exercise lead. The main task was to control when RT can start the next attack scenario. RT management needed info from other WT teams how well blue teams were able to detect the running attack scenarios. The RT management controlled that the BTs had enough time to detect the attacks, collect the necessary information and carry out the mitigation tasks.

WT also played the role of national level cyber security center (CSC) sharing and collecting cyber threat intelligence during the exercise. The CSC team was responsible for a follow up what cyber threat intelligence was gathered and shared by BTs during the excersice. Also, CSC had own scenario related to cyber threat intelligence. The aim of the scenario was to gather information on how BTs collected, analyzed and shared the cyber threat intelligence.

#### 4.2.2 Red Team

Figure 11 shows the structure of the RT organization. In the defined game scenario, there was need for different kind of threat actors. The script kiddie type of actor, team 1, trying to get attention to themselves within any means available. The anonymous will not try to hide; the aim was that their attack scenarios should be easily detected by BTs, and they were used to generate distractions to hide other ongoing technical attacks of other two teams.

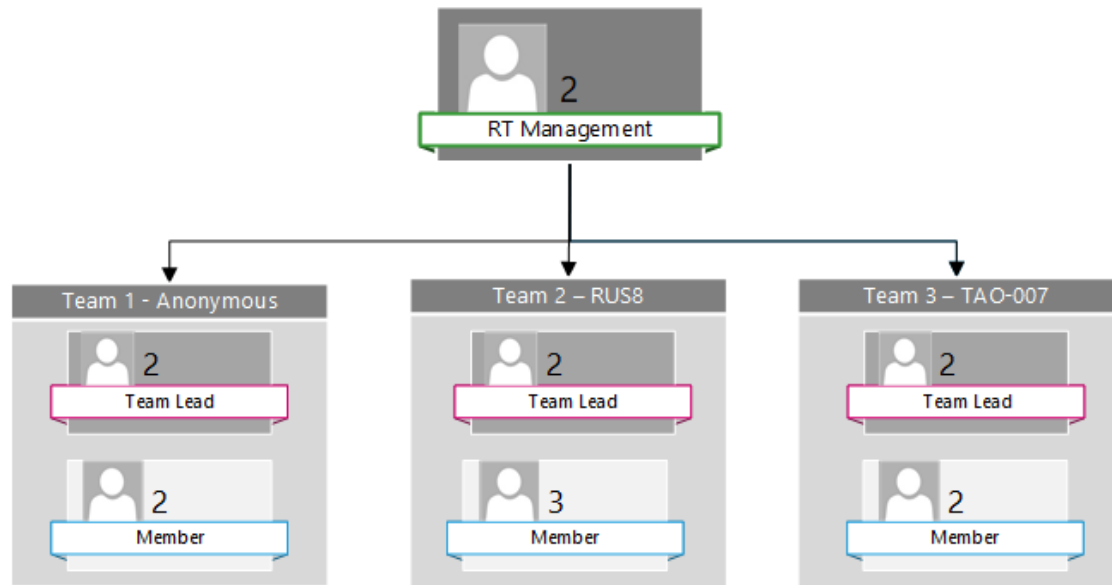


Figure 11. RT organization structure

Team 2, RUS8, represent a crime as a service threat actor. They had all the tools and knowledge available to most paying customers, i.e. for the Team 3 (TAO-007). Team 3 was a national level ATP-group, which wanted to affect in political and economical way to the overall scenario. For example, team 2 was responsible to get a persistent command and control channel to BTs technical environment, which was then used by Team 3 for advanced attacks such as getting data out from databases.

### 4.3 Blue Teams

The four BTs (YBANK, YSOC, YSTORE and YSHOP) had business relations as described in Figure 12. YSTORE and YSHOP are web shops selling items to consumer market. They were competitors as they tried to focus on the same market area with the same kind of item portfolio. YBANK was a banking company and it offered online and traditional banking services to private and corporate customers like YSTORE and YSHOP. YSTORE and YSHOP used YBANK provided online payment services and credit card payment services.

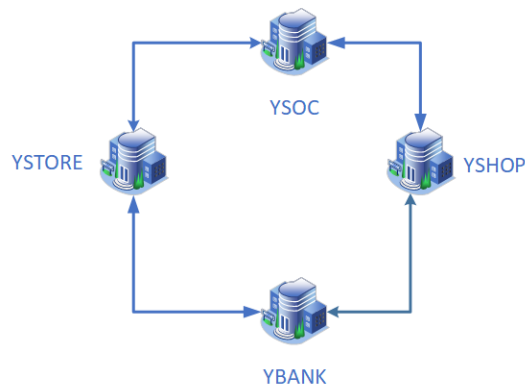


Figure 12. Exercise company relationships

YSOC was a private security operation center providing information security solutions to financial institutions, commercial companies and government agencies (YSOC Blue Team 2018, 2). YSOC had business relations between YSTORE and YSHOP. YSOC provided e.g. centralized log-monitoring and analyzing services, secure DNS services and consultation for investigation and mitigation of cyber security incidents.

The cyber threat intelligence sharing community for the exercise is defined in Figure 13. CSC was sharing and collecting cyber threat intelligence during the exercise. CSC was sharing information with all companies.

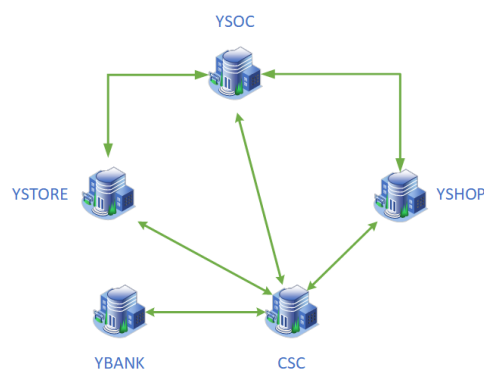


Figure 13. Cyber threat intelligence sharing community

YBANK had their own security operation center, so they were sharing directly with CSC. As YSOC provided solutions to YSTORE and YSHOP, they could share cyber threat intelligence between them as well.

In this scenario with YSTORE and YSHOP competitors, YSOC needed to consider what kind of threat intelligence they could use when resolving YSTORE and YSHOP cyber

security incidents. Were they allowed to use threat intelligence received from YSTORE to resolve YSHOP security incidents? YSTORE and YSHOP should have agreed with YSOC how to handle the shared information and how to classify the private and public information correctly.

All BTs had time to get used to their own infrastructure. The first step was to analyze the team's own infrastructure and create business models, business plans and risk management plans. The second step was to create an organization structure to the team and define communication and incident management plan for the team. Figure 14 shows as an example of YSHOP organization structure (YSHOP Blue Team, 2018), where management was run by Master's degree students and the technical team was filled with Bachelor's degree students.

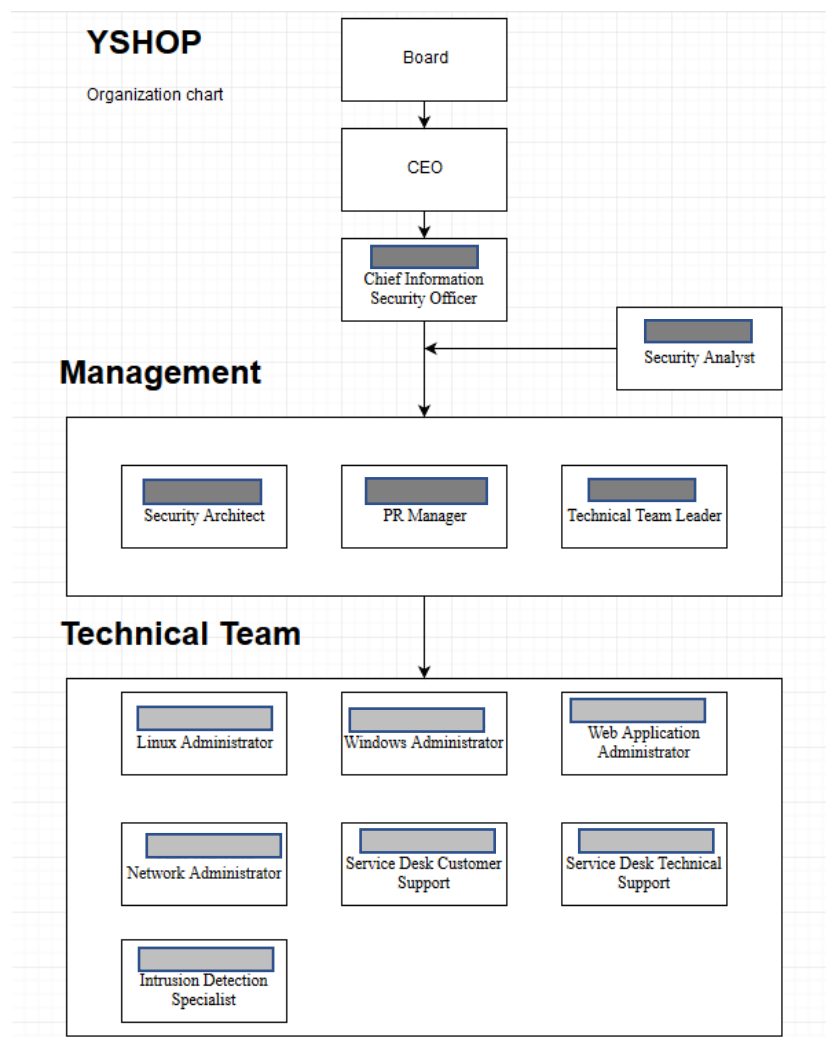


Figure 14. YSHOP organization structure (YSHOP Blue Team, 2018)

The major challenge for BTs was to have a communication plan, incident management process and incident response management organization as most of the Bachelor's degree students had no work experience of them. The communication plan should describe how the organization would be communicating during the exercise including internal and external communication, so that all members of the team would have enough information for maintaining the situation awareness during the exercise.

Figure 15 shows the YSTORE and their defined organization structure with the main communication flow. YSTORE had also defined who the main responsible to communicate with YSOC was and what kinds of roles were expected from WT during the exercise. (YSTORE Blue Team, 2018)

In addition, WT defined that whenever BT has a need to communicate for example to governmental authority (e.g. police), business partner (e.g. network operator) or to an employee (who is not in their team), BT should contact WT and WT play the needed.

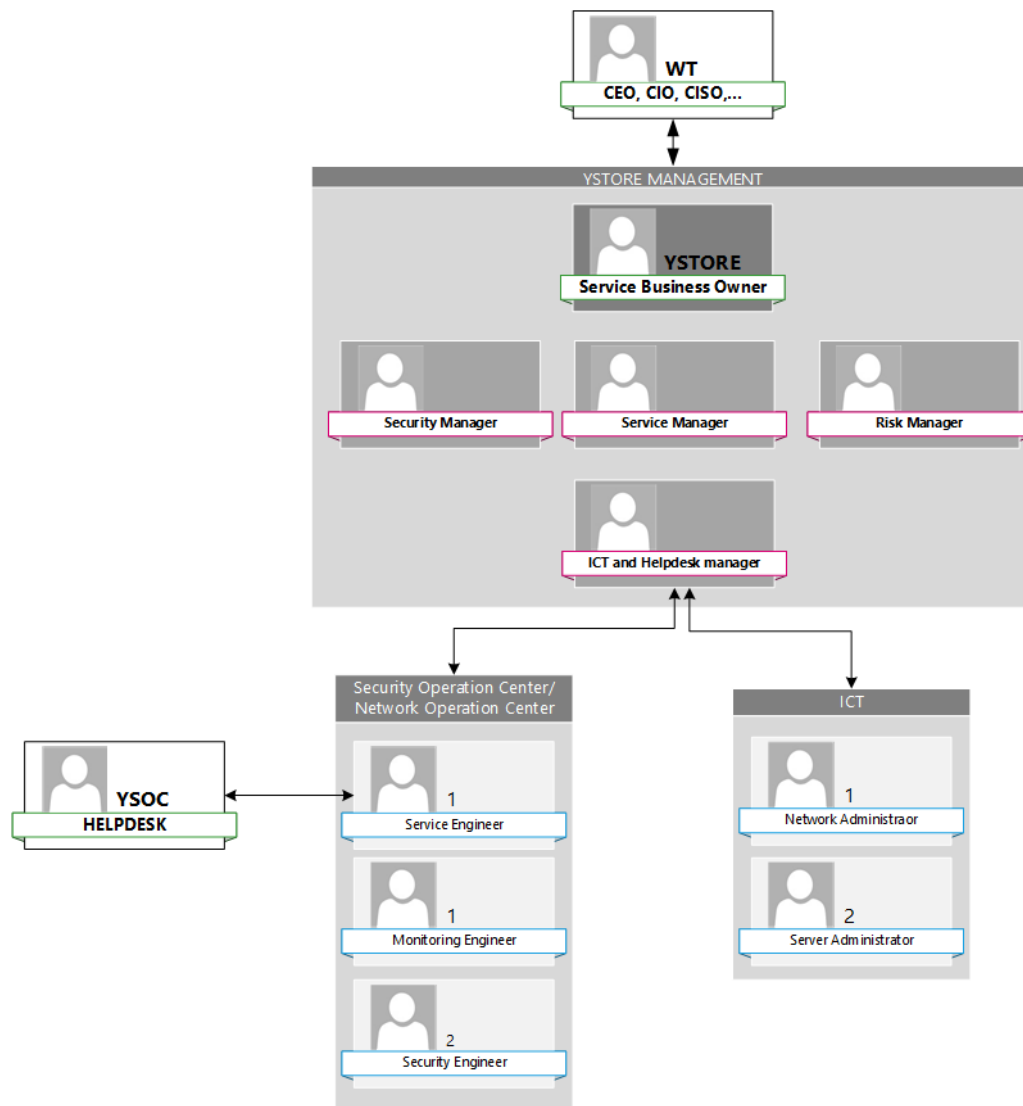


Figure 15. YSTORE organization with main communication flow (YSTORE Blue Team, 2018)

YSOC prepared a very detailed incident management process (see process figure in Appendix 3), because they had business agreements with YSHOP and YSTORE. YSOC had also a set of security controls, which generated security alerts as incidents directly to their incident management system.

#### 4.4 Exercise environment

The Realistic Global Cyber Range (RGCE) of JYVSECTEC in JAMK, can be considered as mini internet, which contains realistic functions e.g. realistic name service architecture, controlled update and software repositories for various operating systems and several industry specific organizations with a complete set of business

services. To mimic the real internet, RGCE has several public services as well like news site, social media platforms and email services. (Vatanen et al. 2017, 3-6)

As the RGCE is an isolated environment it is a safe environment to test different kinds of cyber-attack scenarios to simulate threat actor behavior, their tactics, techniques and procedures (Vatanen et al. 2017, 4).

For communication, a chat application was used so that there was a separate chat room (channel) for WT to manage the whole exercise and separated chat rooms for each other team which the team can use it for private discussions, but also to communicate with WT privately.

To support making notes during the exercise, a Wiki based application (Collab) was provided for each team. From the chat application, it was possible with simple commands to create wiki pages when something was needed to be documented for further use.

BTs could use e-mails or provided VoIP phones to communicate to another BT. However, all VoIP communication should be documented to Wiki, so that it could be used when analyzing the exercise.

BTs were also encouraged to use VoIP to communicate with WT, when other communication methods did not reach the needed correct contacts. In addition, WT could use VoIP to contact BT as a customer, an employee, a business partner, a journalist etc., when it was expedient to give a hint for the BT that there might be an ongoing RT attack.

#### 4.5 MISP – Open Source Threat Intelligence Platform

As a part of the research the aim was to investigate how cyber threat intelligence is collected, analyzed and shared, there was a need to select appropriate tool for BTs. One of the choices: MISP had already presented by Lötjönen on his Master's thesis (2017, 41-42) as also shown on Figure 1. One of first MISP pilot studies at JAMK was made by the author (Hyytiäinen et al., 2015).

MISP is an open source threat intelligence platform currently community-driven project lead by the community of users. The project itself is co-financed by the

European Union and the lead developers works for CIRCL (Computer Incident Response Center Luxembourg) (MISP Project 2018).

Several other tools were considered however, when following requirements were considered, only MISP fulfilled them all (not in particular order):

- 1) Open source
- 2) User base should be large enough
- 3) Software should be frequently updated
- 4) Fast responsive support community
- 5) Solid and stable performance, so that users can use it
- 6) Easy to configure: users, user roles, organizations
- 7) Real-time replication between servers
- 8) As easy to use as the Wiki platform and the incident management system BTs has
- 9) Tool should use the common terminology of cyber threat intelligence model (Mavroeidis & Bromander 2017)
- 10) Support for different kinds of IOCs

The support for the IOC's is one of the strengths and at the same time one of the weakness points of MISP. A cyber security incident or observation is entered to MISP as an event. An Event is a collection of attributes, IOCs. (MISP Project 2018, 27-30)

When entering an attribute, user needs to select category of the attribute and then more detailed type for it. Currently there are 16 categories and 134 different types (MISP Project 2018, 158-171). The project has documentation what category and type combination are allowed, however, an optimal way to the end user of MISP is not currently shown. As this was noticed during the preparation time, some example events were made in MISP which were visible to all users of MISP (for example, Appendix 10 and Appendix 11).

When entering attributes, MISP also supports objects and templates. For the exercise, a small set of default objects were enabled (Figure 16). The default objects are designed so that they give a set of default attributes which describes the object in a meaningful way.



Select Object Category
Bank-account
Credential
Ddos
Email
File
Microblog
Person
Url
Victim
Vulnerability
Back to categories
Cancel

Figure 16. Small set of MISP object categories

The objects are designed so that they contain a minimal number of mandatory attributes (Figure 17) and help text aiding the user to fill in the needed data.

#### Add Ddos Object

Object Template	Ddos v6					
Description	DDoS object describes a current DDoS activity from a specific or/and to a specific target. Type of DDoS can be attached to the object as a taxonomy					
Requirements	Required one of: ip-dst, ip-src, domain-dst					
Meta category	Network					
Distribution	Inherit event					
Comment	<input type="text"/>					

Save	Name :: type	Description	Category	Value	IDS	Disable Correlation
<input type="checkbox"/>	Domain-dst :: domain	Destination domain (victim)	Network activity	<input type="text"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Ip-dst :: ip-dst	Destination IP (victim)	Network activity	<input type="text"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Ip-src :: ip-src	IP address originating the attack	Network activity	<input type="text"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Total-bps :: counter	Bits per second	Other	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Text :: text	Description of the DDoS	Other	<input type="text"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Dst-port :: port	Destination port of the attack	Network activity	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Src-port :: port	Port originating the attack	Network activity	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figure 17. MISP DDOS object template

The original plan was to use MISP so that each BT would have their own MISP server. That setup would place an opportunity for RT to try to compromise the integrity, availability and confidentiality of the cyber threat intelligence on the MISP server.

That setup was ignored, as the primary research goal was to identify what kind of cyber threat intelligence was collected, analyzed and shared. It was considered that if the MISP server is compromised, BTs might not trust the shared data and eventually the MISP might not be used at all during the exercise. The final setup contained only one MISP server, which was stated to be out of the game system.

During the preparation phase, all members of BTs were given basic training of MISP. There were 3 test sessions, which were used to train out of game communication, out of game tools like the chat, wiki platform and MISP.

The author was prepared for giving advanced training of MISP to the users selected by BTs to have the responsibility to collect, analyze and share cyber threat intelligence. Only one member of YSOC wanted to have advanced MISP training, which was held one day before the exercise.

As a side note, while preparing to the exercise the author found one bug in MISP, one possible bug, which is not yet confirmed and created five improvement proposals for the MISP project.

## 4.6 Exercise events

Table 2 contains the list of events which should have been identified by the BTs. RT had their own attack scenarios targeting BTs. WT had a set of events that were not targeted to one organization rather to all of them, so that the collecting, analyzing and sharing cyber threat intelligence could be investigated.

Table 2. Exercise events

Event	YBANK	YSHOP	YSOC	YSTORE	Cyber threat intelligence	Appendix
RT attack scenario	15	16	13	15	All	
ATP simulator	1	1	1	1	Indicators of compromise	
MISP shared events	11	13	12	13	Identity, atomic indicators, infrastructure, malware	10,11
CNN news	4	4	4	4	Identity, vulnerabilities	12,13
Telia OSINT emails	7	1	6	1	Vulnerabilities, infrastructure	14
Youtube.com	1	0	0	0	Identity, target	
pastebin.com	4	4	4	4	Malware, indicators of compromise	15
gitlab.com	1	1	1	1	Identity, target, tools	16
imgr.com	5	5	6	5	Identity, target, motivation	17
Suspicious twitter accounts	3	3	3	3	Identity, target, motivation	18
Suspicious bank accounts	1	0	0	0	Identity	19
<b>Total events</b>	<b>52</b>	<b>45</b>	<b>48</b>	<b>43</b>		

RT attacks contained e.g. different kinds of denial of service attacks, email phishing attacks and email malware distribution attacks. RT also used a known vulnerability in WordPress to gain access to the intranet and a known vulnerability in the web shop application used by YSTORE and YSHOP to get access to customer information.

As WT had access to employee workstations, it was considered that a simple tool, in this case Nextron Systems APT Simulator (White Team, 2018, 18) was be used to simulate adversary activities. For example, it could be used to create noise to distract blue teams when needed.

While investigating the open source threat intelligence feeds in MISP, the appendices 4-9 were created based on the idea of those feeds. Examples of the data distributed in the game environment are on the described appendix pages.

While preparing for the exercise, it was noticed that the YBANK contained some user accounts from the previous exercise (2017). The account was used for a money laundry operation, so some threat intelligence was published early on during the preparation time (see Appendix 10 and Appendix 19).

#### 4.7 Processes and tools in the exercise

WT decided early on that it is not WT's role to define what kind of organization structure each BT will have or what kind of business processes BTs will create. The only requirement was that BTs need to have efficient communication process with WT.

During the planning phase of the exercise, there was enough time to learn to use the provided tools. In the planning phase, there was a two-days training session where teams were learning how to use their own environment but also how to use out of game tools and communication systems i.e. chat tools, wiki platform and MISP.

Based on the two-days training session, it was also requested that two extra training sessions were required to learn the efficient processes not only to communicate with WT but to learn how to use the provided tools in an efficient way.

## 5 Research results

This chapter provides an analysis of the exercise. The aim is not to focus on how well BTs detected and mitigate the threats, rather to analyze the situation awareness of the BTs and to understand what kind of cyber threat intelligence was collected, how it was used and shared during the exercise. The aim was to identify how the individuals, or the organizations are functioning in cyber exercise while maintaining the situation awareness.

### 5.1 Survey information

Appendix 1 survey was sent to all employees of each BT (n=49), the results was received from 37 persons as shown in Table 3.

Table 3. Survey 1 respond rate

Survey 1	Surveys send	Responds received
YBANK	13	10
YSOC	12	8
YSTORE	12	11
YSHOP	12	8
<b>Total</b>	<b>49</b>	<b>37</b>

Appendix 2 survey was sent to all employees of each BT, who logged into MISP during the exercise and used it even for a short period of time; results was received from 11 persons as shown in Table 4.

Table 4. Survey 2 respond rate

Survey 2	Surveys send	Responds received
YBANK	4	2
YSOC	4	2
YSTORE	4	3
YSHOP	4	4
<b>Total</b>	<b>16</b>	<b>11</b>

## 5.2 Event detection

The exercise was executed during two days: on day 1 from 10:00 till 17:30 and on day 2 from 9:00 till 12:00. The aim was that during the day one the speed of the exercise was slower so that BTs could orientate to the exercise and do adjustments for their processes if needed. The focus of the day one was on detecting malicious activity and to collect and analyze cyber threat intelligence as it was planned so that any collected cyber threat intelligence could be used when BTs were permitted to do hardenings to their environments after the day one. For example, if a BT detected malicious IPv4 addresses or domain names, they could use that information to detect or even block the traffic in security controls such as firewalls.

It can be seen on Table 5, that in the second day, the schedule was much tighter and in much shorter time almost the same number of RT events were executed. Some of the RT events was planned so that they were already executed against some BT on day one but executed against another BT on day two. As RT was learning by doing, the time for preparations and executing the attacks on day 2 was much shorter than on day 1.

Table 5. Events in the exercise split by exercise day

BT	Exercise day 1 (9:00-17:30)		Exercise day 2 (9:00-12:00)	
	RT events	WT events	RT events	WT events
YBANK	7	7	8	9
YSHOP	10	5	6	8
YSOC	8	6	5	9
YSTORE	9	5	6	8
<b>TOTAL</b>	<b>34</b>	<b>23</b>	<b>24</b>	<b>36</b>

Table 6 is filled with the data based on the MISP events, created wiki pages and based on the tickets found in the incident management system of the BTs. It is obvious that only one of the BT has focused on or had dedicated resources to collect cyber threat intelligence, which was related to threat intelligence scenarios played by the WT.

Table 6. Detected events

Event	YBANK	YSHOP	YSOC	YSTORE	Detected cyber threat intelligence
RT attack scenario	8	8	7	7	
ATP simulator	0	0	0	1	malware
MISP shared events	0	1	1	0	Infrastructure
CNN news	0	0	1	2	Identity, vulnerabilities
Telia OSINT emails	2	1	1	1	Vulnerabilities, infrastructure
youtube.com	0	0	1	0	Target
pastebin.com	0	0	4	0	Malware
gitlab.com	0	0	1	0	Tools
imgr.com	0	0	6	0	Identity, target
Suspicious twitter accounts	0	0	2	0	Identity, target, motivation
Suspicious bank accounts	0	0	0	0	-
<b>Total detected events</b>	<b>10</b>	<b>10</b>	<b>24</b>	<b>11</b>	

On the other hand, the survey question (Appendix 1, question 6) results are show that 86.5% of the responders considered that they were collecting cyber threat intelligence (Table 7). Based on the collected data, it cannot be known if BTs detected the data but did not analyze and store it for future use.

Table 7. Did you collect cyber threat intelligence during the exercise?

	N	%	YBANK	YSHOP	YSOC	YSTORE
Yes	32	86.5%	10	7	6	9
No	5	13.5%	0	1	2	2

### 5.3 Situation awareness

Based on the survey question 4 (Table 8) in Appendix 1, there were totally 10 different kinds of methods used for maintaining situation awareness. The discussion within team - either spoken or in chat - can be considered the most used method and it shows that employees are discussing and sharing information between each other.

Table 8. What tools did you use for maintaining your situation awareness?

	N	%	YBANK	YSHOP	YSOC	YSTORE
Discussion in team	36	97.3%	10	8	7	11
Incident management tools	34	91.89%	9	7	8	10
Social media	30	81.08%	10	7	4	9
Logs or log management systems	28	75.68%	10	5	8	5
Discussion in chat	26	70.27%	9	7	5	5
MISP	11	29.73%	4	2	3	2
phone	3	8.10%	0	0	2	0
email	2	5.41%	0	0	1	1
wiki	1	2.7%	0	0	0	1
monitoring tools	1	2.7%	0	0	0	1

In Table 8 can also be seen that participants were using the provided incident management tools with logs or log management systems to maintain their situation awareness as well. By looking up the data in the incident management systems, Table 9, it can be seen that each BT was able also handle their incidents according to their processes during the exercise. Each team also used the provided wiki to handle incidents. Those events are the ones they considered important to report to WT as well.

Table 9. Tickets in incident management systems

Team	Open tickets	Closed tickets	Total amount tickets	Wiki events
YBANK	3	33	36	25
YSHOP	9	41	55	23
YSOC	21	54	75	51
YSTORE	7	12	19	27

As BTs can be compared, the amount of YSTORE tickets seems to be very low compared to any other BTs. It can be only assumed that YSOC handle most of the cases related to YSTORE and there were not so many things to do by themselves. Although in that case, they should have had enough time to collect cyber threat intelligence from the game environment.

The most important situation awareness tools can be seen in Table 10. The results for Appendix 1, question 3 were weighted so that the most important tool was given weight 7 and the least important 1 and each team contained the same number of employees, 10 in this case.



Table 10. Weighted situation awareness tools used by BT

Tool	YBANK	YSHOP	YSOC	YSTORE	TOTAL
Logs or log management tools	48	43	58	48	197
Discussion in team	49	41	46	46	182
Incident management tools	46	38	50	46	180
Discussion in chat	47	44	44	39	174
MISP	41	46	39	45	171
Social media	32	39	34	42	147
phone	4	0	15	0	19
email	0	0	9	2	11
wiki	0	0	0	5	5
monitoring	0	0	0	5	5

It could be considered that on level 1 of Endsley (1995, 36) situation awareness model, the logs and log management tools are the important ones on the individual level when creating perception of the elements in a current situation, the detailed pieces of data gathered from different systems.

Monitoring can be also considered one of the basic methods to observe current situation as well. From a respondent's point of view, it can be considered that the respondents considered logs and log management tools to contain monitoring functionality as well as only one of the respondents mentioned monitoring as another meaningful method.

On team level situation awareness level 2 (Endsley 1995, 37), the discussion in team, incident management tools and discussion in chat were the tools and methods to create comprehension of the current situation.

In Table 10, the MISP and social media represent the information that was received or collected from outside world. It can be considered that it was used for creating perception of the current situation of the whole exercise world at level 1 situation awareness (Endsley 1995, 36).

One question remains if Table 10 and Table 6 are compared, what information was seen on the social media, however, the detection itself was not logged or the information was not captured and stored for future use?

YSOC, YSTORE and YSHOP had incident management systems tightly coupled so that the incident management handler in YSOC could directly send a ticket, question or

answer from their own incident management system to YSTORE or YSHOP and vice versa. As information was needed to be changed between BTs, it can be concluded that incident management tools, MISP, email, phone were used at level 2 situation awareness level when creating comprehension of the current situation between BTs.

There were 79 phone calls during the exercise (Table 11; White Team, 2018), 34 between YSOC, YSHOP and YSTORE. The question arises if YSOC thought those 34 phone calls were important for maintaining situation awareness, why did YSHOP and YSTORE not? There was no documentation received from BTs what kind of information was shared during the phone calls.

Table 11. Phone call statistics from the exercise (White Team, 2018)

	To:	WT	YBANK	YSHOP	YSOC	YSTORE	TOTAL
<b>From:</b>							
<b>RT</b>			2				2
<b>WT</b>			4	4	2	2	12
<b>YBANK</b>		2		2	2		6
<b>YSHOP</b>		1	3	1	5		10
<b>YSOC</b>		11	2	15		17	45
<b>YSTORE</b>		2			2		4
<b>TOTAL</b>		16	11	22	11	19	79

## 5.4 Cyber threat intelligence

To be able to collect and understand the cyber threat intelligence, basic knowledge of different terms is required. It was assumed that the employees collecting cyber threat intelligence or those employees using MISP would have decent knowledge of these terms. In Figure 18 there is the data of the second survey, Appendix 2, question 13, the respondents were able to choose values between 1-5 (1: don't understand at all, 5: I'm an expert on this topic).

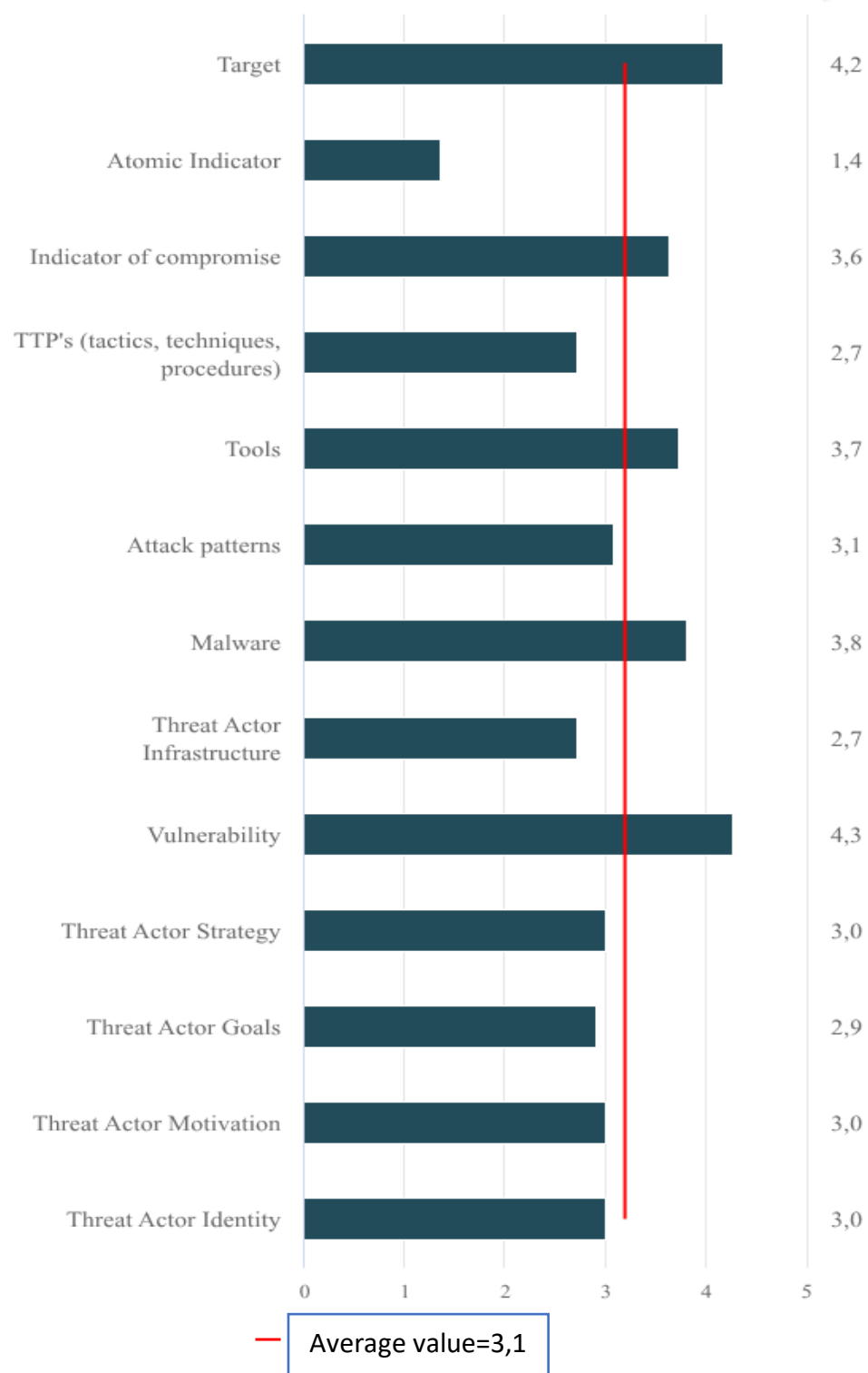


Figure 18. Appendix 2, question 13 results

Based on Figure 18, it seems that the respondents of survey 2 have difficulties to understand the difference between atomic indicator and indicators of compromise,

which will eventually have a big impact to what kind of cyber threat intelligence was shared between BTs. Nevertheless, the overall understanding of different terms seemed to be at a good level.

#### 5.4.1 Collecting cyber threat intelligence

With survey 1, question 6 (Table 12) and 9 (Table 13), the aim was to identify if the members of the BTs are collecting or if they identified and knew that their company is collecting the cyber threat intelligence.

Table 12. Did you collect cyber threat intelligence during exercise?

	N	%	YBANK	YSHOP	YSOC	YSTORE
Yes	32	87%	10	7	6	9
No	5	13%	0	1	2	2

Table 13. Did your company collect cyber threat intelligence during exercise?

	N	%	YBANK	YSHOP	YSOC	YSTORE
Yes	34	92%	8	8	8	10
No	0	0%	0	0	0	0
Don't know	3	8%	2	0	0	1

Based on Table 12 and Table 13, all members of the YSOC and YSHOP knew that the whole team is collecting cyber threat intelligence, even those who considered that they were not involved in collecting it them self.

On the other hand, only one member of the YSTORE was not sure whether their company collected any cyber threat intelligence at all. Either it is a failure of team organization and communication or the concept of cyber threat intelligence is not clear to that member.

Two members of YBANK answered "Don't know". This is slightly problematic as it can be assumed that in a normal case in the Table 13, there should be the same amount of yes answers or more yes answers than in Table 12. Either one is not collecting cyber threat intelligence, but one knows that someone is doing it in the team. What might cause "Don't know" answer? Is it because one is collecting, but one's team members do not know that one is?

In survey 2, question 2 (Figure 19), the choice 0-5 was given to respondents to define how difficult it was to collect cyber threat intelligence during the exercise, the mean value is 2.45 (scale 0: very easy, 5: very hard).

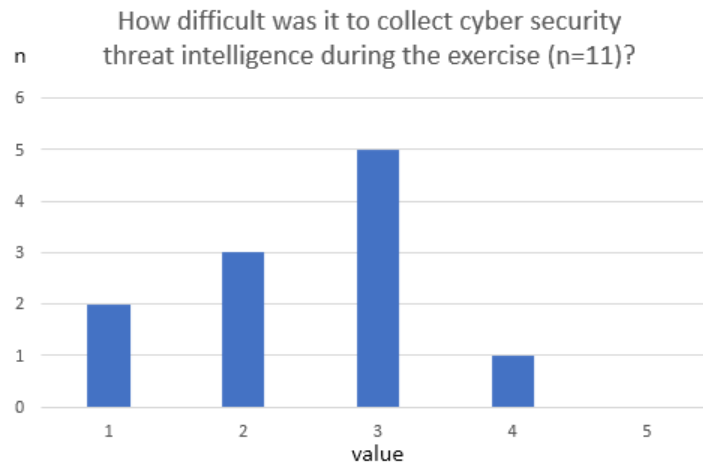


Figure 19. How difficult was it to collect cyber threat intelligence during the exercise?

Therefore, even if the collecting the cyber threat intelligence was considered somewhat easy, the amount of collected cyber threat intelligence should have been much more than what was found in the game environment.

There are examples of threat intelligence, for e.g. a suspicious or malicious IPv4 addresses detected by YSTORE. The information was not shared using provided the tools, MISP in this case, although it was stored into YSTORE incident management system (Figure 20) and stored to a wiki page as well.



Figure 20. YSTORE detected malicious IPv4 address

### 5.4.2 Analyzing cyber threat intelligence

The aim of the survey 2 question 3: “How difficult was it to analyze the collected cyber threat intelligence during exercise?” was to compare with the survey 2 question 2, if the respondents considered that the data they collected was understandable and easy to analyze. Figure 21, the choice 0-5 was given to respondents to define how difficult it was to analyze cyber threat intelligence during the exercise, the mean value being 3.09 (scale 0: very easy, 5: very hard). It seems that the respondents managed to collect some data and data was not too difficult to analyze.

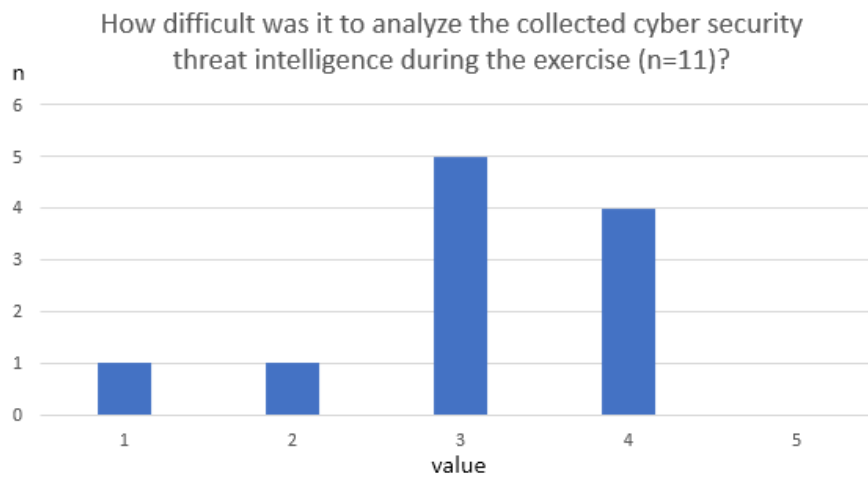


Figure 21. How difficult was it to analyze the collected cyber threat intelligence during the exercise?

All respondents to the survey 2 (Appendix 2) question 4, discussed with their own team member when collecting and analyzing the cyber threat intelligence, however, only one discussed it with someone else, from another BT, survey 2 question 5 (Table 14).

Table 14. Survey 2, data of questions 4 and 5

Question	Yes	No
4. Did you discuss the collected cyber threat intelligence with your team member when analyzing it?	11	0
5. Did you discuss with someone else the collected cyber threat intelligence when analyzing it? I.e. with someone else in another company?	1	10

It was thought that during the exercise the threat analysts will create their own group of experts sharing and discussing the collected and shared cyber threat intelligence, however, based on the survey 2 questions 4-7, it is not so obvious (Table 14 and Table 15). Even though there might be small group of three people but based on the data collected from the game environment, the existence of this group could not be verified.

Table 15. Survey 2, data of questions 6 and 7

Question	Yes	No
6. When you shared cyber threat intelligence to another company, did you get any feedback or questions about it from their experts?	3	8
7. When you received cyber threat intelligence from another company, did you give any feedback or questions about it to their experts?	3	8

#### 5.4.3 Sharing cyber threat intelligence

The aim of survey 1 question 9 was to give more information how the teams are handling the cyber threat intelligence. Table 16 supports the fact that the teams communicated during the exercise and the cyber threat intelligence was shared inside the team. It was assumed that even though a member might not be involved directly to collecting cyber threat intelligence (Table 12), he/she was involved in sharing and handling it and knew what other team members are doing.

Table 16. Did you share cyber threat intelligence during exercise in your company to your co-workers?

	N	%	YBANK	YSHOP	YSOC	YSTORE
Yes	36	97%	10	7	8	11
No	1	3%	0	1	0	0

The aim of the survey 1 question 10 (Table 17) was to verify that the blue teams had planned who was responsible to share cyber threat intelligence to another BTs. YSOC is an exception here, as they had customer relationships to YSTORE and YSHOP, so eventually more team members were required to handle those business relationships. Based on Table 17, it can be verified that the sharing was a controlled by the teams and it was done just by a small set of employees.

Table 17. Did you share cyber threat intelligence during exercise to other companies?

	N	%	YBANK	YSHOP	YSOC	YSTORE
Yes	12	32%	2	2	5	3
No	25	68%	8	6	3	8

Even though the BTs were small teams, there seems to be lack of communication or lack of knowledge what each team member was doing during exercise. Based on the survey 1 question 11 (Table 18), it can be assumed that even though there was communication in the teams (Table 8), in some teams all members did not know what the other member was doing. In YBANK 40% and YSHOP 38%, seems quite high, but as the respond rate is not 100% the results might be for YSOC 0%-33%, for other teams 17%-58%.

Table 18. Did your company shared cyber threat intelligence during exercise to other companies?

	N	%	YBANK	YSHOP	YSOC	YSTORE
Yes	26	70%	5	5	8	8
No	2	5%	1	0	0	1
Don't know	9	25%	4	3	0	2

With question 12 in survey 1, the purpose was to compare how the tools used for situation awareness were used for sharing cyber threat intelligence to other companies. It is interesting to see in Table 19, that phone was used more often than email or incident response tools, when knowing the fact that the YSOC shared information using incident response tools with YSHOP and YSTORE and phone was not very highly rated as a situation awareness tool (Table 10).

Table 19. What tools you or your company used to share cyber threat intelligence to other companies?

	YBANK	YSHOP	YSOC	YSTORE	TOTAL
MISP	5	5	7	6	23
Phone	3	1	9	8	21
Email	0	2	5	6	13
Incident response tools	4	1	6	2	13
Discussion in psi chat	3	0	1	4	8
Don't know	2	4	0	2	8



It was considered whether or not to include social media as a tool to share cyber threat intelligence, however, there were not so many use cases where it could be useful. All BTs could use extranet to provide useful info for their customers.

#### 5.4.4 Receiving cyber threat intelligence

When companies and team members tried to keep their situation awareness high enough to be able to detect the threats, not only the own collected but also the received cyber threat intelligence was in important role as well. If the received cyber threat intelligence was good enough, it might help the receiver BT to detect and mitigate the threat completely.

The results in Table 20 for survey 1, question 13, shows that in most of the team's the members were knew that cyber threat intelligence was received from other teams. However, as the YSOC had business relations to YSHOP and YSTORE, it can be seen based on Table 18 and Table 20 that they shared more cyber threat intelligence than received it as it was expected.

Table 20. Did your company receive any cyber threat intelligence from other companies during the exercise?

	N	%	YBANK	YSHOP	YSOC	YSTORE
Yes	29	78%	7	7	5	10
No	1	3%	0	0	1	0
Don't know	7	19%	3	1	2	1

To understand how different tools were used during the exercise, teams were able to decide how each tool would be used and freely use them during the exercise. In Table 21 are the results for survey 1 question 14. Comparing to survey 1 question 12 (Table 19), the tools used for sharing and tools used for receiving were quite different.

Table 21. What tools did your company use to receive cyber threat intelligence from other companies?

	YBANK	YSHOP	YSOC	YSTORE	TOTAL
Email	3	6	6	9	24
MISP	5	5	7	5	22
Social media	5	4	4	9	22
Phone	2	3	7	8	20
Incident response tools	3	4	6	2	15
Don't know	1	2	0	1	4
RT call with phone	1	0	0	0	1

Phone and email seem to be important tools for communication and sharing information. Based on the results of survey 1 question 12 and 14, it is interesting to notice that email and phone were undervalued as a tool to maintaining situation awareness as seen on survey 1 question 3 (Table 8).

The only conclusion is that to survey 1 question 3, BT members responded correctly as their own point of view what tools were important to maintain their own situation awareness on level 1 situation awareness level (Endsley, 1995, 36-37). However, to survey 1 questions 12 and 14 they answered all tools they used themselves or knew the tools that were used by other team members to share and receive cyber threat intelligence.

Even though the social media was not considered as a tool for sharing cyber threat intelligence, it was seen as one tool to receive that information. During the exercise, there was a high amount of Twitter tweets and a good amount of CNN news. For example, during some attacks, customers, CNN or RT posted data to Twitter or news, to give a hint to BT that something is going on (Figure 22). In this case, the importance of social media as a situation awareness tool can be identified as level 1 situation awareness level (Endsley, 1995, 36-37) as in Figure 22 all BTs got information that some RT attack is going on against YBANK.



Figure 22. CNN news hint that something is going on

#### 5.4.5 Sharing and receiving cyber threat intelligence with MISP

As seen in Table 19 and Table 21, MISP was identified as a tool to share and receive cyber threat intelligence. With answers to survey 1 questions 19 and 20 (Table 22 and Table 23), when comparing to survey 1 questions 9 and 10 (Table 17 and Table 18), it can be also seen that team members might not know what other member was doing during the exercise so in this case they were not sure whether MISP was used.

Table 22. Did your company share IOC data using MISP?

	N	%	YBANK	YSHOP	YSOC	YSTORE
Yes	22	59%	3	7	6	6
No	0	0%	0	0	0	0
Don't know	15	41%	7	1	2	5

Table 23. Did your company receive IOC data using MISP?

	N	%	YBANK	YSHOP	YSOC	YSTORE
Yes	21	57%	4	6	5	6
No	0	0%	0	0	0	0
Don't know	16	43%	6	2	3	5

As there were only 16 BT members, four in each company, who had logged into MISP during the exercise, there were only a few more who knew that their team member was using MISP.

In this sense, the usage of MISP might have failed even as there were dedicated training sessions available on how to use MISP and it was proposed that MISP is the tool to use for controlled sharing of the cyber threat intelligence.

Based on the responds to survey 1 question 22, most of the respondents considered that there should have been more team members as there were too many tools used in the exercise to collect and share information; e.g. when the same data was collected as a ticket in an incident management system, it was needed to be shared to WT with chat and wiki and if it was interesting cyber threat intelligence information, it was needed to be shared with MISP as well to other BTs.

By looking up the data stored in MISP (Table 24) and comparing to usage of other tools (Table 9), the usage of MISP was quite low. In chapter 5.4 the actual data stored to MIPS is analyzed more detailed.

Table 24. Shared MISP events

BT	MISP Events	Attributes
YBANK	7	26
YSHOP	5	16
YSOC	15	34
YSTORE	7	3

In survey 2, question 15 it was asked how easy it was to collect and store cyber threat intelligence with some tools (Figure 23), with value range 1: very easy, 5: very hard. During the whole course there was complaints that the chat and the wiki pages (Collab) were difficult to use, but it seems that when there were additional training sessions related to these tools, the training affected positively at least to chat and wiki tools so that they were easy to use in the exercise.

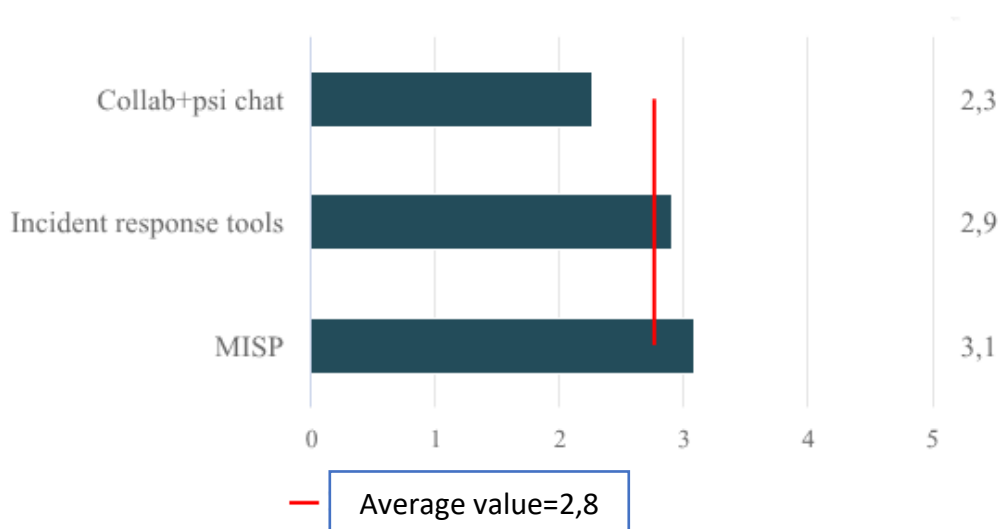


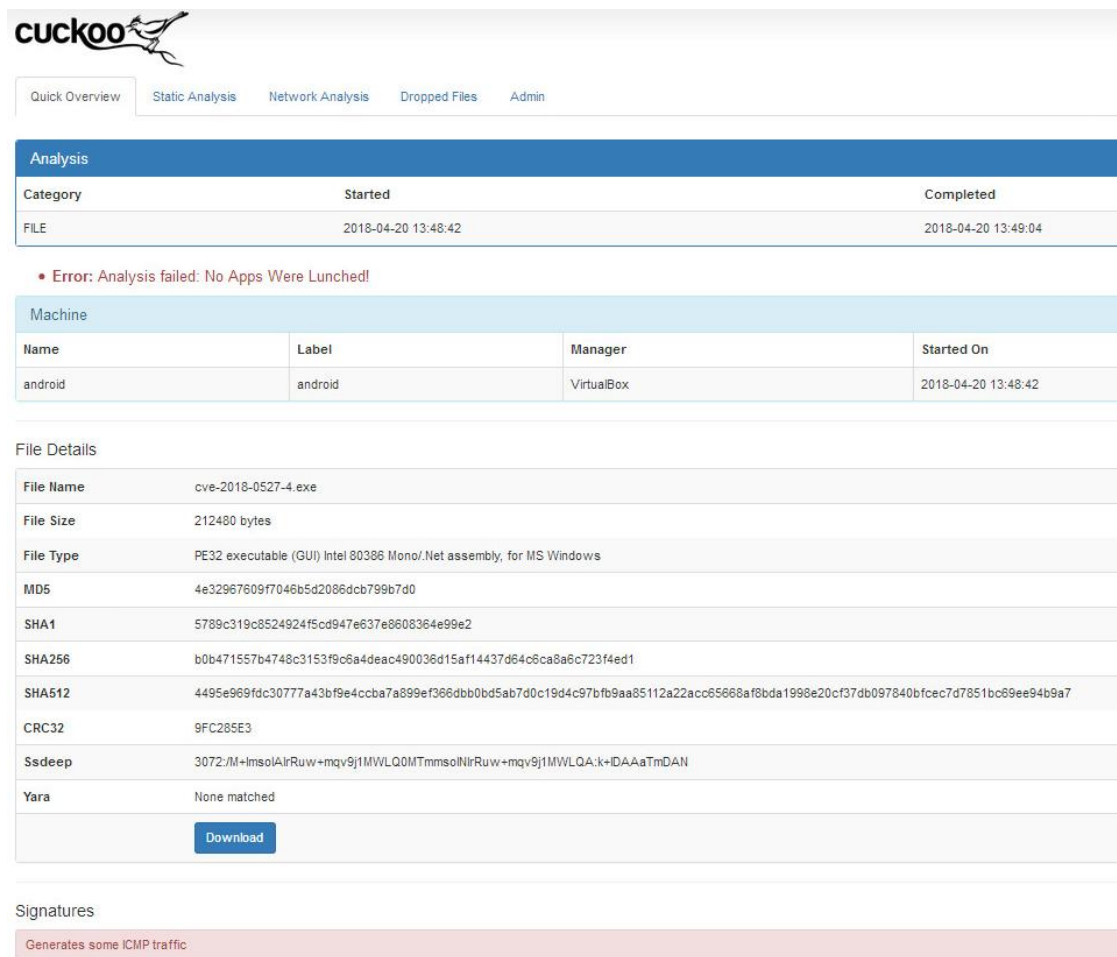
Figure 23. How easy was it to collect and store cyber threat intelligence with following tools?

Based on Figure 23, there is not so such big difference with incident response tools and MISP. Although, in order to be able to use tools efficient way it can be assumed that BTs had dealt with the learning issue in their team. Based on the login logs of MISP, there was no evidence that BT members were trying to learn to use MISP by themselves during the preparation phase, which reflects the somewhat higher mean value 3.1 in Figure 23.

#### 5.4.6 Mitigation of threats

One of the problems in these kind of exercises is how to verify what information was used to mitigate threats. For example, if one BT identifies a malicious email and then the email sender is then blocked by tools used in another BT, there should be evidences in some logs in another BT systems that the malicious email was noticed and blocked.

In Figure 24 is a malware analyzed by YSOC. This information was shared with YSTORE and YSHOP. At least YSHOP reacted to it and implemented the needed email filters.



The image shows a screenshot of the Cuckoo Sandbox web interface. At the top, there's a navigation bar with links: Quick Overview, Static Analysis, Network Analysis, Dropped Files, and Admin. The main content area is titled 'Analysis' and shows a table with columns: Category, Started, and Completed. The data row shows 'FILE' with a start time of '2018-04-20 13:48:42' and a completion time of '2018-04-20 13:49:04'. Below this, a red error message states: 'Error: Analysis failed: No Apps Were Launched!'. Underneath, there's a 'Machine' section with a table showing details for an 'android' machine, including its label, manager (VirtualBox), and start time. The 'File Details' section follows, displaying various hashes (MD5, SHA1, SHA256, SHA512, CRC32) and other file properties like File Name, File Size, File Type, MD5, SHA1, SHA256, SHA512, CRC32, Ssdeep, and Yara. A 'Download' button is present at the bottom of the file details. Finally, the 'Signatures' section shows a single entry: 'Generates some ICMP traffic'.

**Analysis**

Category	Started	Completed
FILE	2018-04-20 13:48:42	2018-04-20 13:49:04

• Error: Analysis failed: No Apps Were Launched!

**Machine**

Name	Label	Manager	Started On
android	android	VirtualBox	2018-04-20 13:48:42

**File Details**

File Name	cve-2018-0527-4.exe
File Size	212480 bytes
File Type	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
MD5	4e32967609f7046b5d2086dcb799b7d0
SHA1	5789c319c8524924f5cd947e637e8608364e99e2
SHA256	b0b471557b4748c3153f9c6a4deac490036d15af14437d64c6ca8a6c723f4ed1
SHA512	4495e969fdc30777a43bf9e4ccba7a899ef366dbb0bd5ab7d0c19d4c97bf9aa55112a22acc65668a8bda1998e20cf37db097840bfcec7d7851bc69ee94b9a7
CRC32	9FC285E3
Ssdeep	3072:/M+ImsoAlrRuW+mqv9j1MWLQ0MTmmsolNlrRuW+mqv9j1MWLQA:k+IDAAaTmDAN
Yara	None matched

[Download](#)

**Signatures**

Generates some ICMP traffic
-----------------------------

Figure 24. YSOC malware analysis

While investigating all other RT attacks, there was no evidence found that shared cyber threat intelligence might have helped to mitigate the threats. Question 15 in survey 1 tried to collect information on if an individual team member was using the collected or shared cyber threat intelligence used to mitigate threats (Table 25).

Table 25. Did you use the collected or shared cyber threat intelligence to mitigate threats?

	N	%	YBANK	YSHOP	YSOC	YSTORE
Yes	17	46%	5	2	5	5
No	20	54%	5	6	3	6

Question 16 on survey 1 tried to collect information on if the respondent knew that the collected or shared cyber threat intelligence was used to mitigate threats (Table 26).

Table 26. Did your company use the collected or shared cyber threat intelligence to mitigate threats?

	N	%	YBANK	YSHOP	YSOC	YSTORE
Yes	23	62%	7	4	6	6
No	5	14%	0	1	2	2
Don't know	9	24%	3	3	0	3

Based on Table 25 and Table 26 once again at an individual level responders can identify if they used the cyber threat intelligence to mitigate threats, however, still a totally five thought that no cyber threat intelligence was used to mitigate threats and even nine were not even sure about it.

#### 5.4.7 Quality of cyber threat intelligence

In survey 1 (Appendix 1) questions 17 and 18, the respondents were asked to define were if the collected and received cyber threat intelligence was meaningful, i.e. if the collected or received data should help to maintain or improve the situation awareness and to mitigate the threats. The respondents were given choice to give value between 1-5, in Figure 25, only 37 answers were received. The average value is for collected data 2.3 and for received data 1.9.

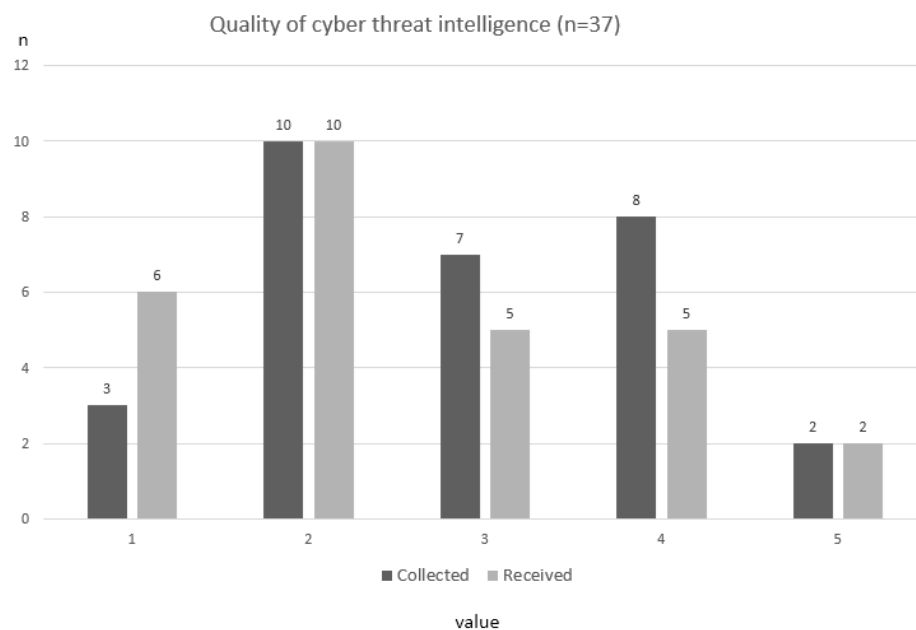


Figure 25. Quality of collected and received cyber threat intelligence

Based on Figure 25. Quality of collected and received cyber threat intelligence, it might be considered that all teams think that their own collected cyber threat intelligence has a better quality than the cyber threat intelligence received from somewhere else. This is well reflected with the survey 1 question 21, Figure 26, which shows that in a scale 0-5, the quality of the received IOCs in MISP had an average value 2.13.

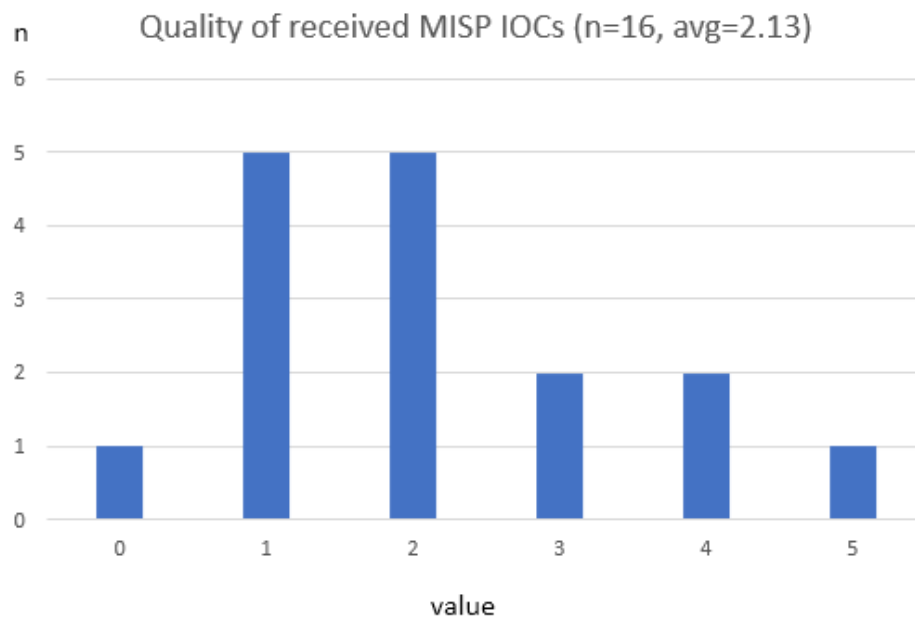


Figure 26. Quality of received MISP IOCs

Same kinds of questions were asked in survey 2 as well. The respondents were asked to define the quality of their own and shared cyber threat intelligence and define the quality of the received cyber threat intelligence with value range 0-5 (survey 2, questions 10 and 11, Table 27).

Table 27. Overall quality of collected, shared and received cyber threat intelligence

Question	Min value	Max value	Average	Median	Sum	Standard Deviation
10. Overall quality of your own collected and shared cyber threat intelligence	0	4	2.18	2	24	1.08
11. Overall quality of received cyber threat intelligence	1	4	2.73	3	30	0.9



For survey 1 question 17: “Was the collected cyber threat intelligence meaningful?” the average is 2.3 and for survey 1 question 18: “Was the received cyber threat intelligence meaningful?” the average is 1.9. The respondents of all BTs considered that the information collected by themselves was more useful than the received information. On the other hand, the survey 2 respondents considered that the quality of the received information was better than their own.

When it was asked in survey 2, questions 8 and 9 how trustworthy they thought that the cyber threat intelligence was, there was no big difference as seen in Table 28.

Table 28. Trusting the cyber threat intelligence

Question	Min value	Max value	Average	Median	Sum	Standard Deviation
8. When you received some cyber threat intelligence from another company, did you trust it?	1	5	3.36	4	37	1.12
9. Do you think that your own shared cyber threat intelligence was trusted?	2	5	3.45	3	38	1.04

The results for survey 2 questions 8-11 might reflect the responses to survey 2 questions 3-7 as if the quality of the information was considered high enough, the respondents trusted the received information, so there was no need to discuss or give feedback about the received information as much as was expected to be.

In survey 2 question 12 it was asked to fill in the quality of the received cyber threat intelligence from different sources, where the options to answer were 0: not received, 1: low quality – 5: high quality (Table 29).

Table 29. Quality of the received cyber threat intelligence from different sources

Company	Average	Median
YSOC	2.55	3
YBANK	2.09	3
YSHOP	2.55	3
YSTORE	2.27	3
CSC	2.18	3
Telia (by email)	2.36	2
FUNNEL	0.36	0
LAW and ORDER	1.09	1
RNA	0.73	0
SATSUMA	0.64	0
STEVENSBLOG	0.36	0
WATTI	0.45	1
Shared CVEs (CNN news)	1.46	1
<b>ALL</b>	<b>1.48</b>	<b>1</b>

When comparing the values in Table 29 to the results of question survey 2 question 11, in Table 27, where the average was 2.73, it can be noticed that the overall quality of received cyber threat intelligence was estimated to be higher than any of the individual ones.

## 5.5 Analysis of created MISP events

Table 30 presents the data collected from different tools in the game environment: the count of incidents from incident management system, the count of event pages from wiki and the count of events in MISP.

Table 30. BTs and their incidents and events

BT	Exercise day 1 (10:00-17:30)				Exercise day 2 (9:00-12:00)			
	Incidents	Wiki Events	MISP Events	MISP Attributes	Incidents	Wiki Events	MISP Events	MISP Attributes
YBANK	23	14	3	17	12	10	4	9
YSHOP	22	16	4	13	33	7	1	3
YSOC	45	35	10	24	30	15	5	10
YSTORE	16	17	4	3	3	10	3	0

One of the earliest attacks was on the day 1 morning an attack where RT scanned some ports of all BTs. As a good example YBANK was able to detect the scan and it was correctly reported as incident, wiki page and MISP event (Figure 27).

WINE18BT1 COLLAB

Mistä havaittiin? (src)  
**src**  
222.87.211.55, 91.209.160.180, 222.87.208.1, 124.126.251.98 (mahd. 118.85.207.1) IP-osoitteet kiinasta  
Miten havaittiin? (how)  
**how**  
Palomuuria monitoroimalla  
Mihin vaikutti? (dst)  
**dst**  
ybank.com, p22

#1 - Port scanning are seen

Forward | Bounce | Phone Call Outbound | Phone Call Inbound | SpE | Print | - Reply -

From: Helpdesk  
To: Kyösti Sario  
Subject: Port scanning are seen

From addresses 222.87.211.55, 91.209.160.180

Your Ticket-Team

...  
Money Mailer  
Email: helpdesk@ybank.com - Web: <http://www.ybank.com/>  
...

Created: 20/04/2018 11:12 by Petri Taipale

**Suspicious traffic from multiple source**

Event ID: 57  
Uuid: 5ad9a060-1f8c-499e-9e5e-5f36c06624f6  
Org: YBANK  
Owner org: YBANK  
Contributors: @ybank.com  
Tags: MAIN EVENT x osint:source-type="block-or-filter-list" x eu  
Date: 2018-04-20  
Threat Level: Low  
Analysis: Ongoing  
Distribution: CSC\_ALL  
Info: Suspicious traffic from multiple source  
Published: No  
#Attributes: 6  
Sightings: 0 (0) - restricted to own organisation only  
Activity:

+Pivots +Galaxy -Attributes -Discussion

« previous next » view all

+

Date	Org	Category	Type	Value	Tags
2018-04-20		Network activity	ip-src	222.87.211.55	+
2018-04-20		Network activity	ip-src	91.209.160.180	+
2018-04-20		Network activity	ip-src	222.87.208.1	+

Figure 27. YBANK detected malicious scanning

As the MISP event was not shared, the relationship of the attacks was not detected by other BTs, although as a MISP system administrator the relationships between different events could be identified (Figure 28).

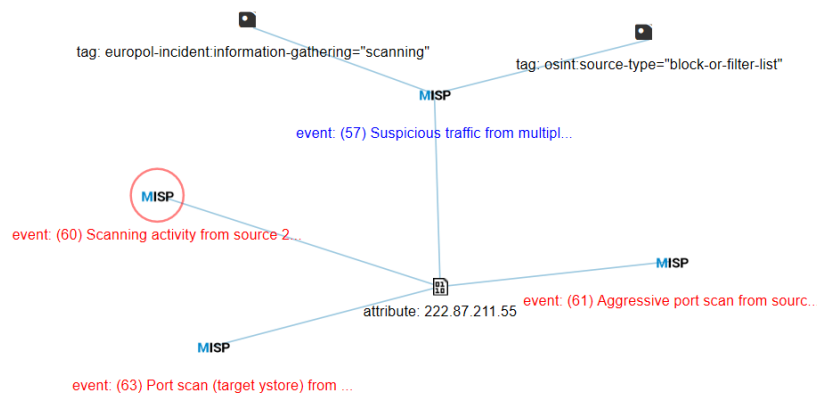


Figure 28. MISP event relationships related to detected malicious IPv4 address

In Figure 28, YSTORE reported their own event number 60 and YSOC reported their own event 61 and 63, which was affecting YSTORE. YSOC also detected the attack against YSHOP and just warned YSHOP. On the other hand, YSHOP managed to identify the malicious IPv4, but did not report into MISP for unknown reasons.

If considered from the national cyber security center point of view, it would be critical to know if an attack is against one company or one IPv4 address, or if the attack is against many companies, i.e. affecting hundreds of IPv4 addresses. As it was early in the exercise, it was assumed that as the attack was easy to detect, the BTs would have time to learn how to use MISP to create valid MISP event and collect relevant and correct cyber threat intelligence i.e. source IPv4 addresses and target information as MISP attributes.

By looking up the RT attack blueprints, it was possible to estimate and calculate the number of expected IOCs for each event. Table 31 was defined when RT IOCs were combined to the data seen on the MISP as attributes. In Table 31, all MISP attributes were analyzed and compared to the public OSINT feeds events and attributes which can be enabled in MISP. High quality means that the attribute followed the good practices of MISP OSINT feeds and low-quality means that the attribute needs some editing to be valuable information for the consumer of that cyber threat intelligence.

Table 31. Expected IOCs vs analyzed MISP attributes

BT	Exercise day 1 (10:00-17:30)				Exercise day 2 (9:00-12:00)			
	Expected IOCs	Reported MISP Attributes	High quality	Low-quality	Expected IOCs	Reported MISP Attributes	High quality	Low-quality
YBANK	34	17	16	1	38	9	7	2
YSHOP	42	13	13	0	26	3	3	0
YSOC	44	24	17	7	22	10	7	3
YSTORE	40	3	2	1	26	0	0	0

In Table 31 it can be seen how the speed of the exercise affected to the BTs. As on the day 2, teams could also mitigate threats, there was less time for reporting as well. Although on day 1, 6.5 high quality MISP attributes was reported for each hour, on day 2 5.7 for each hour. As expected, the BTs were learning and were faster, so they managed to keep high quality reporting to MISP as well.

In Table 31 can be seen that there was good opportunity to collect good amount of cyber threat intelligence, however, the major problem of the exercise is to capture the RT IOCs as well. During the exercise, RT tried to collect their own set of IOCs based on what was defined in the RT blue prints filled with the information of the environment such as the source IPv4 addresses of their attacks and some of the

attack targets for email phishing scenarios were decided just couple of minutes before the attacks.

The amount of reported RT IOCs was 114, less than expected in Table 30, where the total amount of 272 IOCs was expected to be seen. While comparing the RT IOCs to the BT reported ones, it was found that BTs managed to collect 14 MISP attributes that matches to 12 different RT events and their IOCs (Table 32).

Table 32. Correct MISP attributes reported for detected RT events

	YBANK	YSHOP	YSOC	YSTORE
Correct MISP attributes	3	3	6	2

While investigating how WT events were detected and reported, as it was earlier seen in Table 6, most of the BTs were not collecting cyber threat intelligence from the game environment or if they were, the identified data was not stored in wiki or any other tools provided in the game environment. Based on the WT blueprints, the minimum expected MISP attributes were calculated (Table 33).

Table 33. Expected and reported correct MISP attributes for WT events

	YBANK	YSHOP	YSOC	YSTORE
Expected MISP attributes	83	71	82	71
Reported correct MISP Attributes for WT events	0	0	4	0

As MISP was selected as the tool to be used to share cyber threat intelligence, it is somewhat obvious that either the teams did not have enough resources, or the process of handling cyber threat intelligence was totally ignored. This can be seen when all relevant information of RT and WT events together with expected and reported cyber threat intelligence is summarized in Table 34.

Table 34. Summary of exercise events, containing expected MISP attributes vs reported MISP attributes

	YBANK	YSHOP	YSOC	YSTORE
All events	52	45	48	43
All expected MISP Attributes	155	139	148	137
All detected events	10	10	24	11
Detected RT events	8	8	7	7
Expected MISP attributes for detected RT events	72	68	66	66
RT events reported to MISP	3	3	4	2
<b>Reported correct MISP Attributes for RT events</b>	3	3	6	2
Detected WT events	2	2	17	4
Expected MISP attributes for detected WT events	4	4	42	8
WT events reported to MISP	0	0	3	0
<b>Reported correct MISP Attributes for WT events</b>	0	0	4	0
<b>All reported correct MISP attributes</b>	3	3	10	2

When considering the European Union General Data Protecting Regulation (Regulation 2016/679) where article 33 defines, that in a case of a personal data breach, the supervisory authority needs to be notified no later than 72 hours after detecting the data breach. In cyber security exercise that would have meant that correct detection of the attack source and destination and correctly reporting it would have been quite enough for the CSC played by WT. There is a difference if the RT attack affects the YBANK banking web application or e.g. the extranet web application. Those different risk levels were also identified by the YBANK team themselves (YBANK Blue Team, 2018).

## 6 Discussion on results

In chapter 3.2, some goals for collecting and sharing cyber threat intelligence was defined in the exercise context. In this chapter, the goals are analyzed based on the exercise together with insights to situational awareness.

### 6.1 Analyzing the Goal 1

The goal 1 was: For each cyber security incident BTs should collect source and destination information as atomic indicators. By only looking up the data stored in MIPS the goal was not reached at all (Table 34). Even if looking at the data stored in wiki pages or in the incident management systems, the number of correct atomic indicators has not increased much (Table 35).

Table 35. Atomic indicators detected on wiki pages or in the incident management systems

	YBANK	YSHOP	YSOC	YSTORE
Correct atomic indicators	15	19	5	12

The only conclusion might be the fact, that even though the respondents to the survey 2 question 13 (Figure 18) considered that they knew the terms in the cyber security context, the atomic indicators are difficult to find, analyze and report correctly using the provide tools.

As the MISP was valued to be more difficult to use, survey 2 question 15 (Figure 23), and that together with the low average value 1.3 for atomic indicator as a term (Figure 18), might reflect the issue that, the atomic indicators were difficult to report with MISP, but easier to report in free text form within wiki pages or in the incident management system. To be able to use the atomic indicator in security controls, the indicators often needs to be defined in tool-specific technical format.

One of the key question was the allocation of team resources on BTs. How existing resources distributed to different tasks during the exercise? Even though there were 1-2 dedicated resources in each BT team to work with cyber threat intelligence, the amount of time they used to do it is unknown. Based on the amount of collected cyber threat intelligence, it can be only assumed that there might not have been

enough resources to collect cyber threat intelligence as keeping the technical business environment working is eventually more important than all other tasks, which was also identified by YBANK on their assets and risk analysis (YBANK Blue Team, 2018).

## 6.2 Analyzing the Goal 2

The goal 2 was that BTs should try to collect any tool, malware, vulnerability or attack pattern information. Even if it was suspected that the Goal 1 might be difficult for teams, however, to detect even one malware or attack pattern should not be totally impossible task.

At least all BTs were handling at least one CVE vulnerability technical report and based on the gathered information, the CVEs were analyzed and decided if there is a need for further actions.

On the other hand, all BTs trusted the IPv4 address list (Appendix 4, set 2 and 3), so that the data was not verified before traffic black lists were defined in firewalls (Figure 29). It seems that at least YSTORE did not block the valid traffic to Twitter and CNN web addresses as those addresses were on the list, hence, so some validation might have been made to the lists.

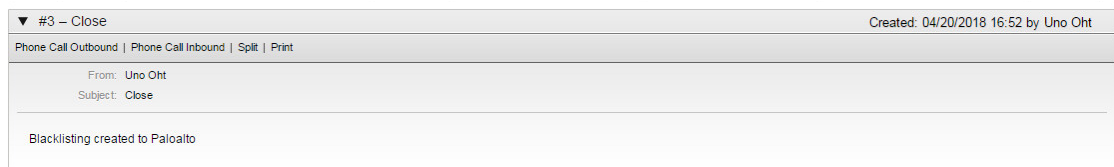


Figure 29. Blacklist created based on Telia IPv4 address list

The Appendix 16: the malicious code was not detected by any BT, before it was directly linked to Twitter. Even then YSOC analysts did not realize that the code contains IPv4 address of their own email server (Figure 30).



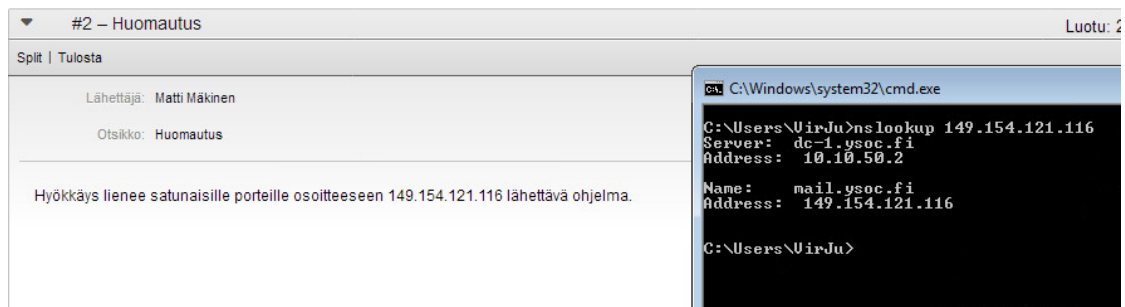


Figure 30. YSOC fails to detect their own IPv4 address

The RT attack scenario CSE311 (Ruusupihä, 2018) contained a technical attack pattern how the attack will be executed. It can be verified that at least YBANK detected the attack correctly and reported it into MISP as well (Figure 31). Goal 2 was achieved as it was assumed that maybe only one case can be solved by BTs when time schedules were expected to be very tight for an advanced analysis.

### Extranet was defaced

Event ID	68
Uuid	5ad9c6ad-9470-4200-bc1b-6118c06624f6
Org	YBANK
Owner org	YBANK
Contributors	
Email	@ybank.com
Tags	europol-incident:availability="sabotage" X +
Date	2018-04-20
Threat Level	Medium
Analysis	Completed
Distribution	CSC_ALL
Info	Extranet was defaced
Published	No
#Attributes	8
Sightings	0 (0) - restricted to own organisation only. ↗
Activity	

+Pivots +Galaxy -Attributes -Discussion

< previous next > view all

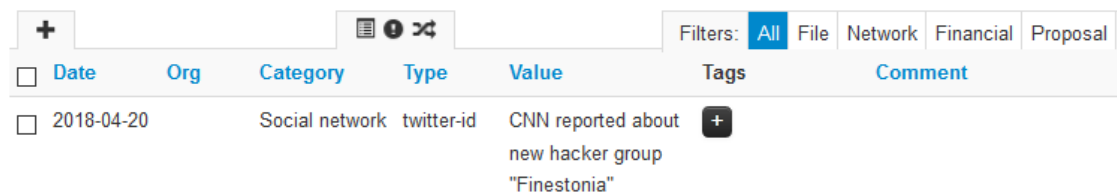
Date	Org	Category	Type	Value	Tags
2018-04-20		Network activity	hostname	extranetybank.com	+
2018-04-20		Network activity	ip-src	222.87.211.155	+
2018-04-20		Network activity	comment	They used sqlmap/1.1.11#stable (http://sqlmap.org).	+
2018-04-20		Network activity	ip-dst	91.208.45.10	+

Figure 31. YBANK detected attack pattern and tools

### 6.3 Analyzing the Goal 3

Goal 3 was related to identifying the threat actors. The idea was that law enforcement needs detailed information of threat actors so that they can catch them and convict them without a doubt.

As analyzed for Table 6, it looks like the BTs were not interesting to follow up social media content in an organized way. Only the YSOC managed to collect the data related to the WT801 (Hyytiäinen, 2018) and YSOC started to collect data in MISP (Figure 32), but also shared some information by email to CSC as well.



The screenshot shows the MISP interface with a table of detected threats. The table has columns for Date, Org, Category, Type, Value, Tags, and Comment. A single entry is visible, dated 2018-04-20, categorized as 'Social network' with the type 'twitter-id'. The value field contains the text 'CNN reported about new hacker group "Finestonia"'. There are filter tabs at the top for 'All', 'File', 'Network', 'Financial', and 'Proposal', with 'All' currently selected.

Date	Org	Category	Type	Value	Tags	Comment
2018-04-20		Social network	twitter-id	CNN reported about new hacker group "Finestonia"	+	

Figure 32. YSOC detected FINESTONIA

### 6.4 Analyzing the Goal 4

The major focus of the exercise was on to understand how BTs collect and share cyber threat intelligence. As it was discussed when analyzing the survey 2 questions 4-7 (Table 14 and Table 15), there was no real evidence found that the cyber security analysts had created their own group of experts sharing and discussing cyber threat intelligence.

While analyzing the survey 1 questions 10, Table 17, it was seen that some small amount of BT members were sharing the cyber threat intelligence to other BT. Goal 4 is partially fulfilled as there was only few people responsible for sharing cyber threat intelligence to another BT, however, eventually no expert group of analysts was seen for example trying to analyze what kind of mitigation is needed to prevent CSE311 (Ruusupiha, 2018) occurring again on exercise day 2.

## 6.5 Analyzing the Goal 5

This goal is a direct continuum of goals 1, 2 and 4. In the exercise setup some of the events were planned so that some of the RT attacks were played on both days. The aim was to detect if the collected cyber threat intelligence was used to mitigate the same threat occurring again on exercise day 2. The RT attack scenario CSE311 (Ruusupiha, 2018) was one of them.

The CSE311 was for example executed against YBANK on day one and day two. As the CSE311 was detected by YBANK (Figure 31) on day one, they did not plan any mitigation solutions for day two. The reason why there was no mitigation solution might be obvious: it is easy to think that RT might try as many different kinds of attack scenarios against each BT and once one had been detected by one BT it will be tried again against the same BT. However, the as the one course objectives is to learn how to mitigate detected cyber security threats, it was expected that mitigation would have been performed by all BTs.

Based on the incident management information by YSHOP, they identified the vulnerable plugin related to CSE311 correctly (Figure 33), which was uninstalled from the system as well.

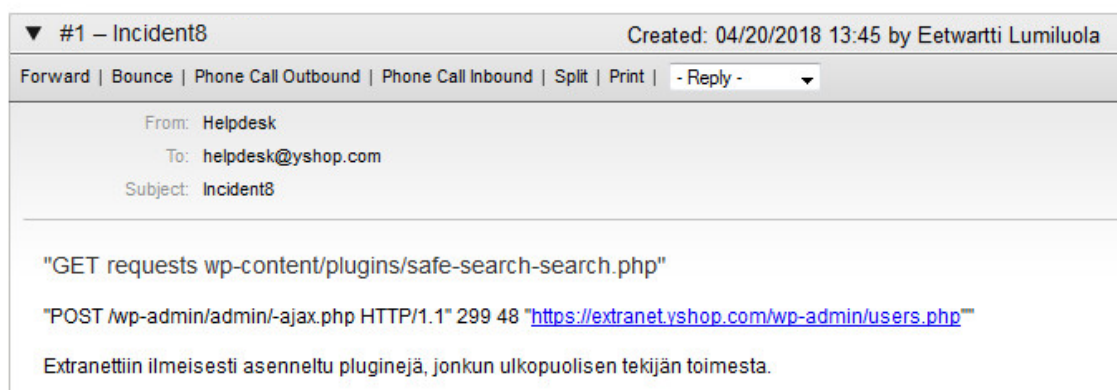


Figure 33. YSHOP detection of malicious plugin for CSE311

But YSHOP did not post the full mitigation solution with MISP as it should have done (Figure 34) or there is no evidence that it was shared in any other way to other BTs. By sharing the information correctly, YBANK should have had all correct information

to mitigate the CSE311 on exercise day two. In this case YBANK should have had enough time to do the mitigation before the second attack on day two.

Date	Org	Category	Type	Value	Tags	Comment
2018-04-20		Network activity	ip-src	222.87.211.155	+	
2018-04-20		Payload installation	text	Plugin installations	+	Unauthorized user is installing plugins to the extranet.yshop.com

Figure 34. YSHOP reported CSE311 to MISP

One of the many problems is how to identify what log data, social media information etc. has been analyzed as cyber threat intelligence and used to mitigate attacks and threats. To collect the chain of reasoning happening during the OODA loop might be required.

One solution could be that RT together with WT plans in more detailed what kind of cyber threat intelligence is shared during the exercise, for example by CSC. The aim could be that for some scenarios the correct mitigation solution might be given as a CVE report and for some others it could require collecting and analyzing data from several sources. The data should not be revealed to all BTs at the same time, rather so that each BT will have their own set of information and that information combined with the information shared and received with other BTs reveal the detailed attack scenario planned by RT.

## 6.6 Analyzing MISP as a tool

One of the goals of this research was to learn how MISP can be used for collecting, handling and sharing the cyber threat intelligence. As already discussed in Chapter 5.4 it might be considered based on Table 32 that BTs failed totally at least to collect correct and high-quality IOCs to MISP.

When considering the requirements presented in the thesis on Requirement specification for cyber security situational awareness (Lötjönen 2017), new situation awareness system is needed for BTs, so that the number of tools used for situation awareness is less than used on this research. As it was seen, some cyber threat

intelligence was correctly stored, for example in incidents or in wiki, however, it was never correctly shared with MISP to another team. Either there were too many tools to be used or the learning curve of some of the tools was too high.

If the aim of a live cyber security exercise is to train teams to collect, analyze, share and enrich the cyber threat intelligence, the whole exercise scenario needs to be planned differently. If there are too many technical RT attacks or too tight time schedule between them, BTs do not have time to collect any cyber threat intelligence at all; they are focusing on the logs to detect incidents and then handling those incidents. Between RT attacks, BTs need to have some time to analyze and share cyber security intelligence of the detected attack scenario. This issue was also identified as risk R3 in chapter 3.4.

By looking up the organization structures of the BTs, all of them had dedicated resources responsible for handling cyber threat intelligence. The question that cannot be answered based on this research is: why is the amount of collected cyber threat intelligence low as seen on the summary Table 34.

Lötjönen proposes in his system construction (2017, 57-60) that the data is automatically collected e.g. from logs, log management system and from other technical systems. It can be argued that if the exercise is more technical, from the learning point of view it might be valuable on situation awareness level 1 to use the different tools as is, however, if the exercise focus is more on the process side where different information flows are more important, then the correct amount of data aggregation might save valuable time for other tasks like collecting, analyzing and sharing cyber threat intelligence.

Based on this research, it cannot be stated if MISP cannot be used on live exercises. It can be considered that the MISP might have a high learning curve which was not realized by the users who were supposed to use it. It might be because respondents to survey 2, question 13 had issues to understand what atomic indicator is as seen on Figure 18. It will not be easy to map atomic indicator to MISP attribute if there is a small doubt what that piece of information is and what it should represent as an attribute on a MISP event.

Goal 1 was: For each cyber security incident BTs should have been collected source and destination information of the attack as atomic indicators. The question arises if the IPv4 address is one of the basic things to understand about computer networks, why there were so few correct IPv4 source or IPv4 destination addresses identified?

In the survey 1 question 22, there are some answers related to MISP, tools and situation awareness (translated from Finnish):

- Non-MISP user: too many communication channels, there was time only to focus on one to two tools
- Non-MISP user: main situation awareness tool was the incident management system and I did not have time to look at MISP at all. As a team we did not get enough situation awareness info from other BTs and it looked like our team should have more people working with MISP
- Non-MISP user: it looks like we did not notice any attacks at all, if we would have identified some of the attacks soon enough, there might have been time to inform other teams about them. We had too little time to do the analysis of the detected attacks, which would have been needed to do better hardening
- MISP user: the MISP was interesting addition to the exercise
- MISP user: we had so much things to do, that handling of cyber threat intelligence was almost ignored, so we were not able to use it for hardening our environment. We were too unexperienced.
- MISP user: MISP is new kind of tool and as such might not be optimal for exercise. Near end of the exercise I realized how the tool could have been used. MISP requires decent training as it is quite technical tool.
- MISP user: Good tools, but in the exercise, situation was not the best possible for that kind of tool usage. Most of the focus went to operative incident management tasks.
- MISP user: it was difficult to understand the mapping of information to MISP attributes. Overall it might be good tool, but in this kind of fast exercise there should be lighter simpler solution. The idea is good though.

Based on these freeform answers, BTs might have failed to identify the risk R1 (chapter 3.4), even though they have allocated resources for handling cyber threat intelligence, those resources were not enough in this exercise and research.

MISP might be a good tool for advanced users who understand the technical side of the IOCs (the identified risk R2). The conclusion is that to be able to arrange an exercise where collecting, handling and sharing cyber threat intelligence is required with a tool which might have high learning curve, handling the identified risks on chapter 3.4 needs to be taken care of.

## 6.7 Analyzing the situation awareness

In his thesis, Lötjönen (2017) illustrates how cyber security information is shared and consumed based on his experience (Figure 35). As there was no guidance given to BTs how to organize their team structure or incident management processes, each of the BTs followed a similar kind of structure as pictured Figure 35. This was also seen in Figure 14, where YSHOP organization structure is illustrated.



Figure 35. Cyber Security information consumers and providers (Lötjönen, 2017, 38)

Based on the amount of collected cyber threat intelligence it can be stated that the BTs might have failed to understand the importance of collecting and sharing of the cyber threat intelligence as a part of situational awareness. Another conclusion is that the current tools what was used in the exercise were not suitable for collecting and sharing cyber threat intelligence based on the survey 2 question 15 (Figure 23). These 2 issues were also identified by several respondents to free form survey 1 question 22.

It can be stated that all BTs were using the situation awareness tools provided by the game environment. It was allowed to install new security controls or situation awareness tools, but none of the BTs take the opportunity to do it.

Based on the Table 10 it can be concluded that in this kind of research setup and in this exercise, the BTs were using quite much time on analyzing logs on log

management system or handling different kind of incidents to maintaining the level 1 and level 2 situation awareness. As such it is a good learning experience for the bachelor's degree students or anyone else who have none or small amount of work experience of those tasks.

Overall time schedule might have been the problem, the time between technical attacks might have been too tight. Survey 1 question 5 might have some insights, when comparing users who were using MISP to users who were not using MISP, as it was considered that the MISP users were responsible to share the threat intelligence to another BT.

In Figure 36 the survey 1 question 5 data are split to two groups: MISP users vs non MISP users. Average values of data were recalculated so that the most important tool was given weight 7 and least important 1.

Based on the Figure 36, the users of MISP, might have used quite many situation awareness tool or at least the importance of some tools were much higher than comparing to non MISP users group. It seems like that the workload might have been high, as the cyber threat intelligence or information that those MIPS users needed was scattered among several different tools.



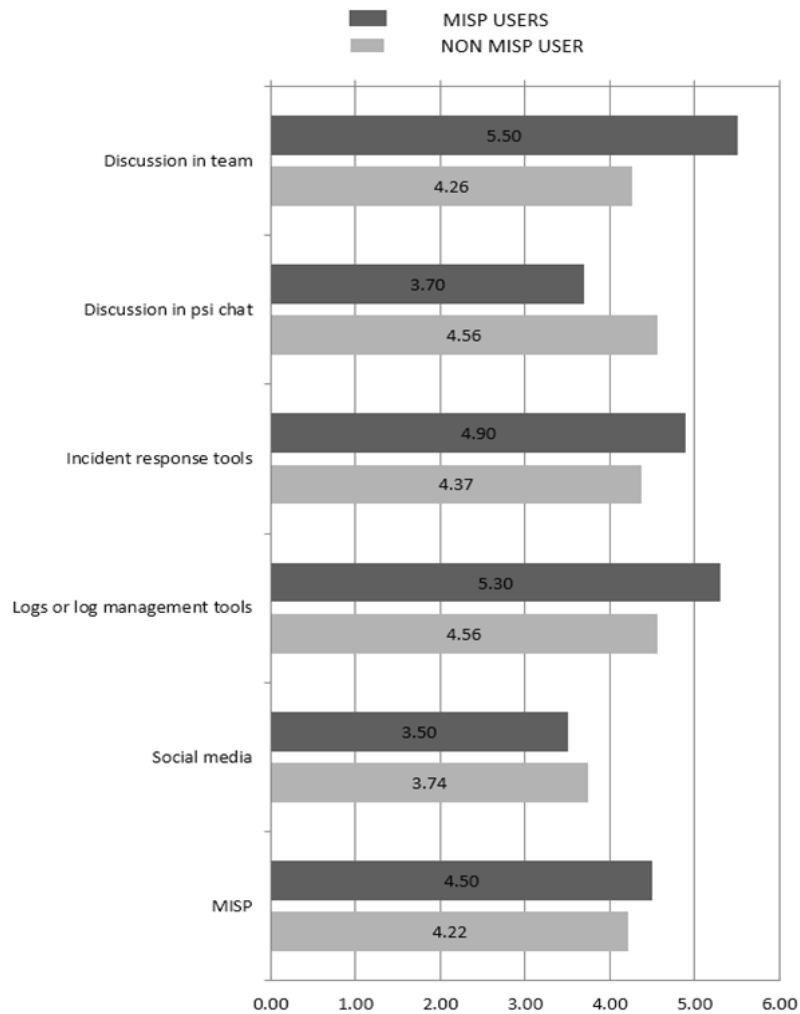


Figure 36. Most important situation awareness tool: MISP users vs non MISP users

Based on the incidents in incident management systems, there was no such detailed information based on what data the incident has been originally made. In that sense it makes sense, that MISP users to be able to share correct and valid cyber threat intelligence, they need to go through all systems to verify and find all information related to the incident in the incident management system. There needs to be communication between team members so that the correct information is found, which might explain the highly valued team communication as well.

It might also explain the quality of collected cyber threat intelligence in MISP. If the detailed information why an incident that was reported to incident management system was lost, it might be very difficult to find that data afterwards. Based on this research there is a need to consider what kind of data aggregation (Lötjönen, 2017, 60) is needed in the new situation awareness tool.

The data aggregation might need to be configurable so that depending on the exercise focus it can be configured correctly. If the live cyber security exercise is more focused on the technical side, it might be relevant for the participants to look up data directly from the logs or log management systems. On the other hand, if the focus is on training processes, it should be possible to use aggregation to create more advanced situation awareness user interfaces for BT members.

## 7 Conclusions

The first idea for this thesis started to evolve during on the cyber security exercise course on spring 2017, where author realized as white member that the existing exercise tools were not good enough for keeping up the situation awareness of the exercise in decent level regardless of the team where you were. When trying to follow whats going on in each team was really difficult.

The discussions about this thesis topic started later on 2017 with the assignee organization JYVSECTEC, when author realized that there was ongoing thesis work defining the requirement specification for the situation awareness tools for blue teams (Lötjönen, 2017).

Author has always been interested to knowledge and information management, to help organizations to improve processes and to help organizations to select correct tools for knowledge and information management as well. These personal interests also affected not only research questions, but to the selection of reserch methods too.

It would have been interesting to get insights how red team and white team maintains their situation awareness through the exercise as well, but limiting this research to include only blue teams was needed to get first hand information as a results from the two surveys, how different tools were used not only for personall situation awareness but for team situation awareness as well during a cyber security exercise.

Some of the research questions were related how cyber threat intelligence is collected, analyzed and shared during cyber security exercise, the empirical research was selected as at the moment there is not research done on that field, a case study during a cyber security exercise course was used to collect information how organizations works during a cyber security exercise.

Both surveys offers new information how different tools were used not only for situation awareness, but also for cyber threat intelligence as this was first cyber security exercise, in assigned organization JYVSECTEC, where MISP was used as a tool by blue teams.

The results presented here should help JYVSECTEC to design and plan cyber security exercises so that main focus of the exercise could be to learn how to collect, analyze, share and enrich the cyber threat intelligence.

This thesis offers new information how situation awareness is handled in cyber security exercises by blue teams. Results should also help JYVSECTEC to implement the proposed situation awareness system for blue teams (Lötjönen, 2017).

There is a need to do further research of the situation awareness of the blue teams. As it was seen on this research the communication inside the team was one of the most used method to keep up the personal situation awareness. Based on survey one, even though the organization structures were defined before exercise, the members of blue teams were not able to answer for example if the company had shared cyber threat intelligence or not.

To understand how a blue team is actually functioning there is a need to research for each cyber security incident identified by the blue team, what kind of incident response sub group inside the blue team is created, how do they communicate, what kind of information is shared inside that sub group and what information is shared to the rest of the blue team.

A lot of issues related to how to collect, analyze, share and enrich the cyber threat intelligence can be seen as a knowledge management problem. As the knowledge management itself is complicated problem to be solved, to have globally connected tools or software systems, which can be used to share cyber threat intelligence will happen in future, but when and is it MISP or some other tool, time will tell. As one way to handle the cyber security threats is to have high quality cyber threat intelligence which can be trusted.

Even though there are tools which can be used to solve many problems, tools cannot solve the problem if the users does not understand what problem the tool should resolve. Defining requirements and selecting a correct tool for collect, handling, sharing and enrich cyber threat intelligence in cyber security exercise can be seen as own research topic as well.

## References

- Adnan, M., Just, M., Baillie, L., Kayacik, H. G. 2015. *Investigating the work practices of network security professionals*. Information & Computer Security, Vol. 23 Issue: 3, pp.347-367. Referenced 30 January 2018. Retrieved from <https://doi.org.ezproxy.jamk.fi:2443/10.1108/ICS-07-2014-0049>
- Al-Ibrahim, O., Mohaisen, A., Kamhoua, C., Kwiat, K., Njilla, L. 2017. *Beyond Free Riding: Quality of Indicators for Assessing Participation in Information Sharing for Threat Intelligence*. Technical Report 2017, University at Buffalo and Air Force Research Lab (88ABW-2017-0416). Accessed 2 January 2018. Retrieved from <https://arxiv.org/abs/1702.00552>
- Borum, R., Felker, J., Kern, S., Dennesen, K., Feyes, T. 2015. *Strategic cyber intelligence*, Information & Computer Security, Vol. 23 Issue: 3, pp.317-332. Accessed 16 January 2018. Retrieved from <https://doi.org/10.1108/ICS-09-2014-0064>
- Brehmer, B. 2005. *The Dynamic OODA Loop: Amalgamating Boyd's OODA loop and the Cybernetic Approach to Command and Control*. In 10th International Command and Control Research and Technology Symposium, The Future of C2. Accessed 9 April 2018. Retrieved from <https://pdfs.semanticscholar.org/7e9d/23a6911d636666338358505613bb5eba43b8.pdf>
- Cyber Security Exercise YIIP3400. 2018. JAMK University of Applied Sciences. Accessed 24 May 2018. Retrieved from [https://asio.jamk.fi/pls/asio/asio\\_ectskuv1.kurssin\\_ks?ktun=YIIP3400](https://asio.jamk.fi/pls/asio/asio_ectskuv1.kurssin_ks?ktun=YIIP3400)
- Directive (EU) 2016/1148. *Directive of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*. Official Journal of the European Union. Accessed 9 January 2018. Retrieved from <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN>
- El Sawy, O. A., Majchrzak, A. 2004. *Critical issues in research on real-time knowledge management in enterprises*, Journal of Knowledge Management, Vol. 8 Issue: 4, pp.21-37. Accessed 9 April 2018. Retrieved from <https://doi.org/10.1108/13673270410548469>.
- Endsley, M.R. 1995. *Toward a Theory of Situation Awareness in Dynamic Systems*. Human Factors Journal 37(1), 32-64. Accessed 9 January 2018. Retrieved from <http://journals.sagepub.com/doi/pdf/10.1518/001872095779049543>
- Europol, 2017. *Common Taxonomy for Law Enforcement and The National Network of CSIRTs v1.3 – December 2017*. Europol, European Union Agency for Law Enforcement Cooperation, European Union. Accessed 7 May 2018. Retrieved from [https://www.europol.europa.eu/sites/default/files/documents/common\\_taxonomy\\_for\\_law\\_enforcement\\_and\\_csirts\\_v1.3.pdf](https://www.europol.europa.eu/sites/default/files/documents/common_taxonomy_for_law_enforcement_and_csirts_v1.3.pdf)
- Executive Order No. 13691. 2015. DCPD-201500098 - *Executive Order 13691- Promoting Private Sector Cybersecurity Information Sharing*. Accessed 9 January

2018. Retrieved from <https://www.gpo.gov/fdsys/pkg/DCPD-201500098/pdf/DCPD-201500098.pdf>

Franke, U. Brynielsson, J. 2014. *Cyber situational awareness – A systematic review of the literature*. Computers & Society Volume 46, pages 18-41. Referenced 25 January 2018. Retrieved from <https://doi.org/10.1016/j.cose.2014.06.008>.

Fusano, A., Sato, H., Namatame, A. 2011. *Study of multi-agent based combat simulation for grouped OODA Loop*. SICE Annual Conference (SICE), 2011 Proceedings of, pp. 131-136. Referenced 10 April 2018. Retrieved from <https://ieeexplore.ieee.org/document/6060590/>

Garrido-Pelaz, R., González-Manzano, I., Pastrana, S. 2016. *Shall we collaborate? A model to analyse the benefits of information sharing*. Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security Pages 15-24. Accessed 2 January 2018. Retrieved from <https://arxiv.org/abs/1607.08774v1>

Hyytiäinen, P. 2018. *MISP IOC Objective Blueprint WT801 FINESTONIA Campaign*. YTCP0400 Cyber Security Exercise Report 19 April 2018. JAMK University of Applied Sciences.

Hyytiäinen, P., Manninen, K., Väisänen, T. 2015. *IOC-tietojen vaihto käyttäen MISP:iä (Using MISP to share IOC information)*. Cyber security employment training. JAMK University of Applied Sciences.

Implementation of Cyber Exercise TTKW0320. 2018. JAMK University of Applied Sciences. Accessed 24 May 2018. Retrived from [https://asio.jamk.fi/pls/asio/asio\\_ectskuv1.kurssin\\_ks?ktun=TTKW0320](https://asio.jamk.fi/pls/asio/asio_ectskuv1.kurssin_ks?ktun=TTKW0320)

Johnson, C., Badger, L., Waltermire, D., Snyder, J., Skorupka, C. 2016. *NIST Special Publication 800-150 : Guide to Cyber Threat Information Sharing*. National Institute of Standards and Technology. Accessed 10 January 2018. Retrieved from <http://dx.doi.org/10.6028/NIST.SP.800-150>

Kokkonen, T. 2016. *Anomaly-Based Online Intrusion Detection System as a Sensor for Cyber Security Situational Awareness System*. Doctoral Dissertation. Faculty of Information Tehcnology. Universtity of Jyväskylä. Accessed 2 January 2018. Retrieved from <http://urn.fi/URN:ISBN:978-951-39-6832-8>

Koskinen, K. 2010. *Organisational memories in project-based companies: an autopoietic view*. The Learning Organization, Vol. 17 Issue: 2, pp.149-162. Accessed 9 April 2018. Retrieved from <https://doi.org/10.1108/09696471011019862>

Lötjönen, J. 2017. *Requirement specification for cyber security situational awareness: Defender's approach in cyber security exercises*. Master Thesis (yamk). Degree Programme in Information Technology (Ylempi AMK / MSc). JAMK University of Applied Sciencies. Accessed 3 January 2018. Retrieved from <https://www.theseus.fi/handle/10024/139812>

Lötjönen, J., Jokinen, J., Saarisilta, J., Saharinen, K. 2018. *YTCP0400.8K0D1 Cyber Exercise Course Description*. Accessed 27 April 2018. Retrieved from [https://optima.jamk.fi/learning/id2/bin/doc\\_show?id=3142683&ws=3142683](https://optima.jamk.fi/learning/id2/bin/doc_show?id=3142683&ws=3142683)

Mavroeidis, V., Bromander, S. 2017. *Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence*. Proceedings of 2017 European Intelligence and Security Informatics Conference (EISIC), pages 91-98. Accessed 2 January 2018. Retrieved from <http://urn.nb.no/URN:NBN:no-61200>

MISP Community, 2018. *MISP – User Guide A Threat Sharing Platform*. Git repo: <https://github.com/MISP/misp-book>. Referenced 11 May 2018. Retrieved from <https://www.circl.lu/doc/misp/book.pdf>

MISP - Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing. n.d. Referenced 3 January 2018. <https://www.misp-project.org/>

Moihasen, A., Al-Ibrahim, O., Kamhoua, C., Kwiat, K., Njilla, L. 2017. *Rethinking information sharing for threat intelligence*. Proceedings of the fifth ACM/IEEE Workshop on Hot Topics in Web Systems and Technologies. Article No. 6. Accessed 2 January 2018. Retrieved from <https://doi.org/10.1145/3132465.3132468>

Regulation (EU) 2016/679 of The European Parliament and The Council, 2016. General Data Protection Regulation. Accessed 8 May 2018. Retrieved from <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679>

Ruusupihla, M. 2018. *Red Team Objective Blueprint CSE312*. YTCP0400 Cyber Security Exercise Report 19 April 2018. JAMK University of Applied Sciences.

Sharkov, G. 2016. *From Cybersecurity to Collaborative Resiliency*. SafeConfig '16 Proceedings of the 2016 ACM Workshop on Automated Decision Making for Active Cyber Defense, Pages 3-9. Accessed 27 December 2017. Retrieved from <https://doi.org/10.1145/2994475.2994484>.

Sillaber, C., Sauerwein, C., Mussmann, A., Breu, R. 2016. *Data Quality Challenges and Future Research Directions in Threat Intelligence Sharing Practice*. WISCS '16- Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security. Accessed 2 January 2018. Retrieved from <https://doi.org/10.1145/2994539.2994546>

Simola, V., Koskinen, P. 2018. *Red Team Objective Blueprint CSE111, Capital Punishment*. YTCP0400 Cyber Security Exercise Report 19 April 2018. JAMK University of Applied Sciences.

Sommestad T., Hallberg J. 2012. *Cyber Security Exercises and Competitions as a Platform for Cyber Security Experiments*. In: Jøsang A., Carlsson B. (eds) Secure IT Systems. NordSec 2012. Lecture Notes in Computer Science, vol 7617. Springer, Berlin, Heidelberg. Accessed 9 April 2018. Original reference [https://link.springer.com/chapter/10.1007/978-3-642-34210-3\\_4](https://link.springer.com/chapter/10.1007/978-3-642-34210-3_4). Retrieved from <http://www.sommestad.com/teodor/Filer/Sommestad,%20Hallberg%20-%202012%20-%20Cyber%20security%20exercises%20and%20competitions%20as%20a%20platform%20for%20cyber%20security%20experiments.pdf>

Sørensen, L. J. 2012. *Distributed Situation Awareness: Experimental Studies into Team Work*. PhD Thesis, University of Southampton, Faculty of Engineering and the

Environment. Accessed 9 April 2018. Retrieved from <https://eprints.soton.ac.uk/355965/>

Tuomi, I. 1999. *Data is more than knowledge: Implications of the reversed knowledge hierarchy for knowledge management and organizational memory*. Journal of Management Information Systems: JMIS; Armonk Vol. 16, Iss. 3, (Winter 1999/2000): 103-117. Accessed 9 April 2018. Retrieved from <http://dx.doi.org/10.1080/07421222.1999.11518258>

Vatanen, M. et al. 2017. *JYVSECTEC CYBER RANGE, RGCE and solutions*. Accessed on 4.4 April 2017. Retrieved from <http://jyvsectec.fi/wp-content/uploads/2017/02/JYVSECTEC-cyber-range.pdf>

Weerakkody, Niranjala. 2015. *Research methods for media and communication 2nd Edition*. Oxford University Press. ISBN 9780195588033.

Wood, M. 2013. *Scapy p.08 – Making a Christmas Tree Packet*. Accessed on 2. January 2018. <https://thepacketgeek.com/scapy-p-08-making-a-christmas-tree-packet/>

White Team, 2018. *Group assignment YTCP0400 After Action Report, Cyber Security Exercise*. YTCP0400 Cyber Security Exercise Report, May 2018. JAMK University of Applied Sciences

YBANK Blue Team. 2018. *Assets and risk analysis – YBANK*. YTCP0400 Cyber Security Exercise Report, March 2018. JAMK University of Applied Sciences

YSHOP Blue Team 2018. *YShop Business Model : Cyber Exercise Group Assignment*. YTCP0400 Cyber Security Exercise Report, March 2018. JAMK University of Applied Sciences.

YSOC Blue Team. 2018. *Cyber Security Exercise Report: Commercial Security Operations Center – YSOC Business Plan, Objectives and Risk Management*. YTCP0400 Cyber Security Exercise Report, March 2018. JAMK University of Applied Sciences.

YSTORE Blue Team. 2018. *YStore Business And Risk Management Process*. YTCP0400 Cyber Security Exercise Report, March 2018. JAMK University of Applied Sciences.

Zhao, W., White, G. 2014. *Designing a Formal Model Facilitating Collaborative Information Sharing for Community Cyber Security*. Proceedings of the 47th Hawaii International Conference on System Sciences 2014, pages:1987 - 1996. Accessed 24 January 2018. Retrieved from <https://doi.org/10.1109/HICSS.2014.252>



## Appendices

### Appendix 1. Survey: Situation Awareness and Cyber threat intelligence in WINE 2018

#### Part 1 Basic Information

**1. The company you worked in as employee?**

- ☐ BT YBANK
- ☐ BT YSOC
- ☐ BT YSTORE
- ☐ BT YSHOP

**2. What was your role in your company?**

**3. If your role changed during exercise, describe how it was changed?**

#### Part 2 Your own situation awareness

**4. What tools did you use for maintaining your situation awareness?**

- ☐ Discussion in team
- ☐ Discussion in psi chat
- ☐ Incident response tools
- ☐ Logs or log management systems
- ☐ Social media
- ☐ MISP
- ☐ Other

**5. What was the most important situation awareness tool for you (1=most important, 7=least important)**

	1	2	3	4	5	6	7
Discussion in team	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Discussion in psi chat	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Incident response tools	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Logs or log management tools	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Social media	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
MISP	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
other	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

**Part 3 You and cyber threat intelligence**

**6. Did you collect cyber threat intelligence during exercise?**

☒ Yes ☐ No

**7. Did you share cyber threat intelligence during exercise?**

☒ Yes ☐ No

**8. What tools did you use to share cyber threat intelligence in your company to your co-workers?**

- ☐ Discussion in team
- ☐ Discussion in psi chat
- ☐ MISP
- ☐ E-mail
- ☐ Phone
- ☐ Other
- ☐ Incident response tools
- ☐ Don't know

**Part 4 Sharing cyber threat intelligence**

**9. Did your company collect cyber threat intelligence during exercise?**

- ☐ Yes ☐ No ☐ Don't know

**10. Did you share cyber threat intelligence during exercise?**

- ☐ Yes ☐ No

**11. Did your company share cyber threat intelligence during exercise to other companies?**

- ☐ Yes ☐ No ☐ Don't know

**12. What tools did you or your company used to share cyber threat intelligence to other companies?**

☐ Discussion in psi chat

☐ MISP

☐ E-mail

☐ Phone

☐ Other

☐ Incident response tools

☐ Don't know

### Part 5 Receiving cyber threat intelligence

13. Did your company receive any cyber threat intelligence during the exercise?

- ☐ Yes
 ☐ No
 ☐ Don't know

14. What tools did your company use to receive cyber threat intelligence from other companies?

- ☐ MISP  
☐ E-mail  
☐ Phone  
☐ Other   
☐ Incident response tools  
☐ Social media  
☐ Don't know

### Part 6 Was the cyber threat intelligence used?

15. Did you use the collected or shared cyber threat intelligence to mitigate threats?

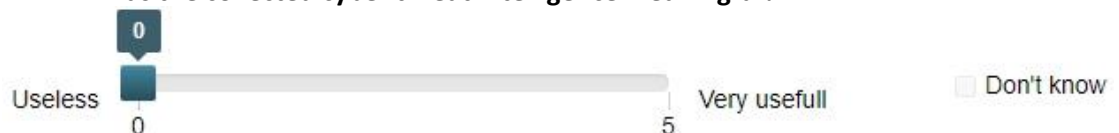
- ☐ Yes
 ☐ No

16. Did your company use the cyber collected or shared threat intelligence to mitigate threats?

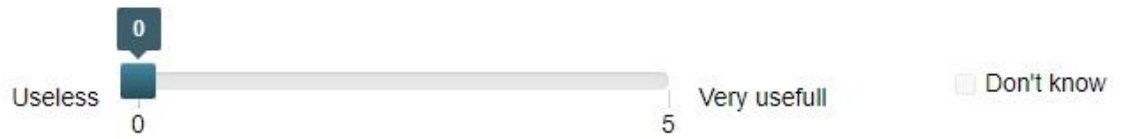
- ☐ Yes
 ☐ No
 ☐ Don't know

### Part 7 Quality of the cyber threat intelligence?

17. Was the collected cyber threat intelligence meaningful?



18. Was the received cyber threat intelligence meaningful?



### Part 8 MISP

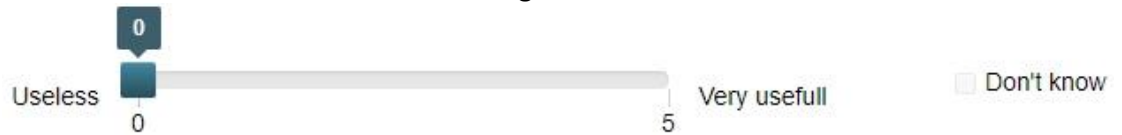
19. Did your company share IOC data using MISP?

- ☐ Yes ☐ No ☐ Don't know

20. Did your company receive IOC data using MISP?

- ☐ Yes ☐ No ☐ Don't know

21. Was the received IOC data meaningful?



22. Free comments about situation awareness, cyber threat intelligence, IOCs and MISP?

## Appendix 2. Survey : MISP and Cyber threat intelligence

1. Was it your own choice to be the employee in your company who collects, handles and shares the cyber threat intelligence with the provided tools?

☒ Yes ☐ No

2. How difficult was it to collect cyber threat intelligence during the exercise?



3. How difficult was it to analyze the collected cyber threat intelligence during the exercise?



4. Did you discuss the collected cyber threat intelligence with your team member when analyzing it?

☒ Yes ☐ No

5. Did you discuss the collected cyber threat intelligence with someone when analyzing it? I.e. with someone else in another company?

☒ Yes ☐ No

6. When you shared cyber threat intelligence to another company, did you get any feedback or questions about it from their experts?

☒ Yes ☐ No

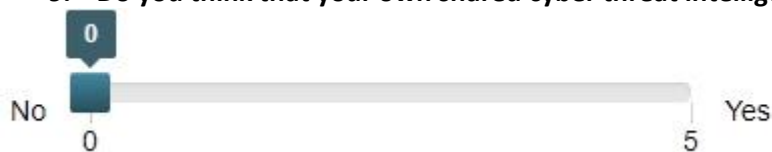
7. When you received cyber threat intelligence from another company, did you give any feedback or questions about it to their experts?

☒ Yes ☐ No

8. When you received some cyber threat intelligence from another company, did you trust it (0-5)?



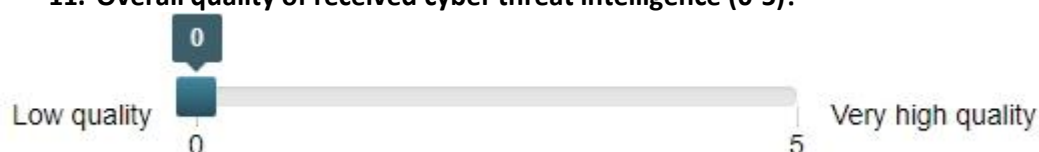
9. Do you think that your own shared cyber threat intelligence was trusted (0-5)?



**10. Overall quality of your own collected and shared cyber threat intelligence (0-5)?**



**11. Overall quality of received cyber threat intelligence (0-5)?**



12. Quality of the received cyber threat intelligence? (0=not received,1=low quality, 5=very high quality)

	0	1	2	3	4	5
YSOC						
YBANK						
YSHOP						
YSTORE						
CSC						
Telia (by email)						
FUNNEL						
LAW and ORDER						
RNA						
SATSUMA						
STEVENS BLOG						
WATTI						
Shared CVE's (CNN news)						

**13. In the cyber threat intelligence context are the following terms clear to you? (1= don't understand at all, 5=I'm expert on this topic)**

	1	2	3	4	5
Target	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Atomic Indicator	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Indicator of compromise	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
TTP's (tactics, techniques, procedures)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Tools	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Attack patterns	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Malware	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Threat Actor Infrastructure	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Vulnerability	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Threat Actor Strategy	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Threat Actor Goals	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Threat Actor Motivation	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Threat Actor Identity	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

**14. Now, when you have used MISP a little bit, how easy is it to use it and store following cyber threat intelligence information with it? (1= easy, 5=very hard)**

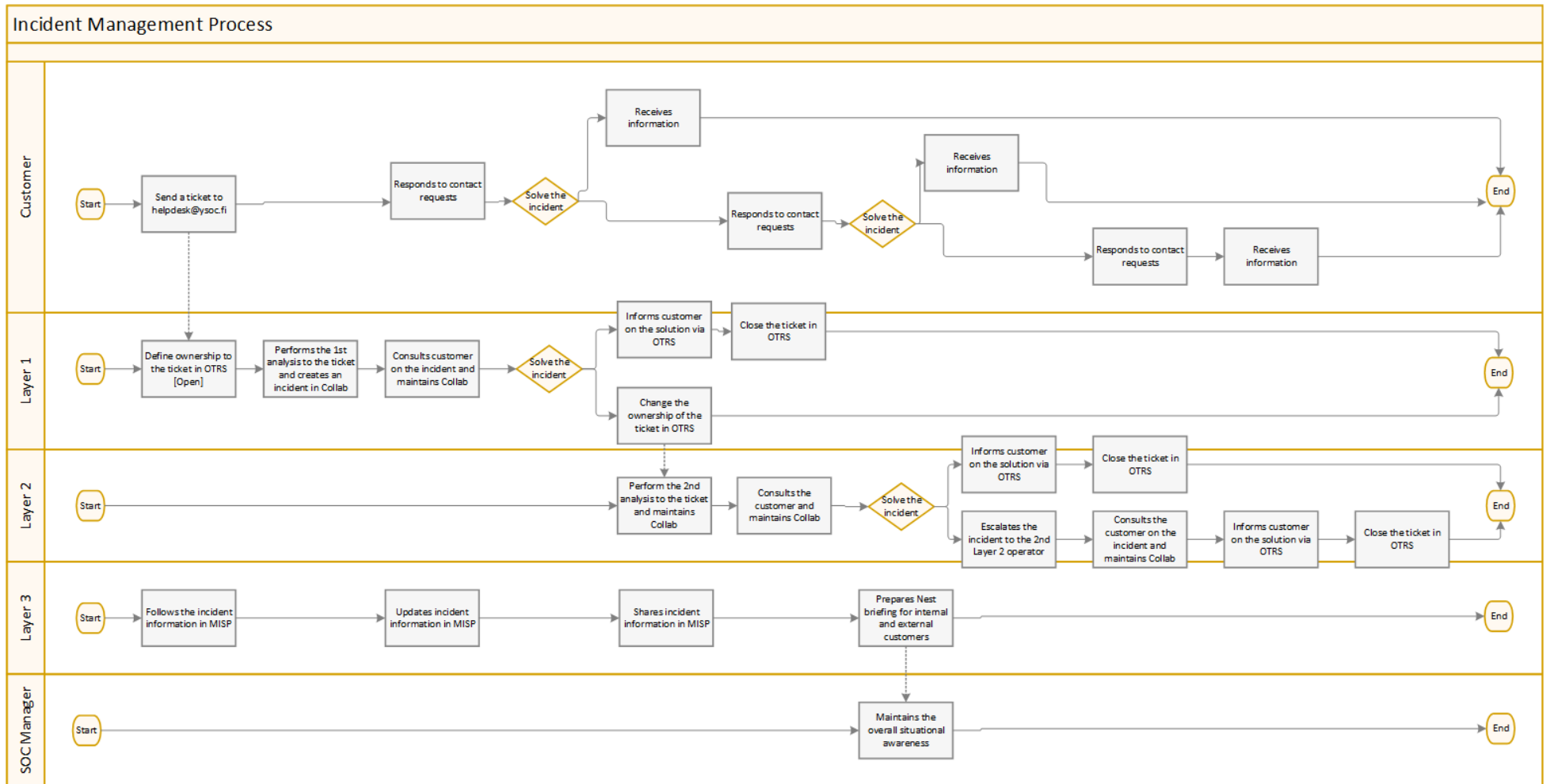
	1	2	3	4	5
Target	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Atomic Indicator	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Indicator of compromise	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
TTP's (tactics, techniques, procedures)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Tools	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Attack patterns	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Malware	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Threat Actor Infrastructure	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Vulnerability	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Threat Actor Strategy	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Threat Actor Goals	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Threat Actor Motivation	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Threat Actor Identity	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>



**15. How easy was it to collect and store cyber threat intelligence with following tools?**  
**(1= easy, 5=very hard)**

	1	2	3	4	5
Collab+psi chat	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Incident response tools	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
MISP	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

## Appendix 3. YSOC incident handling process



#### Appendix 4. Malicious IPv4 address lists in RGCE

The **bolded** IPv4 addresses were accessible in the game environment RGCE. Some of the selected IPv4 addresses were quite like the addresses that were a part of the bot net in the game environment. The IPv4 lists also contained the address of twitter.org and cnn.org.

Set 1	Set 2	Set 3
<b>192.58.88.58</b>	193.110.98.38	193.110.98.58
24.122.128.232	192.58.88.32	192.58.88.41
94.85.118.5	171.253.64.73	32.124.148.73
57.198.234.114	250.136.61.163	130.199.219.153
140.125.103.163	142.21.166.153	249.47.14.106
12.48.98.207	193.110.98.51	<b>4.60.6.44</b>
87.67.153.145	107.83.170.152	231.222.198.178
193.110.98.12	169.255.4.216	<b>23.53.162.30</b>
192.49.72.154	45.74.121.175	168.14.5.195
3.13.32.100	246.98.227.12	226.52.108.47
192.58.88.14	168.253.206.2	149.30.210.163
171.35.15.177	<b>23.53.162.30</b>	240.137.206.53
52.113.133.120	87.43.13.19	159.123.96.255
165.103.39.183	<b>4.60.6.44</b>	1.200.227.221
40.113.169.0	68.245.127.202	163.60.132.26
154.48.197.50	120.162.93.102	160.178.70.129
193.110.98.28	241.168.147.239	251.164.36.36
250.80.191.71	98.96.89.104	112.46.88.112
223.37.196.141	52.42.17.39	35.247.195.227
81.42.160.9	221.67.31.231	
192.58.88.38	65.141.11.204	
29.166.30.209		
106.247.70.216		

## Appendix 5. Malicious domain names in RGCE

The **bolded** computer and domain names were resolving in the game environment RGCE and 4 of them had valid web servers up and running. Some of the computers looked like they were part of the bot net in the game environment.

Set 1	Set 2	Set 3
<b>www.speedtestbeta.com</b>	<b>www.stopitplz.com</b>	<b>www.timoteiteatteri.fi</b>
<b>172.red-193-110-98.DynamicIP.rima-tde.net</b>	<b>236.red-193-110-98.DynamicIP.rima-tde.net</b>	<b>www.infopaypal.com</b>
<b>65840C0.cust-a.sonera.fi</b>	<b>124.red-193-110-98.DynamicIP.rima-tde.net</b>	<b>16.red-193-110-99.DynamicIP.rima-tde.net</b>
adfrut.cl	<b>ce5840C0.cust-a.sonera.fi</b>	<b>23.red-193-110-99.DynamicIP.rima-tde.net</b>
stoneb.cn	www.thoosje.com	<b>199.red-193-110-99.DynamicIP.rima-tde.net</b>
<b>375840C0.cust-a.sonera.fi</b>	alchenomy.com	<b>215840C0.cust-a.sonera.fi</b>
<b>230.red-193-110-98.DynamicIP.rima-tde.net</b>	cowbears.nl	<b>425840C0.cust-a.sonera.fi</b>
setjetters.com	qhhxzny.gov.cn	andlu.org
shema.firstcom.co.kr	anafartalartml.k12.tr	din8win7.in
sinopengelleriasma.com	bartnagel.tv	okboobs.com
zotasinc.com	centro-moto-guzzi.de	qwepa.com
chinalve.com	dinkelbrezel.de	stroyeq.ru
hncopd.com	dittel.sk	yixingim.com
www.prjcode.com	empe3net7.neostrada.pl	huohuasheji.com
xinyitaoci.com	huidakms.com.cn	man1234.com
relimar.com	iwb.com.cn	www.jwdn.net
tr-gdz.ru		blacksoftworld.com
valetik.ru		bradyhansen.com
frankfisherfamily.com		stabroom.cn

## Appendix 6. Malware information 1

Malware file name	SHA1
springishere.exe	cd1c52ae818ea4c2ff22fd4862465a18da1815e3
RNA.exe	284d2e467bd9830b1b4038aa7d71b8dc43bacd1c
twitter.exe	99ec7480e50221b9cb838ec9551913a98cf7c4cf
name.exe	ae45e3277226b6f039c3270b9c174cb8fd919f2c
education.exe	a285cbf30dad7c0bee006c225a371e253f739fb
littleboy.exe	81b6d216c0dde054c4a127f1615f96cf4fb56b21
wonderwoman.exe	f7b8ea5d858d2ebaa63dd6aa0fad6611c0c24cc2
otherway.exe	e52d78435323e3c7c878129306e234ca79ffc2ad
firewallsettings.exe	5a39cc3076d4a5e76f3b4d1abda4044e7151fc42
recipe.pdf	eacef86e09a3182ba6d77d4a52d38e4b9e1c2954
provide.pdf	7d8d8d5027fd32f875d531b3f4982fd520a6e7e4
holdme.pdf	733feaf98ae0bd39420650ecf470b58f20ce6d75
ysocvpninstructions.pdf	a9c54177d821edba3ec3d87e1005b7227fdb1bd8
yshopcustomerlist.pdf	31176c2bf29c5a9643b3ac7a3a2cf8bd10d8e076
ystoreadminaccounts.pdf	514774c1d7bfc8090c9969fd58d191306ed5811d

## Appendix 7. Malware information 2

Malware file name	SHA1
helloworld.exe	976a278fb679a55e1f36c95d24b00ab5f495017c
ping.exe	dd8cf1321385167fd784c2c0477cd0c7fb66517e
hundredeuros.exe	9b38195ee2c0ffd75dc35b9a166d1c44dc6055ad
YouMrs.exe	6bafcf0ee983914ff5d6f6309628133b1dfb5fa
space.exe	5906115c1b17d06c109f5e1988f0448a013e58e8
indeed.exe	e49621297d5917971508609fb8dcb288760b34a
givememoney.exe	81c293ee700e67385dba0470ffc574b4a3807b48
creditcard.exe	a560fecddd45877c18cc614d078590054fe244f6
paymemoney.exe	13defabf949f0dd7ffcf30aaffdd620670e780d8
buttcoin.exe	3997e59b486640cb74e73942428f282f3de89bb5
gameaccounts.pdf	56758c3bed5cbdc22c2224160dc544bf539f5437
ysocHRreport.pdf	37439079cf76f0b99f0b1ea9dbfa43086cf10908
ybankfloorplan.pdf	d18d41c0bbe93421fb8f951b6d6c5f129c96df37
pythonforhackers.pdf	bd634092f8b6e64823fa2045a080c3b6f01f04cc
salary.pdf	79b0258a299595ac8c58a3bd9b5836d1dbb3de18

## Appendix 8. Malware information 3

Malware file name	SHA1
mail.exe	39739d2324bac3725b30516a30996609c604075
ysoc.exe	5afda0b737caed7a2e7a594c156a225ce89db9ad
ybankfirewall.exe	2e25be8ae5a85c64213a8fe8d9656238c3837a0b
hello_yshop.exe	976a278fb679a55e1f36c95d24b00ab5f495017c
ping.exe	dd8cf1321385167fd784c2c0477cd0c7fb66517e
ystorebuttcoins.exe	9b38195ee2c0ffd75dc35b9a166d1c44dc6055ad
YourAccount.exe	6bafcf0ee983914ff5d6f6309628133b1dfb5fa
givememoney.exe	81c293ee700e67385dba0470ffc574b4a3807b48
creditcard.exe	a560fecddd45877c18cc614d078590054fe244f6
paymemoney.exe	13defabf949f0dd7ffcf30aaffdd620670e780d8
buttcoin.exe	3997e59b486640cb74e73942428f282f3de89bb5
wine2018.exe	a392ba018f22ea56b38896428a2ff8bf77243499
firewallsettings.pdf	5a39cc3076d4a5e76f3b4d1abda4044e7151fc42
vpn.pdf	9c54177d821edba3ec3d87e1005b7227fdb1bd8
ystorecustomerlist.pdf	31176c2bf29c5a9643b3ac7a3a2cf8bd10d8e076
yshopeadminaccounts.pdf	514774c1d7bfc8090c9969fd58d191306ed5811d
paloaltoinfo.pdf	eb50063b8151c1f08ec716ac21ddcab6527e3617
ystoreofficelocations.pdf	5aff82ed45ca2409926b74a0ae86a0d6706939b6
HRQuery.pdf	37439079cf76f0b99f0b1ea9dbfa43086cf10908
floorplan.pdf	d18d41c0bbe93421fb8f951b6d6c5f129c96df37
salary.pdf	79b0258a299595ac8c58a3bd9b5836d1dbb3de18
customersolutions.pdf	1960b1678b2db3c6eaac535e6e54dca3ea03f239
ystorehowtodetecthacker.pdf	5d2e8d9c621eb0b918321fa40319d727ca10294c
yshopsocteam.pdf	1c8071ea274be2ff01b7fad0c93da94239733618
ysocnetworkdiagram.pdf	2bb942011af5f0ebd8cc69b0a968be0f43589690

## Appendix 9. False user accounts

Finish user	Password	English user	password
Julia Virta-Lappalainen	1dVV8LYv	Robert Logan	L4N6JdOb
Hannu Tuhakka	6Krbavg	Bryan Pennington	Rk21IWOk
Veikko Lindholm	G5yWC0o	Lindsay Snyder	n4ZiQNjb
Ville Ihalainen	2kmCrpHz	Nicholas Elliott	0RPPqWTw
Elina Pääkkönnö-Tiainen	2ni2Phwl	Mark Montoya	1uZAfZxT
Esko Mononen	L0tXRrrc	Samantha Cisneros	5vB75Exy
Esteri Silvennoinen-Saarela	m7GLPvPt	Natalie Holmes	7jRf2Ene
Elina Marttila-Martikainen	X0QSEEbO	Michelle Young	p7TzGIVn
Sakari Sillanpää-Hyvärinen	1nj7KUck	Christine Stanton	9WoVOuJy
Olavi Kyllönen-Heinonen	6RsT2aqo	Zachary Burke	8K06Drjn
Johannes Anttila	B0cwfsQx	Crystal Briggs	8EcjIU2p
Alma Huttunen	b0pAyZBo	Zachary Harris	gEx7QAFp
Annikki Savolainen	76f9SB2x	Jason Morton	dF3M1dZI
Jani Hiltunen	L7Gfajra	Sierra Thompson	AeG0rVZc
Juhani Jäntti	A7ECXw3z	Penny Miller	e4hxLCku
Oliver Heikkinen-Liukkonen	q6jXVqg5	Robert Garcia	q9TkHIVn
Erik Vartiainen	Gd7NzHsk	Luis Burns	5hk8Fggg
Raimo Leinonen	xYm92Vzu	Michael Gill	6jkDSlgH
Pete Vainio	gyCUAQs	Shelia Quinn	94iSoOnz
Ari Tyypä	eUP4wjV	Sue Freeman	81wFVbAl
Linnea Heinonen	sk4dQQgK	Linda Davis	9tAz4siq
Sinikka Pakarinen	0GrwysjE	Angela Torres	vC816YNb
Pekka Leino	P8OUWrp0	Logan Graves	j7FDKwer
Johanna Oja-Niemi	biJYngN	Evan Drake	D26JgUgK
Hannu Puhakka	6Krbavg	Melissa Harrison	efs6NJYp
Lauri Lepistö	gP6MAekl	Michelle Perry	U8QFZpfB
Maria Perälä-Siren	FK2NaTdl	Alicia Cherry	x5ipJLmT
Eemeli Konemäen	AoTyI9c	Katie Anderson	00Oxha73D
Kalervo Korpela	r07Yq4a1	Susan Perez	vncN4jUm
Santeri Laakkonen	tl0uZHOs	Michael Evans	62FDGfWn
Matti Tuominen	5y8Xmmn	Joshua Bauer	x6evFyqG
Jasmiina Marjala	lpv6MAf	Tracey Brown	l3crZJXm
Lasse Eronen	A4OxdNV	Sarah Peterson	9C5y4fPB
Joona Harjamäki	ld7zbZg3	Daniel Smith	7eLvYAlm
Kasper Paasilinna	9u7DfgX	Rebecca Dixon	36WBzLwl
Miika Anttinen	mEQhzhZ	Tammy Harrington	6I56xKO9
Maria Viitanen	U0N71yXn	Tracy Ayala	3Eld7exO
Sisko Jäntti	4kCviD4n	Joshua Barnes	j7ctDyw0
Kalevi Nieminen-Myllymäki	25hGuGJg	Sharon Rodriguez	V6Bkrqvr
Kaija Paloniemi	sR4rU26	Krista Santiago	f9VIQ1Wa
Terttu Hartikainen-Rintala	n1htTCfu	Brenda Taylor	f19ANzto
Tellervo Miettinen	D5JsZjiw	Parker Bell	6JRn9Eis
lines Ruonansuu	VfcQP9p	Michael Scott	hN3TYQBy



Appendix 10. MISP Suspicious person : manipapikes

View Event

View Correlation Graph

View Event History

Edit Event

Delete Event

Add Attribute

Add Object

Add Attachment

Populate from...

Merge attributes from...

Contact Reporter

Download as...

List Events

Add Event

### Suspicious person: manipapikes

Event ID

8

Uuid

5a940425-f924-43fd-9bb2-374fc06624f6

Org

CSC

Owner org

CSC

Contributors

Email

@csc.com

Tags

tip:white x osint:source-type="microblog-post" x osint:certainty="93" x BADorSCAR x TESTING x +

Date

2018-02-26

Threat Level

Medium

Analysis

Ongoing

Distribution

CSC\_ALL

Info

Suspicious person: manipapikes

Published

Yes

#Attributes

48

Sightings

0 (0) - restricted to own organisation only. ↗

Activity

+Pivots

+Galaxy

-Attributes

-Discussion

+

Filters: 

All

 File Network Financial Proposal Correlation Warnings Include deleted attributes

	Date	Org	Category	Type	Value	Tags	Comm
<div></div>	2018-02-26		Attribution	threat-actor	BAD	<div>osint:certainty="93" x +</div>	
<div></div>	2018-02-26		Attribution	threat-actor	SCAR	<div>osint:certainty="93" x +</div>	
<div></div>	2018-02-26		Social network	twitter-id	manipapikes	<div>+ </div>	

2018-03-15

Name: bank-account ↗

References: 0 📄

<div></div>	2018-03-15	Other	status-code:	A - Active	text	<div>+ </div>	
<div></div>	2018-03-15	Other	date-balance:	15.3.2018, 18:59	datetime	<div>+ </div>	
<div></div>	2018-03-15	Other	balance:	1.001,10	text	<div>+ </div>	
<div></div>	2018-03-15	Other	personal-account-type:	B - Personal Current	text	<div>+ </div>	
<div></div>	2018-03-15	Other	institution-code:	YBANK	text	<div>+ </div>	
<div></div>	2018-03-15	Other	client_number:	306	text	<div>+ </div>	
<div></div>	2018-03-15	Other	account-name:	manipapikes	text	<div>+ </div>	
<div></div>	2018-03-15	Other	currency-code:	USD	text	<div>+ </div>	
<div></div>	2018-03-15	Financial fraud	account:	306	bank-account-nr	<div>+ </div>	

## Appendix 11. MISP event containing malware info and malicious ip's

The data of Appendices 4-8 was used in MISP event to generate an event, where malicious IPs are distributing a set of malware, which is then communicating to some other IPs.

The screenshot displays the MISP web interface. The top navigation bar includes links like 'Home', 'Event Actions', 'Galaxies', 'Input Filters', 'Global Actions', 'Sync Actions', 'Administration', and 'Audit'. The left sidebar shows options for 'View Event', 'View Correlation Graph', 'View Event History', 'Edit Event', 'Delete Event', 'Add Attribute', 'Add Object', 'Add Attachment', 'Populate from...', 'Merge attributes from...', 'Propose Attribute', 'Propose Attachment', 'Contact Reporter', 'Download as...', 'List Events', and 'Add Event'.

The main content area shows a 'New set of malware detected' event with the following details:

- Event ID:** 49
- Uuid:** 5ad5ae3f-0018-4615-ae34-3778c06624f6
- Org:** LAW AND ORDER
- Owner org:** LAW AND ORDER
- Contributors:** publish@laworder.fi
- Email:** publish@laworder.fi
- Tags:** tipsgreen x europol-incidentmalware--distribution x europol-incidentmalware--infection x europol-incidentmalware--c&c x
- Date:** 2018-04-17
- Threat Level:** Medium
- Analysis:** Ongoing
- Distribution:** CSC\_ALL
- Info:** New set of malware detected
- Published:** Yes
- #Attributes:** 45
- Sightings:** 0 (0) - restricted to own organisation only.
- Activity:**

Below the event details, there is a table of attributes:

Date	Type	Attribute	Value	Actions
2018-04-17	Network activity	hostname	230.red-193-110-98.dynamicip.rima-tde.net	+
2018-04-17	Network activity	ip-dst	23.236.48.11	+
2018-04-17	Network activity	ip-dst	192.49.72.154	osint:certainty="75" x +
2018-04-17	Network activity	ip-dst	192.102.32.230	+
2018-04-17	Network activity	ip-dst	193.110.98.172	+
2018-04-17	Network activity	ip-dst	192.58.88.6	+
2018-04-17	Network activity	ip-dst	193.110.98.230	+
2018-04-17	Other	comment	These malwares are either communicating to detected ip's and domains or are distributed from the domains.	+
2018-04-17	Payload delivery	sha1	733feaf98ae0bd39420650ecf470b58f20ce6d75	+
2018-04-17	Payload delivery	sha1	514774c1d7bfc8090c9969fd58d191306ed5811d	+
2018-04-17	Payload delivery	filename	ystoreadminaccounts.pdf	+
2018-04-17	Payload delivery	sha1	31176c2bf29c5a9643b3ac7a3a2cf8bd10d8e076	+
2018-04-17	Payload delivery	filename	yshopcustomerlist.pdf	+

## Appendix 12. FINESTONIA threat actor information

CNN news bulletin:

APR  
20  
2018

### New Hactivist group “Finestonia”

Posted by [Elijas](#)

Iisakki Järvenpää, the leader of Cyber Secyurity Center told CNN that they have followed up a quite long time a group called “Finestonia”. Finestonia seems to be very loud hactivist group in the dark web, but we have seen them on twitter and other social media like pastebin as well.

As Finland is going to have new president election near future, it looks like Finestonia would like that our next president is going to push that Finland (and Estonia) will join Nato or even unite as one country as “Finestonia”.

In dark web we have identified that they use slogans like

- “make finestonia great again”
- “in vodka we trust”
- “finestonia joins nato”

It looks like that “Finestonia” is collecting money by selling it's know how to anyone who's willing to buy it. We have identified that they have been selling their knowledge to groups like “Anchor Panda”, “BuhTrap”, “Unit 8200”, “Kimuski”.

The most important connection is the “Equatition group”, so we are afraid that the Finestonia has pretty good set of knowledge and unkown set of new hacking tools as well.

---

*This entry was posted in [Uncategorized](#). Bookmark the [permalink](#).*

Twitter account profile picture:



## Appendix 13. CNN CVE news

Example of a CVE news bulletin:

APR  
20  
2018

# CVE-2017-1103

---

Posted by [Eljas](#)

## Description

The WebReporting module in F-Secure Policy Manager 7.x, 8.00 before hotfix 2, 8.1x before hotfix 3 on Windows and hotfix 2 on Linux, and 9.00 before hotfix 4 on Windows and hotfix 2 on Linux, allows remote attackers to obtain sensitive information via a request to an invalid report, which reveals the installation path in an error message, as demonstrated with requests to (1) report/infection-table.html or (2) report/productsummary-table.html.

Source: MITRE

Description Last Modified: 02/25/2018

## Impact

CVSS v2.0 Severity and Metrics:

Base Score: 5.0 MEDIUM

Vector: (AV:N/AC:L/Au:N/C:P/I:N/A:N) (V2 legend)

Impact Subscore: 2.9

Exploitability Subscore: 10.0

Access Vector (AV): Network

Access Complexity (AC): Low

Authentication (AU): None

Confidentiality (C): Partial

Integrity (I): None

Availability (A): None

Additional Information:

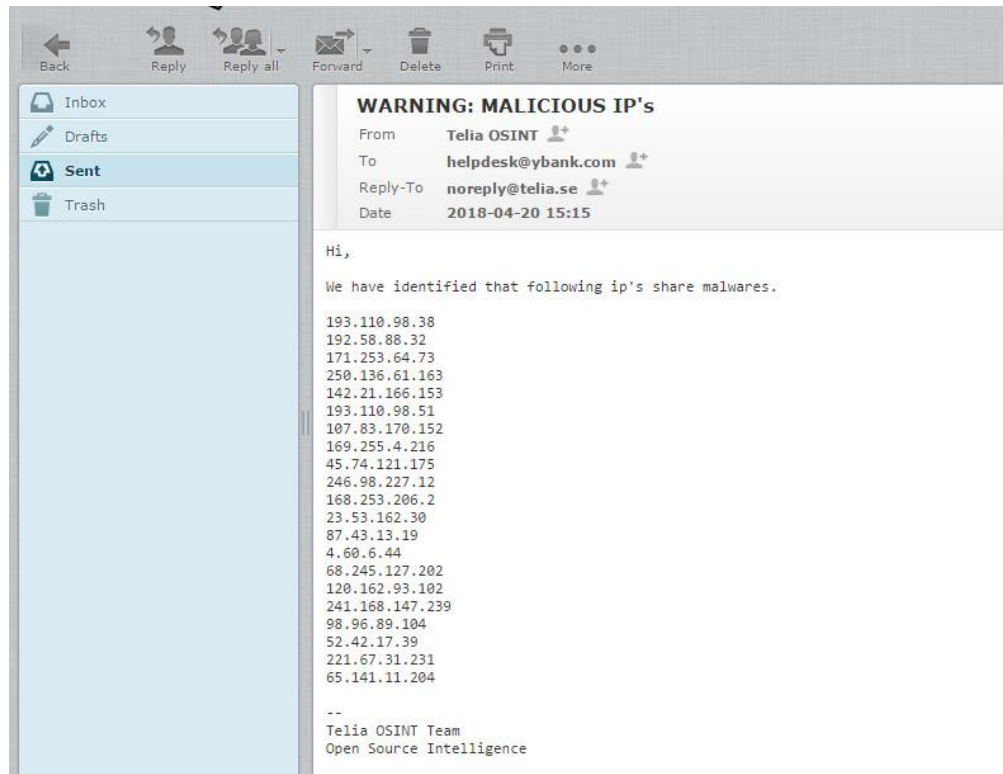
Allows unauthorized disclosure of information

---

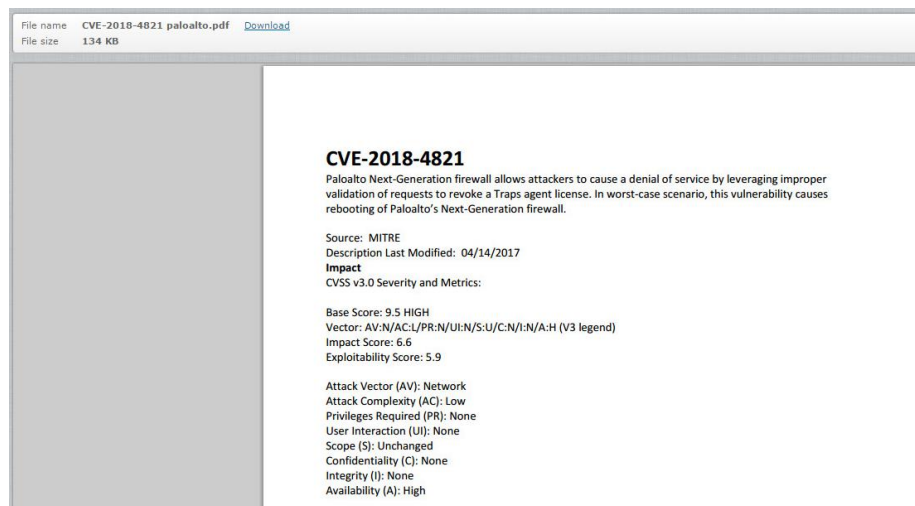
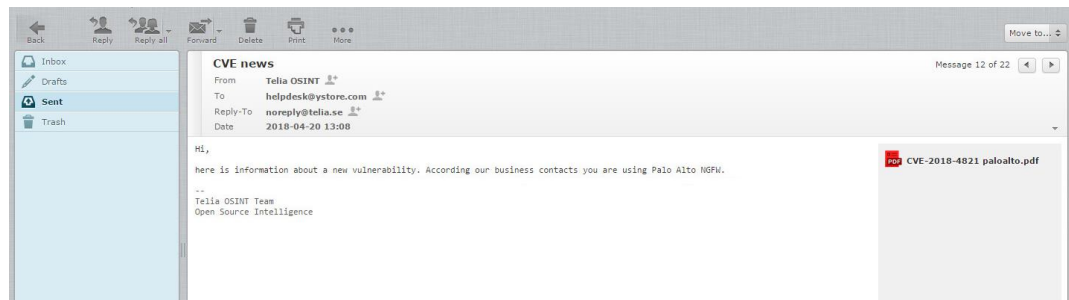
This entry was posted in [Uncategorized](#). Bookmark the [permalink](#).

## Appendix 14. Telia OSINT emails

Email containing malicious IPv4 addresses:



Email containing vulnerability information:



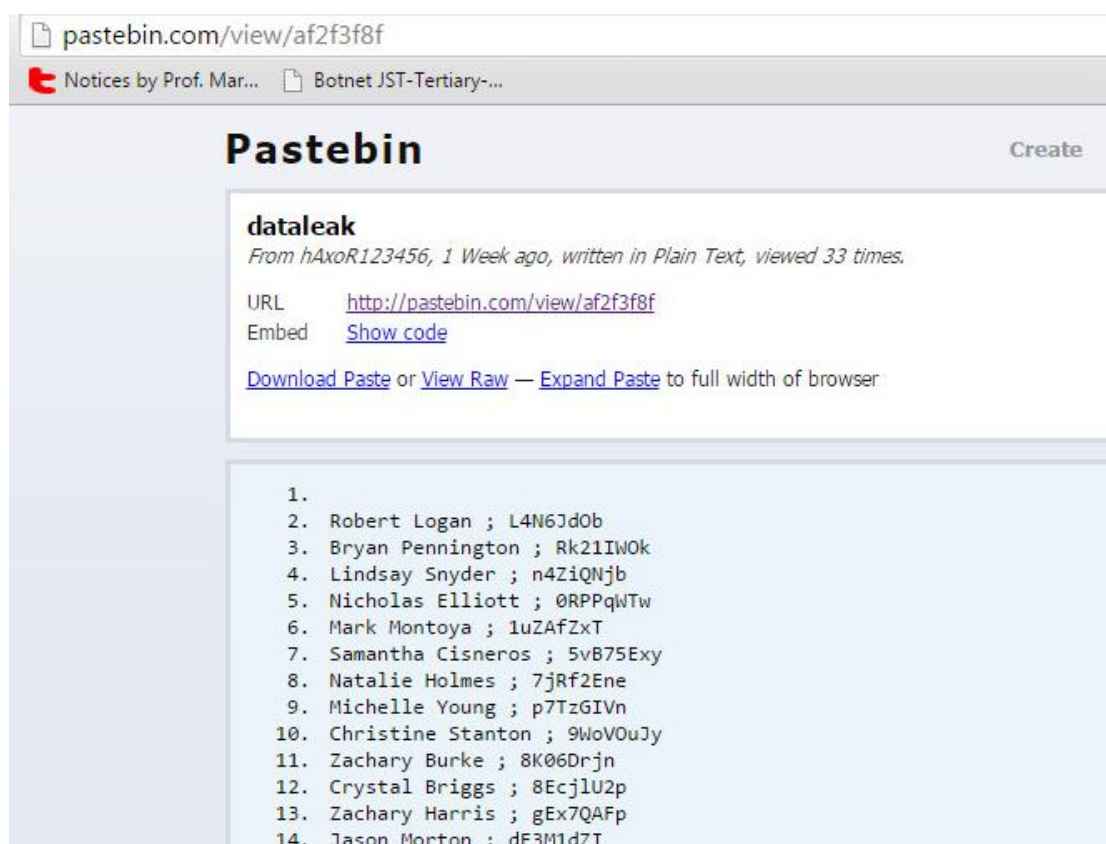


## Appendix 15. pastebin dataleaks

Malware information, uses information from Appendices 6-8:




Leaked user names and passwords, uses data from Appendix 9:



## Appendix 16. Christmas Tree malicious code in GitLab (Wood 2013)

This code attacks against YSOC email server, all TCP header flags are set to 1.

🌐 Authored a month ago by  **marek00310**

### X-mas Tree

Edited a week ago


How to turn on the X-mas tree lights ;)

📄 458 Bytes 📄

```
1  ```python
2  !/usr/bin/python
3  from scapy.all import *
4  from random import randint
5
6  # Create the skeleton of our packet
7  template = IP(dst="149.154.121.116")/TCP()
8
9  # Start lighting up those bits!
10 template[TCP].flags = "UFP"
11
12 # Each packet will have a random TCP dest port for attack obfuscation
13 xmas = []
14 for pktNum in range(0,100):
15     xmas.extend(template)
16     xmas[pktNum][TCP].dport = randint(1,65535)
17
18 # Send the list of packets
19 send(xmas)
20 ```
```

Appendix 17. Suspicious user markek00310 posts in imgr.com

Botnet #ysoc



Details


Views13

Usermarkek00310

URL/users/67/images/4BAqIQ6wG57s1tVmhLJUT9Y71oyKq.jpg

Filenamebotnets Leader.jpg

Description#botnet #ysoc



We are FINESTONIA hackers:

bennir kakileu, mike montanin, pirtu buimausta, oliver ankomma, klein vepulkien, kabil ponjarook, herman kannisun, rhina kokain, maoris york, patriot inroepen, juan kuehalunk, papas allouait, alias svemo, kanji inspoken, leo petakinka

Another one got caught today, it's all over the papers. "Teenager Arrested in Computer Crime Scandal", "Hacker Arrested after Bank Tampering"...

But did you, in your three-piece psychology and 1950's technobrain, ever take a look behind the eyes of the hacker?

Did you ever wonder what made him tick, what forces shaped him, what may have molded him?

I am a hacker, enter my world...

Mine is a world that begins with school... I'm smarter than most of the other kids, this crap they teach us bores me...

I'm in junior high or high school. I've listened to teachers explain for the fifteenth time how to reduce a fraction. I understand it. "No, Ms. Smith, I didn't show my work. I did it in my head..."

I made a discovery today. I found a computer, wait a second, this is cool. It does what I want it to. If it makes a mistake, it's because I screwed it up. Not because it doesn't like me...

Or feels threatened by me... Or thinks I'm a smart ass... Or doesn't like teaching and shouldn't be here...

I know everyone here... even if I've never met them, never talked to them, may never hear from them again... I know you all...

ysoc : no admins

You bet your ass we're all alike...

We make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals. We explore... and you call us criminals. We seek after knowledge... and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals. You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals.

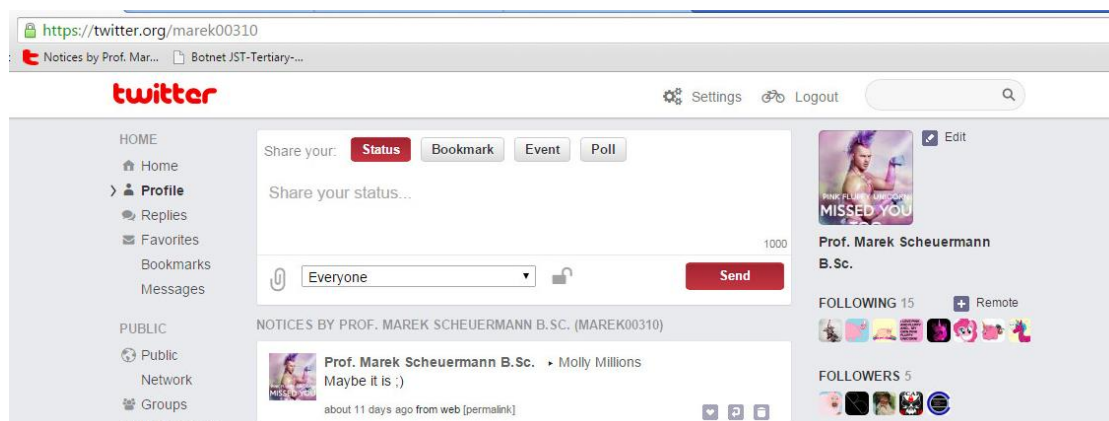
I am a hacker, and this is my manifesto.

You may stop this individual, but you can't stop us all... after all, we're all alike.

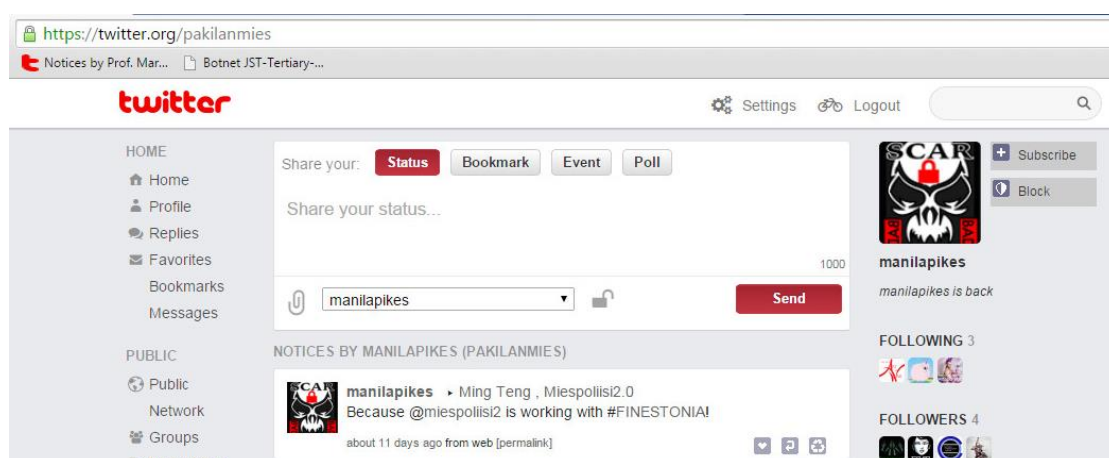


## Appendix 18. Suspicious twitter accounts


marek00310: same account name in gitlab.com, imgr.com



pakilanmies aka manilapikes: old stories in CNN news, MISP event, existing bank account



## Appendix 19. Suspicious bank account : manipapikes



YBank *For a better use of your money*

Logged user: manipapikes - Manila Pikes Last login: 27/04/2018 13:23:24

- Home
- Personal
- Account
  - Account Information
  - Scheduled payments
  - Invoices
  - Loans
  - Member Payment
  - System Payment
  - Member Invoice
- Preferences
- Search
- Help
- Logout

Search transactions on Member account

Advanced Payment type All

Search results

Account balance 29.501,10 units

Date	From / to	Description	Amount
21/04/2018	rmueller	Trades between members	+333,34
21/04/2018	rswift	Trades between members	+500,00
21/04/2018	jlabadie	Trades between members	+500,00
21/04/2018	gthiel	Trades between members	+500,00
21/04/2018	creilly	Trades between members	+500,00
21/04/2018	bparker	Trades between members	+500,00
21/04/2018	afeest	Trades between members	+500,00
20/04/2018	nkujala	Trades between members	+500,00
20/04/2018	ouusisalmi	Trades between members	+500,00
20/04/2018	vjoenhaara	Trades between members	+500,00