Design, Build an Effective Evaluation and Monitoring Solution

AKM HASAN

Student ID – 9755484

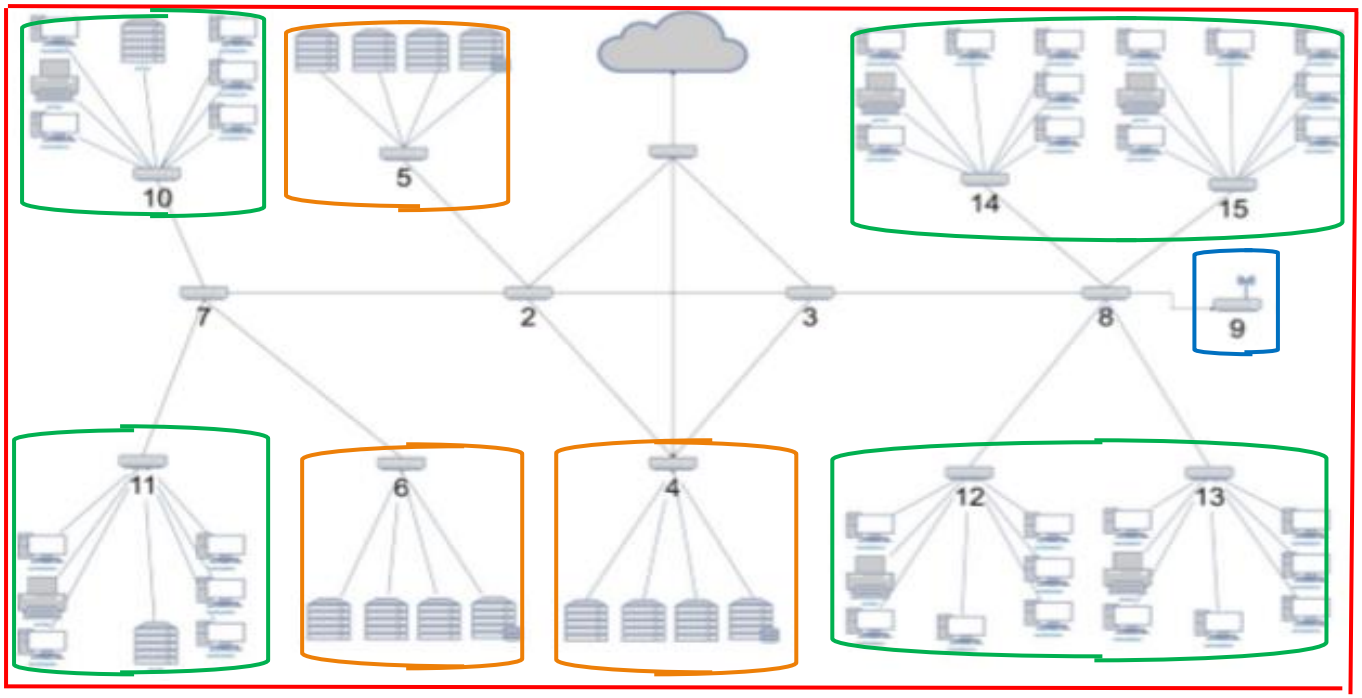
hasana19@uni.coventry.ac.uk

MSc Cyber Security – Coventry University

7025CEM - Intrusion Detection and Response

Dr. Christo Panchev

Coursework Due Date: 14 Dec 20



1. I am going to handle a client network; therefore, I would design and build an effective evaluation and monitoring solution for Clint. As a network security evaluation specialist, I will analyse, elucidate, and address those issues below, which raised by the client.

We must remember it is a very busy, non-stop, and high-volume data centre. Also, this network owns all the data created, processed, stored, and communicated on the network system is official, official-sensitive, and protected.

To detect any such type of attacks, it is important that the organisation has effective measures in place, and they have got a very efficient SoC team. Before doing

anything, I would like to ask the client's SoC team to use colour zones methodologies to help them and divided the infrastructure into the **Red**, **Green**, **Orange**, and the **Blue** Zone.

Most of the time the attack will come from the outside of this network (client network), which is Red. I would advise them to spend a lot of time defending their boundary between ethos and the outside world. The three servers' farms are in the **Orange** zone vie respective gateway nodes numbered **4, 5**, and **6**. This is because they must receive the connections from the **Red** zone. These are issues as they are a nice fascinating target for somebody from outside the network trying to compromise the system. Looking at the **Orange** zone does not mean what is happening in the client network.

In theory, the **Blue** zone is node **9** is a series of APs providing Wi-Fi networking of the offices, but the SoC team must know the signal will go well beyond the walls of the building. So, this has to potential to reconfirmation and to react as an entry point to the network, which is node **1** or the main entry point of the network.

The **Green** zone is located inside the office or we can see in the picture (figure 1), the gateway **10 – 15** connected to the client nodes distributed across subnets. The organisation staff and the SOC team could think this is completely safe, as it is mostly a restricted part of their network, but an insider attack is a very real issue. Some of the insider attacks might be because of human error and some might be corporate espionage! Regardless of which it is, I need to help the SoC team to protect this part of the infrastructure as well. *(Idea from course materials, Day 2 -1, the big question)*

Firstly, I would advise to set up a stronger Network Security Monitoring (NSM) process, the SoC team of the organisation can work as an NSM team, and the NSM will be the only process of collection and analysis of the client network traffic and endpoint events in order to detect and respond to intrusions.

However, I would advise the SoC team to collect "full packet data" and the data sources are network-based. Because full packet data is the most complete collection of network traffic, it contains raw data and whole packets, we can say packet header and payloads have in this data. It will give the SoC team more flexibility to analyse and further investigate if be needed. Also, if we need "session data" or "statistical data" for an investigation, we can extract from "full packet data"

Furthermore, the client has a lot of resources including the specialist hardware and more than enough space to collect "full packet data" merely my job to help them to identify that a live intrusion incident, where they can actively monitor the intruder or intruders with the aim of finding out where they are and what their intention to do.

I would advise the SoC team to collect "full packet data" from their specific segment of the network, which is node **4** or **5** within their three server farms.

Alongside this, it is (full packet data) very attractive for the insider attacker to collect and use such data for malicious purposes or supply to other nations/ espionage to

organise a sabotage attack to the client network. That is why the SoC team needs to keep on eye within the organisation as well.
(Ideas ScienceDirect – Full Packet Capture, a few ideas from 7025CEM community discussion (anticipation the topic), an idea from the course materials Day 2-1, first three-part and own evaluation)

To support this the SOC needs to consider two main areas are, Sensor positioning for seeing all relevant traffic, and analysis and correlation tools for collect, analyse and correspond the information extracted from the traffic and endpoint event.
I would say the SoC team to enable Switched Port Analyser (SPAN) is the best option for the current situation. SPAN takes benefit of the port mirroring of the network switch where the traffic from one or more ports can be copied into a single mirror port. SoC team can then connect their network intrusion detection system (NIDS) to the mirror port and collect and/or analyse all the traffic.

Another significant benefit of SPAN is it does not require extra hardware and we can configure this from a remote location; the cost will be very consuming resources from the existing infrastructure (switch).

Now, my one of the big priorities is to collect information from the endpoint and that is why I would suggest the SoC team for ESM, SoC team would install sensors on endpoints or at least one of the nodes **4, 5** or **6** (figure 1 picture) and their workstations having access to the critical assets and pull relevant event data; it could become from OS, application logs, host-based firewall, etc.

In addition to all this, I would not leave the option behind the security information and event management (SIEM); in order to implement SIEM, I would always prefer ELK, it integrates three open-source projects: Elasticsearch, Logstash, and Kibana. Elasticsearch is a powerful analytics and search engine that has been deployed in many large-scale projects thus far. It is scalable and fast, document-oriented NoSQL providing full text and structured search. *(This specific paragraph quoted from the course materials, Day 2-1, part 5, ELK to evolve own idea in order to synchronise the answer with rest of the research)*

Finally, I need to go through with the SoC team because this is a robust, high-volume network, and parts of it get very at pick times. Any activity of collecting traffic from the network would be really challenging; therefore, in the circumstance of the above activities, it would require a huge processing period of time in peak time (day time), so I strongly believe, it is better to collect data in off-peak time or in special circumstance (very emergency) if the higher authority of client network allow to stop other actives within the network until the investigation to be finished and then we can collect data in peak time, but it needs to be filtered before it is stored.
(Sciencedirect.com. 2020. *Full Packet Capture - An Overview | ScienceDirect Topics*. [online] Available at: <https://www.sciencedirect.com/topics/computer-science/full-packet-capture> [Accessed 10 November 2020])

2. I would set up a stronger Network Security Monitoring team in order to analysis of this network traffic and endpoint events in order to detect and respond to intrusions.

At this point, the SoC team can extract both data (Session and statistical) from their "full packet data" collection. But, if I must choose between "session data" and "statistical data", I will go for statistical data collection, reason, this specific data gives the SoC team an idea about intruder intention by giving details in the packet headers. This data further reduces the amount of information we collect, but not only packet headers but also, by collecting and storing some statistical information about the traffic. The "statistical data" literally is will depend on the client networks environment that SoC is monitoring, for the infrastructure and potential threats.

It does not mean the "session data" is in a very bad position, as the "session data" contains information about a TCP session of a communication exchange. This data is simply a way to store data for individual users against a unique session ID. Session IDs are sent to the browser via session cookies and ID is used to retrieve existing session data; also, this data follows a simple workflow. When it (session) started PHP will either retrieve an existing session using ID passed. *(ideas-right.co.uk and ww.php.net)*

"Session data" allows the SoC team to see overall communication and any kind of activity patterns of potential or actual intruders i.e. where and when?

To the end, the critical step of NSM is the collection of network traffic and endpoint events; especially, the quality and completeness of the data the SoC team will collect are vital for the success of the later detection and response phases. With the discussion of both forms of data, I can say that if the NSM keeps collecting "session data" and "statistical data" and analyse, it must help for detection intruder and response very quickly.

In figure **1**, I would like to advise the SoC team to collect data from nodes **1, 5,** and **15,** the reason behind, node **1** is the main gateway node and they (SoC) need to make sure that is more secure. The first most likely target would be gateway **1** for the attackers or espionage, and gateway node **15** is the connect to clint nodes; therefore, the SoC team can monitor most of the endpoint activities if intruder attempt to do something bad and finally, gateway node **5** is one of the servers within three servers at the client network.

The SoC team can extract the "statistical data" from the previous collection, and they (SoC) can use various tools and configure in their network. Statistical data collection and analyse normally involve some statistical tools; there are various software packages to perform statistical data analysis. I can talk about a few software, i.e., **Stat, Soft**, etc.

To the end, there are several factors the SoC team need to consider when deciding what data, they are going to collect and how they are storing, including how useful the data is for the analysis, how they are going to process it, as well as related legal and ethical issues; so, it is better always let the client network to follow their own methodology and governance.

3. A senior network administrator of the client network is considering deploying various packets filters across the network to help minimise undue traffic and prevent exposure of critical services, but she has asked me for advice on the choice between Snort and Suricata. We all know they are both widely known products available for deployment as IDS and more.

However, Snort is the foremost popular open-source Intrusion Detection System/ Intrusion Prevention System (IDS/IPS) in the world, it is now developed by Cisco. Snort IPS is rule-based, and its real deployment is only as effective as its rules data set. This IPS uses a series of rules that help elucidate malicious network activities, and those rules to find packets that match against them and its internal system raise an alarm its users. *(www.snort.org)*

I can give an example is, tcpdump a packet sniffer, as a packet logger, which is helpful for network traffic debugging if be needed. *(www.snort.org)*

Furthermore, we can download and configure it (Snort) for any personal and business use. There are a few freely available rules data sets and some commercial ones that provide more extensive coverage, as well as being able to detect the latest types of attacks; when it is downloaded and configured, we can set up Snort rules by two sets. These are Community Ruleset and Snort Ruleset, but if we think about its authenticity, then we can see that it has been approved by Cisco Talos; their subscribers would receive the ruleset in real-time as they would release for their (Cisco) customer.

Alongside this, if we think and talk about Suricata, it is a free, opensource, mature, fast robust, and signature-based Intrusion Detection System/ Intrusion Prevention System (IDS/IPS). Suricata's functionality is very similar to Snort. But this detection engine has a different architecture, which can give us a lot of supremacy; for example, the multi-threaded option makes this engine highly scalable. This engine (Suricata) can use hardware acceleration; therefore, it is capable of real-time intrusion detection (IDS), and in order to intrusion prevention (IPS) and help the SoC team for network security monitoring (NSM).

The interesting point of Suricata is, it can support to SoC team to extract data from the monitored traffic i.e. file, SSL certificate, etc. Which the SoC team of client network can use for a firm investigation; also, this engine inspects network traffic using a powerful and extensive rule and signature language.

Moreover, if I talk about Suricata, it has standard input and output formats with tools like existing SIEMs, Kibana, and other databases become effortless; I would say, this engine is a fast-paced community-driven development, which only focused on security and efficiency. It utilises Netmap to enhance performance and minimise CPU utilisation. *(Suricata. 2020. Suricata. [online] Available at: <https://suricata-ids.org/> [Accessed 10 November 2020])*

"The Suricata project and code is owned and supported by the Open Information Security Foundation (OISF), a non – profit foundation committed to ensuring Suricata's development and sustained success". *(Suricata. 2020. Suricata. [online] Available at: <https://suricata-ids.org/> [Accessed 10 November 2020])*

Now, if I do compare Snort and Suricata I have to say, one of the main benefits of Suricata, this is developed recently than Snort; therefore, many features are on board those are vitally unmissable nowadays. One of my most favourite features is, it supports multithreading, which Snort does not support, no matter how many cores a CPU contains, it is (Snort) only can support a single core.

After all those elucidations above, I would advise the senior network administrator of GCHQ to implement Suricata in order to achieve a great result for IDS/ IPS.

4. As a network security evaluation specialist, I would advise the IT team of the client network to use ITILv4, because it is the new version of ITIL.

However, before discussing anything about ITILv4 or how this ITIL help the system, we investigate it why ITSM, why any change will have an impact on the rest of the business; its negative and positive site; and finally, I would come back to the ITILv4 that how the use of ITIL (we need to choose, which one) can help the system of this network and how the system can help the client better implement of ITIL?

Those who we work in the Cyber Security department have an interest in the technical aspect of the role, but merely as important are the process and procedures we follow to ensure that our network systems/ IT systems are in a good condition in order to fulfil the organization's demand. To achieve this is to realise we are not managing the IT system; however, if we really want to find out what is the ITSM, I will say that a useful way of thinking of an IT service that adds value to the organisation, or it is processed.

But ITIL is Infrastructure Library, which created for ensuring better use of IT services and resources. Now we can come to the point is, one of the strengths is ITIL's flexibility, but in some areas, we can see as a weakness, as it can lead to uncertainty and it cannot explain what exactly needs to be done.

At this point, I would like to say the ITIL designed to help network IT teams implement utilise all the best practices in order to deliver its IT service; also, it can be implemented to help improve the client network's SoC team.

But this is not the case, still, there is a question about using the ITILv3 and ITILv4. We all know by now, ITILv3 is the previous version of the standard and this is the most common one for its use; it last updated was in 2011. The ITILv3 covers understanding for the IT customers, ITILv3 meets the customer's needs, but its IT capabilities and some resources required to develop in order to execute them (those offerings) successfully.

Whereas ITILv4 is major mend of ITIL. It makes the framework nimbler and incorporates ideas from the previous version. It is (ITILv4) pretty much like ITILv3 except for several key deferences.

I can say, "The service value system (SVS) is a key component of ITIL 4, which facilitates value co-creation. The service value system (SVS) also can create value for those organisations". (Axelos.com. 2020. *From V3 To 4 – This Is The New ITIL | AXELOS*.

[online] Available at: <https://www.axelos.com/news/blogs/february-2019/from-v3-to-4-this-is-the-new-itil> [Accessed 10 November 2020])

ITILv4's continual improvement is very similar to ITILv3 (CSI stage); but now, if I talk about the process of ITILv4 it's 8 more processes than ITILv3, as ITILv3 was 26 process and 34 practice for ITILv4 in order to achieve its object.

Furthermore, I would like to say a holistic approach to service management is key in ITIL 4. It defines four dimensions, and the four dimensions are:

•Organizations and people
•Information and technology
•Partners and suppliers
•Value streams and processes
(Axelos.com. 2020. *From V3 To 4 – This Is The New ITIL | AXELOS*. [online] Available at: <https://www.axelos.com/news/blogs/february-2019/from-v3-to-4-this-is-the-new-itil> [Accessed 10 November 2020])

To the end, I would say to the IT team of client network to use ITILv4, as it is the latest version and will help IT system of this network the system can help the client better implement of ITIL.

5. I would like to advise and want to give a firm recommendation of Artificial Intelligence (**AI**) to determine if the client network system is working according to specifications and goals.

IBM was the first company that proposed **AI** and they suggested four properties are, self-configuration, self-healing, self-optimisation, and self-protection. *(These four properties above ideas have taken from Dr. Christo's question on AULA, Day 5-2, "putting it together" and https://link.springer.com/book/10.1007%2F978-1-4471-5007-7).*

Now we can say the **AI** is intelligence demonstrate by machines, exactly like the human autonomic nervous system, which is outside of human control, so we could think of it as intelligence. However, when we look to the data centre, it maintains and protects by human operators; that is why it is reasonable to turn this field of **AI** to innovative technologies and ideas in order to achieve our aim of autonomic computing.

Day by day, these machines become increasingly capable. If I give my concern the client, they should think with respect to the qualifications of the tester, I have to say that in the **AI** system, an agent, in this factor, is a piece of software, normally relatively small, that is autonomous. This is means we do not tell the system (basically an agent) what to do, but the system decides and performs what to do and when to do, as it makes its own decision to perform a particular task.

There are many types of agents, i.e. Simple reflex agent, Model-based reflex, Goal-based agents, Utility-based agents, but when we talk about the Learning-based agents, I can say, it can learn new knowledge about its environment, and it knows how it interacts. It also can change its behaviour and can observe the effects of any current task.

Undoubtedly, I would say, this **AI** system one of the great tools with its innovative experience it is perfect for the job in this IT system. One of the great advantages is its speed, as it is a very quick response for any simple solution and another one is the property of emergent behaviours.

Alongside the **AI**, **APT** attacks are increasing threat, as I can see that some years ago, most of the cyber-attacks was based on malware camping, but nowadays the attackers and intruder had changed their pattern, and we are now quite effective at defending against these kinds of the incident and sophisticated attack. But nowadays, we would try to implement tools, tactics, and procedures (TTP), and this is we have got from cyber threat intelligence (CTI); it allows us to move from the passive mode to proactive defence mode, technically a one step ahead than the attackers.

Now in order to protect the critical asset like this client network, the work on defining the CTI objectives will start identifying potential risk and any impacts of this organisation, but this depends on the network's aim that what they want to be protecting, i.e. sensitive data, intellectual property, critical investiture or the high volume top-secret data.

I would say, does not matter how sophisticated the client network's attack prevention system is, it is merely a matter of time before they compromised; however, I would advise the client to build up their cyber defences; ESM to detect attack; can apply for their NSM/ ESM. Once they will accept these ideas, they can start threat hunting.
(An idea from the course materials Day 5 – 2, part 3 and my own answer to question 1)

6. If I start from the very beginning, for the **Red**, **Green**, **Orange**, and **Blue** Zone monitoring the client network need a special team, which will monitor the client network system for **24/7** and **365** days. Therefore, we need at least a **4** men team. Because they are doing the overtime shift with their daily job for this particular purpose that is why they should get an extra allowance. I would say **£20000.00** for all **4** employees with their regular yearly pay.

For the rest of the SoC team would not cost any extra, as the team is able to monitor the NSM activities anyway.

Moreover, the SoC team does not require any extra hardware for **SPAN** but Cisco Switch Probe device would cost a little high price than others, it is **£6350.00** ext VAT (if we buy Cisco Catalyst C9300-48U-A L2/L3 Gigabit Ethernet (10/100/1000)); I would recommend **7** of them and its cost is **£44450.00** ext VAT.

To enhance the SoC ability, I would say the client could take the free trial of **ELK**, and later they can add the paid version with their necessity. I would say **£10000.00** for the near future cost.

For statistical data collection or NSM, I would advise them to spend **£20000.00** for the endpoint activities, i.e. monitors. However, within **Snort** and **Suricata**, I would always prefer **Suricata**, as I mentioned above, it is a free, open-source, mature, fast, and robust network. But I would advise the client to reserve **£5000.00** (**$399**/ sensor

for business use) for **Snort** if the SoC team want to use Snort by any chance for any specific needs, i.e. rule-based activities.

For ITIL, including any extra training, I would say another **£20000.00** for the SoC team members further education and activities.

Consequently, the client might send some of their best staff from the SoC team to complete the **AI** course in order to improve the **Artificial Intelligence** activities in the SoC team to prevent threats. The **AI** course cost normally depends on the institute, it starts from **£3600.00** to **£6000.00**. I would say, keep **£20000.00** for the client network's **AI** qualification.

And finally, another **£10000.00** for essential anti-virus (yearly plan) at least for **2** years and other materials, i.e. long cables, cable ties, extra sockets, switches, Ethernet cable, **RJ 45** cable and **2** extra monitors in an emergency.

All the estimate I have given is **£149450.00** basis of the client's requirement.

References

[1] A few ideas from 7025CEM community discussion (anticipation the topic), an idea from the course materials Day 2-1, the first three-part, and own evaluation.

[2] Axelos.com. 2020. *From V3 To 4 – This Is The New ITIL | AXELOS*. [online] Available at: <https://www.axelos.com/news/blogs/february-2019/from-v3-to-4-this-is-the-new-itil> [Accessed 10 November 2020].

[3] En.wikipedia.org. 2020. *Snort (Software)*. [online] Available at: <https://en.wikipedia.org/wiki/Snort_(software)> [Accessed 10 November 2020].

[4] En.wikipedia.org. 2020. *Suricata (Software)*. [online] Available at: <https://en.wikipedia.org/wiki/Suricata_(software)> [Accessed 10 November 2020].

[5] Eventbrite. 2020. *Webinar - Opnsense And Suricata A Great Combination, Let'S Get Started!*. [online] Available at: <https://www.eventbrite.com/e/webinar-opnsense-and-suricata-a-great-combination-lets-get-started-tickets-117996028297?aff=rss> [Accessed 10 November 2020].

[6] Exchange, O., Cybersecurity, A. and Exchange, O., 2020. *Open Threat Exchange (OTX) | Alienvault | AT&T Cybersecurity*. [online] Cybersecurity.att.com. Available at: <https://cybersecurity.att.com/open-threat-exchange> [Accessed 10 November 2020].

[7] For the last two line, the quotation of No. 5 paragraph (Check it) has taken from the course materials, Day 2-1, part 3 for more interactive the answer.

[8] Gchq.gov.uk. 2020. *Overview*. [online] Available at: <https://www.gchq.gov.uk/section/mission/overview> [Accessed 10 November 2020].

[9] General Data Protection Regulation (GDPR). 2020. *General Data Protection Regulation (GDPR) – Official Legal Text*. [online] Available at: <https://gdpr-info.eu/> [Accessed 10 November 2020].

[10] Hks.harvard.edu. 2020. *Leading In Artificial Intelligence: Exploring Technology And Policy (Online)*. [online] Available at: <https://www.hks.harvard.edu/educational-programs/executive-education/leading-artificial-intelligence?utm_source=google&utm_medium=cpc&utm_content=lai&utm_campaign=program-international> [Accessed 10 November 2020].

[11] Infosec Resources. 2020. *Open Source IDS: Snort Or Suricata? [Updated 2019] – Infosec Resources*. [online] Available at: <https://resources.infosecinstitute.com/open-source-ids-snort-suricata/#:~:text=One%20of%20the%20main%20benefits,much%20more%20recently%20than%20Snort.&text=Fortunately%2C%20Suricata%20supports%20multithreading%20out,will%20be%20used%20by%20Snort.> [Accessed 10 November 2020].

[12] Cablendevices.co.uk. 2020. *Cisco Catalyst C9300-48U-A Managed L2/L3 Gigabit Ethernet (10/100/1000) Grey*. [online] Available at: <https://cablendevices.co.uk/catalog/product/view/id/7970/s/cisco-catalyst-c9300-48u-a-managed-l2-l3-gigabit-ethernet-10-100-1000-grey/?gclid=CjwKCAiAkan9BRAqEiwAP9X6UfsF1rubDHfTIuVR4gUydg7Fu8Z1Q02EGwrjgfl31CkCllspMMHG1xoC5qAQAvD_BwE> [Accessed 10 November 2020].

[13] ISO. 2020. *ISO/IEC 20000-1:2018*. [online] Available at: <https://www.iso.org/standard/70636.html> [Accessed 10 November 2020].

[14] An idea from the course materials Day 2-1, part 6, Snort and Suricate, and own evaluation, and for anticipation the topic took an idea from 7025CEM community discussion.

[15] Axelos.com. 2020. *From V3 To 4 – This Is The New ITIL | AXELOS*. [online] Available

at: <https://www.axelos.com/news/blogs/february-2019/from-v3-to-4-this-is-the-new-itil> [Accessed 10 November 2020].

[16] Locate.coventry.ac.uk. 2020. [online] Available at: <https://locate.coventry.ac.uk/primo-explore/fulldisplay?docid=COV_ALMA5184074880002011&vid=COV_VU1&search_scope=LSCOP_COV&tab=local&lang=en_US&context=L> [Accessed 10 November 2020].

[17] Locate.coventry.ac.uk. 2020. [online] Available at: <https://locate.coventry.ac.uk/primo-explore/fulldisplay?docid=COV_ALMA51104420090002011&vid=COV_VU1&search_scope=LSCOP_COV&tab=local&lang=en_US&context=L&isFrbr=true> [Accessed 10 November 2020].

[18] NIST. 2020. *National Institute Of Standards And Technology* | *NIST*. [online] Available at: <https://www.nist.gov/> [Accessed 10 November 2020].

[19] NIST. 2020. *National Institute Of Standards And Technology* | *NIST*. [online] Available at: <https://www.nist.gov/> [Accessed 10 November 2020].

[20] O'Reilly Online Learning. 2020. *LAN Switching First-Step*. [online] Available at: <https://www.oreilly.com/library/view/lan-switching-first-step/1587201003/1587201003_ch11lev1sec3.html> [Accessed 10 November 2020].

[21] Oisf.net. 2020. *Open Information Security Foundation* | *Community Driven, Open Source*. [online] Available at: <https://oisf.net/> [Accessed 10 November 2020].

[22] One specific paragraph quoted from the course materials, Day 2-1, part 5, ELK to evolve its own idea in order to synchronise the answer with the rest of the research (this already mentioned on the answer).

[23] Cpni.gov.uk. 2020. *The UK Is A High Priority Espionage Target.* | *Public Website*. [online] Available at: <https://www.cpni.gov.uk/espionage> [Accessed 10 November 2020].

[24] Php.net. 2020. *PHP: Basic Usage - Manual*. [online] Available at: <https://www.php.net/manual/en/session.examples.basic.php> [Accessed 10 November 2020].

[25] Platform, H., Forensics, N., Security, E., Security, E., Demand, D., Services, F., Systems, I., Intelligence, T., Validation, S., Defense, M., Response, I., Consulting, C., Demand, E., Training, C., Stories, C., Success, C., Portal, C., Support, C., Programs, S., Notices, S., Products, S., Portal, D., Overview, P., Resellers, F., Partners, T., Partners, C.,

Providers, G., Locator, P., Center, P., Partner, B., Reports, A., Reports, T., Industry, T., Groups, A., Blogs, R., Security?, W., Cloud, C., Validation, S., Magazine, T., Downloads, F., Market, F., Training, E., FireEye?, W., Honors, A., Directors, B., Relations, I., FireEye, C., Releases, P., Opportunities, J., Solutions, M. and Intelligence, T., 2020. *Cyber Threat Intelligence | Fireeye*. [online] FireEye. Available at: <https://www.fireeye.com/mandiant/threat-intelligence.html> [Accessed 10 November 2020].

[26] Presentations. 2020. *Saïd Business School, University Of Oxford Oxford Artificial Intelligence Programme*. [online] Available at: <https://onlineprogrammes.sbs.ox.ac.uk/presentations/lp/oxford-artificial-intelligence-programme/?ef_id=c:337596651106_d:c_n:g_ti:aud-671108234543:kwd-20061192138_p:_k:%2Bai_m:b_a:69241337433&gclid=CjwKCAiAkan9BRAqEiwAP9X6UbP3g5t6ifZ7M2_iZtmqLAre0xkvjfq8pzZLfj9gWkj5MeGN7XvKkxoCUy0QAvD_BwE&gclsrc=aw.ds> [Accessed 10 November 2020].

[27] Assumption of a client network, an idea from the course materials Day 1-2, parts 2, 3 and 4, ITIL, ITSM and ITILv3 and 4, and own evaluation.

[28] Axelos.com. 2020. *ITIL | IT Service Management | ITSM | AXELOS*. [online] Available at: <https://www.axelos.com/best-practice-solutions/itil> [Accessed 10 November 2020].

[29] Redscan. 2020. *The Growing Importance Of Endpoint Security Monitoring | Redscan*. [online] Available at: <https://www.redscan.com/news/the-growing-importance-of-endpoint-security-monitoring/> [Accessed 10 November 2020].

[30] Sans.org. 2020. *SANS Institute: Reading Room - Forensics*. [online] Available at: <https://www.sans.org/reading-room/whitepapers/forensics/implementing-full-packet-capture-37392> [Accessed 10 November 2020].

[31] Sciencedirect.com. 2020. *Full Packet Capture - An Overview | Sciencedirect Topics*. [online] Available at: <https://www.sciencedirect.com/topics/computer-science/full-packet-capture> [Accessed 10 November 2020].

[32] Servicenow.com. 2020. *Now Platform - The Cloud Platform For Work - Servicenow*. [online] Available at: <https://www.servicenow.com/now-platform.html> [Accessed 10 November 2020].

[33] Snort.org. 2020. *How Much Does A Subscription Cost?*. [online] Available at:

<https://www.snort.org/faq/how-much-does-a-subscription-cost> [Accessed 10 November 2020].

[34] Elastic. 2020. *Elastic Stack: Elasticsearch, Kibana, Beats & Logstash | Elastic*. [online] Available at: <https://www.elastic.co/elastic-stack?ultron=B-Stack-Trials-EMEA-UK-Exact&gambit=Elasticsearch-ELK&blade=adwords-s&hulk=cpc&Device=c&thor=elk%20stack%20cost&gclid=CjwKCAiAkan9BRAqEiwAP9X6UdF-t_anfsLyo42-aUUj3PLtQoPgvCCgxRNL6vAVEBZaf1dmtpX8FRoCYyYQAvD_BwE> [Accessed 10 November 2020].

[35] Snort.org. 2020. *Snort - Network Intrusion Detection & Prevention System*. [online] Available at: <https://www.snort.org/#get-started> [Accessed 10 November 2020].

[36] Statistics Solutions. 2020. *Statistical Data Analysis - Statistics Solutions*. [online] Available at: https://www.statisticssolutions.com/statistical-data-analysis/ [Accessed 10 November 2020].

[37] Support, P., Switches, C. and TechNotes, C., 2020. *Catalyst Switched Port Analyzer (SPAN) Configuration Example*. [online] Cisco. Available at: <https://www.cisco.com/c/en/us/support/docs/switches/catalyst-6500-series-switches/10570-41.html> [Accessed 10 November 2020].

[38] Suricata. 2020. *OISF*. [online] Available at: <https://suricata-ids.org/about/oisf/> [Accessed 10 November 2020].

[39] Suricata. 2020. *Suricata*. [online] Available at: <https://suricata-ids.org/> [Accessed 10 November 2020].

[40] Bowcott, O., 2020. *GCHQ Data Collection Regime Violated Human Rights, Court Rules*. [online] the Guardian. Available at: <https://www.theguardian.com/uk-news/2018/sep/13/gchq-data-collection-violated-human-rights-strasbourg-court-rules> [Accessed 10 November 2020].

[41] Course materials Day 5 -, part 4, to evaluate the answer.

[42] Suricata. 2020. *Suricata*. [online] Available at: <https://suricata-ids.org/> [Accessed 10 November 2020].

[43] Suricata. 2020. *Suricata*. [online] Available at: <https://suricata-

ids.org/#:~:text=Suricata%20is%20a%20free%20and,NSM)%20and%20offline%20pcap%20processing.> [Accessed 10 November 2020].

[44] Taylor & Francis. 2020. *GCHQ And British External Policy In The 1960S*. [online] Available at: <https://www.tandfonline.com/doi/full/10.1080/02684520802449526?casa_token=C4evkmiyozcAAAAA%3AG9CvFyCaD8nyCiwAX36ySayI0unsVQCy6bIIFzvYmJ_kRSLjvbjxr857Z9hFKzy8M4XWTcsNIUyOig> [Accessed 10 November 2020].

[45] En.wikipedia.org. 2020. *Advanced Persistent Threat*. [online] Available at: <https://en.wikipedia.org/wiki/Advanced_persistent_threat> [Accessed 10 November 2020].

[46] For the last paragraph, I took an idea from the course materials Day 5 – 2, part 3, and my own answer to question 1.

[47] The six-value added from the study materials, day 1-2, part three to evaluate the answer.

[48] From Dr. Christo's question, Day 5-2, "putting it together" and https://link.springer.com/book/10.1007%2F978-1-4471-5007-7.

[49] Also, another assumption from the figure 1 picture and ideas from course materials, Day 2 -1, the big question on AULA.

[50] Also ideas from the course materials Day 2-1, 4 & 5 part for implementing tools and analysis further details.

[51] Course materials Day 5-2, part 1 - 7, own evaluation on AI, APTs, Threat Intelligence and basis of GCHQ's assumption, also ideas from 7025CEM community questions from Dr. Christo.

[52] En.wikipedia.org. 2020. *Artificial Intelligence*. [online] Available at: <https://en.wikipedia.org/wiki/Artificial_intelligence> [Accessed 10 November 2020].

[53] En.wikipedia.org. 2020. *GCHQ*. [online] Available at: <https://en.wikipedia.org/wiki/GCHQ> [Accessed 10 November 2020].

[54] En.wikipedia.org. 2020. *ITIL*. [online] Available at: https://en.wikipedia.org/wiki/ITIL [Accessed 10 November 2020].

[55] Assumption of a client network, also a few ideas from 7025CEM community discussion (anticipation the topic), an idea from the course materials Day 2-1, first three, four, and five-part and own evaluation.