MS in Cyber Security

Assignment on the Cyber Security methods and techniques to develop a solution to a business problem

Table of Contents

Introduction

Globally, the health care sector is central and indispensable to human existence. There has been a significant increase in the use of information and communication in the health care service industry in recent years. One of the clinical services that have been automated is patient appointments with the doctor. Scheduling patients is a complex process that plays an essential part in health care. In this assignment, we will examine the advantages of the **web-based appointment and scheduling management information system (ASMIS**) at the Queens medical center, as well as the cyber security risks associated with the automated web appointment.

What is ASMIS?

A user, guest, or patient can use the Queens Medical Centre's website, and with this online tool, they can quickly schedule appointments. Patients can schedule an appointment with a consultant via a hospital's website or their mobile device. They need to open the Queens Medical center's website in a web browser to access options such as doctor information, their availability, and consultation scheduling. Upon booking, it will collect the following **patient information**: Name, address, phone number, patient identification number, and payment information. This web-based appointment and scheduling management information system (ASMIS) is incredibly cost-effective for a hospital to adopt and simple to use and maintain.

Benefits of ASMIS

Patients or users can schedule consultations, laboratory testing, pharmacy, medicines/treatments availability, and insurance/claims. In today's fast-paced society, everything is internet-based technology, and thus automated appointment scheduling makes patients' lives easier. ASMIS offers users in hospital infrastructure

direct assistance without error. Users have the freedom to schedule their appointments according to their preferences. The system will provide all patients with quick and convenient access to health services. Using use case UML diagrams, illustrated the ASMIS concept and its operation at Queens Medical Center in Figure1.

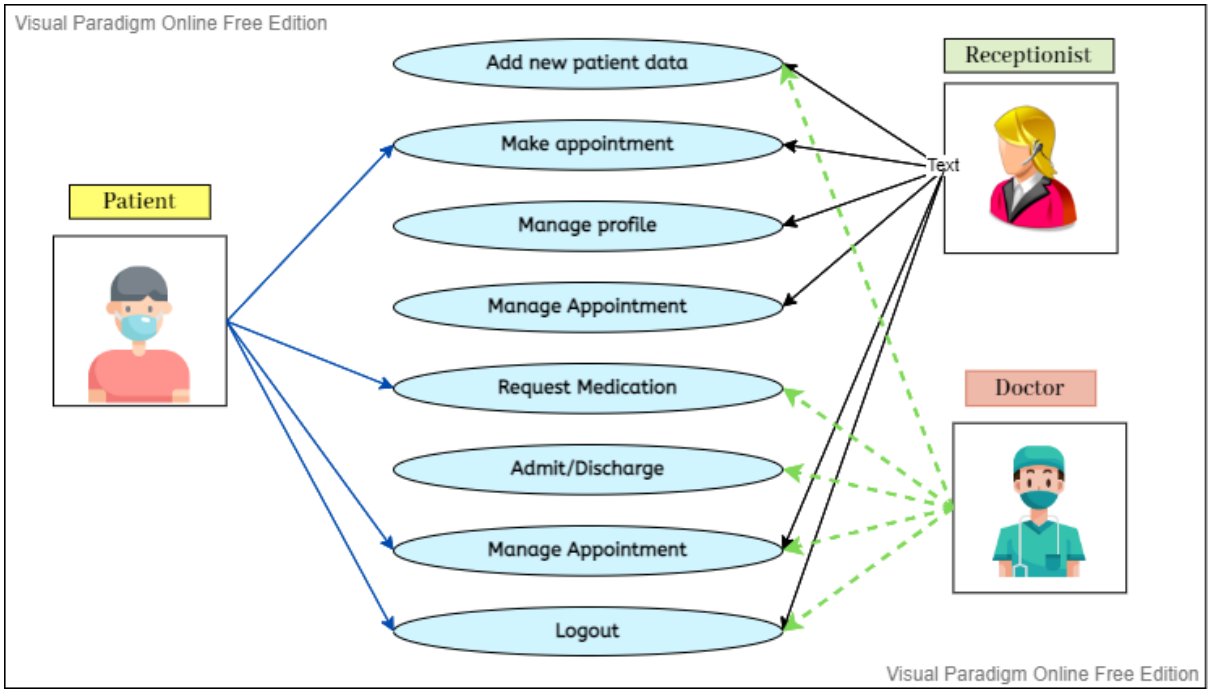

Figure1: UML diagram of ASMIS

Queens Medical Center Infrastructure

Using an ASMIS, Queens medical center infrastructure ***UML diagrams illustrate (Figure3)*** the flow of user or patient traffic. The Queens medical center has a website that allows visitors to schedule appointments and perform other medical-related tasks.

Due to an increase in cyber-attacks and threats, let's analyze the Queens Medical Centre's network, security architecture in order to identify the network's weaknesses, the likelihood of cyber threats, how cyber assaults can occur, and methods for

mitigating these risks. "Protecting hardware is as simple as keeping it locked away, chaining it to a desk, or purchasing a backup copy. Information is becoming a bigger issue. It can exist in multiple locations, travel across the globe in a matter of seconds, and be taken from you without your knowledge." [Bruce Schneier, 1994]. Medical center network is categorized into 3 layers with cyber threats associated with it as follows in Figure2.

- ✓ Application Layer
- ✓ Network Layer
- ✓ Perception Layer

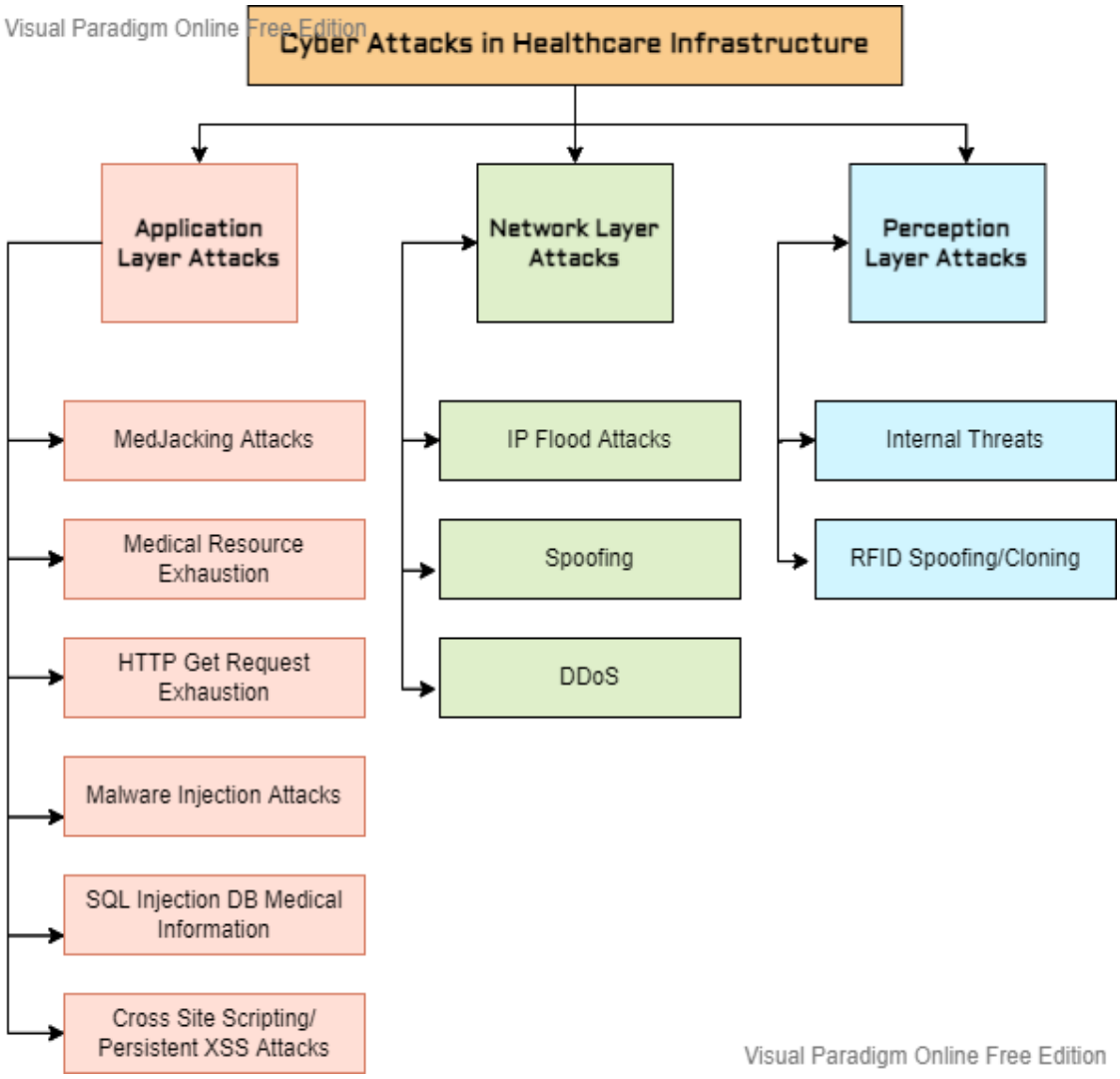

Figure2: Queens Medical Center Infrastructure threat layers

Internet to ASMIS Traffic flow

Once a user accesses the official website for Queen's medical, they will begin to navigate the site. The traffic from the user's computer or mobile device will reach the service provider's network before entering the hospital's network. The service provider router is the initial point of entry; once traffic reaches it, it is sent to the webserver depending on routing information. Once it reaches DMZ-protected web servers, it will provide appointment scheduling, consulting, and payment choices. These are decided by the webserver using an API through a corporate firewall before reaching the database server. Enterprise workstation traffic will run every other site through this firewall's entry point. Similarly, users that join a wireless network will have direct access to the internet via a service provider router. The hospital's Internet traffic will reach the corporate firewall and then flow through the router to the internet.

Sequence of attack and Threat Modelling techniques

The threat sequence has been mapped according to the ***MITRE ATT&CK***. First, the attacker must have access to a client running the web application via the Internet. Using cross-site scripting and other approaches, he exploits vulnerabilities to execute malicious code.

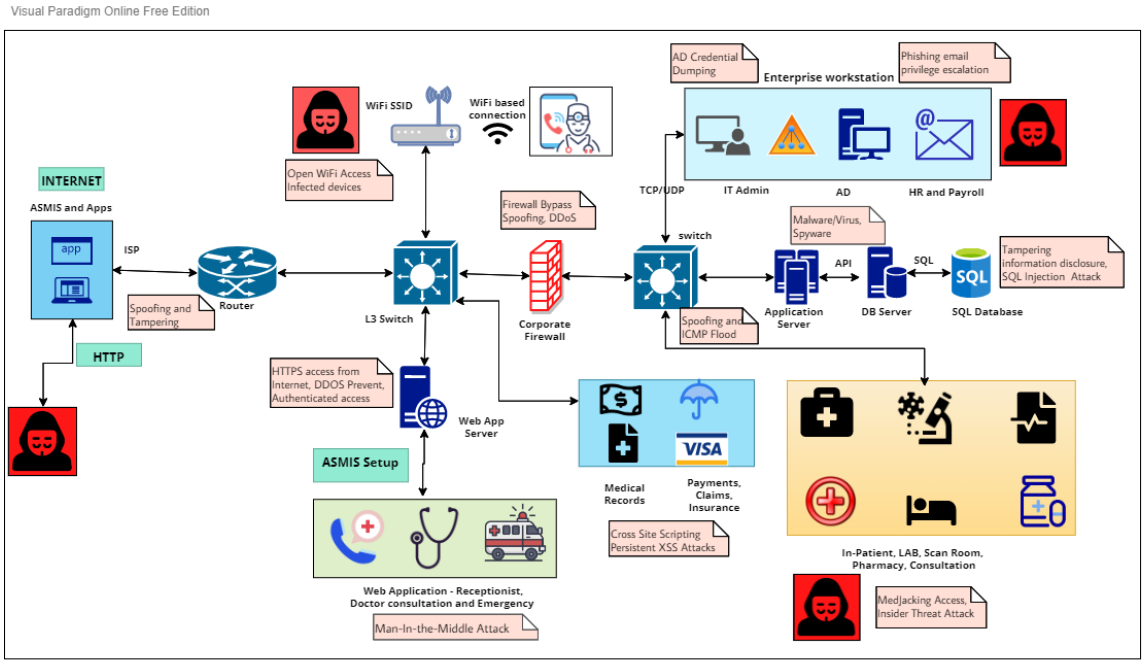

Figure3: Cyber-attack possibilities in Queens Medical Center Infrastructure

Now hacker is able to log into the application, potentially as an administrator. Once an attacker has obtained access to a system, he is able to establish such a high level of persistence that he cannot be removed. To escape detection, he impersonates a user throughout. Currently, adversaries employ credential dumping and network and host enumeration. Now that the ***hacker has complete access to the SQL Database***, they are able to conduct bulk queries to retrieve all of Queens Medical Center's data. If this information is leaked or sold, it could harm an organization's reputation. It may result in monetary loss or regulatory fines. Kill Chain is used to describe the attack's sequence. "Threats are a reflection of security holes. There is a cyber threat because we are weak. Consistent cyber-resilience requires an accurate understanding of digital and behavioral gaps." [Stephane Nappo, 2020]

Identifying Cyber-threats

As mentioned in the Figure3 following are the possibilities of cyber-attacks in this medical center.

- **Malware**:

Malware is software that is meant to steal information or cause harm to computers or software systems. It refers to the different types of harmful software, including viruses, spyware, and ransomware.

- **Cross-Site Scripting (XSS):**

Cross-Site Scripting Targets are not directly targeted; instead, vulnerable websites and web applications are exploited to conduct cross-site scripting assaults when users interact with them. For instance, when an unwary person visits a compromised website, the attacker's malicious script is opened and executed in the affected system browser

- **SQL injection attack:**

SQL injection and ad hoc are only two of the potential attack methods. IIS and SQL Server are just two of the possible targets. Any Windows component supporting MS Jet and ACE that allows users to run any query on a controlled database with MS Jet and ACE could be vulnerable.

- **Phishing attack:**

Phishing assaults have become one of the most frequent forms of cybercrime due to their effectiveness and minimal risk. They can circumvent detection techniques and offer little prospect of arrest or penalty. Email is the major source of phishing and phishing is most common in any organization.

- **Man-in-the-middle (MITM) attack:**

A hacker intercepting communication between you and an external party is called a Man-in-the-Middle Attack. Email, social networking, WiFi eavesdropping, SSL Decryption, general internet activity, and even phone calls can all be used in this attack. A hacker could also intercept personal information shared by a user via a website.

- **Spoofing:**

Spoofing is impersonating another person or entity. This is a frequent threat and easily executed by an attacker to gain medical center system access. Having robust authentication processes is a typical example of safeguards used to counteract such threats.

- **DDoS attack:**

A Distributed Denial of Service (DDoS) assault is a form of a Denial of Service (DoS) attack that leverages many attacker machines to flood the target with fictitious traffic. To attain the requisite scale, DDoS is frequently carried out using botnets that can co-opt millions of infected devices to participate in the attack without their knowledge, even though they are not the intended target.

- **Medjacking:**

According to a new World Economic Forum assessment on cyber risk, cyberattacks on life-saving medical devices such as heart pacemakers pose a severe threat and might be launched by terrorist organizations or even country states. The technique of hacking a medical device with the purpose of hurting or threatening a patient, known as medjacking, has been described as a "ticking time bomb," and the threat is

regarded as so severe that in 2015, the FBI felt obligated to issue a security alert warning.

- **Internal Threats:**

As a result of their legitimate access to private systems, insiders are particularly vulnerable because they are exempt from typical cybersecurity measures like intrusion detection equipment and physical security. "Insider dangers aren't taken as seriously as external threats, such a hack, according to our findings in our research. However, internal threats were far more costly than foreign ones for corporations. Insiders who are skilled at concealment can do so for months, years, or even indefinitely" [Dr. Larry Ponemon, 2021]

- **Tampering and Repudiation:**

To tamper is to alter anything without permission. Typically, tampering compromises integrity. Repudiation is denying having done something or taking responsibility for anything that has occurred.

Importance of Threat Modelling

Threat modelling makes the admins completely identify important threat occurrences, allowing them to concentrate on developing effective control methods to protect the system's critical components. This makes it more difficult for an enemy to compromise critical system components by gaining a footing and turning through the system. Users may approach threat analysis from three different perspectives:

- **Management level**
- **System level**
- **Application-level**

Preventing Cyber-Attacks and Mitigation

Following technologies are mainly used to prevent and mitigate hacking in any organization.

- ✓ NGFWs - Firewalls
- ✓ Vulnerability management tools and scanning
- ✓ Anti-virus
- ✓ Email Gateways
- ✓ Patching servers and Software's/OS versions UpToDate
- ✓ Access restrictions and RBAC
- ✓ Training all employees on Security aspects

We will see the usage of Next-Generation Firewalls – NGFW for preventing, mitigating, and analyzing cyberattacks.

NGFWs - Solution for Cyber Issues

The network infrastructure of the Queens Medical Center must be controlled by installing a DMZ firewall between the Service provider router and the DMZ web server hosting the web application. Between the enterprise network and the datacenter's web servers and databases, a corporate firewall must be installed.

The following strategies must be implemented in NGFW as mentioned in Figure4:

- ✓ Prevent access from **Bad host IP addresses/Regions** based on IANA's analysis
- ✓ Only **HTTPS traffic from the Internet should be permitted** to access the web application.

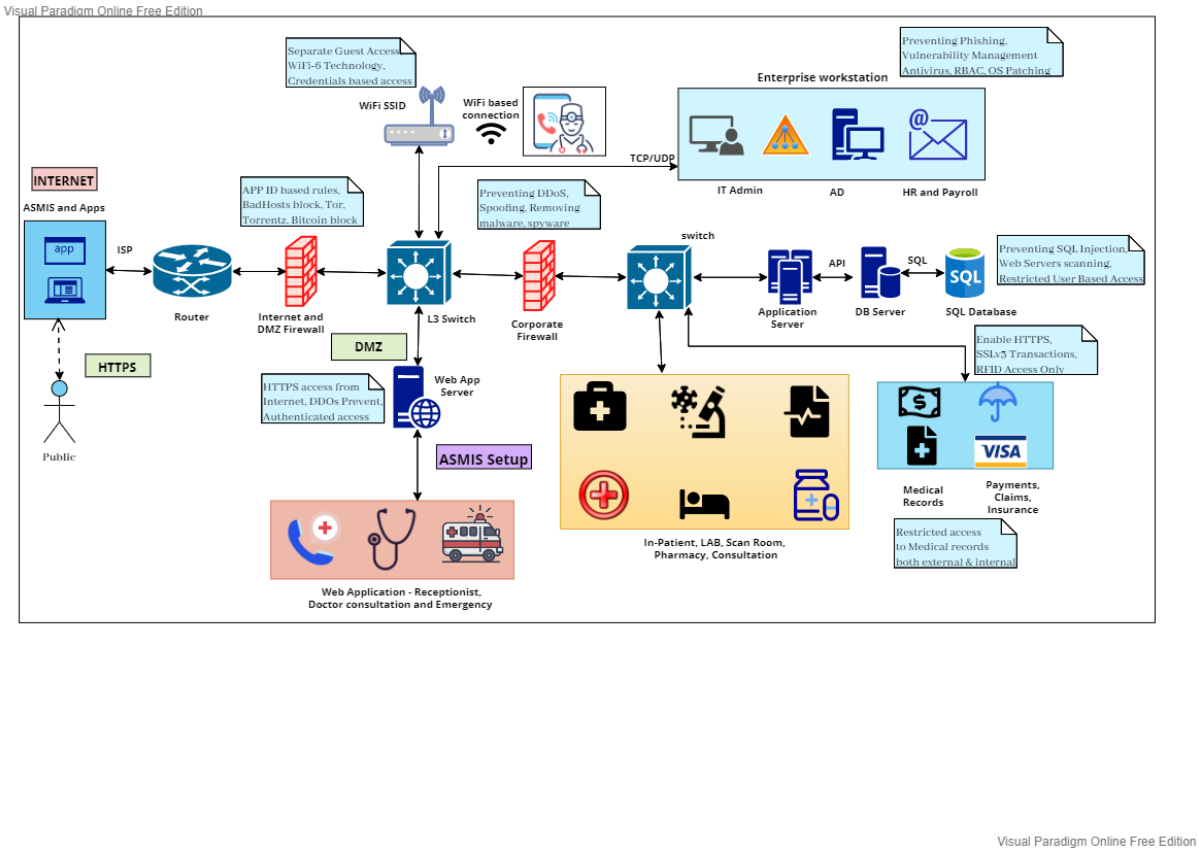

Figure4: Cyber-attack prevention and Mitigation in Queens Medical Center

- ✓ Access to **susceptible websites**, such as **BitTorrent, Bitcoin, Tor Web,** and **Net-Bios SMB ports**, from internal users to the internet are **blocked** and vice versa.
- ✓ **Web server should be installed in the DMZ zone** and moved behind the DMZ Firewall.
- ✓ **Vulnerable ports** such as FTP, HTTP, RDP, SSH, and TELNET should be **banned** between the Internet and Web applications and internal networks.
- ✓ Firewall security rules should be implemented as **Layer 7 Application ID-based (APP ID),** which supports SSL and Web-browsing applications instead of Ports 443, 80,22.
- ✓ All security rules, including **Antivirus, Vulnerability filtering, URL** and Data file **filtering**, must be bound to strict security standards.

- ✓ The corporate firewall should be established using the processes and stringent **user ID-based access to databases**, application servers, and medical records should be granted to internal users.
- ✓ To maintain security, **Wi-Fi 6 technology** must be implemented in wireless routers, and **guests should only have access to the internet** and not internal applications.
- ✓ All firewall logs must be provided to Splunk or any log server for monitoring, analysis, and **detection of compromised hosts and mitigation**
- ✓ The use of **Remote Access VPN** should **not** be permitted in all Healthcare organizations.
- ✓ In order to prevent online applications from being hacked, it is necessary to activate a **web application firewall (WAF)**
- ✓ **Restrict any file/software downloads** from the Internet and upload to the internet
- ✓ Features like **Intrusion detection system (IDS) and Intrusion prevention system (IPS) and WildFire** should be enabled

Strength and Weakness of Firewalls

Following are the primary strength of NGFWs:

- ✓ It prevents the majority of cyberattacks
- ✓ Simple to configure and operate
- ✓ Restricted Access
- ✓ Access Control policy
- ✓ Threat and all Traffic Monitoring
- ✓ Better Privacy

Furthermore, we have illustrated the weakness of NGFWs as follows.

- ✓ Cost and Licensing
- ✓ Backdoor exploits
- ✓ internal attacks
- ✓ Defenceless against all malware types
- ✓ Performance and throughput

Conclusion

This UML case diagram demonstrates the Queen's Medical Centre's ASMIS advantages and potential cyber dangers. We have examined the possibility of cyber assaults and how to prevent and minimize them using next-generation firewalls. In order to tackle a broader spectrum of cyberattacks, next-generation firewalls integrate firewall security with sophisticated features. In addition, we have thoroughly examined the other strategies for preventing cyber-attacks to this medical Centre.

References

Akinode,John Lekan, Oloruntoba S.A (December 2017). *Design and Implementation of a Patient Appointment and Scheduling System*. Published in IARJSET - International Advanced Research Journal in Science, Engineering and Technology Vol. 4, Issue 12. ISO 3297:2007 Certified.

Zhao P, Yoo I, Lavoie J, Lavoie B, Simoes E. *Web-Based Medical Appointment Systems*: A Systematic Review. J Med Internet Res 2017;19(4):e134 URL: https://www.jmir.org/2017/4/e134. DOI: 10.2196/jmir.6747

A. Djenna and D. Eddine Saïdouni, "*Cyber Attacks Classification in IoT-Based-Healthcare Infrastructure*," 2018 2nd Cyber Security in Networking Conference (CSNet), 2018, pp. 1-4, doi: 10.1109/CSNET.2018.8602974.

Beavers, J., Pournouri, S. (2019*). Recent Cyber Attacks and Vulnerabilities in Medical Devices and Healthcare Institutions*. In: Jahankhani, H., Kendzierskyj, S., Jamal, A., Epiphaniou, G., Al-Khateeb, H. (eds) Blockchain and Clinical Trial. Advanced Sciences and Technologies for Security Applications. Springer, Cham. https://doi.org/10.1007/978-3-030-11289-9_11

NATALIYA SHEVCHENKO (DECEMBER 3, 2018) *Threat Modeling: 12 Available Methods.* Available from https://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods/ [Accessed 05 May 2022].

Georgiadou, Anna, Spiros Mouzakitis, and Dimitris Askounis. (2021). "*Assessing MITRE ATT&CK Risk Using a Cyber-Security Culture Framework*" Sensors 21, no. 9: 3267. https://doi.org/10.3390/s21093267

APP-ID in Palo Alto Networks. https://www.paloaltonetworks.com/technologies/app-id [Accessed on 8 May 2022].

H. Ahmed, A. Alsadoon, P. W. C. Prasad, N. Costadopoulos, L. S. Hoe and A. Elchoemi, "*Next generation cyber security solution for an eHealth organization*," 2017 5th International Conference on Information and Communication Technology (ICoIC7), 2017, pp. 1-5, doi: 10.1109/ICoICT.2017.8074723.

Fagade, T., Spyridopoulos, T., Albishry, N., Tryfonas, T. (2017). *System Dynamics Approach to Malicious Insider Cyber-Threat Modelling and Analysis*. In: Tryfonas, T. (eds) Human Aspects of Information Security, Privacy and Trust. HAS 2017. Lecture Notes in Computer Science(), vol 10292. Springer, Cham. https://doi.org/10.1007/978-3-319-58460-7_21.