| Attack | Description | Attacked Devices | Solutions |
| --- | --- | --- | --- |
| DOS(Denial-of-Service) | An attacker can flood the workstation in the patient's room by sending multiple communication packets over the internet;this might prevent the medical team from accessing the EHR, interfering with patient care, the medical team would have to revert to using paperwork which will be inefficient.  Vector:  -Social Engineering Techniques.  -Insertion of infected USB.  -Malicious email  -Electromagnetic interference. | -EHR Server  -Central Monitoring Station  -Communication box  -Workstation  -Infusion Pump  -Syringe Pump  -Body heater  -Medical Ventilator  -Feeding Pump  -Monitor | When flood volumes exceed the capacity of the network connection being targeted, it is typically necessary to intercept the incoming traffic upstream to filter out the attack traffic from the legitimate traffic. Such defenses can be provided by the hosting Internet Service Provider (ISP) or by a 3rd party such as a Content Delivery Network (CDN) or providers specializing in DoS mitigations.[6]  Depending on flood volume, on-premises filtering may be possible by blocking source addresses sourcing the attack, blocking ports that are being targeted, or blocking protocols being used for transport.  As immediate response may require rapid engagement of 3rd parties, analyze the risk associated to critical resources being affected by Network DoS attacks and create a disaster recovery plan/business continuity plan to respond to incidents. |
| Electromagnetic interference | An attacker emits disruptive radiation near a device which affects the availability or activity of the device. For example the Syringe Pump which operates based on infrared radiation technology.  **Vector:**  -Disruptive radiation near the device. | -Infusion Pump  -Syringe Pump |  |
| Man-in-the-Middle | The attacker can steal the data or change it, so the recipient doesn’t receive the original (intended)data. In this case, the patient may not receive the proper treatment, since the medical information shared between devices is incorrect.  **Vector:**  -Social Engineering Techniques.  -Insertion of infected USB.  -Malicious email | -EHR Server  -Central Monitoring Station  -Communication box  -Workstation  -Infusion Pump  -Syringe Pump  -Body heater  -Medical Ventilator  -Monitor | -Disable legacy network protocols that may be used to intercept network traffic if applicable, especially those that are not needed within an environment.  -Ensure that all wired and/or wireless traffic is encrypted appropriately. Use best practices for authentication protocols, such as Kerberos, and ensure web traffic that may contain credentials is protected by SSL/TLS.  -Use network appliances and host-based security software to block network traffic that is not necessary within the environment, such as legacy protocols that may be leveraged for AiTM conditions.  -Limit access to network infrastructure and resources that can be used to reshape traffic or otherwise produce AiTM conditions.  -Network intrusion detection and prevention systems that can identify traffic patterns indicative of AiTM activity can be used to mitigate activity at the network level.  -Network segmentation can be used to isolate infrastructure components that do not require broad network access. This may mitigate, or at least alleviate, the scope of AiTM activity.  -Train users to be suspicious about certificate errors. Adversaries may use their own certificates in an attempt to intercept HTTPS traffic. Certificate errors may arise when the application’s certificate does not match the one expected by the host. |
| Spyware | An attacker installs spyware on a system/server. Such spyware enables the attacker to steal medical and private information about the patient and his/her treatment.  **Vector:**  -Social Engineering Techniques.  -Insertion of infected USB.  -Malicious email. | -EHR Server  -Central Monitoring Station  -Communication box  -Infusion Pump | Use trusted antivirus software with anti-spyware and anti-malware features  Don’t download suspicious-looking email attachments  Don’t click on online pop-ups (or block them entirely with a secure browser)  Don’t open links received in text messages from unknown numbers  Avoid chatting with strangers in messaging apps  Keep your computer and mobile operating systems up-to-date |
| Alert Attack - Missing Alerts(devices) | An attacker can cause the device to fail to issue alerts when they needed. In this case, the medical team will be unaware of the patient's condition, preventing the patient from receiving proper treatment. For example, an attacker can insert an infected USB(such as a keyboard) into the server of the central monitoring station in order to disable the monitor´s alerts remotely.  **Vector:**  -Social Engineering Techniques.  -Insertion of infected USB.  -Malicious email.  -Firmware updates. | -Infusion Pump  -Syringe Pump  -Body heater  -Medical Ventilator  -Monitor | You can’t eradicate false alerts, unfortunately. Finetuning monitoring rules help reduce them, but the reduction is insignificant at best. However, using a CSPM and other monitoring tools can help cybersecurity professionals contextualize the alerts or provide sufficient information for factual investigation and threat mitigation. Another possible countermeasure is to provide easy one-click remediation so security staff can quickly and easily mitigate common threats or even provide step-by-step instructions on how to remediate these threats.  Below are some features to consider in a CPSM tool to help reduce alert fatigue for your security staff.  **1-Contextualize alerts:**  A Cloud Security Posture Management (CSPM) should allow you to quickly identify and zoom in on suspected assets to understand the context of the threat in light of configuration and activity perspectives associated with event severities.  This significantly reduces the time required to investigate each alert. You can quickly identify and dismiss a false alert, take immediate action to mitigate the threat, or remediate the vulnerability.  **2-Provide actionable insights**  Prevention is always better than cure. Why wait for the alerts to come through? Imagine seeing a history of all changes made to your multi-cloud environment, each accompanied by an actionable insight that helps you know of potential threats to your cloud infrastructure and even guides you on taking proactive action to mitigate the potential threats.  Having such a feature will also allow your organization to stay audit-ready for international standards such as ISO 27001, SOC 2, industry-specific and territorial standards such as PCI DSS for the payments industry, Singapore's MAS TRM, Indonesia’s POJK 38, Australia’s APRA, and the Thai PDPA.  **3. Custom rules and threat level flagging**  Every organization has unique security and business needs; yours is no different. You may have some in-house security rules to monitor. Some organizations also have cloud assets more important than others compared to their industry peers.  You can reduce alert fatigue by monitoring these in-house rules and assets, setting the right criticality flags for each, and prioritizing them. For example, you may want to get alerts whenever there’s any change on an AWS S3 bucket containing Personal Identifiable Information (PII) data.  Going further, a CSPM should allow you to create monitoring groups where you can specify the criticality level and automatically apply it to other flagged critical assets in your organization. This will help you reduce alert fatigue.  **4. Quick remediation of threats and vulnerabilities**  Your security staff should also be able to quickly and easily remediate common and minor vulnerabilities and threats and receive step-by-step instructions on mitigating specific vulnerabilities.  In fact, selecting all common and minor vulnerabilities and then bulk-remediating them with a single click of the mouse will significantly reduce the time your security staff spends on remediation.  Another way you can help your security staff stave off alert fatigue and upskill simultaneously is by ensuring that the CSPM tool offers step-by-step instructions for remediating vulnerabilities. For example, your security staff may choose to remediate common and minor vulnerabilities with the one-click option while using the step-by-step playbook for more complex remediations and learn from that. |
| Alert Attack - False Alerts(devices) | An attacker can cause a device to issue an alert when it is not needed. The sound of the alarms may frustrate the medical team, and over time this may cause them to ignore the alarms(e.g., they may fail to respond to a patient's deteriorating condition). For example , an attacker can utilize social engineering techniques in order to encourage someone to insert an infected USB(such as keyboard) into the server of the central monitoring station; this will enable the attacker to change the required threshold for alerts, so the monitor´s alerts are triggered frequently.  **Vector:**  -Social Engineering Techniques.  -Insertion of infected USB.  -Malicious email.  -Firmware updates. | -Infusion Pump  -Syringe Pump  -Body heater  -Medical Ventilator  -Monitor | You can apply the same mitigations of **Alert Attack - Missing Alerts(devices).** |
| Data Manipulation | An attacker can change existing data, so the patient's medical condition will be displayed incorrectly on the device.  **Vector:**  -Email/phishing.  -Firmware updates.  -Insertion of infected USB. | -EHR Server  -Central Monitoring Station  -Communication box  -Infusion Pump  -Syringe Pump  -Body heater  -Monitor | **Encrypt Sensitive Information:**  Consider encrypting important information to reduce an adversary’s ability to perform tailored data modifications.  **Network Segmentation:**  Identify critical business and system processes that may be targeted by adversaries and work to isolate and secure those systems against unauthorized access and tampering.  **Remote Data Storage:**  Consider implementing IT disaster recovery plans that contain procedures for taking regular data backups that can be used to restore organizational data.[1] Ensure backups are stored off system and is protected from common methods adversaries may use to gain access and manipulate backups.  **Restrict File and Directory Permissions:**  Ensure least privilege principles are applied to important information resources to reduce exposure to data manipulation risk. |
| Ransomware | An attacker can use ransomware for financial gain. The attacker may publish the patient's personal information, encrypt data, or prevent access to critical patient information.  **Vector:**  -Malicious email attachments and links.  -Malicious USB device.  -Firmware update via Wi-Fi. | -EHR Server  -Workstation | **Antivirus/Antimalware:**  Anti-virus can also automatically quarantine suspicious files.  **Network Intrusion Prevention:**  Network intrusion prevention systems and systems designed to scan and remove malicious email attachments can be used to block activity.  **Restrict Web-Based Content:**  Block unknown or unused attachments by default that should not be transmitted over email as a best practice to prevent some vectors, such as .scr, .exe, .pif, .cpl, etc. Some email scanning devices can open and analyze compressed and encrypted formats, such as zip and rar that may be used to conceal malicious attachments.  **Software Configuration:**  Use anti-spoofing and email authentication mechanisms to filter messages based on validity checks of the sender domain (using SPF) and integrity of messages (using DKIM). Enabling these mechanisms within an organization (through policies such as DMARC) may enable recipients (intra-org and cross domain) to perform similar message filtering and validation.  **User Training:**  Users can be trained to identify social engineering techniques and spear phishing emails. |
| Delay Attack | An attacker delays the transmission of data to medical devices or online displays. Most of the devices in the ICU require continuous and real-time data, so the medical team can monitor the patient's condition and provide him/her appropriate and timely treatment.  **Vector:**  -Malicious email attachments and links.  -Firmware update | -EHR Server  -Central Monitoring Station  -Communication box  -Workstation  -Infusion Pump  -Syringe Pump  -Body heater  -Medical Ventilator  -Feeding Pump  -Monitor | You can apply the same mitigations as **Ransomware**. |
| Session Hijacking | An attacker uses an existing session between devices in order to gain unauthorized access to information in a computer system. In this case, the attacker can send malicious commands, steal medical data, etc.  **Vector:**  -Malicious email(with malicious files/links).  -Packet sniffing(cookie thefts) | -Central Monitoring Station  -Communication box  -Infusion Pump | -Use strong passwords and multifactor authentication. These techniques protect accounts from being accessed by hackers if they manage to steal a user’s session ID (Alkove, 2021).  -Only share session IDs with trusted sources. Be careful when sharing links or sending requests to websites, as these may include session IDs.  -Use a VPN. A VPN helps prevent attackers from intercepting traffic, making it more difficult for them to steal session IDs (McCann & Hardy, 2022).  -Keep software up to date. Make sure to keep operating systems and software up to date with the latest security patches to prevent attackers from exploiting vulnerabilities to access users’ sessions.  -Take cybersecurity training. Cybersecurity threats are constantly evolving, so it’s essential to stay informed on the latest attack techniques and how to prevent them. Consider getting certified in various cybersecurity domains, including ethical hacking, incident handling, and penetration testing. |
| Centralized Alert Attack - Missing Alerts(nurses’station) | Similar at Alert Attack - Missing Alerts(devices)  **Vector:**  -Social Engineering Techniques  -Insertion of infected USB  -Malicious email/phishing. | -Central Monitoring Station  -Communication box  -Infusion Pump | You can apply the same mitigations of **Alert Attack - Missing Alerts(devices**). |
| Centralized Alert Attack - False Alerts(nurses’station) | Similar at Alert Attack - False Alerts(devices)  **Vector:**  -Social Engineering Techniques  -Insertion of infected USB  -Malicious email/phishing. | -Central Monitoring Station  -Communication box  -Infusion Pump | You can apply the same mitigations of **Alert Attack - Missing Alerts(devices).** |
| Malicious Firmware Update | An attacker can install a malicious firmware update in order to change default commands or settings, so the devices will perform different actions than those required.  **Vector:**  -Social engineering(the attacker impersonates the software company) | -EHR Server  -Central Monitoring Station  -Communication box  -Syringe Pump  -Body heater  -Medical Ventilator  -Feeding Pump  -Monitor | **Access Management:**  All devices or systems changes, including all administrative functions, should require authentication. Consider using access management technologies to enforce authorization on all management interface access attempts, especially when the device does not inherently provide strong authentication and authorization functions.  **Audit:**  Perform integrity checks of firmware before uploading it on a device. Utilize cryptographic hashes to verify the firmware has not been tampered with by comparing it to a trusted hash of the firmware. This could be from trusted data sources (e.g., vendor site) or through a third-party verification service.  **Boot Integrity:**  Check the integrity of the existing BIOS or EFI to determine if it is vulnerable to modification. Use Trusted Platform Module technology. [4]Move system's root of trust to hardware to prevent tampering with the SPI flash memory. [5]Technologies such as Intel Boot Guard can assist with this. [6]  **Code Signing:**  Devices should verify that firmware has been properly signed by the vendor before allowing installation.  **Communication Authenticity:**  Protocols used for device management should authenticate all network messages to prevent unauthorized system changes.  **Encrypt Network Traffic:**  The encryption of firmware should be considered to prevent adversaries from identifying possible vulnerabilities within the firmware.  **Encrypt Sensitive Information:**  The encryption of firmware should be considered to prevent adversaries from identifying possible vulnerabilities within the firmware.  **Filter Network Traffic:**  Filter for protocols and payloads associated with firmware activation or updating activity.  **Human User Authentication:**  Devices that allow remote management of firmware should require authentication before allowing any changes. The authentication mechanisms should also support Account Use Policies, Password Policies, and User Account Management.  **Network Allowlists:**  Use host-based allowlists to prevent devices from accepting connections from unauthorized systems. For example, allowlists can be used to ensure devices can only connect with master stations or known management/engineering workstations.  **Network Segmentation:**  Segment operational network and systems to restrict access to critical system functions to predetermined management systems.  **Software Process and Device Authentication:**  Authenticate connections from software and devices to prevent unauthorized systems from accessing protected management functions.  **Update Software:**  Patch the BIOS and EFI as necessary. |
| cryptominer | An attacker can use the server in order to mine cryptocurrency. The mining may impair system performance and cause high power consumption.  **Vector:**  -Cryptojacking(code hosted on Web Applications)  -Social engineering(penetration of malware crypto mining) | -EHR Server  -Infusion Pump | -Practice strong security hygiene. IT hygiene is foundational to security. Regularly patching vulnerable applications and operating systems, and protecting privileged user accounts, are essential practices for optimal security posture.  -Educate your employees. Ensure all employees complete comprehensive training on the importance of keeping sensitive data safe, best practices to prevent crypto jacking, and a thorough understanding on the different ways cyber attacks can happen.  -Deploy a true next-generation endpoint protection platform (EPP). Organizations must be prepared to prevent and detect all threats, including known and unknown malware, as well as identifying in-memory attacks. This requires a solution that includes next-gen AV protection, as well as endpoint detection and response (EDR), to prevent attacks and gain full visibility throughout the environment. |
| Configuration manipulation | An attacker modifies/sets device settings without the medical team´s awareness, causing the device to operate differently than intended.  **Vector**:  -Social Engineering Techniques  -Insertion of infected USB  -Malicious email/with malicious file/link.  -Firmware update | -EHR Server  -Central Monitoring Station  -Communication box  -Workstation  -Infusion Pump  -Syringe Pump  -Body heater  -Medical Ventilator  -Feeding Pump  -Monitor | You can apply the same mitigations as **Data Manipulation**. |
| Abuse or Legitime Operations | An attacker obtains access to device(e.g., by influencing a member of the medical team to insert an infected USB into the device), then the attacker can send commands to the device without the medical team's awareness.  **Vector:**  -Social Engineering Techniques  -Insertion of infected USB  -Malicious email/with malicious file/link.  -Firmware update | -Monitor | You can apply the same mitigations as **Data Manipulation**. |