Threats and Threat Analysis

Cybersecurity in Hospitals

Dräger

Technology for Life

The application of computer based, networked technology to the healthcare industry can improve patient health outcomes, while promoting efficient and effective operations for healthcare organizations. While its benefits are indisputable, the increasing reliance on this technology opens the door for new risks, including Cybersecurity risks for patients, healthcare organizations, and medical device manufacturers.

Medical devices, health information databases and administrative systems have a range of potential threats and impacts from simple administrative annoyances to severe harm to patients.

For example:

- Direct attacks on patient health by tampering with medical devices used to treat and monitor patients' health (e.g. anesthesia devices, intensive care ventilators, patient monitors, pacemakers, infusion pumps).
- Disabling access to, or denying the use of medical devices or records leading to delay in treatment, disruption of healthcare organization operations, and potential financial harm.
- Disclosure of Personal Identifying Information (PII) and Protected Health Information (PHI), leading to legal issues for healthcare providers and medical device manufacturers.

The size and scope of healthcare attacks have grown over recent years. The US FDA Former Director of Medical Device Cybersecurity, Kevin Fu, called an early 2021 incident a „watershed moment" for medical device security. „Instead of ransomware simply disabling access to say, electronic health records, which is still quite inconvenient, in this case the remediation process to the ransomware caused an outage such that patients could not receive that particular therapy from the medical device," Fu said. „That was something we haven't seen before."1

And the potential threat will continue to grow: The 2021 Cybersecurity Predictions from the United States Department of Health & Human Services (Office of Information Security) reported that through the Internet of Medical Things (IoMT) healthcare will increase its attack surface rather than shrinking its attack surface.
PowerPoint Presentation (hhs.gov)

Due to this increasing threat, it is critical that vulnerabilities in medical devices and healthcare information systems be systematically analyzed and countered to prevent potential attacks early on and protect patients from harm.

We at Dräger manufacture products that are used in therapy and treatment scenarios. In the event of a cybersecurity incident, these devices can directly impact the health of patients, the privacy of their personal information, or the security of hospital IT equipment.

"Vulnerabilities are simply weaknesses in the system and are not as commonly confused as other terms. It's what makes threats possible and/or more significant.[0]"

Common vulnerabilities include things like:

- Cleartext transmission of sensitive data
- Failure to check authorization to sensitive resources
- Failure to encrypt sensitive data at rest

"A **threat** is a negative event that can lead to an undesired outcome, such as damage to, or loss of, an asset.[0]"

Some examples of threats are:

- Malware is placed on a medical records system which encrypts medical records unless a ransom is paid.
- An attacker exploiting an unprotected interface on a patient monitor to remotely change alarm settings, potentially leading to misdiagnosis and patient harm.
- An attacker rendering a hospital network unresponsive with a Denial-of-Service attack.

"A **risk**, in plain language, is a chance of something bad happening combined with how bad it would be if it did happen. It's essentially a negative scenario you want to avoid, combined with its probability and its impact.[0]"

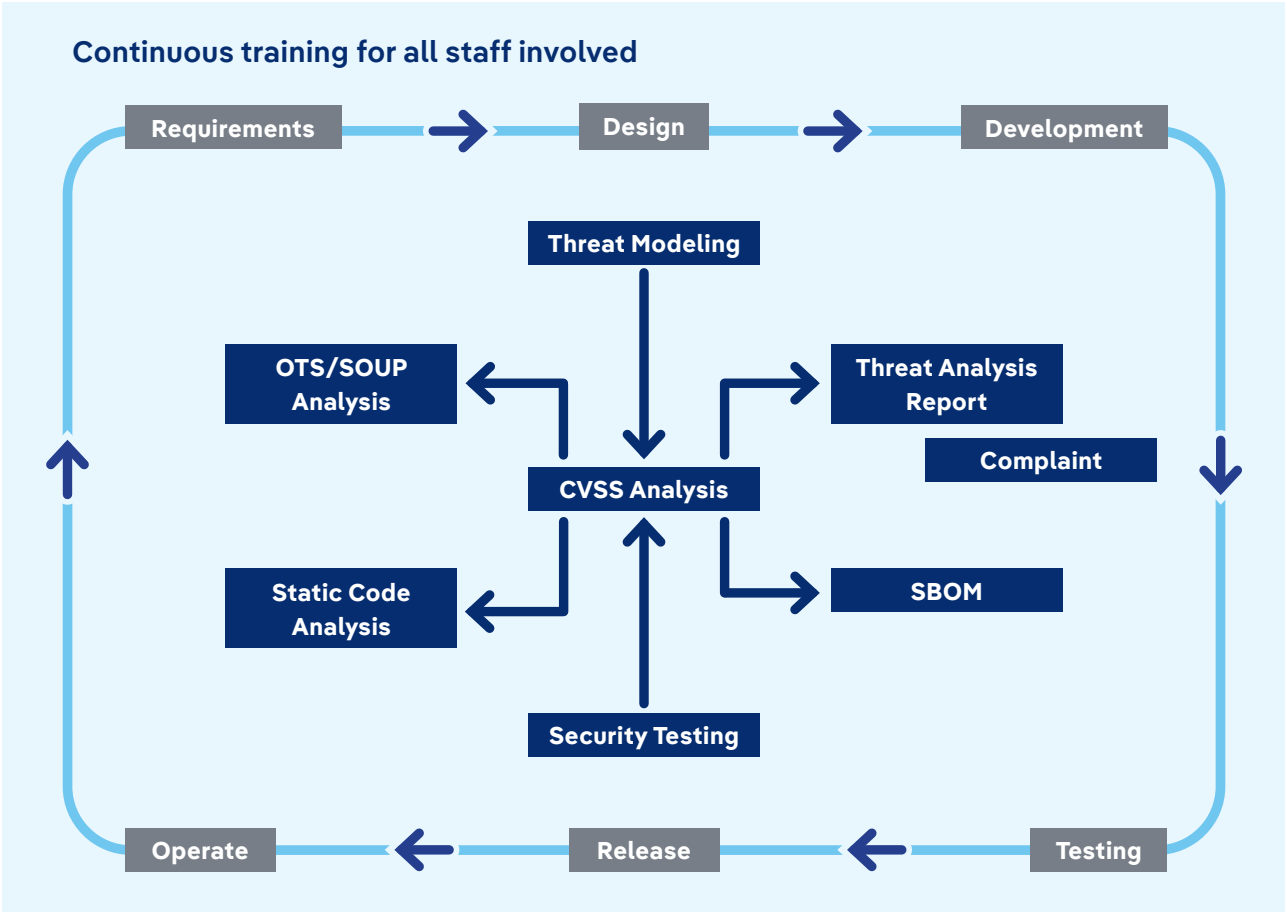
Dräger's Methodology to Identify and Classify Vulnerabilities and Threats

We take proactive steps to mitigate threats by integrating a methodology called "Threat Analysis" into the development process of our devices and systems as a part of the Secure Development Life Cycle (SDLC). Threat analysis is a process that identifies threats to a system and evaluates their severity. It describes the nature of the threats and impacted assets, scored by criticality. The results are then used to make improvements to the security of the devices and systems.

Secure Software Development Life Cycle (SDLC) is a security-oriented process used to design, implement, test, and employ an information system of high quality and security. A team of security experts are available to the product development team throughout the life cycle to consider potential Cybersecurity issues of the device.

The elements of the Threat Analysis can be mapped to the phases of our SDLC. The high-level goals and related activities of the threat analysis within the SDLC are:

- A Threat Model is created, which includes all functionality within the system and communication between these functions. The dataflows are analyzed to identify vulnerabilities and create a list of threats to the system.
- All third-party software is documented and checked on a regular basis for known vulnerabilities.
- Once the product is at a stable status, internal and external testing is performed. The device is checked against the requirements for the product. External independent testers will perform tests of known cybersecurity attacks against the Dräger medical device.
- After the release to the field, vulnerabilities are monitored via Field Complaints.



The results of all these activities are collected in the Dräger Threat Analysis report and the Software Bill of Materials (SBOM), which are kept as a continuously updated record for the medical device. Critical threats may lead to a maintenance release for the medical device, while less critical defects will be used as input for the next development cycle for the medical device. In the following section we will describe the tools and flows in the Dräger Threat Analysis process.

Threat Modeling starts with the "requirements" phase. This is a structured process that identifies security requirements, pinpoints security threats and potential vulnerabilities, quantifies threat and vulnerability criticality, and prioritizes remediation methods before the release of software. Data flow diagrams are used to ensure there are no gaps in communications or the processing of insecure data. STRIDE analysis on data flow diagrams provides a model scoring them by criticality. The **STRIDE** model uses the following categories of threats: **S**poofing identity, **T**ampering with data, **R**epudiation threats, **I**nformation disclosure, **D**enial of service, and **E**levation of privileges. Working with product Subject Matter Experts (SMEs), the threat model is created and verified, and vulnerabilities are triaged to ensure threats are reviewed by developers, analysts, testers, and product SMEs. Based upon the findings from the reviews, possible threats are derived, and exploitability is determined using the Common Vulnerability Scoring System (CVSS) analysis technique.

OTS/SOUP Analysis (**O**ff-**T**he-**S**helf / **S**oftware **o**f **U**nknown **P**rovenance) is another part of the development process which uses the list of OTS / SOUP items created for the **Software Bill of Materials (SBOM)**. Public vulnerability databases, such as National Vulnerability Database NVD (LINK), Common Vulnerabilities and Exposure CVE (LINK) details, and VulnDB [LINK] are searched for known vulnerabilities. Signal sources are reviewed including Health-ISAC Daily Security Intelligence Report [LINK], German Alliance for Cybersecurity (LINK) mailing list, and Cybersecurity trade journals for potential vulnerabilities in third-party software. Vendor documentation websites are used to contact vendor tech support, inquire about vulnerabilities, and capture vulnerabilities and threats within third-party software. These vulnerabilities are evaluated to determine if they affect the product.

Static Code Analysis is performed and continues through the **Security Testing** phase. It is a method of debugging that is done by examining the source code without executing the program. This process helps ensure the code adheres to industry standards. Static analysis is generally good at finding coding issues such as: programming errors, coding standard violations, undefined values, syntax violations, and security vulnerabilities. The findings are discussed with peers and product SMEs.

Security Testing can be performed on early prototypes in the development phase. Software and hardware tools are used to test for vulnerabilities and determine if the data and resources of the software are protected from possible malicious actors. Security testing also reveals flaws in the data flow and security mechanisms to ensure the software maintains functionality. It can include vulnerability and compliance scanning, fuzz testing (e.g., USB fuzzing, network fuzzing), network flood testing, and even engage third-party penetration testing to test our devices and systems.

Using **Common Vulnerability Scoring System (CVSS)** Analysis provides a way to capture the key characteristics of a vulnerability. All findings in the **Threat Modeling, OTS/SOUP Analysis, Static Code Analysis** and **Security Testing** are evaluated in a **CVSS Analysis** and produce numerical scores reflecting their severity. CVSS is a published standard used by organizations worldwide and continues to improve. We use the CVSS exploitability sub score to categorize all identified threats (Threat Model, SBOM, Security Testing, Field Complaints) in a form compatible to our Risk Analysis Process (RAP).

The **Threat Analysis Report** is a deliverable with our software that identifies security related device characteristics of a product. Threat analysis describes the entire ecosystem of the product. It captures vulnerabilities and threats from the threat model and security testing efforts. The **Threat Analysis Report** is used as input into the Risk Management Process (RMP).

The Software Bill of Material (SBOM) is delivered with each product release and contains a list of third-party components included in our software. For each of the OTS/SOUP items listed, any known vulnerabilities are listed along with their disposition. Additionally, any threats identified from the OTS/SOUP Analysis are captured here. Like the Threat Analysis, it is used as input into the Risk Management Process (RMP).

After the release of a product, customers file **complaints** to report issues. They are triaged to determine if the complaint is Cybersecurity related, and if the complaint is isolated to Dräger developed hardware or software, or third-party hardware or software. Based upon the findings from the discussion, possible threats are derived, and the exploitability is determined using the CVSS analysis technique.

Dräger Coordinated Disclosure Statement. We maintain a product security page at https://www.draeger.com/security/ to provide contact details, as well as information concerning the procedures to test and report vulnerabilities and security issues. This page also provides information concerning the procedures that follow any incident and public product related security advisories.

Summary

We at Dräger are keenly aware of our responsibility toward the risks, vulnerabilities, and threats to our medical devices and the potential effects on patients. Industry standard tools and processes create a trusted platform to evaluate the security of our devices. The Dräger Product Security Team collaborates and works with development engineers to ensure that risks, vulnerabilities, and threats that may lead to attacks on our products do not negatively impact the care of patients or the integrity of patient data on our medical devices and systems.

Notes

[0] Daniel Miessler: The Difference Between Threats, Threat Actors, Vulnerabilities, and Risks - Daniel Miessler

[1] https://www.medtechdive.com/news/cyber-attacks-security-medical-devices-kevin-fu-advamed/607483/.

Corporate Headquarters
Drägerwerk AG & Co. KGaA
Moislinger Allee 53–55
23558 Lübeck, Germany

www.draeger.com

Region Europe
Drägerwerk AG & Co. KGaA
Moislinger Allee 53–55
23558 Lübeck, Germany
+49 451 882 0
+49 451 882 2080
info@draeger.com

Region Asia Pacific
Draeger Singapore Pte. Ltd.
61 Science Park Road
The Galen #04-01
Singapore 117525
+65 6872 9288
+65 6259 0398

Manufacturer:
Drägerwerk AG & Co. KGaA
Moislinger Allee 53–55
23542 Lübeck, Germany

Region Middle East, Africa
Drägerwerk AG & Co. KGaA
Branch Office
P.O. Box 505108
Dubai, United Arab Emirates
+971 4 4294 600
+971 4 4294 699
contactuae@draeger.com

Region Central and South America
Dräger Indústria e Comércio Ltda.
Al. Pucurui - 51 - Tamboré
06460-100 - Barueri - São Paulo
+55 (11) 4689-4900
relacionamento@draeger.com

Locate your Regional Sales Representative at:
www.draeger.com/contact

102605 | 2311-2 | PR | LE | Subject to modifications | © 2023 Drägerwerk AG & Co. KGaA