Dräger

Industry: Medical and Safety Technology

Founded: 1889

Headquarters: Lübeck, Germany

Website: www.draeger.com

Detlef Köble

Product Security Manager at Dräger

"VulnDB enables us to actually manage vulnerabilities with the current resources that we have. It enables us to focus on our unique tasks and save time. VulnDB is exactly what we were looking for."

About Dräger

Dräger manufactures medical and safety technology products that are used all over the world. Dräger has grown into a worldwide enterprise, servicing hospitals, fire departments, emergency services, authorities, and in mining as well as industry.

About VulnDB

Risk Based Security's VulnDB® is the premier independent vulnerability intelligence solution.

Learn More at:

www.riskbasedsecurity.com

VulnDB® Enables Continuous Product Security for Dräger

With VulnDB, Dräger has comprehensive vulnerability intelligence that includes both Open Source Software (OSS) and commercial software, enabling continuous security during development and post-release.

Dräger is a leading manufacturer of medical and safety technology products, servicing hospitals, emergency response services, law and regulatory enforcement, and other industries across the world. Under their guiding philosophy of "Technology for Life", Dräger's unique offerings serve a singular purpose – to protect, support and save lives.

Operating under this mission involves responsibilities that go beyond manufacturing. To ensure the well-being of those who depend on their technology, Dräger needs to make sure their products are designed securely from the start, that their security teams can continuously monitor for vulnerabilities, and that they have the ability to remediate issues in a timely manner. It is the duty of Detlef Köble, Product Security Manager at Dräger, to operationalize this idea of continuous product security.

> "You need to build products that are as secure as possible. If vulnerabilities are not discovered, or if we don't handle security in the right way, it is a big risk to patients who are being treated by our products. We need to build and maintain them to make sure they are protected against attacks."

Integrating Security From the Start

This was the first obstacle that Köble faced. Before VulnDB, Dräger heavily relied on CVE/NVD for their vulnerability intelligence. Even when following best practices like establishing a Software Bill of Materials (SBOM), Köble found that his teams ultimately lacked comprehensive and actionable intelligence. NVD's lack of detail and sparse coverage of third-party software often left Köble's team spending time and effort conducting lengthy manual research with mixed results.

Analysts could not find all of the software components listed in their SBOM. Legacy products that used lesser known OSS or older software were often missing from CVE/NVD. To make things even more difficult, NVD entries for the components that *could* be found sometimes missed key details or contained errors. This incomplete data compromised their ability to perform timely vulnerability management.

> We needed an information provider and not a tool. We needed detailed, comprehensive data and pre-assessed vulnerabilities so we could save resources to focus on tasks that were unique to us.

What is an SBOM?

A Software Bill of Materials (SBOM) is documentation that lists the various components used by the software. This can include all sorts of third-party libraries, Open Source Software, and commercial libraries.

SBOMs are especially valuable for identifying vulnerabilities and assessing associated threats, enabling organizations to understand where their software originates from.

SBOMs can also be shared with regulatory agencies.

Better Data with VulnDB

The inefficiencies of CVE and NVD quickly put Dräger on the path to finding proper vulnerability intelligence. Köble wanted an information provider that could supply easy-to-consume intelligence. But Köble also found that Dräger's unique position in the industry required an additional need. The solution would also need to have in-depth coverage of commercial software in addition to third-party components; something that conventional scanning solutions could not provide.

> For our industry, scanning alone was not enough for vulnerability assessment. There wasn't a scanning product that could do everything we needed.
>
> We were looking for a provider that could cover both commercial software and OSS. It was important that we could perform vulnerability monitoring and pre-assessment of our software components. It was important that we had a comprehensive vulnerability data source.

Did You Know?

- CVE fails to report over 90,000 confirmed vulnerabilities
- The vulnerabilities CVE does report are often late and limited in detail

Enabling Continuous Product Security

VulnDB's powerful data and features empowered the processes that Köble put in place during development, but the greatest challenge would be maintaining security post-release. Dräger's medical devices are located all over the world, servicing an industry that has experienced the most data breaches since 2017.[1] Every new vulnerability disclosed increases the chance that a threat actor will try to exploit weaknesses. But Köble also knew that at any given time, critical metadata could be released, transforming vulnerabilities previously thought of as low priority into immediate threats.

> "You can't say your product is free of vulnerabilities. It may be for a certain period of time, but it could be hit the next day because new vulnerabilities are disclosed on a daily basis. Dräger always takes this into account. Exploitability will always change and we know that security is a permanent process."

In order to provide "Technology for Life", Köble knew that monitoring the threat landscape would be critical for the long-term safety of their customers and their patients. Aware that any device could be attacked, Köble needs to be confident that Dräger products are not the weak link in a hospital's network.

> "Most of our products are therapy and monitoring devices, so if it becomes impaired by an attack, it can have a real, serious impact on a patient's health. Therefore, we must be very careful. It's not enough to just find the 'top 10' vulnerabilities; you have to consider all the vulnerabilities that can affect the product, and then you have to actually manage them. To do that you need really good information so that you can arrive at the best decisions."

Vulnerability management is only effective if organizations can identify the vulnerabilities that affect them and remediate them in a timely manner. With VulnDB, Dräger can do just that with real-time email alerts that notify them when new vulnerabilities affecting their products are released. Once aware, Dräger can pull data on a daily basis via VulnDB's RESTful API without having to scan. This flexibility, coupled with comprehensive vulnerability intelligence enables Dräger to perform continuous Product and Application Security and other DevSecOps functions.

VulnDB has made lengthy manual research processes a relic of the past. Using VulnDB as their main source for vulnerability intelligence, Dräger is able to perform continuous vulnerability monitoring and fast track remediation using VulnDB's scanless, independently researched, and comprehensive vulnerability intelligence.

[1] 2021 Mid Year Data Breach QuickView Report

VulnDB Drives Informed Decisions

- Includes vulnerability in COTS and third-party code, Vendor Risk Ratings, and more
- Provides timely vulnerability alerts without scanning
- Trusted by leading brands including Red Bull and Adobe
- Integrates with leading tools and ticketing systems

VulnDB Features

- Real-time intelligence
- Independent research and analysis
- Coverage of COTS, IT, OT, IoT, OSS and dependencies
- Vendor Risk Ratings
- Product Risk Ratings
- Detailed exploit information
- Actionable solution information
- Over 60 classifications

Experience the Comprehensive Intelligence and Powerful Features of VulnDB

Speak to your sales representative or visit **https://vulndb.cyberriskanalytics.com/** to request a demo today.

"VulnDB enables us to actually manage vulnerabilities with the current resources that we have. It enables us to focus on our unique tasks and save time. VulnDB is exactly what we were looking for."

Contact Risk Based Security

3308 W Clay St,

Richmond, VA 23230

(855) RBS-RISK

sales@riskbasedsecurity.com

www.riskbasedsecurity.com

https://vulndb.cyberriskanalytics.com/