CYCOGNITO

CASE STUDY: HEALTHCARE

Healthcare Conglomerate Asklepios Significantly Improves Risk Exposure with CyCognito

Gains continuous monitoring and cyber risk prioritization to protect the organization and patient information

Key Results

- Ensured compliance with BSI Act and the European Union's forthcoming NIS 2 regulation
- Enhanced security posture through continuous monitoring and the discovery of previously unidentified assets and vulnerabilities
- Reduced the need for time-consuming penetration testing and streamlined remediation efforts, saving time
- Achieved significant reductions in external attack surface by shutting down unmanaged websites
- Gained comprehensive reporting to inform the Board of Directors about risk levels and security improvements

Story

Keeping patient data safe while complying with an ever-growing number of government regulations is critical for any healthcare organization. The challenge is compounded when navigating the complex IT landscape of a sprawling hospital network with limited resources. The constant threat of cyber-attacks targeting sensitive patient data, coupled with the necessity to operate around the clock, demanded a robust, efficient exposure management strategy.

Daniel Maier-Johnson, Chief Information Security Officer (CISO) of Asklepios, takes a centralized IT approach, supported by a team of 330 IT staff members divided into four sub-departments. This setup ensures harmonization and security standardization across the board.

ASKLEPIOS

CUSTOMER PROFILE

Asklepios Kliniken GmbH is Germany's second-largest private healthcare provider, operating 170 medical facilities, including 70 hospitals, and employing 50,000 people. The hospital network offers services in virtually every area of medicine, patient care, rehabilitation, emergency, and ambulatory. Three of its hospitals are designated as critical care facilities, also known as KRITIS, and are subject to legal requirements such as the Act on the Federal Office for Information Security (BSI Act - BSIG).

Asklepios' dedicated IT team of 330 manages an extensive IT environment, including some 5,000 servers, 25,0000 endpoints, and about 8,000 network devices.

"Within Asklepios, we have a very centralized approach, everything we do, we try to do from shared services," Maier-Johnson says.

To keep its technology as simple as possible, Asklepios' operations use one patient information system and one Enterprise Resource Planning (ERP) platform. The company leverages virtual desktops, which are particularly useful at facilities without an onsite IT presence.

"One of our larger challenges involves being very careful and protecting our sensitive patient data," Maier-Johnson says. "The second challenge we have is we run operations 24 hours a day, seven days a week, from the hospital side. Emergency rooms are never closed; they are always open, and our technology systems must always be available."

> **Whatever you do, you need some kind of transparency, some kind of information about how your outward-facing landscape looks to hackers. I would recommend CyCognito because it's easy to use."**
>
> **Daniel Maier-Johnson**
> CISO

Cybersecurity is a critical staff function for the technical security team and is supported by Markus Diehm, Security Analyst within the Cyber Security department. His team is responsible for the technical security of Asklepios' IT landscape, which includes antivirus protection, network detection, and vulnerability management.

Prior to implementing CyCognito, Asklepios spent a lot of effort and hours on lengthy and expensive penetration testing. They also lacked a comprehensive view of its external facing assets. The primary focus on protecting sensitive patient data, alongside maintaining uninterrupted hospital operations, underscored the need for an efficient exposure management strategy.

Protecting Patient Data Is Critical

Protecting sensitive patient data and maintaining an "always-on" operation of 50,000 employees with a team of 330 means "we have to be very efficient and very accurate," says Maier-Johnson. With healthcare data being highly valued on the black market, the risk of cyber-attacks is a constant concern. The security team is always on high alert, protecting all of Asklepios while securing potential vulnerabilities.

"Hackers like health data because with health data, you cannot only blackmail the company; you also can blackmail the patient himself... it has the same value for the customer as it has for the hospital itself," he says.

Like many healthcare organizations, Asklepios has implemented a range of detection and prevention tools alongside remediation, containment, and restoration measures. According to Maier-Johnson, these tools are deployed both on the client and server sides, as well as within the network infrastructure.

"With CyCognito, we have a dashboard where all it takes is one click to see any asset with an external interface and its vulnerabilities. Now we can focus full time on how we can fix it."

CyCognito has provided a critical addition by offering insight into potential hackers' perspectives, granting the organization a deeper understanding of vulnerabilities from an external standpoint.

"CyCognito is one of the first most important tools to understand what a hacker can see; it saves a lot of time and helps us to capture all the assets and all the vulnerabilities," he says.

Enhances External Defense

Instead of doing manual, time-consuming scans, CyCognito enabled Asklepios to shift its approach from labor-intensive penetration testing to automated, continuous external monitoring. "We're using CyCognito to automate as much as possible," says Maier-Johnson. This shift not only saves time but also provides Asklepios greater visibility into its external attack surface to manage risk more efficiently and effectively. This efficiency gain has allowed for more focused efforts on enhancing defenses and closing vulnerability gaps.

"We use it to see how we can build our wall higher and higher so nobody climbs the wall, and there are no holes or cracks that somebody can sneak through," Maier-Johnson says.

Diehm previously held a firm, static picture of the company's 500 IP addresses, certificates, and some 1,000 outside assets. "When we implemented CyCognito, I was surprised at how our infrastructure looked because you don't get this overview from anything else," he says. "With one click with CyCognito, it was easy to understand the security maturity of our public-facing IT landscape."

He was also surprised to see how much the company's external attack surface changes on a weekly basis. "I get an update weekly and quickly get an overview of new assets that have been added or possible vulnerabilities, and then our remediation process is triggered," he says. "Before, it took hours to check on our assets and many penetration tests to identify a vulnerability."

"Now, I get that with one click in CyCognito. And I don't need much time."

Closes Vulnerability Gaps

While his team monitors and detects potential security vulnerabilities, the organization's other IT departments are responsible for fixing what his team finds, he explains. Rather than passing the problem along, Maier-Johnson's team also provides information – provided by CyCognito – on how to remediate.

"We can say not only have we found something, but also we can say this is how you can fix it," he says. The cybersecurity team then uses CyCognito to see if a particular asset vulnerability has been fixed or not, at which time they can follow up.

Risk Prioritization and Remediation

With such a large organization, and one that's constantly changing, Maier-Johnson understands his team may never fix everything. "But we need to start with the most critical and the most important," he says.

By facilitating a risk-based approach to IT security, CyCognito has improved Asklepios' cybersecurity posture by providing transparency and efficiency in identifying and prioritizing vulnerabilities to remediate first.

"CyCognito is very, very important for us in our overall complete security picture," he says.

Boosts Regulatory Compliance

Because three of its largest hospitals are deemed essential infrastructure (KRITIS), Asklepios must conform to several national regulations regarding its technology infrastructure. The hospital network must comply with regulatory compliance, particularly under the BSI ACT, which includes the collection and security of patient data. "Although there are very basic requirements, you have to operate an IT system in a secure way; otherwise, you have a deviation from the regulation," says Maier-Johnson.

> **When we implemented CyCognito, I was surprised at how our infrastructure looked because you don't get this overview from anything else."**
>
> **Markus Diehm**
> Manager, Information Technology

Facing stringent BSI ACT regulations, Asklepios leverages CyCognito to swiftly identify and address compliance deviations and security vulnerabilities.

"CyCognito helps us identify deviations or violations very quickly, and we can be very efficient at fixing them," Maier-Johnson says. "We receive concrete tips, hints, and measurements on how various IT departments can fix them."

Gains Executive Reporting

CyCognito's reporting capabilities have proven invaluable in communicating security status and improvements to Asklepios' Board of Directors. CyCognito helps Asklepios identify asset vulnerabilities much quicker and provides concrete measurements, he says. The easy-to-use platform creates reports he takes to the Board of Directors.

"We can show the board 'here's what we've seen in the last quarter and the changes from the quarter before and so on,'" Maier-Johnson says. "We can also show them trends about how we are fixing our external surface."

"The entry-level screens are very easy to use, so executives can get a higher-level picture, and then the technical team can take a deep dive to get into the technical information you need," Diehm says. "Our infrastructure has grown over the years. CyCognito is helping us get a clue to what's going on outside our internal environment."

Looking into the Future

Asklepios faces the upcoming revised European Union (EU) NIS 2 cybersecurity directive, which outlines increased measures for resilience against cyberattacks, minimizing vulnerabilities, and improving cyber defense. NIS 2 will be in effect October 2024.

CyCognito's automatic detection of the external attack surface is state-of-the art and provides transparency, which will help the organization keep compliant with BSI ACT and NIS 2 regulation.

"CyCognito provides transparency about your organization's situation," Maier-Johnson says. "If you are a ship sailing in the fog, with no clue where you are, and have no radar, no lighthouse, and no acoustic signals, you have no clue. You need a monitor to send you measurements of where you are."

"Whatever you do, you need some kind of transparency, some kind of information, how your outside facing landscape looks like for hackers. I would recommend CyCognito because it's easy to use."