Interviewer: Can you please tell me about yourself?

Expert: My name is “Expert”. I work at ““COMPANY A””, the center for IT and medical technology. I work with a team that detects and responds to incidents that may occur on our endpoints. By endpoints, I mean our servers and workstations - the client computers that people use for daily work.

I'm working in the security platform where we get real-time alerts. We have monitoring on all our systems to observe whether something suspicious is happening on machines and servers. Based on that, we determine the best solution or response to a given situation.

Our team is approximately ten people. We have another team looking at the more proactive side while we focus on detection and response. The other team develops mitigations and strategies to make sure the perimeter is more secure so we don't have to go into the response and detection part.

In our work, we look through a lot of data and logs to determine the scope of a given incident or case. We follow established incident response procedures where we identify an issue, determine the scope of engagement by looking into indicators of compromise, figure out the scope of a given incident, and try to contain it to prevent it from spreading to other computers.

Interviewer: How does “COMPANY A” ensure the security and integrity of hospital IT infrastructures? I know from your profile that you work with Azure-based solutions. Can you comment about that? How secure are the systems?

Expert: On my profile I have some Azure certifications and experience, though that's not my current role. We have another team dedicated to the cloud part. For cloud security, the other team I mentioned is responsible for Prisma Cloud, which monitors policy violations in cloud incidents.

While we have a cloud department with their own tenant, we provide solutions where applications get scanned throughout the development lifecycle. We use a "shift left" strategy where code is scanned for vulnerabilities before going into production. This is all an automated process within our cloud solutions for cloud posture management.

In terms of overall security, we try our best. We have many thousands of endpoints. We try to find all active endpoints or hosts on the internet and deploy our agent, which allows us to get real-time monitoring on all our internet-connected endpoints. With this, we can deploy prevention policies for various behaviors. We define rules and manage what is allowed and not allowed on a system.

We ensure all our assets have an agent so we can see what's happening. We create custom alerts and rules based on the current threat landscape. We're in the healthcare sector, which is classified as critical infrastructure. These types of businesses are targets for threat actors, either for financial gain or sometimes for political reasons if we're not in good terms with countries like Russia or China.

We're very cautious about what software is being used, what systems, and which suppliers. It's no secret that we're skeptical of anything Russian or Chinese-related due to the geopolitical atmosphere and our own experiences. For example, we were one of the first companies in Denmark to block the usage of DeepSeek (a Chinese AI similar to OpenAI) because it was discovered that data was being sent to China. In China, if you have a business operating there, the government has the right to access all company data. We're concerned about this because we work with PhD students doing research, and if these business secrets get into competitors' hands, that would be harmful.

Our XDR (extended detection and response) agents collect logs from our firewalls, system behavior, and user context. We take all this information collectively to determine whether something malicious is occurring or if it's a false positive. It's also about understanding the organization's environment. We're a large organization with people doing custom code for automation, which sometimes triggers alerts that we need to investigate case by case.

As we learn the organization and infrastructure better, we're able to fine-tune our security products to reduce false positives. We try to deploy the latest updates for all systems, though we acknowledge that in healthcare, we have many scanners that might only work with certain legacy operating systems. For those, we implement other mitigations regarding access to these machines. We don't simply replace servers because it's costly, and sometimes these are critical machines where lives are at stake. So while we strive for best practices, realistically, security is more about processes and people. In healthcare, our primary concern is saving lives, but we try our best to keep everything updated, and when that's not possible, we implement other mitigation strategies.

Interviewer: What are the biggest cybersecurity threats facing Danish hospitals, and how does “COMPANY A” mitigate those risks?

Expert: Through multiple annual threat intelligence reports, social engineering remains the predominant technique used by external threat actors. This includes phishing emails and SMS phishing as the primary vectors for initial system access. While we're not specifically targeted, we have email filtering solutions to mitigate these threats.

Phishing remains commonly used because it's easy to automate and mass distribute. With generative AI, it's now easier for adversaries to craft better-looking phishing emails by gathering information from places like LinkedIn to personalize attacks.

The most detrimental threat I'm aware of was a ransomware incident before I started working here, around 2017-2018. Ransomware is very destructive because it renders affected systems useless by encrypting all data and demanding payment. The only real mitigation for these extortion techniques is having a good backup plan corresponding to system criticality and risk appetite, and determining how quickly you can recover.

What I've personally experienced was less detrimental - DDoS attacks against our website. Our site (regionh.dk) went down for about an hour, committed by what appeared to be a Ukrainian-based hacker group called NoName57, though it was suspected to be Russian actors proxying

their IP. This group also conducted DDoS attacks against Copenhagen Airport's website and another site called "Cold Traffic" which regulates driving laws. While not major in impact, it was interesting that they targeted an airport website, a healthcare website, and a traffic regulation website - all of which could be categorized as critical infrastructure. But these attacks didn't cause any significant disruptions to hospital operations.

Interviewer: Since we're touching the topic of Russia and Ukraine, how would you comment on the cyber attacks that happened before the war started?

Expert: We have an internal list of IP addresses from countries we block from accessing our systems. While this isn't foolproof given how IP addresses, VPNs, and traffic disguising work, it helps clean up automated attacks from "script kiddies" who use readily available tools. Just by implementing geo-blocking, we reduced network-based attacks from these countries by approximately 70%.

Our security follows a "defense in depth" strategy with different security layers. From the firewall perspective, we control which systems can interact with each other through network segmentation. We have client agents on computers so if there is a breach, we can detect it. There are multiple layers of protection throughout our infrastructure.

Interviewer: How does “COMPANY A” balance the need for accessibility and usability with strong cybersecurity measures in hospital IT systems?

Expert: It's an ongoing process involving communication with the people who use these systems. We have an internal workflow where hospital staff can create "demands" - requests for new programs, systems, or hardware. These demands go through a process where another department qualifies the information, and then they undergo a security check by us and a compliance check to ensure GDPR requirements are upheld.

We examine the technical specifications, checking if systems have end-of-support issues or if alternatives already exist that could be used instead. That's how we qualify the demands from hospitals to evaluate security or potential alternatives. All of this is audited in our configuration management database (CMDB) so we can trace what was done, why something was denied or accepted, and who made those decisions.

Interviewer: How does “COMPANY A” collaborate with national and international cybersecurity agencies to protect hospital infrastructure against cyber threats?

Expert: We have our own security vendors who host events where customers learn about the latest security news and system updates. We also participate in a threat-sharing platform with different regions in Denmark. If one region experiences a threat, they submit their findings to this platform so everyone is aware, especially if it's targeted - because if one hospital is targeted, others likely will be too.

We receive threat intelligence from numerous government organizations that conduct security research. Our security vendors also have researchers constantly monitoring new vulnerabilities or

techniques used by threat actors worldwide. It's a very community-based knowledge sharing approach to collaboration.

Interviewer: What are the key considerations when ensuring compliance with GDPR and other data protection regulations in hospital digitalization efforts?

Expert: While not specifically my department, we have tools configured with policies to detect certain data patterns that could be considered personally identifiable information or social security numbers. This is continuously being developed because there can be many false positives where data patterns look like other things.

We have tools that detect emails being sent externally from the company. If they match certain conditions, we can see that and confront the senders or even block the transmission. We regularly test for data patterns, and based on this, can create internal cases. Another department handles reporting to "Data Tilsynet" (the Danish Data Protection Agency) within the required 72 hours if we have a data breach.

For protecting information, we monitor data patterns to identify potential data exfiltration. We have private folders specifically designed to either self-delete or restrict access to people who have a legitimate work-related need to access patient journals and similar sensitive information.

Interviewer: How does digitalization in hospitals impact data security, particularly regarding sensitive patient information such as CPR numbers?

Expert: Systems that handle patient data or other sensitive information are usually restricted to certain accounts, computers, or networks, depending on the application's needs and where the data will reside. For very sensitive data where network security isn't sufficient, we sometimes preserve data on local disks to prevent interception.

For doctors or researchers who need to collaborate with hospitals or universities outside Denmark, we have a secure solution for sending data. Recipients get temporary access to a data package, and depending on the data sensitivity, we require agreements between the sender (data controller) and recipient (data processor) before any data is transmitted. You can't just send data anywhere - you need a written contract in place to use our platforms and define who receives the data.

Interviewer: How do you think general cyber warfare has affected hospital cybersecurity? How is the healthcare system affected by cyber warfare?

Expert: If you want to conduct cyber warfare and have no morality, targeting critical infrastructure with life-dependent machines connected to patients would be devastating. With recent international events, it seems there's growing desensitization to violations of international law. Just as bombing hospitals is a war crime, targeting hospital systems is equivalent to meaninglessly killing innocent people. It's something we take very seriously, especially given the political climate and violations of standard war procedures.

Interviewer: Since the US has expressed interest in buying Greenland, creating tension between Denmark and the US, how would you comment on these situations?

Expert: We're closely monitoring statements from the US and what Trump is saying, especially regarding Greenland, where he hasn't excluded the use of military power. Due to these comments, we're evaluating how to approach the products we currently use.

There was a recent article suggesting European companies should have exit plans ready for cloud platforms like Microsoft, Google, IBM, and Amazon. This is because Trump has fired multiple people from the Department of Justice who ensured contractual obligations between the USA and Europe regarding data privacy would be upheld. This raises concerns about whether America might follow China's approach to data access, which is why the article recommended European organizations have plans to migrate to European-based cloud platforms.

We're also considering blocking access to emerging AI tools like what Musk is developing with "X AI." We haven't made that decision yet, but it's something we've discussed internally due to these concerns about Denmark potentially being treated as an enemy. It's a weird political climate where supposed allies threaten each other.

Interviewer: You mentioned medical equipment and potential casualties from cybercrimes. Can you explain how medical equipment controlled by computers could be penetrated?

Expert: There are many tactics and techniques, but any attack requires access to a machine. This could happen through phishing emails where someone clicks on something and provides credentials, or through careless users who might store passwords in text files on their computers. If attackers gain initial access, they can move laterally through the network.

To mitigate this, we employ multi-factor authentication for important services, requiring more than just passwords - something you have, like a phone, or something you are, like a fingerprint. This makes it much harder for attackers who only have password information.

Attacks can happen in many ways, but the common thread is gaining network access, which should be difficult enough by itself. Once inside, attackers target the most easily exploitable systems, which can include critical systems. When an attacker breaches a network, they try to cause maximum damage or extract as much information as possible in the shortest time. Adding complexity through multiple security layers discourages attackers by making their efforts too difficult or expensive to pursue.

Interviewer: What future trends do you foresee in hospital cybersecurity, and how should infrastructure evolve to address emerging threats?

Expert: With the rise of AI, cybersecurity needs much more automation. We need automated responses to counter automated attacks. Instead of focusing on specific hacker tools, we should look holistically at the techniques being used, since there might be many exploits created daily, but the underlying techniques remain similar. Only about four new techniques emerge annually.

Another significant threat is the advancement of deepfakes - AI-generated videos using someone's face or voice clone. I personally tried cloning my voice with just 30 seconds of recording, and it sounded remarkably like me with just one sample. For a high-quality clone, you typically need about 15 samples. In the future, if we can't distinguish between AI-generated video calls that respond in real-time and genuine ones, this poses serious information security risks.

We also need to consider the high-stress work environments in hospitals, like emergency departments. Under pressure, staff might be more susceptible to social engineering attempts that mimic a superior's voice or instructions.

We need improved physical security awareness too - using identity cards properly, not holding doors open for others without verification, and being more cautious about social interactions that could compromise security protocols. These things seem logical but are often overlooked in practice because of our human tendency to be helpful.

Interviewer: What role does identity and access management play in securing hospital IT environments, and how does Azure support these security measures?

Expert: I can't speak much about Azure specifically since I don't work with it directly, but I know that not everyone has Azure access. Those who do have access are administrators with rights to certain subscriptions or resource groups. Whoever owns a resource group is responsible for ensuring correct access management.

At a recent event from our security vendor, they reported that almost 99% of all cloud accounts are overprivileged, which I'm inclined to believe. Having a good overview of who has access to what is heavily encouraged in our systems. Whenever a user access change is requested, it must go through our change management process where everything is documented.

We have alert notifications when users suddenly join higher-privileged groups, which is monitored through our XDR agents. Access management responsibility varies by system, but for all our internal solutions, we have designated technical people responsible for vendor contact regarding configurations, updates, etc. These individuals should ensure proper identity and access management for their respective systems.

Interviewer: How would you comment about identity theft prevention? We spoke about AI and two-factor authentication.

Expert: Ideally, we'd deploy multi-factor authentication everywhere so we don't solely rely on usernames and passwords, which anyone could potentially know. Instead, we'd incorporate something personal or physical that you have, like your phone. Realistically though, some systems don't support multi-factor authentication.

For physical security, our information security department runs awareness campaigns through wallpapers and other media reminding people to lock their screens, secure their ID cards, and follow basic security practices. Awareness is key.

For critical systems, we try to implement additional authentication factors beyond just username and password. In a perfect scenario with multi-factor authentication, you have something you know (password), something you have (phone), and something you are (biometric like fingerprint). These combined factors make bypassing security extremely difficult and expensive - potentially costing thousands of dollars to compromise. Nothing is 100% secure, but the goal is making systems secure enough that breaching them becomes too expensive or infeasible for attackers. This approach is especially important for our most critical systems.