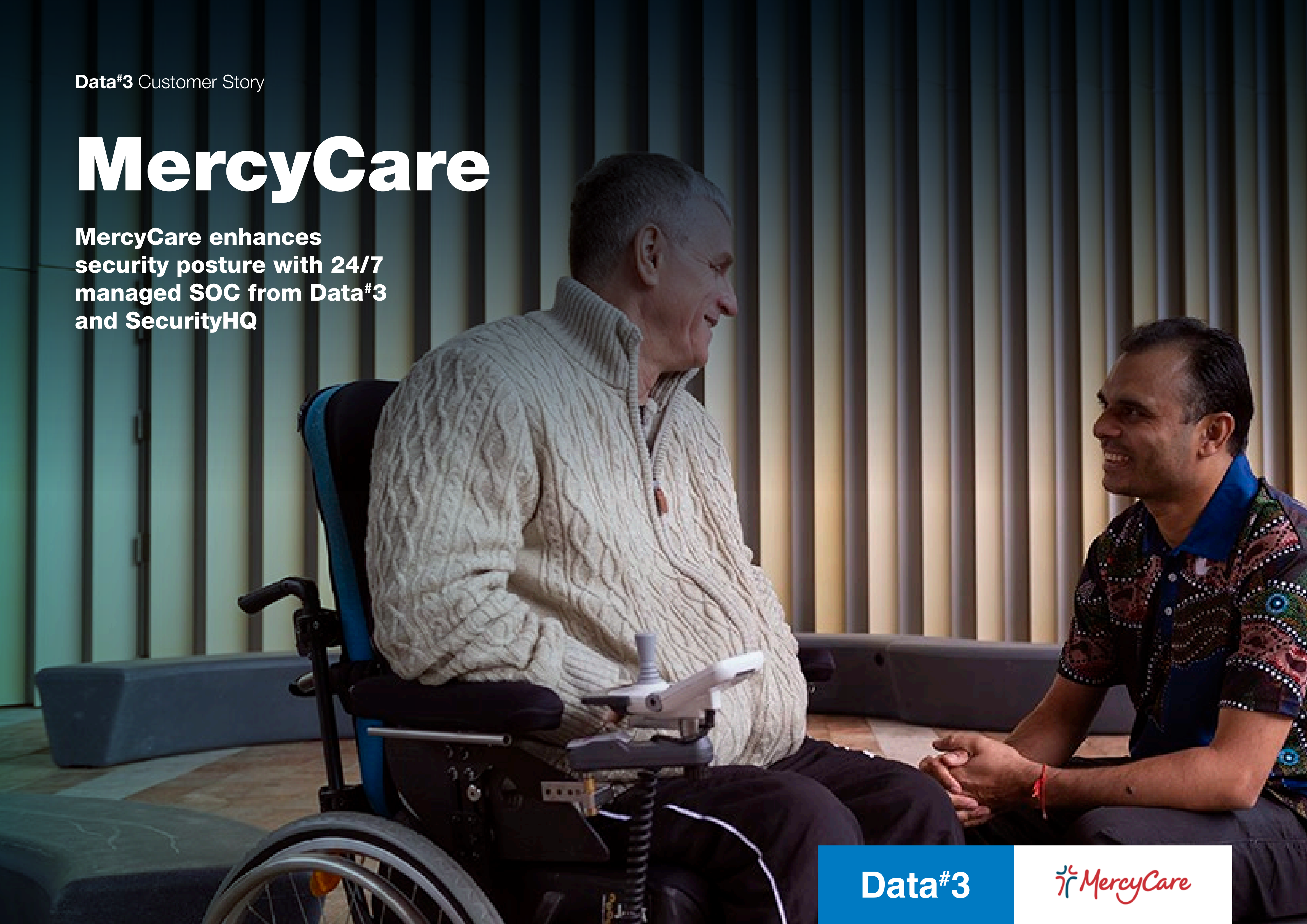
Data#3 Customer Story

MercyCare

MercyCare enhances security posture with 24/7 managed SOC from Data#3 and SecurityHQ



Data#3

MercyCare

Data#3 | MercyCare

Testimonial

“What connected us with Data#3, and their partnership with SecurityHQ was that they didn’t talk only about what they could provide in terms of technology, they connected with our values and how they could provide services that help us to achieve our goals. Our values connected from both technology and non-technology points of view.”

Armin Adineh, Manager – Information Technology, Business Services & Systems, MercyCare.

Objective

With an increasingly challenging cyber landscape, MercyCare sought to enhance their risk mitigation and response capabilities by accessing expertise and 24/7 monitoring services.

Approach

Following an audit that recommended upgrades to their cyber security strategy, MercyCare sought to find a partner with the right level of expertise who could help improve their security posture.

Project Highlight

“Data#3 has a team of technicians with a strong focus on new technology trends. By combining Data#3's expertise with SecurityHQ's service, we felt confident that we would be able to adopt a more proactive approach towards organisational security.”

Armin Adineh, Manager – Information Technology, Business Services & Systems, MercyCare.

Benefits

- Single platform to access capabilities of a leading MSSP
- Contextually based alerts
- Removal of false positives and noise
- Increased threat visibility
- 24/7 monitoring and incident response
- Guidance and mentoring for MercyCare team
- Staff and vulnerable clients are better protected
- Security skills and experience available 24/7
- Defined process in place to reduce risk
- Brand reputation is better protected

Solutions & Services

✓ Managed SOC

✓ Managed Services

✓ Security

MercyCare

> **“Security is especially important because we handle a lot of personal information about clients, service users and members of our workforce. We are committed to providing the best care and support to our clients, families and communities.”**

**Armin Adineh,
Manager – Information Technology,
Business Services & Systems,
MercyCare.**

The Background

MercyCare supports the Western Australian community, providing services ranging from early childhood settings to aged care. Their 1,400+ staff are dedicated to providing quality care and support to Western Australians through every stage of life’s journey.

The small, busy IT team at MercyCare is acutely aware of the sensitive nature of the organisation’s data, and the need to be proactive in taking steps to ensure it is well protected. An external audit confirmed that it was time to seek additional security expertise.

The Challenge

The security landscape is fast-changing. With the number of Australian organisations affected doubling in the two years to June 2022, the small, busy IT team at MercyCare, led by Armin Adineh, Manager – Information Technology, Business Services & Systems, said it was essential to take a proactive approach.

“We were a new team, and the growing risk of cyber security incidents locally had caught our attention. We were concerned about the impact an incident could have on our ability to provide care for our clients and service users, and we knew we didn’t have sufficient visibility of the network to ensure we were protected. This was compounded by a lack of documentation and understanding of our network. For us, the main thing was knowing what was happening in our systems, identifying vulnerabilities and prioritising them based on risk and impact.”

The IT team was conscious of its responsibility to some of the state’s most vulnerable; MercyCare handles personal and health-related information relating to clients, as well as staff records and financial information. The organisation also have a policy that all data must reside in Australia.

“Security is especially important because we handle a lot of personal information about clients, service users and members of our workforce. We are committed to providing the best care and support to our clients, families and communities. To do this, we need to take all necessary steps to keep information secure and operate in line with corporate compliance standards.”

“From a risk point of view, if there were ever a breach, there is potential for financial and reputational damage for our organisation, but it could also have an impact on our clients and families.”

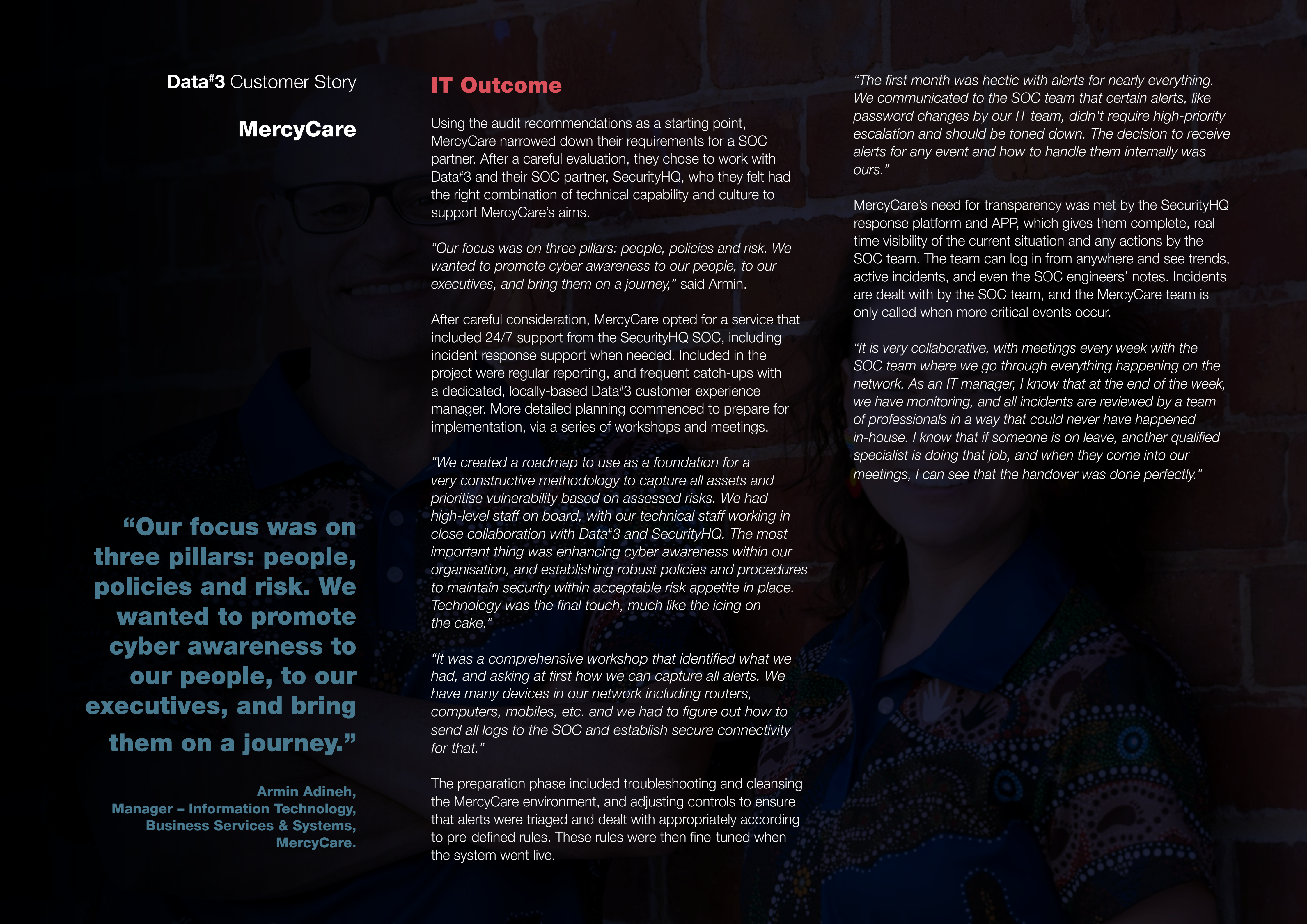
Among the challenges that Armin’s team identified was the need for round-the-clock monitoring and response from a skilled workforce. That simply wasn’t feasible given the resources available in-house. The number of alerts on any day was enormous.

“We were getting over a million security logs in a month. The task of correlating this together, and separating false positives from identified vulnerabilities, was huge, and we could not have maintained that effort at the same time as managing business as usual activities with a limited budget, it would put an unprecedented amount of pressure on our team,” explained Armin.

“Due to budgets and also other aspects of a tough market, we felt we couldn’t have the solution in-house, and we started looking at a security operations centre (SOC). If we went with a solution in-house, we would have to have at least two people to cover leave, and then what are you going to do after hours? Our adversaries won’t stop attacking after hours or because it is Christmas.”

To ensure that appropriate choices were made around possible solutions, and gain a complete picture of the situation, MercyCare invested in an independent security audit. This confirmed that external expertise was needed.

“The audit showed that we needed to have a security team to review and maintain our environment. Based on our assessed requirements and resources, the consultants with the auditors identified that a SOC was the right way to go.”



“Our focus was on three pillars: people, policies and risk. We wanted to promote cyber awareness to our people, to our executives, and bring them on a journey.”

**Armin Adineh,
Manager – Information Technology,
Business Services & Systems,
MercyCare.**

IT Outcome

Using the audit recommendations as a starting point, MercyCare narrowed down their requirements for a SOC partner. After a careful evaluation, they chose to work with Data#3 and their SOC partner, SecurityHQ, who they felt had the right combination of technical capability and culture to support MercyCare’s aims.

“Our focus was on three pillars: people, policies and risk. We wanted to promote cyber awareness to our people, to our executives, and bring them on a journey,” said Armin.

After careful consideration, MercyCare opted for a service that included 24/7 support from the SecurityHQ SOC, including incident response support when needed. Included in the project were regular reporting, and frequent catch-ups with a dedicated, locally-based Data#3 customer experience manager. More detailed planning commenced to prepare for implementation, via a series of workshops and meetings.

“We created a roadmap to use as a foundation for a very constructive methodology to capture all assets and prioritise vulnerability based on assessed risks. We had high-level staff on board, with our technical staff working in close collaboration with Data#3 and SecurityHQ. The most important thing was enhancing cyber awareness within our organisation, and establishing robust policies and procedures to maintain security within acceptable risk appetite in place. Technology was the final touch, much like the icing on the cake.”

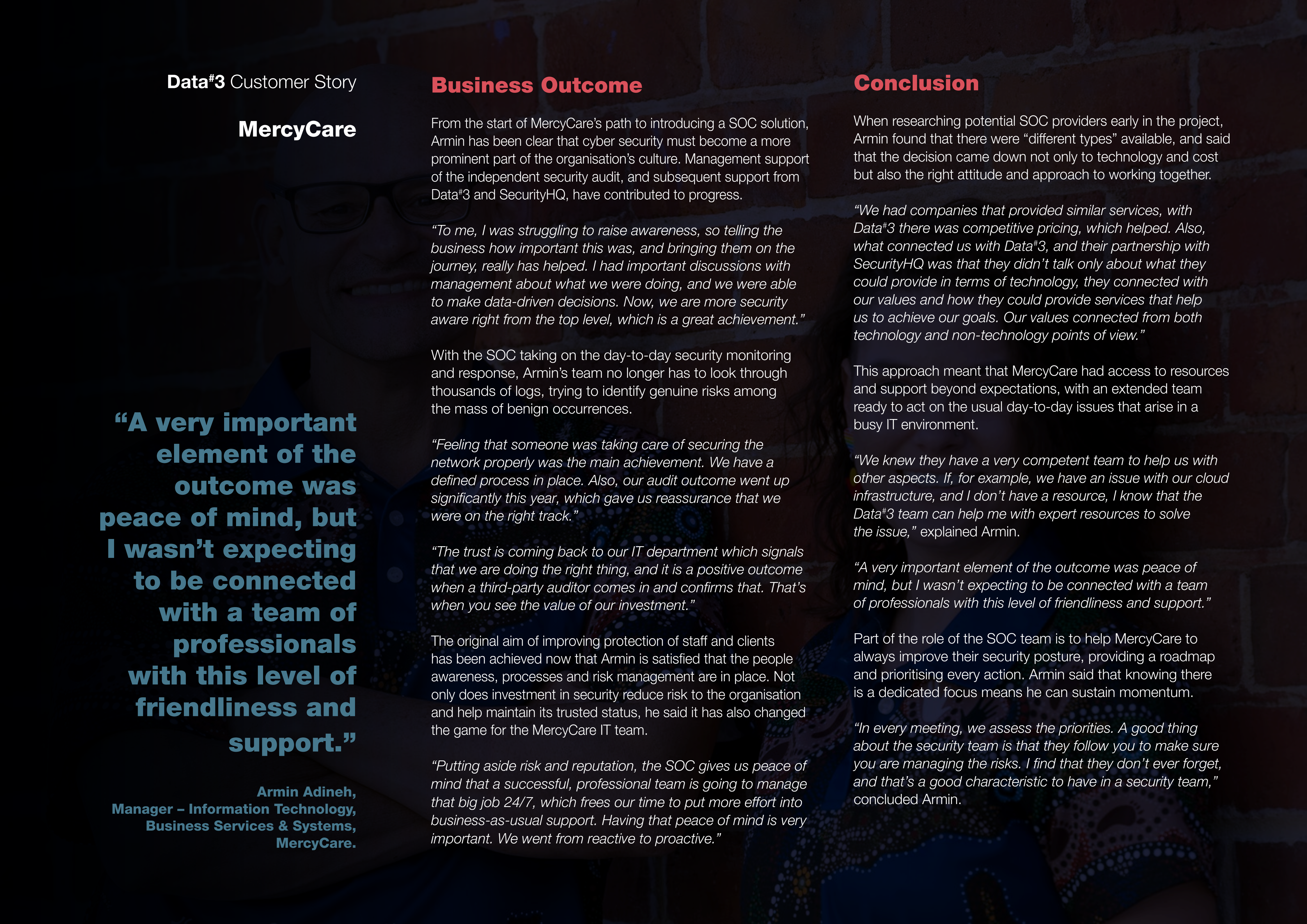
“It was a comprehensive workshop that identified what we had, and asking at first how we can capture all alerts. We have many devices in our network including routers, computers, mobiles, etc. and we had to figure out how to send all logs to the SOC and establish secure connectivity for that.”

The preparation phase included troubleshooting and cleansing the MercyCare environment, and adjusting controls to ensure that alerts were triaged and dealt with appropriately according to pre-defined rules. These rules were then fine-tuned when the system went live.

“The first month was hectic with alerts for nearly everything. We communicated to the SOC team that certain alerts, like password changes by our IT team, didn't require high-priority escalation and should be toned down. The decision to receive alerts for any event and how to handle them internally was ours.”

MercyCare’s need for transparency was met by the SecurityHQ response platform and APP, which gives them complete, real-time visibility of the current situation and any actions by the SOC team. The team can log in from anywhere and see trends, active incidents, and even the SOC engineers’ notes. Incidents are dealt with by the SOC team, and the MercyCare team is only called when more critical events occur.

“It is very collaborative, with meetings every week with the SOC team where we go through everything happening on the network. As an IT manager, I know that at the end of the week, we have monitoring, and all incidents are reviewed by a team of professionals in a way that could never have happened in-house. I know that if someone is on leave, another qualified specialist is doing that job, and when they come into our meetings, I can see that the handover was done perfectly.”



“A very important element of the outcome was peace of mind, but I wasn’t expecting to be connected with a team of professionals with this level of friendliness and support.”

**Armin Adineh,
Manager – Information Technology,
Business Services & Systems,
MercyCare.**

Business Outcome

From the start of MercyCare’s path to introducing a SOC solution, Armin has been clear that cyber security must become a more prominent part of the organisation’s culture. Management support of the independent security audit, and subsequent support from Data#3 and SecurityHQ, have contributed to progress.

“To me, I was struggling to raise awareness, so telling the business how important this was, and bringing them on the journey, really has helped. I had important discussions with management about what we were doing, and we were able to make data-driven decisions. Now, we are more security aware right from the top level, which is a great achievement.”

With the SOC taking on the day-to-day security monitoring and response, Armin’s team no longer has to look through thousands of logs, trying to identify genuine risks among the mass of benign occurrences.

“Feeling that someone was taking care of securing the network properly was the main achievement. We have a defined process in place. Also, our audit outcome went up significantly this year, which gave us reassurance that we were on the right track.”

“The trust is coming back to our IT department which signals that we are doing the right thing, and it is a positive outcome when a third-party auditor comes in and confirms that. That’s when you see the value of our investment.”

The original aim of improving protection of staff and clients has been achieved now that Armin is satisfied that the people awareness, processes and risk management are in place. Not only does investment in security reduce risk to the organisation and help maintain its trusted status, he said it has also changed the game for the MercyCare IT team.

“Putting aside risk and reputation, the SOC gives us peace of mind that a successful, professional team is going to manage that big job 24/7, which frees our time to put more effort into business-as-usual support. Having that peace of mind is very important. We went from reactive to proactive.”

Conclusion

When researching potential SOC providers early in the project, Armin found that there were “different types” available, and said that the decision came down not only to technology and cost but also the right attitude and approach to working together.

“We had companies that provided similar services, with Data#3 there was competitive pricing, which helped. Also, what connected us with Data#3, and their partnership with SecurityHQ was that they didn’t talk only about what they could provide in terms of technology, they connected with our values and how they could provide services that help us to achieve our goals. Our values connected from both technology and non-technology points of view.”

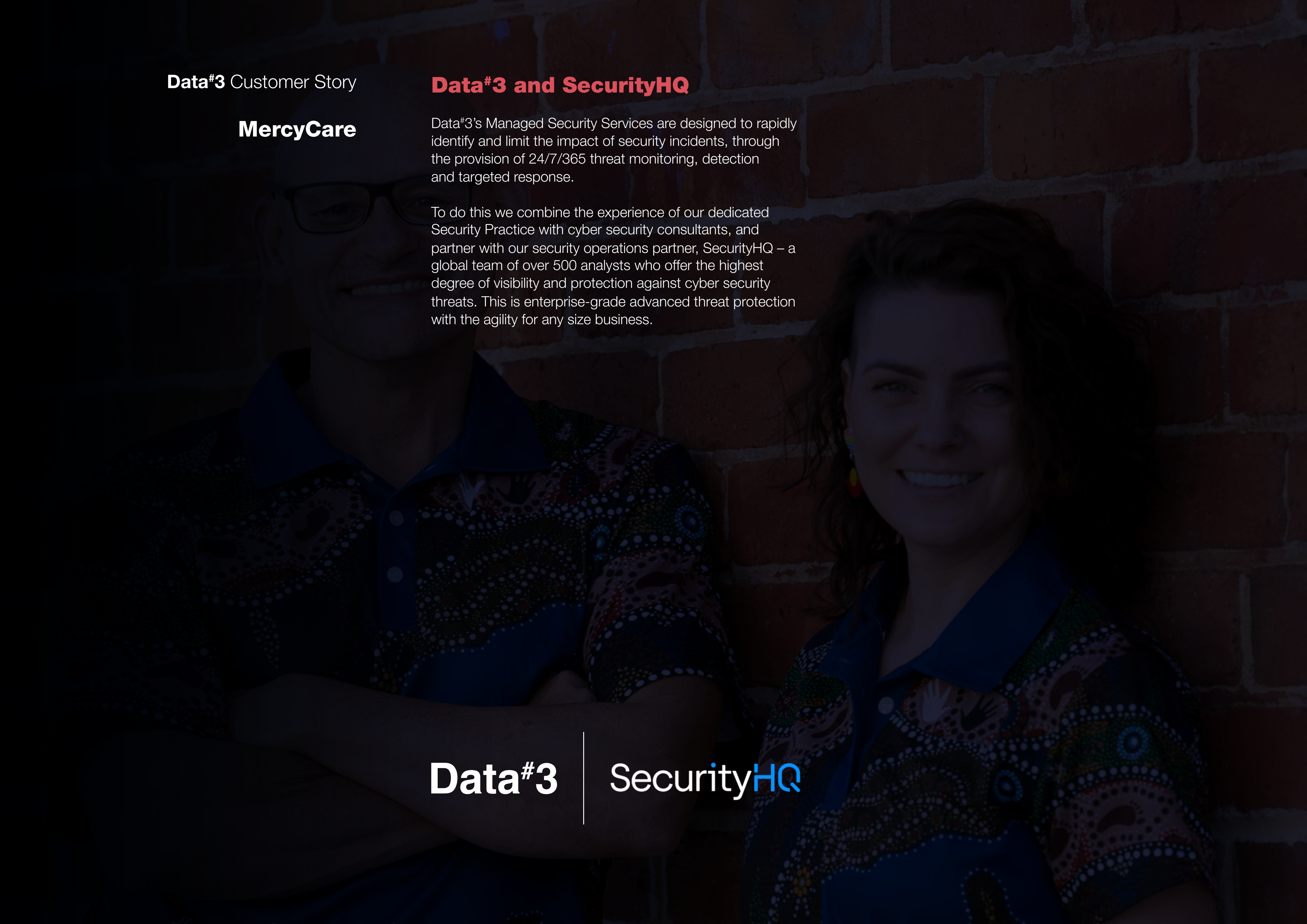
This approach meant that MercyCare had access to resources and support beyond expectations, with an extended team ready to act on the usual day-to-day issues that arise in a busy IT environment.

“We knew they have a very competent team to help us with other aspects. If, for example, we have an issue with our cloud infrastructure, and I don’t have a resource, I know that the Data#3 team can help me with expert resources to solve the issue,” explained Armin.

“A very important element of the outcome was peace of mind, but I wasn’t expecting to be connected with a team of professionals with this level of friendliness and support.”

Part of the role of the SOC team is to help MercyCare to always improve their security posture, providing a roadmap and prioritising every action. Armin said that knowing there is a dedicated focus means he can sustain momentum.

“In every meeting, we assess the priorities. A good thing about the security team is that they follow you to make sure you are managing the risks. I find that they don’t ever forget, and that’s a good characteristic to have in a security team,” concluded Armin.



Data#3 and SecurityHQ

Data#3's Managed Security Services are designed to rapidly identify and limit the impact of security incidents, through the provision of 24/7/365 threat monitoring, detection and targeted response.

To do this we combine the experience of our dedicated Security Practice with cyber security consultants, and partner with our security operations partner, SecurityHQ – a global team of over 500 analysts who offer the highest degree of visibility and protection against cyber security threats. This is enterprise-grade advanced threat protection with the agility for any size business.

Data#3 | SecurityHQ