Melbourne Racing Club

Melbourne Racing Club introduces 24/7 SOC and incident response support to bolster cyber security

Data#3

MRC Melbourne Racing Club

Data#3 | **MRC** Melbourne Racing Club

Objective

With cybercrime increasing in frequency and complexity, Melbourne Racing Club sought a security partner to help improve visibility for vital round the clock support, to support its IT team.

Approach

Melbourne Racing Club reached out to trusted partners including Data#3 to request proposed solutions. A proof of concept showed that the solution and joint expertise Data#3 and SecurityHQ offered was a great fit to meet their requirements.

Project Highlight

"For us, the highlight was improving our business security posture. Partnering with Data#3 and SecurityHQ for the managed SOC solution meant we were able to achieve a more robust, stable scenario and respond to incidents quickly."

VJ Borgohain, General Manager – Technology, Melbourne Racing Club.

Benefits

- Increased visibility of security threats 24/7/365

- Cyber security expertise and incident response available round the clock

- Intelligent security analytics deployed

- Contextually based alerts with removal of false positive and noise

- Upskilled IT team supported by 300+ security specialists worldwide

- Reduced risk and greater insight into the Melbourne Racing Club environment

- As a service model with predictable costs

- Tangible, documented steps taken to protect clients, partners and suppliers

Solutions & Services

- ☑ Security
- ☑ Managed Services

Testimonial

"We lean on Data#3 and SecurityHQ to provide that expert advice and help us align the technology stack in our environment going forward. Whether we're doing a refresh or other projects, it gives us more visibility and helps us enhance our security posture."

VJ Borgohain, General Manager – Technology, Melbourne Racing Club.

Melbourne Racing Club

> **"For us, the highlight was improving our business security posture. Partnering with Data#3 and SecurityHQ for the managed SOC solution meant we were able to achieve a more robust, stable scenario where we could respond to incidents quickly."**
>
> **VJ Borgohain, General Manager – Technology, Melbourne Racing Club.**

The Background

Melbourne Racing Club (MRC) offers a world-class visitor experience to its sporting, entertainment and hotel venues. Formed in 1875, the organisation's history plays a central role in Australia's cultural heritage.

The organisation has a busy ICT team that primarily operates during business hours, supporting the business as well as partners using the network at its venues. A modern cyber security solution was needed to aid the ICT team in protecting against evolving risks.

The Challenge

With many high-profile organisations getting hit by cyberattacks, MRC was acutely aware that every organisation must tackle this growing risk. To do so it would take the right mix of people, process and technology, and would require 24/7 resources. MRC General Manager – Technology, VJ Borgohain, said that monitoring and addressing cyber incidents involved considerable manual effort and was performed in-house.

"We had almost all of our detection and response service in-house, using different platforms and software that monitored our environment. It was up to the infrastructure team to look at that and take actions. The issue was that we all wear multiple hats; we are not dedicated security consultants, we knew we needed a partner with the expertise to monitor what comes in almost in real-time," said Borgohain.

"We work at specific times, not 24/7. Outside of business hours, we lacked the coverage needed to respond quickly."

The tasks involved in evaluating risk were increasingly time-consuming, and staff had to balance working through a volume of alerts with other priorities. Their skills were in demand to provide ICT expertise for the many events and activities that MRC hosts, ranging from sports events to conferences and charitable endeavours with the MRC Foundation.

"We knew we really needed some help, and reached out to several partners including Data#3, who took us through their managed SOC offering in partnership with SecurityHQ. We really liked what Data#3 and SecurityHQ offers in terms of 24/7 access to 300+ security consultants at SOC operations centres all over the world. This combined with the expertise of the Data#3 team meant we knew our environment would be monitored 24/7 and that we could respond to incidents quickly," explained Borgohain.

While the solution met MRC's requirements, including onshore data storage, on paper, Borgohain was keen to take a closer look at how it would work in the real world. Data#3 and SecurityHQ organised a proof of concept (POC) so they could try the managed SOC solution and consulting proposal for themselves. The speed of the Data#3 and SecurityHQ partnership was quickly put to the test.

"We went through a POC and got to understand how it all operated. In that time, we did detect an incident in the POC environment, and put it to the test. We had only set up the trial to look at a few key things in our environment. While our tools in-house also picked up the issue, Data#3 and SecurityHQ helped us to react quickly, preventing a potential problem from escalating further."

Melbourne Racing Club

"We may still get a call at 1am, but we know that it is a verified incident when that happens. There is a definite improvement in our security posture, and we know this will be an ongoing journey for us."

VJ Borgohain, General Manager – Technology, Melbourne Racing Club.

IT Outcome

The Data#3 team onboarded MRC to the managed SOC solution in a carefully managed transition. Intelligent security analytics was deployed, and the team got to work. The most noticeable changes since implementing the new Data#3 and SecurityHQ managed SOC solution have, to Borgohain, been the increased visibility and reduced false positives and noise that make it easier to pinpoint threats from the vast number of logs created daily.

"I can see from our latest monthly report that we had around 1.1 billion logs, with 2.87 million alerts, and 264 of these were from related activities, with the managed SOC narrowing it down to 49 items for further investigation."

The MRC team can view incidents on a single dashboard, making it easy to get an overall picture of the current situation and drill down into individual events. They can see in real-time any actions taken by the SOC analysts, and share any measures taken in-house. The managed SOC is used as an extension of the MRC team, giving them greater reach and allowing them to direct their efforts where they can add most value.

"Earlier, we were dependent on someone in the team looking at those logs and any alerts. They would have to process, analyse, and see what the event involved. Now the Data#3 and SecurityHQ team looks at it first and we only need to look further if it is relevant to our environment. We don't have to look at logs anymore, we are more efficient and better protected," stated Borgohain.

"We used to use several tools that we would navigate through to get a picture. Now, we get a ticket created in our dashboard and that's all we need to look at. We can invest that time doing other things in the business that enable progress."

One of the challenges at MRC had been the rapid nature of response needed as the threat landscape changed and attacks increased in sophistication. Where once, the logs would have been checked in the morning, competing for attention with many other tasks, the MRC environment is now monitored around the clock by skilled security analysts, so that responses can happen more immediately.

"For us, the highlight was improving our business security posture. Partnering with Data#3 and SecurityHQ for the managed SOC solution meant we were able to achieve a more robust, stable scenario where we could respond to incidents quickly."

"We may still get a call at 1am, but we know that it is a verified incident when that happens. There is a definite improvement in our security posture, and we know this will be an ongoing journey for us. Every month, every day, we want to keep on improving. We try to put in as many controls as we can, and we rely on our partners where we don't have the resources available."

"We get that accountability from Data#3 and SecurityHQ that saves us from constantly worrying if we are doing enough, as we used to feel when we were doing this in-house."

VJ Borgohain, General Manager – Technology, Melbourne Racing Club.

Business Outcome

When it comes to cyber security, Borgohain emphasised the importance of the entire organisation, from senior management to every worker, playing their part. The POC was an important element in gaining support.

"We do our part in making the business aware of cyber incidents including what they should and should not do. We then report to management about our security posture."

The insights available from the SOC solution are proving invaluable to Borgohain's team and have opened new insights into the task at hand. The platform includes powerful analytics that offer information about the types, frequency, and origins of attacks. Looking ahead, Borgohain expects to see the "usual increase" in cyber activity around major events in the spring racing calendar, but he is already enjoying a clearer picture.

"We can see that the last few months have ramped up. It has already been good to have the monthly report to gain visibility of trends; SecurityHQ now does the numbers and logs so I can look at and compare current activity to previous months and see how we are travelling. There are definitely peaks and troughs, and we can plan accordingly."

Having access to a worldwide team of cyber security specialists for a predictable monthly fee has proven advantageous to the in-house team and working together has led to upskilling opportunities.

"We are constantly looking at what more we can do from a security perspective, because it is important to always improve. We lean on Data#3 and SecurityHQ to provide that expert advice and help us align the technology stack in our environment going forward. Whether we're doing a refresh or other projects, it gives us more visibility and helps us enhance our security posture," reported Borgohain.

Conclusion

In a fast-evolving security landscape, Borgohain was clear that technical solutions alone are only part of the story. He said it is vital to have the right people and processes in place to continually adjust and improve security posture.

"We get that accountability from Data#3 and SecurityHQ that saves us from constantly worrying if we are doing enough, as we used to feel when we were doing this in-house. Some weeks, my team is especially busy with different big events, provisioning technology for our customers, and now we have peace of mind knowing that our security monitoring is being taken care of."

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 cybersecurity consultants, and partner with our security operations partner, SecurityHQ – a global team of over 350 analysts who offer the highest degree of visibility and protection against cybersecurity threats. This is enterprise-grade advanced threat protection with the agility for any size business.

Data#3 | **SecurityHQ**