



Qatar prepares for sporting excellence with Kaspersky



Qatar Olympic
Committee

2022

The Qatar Olympic Committee partner with Kaspersky to strengthen their defenses in the face of increasing cyberthreats as they shape up to host more world-class sporting events

The Qatar Olympic Committee is dedicated to promoting sport in Qatari society and representing the country internationally.



Semi-Governmental Organizations

- Doha, Qatar
- Using Kaspersky Endpoint Security for Business, Kaspersky Anti Targeted Attack Platform, Kaspersky Private Security Network, Kaspersky CyberTrace, Kaspersky Threat Data Feeds, Kaspersky Threat Lookup and Kaspersky Endpoint Detection and Response
- Incident response support
- 500+ employees

“Kaspersky exceeded my expectations with their features and by listening to what we needed. They gave us confidence in the product and the people behind it and enabled us to have a more secure network.”

Rashid AlNahlawi
IT Security Consultant,
Qatar Olympic Committee

The overall vision of the Qatar Olympic Committee is to make Qatar a leading nation in world peace, through innovative sports development programs and first-of-their-kind events in the Middle East. The Qatar Olympic Committee aims to promote the benefits of sport to the Qatari nation, support Qatari athletes in their development by providing world-class facilities and training, and showcase Qatari athletes on the international stage.

Challenges

The Qatar Olympic Committee were seeking a cybersecurity partner to help them safeguard their reputation, secure their data and be alert to the growing number of cyberthreats in Qatar.

Reputation and security have always been seen as top priorities for the Qatar Olympic Committee because they are a high-profile and government-backed organization. Now that they host world-class sporting events and are even looking towards a bid for the Olympics itself, these issues have become even higher on the agenda. This is because such events increase the threat of attack even further, and multiply the negative consequences in the case of a cybersecurity breach.

Cybersecurity incidents can harm reputations and business relationships, and so there was an awareness within the organization that they must be proactive in preventing incidents, as opposed to dealing with any problems when they occur.

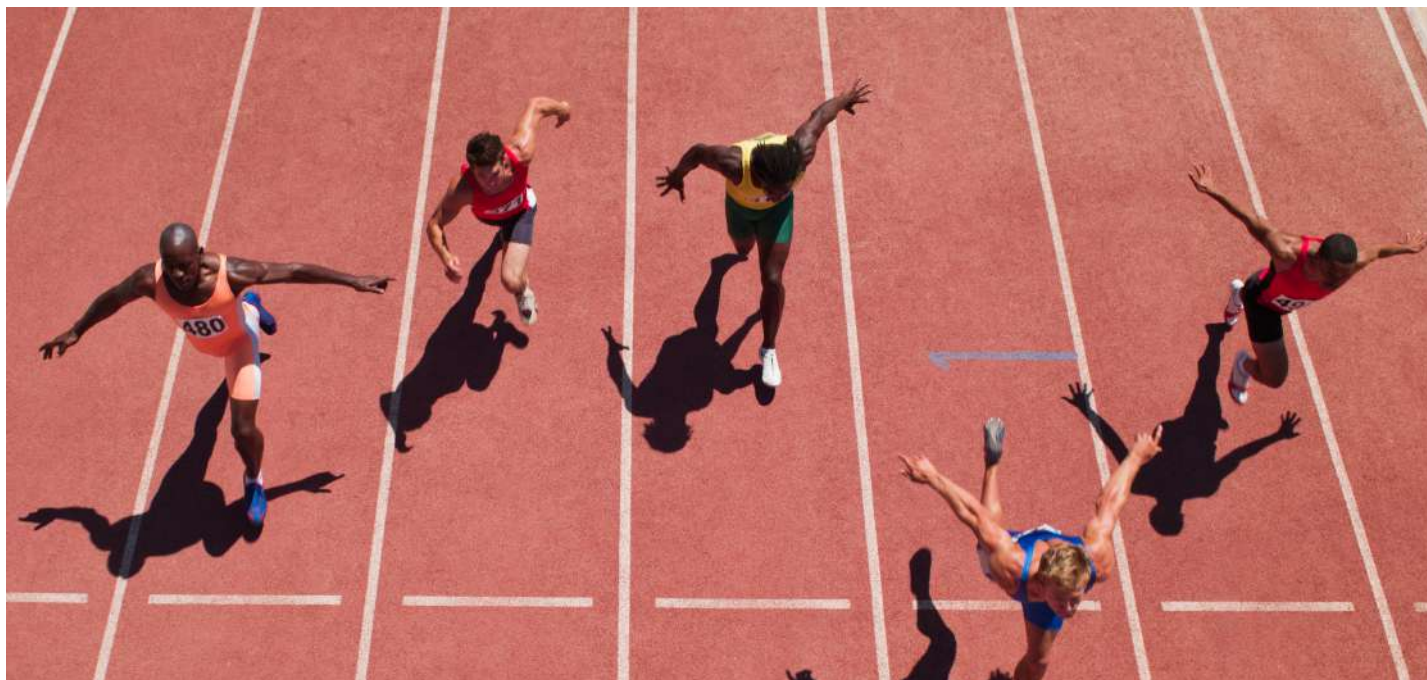
The Qatar Olympic Committee also places a high value on the security of their internal and external communications, and maintaining the confidentiality of information is very important. They were therefore seeking a solution that maintained the confidentiality of their data while allowing their day-to-day operations to flow normally.

Cyberthreats and attacks are growing in volume and sophistication across the world, and Qatar is no exception. Indeed, due to its important location and growing profile, it is fast becoming a prime target for cybercriminals.

To protect its networks from any incoming threats, the Qatar Olympic Committee has a Security Information and Event Management (SIEM) system in place, and was looking to enrich the threat intelligence capabilities of the system by working with a trusted cybersecurity partner.

The Kaspersky Solution

Kaspersky provided the Qatar Olympic Committee with an end-to-end integrated cybersecurity solution featuring Kaspersky Endpoint Security for Business, Kaspersky Anti Targeted Attack Platform, Kaspersky Private Security Network and Kaspersky CyberTrace.



Detection

Solutions improve detection rates and accelerate response



Performance

Internal teams have new tools to repel attacks and enhance security



Cost effective

Feature packed solutions at competitive prices



Support

Kaspersky teams are always available to help with any queries

Kaspersky Endpoint Security For Business

Kaspersky Endpoint Security for Business has been implemented on all endpoints including workstations and mobile devices, along with mail server security, to provide multi-layered adaptive protection against endpoint risks such as phishing, social engineering and ransomware attacks.

The implementation uses light agents controlled from a centralized dashboard which also facilitates remote management and patching of endpoints, making it easier for IT teams to patch in real-time.

Kaspersky Anti Targeted Attack Platform

Kaspersky Anti Targeted Attack Platform has empowered the internal Security Operations Center (SOC) team of the Qatar Olympic Committee to handle and respond quickly to incidents. The platform monitors data from various sensors including endpoints, networks and mail servers, and analyzes this in real time to alert the team of any incidents or suspicious behavior. The SOC team is then able to isolate and analyze incidents using an advanced sandbox and test their responses before deployment. The team has also been able to be more proactive by conducting manual threat hunting across the network and endpoints.

"KATA is something that you cannot see outside Kaspersky's world, and ahead of any product that I have ever seen," says the Qatar Olympic Committee's IT Security Consultant, Rashid AlNahlawi. "It combines seven advanced technologies to analyze, detect and deter threats originating from three different channels - mail, web and endpoint. This adds flexibility to most previous methods of customizing threat detection and response. In effect, with KATA Kaspersky has extended the definition of endpoint detection and response from a supporting security system to a 'Swiss knife' platform for security detection, threat hunting and forensics.

"Detections are almost instant, and include very clear presentation and extensive information on all causes of the threat. My and my team's cybersecurity knowledge have been enriched by reading the information on detections provided by KATA, and we all feel more confident in our skills. It also has a powerful threat hunting capability to drill down on individual cases or events. We don't need to validate issues using different applications or screens apart from KATA's, and it's very easy to use."



Threat intelligence

To provide the Qatar Olympic Committee with real-time threat intelligence, Kaspersky implemented Kaspersky Private Security Network and Kaspersky CyberTrace. Kaspersky Private Security Network provides real-time threat intelligence, while CyberTrace ensures that intelligence is matched with other sources and fed into the SIEM system to help build a proactive intelligence-driven defense.

Kaspersky Private Security Network delivers accurate cloud-based threat intelligence with minimal false positives, all without releasing any data outside the organization's perimeters. Kaspersky Private Security Network and CyberTrace together enable the SOC team to detect threats quickly and respond appropriately.

In addition to the solutions provided, Kaspersky also supports the Qatar Olympic Committee's IT security team with a full incident analysis and response service.

Outcomes

"Since implementing the Kaspersky solutions, the Qatar Olympic Committee has experienced a far higher detection rate of incoming cyberthreats and has been able to deter them effectively," continues Rashid AlNahlawi. "Regular updates from Kaspersky have meant that any emerging global threats are fully factored in and countermeasures deployed in a very quick time".

"The solutions in place have helped internal teams mitigate numerous attacks that their previous security control would not have been able to detect or repel, and the existing SIEM solution has been enhanced and is now detecting threats more effectively".

"The internal SOC team has now been fully equipped with an arsenal of tools to repel any attack. We found the new tools intuitive to use and with only a short learning curve for them to become proficient. As a result, we are now more capable, more productive and more able to focus on the organization's priorities rather than constant firefighting".

"We're pleased with the scalability of the solutions that have been implemented, since they expect to see substantial growth in the coming years," he concludes.

The Qatar Olympic Committee commented that the support provided by Kaspersky during the implementation phase and when responding to incidents was especially helpful and they are now considering moving to a managed service model.

Overall, compared to their previous security control, the Qatar Olympic Committee is more protected, more responsive, and better able to deal with the growing levels of cyberthreats that they are facing thanks to their partnership with Kaspersky.

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
IT Security for Enterprise: kaspersky.com/enterprise

www.kaspersky.com

kaspersky BRING ON
THE FUTURE

2022 AO Kaspersky Lab. All rights reserved.
Registered trademarks and service marks are the property of their respective owners.