The Inter-Services Cyber Network Defence Challenge

When representatives from the MOD met to take part in the Inter-Services Cyber Network Defence Challenge, it was not only their cyber security technical skills that got put through their paces. The need for precise communications, rapid decision making and above all, teamwork was paramount for the winning team to be crowned the Cyber Defender Capture The Flag Champions.

Hands on challenges designed to test the best:

The 2018 Inter-Services Cyber Network Defence Challenge (ISCNDC) pitted four teams – Army, Royal Navy, Royal Air Force and Civil Service – against each other to compete for the coveted ISCNDC Challenge Champion award at QA's Cyber Lab in London.

Designed to test both individual technical ability and the teamwork skills of experienced Cyber Professionals, the Capture The Flag (CTF) event focuses on teaching those who attend to detect and respond to Cyber attacks.

QA's state-of-the-art Cyber Lab enables the teams to learn in a way that no other training does. Through collaboration, competition and simulation, those that attend experience real time cyber-attacks in a safe, controlled environment.

Working against the clock, the teams work together to solve Cyber Security challenges, deploying solutions to solve the tasks, enabling them to 'capture the flag' and earn points in their bid to be crowned champions.

With constant guidance from QA's expert Cyber instructors, the teams are supported throughout the experience to ensure their learning is maximised.

> "We were given multiple time sensitive tasks, requiring us to employ clear communications and engage the versatile skills of our team to meet the demands of the scenario.
>
> **The event provided a clear opportunity to develop my technical skills alongside my leadership skills"**

Four days of Cyber Security Challenges

Run over four days in QA's unique Cyber Lab in London, the teams experience a range of carefully constructed Cyber challenges to test their Cyber Security skills and leadership.

With the challenges scored, this event fuses hands-on immersive learning with the added incentive of competition to give the attendees a truly unique learning experience.

Day 1 : Saw the participants placed in unfamiliar roles, working as teams to deal with a seismic challenge in the morning's Crisis Management session. Strong prioritisation and communication skills were required as the scenario unfolded. The afternoon session introduced the role of OSINT in cyber defence and forensics.

Day 2 : The second day focused on threat hunting and was designed to test the various cyber disciplines of CTF participants as part of a time-bound event. The tiered threat hunting challenges test even the most experienced Cyber Defenders through advanced labs that offer a complex labyrinth of systems within which the teams must work to find flags and earn points.

Day 3 : Broken into four challenge rounds, day three tested the participants' individual and team skills to the maximum. Whether dealing with cryptographic puzzles, decoding data, securing compromised systems or performing a number of other tasks covering the expansive suite of tools within the Kali Linux environment, this day was designed to push their capabilities to the limit.

Day 4 : The final day culminated with the teams being subjected to an intensive series of real-time attacks that they must dynamically respond to and defend against. Day four is arguably the most hotly contested (there's points at stake), with rewards scored by teams when they identify and secure vulnerabilities, but also the reality that every second of system downtime costs 'money'.

" This was an amazing opportunity to represent my team and understand my own skills, leadership and personal capability for Cyber..."

To learn more about running a Cyber Security challenge event, or courses and certifications in Cyber, contact QA

QA.COM/CYBER

0345 074 7978

QA transforming performance through learning