The competition will be marked by your ability on solving challenges and will be later reviewed by a panel of Judges. The national's competition has been designed in line with the finals [Lyon] and below is the list of skills required for the 3 days comp.

SKILLS REQUIRED

- Networking – TCP/IP Layers
- DNS architecture and its components
- Application protocols like HTTP, FTP, TLS, HTTPS, SSH etc.
- Network Security – Firewalls (Palo Alto), Zones, ACLs, Advance features relevant to enterprise Network like SSL VPN etc.
- Firewall/NGFW – Concepts and hands-on
- IP Networking -Switches, routers, Enterprise Network architecture.
- HTML, browser developer tools, XML, JavaScript, web application exploits,
- Python and other scripting languages.
- Operating Systems concepts
- Windows Operating System
- Advance Windows feature like Active Directory, Windows Logging Management, etc.
- Linux operating system and different flavors.
- Kali Linux & different tools like Nmap, Metasploit etc.
- Common attack tools and techniques.
- Knowledge of Kill Chain and Mitre ATT&CK framework.
- Vulnerability assessment
- Reverse Engineering
- SIEM (Splunk) – Understanding of Basic search and Regex Queries
- User Identity and Access Control
- Malware Analysis, knowledge of common tools like Autopsy
- Memory dump analysis, useful tools Volatility
- Different APT Attack lifecycle
- Incident Response Process Understanding
- Basic Computer Programming/Coding knowledge
- Forensics Skills
- Team Co-ordination
- Problem solving techniques.
- Documentation

I just wanted to provide an update, that I have recently spoken with the chief judge for the Cyber Security competition, and as I said on the training weekend, the basic breakdown for the competition is:

- Infrastructure Setup and Security Hardening – Particularly Active Directory, and firewall knowledge (he isn't sure whether it will be a Palo Alto VM yet, but says that this is strongly encouraged)
- Cyber Security Incident Response – Wireshark, Splunk, Event Viewer
- Capture The Flag – He strongly encourages a deep understanding of Linux, and it's tools

If I get anymore specifics I will provide you with updates.

It should be noted that Mick said in the meeting for competitors last night, that internet access will provided for the competition for the skills that require it. Cyber Security was specifically mentioned as being one that would get internet access.

	Team Red	Team Blue
Day 1	Module A Enterprise Network Security Hardening	Module D Network Forensics and Analysis
Day 2	Module B Application Security Hardening	Module E Digital Forensics and Investigation
Day 3	Module C Investigative Network Security	Module F Process Investigation and Behavioural Analysis