Assessment Blueprint – Questionmark Critical Cyber Diagnostic Test by CyberVista

Status: Final

Date: 6 May 2021

Approved by: Questionmark and CyberVista Assessment Experts

General information

Purpose of assessment	To measure proficiency in a cybersecurity knowledge and skills across seven key domains based on the NICE Framework.
Level of skill	Intermediate - it is designed to test specialist cybersecurity knowledge rather than day-to-day best practise.
Target audience	• Job roles with specific responsibility for managing cybersecurity such as security engineers and security operations center (SOC) analysts; • Job roles which involve handling sensitive data such as network administrators and solutions architects.
Limitations	Due to time limitations, this assessment cannot cover all seven domains exhaustively, so the skill level of the questions is higher than other diagnostics. This means the results can identify weaknesses and strengths, but not a comprehensive range of proficiency levels.
Topic coverage	This assessment is based on an analysis of security professionals and directly aligns to the Workforce Framework for Cybersecurity, known in the US as the NICE Framework. It consists of the 7 domains, see below for the areas covered.

www.questionmark.com

USA
35 Nutmeg Drive
Suite 330
Trumbull, CT 06611
+1 (203) 425 2400
(800) 863 3950

UK
New Kings Beam House
22 Upper Ground
South Bank
London SE1 9PD
+44 (0) 20 7263 7575
0800 731 5895

Germany
Hopfenstr. 8,
80335, Munich
+49 (0) 89 220 61272

Australia
RSM Australia, Level 13
60 Castlereagh Street
Sydney NSW 2000
GPO Box 5138
Sydney NSW 2001
+61 2 8073 0527

Language	Test is presented in US written English. Participants can be native English speakers or should have at least B2 level of English if not a native speaker.
Format	Online test presented in Questionmark software, automatically scored.
Accessibility	Some questions contain graphics/images/media.
Time limit	30 minutes.
Number of questions	Participant to be presented with 21 questions out of 28.
Question types to be used	Combination of: • multiple choice • multiple response • ranking • hotspot • text match • matching
Scoring	All questions weighted equally (one point per question). No negative scoring.
Feedback	Participant to be given at end of test: • Overall score • Helpful question level feedback for wrong answers, giving the correct answer
Learning Resources	This is a subset of the diagnostic used as the baseline in CyberVista's Critical Knowledge Course which teaches the foundational knowledge and skills needed for a cybersecurity professional, no matter where they sit within the organization.

Detailed topic coverage:

- Network fundamentals: basic concepts and techniques of computer networks
- Threats and attacks: common types of cyberattacks, vulnerabilities they exploit, and effective countermeasures
- Network security: security mechanisms and techniques implemented in secure computer networks
- Security engineering: general cryptography, identity and access mechanisms, and physical security controls
- Risk management and governance: risk management, business continuity, governance, and compliance strategies for organizations
- Security operations: basic security and business functions, strategies and tasks employed by secure organizations
- Offensive and defensive schema: offensive and defensive concepts and practices employed by blue, red, and purple teams

If you have any questions, please ask your Questionmark account manager or reach out to content@questionmark.com.

www.questionmark.com

USA
35 Nutmeg Drive
Suite 330
Trumbull, CT 06611
+1 (203) 425 2400
(800) 863 3950

UK
New Kings Beam House
22 Upper Ground
South Bank
London SE1 9PD
+44 (0) 20 7263 7575
0800 731 5895

Germany
Hopfenstr. 8,
80335, Munich
+49 (0) 89 220 61272

Australia
RSM Australia, Level 13
60 Castlereagh Street
Sydney NSW 2000
GPO Box 5138
Sydney NSW 2001
+61 2 8073 0527