Which Blue Team Would You Belong On?

a Cybersecurity Awareness Month quiz brought to you by CRITICALSTART

A blue team's job is to defend and protect a company's information systems. They detect vulnerabilities, identify threats and prevent breaches. There are several different types of blue teams in the cybersecurity world – which one would you belong on?

Question 1 – Which activity would you prefer?

A. Paintballing
B. Reading
C. Cooking/baking
D. Playing computer/video games

Question 2 – What's your favorite type of game?

A. First person shooter like Counter-Strike
B. Strategy like Risk
C. Mystery/sleuth like Clue
D. Role-playing like World of Warcraft

Question 3 – Which job would you prefer?

A. Cop or army
B. Market researcher
C. Forensic scientist
D. Bodyguard

Question 4 – How would you react in a tricky situation?

A. Jump right in and respond quickly
B. Try to find out all the information before reacting
C. Analyze what happened and find out why
D. Take a look at the situation from all angles

Question 5 – Which best describes you?

A. I'm always ready to go and take action
B. I like to plan ahead
C. I'm very detail-oriented
D. I like helping others

Which Blue Team Would You Belong On?

a Cybersecurity Awareness Month quiz brought to you by CRITICALSTART

If you got mostly A's, you would be on the Cyber Incident Response Team (CIRT)!

The CIRT is always ready to take action the moment a breach occurs. Services include reactive emergency response and incident readiness, proactive planning & strategy, IR retainers and digital forensics investigations. Our experienced team acts as an extension of your security team to enhance your ability to respond to a security incident, minimize your risk and improve your security posture.

If you got mostly B's, you would be on the Cyber Research Unit (CRU) !

The CRU amplifies the effectiveness of your security tools and improves your overall SOC efficiency. Threat detection content and cyber threat intelligence are important tools in fighting cybercrime. This team helps you stay one step ahead of threat actors by researching new and emerging threats and providing guidance on addressing them, as well as quickly developing and deploying new detections to prevent breaches.

If you got mostly C's, you would be on the Digital Forensics & Incident Response (DFIR) Team!

Our CIRT Team's Incident Response (IR) services include crisis management through critical stages of an incident, 24/7/365 monitoring and threat hunting, briefings with final reports and malware reverse engineering. Digital Forensics Services provides forensics investigators with experience in governance standards for highly sensitive investigations, courtroom testimony, forensic imaging and analysis for comprehensive investigation results, final investigative reports from an executive to a technical level and evidence seizure, chain-of-custody and secure storage that directly align with the NIST framework.

If you got mostly D's, you would be in the Security Operations Center (SOC)!

As part of our MDR service, our SOC provides 24/7/365 security monitoring, investigation and response, consistently meeting or exceeding one-hour SLAs for Time to Detection (TTD) and Median Time to Resolution (MTTR). This team is comprised of security experts who focus on simplifying cybersecurity and optimizing business outcomes. Upon receiving an alert that was not automatically resolved by our ZTAP™ platform, our SOC analysts determine the scope of the problem to build a full narrative of the threat. Then they communicate with your security team through ZTAP and MOBIL**SOC**®, our iOS and Android app, to contain and respond to alerts.