Testing cybersecurity countermeasures in a network is an essential step to ensure that the security measures you have put in place are effective and adequate. Here are some steps you can take to test your cybersecurity countermeasures in a network:

1. Penetration testing: Penetration testing is a simulation of a real-world cyber attack on your network. The objective of this test is to identify any vulnerabilities that exist within your system, which attackers could exploit to gain unauthorized access to your network.
2. Vulnerability scanning: Vulnerability scanning is an automated process that scans your network for potential vulnerabilities. This test can identify weak passwords, outdated software, and other common vulnerabilities that could be exploited by attackers.
3. Social engineering testing: Social engineering testing involves simulating attacks that manipulate people to disclose sensitive information or perform actions that could compromise the security of the network. This type of testing can include phishing attacks or physical security breaches.
4. Firewall testing: Firewall testing can help you identify any weaknesses in your firewall configurations, which can be used by attackers to bypass your network defenses.
5. Intrusion detection testing: Intrusion detection testing can help you verify that your intrusion detection systems are working correctly and effectively. This test can involve simulating an attack and checking if your systems are able to detect and alert you to the attack.
6. Security Information and Event Management (SIEM) testing: SIEM testing is a method of testing the effectiveness of your security monitoring and alerting capabilities. This test can include simulating different types of attacks and monitoring how well your system detects and alerts you to the threats.