Red teaming is a test to ensure cybersecurity. It answers the question: if your system gets attacked, then will your important assets be safe or not? In other words, you observe your network from the opponents' viewpoint.

## Five reasons why

The following five reasons justify why you should use the red teaming test on your network:

### Safeguard your critical assets

You cannot measure the potential danger coming ahead until you step in the shoes of the intruder. A system or network having essential and crucial information is always under threat. Thus, you should be able to safeguard your critical assets. One way to do this is by red teaming test, in which you focus on any impacts of an outside attack on your assets.

### Free from internal biases

The previous penetration tests had a flaw in internal biases. The internal team would set their scope for the test, which was based on internal preferences. However, this bias is not present in red teaming because no constraints can apply to the test. The scope of this test is wider and actual path of attack is found.

### Discover the weakness of your system

The testing team may overlook your system's weaknesses and loopholes, but the red team can expose all these fault lines. Red teams are not a part of your organization, which is why they will do an in-depth search from your system. Thus, you won't just probe over one same spot all over again.

### Test your response capabilities

We usually develop a network strong enough to stop an attack, but to be sure about our system's response capabilities, it is vital to have red teaming. You will get to know about your system's real-time incident mitigation capabilities to stop a real attack. If you conduct conjunction with the red and blue team, then your response capabilities will become an open and shut case.

### Cost-effective bespoke toolsets

Red teams use custom toolsets which a real attacker uses to hack your information. Thus, you can prevent a massive loss of your company/organization with a red team's help. As 'Prevention is better than cure,' so if you invest at this level for a red team, it is better than to wait for a real attack.

## Conclusion

The red teaming results will provide you with a clear picture of the possible threats your system can face. Thus, it is beneficial to hire a red team than to allow intruders to take your precious information.