Red Team assessment is an increasingly popular way for organisations to get a realistic approach towards their overall security. Attack surfaces of organisations are constantly growing. Hence, identifying vulnerabilities that an attacker can potentially target is an invaluable task. Red teaming is likely to become a more popular methodology in future. Here are some trends that are most likely to drive the future of red team assessments.

**Intelligence-Driven**

With a large amount of data available for known vulnerabilities, red team assessments in the future will focus more on potential attacks expected to take place. By aggregating and analysing data such as vulnerabilities, hacking tools and techniques, and common attacks, organisations can identify an attack they are most likely to face and also classify the possible targets.

**Security Regulations**

The regulatory landscape in recent years has dramatically evolved. Data breach threats have driven governments to pass security regulations to protect user data. Some of these regulations include the well-known General Data Protection Regulation (GDPR), HIPAA, SOX and PCI DSS. It seems likely that red team assessments will be driven by the requirement to demonstrate compliance with the applicable standards and regulations. Some of these regulations require routine testing, whereas all of them charge heavy fines for incompliance. When non-compliance costs outweigh the costs of security testing, red team assessments with compliance focus will gain more popularity for testing an organisation’s security posture.

**Machine Learning and Automation**

A Red Team assessment aims to simulate how hackers can attack an organization, so as to identify vulnerabilities. It typically includes a procedure mixing structure with flexibility. However, many activities the red team performs are repetitive and based upon information collected from previous assessments. These activities are suited to an automation tool that can decide the next logical step based upon the previous information it holds.

As artificial intelligence and machine learning mature, red teams can more likely use them in their operations. An ML based tool can provide scalability to red teams and allow security analysts to focus more on attack vectors with higher potential.

**Human-Focused Assessment**

Social engineering in a security assessment can sometimes be a hard sell with some customers. At times, it can backfire if not managed properly, since employees may backfire if they feel that the management has caught them not complying with security policies. However, the reality is that human error is the biggest factor resulting in cyber-attacks, hence, targeted the most. As customers realise the importance of testing vulnerabilities associated with employee negligence, Red Team assessments are likely to become more human-focused.

Aardwolf Security provides complete best Red Team assessments to meet your security needs. Contact us today to find out more.