异常检测与响应(EDR)是现代安全领域中的一种重要技术，它的目的是识别有害的活动，威胁和被攻击的行为，并启动一系列反应，以防止系统和网络的损害。的网络安全方案，包括防火墙、反病毒、入侵检测和其他形式的安全控制，可以防止外部恶意攻击。但是，今天，攻击者正在使用植入系统内部的各种技术来绕过安全层级，对系统和数据造成严重损害。异常检测与响应系统可以解决这一问题，并允许安全团队更有效地检测、识别和响应有害活动和攻击。

EDR工作原理非常简单：它使用多种技术来记录、用户、和文件的运行，以检测异常活动和行为，判断其类型，并根据可靠的证据响应潜在的情况。 EDR可以对网络中发生的各种活动进行实时监控，它还可以帮助安全团队发现安全漏洞，并有效地响应安全事件和威胁。EDR可以收集有关被攻击和被盗的存储文件、已执行的程序以及活动的其他相关信息，使安全团队能够更好地理解安全漏洞，并从中采取有效的补救措施来阻止恶意攻击和数据泄露。

EDR的实施主要取决于企业的安全态势感知，以前的安全方案主要关注网络层次的安全态势感知，而EDR则考虑级、文件级和内存级，以及系统上已安装的程序和文件。 EDR可以更有效地实时监控和跟踪用户和的行为，还可以通过恶意文件和来发现威胁。

EDR还可以提供深入的可视化运行，使安全团队可以快速响应和处理安全问题，防止攻击行为和数据泄露同时，还能够更好地发现潜在的攻击和威胁。此外，EDR还支持安全团队能够收集重要的后果证据，从而对其他攻击行为和潜在威胁建立更加完整的侦查网络。

EDR技术正越来越重要，它可以帮助企业构建安全层级，防止外部攻击，并更有效地应对内部恶意活动。EDR可以将企业的安全层级提升到新的高度，让企业的数据安全更好的保护。