警报疲劳不仅仅代表安全运营中心 （SOC） 团队的不便;它对企业安全构成了切实的威胁。当分析师每天面对成千上万个警报的洪流时，每个警报都需要进行分类、调查和关联，宝贵的时间很容易浪费在误报上，可能会忽略整个企业数据泄露的真正指标。