Переработки, неудовлетворённость и выгорание – что ещё отпугивает кадры в ИБ-отрасли?

Согласно новому отчёту компании Bitdefender – это румынская компания, которая разрабатывает и производит программное обеспечение для защиты от вредоносного ПО и интернет-угроз, включая антивирусное ПО, фаерволы, VPN и инструменты для безопасности сетей и мобильных устройств. Bitdefender использует инновационные технологии машинного обучения и искусственного интеллекта для обнаружения и блокировки угроз. Компания была основана в 2001 году и зарекомендовала себя как одна из ведущих производителей антивирусов." data-html="true" data-original-title="Bitdefender" >Bitdefender, более 70% специалистов по кибербезопасности часто вынуждены работать по выходным для решения проблем безопасности в своих организациях.

Высокая нагрузка тесно связана с неудовлетворённостью работой, что подтверждают 64% из 1200 опрошенных специалистов. Они заявили о намерении искать новую работу в течение ближайших 12 месяцев.

Особенно остро проблема выгорания и неудовлетворённости работой стоит среди британских специалистов, где 81% часто работают по выходным, а 71% планируют сменить работу. В Германии 77.1% специалистов работают по выходным, а более трёх четвертей (76.6%) намерены искать новую работу в ближайшее время. В США же около 70% специалистов часто работают по выходным, а 62.2% планируют сменить работу.

Навыки в области кибербезопасности остаются критически важными, несмотря на сокращения в командах безопасности. В отчёте отмечается, что 57% организаций за последние 12 месяцев столкнулись с утечками данных, что на 6% больше по сравнению с прошлым годом.

Тремя основными угрозами, по мнению опрошенных, являются фишинг и социальная инженерия (33%), уязвимости ПО и 0day-бреши (32.2%), а также вымогательское ПО (29.3%). Кроме того, почти все специалисты (96%) выразили озабоченность влиянием ИИ на ландшафт угроз.

Отчёт также подчёркивает вызовы, связанные с облачными сервисами, где 43.6% респондентов назвали утечки данных основной проблемой. За этим следуют несанкционированный доступ к облачным сервисам (42.7%) и некорректная настройка хранилищ (42.2%).

Основные проблемы при управлении облачными средами включают управление идентификацией и доступом (38.7%), поддержание облачной безопасности (38%) и теневое ИТ (35.9%).

Несмотря на все эти опасения, 94% респондентов уверены в способности своих организаций противостоять угрозам, таким как вымогательское ПО, фишинг и уязвимости нулевого дня.

Тем не менее, 71% опрошенных считают, что их решения по безопасности не оправдали ожиданий, что значительно выше по сравнению с 54% в прошлом году.

Надежду вселяет то, что 93% специалистов уверены в скором увеличении инвестиций в проактивные меры безопасности, такие как оценка рисков, тестирование на проникновение и упражнения по моделированию атак.

Отчёт Bitdefender подчёркивает серьёзные проблемы в сфере кибербезопасности, с которыми сталкиваются специалисты, включая чрезмерную рабочую нагрузку, высокий уровень выгорания и неудовлетворённости работой.

Несмотря на осознание организациями важности кибербезопасности и готовность инвестировать в неё, существующие решения часто не оправдывают ожиданий.

Чтобы сохранить квалифицированные кадры и обеспечить эффективную защиту, компаниям необходимо пересмотреть подходы к управлению рабочей нагрузкой специалистов по кибербезопасности, улучшить условия труда и постоянно внедрять инновационные проактивные меры безопасности.