

Независимые исследователи безопасности смогут протестировать защищенность сайтов СОГАЗа и получить вознаграждение при обнаружении потенциальных угроз. Сумма выплаты будет зависеть от уровня критичности выявленного риска.

Цель программы — совершенствование инструментов кибербезопасности и повышение устойчивости информационных систем компании к атакам.

В программе участвуют 14 сайтов и онлайн-сервисов компании, среди которых официальный сайт, личный кабинет клиента, онлайн-сервис подачи обращений для клиентов и т.д.

Михаил Ильин, заместитель председателя правления СОГАЗа: «Клиенты доверяют нам защиту своих финансовых интересов, имущества, бизнеса, а также жизни и здоровья. Поэтому обеспечить сохранность данных и надежность работы всех онлайн-сервисов не просто наша обязанность, а стратегический приоритет. Мы понимаем, что безопасность это не только технические меры, но и сотрудничество с сообществом исследователей. Их уникальный взгляд и опыт помогают нам выявлять уязвимости до того, как они станут угрозой. Вместе мы создаем более безопасную среду для наших клиентов и партнеров».

Евгений Волошин, директор департамента анализа защищенности и противодействия мошенничеству, BI.ZONE: «СОГАЗ уделяет большое внимание развитию цифровых сервисов и предлагает клиентам современные технологические решения. Выход на багбаунти — это еще один шаг в сторону повышения уровня защищенности сервисов. Благодаря помощи независимых исследователей компания сможет постоянно получать информацию об уязвимостях внешнего периметра, оперативно исправлять баги и предотвращать их эксплуатацию злоумышленниками».

BI.ZONE Bug Bounty — это платформа для проверки защищенности внешней

инфраструктуры с привлечением независимых исследователей. Компании размещают программы на платформе и получают отчеты об обнаруженных уязвимостях. Багхантеры при этом выбирают интересные для себя программы, ищут уязвимости и получают денежное вознаграждение за подтвержденные баги.

Википедия страхования