

Алексей Комаров, региональный представитель УЦСБ: «Для игроков рынка ИБ распахнулось огромное окно возможностей»

На online-конференции AM Live «Безопасность АСУ ТП», прошедшей 17 ноября 2023 года, компанию УЦСБ представил региональный представитель в г. Москва Алексей Комаров.

В прямом эфире эксперты обсудили, что важного произошло в сфере информационной безопасности промышленных предприятий (АСУ ТП) за год. Как предприятия справляются с кадровым голодом и ускоренным импортозамещением в ИТ и ИБ (в том числе для исполнения Указа Президента РФ №166), а также какие проблемы при этом возникают и как их решать.

Обсуждая вопросы выявления инцидентов в АСУ ТП и общей практики использования SOC для промышленных предприятий, Алексей Комаров отметил:

«Общие подходы к выявлению инцидентов в АСУ ТП не сильно отличаются от классических. Более того, делать это в АСУ ТП немного проще, так как инфраструктура там менее изменчивая, а все процессы стационарные, в отличие в корпоративной сети.

Что касается мониторинга АСУ ТП, тренд на его подключение уже давно не новый. У нас в УЦСБ есть свой Security Operation Center (SOC), и с первых дней его работы с 2020 года у нас уже были промышленные Заказчики, для которых мы осуществляли мониторинг как раз-таки промышленного сегмента. Мониторинг в АСУ ТП — это то, с чего обычно начинаются все процессы. Ведь чтобы массово дойти до превентивного воздействия и автоматизации реагирования в АСУ ТП потребуются еще несколько лет, а мониторинг уже сейчас можно запустить быстро, при этом получая максимальную отдачу. Так, прозрачное понимание того, как именно в компании работают промышленные сегменты, из чего они состоят, какие потоки данных там ходят — это уже огромный плюс».

Кроме того, в рамках дискуссии эксперт УЦСБ отметил, что проблема с уходом зарубежных вендоров заключается не в патчинге и закрытии уязвимости, сколько в прекращении гарантийной и сервисной поддержки.

«На предприятиях промышленная безопасность даже несколько важнее, чем информационная. Сейчас основная задача компаний — это сделать так, чтобы их производственно-технологический комплекс бесперебойно работал даже при отсутствии технической поддержки вендора», — подытожил Алексей Комаров.