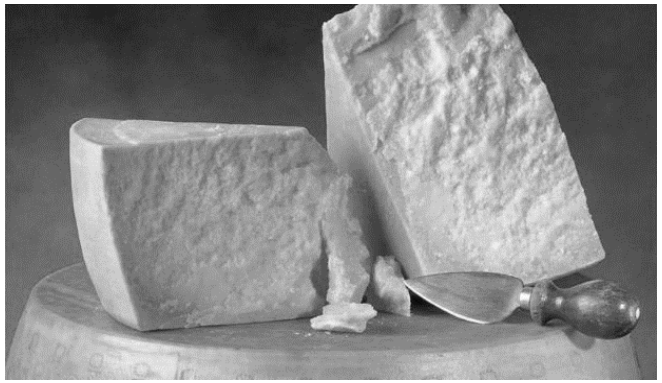
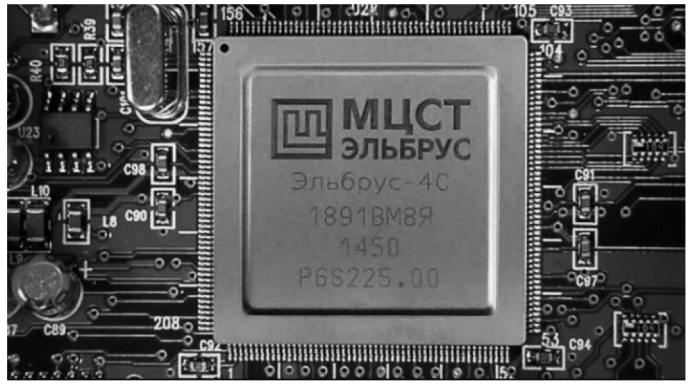
Роль центров мониторинга современной системе информационной безопасности РФ

SOC ФОРУМ

SOC-Форум 2015.
«Ты помнишь, как все начиналось…»

Что произошло в мире за 5 лет





Что произошло в ИБ-отрасли за 5 лет

187-ФЗ
и нормативная база по КИИ

Концепция создания **ГосСОПКА**

ФинЦЕРТ

Массовые эпидемии
WannaCry, Petya, NotPetya

Атакующее ПО Vault 7 и Vault 8

Закон о запрете иностранного ПО

Solar Security

Роль центров мониторинга современной системе информационной безопасности РФ

SOC ФОРУМ

«Ландшафт угроз за пять лет изменился на 100%. От шифровальщиков мы пришли к майнерам. Начали понимать, что есть целевые атаки. Социальная инженерия перестала быть уделом талантливых психологов.»

«Отрасль повзрослела. У нее начался тот самый пубертатный период, как у подростков, когда они уже понимают, что и не дети, но еще не взрослые... Отрасль осознала, что «старое ИБ» – это днище, что нужно строить ИБ по-новому. Но пока не очень знают как...»

«В отрасль пришло катастрофическое количество дилетантов. Начался наплыв непрофессиональных «безопасников» без достаточного технического и теоретического бэкграунда, но зато знающих все про «личный бренд»...

«Касательно атак или взломов – тут не было ни одного «черного лебедя», условно говоря, нового Stuxnet не случилось. Не было ничего ни в техническом, ни в регуляторном поле, чего нельзя было бы предсказать...»

«Отрасль требует перемен. Заказчики, только сталкиваясь с атаками, начинают финансировать ИБ.»

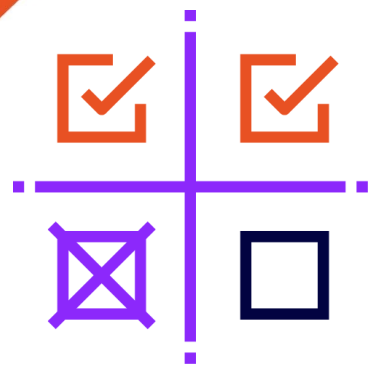
«А в это время российские вендоры, лоббируемые законодателями, под предлогом импортозамещения начинают агрессивно продавать свои поделки»

«Как изменилась отрасль за 5 лет?»

Роль центров мониторинга современной системе информационной безопасности РФ

SOC ФОРУМ

«Как регулирование по КИИ помогло вам в вашей ежедневной работе?»



«В общем никак, и не должно было никак помочь. Российское регулирование по КИИ ориентировано на помощь государству, снижение рисков для государственных систем.

Сама по себе инициатива нужная и полезная, а также требующая доточки, притирки и адекватного совестного поиска способов реализации и надзора»

«Единственный плюс, как мне видится, в настоящий момент – это донесение до руководства компаний важности ИБ, и вообще некая популяризация ИБ»

«Единственный профит – дополнительный аргумент для завязывания диалога о процессном обеспечении безопасности с функциональными специалистами.»

«В целом подняло ли оно уровень защищенности КИИ в стране?»

«Пока сам уровень эти действия не повысили. Это только начало пути, когда повышается уровень осведомленности, но не реализации самих норм.

Появился единый базис для подобных систем в виде унифицированных форм сбора информации об инцидентах, единого протокола обмена этой информацией.

Пока в основном никак. По результатам категорирования только планируются создание и доработка защитных механизмов.»

Нет. Период должен быть больше: как влияние на спрос-предложение, так и регуляторика имеют накопительный эффект, проявляющийся в более долгий срок»

«Если что-то и успели сделать – это приятное исключение.

Роль центров мониторинга современной системе информационной безопасности РФ

SOC ФОРУМ

«Идея взлетает. Ожидания чуда не подтвердились, но в целом все движется в правильном направлении»

«Подключения к ГосСОПКА идут. Но большего я от этого взаимодействия не вижу. Подключенные организации получают от этого взаимодействия не более, чем от реально действующих CERT'ов»

«Если идея взлетит, мы не должны этого заметить. Любая хорошая реализация безопасности, если она успешно интегрирована и оправдывает ожидания – работает тихо и незаметно»

«В процессе взлета. Пока рано давать оценки, но динамика подключения хорошая. Первый опыт информационного взаимодействия положительный, но ожидания намного выше.

Конечно, нет. Пока это гора бумаги. Пугалки интеграторов и регуляторов.»

ГосСОПКА. «Взлетела ли идея? Подтвердились ли ожидания?»

Роль центров мониторинга современной системе информационной безопасности РФ

SOC ФОРУМ

«Ожидания от регуляторов. Направления развития отрасли»

1. *«Убрать конфликты между различными регуляторными требованиями, гармонизировать законодательство между собой.»*
2. *«Больше документов в формате рекомендаций, может быть объединенных одной гос. программой.»*
3. *«Взаимовыгодного сотрудничества с экспертным сообществом. В текущей ситуации регуляторам будет сложно в одиночку разрабатывать современные и эффективные методики, инструменты и подходы.»*
4. *«Четкого и понятного плана по выпуску и контролю исполнения НПА, большей открытости и прозрачности, в том числе в плане собственных ключевых показателей.»*
5. *«Регламентирования деятельности по осведомленности пользователей (тематика, периодичность и пр.). Перспективно, потому что дешево и сердито.»*
6. *«Формирования конкурентного рынка - экосистемы интегрируемых решений по ИБ (не продуктов, а именно решений). Стимулирование имеет смысл направить в эту сторону.»*

SOC
ФОРУМ