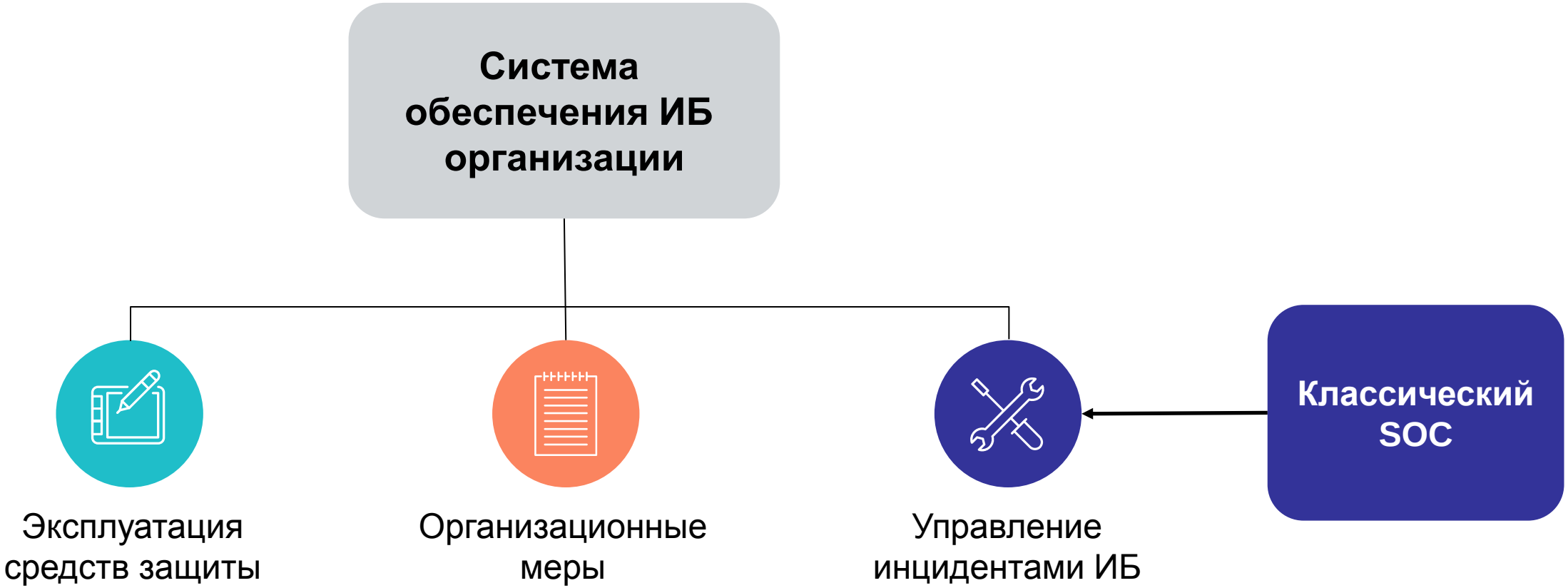
SOC 2.0. Аппетит приходит во время еды

Андрей Янкин,
Руководитель отдела консалтинга Центра информационной безопасности

SECURITY OPERATION CENTER



SOC 1.0: ФУНКЦИИ

Обработка данных в реальном времени	Работа с внешними источниками информации, стратегическое планирование	Анализ и реагирование на инциденты	Анализ цифровых образцов	Обеспечение работоспособности инструментов SOC	Аудит и отслеживание внутренних угроз	Сканирование и оценка защищенности	Прочее
Call-центр	Сбор внешних данных и их анализ	Анализ инцидентов	Сбор цифровых образцов	Поддержка работы граничных систем сетевой безопасности	Сбор и хранение данных аудита	Создание и актуализация карт сети	Оценка средств защиты
	Распространение информации из внешних источников	Слежка за нарушителем		Поддержка работы инфраструктуры SOC			Консультирование по вопросам информационной безопасности
Мониторинг и разбор данных в режиме реального времени	Подготовка материалов для внешнего распространения	Координация реагирования на инциденты	Анализ вредоносного кода	Поддержка работы сенсоров	Управление и обработка данных аудита	Сканирование уязвимостей	Повышение осведомленности
	Обогащение правил SOC на основе внешних данных	Внедрение контрмер		Создание собственных правил и сигнатур	Поддержка при работе с внутренними угрозами	Оценка защищенности	Оперативное информирование
	Стратегическое планирование	Работы по реагированию на инцидент на пострадавшей площадке	Анализ прочих цифровых образцов	Подбор и внедрение решений, использующихся в работе SOC	Расследование случаев внутренних нарушений	Тестирование на проникновение	Распространение наработок
	Оценка угроз	Удаленное реагирование на инцидент		Разработка решений, использующихся в работе SOC			Взаимодействие с общественностью и СМИ

ФИЗИЧЕСКАЯ БЕЗОПАСНОСТЬ

«A SOC is distinct from:

- ✓ …
- ✓ **Physical security monitoring** (e.g., “gates, guards, and guns”) …»

ФИЗИЧЕСКАЯ БЕЗОПАСНОСТЬ

- ✓ **ПЕРВЫЙ ШАГ:** подключение СКУД
- ✓ **МАКСИМУМ:** создание центра мониторинга физической и инженерно-технической безопасности на базе SOC

ФИЗИЧЕСКАЯ БЕЗОПАСНОСТЬ

ФИЗИЧЕСКАЯ БЕЗОПАСНОСТЬ

ФИЗИЧЕСКАЯ БЕЗОПАСНОСТЬ

СЛОЖНОСТИ:

- ✓ Подчинение разным подразделениям
- ✓ Разные схемы обработки инцидентов и реакции на них
- ✓ Необходимость программной надстройки над SIEM и PSIM

БОРЬБА С МОШЕННИЧЕСТВОМ

ПРОСТЫЕ СЛУЧАИ МОГУТ БЫТЬ ОБНАРУЖЕНЫ SIEM:

- ✓ Хищение данных
- ✓ Злоупотребления администраторов
- ✓ Неавторизованный доступ

БОРЬБА С МОШЕННИЧЕСТВОМ

У SIEM ЕСТЬ ФУНДАМЕНТАЛЬНЫЕ НЕДОСТАТКИ:

- ✓ Работает с событиями, а не с состояниями
- ✓ Ограниченные возможности по изменению работы корреляционного движка

ОРГАНИЗАЦИОННЫЕ ПРОБЛЕМЫ:

- ✓ Невозможность совмещения дежурных смен – SoD
- ✓ Различное подчинение

БОРЬБА С МОШЕННИЧЕСТВОМ

СТРОИТЕЛЬСТВО «СТРАТЕГИЧЕСКОГО» УРОВНЯ

SOC ОБЛАДАЕТ:

- ✓ Статистикой по инцидентам ИБ
- ✓ Компетенциями в практической безопасности
- ✓ Данными по эффективности защитных мер

Логично желание использовать эти данные для стратегического развития ИБ

СТРОИТЕЛЬСТВО «СТРАТЕГИЧЕСКОГО» УРОВНЯ

ТРЕБУЕТСЯ РАСШИРЕШНИЕ ВОЗМОЖНОСТЕЙ SIEM:

- ✓ Расширенные данные по инцидент-менеджменту
- ✓ Данные Cyber Threat Intelligence (CTI)
- ✓ Функционал прогнозирования, визуализации, статистического анализа

СТРОИТЕЛЬСТВО «СТРАТЕГИЧЕСКОГО» УРОВНЯ

НЕОБХОДИМА НАДСТРОЙКА НАД ТЕХНИЧЕСКИМИ СРЕДСТВАМИ SOC:

- ✓ BI
- ✓ GRC
- ✓ Доработанная, самописная, скомпонованная из разных решений

СТРОИТЕЛЬСТВО «СТРАТЕГИЧЕСКОГО» УРОВНЯ

РЕАЛЬНОСТЬ:

- ✓ Большому начальству «стратегический уровень» интересен в первую очередь
- ✓ Требования к SOC получают перекос, основные функции SOC делаются по остаточному признаку
- ✓ Задача строителя SOC – найти баланс и, строя SOC, построить-таки сам SOC

АДМИНИСТРИРОВАНИЕ СЗИ СИЛАМИ SOC

ПУТЬ СОЗДАНИЯ НЕЭФФЕКТИВНОГО SOC ИЛИ ЕГО ДЕГРАДАЦИИ:

- ✓ Отвлечение дежурной смены
- ✓ Нарушение SoD
- ✓ И то, и другое делается плохо

АДМИНИСТРИРОВАНИЕ СЗИ СИЛАМИ SOC

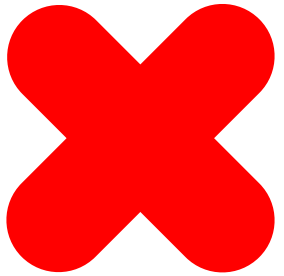
ЗАЧЕМ?

- ✓ Изначально неверная архитектура
- ✓ «Естественный» рост SOC в СОИБ
- ✓ Политические причины
- ✓ Обоснование бюджетов модной темой SOC

ЧТО ДЕЛАТЬ?

- ✓ Создать внутри SOC искусственную стену, отделяющую администрирование от настоящего SOC

ПОЭТАПНОЕ ВНЕДРЕНИЕ SOC



Спасибо!

Андрей Янкин,
Руководитель отдела консалтинга Центра информационной безопасности
тел: +7 (495) 411-7601
av.yankin@jet.su

тел. +7 (495) 411-7601
ул. Большая Новодмитровская, 14/1

www.jet.su