ОПЫТ ПОСТРОЕНИЯ КОРПОРАТИВНОГО ЦЕНТРА ГОССОПКА

Павлов Алексей Викторович

Руководитель отдела пресейла

РТК-Солар

Сказочное банное

Февраль, 2018

Дано:

Федеральный закон ФЗ-187 «О безопасности критической информационной инфраструктуры Российской Федерации»

Приказы ФСБ:

№368 Об утверждении Порядка обмена информацией о компьютерных инцидентах и Порядка получения субъектами КИИ информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения

№367 Об утверждении Перечня информации, представляемой в ГосСОПКА и Порядка представления информации в ГосСОПКА

№366 О НКЦКИ

Проекты приказов ФСБ:

Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации

Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты

Методические рекомендации ФСБ:

Варианты организации защищенного канала

Регламент взаимодействия

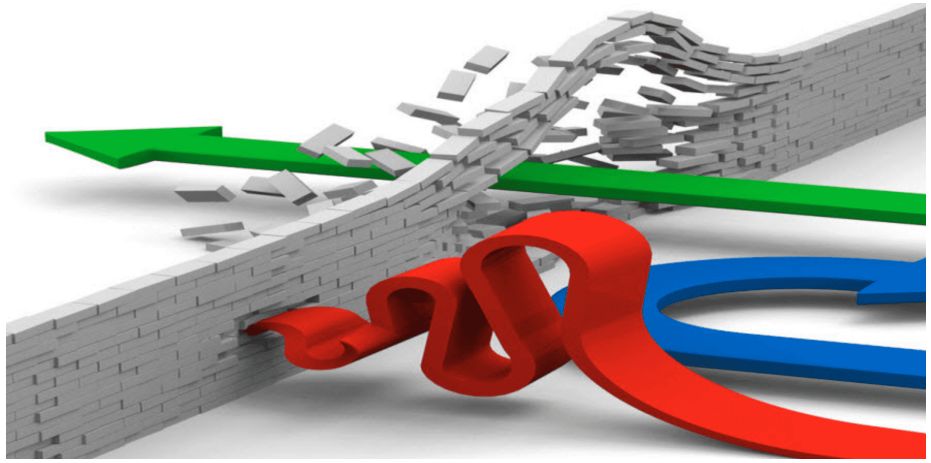
Требования к Подразделениям

Методические рекомендации по обнаружению КА на ИР

Методические рекомендации по проведению мероприятий по оценке степени защищенности от компьютерных атак

Методические рекомендации по установлению причин и ликвидации последствий компьютерных инцидентов, связанных с функционированием информационных ресурсов российской федерации

Направления деятельности

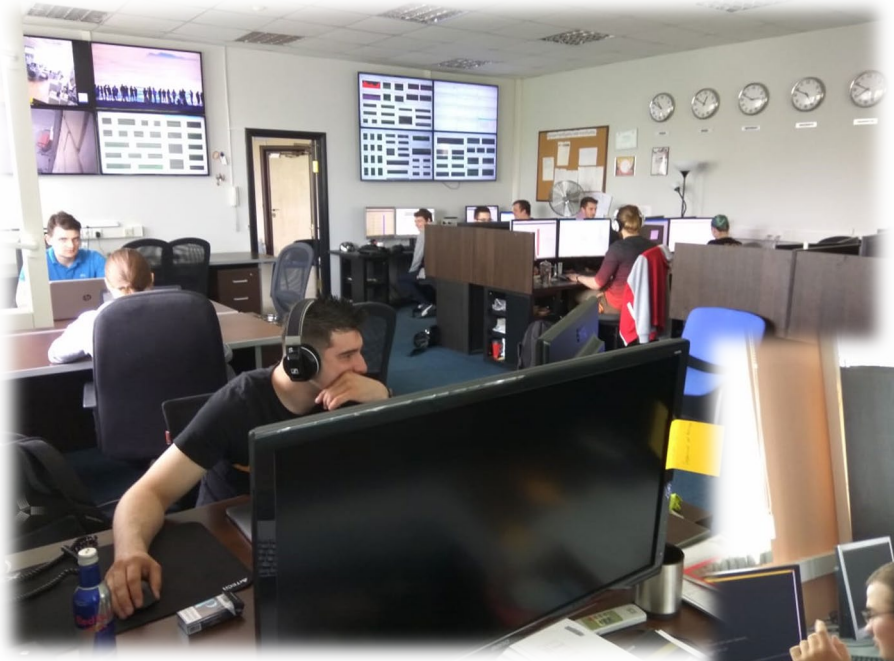


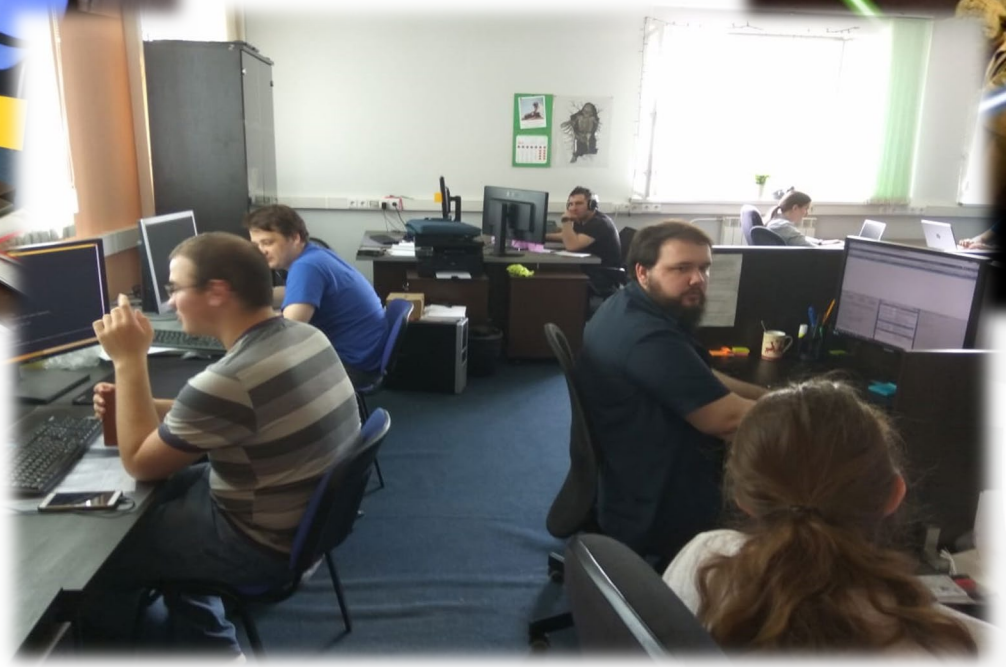
А еще...

- Разработка документов, регламентов
- Эксплуатация средств ОПЛ
- Анализ угроз безопасности

Нюансы…

Силы ГосСОПКА





Силы ГосСОПКА

1-я линия:
Взаимодействие с персоналом и пользователями
Обнаружение КА и инцидентов
Обслуживание средств центра ГОССОПКА

2-я линия:
Оценка защищенности
Ликвидация последствий КА
Установление причин КИ

3-я линия:
Аналитическая работа по инцидентам и угрозам, развитие направлений ИБ
Экспертная поддержка по специализации, работа по повышению уровня защищенности, развитие
Нормативно-правовое сопровождение
Руководство центром ГОССОПКА

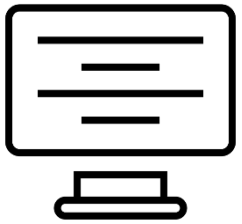
Линии SOC

Руководитель SOC

Группа развития JSOC

Группа расследования

Группа управления качеством



Группа инцидентов ИБ

- Аналитики
- 2-ая линия
- 1-ая линия

Группа эксплуатации СЗИ

- Администраторы ИБ
- 2-ая линия
- 1-ая линия

Силы ГосСОПКА vs линии SOC

- Первая линия не выявляет инциденты, а работает по playbook с уже зафиксированными КИ и КА
- Взаимодействие с заказчиком и НКЦКИ осуществляет выделенный аналитик и сервис-менеджер JSOC
- Ликвидация последствий КА осуществляется группой лиц с привлечением различных специалистов. Координатор – выделенный аналитик JSOC
- Установление причин КИ – узкоспециализированные эксперты, привлекаемые по запросу
- Развитие СОПЛ – выделенная группа развития, не взаимодействующая с заказчиками
- Тюнинг СОПЛ под заказчика – задача аналитика

Нюансы...
Обработка инцидентов

Гарантированно определить инцидент без обратной связи от субъекта невозможно:

Тип инцидента	Возможные ложные срабатывания
Несанкционированный доступ к системе	• новый администратор • аварийная задача • служебная необходимость
Новый хост на периметре	• опубликованная бизнесом система
Сканирование подсетей	• инвентаризация ИТ-систем • тест на проникновение • поиск принтеров
Обращение к ЦУ ботнета	• ошибки фида • обращение к другому сайту хостинга • Skype

Нюансы...
Реагирование на инциденты

- Стратегия локализации
- Принятие решения
- Выполнение действий по локализации

? Кто принимает решение

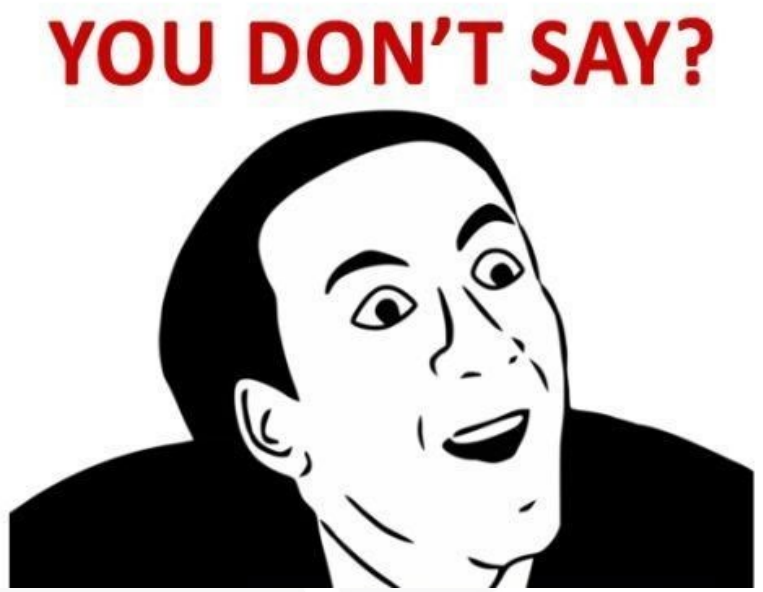
? Кто выполняет и в каких случаях

? Автоматизация

RAT	TIDetection	CriticalProcessStopped
TOR	VirusEpidemy	RegistryModification
VirusFoundAndNotCured	DNSTunneling	MinerDetection
Bruteforce	WebAttack	UnknownConnectionToCriticalHost
PasswordReset	CriticalIPSAlert	DDoS
InternalNetworkScan	NewServiceInstall	HackToolsDetect

Нюансы...
Установление причин КИ

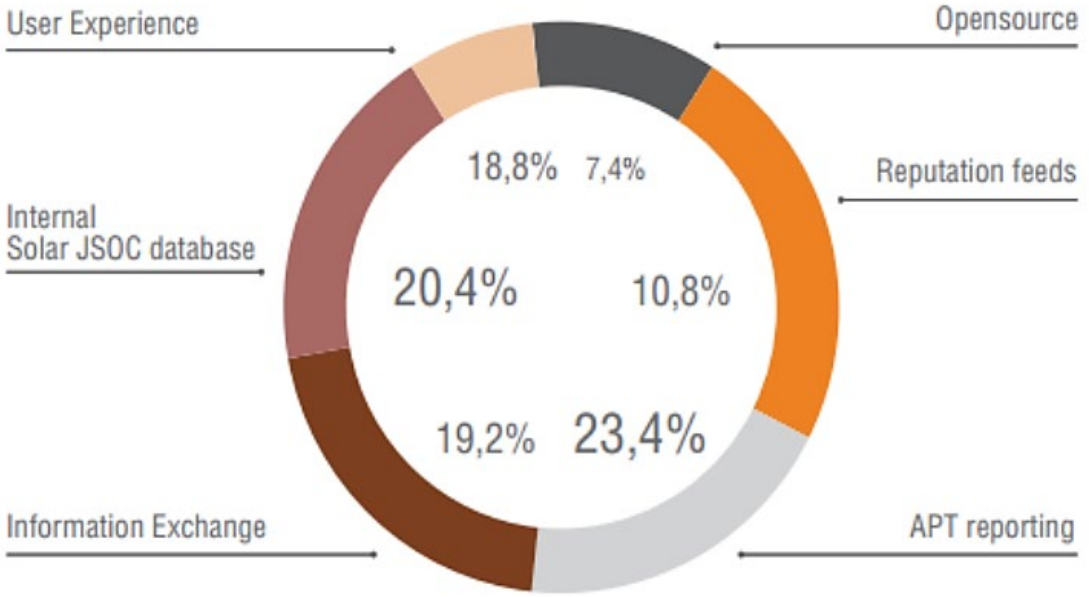
- Установление причин возникновения компьютерного инцидента
- Анализ инструментов, примененных при компьютерном инциденте (ВП, RAT, NS)
- Выявление последствий компьютерного инцидента: масштабов вредоносного воздействия и причиненного ущерба
- Выработка компенсирующих мер защиты информации и участие в устранении уязвимостей и рисков информационной безопасности
- Анализ результатов устранения компьютерных инцидентов, корректировка мер по недопущению повторения инцидента



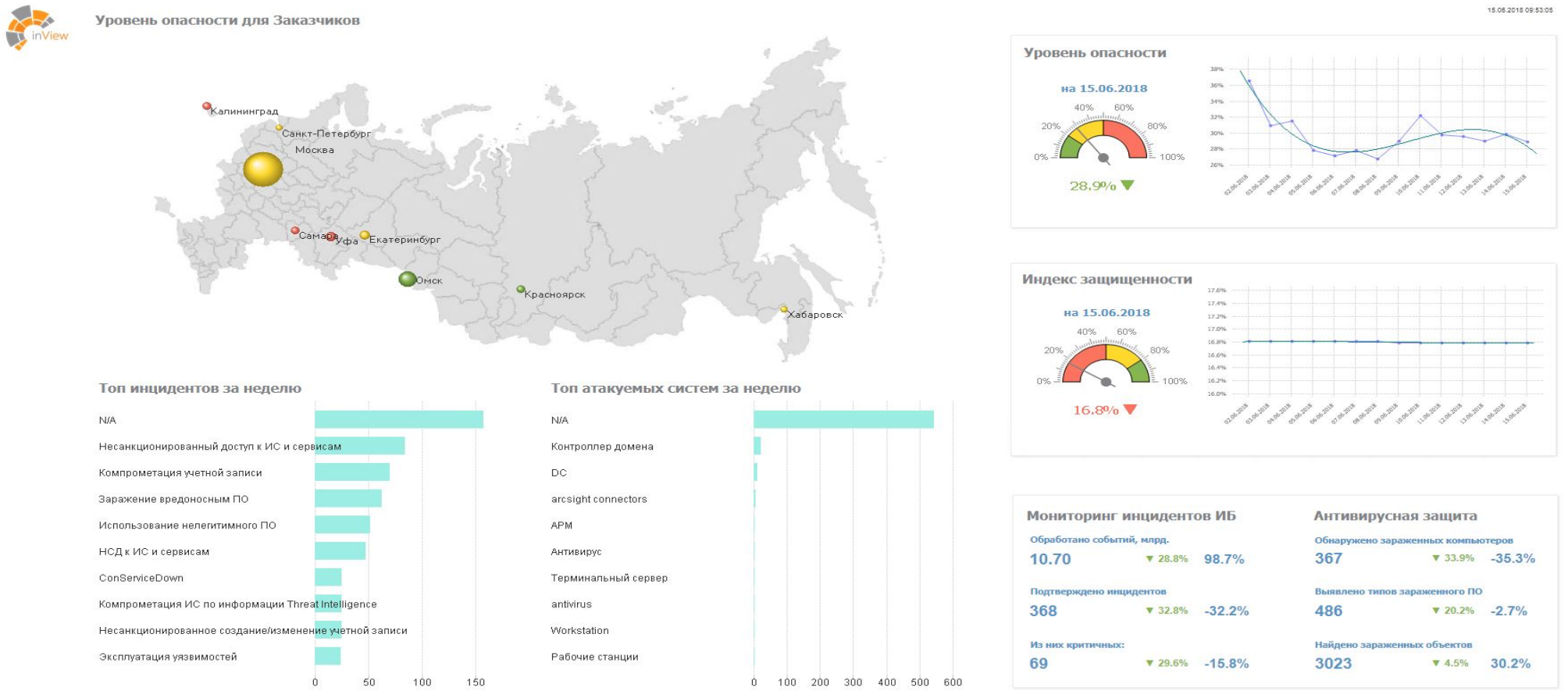
Нюансы...
Анализ угроз безопасности

- Сбор
  - Внутренний intelligence
  - Исследование доступных источников
  - Информация от НКЦКИ
  - **Работа с коммерческим intelligence**:
- ***Анализ информации***
- ***Применение***

Статистика по использованию разных типов Intelligence в детектировании инцидентов



Эффективный контроль за состоянием защищенности



Спасибо!

Сказочное банное