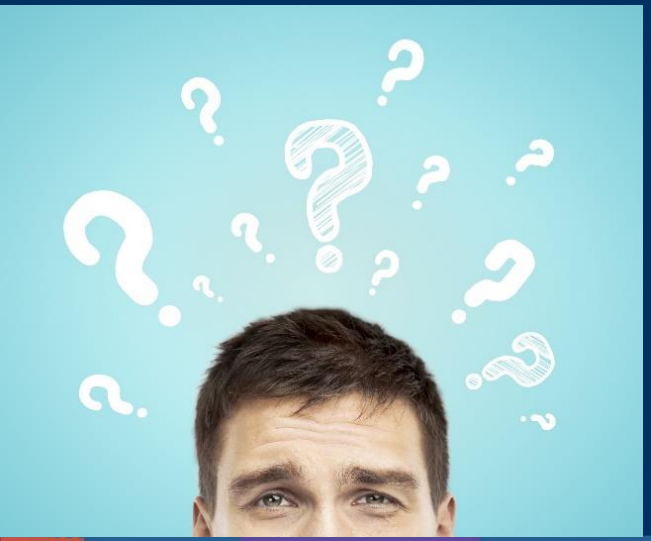
Создание центра мониторинга и подключение к ГосСОПКА с помощью решения ViPNet TDR

Создание центра мониторинга

Определения



- Центр обеспечения безопасности (Security Operations Center (SOC))
- Центр обеспечения кибербезопасности (Cybersecurity Operations Center (CSOC))
- Центр реагирования на компьютерные инциденты (Computer Incident Response Center (or Capability) (CIRC))
- Центр реагирования на инциденты компьютерной безопасности (Computer Security Incident Response Center (or Capability) (CSIRC))
- Команда реагирования на инциденты компьютерной безопасности (Computer Security Incident Response Team (CSIRT))
- Команда реагирования на компьютерные инциденты (Computer Incident Response Team (CIRT))
- Группа экстренного реагирования на компьютерные инциденты (Computer Emergency Response Team (CERT))

Функции центра мониторинга

- Обнаружение вторжений на сетевом уровне и уровне конечных узлов
- Сбор, корреляция событий и управление инцидентами ИБ
- Обнаружение и оценка уязвимостей
- Реагирование и на инцидент и устранение последствий
- Оценка рисков ИБ и проведение мероприятий по их снижению
- Формирование отчетности и взаимодействие с регуляторами

Managed Detection and Response

- обнаружение
- реагирование
- проведение расследования
- сбор доказательной базы
- отчетность

Мониторинг информационной безопасности средств и систем информатизации

	Наименование оборудования	Технические и (или) функциональные характеристики
22	Средства (системы) контроля (анализа) защищенности информационных систем	Автоматизированная инвентаризация ресурсов информационных систем (сбор информации об узлах информационных систем и об используемом в них программном обеспечении), выявление уязвимостей (кода, конфигурации и архитектуры) в них, анализ и управление выявленными уязвимостями с учетом угроз. Должны иметь сертификаты соответствия ФСТЭК России
24	Средства управления информацией об угрозах безопасности информации	Автоматизированный сбор и анализ информации, поступающей из различных источников, об угрозах безопасности информации. Должны иметь формуляры, оформленные разработчиками (производителями) данных средств. В случае невозможности оформления формуляров разработчиками (производителями) данных средств (свободнораспространяемое программное обеспечение) формуляры оформляются лицензиатами (соискателями лицензии)
25	Средства управления событиями безопасности информации	Автоматизированный сбор, анализ и корреляция данных о событиях безопасности информации, регистрируемых компонентами информационных систем, идентификация по заданным индикаторам типовых инцидентов информационной безопасности и их локализация. Должны иметь сертификаты соответствия ФСТЭК России

Положение о лицензировании деятельности по технической защите конфиденциальной информации, утвержденное постановлением Правительства Российской Федерации от 3 февраля 2012 г. N 79. Перечень утвержден директором ФСТЭК России 19 апреля 2017 г.

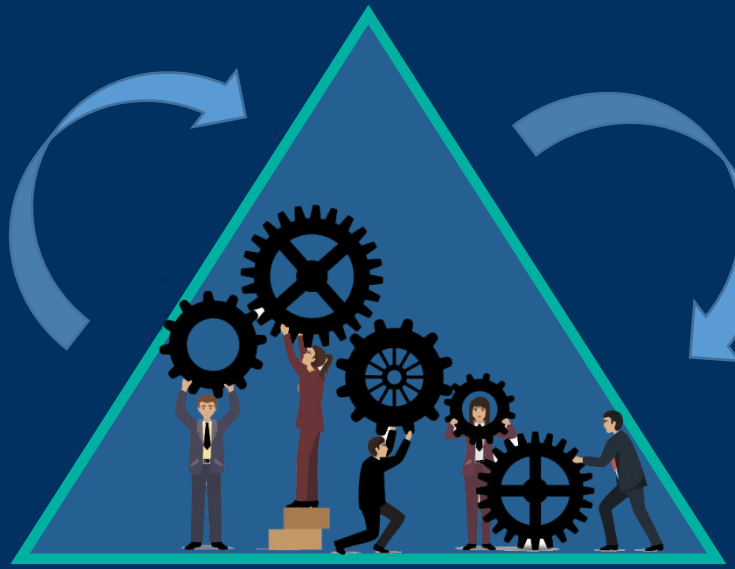
Мониторинг информационной безопасности средств и систем информатизации

	Наименование оборудования	Технические и (или) функциональные характеристики
26	Средства управления инцидентами информационной безопасности	Автоматизированная регистрация информации об инцидентах информационной безопасности информационных систем, предоставление рекомендаций по реагированию на них, формирование и модификация шаблонов инцидентов информационной безопасности, в том числе рекомендаций по реагированию на них. Должны иметь формуляры, оформленные разработчиками (производителями) данных средств. В случае невозможности оформления формуляров разработчиками (производителями) данных средств (свободнораспространяемое программное обеспечение) формуляры оформляются лицензиатами (соискателями лицензии)
27	Средства защиты каналов передачи данных	Должны обеспечивать конфиденциальность и целостность данных, передаваемых по каналам связи между информационной системой, используемой для управления информационной безопасностью, и информационными системами, в отношении которых осуществляется мониторинг. Должны иметь сертификаты соответствия ФСБ России
28	Системы защиты информации информационных систем, используемых для мониторинга информационной безопасности	Системы защиты информации информационных систем, используемых для оказания услуг по мониторингу информационной безопасности информационных систем, должны соответствовать Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденным приказом ФСТЭК России от 11 февраля 2013 г. N 17, применительно к первому классу защищенности государственных информационных систем

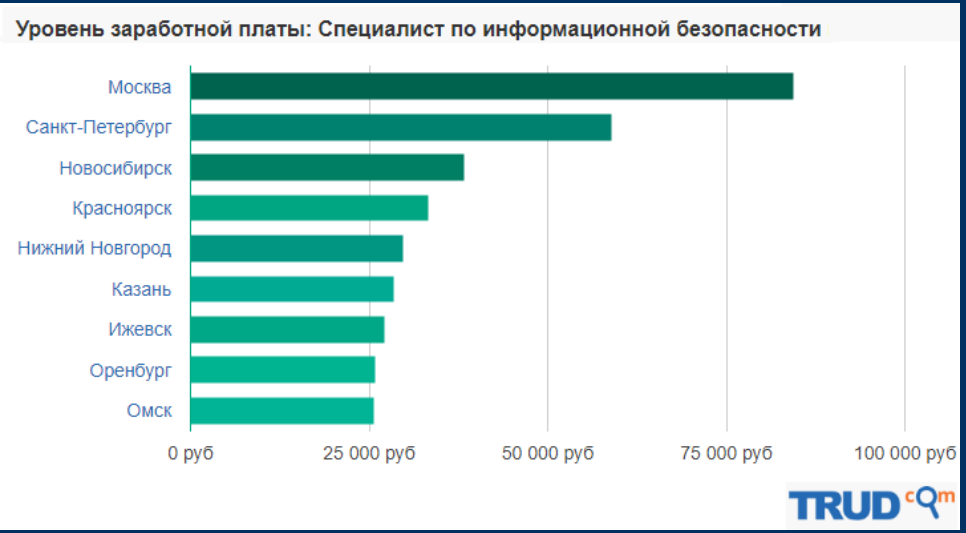
Проблемы построение SOC

SOC это....

ТЕХНО infotecs 2020 ФЕСТ



Люди



«Нехватка квалифицированных кадров в области кибербезопасности и дефицит экспертизы - отчетливая тенденция на рынке ИБ, с которой нам часто приходится сталкиваться. Особенно это касается регионов, где нехватка знаний в области кибербезопасности приводит к существенному отставанию специалистов от глобального развития киберугроз»

© ComNews 2019

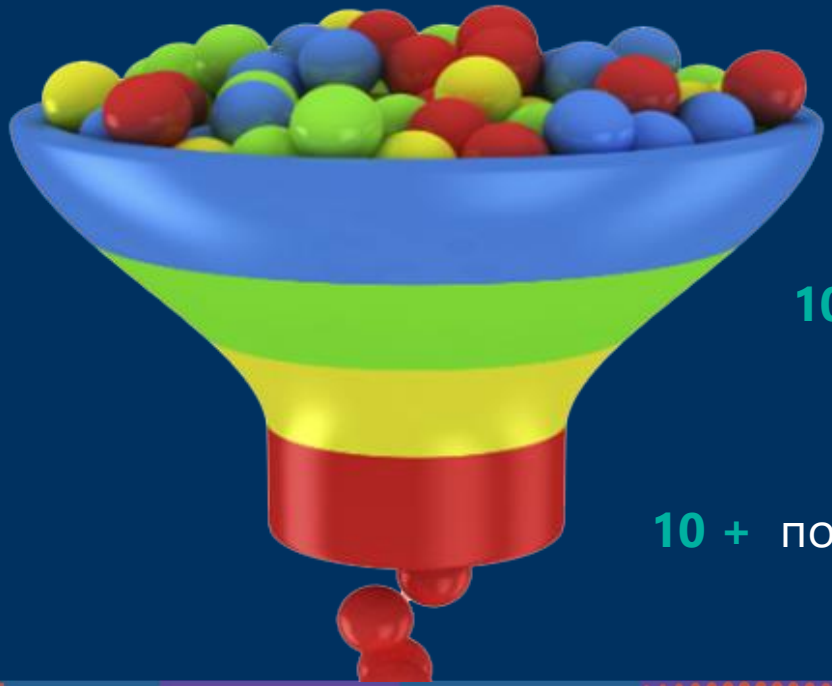
http://www.comnews.ru/content/117306/2019-01-28/ib-ne-hvataet-lyudey-finansov-i-planirovaniya

Инструменты

Причины неудовлетворенности системой SIEM

IDC ANALYZE THE FUTURE

Процессы



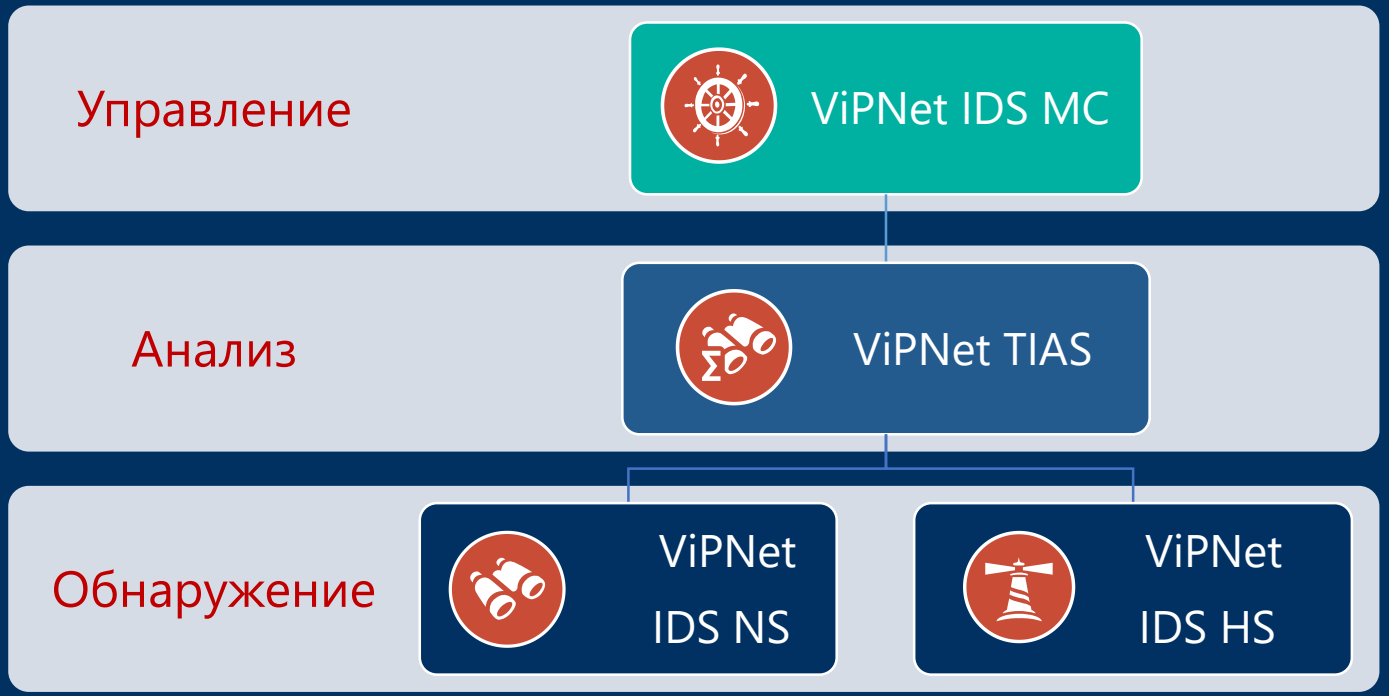
1 000 000 000 + исходных событий

100 000 + подозрений на инциденты

10 + подтвержденных инцидентов

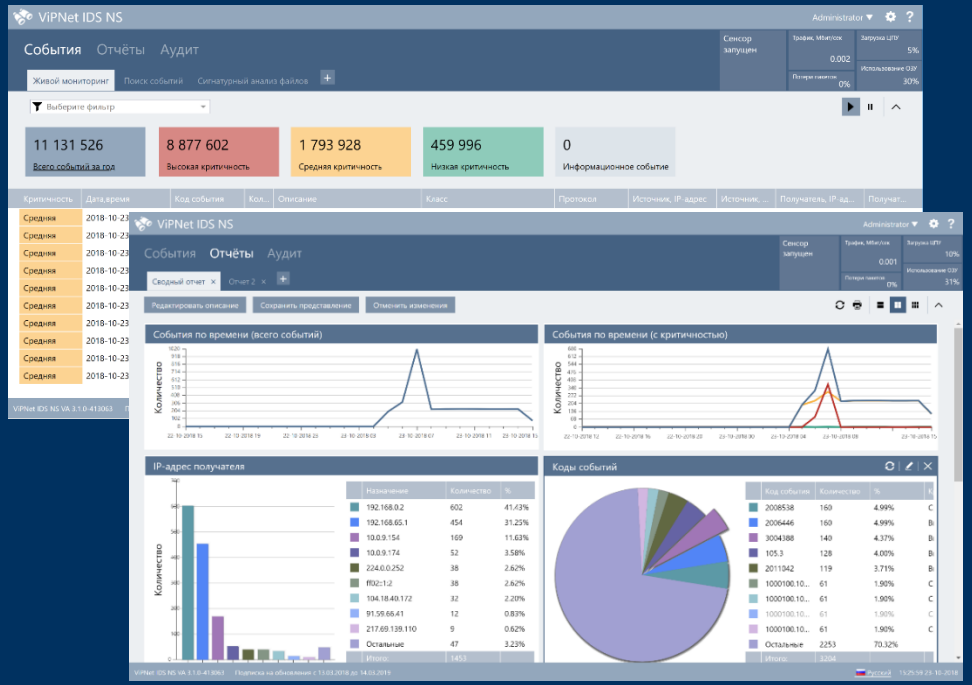
Решение ViPNet TDR

Состав решения TDR



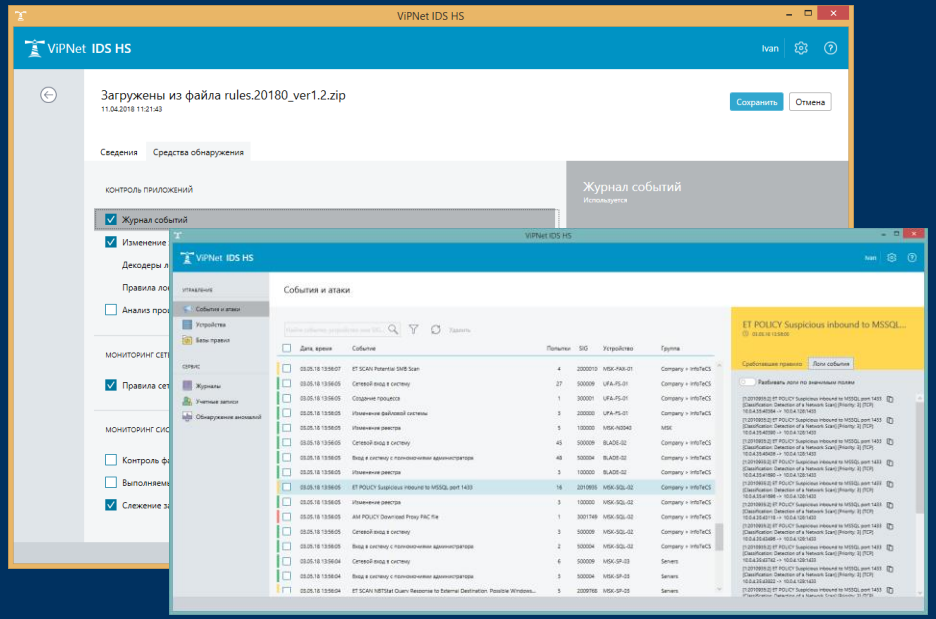
ViPNet IDS NS

- **обнаруживать** события ИБ в трафике
- **оповещать** о событиях
- **хранить** события
- **работать** с событиями
- **управлять** правилами и настройкой сигнатур



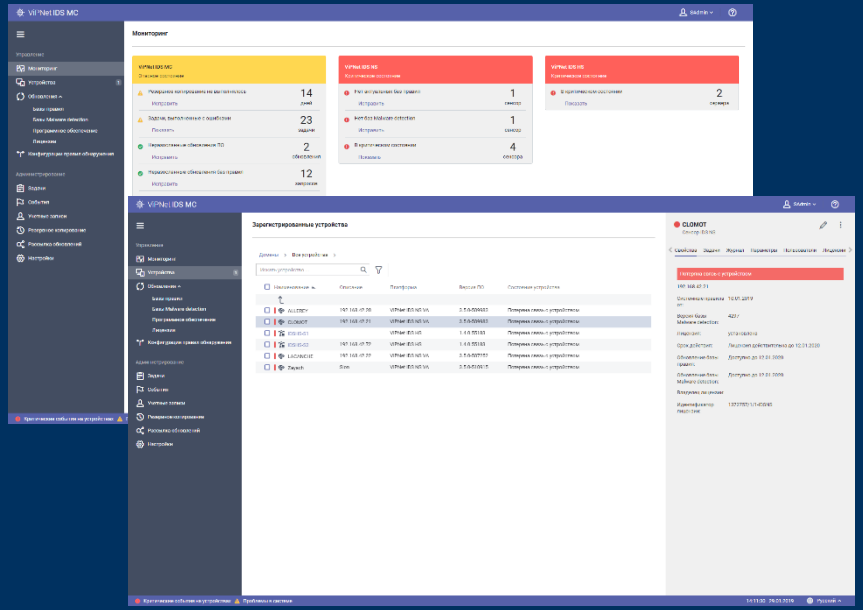
ViPNet IDS HS

- **выявлять** подозрительную активность внутри ОС:
  - файловая активность
  - изменения в реестре
  - неизвестные процессы
- **определять** атаки, которые “не видит” сетевой сенсор
- **обнаруживать** атаки после расшифровки входящего трафика



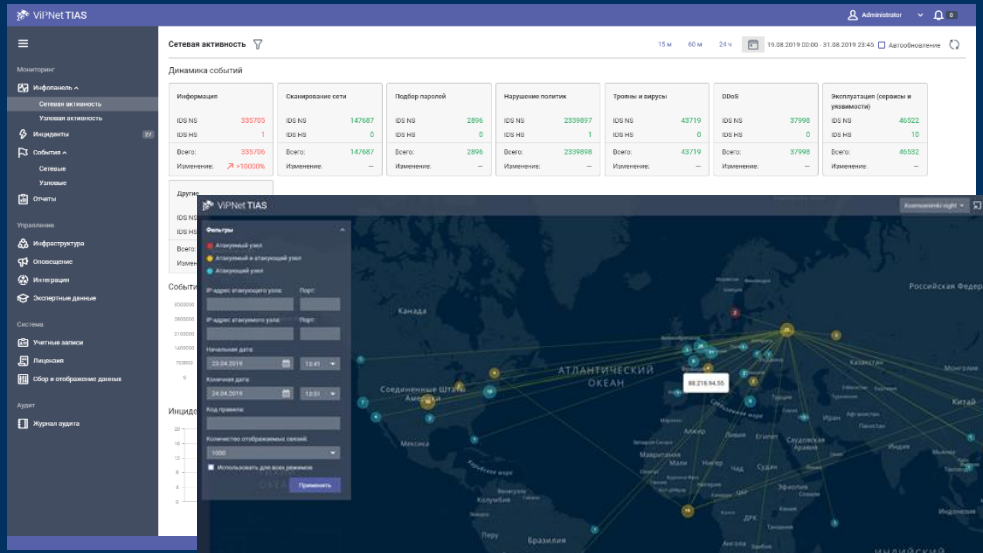
ViPNet IDS MC

- **настраивать** структуру и параметры сенсоров
- **управлять** конфигурациями правил
- **мониторить** работоспособность сенсоров
- **обновлять:**
  - базы решающих правил
  - базы сигнатур вредоносного ПО
  - экспертные данные



ViPNet TIAS

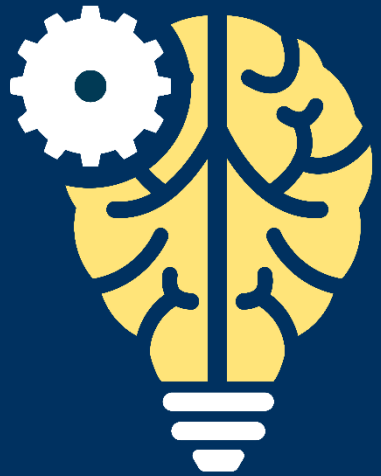
- **анализировать** события от сенсоров ViPNet IDS
- **выявлять** инциденты
- **оповещать** об инцидентах
- **проводить** расследования
- **давать** рекомендации
- **формировать** отчеты



Как это работает?

Отличительные особенности

Machine Learning



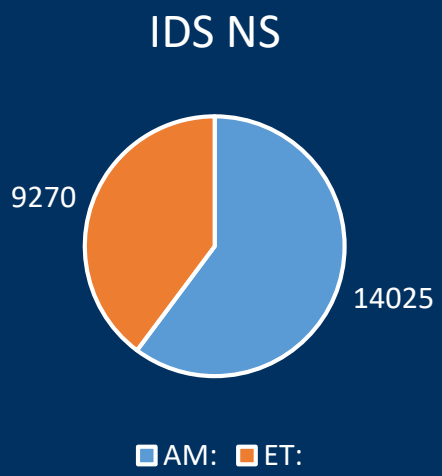
- математическая модель принятия решений
- алгоритмы машинного обучения
- ежемесячное переобучение
- выявление атак нулевого дня

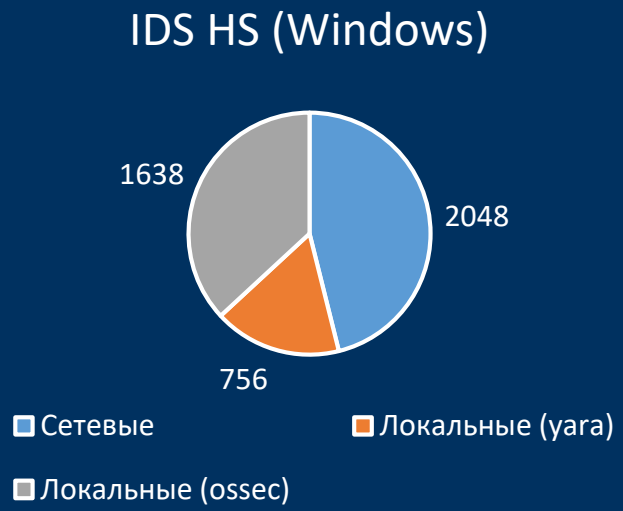
Threat Intelligence

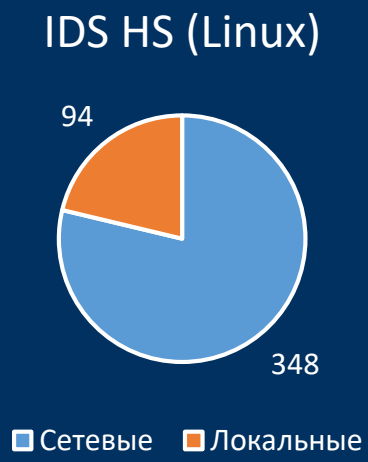
- индикаторы атак и компрометации
- ТТП - тактики, техники, процедуры
- информационный обмен:
  - СОПКА
  - ФСТЭК
  - RU-CERT
- опыт клиентов - верифицированная и обезличенная информация

О решении в цифрах

Базы решающих правил







Производительность и потребность в ресурсах

ViPNet IDS NS

анализ трафика
до 6 Гбит/с

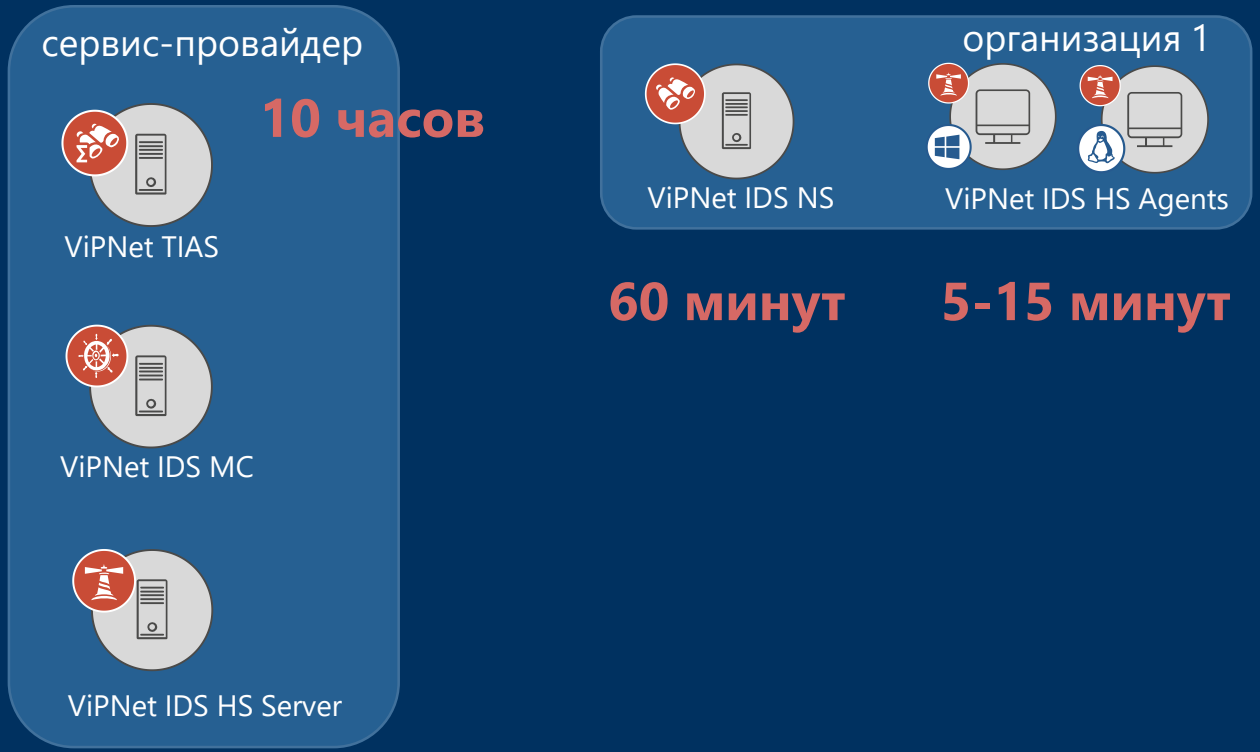
ViPNet TIAS

анализ до 5 000
событий/с

ViPNet IDS HS Agent

потребляет ~ 60 Мбайт
оперативной памяти

Внедрение решения



Перспективный Мониторинг

963 инцидента
за 2019 год

<60 мин.
на реагирование

более 30
операторов,
исследователей,
аналитиков

ФСК ЕЭС

более 40 организаций подключались
на мониторинг за последние 3 года

Учебный центр

367 человек обучено на курсе «Администрирование IDS и TIAS»

14 ВУЗов имеют лаборатории, оснащенные ViPNet IDS и TIAS

Варианты исполнения

ТЕХНО 2020 infotecs ФЕСТ

Сервер 1U

- ViPNet IDS NS 1000-2000
- ViPNet TIAS 1000-5000

Desktop

- ViPNet IDS NS 100

Virtual Appliance

- ViPNet IDS NS VA
- ViPNet TIAS VA

Software

- ViPNet IDS HS Server
- ViPNet IDS HS Agent

Сертификаты

- ViPNet IDS 3. Сертификат ФСБ России СОА класс класса В
- ViPNet IDS 3. Сертификат ФСТЭК России СОВ уровня сети 4 класс (ноябрь 2020)
- ViPNet IDS HS. Сертификат ФСТЭК России СОВ уровня узла 4 класс
- ViPNet TIAS. Сертификат ФСТЭК России. НДВ 4 уровень, соответствие ТУ

ГосСОПКА

Структура ГосСОПКА

В 2018 году средствами ГосСОПКА было выявлено более 4,3 млрд компьютерных воздействий на критическую информационную инфраструктуру, из них более 17 тысяч наиболее опасных компьютерных атак

Мурашов Н.Н

Приказы ФСБ России

- **Перечень информации,** предоставляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка предоставления информации в ГосСОПКА (Приказ № 367 от 24 июля 2018 года)
- **Порядок обмена** информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации… (Приказ от 24 июля 2018 г. N 368)
- **Требования к средствам,** предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты (Приказ от 06.05.2019 №196)
- **Порядок 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 (Приказ ФСБ России от 19.06.2019 N 282)

Приказ ФСБ России №282 от 19.06.2019

- Информация о компьютерном инциденте, связанном с функционированием значимого объекта критической информационной инфраструктуры, направляется субъектом критической информационной инфраструктуры в НКЦКИ **в срок не позднее 3 часов** с момента обнаружения компьютерного инцидента, а в отношении иных объектов критической информационной инфраструктуры — **в срок не позднее 24 часов** с момента его обнаружения
- Информирование осуществляется путем направления информации в Национальный координационный центр по компьютерным инцидентам в соответствии с определенными НКЦКИ форматами

Проект ФЗ о внесении изменений в КОАП:
Непредставление или нарушение порядка либо сроков представления в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации информации, предусмотренной законодательством в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, – влечет наложение административного штрафа:

- на должностных лиц в размере от десяти тысяч до пятидесяти тысяч рублей
- на юридических лиц – от ста тысяч до пятисот тысяч рублей

Перечень мероприятий

Класс В

ТЕХНО 2020 infotecs фест

- Взаимодействие с НКЦКИ
- Разработка регламентирующих документов
- Эксплуатация средств ГосСОПКА
- Прием сообщений об инцидентах
- Регистрация атак и инцидентов
- Анализ событий ИБ
- Инвентаризация
- Анализ угроз ИБ
- Составление и актуализация перечня угроз
- Выявление уязвимостей
- Подготовка предложений по повышению уровня защищенности
- Составление перечня инцидентов
- Ликвидация последствий
- Анализ результатов ликвидации последствий

Варианты подключения

ТЕХНО 2020 infotecs ФЕСТ

Самостоятельное подключение

ГОССОПКА

Субъект ГосСОПКА

- Заключить соглашение с 8Ц ФСБ России
- Выполнить организационные и технологические требования к центру ГосСОПКА
- Обеспечить взаимодействие с технической инфраструктурой НКЦКИ

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Объект КИИ

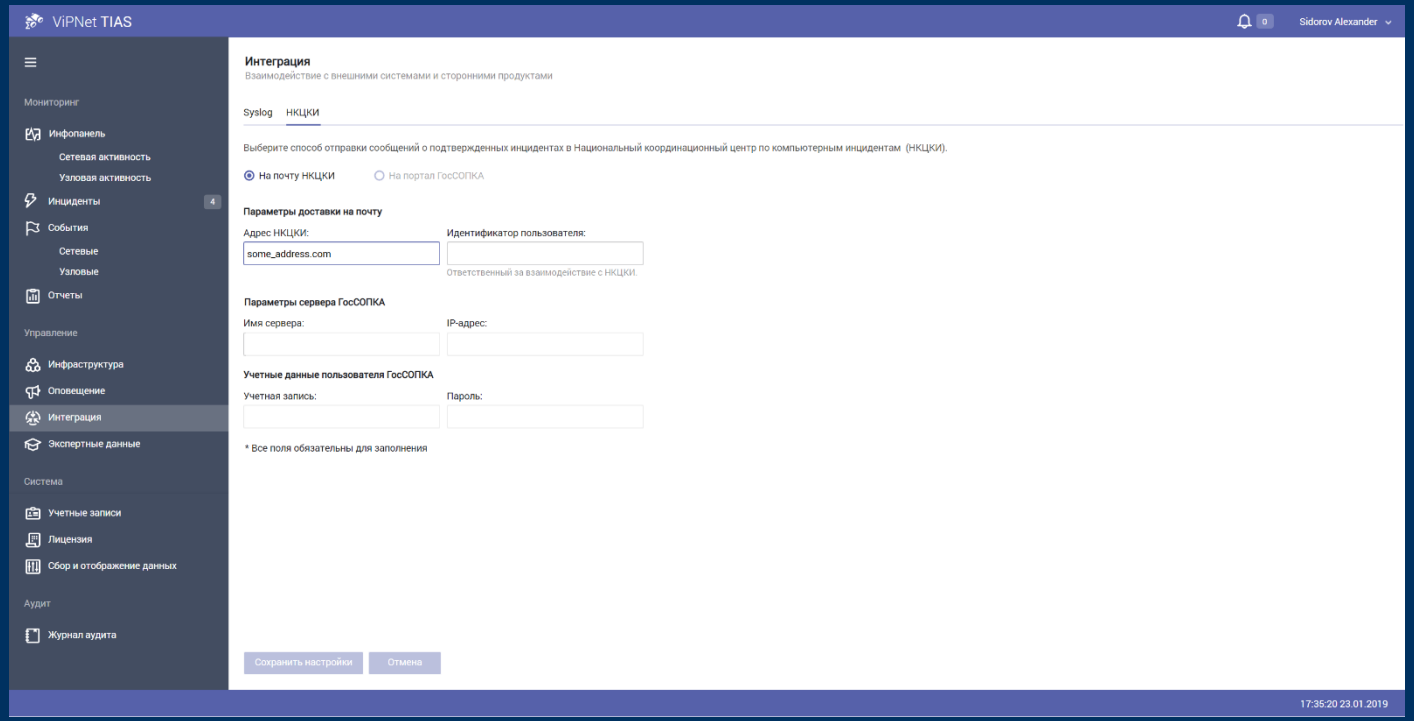
Подключение через корпоративный центр

ГОССОПКА

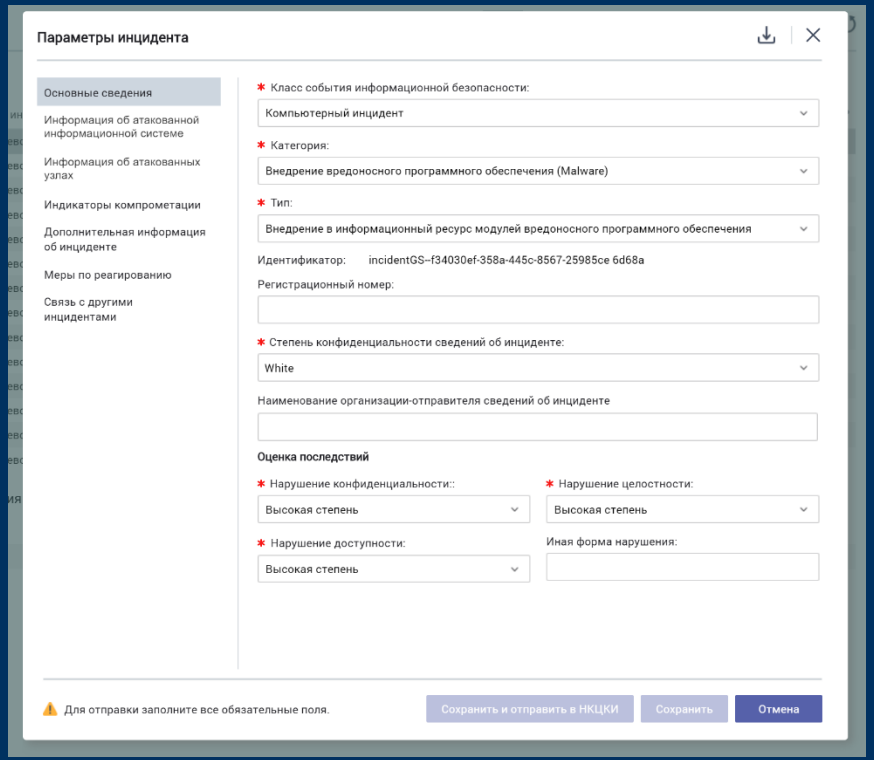
Корпоративный центр ГосСОПКА

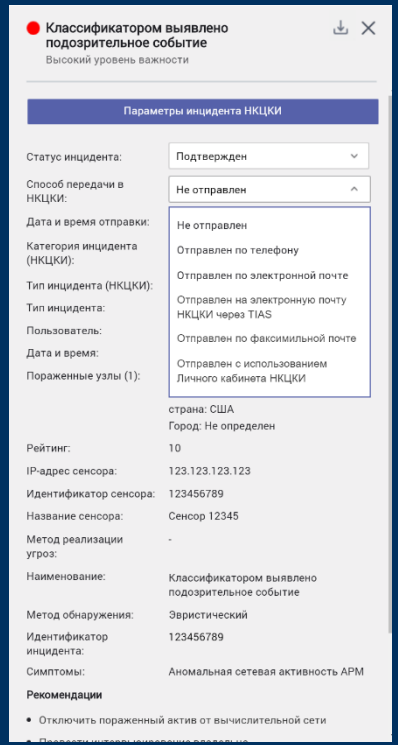
- Заключить соглашение с корпоративным (ведомственным) центром ГосСОПКА
- Уведомить НКЦКИ о включении своих ресурсов в зону ответственности центра

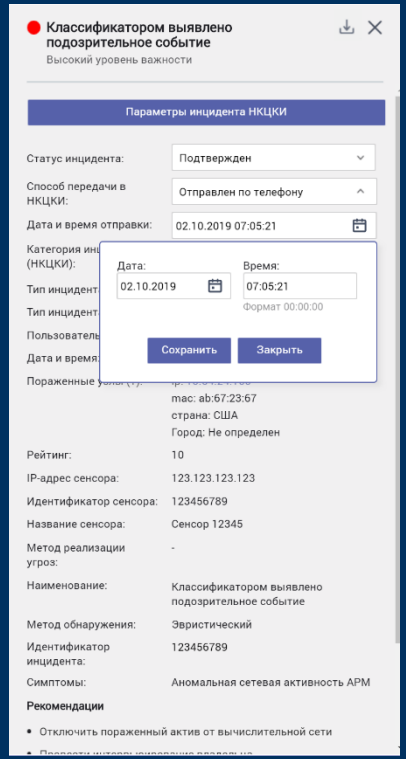
ViPNet TIAS 3.5



Карточка инцидента в формате НКЦКИ







ТЕХНО 2020 infotecs Фест

Спасибо за внимание!