MDR-сервисы на базе решения ViPNet TDR

Светлана Старовойт

Что такое MDR?

Определения

- **Управляемое обнаружение и реагирование (MDR)** — это служба кибербезопасности, которая сочетает в себе технологии и человеческий опыт для поиска, мониторинга и реагирования на угрозы.
- **Основное преимущество MDR** заключается в том, что он помогает быстро выявлять и ограничивать влияние угроз без необходимости в дополнительном персонале.

(c) 2021 Managed Detection and Response (MDR) Services Buyers Guide

Прогноз Gartner: к 2025 году 50% организаций будут использовать сервисы MDR

Как работает MDR?

- Приоритизация и анализ событий;
- Threat Hunting;
- Проведение расследования;
- Реагирование;
- Устранение последствий.

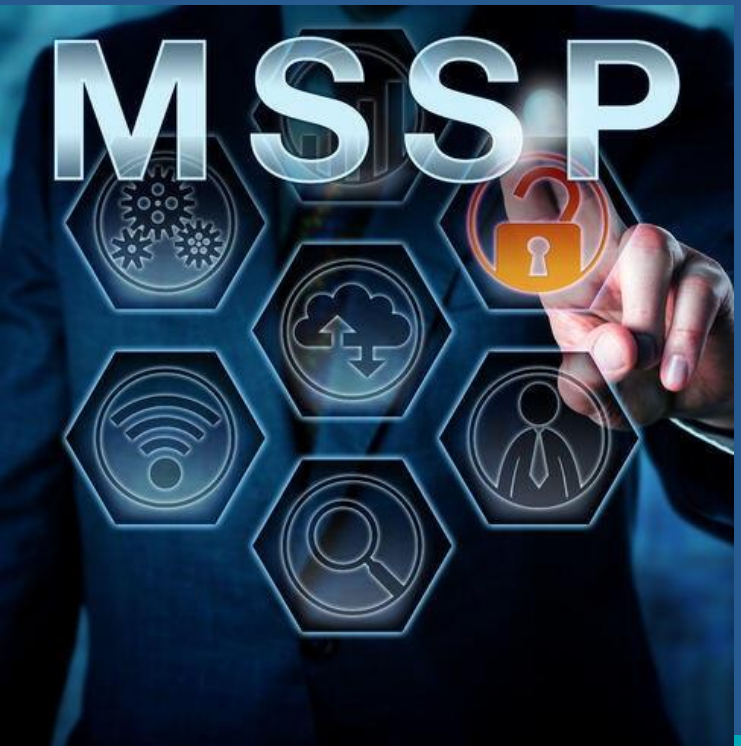
Что отличает MDR Security от других решений?

MDR vs EDR

EDR:

- Отслеживает и сохраняет поведение и события на конечных точках;
- Может автоматически блокировать известную угрозу;
- Нет полной картины для выявления сложных угроз;
- EDR – часть MDR.

MDR vs MSSP



MSSP:

- Являются предшественниками MDR;
- Включают более широкий спектр ИБ-услуг (управление активами, обновлениями, уязвимостями);
- Обычно не реагируют на угрозы активно;
- Клиенты MSSP должны привлекать дополнительных консультантов для выявления и расследования сложных угроз.

MDR vs SIEM

Причины неудовлетворенности системой SIEM © IDC

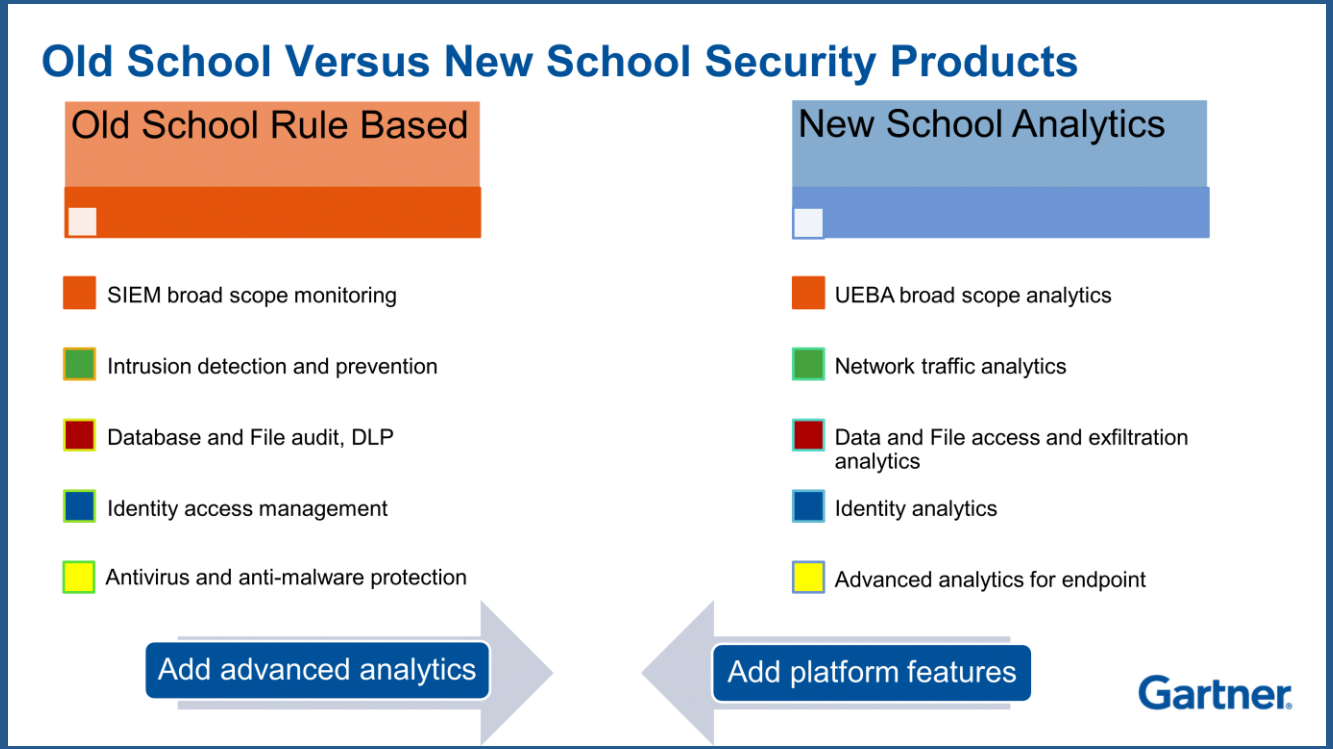
Все SIEM объединяет то, что их клиенты сталкиваются с трудностями в понимании результатов работы SIEM. 45% пользователей SIEM говорят, что им не хватает собственных знаний для полноценного использования своего решения SIEM. SIEM также могут быть дорогими и ресурсоемкими.

(c) 2021 Managed Detection and Response (MDR) Services Buyers Guide

ТЕХНО infotecs 2021 ФЕСТ

Бизнес-факторы внедрения MDR

Драйвер №1: Нужны сложные дорогие инструменты

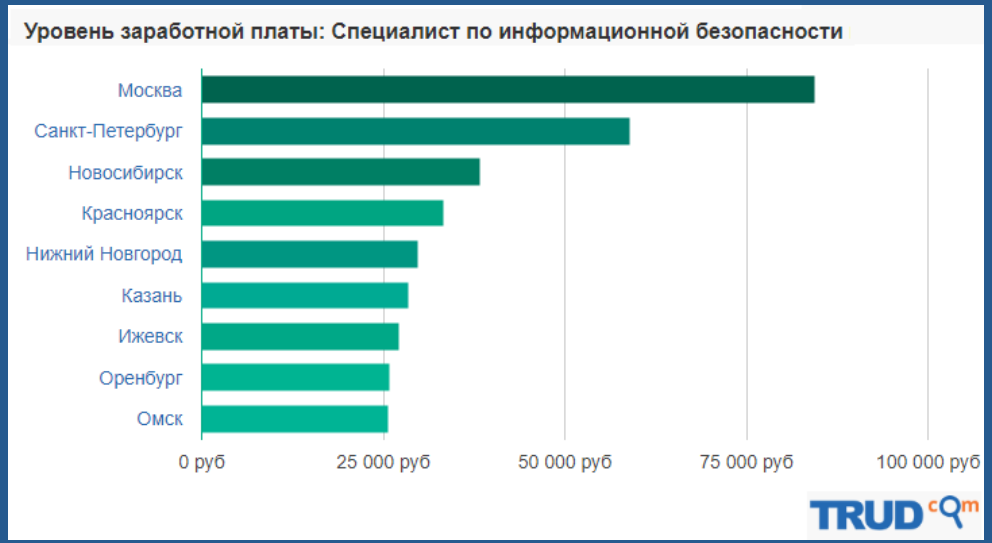


Использование устаревших инструментов

Драйвер №2: Персонал/ресурсы

Сегодня у большинства организаций есть инструменты безопасности в своем стеке, которыми у них нет времени управлять

(c) 2021 Managed Detection and Response (MDR) Services Buyers Guide



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

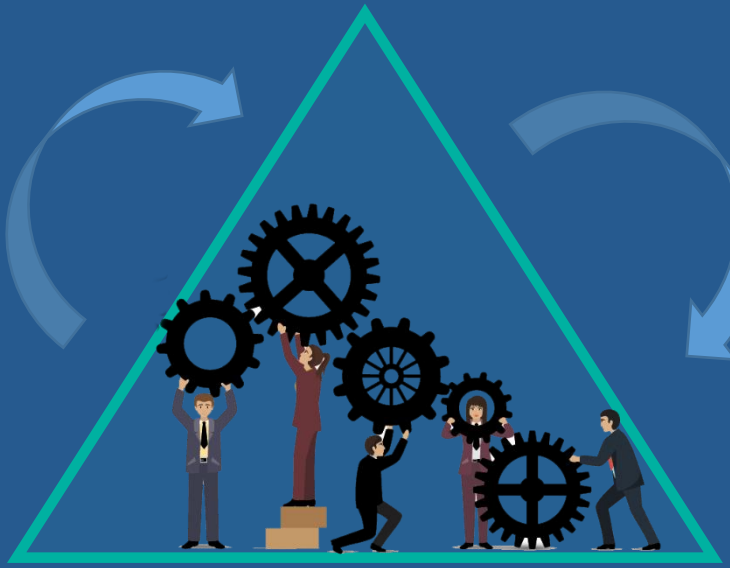
Драйвер №3: Неконтролируемый рост предупреждений от средств безопасности

Еще одна проблема – управление огромным количеством предупреждений от всех этих новых систем безопасности.
Это не новая проблема, но она растет на порядки по мере увеличения количества конечных точек, в том числе IoT, BYOD, удаленных сотрудников, подключенных партнеров по цепочке поставок и гибридных сетей.

(c) 2021 Managed Detection and Response (MDR) Services Buyers Guide

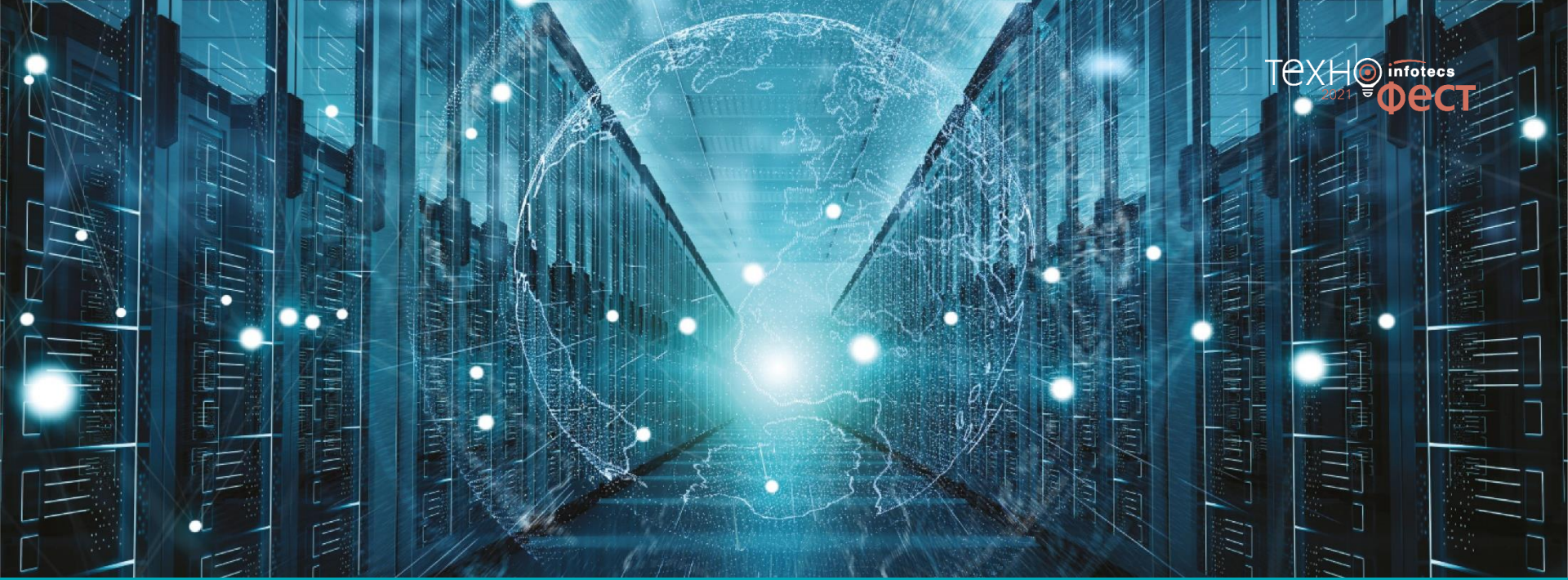
MDR это….

ЛЮДИ



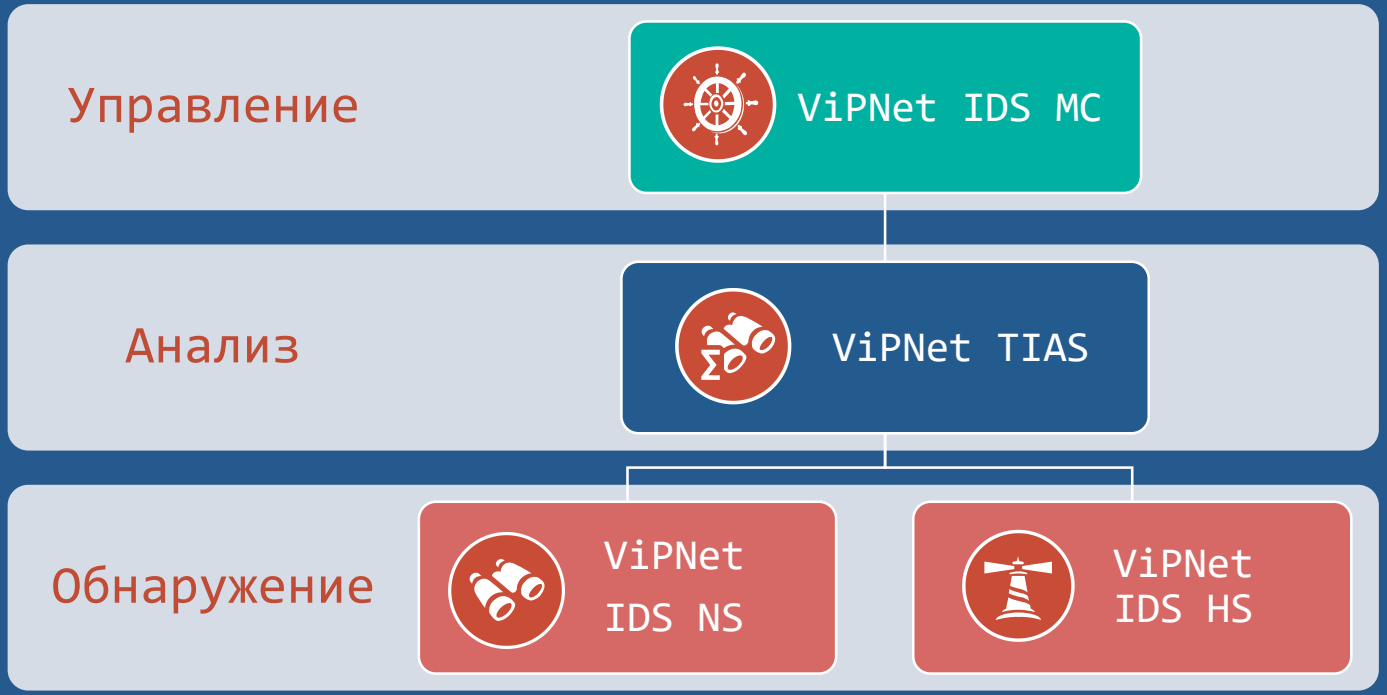
ПРОЦЕССЫ

ИНСТРУМЕНТЫ



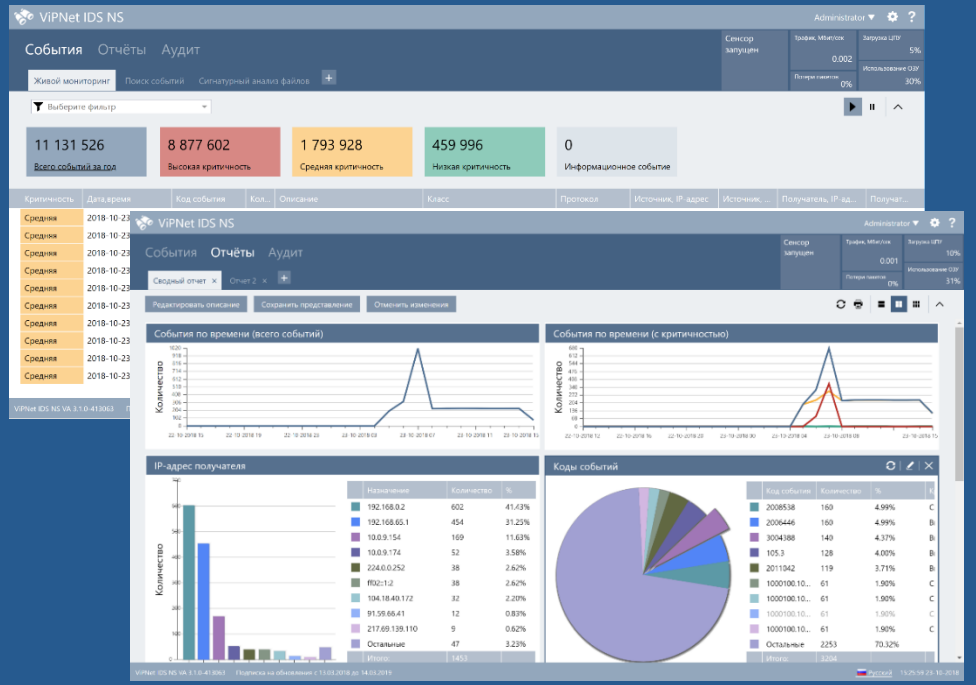
Решение ViPNet TDR

Состав решения ViPNet TDR



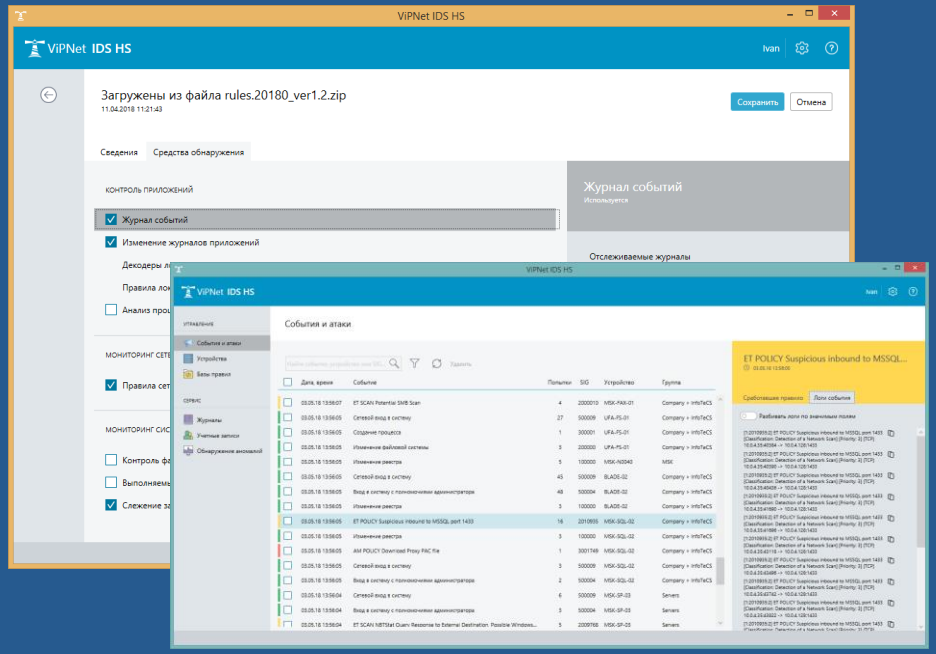
ViPNet IDS NS

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



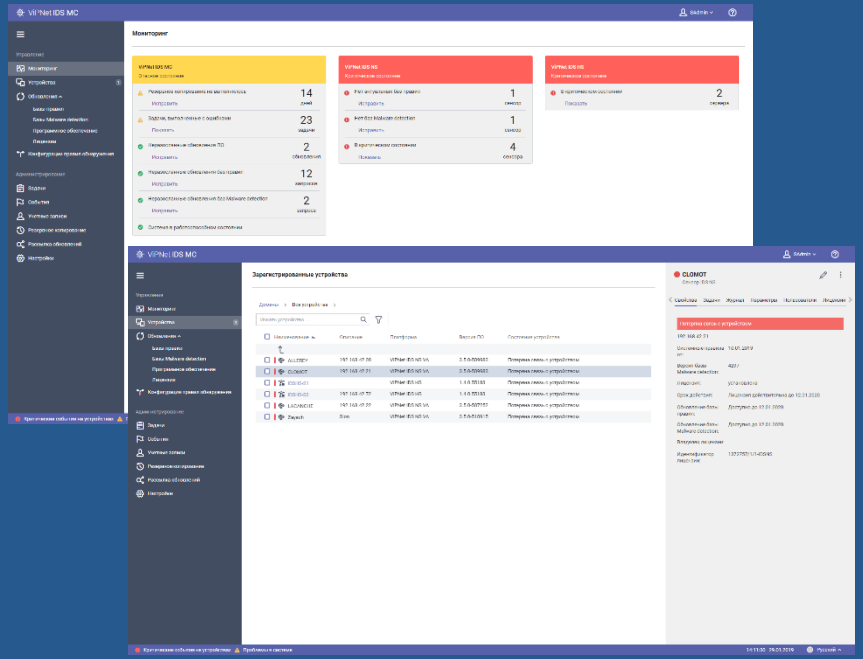
ViPNet IDS HS

- 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.



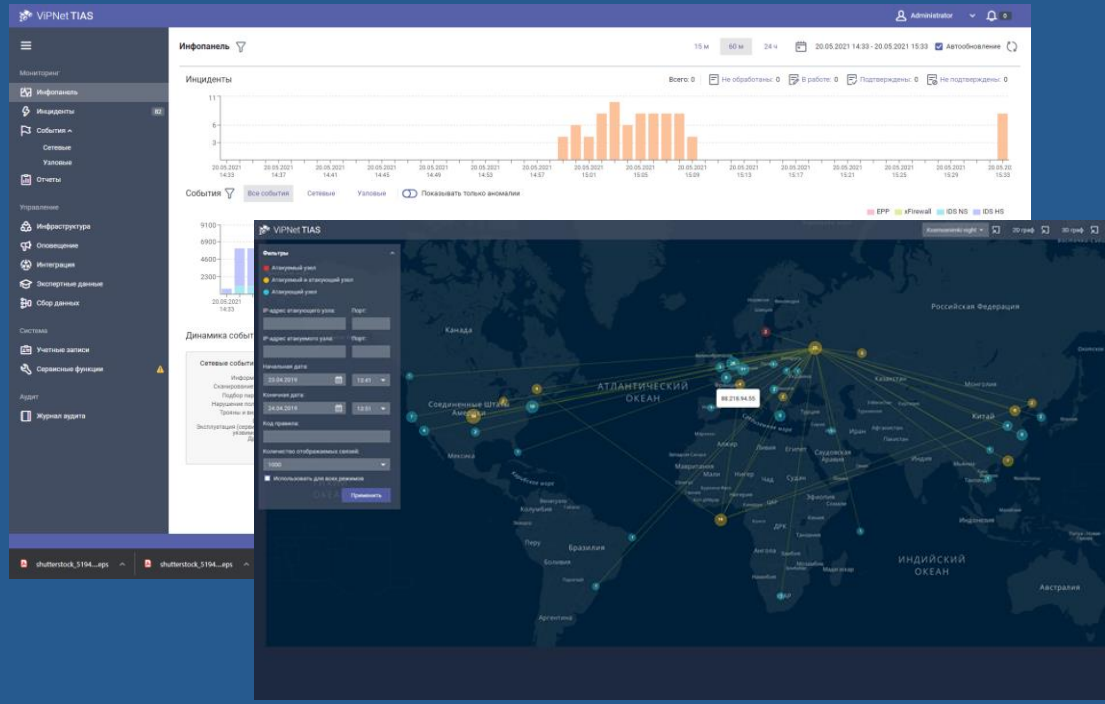
ViPNet IDS MC

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

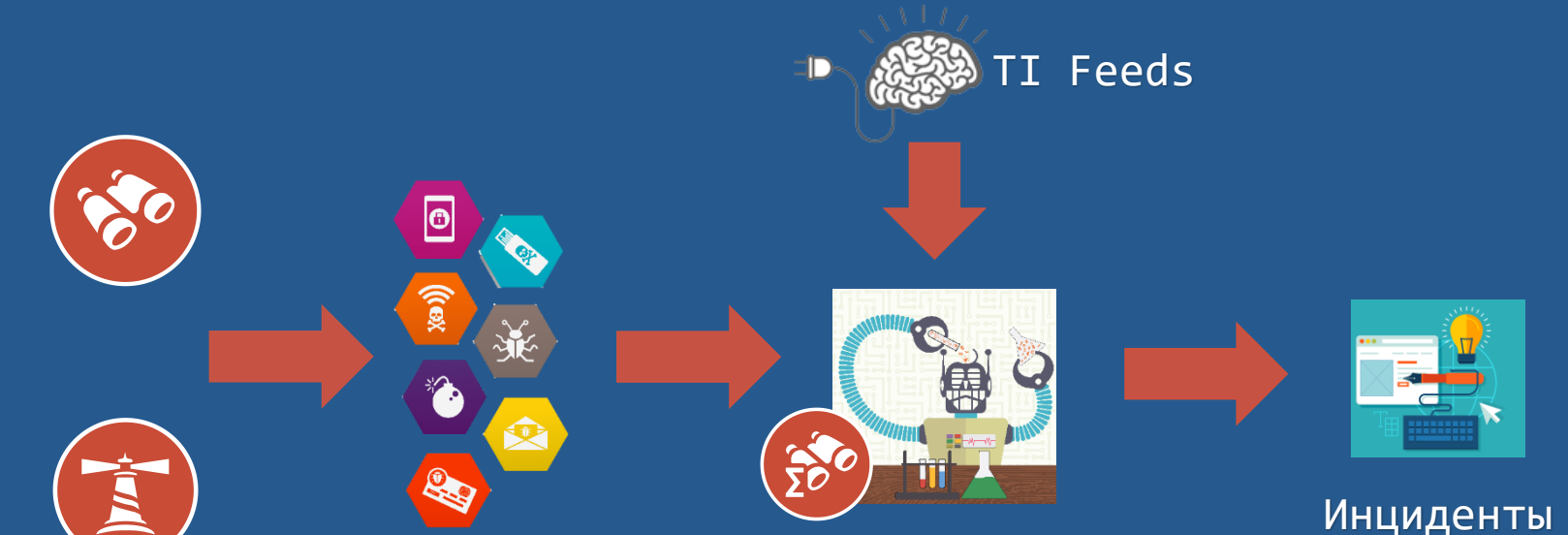


ViPNet TIAS

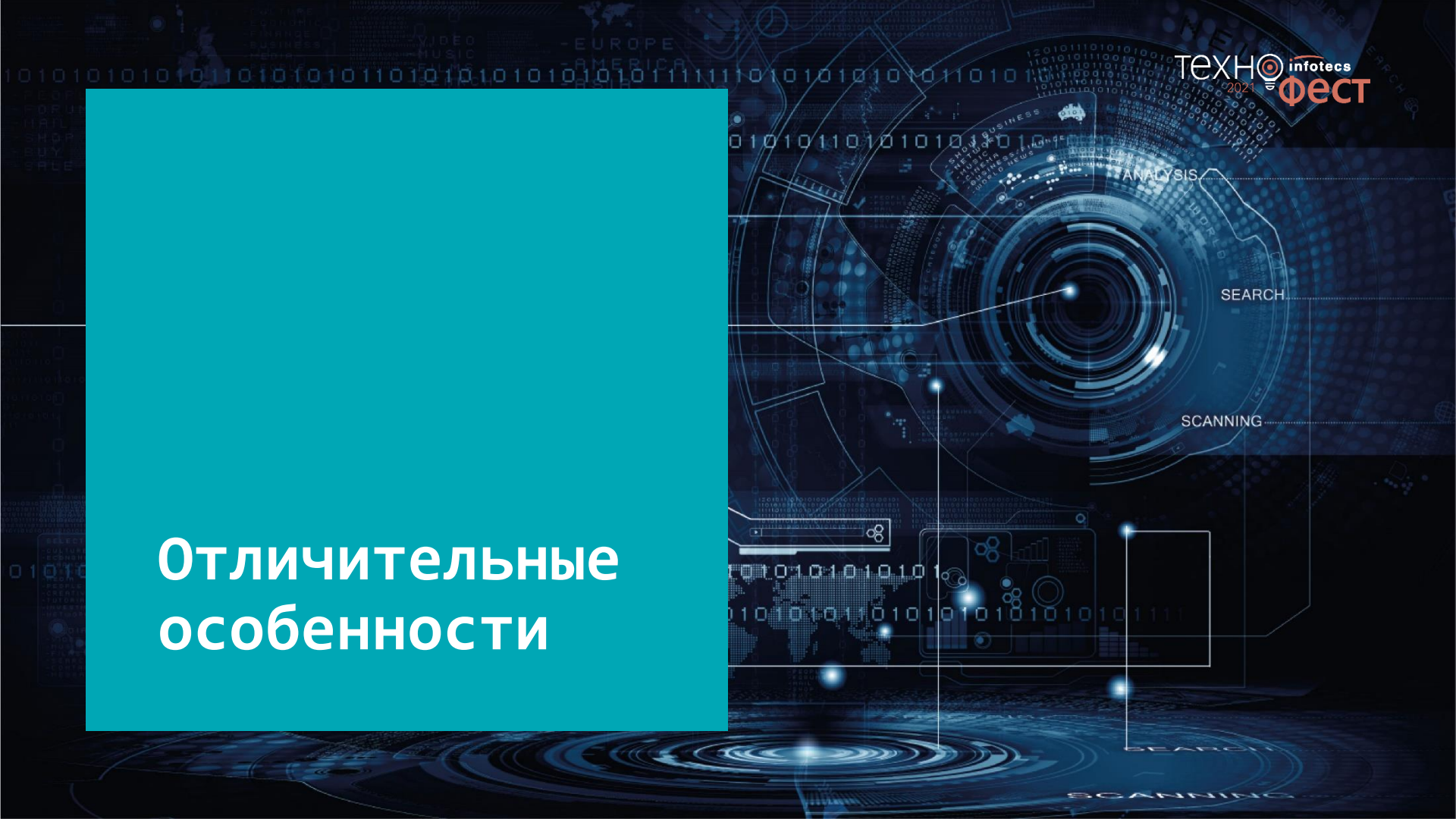
- анализировать события от сенсоров ViPNet IDS;
- выявлять инциденты;
- оповещать об инцидентах;
- проводить расследования;
- давать рекомендации;
- формировать отчеты.



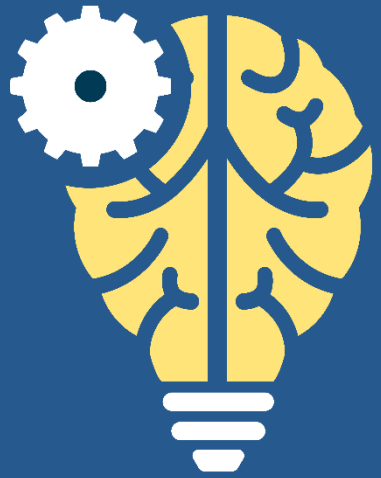
Как это работает?



Отличительные особенности



Machine Learning



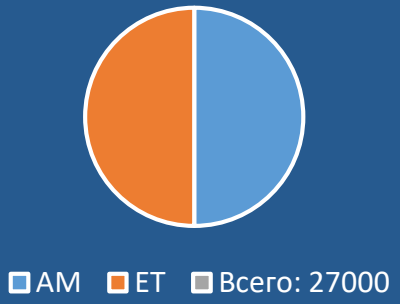
- математическая модель принятия решений;
- алгоритмы машинного обучения;
- ежемесячное переобучение;
- выявление атак нулевого дня.

Threat Intelligence

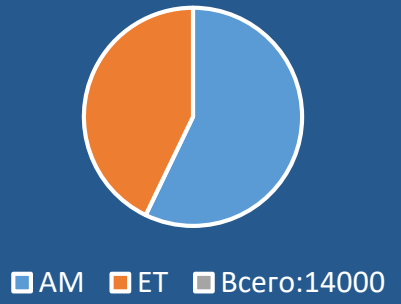
- индикаторы атак и компрометации;
- ТТП – тактики, техники, процедуры;
- информационный обмен:
  - СОПКА,
  - ФСТЭК,
  - RU-CERT.
- опыт клиентов – верифицированная и обезличенная информация.

Обновление правил и экспертных данных

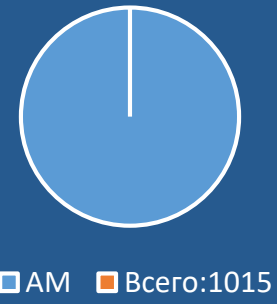
Правила IDS NS



Правила IDS HS

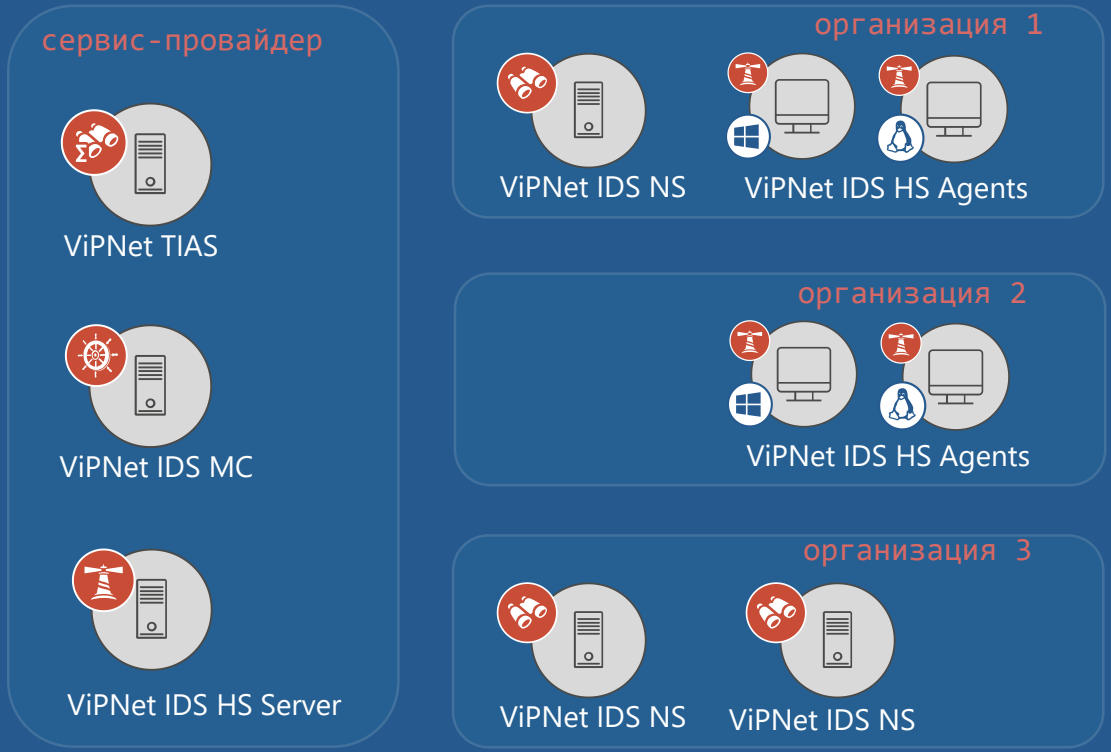


Правила TIAS



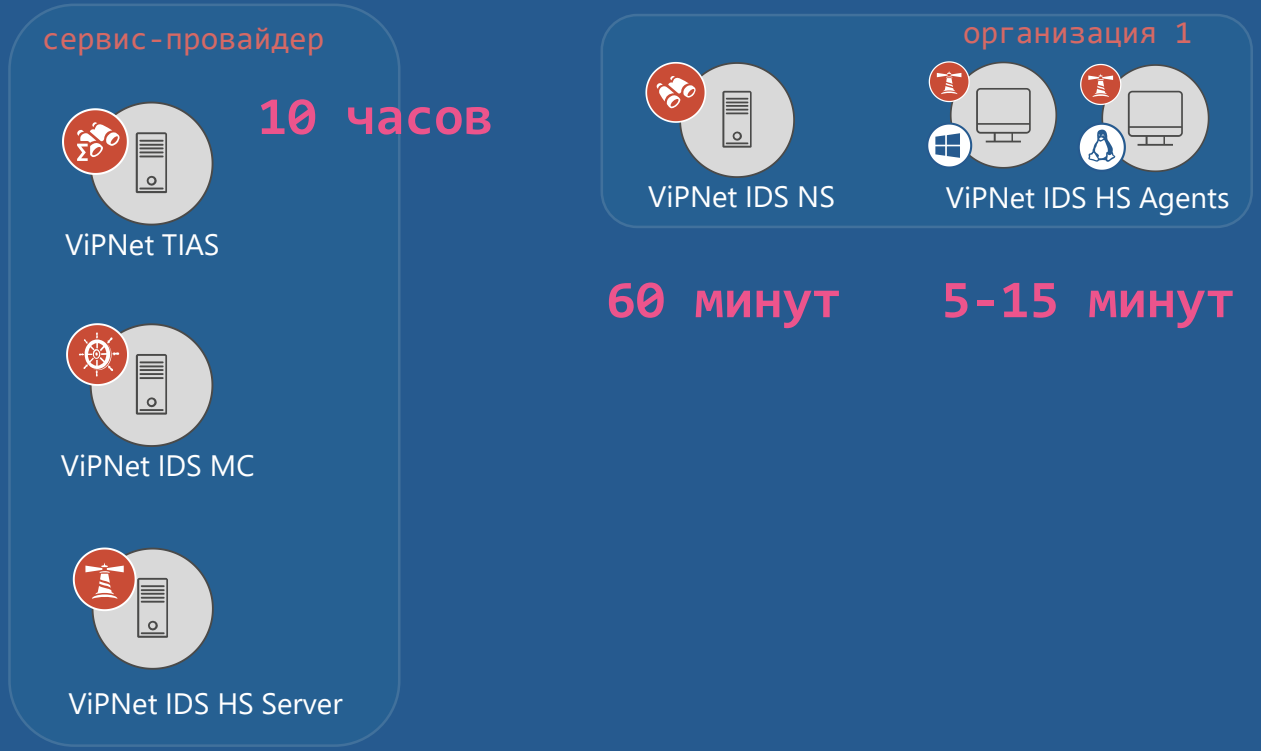
- **Ежедневное обновление правил;**
- **Ежемесячное переобучение математической модели.**

Облачный сервис на базе решения



- мастер подключения организации;
- активация и настройка сенсоров из IDS MC;
- мульти-арендный доступ;
- учет лицензий по организациям.

Внедрение решения



Перспективный мониторинг

- Центр мониторинга компьютерных атак
- Разработка правил snort IDS
- Threat Hunting
- Внедрение процедур безопасной разработки ПО
- Расследование компьютерных инцидентов
- Анализ защищённости и пентесты
- Подключение к ГосСОПКА

более **30** операторов, исследователей, аналитиков

И еще более 40 организаций подключались на мониторинг за последние 3 года.

Учебный центр

367 человек обучено на курсе «Администрирование IDS и TIAS»

16 ВУЗов имеют лаборатории, оснащенные ViPNet IDS и TIAS

Минутка патриотизма

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.

ГосСОПКА

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.

Перечень мероприятий

Класс В

- Взаимодействие с НКЦКИ;
- Разработка регламентирующих документов;
- Эксплуатация средств ГосСОПКА;
- Прием сообщений об инцидентах;
- Регистрация атак и инцидентов;
- Анализ событий ИБ;
- Инвентаризация.

Класс Б

- Анализ угроз ИБ;
- Составление и актуализация перечня угроз;
- Выявление уязвимостей;
- Подготовка предложений по повышению уровня защищенности;
- Составление перечня инцидентов.

Класс А

- Ликвидация последствий;
- Анализ результатов ликвидации последствий.

Варианты подключения

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

Объект КИИ

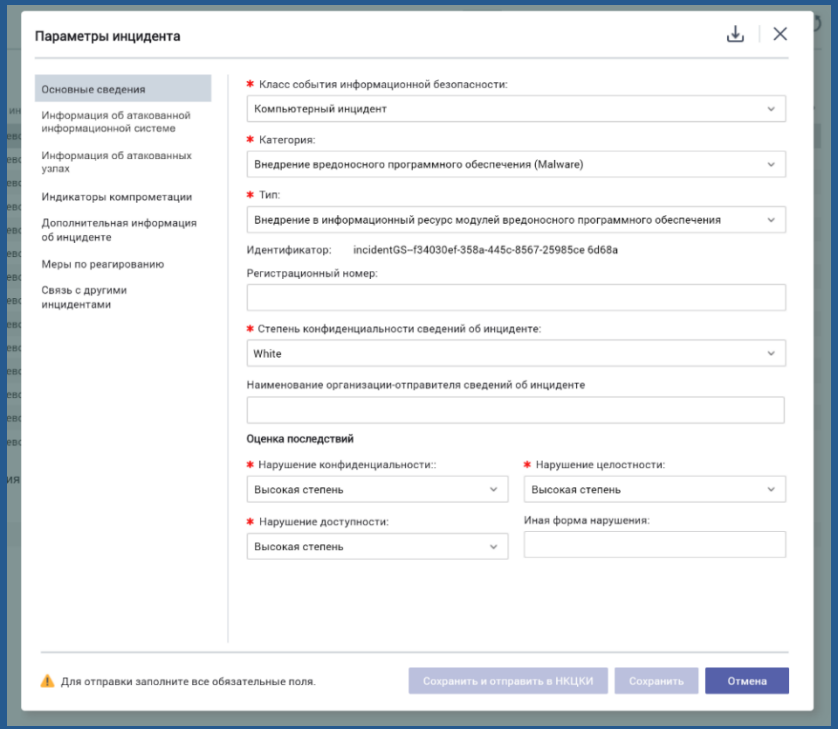
Подключение через корпоративный центр

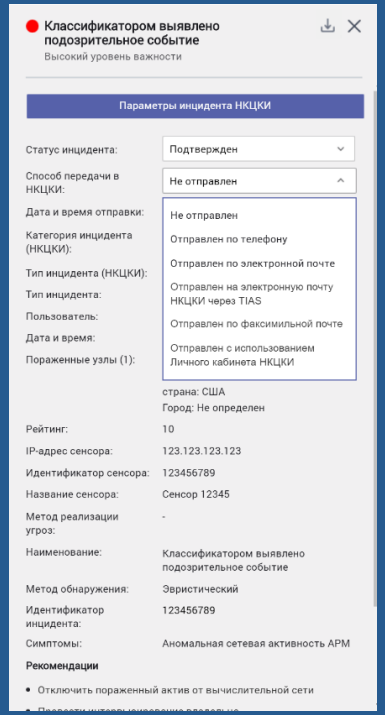
ГОССОПКА

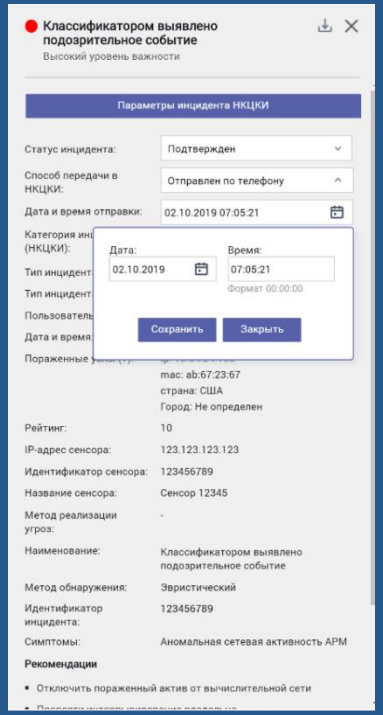
Корпоративный центр ГосСОПКА

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

Карточка инцидента в формате НКЦКИ







Сертификаты

ФСБ России
СОА класса В
Система IDS 3 в составе:

- ПАК ViPNet IDS NS
- ПО ViPNet IDS MC
- ПАК ViPNet

СЗИ
ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ СФ/СЗИ-0394

Выдан "22" июня 2020 г. Действителен до "30" июня 2023 г.

ФСТЭК России
СОВ 4 класс, ТДБ 4 уровень
Система IDS 3 в составе:

- ПО ViPNet IDS NS
- ПО ViPNet IDS MC
- ПО ViPNet TIAS

СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ
ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 4329

Выдан: 24 ноября 2020 г.
Действителен до: 24 ноября 2025 г.

Заявитель: АО «ИнфоТеКС»
Адрес: 127287, г. Москва, Старый Петровско-Разумовский проезд, д. 1/23, стр. 1
Телефон: (495) 737-6192

НАЧАЛЬНИК 2 УПРАВЛЕНИЯ ФСТЭК РОССИИ
Д.Шевцов

ТЕХНО 2021 infotecs Фест

Спасибо за внимание!

Подписывайтесь на наши соцсети

@infotecs.ru

@vpninfotecs

@InfoTeCS_Moscow