Практический опыт защиты КИИ на базе продуктов VipNet

Новые технологии - новые угрозы …
1. Защита АСУ ТП


Хакеры остановили крупнейший трубопровод США. За атакой могут стоять преступники из постсоветских стран

Мэри-Энн Рассон
Бизнес-корреспондент

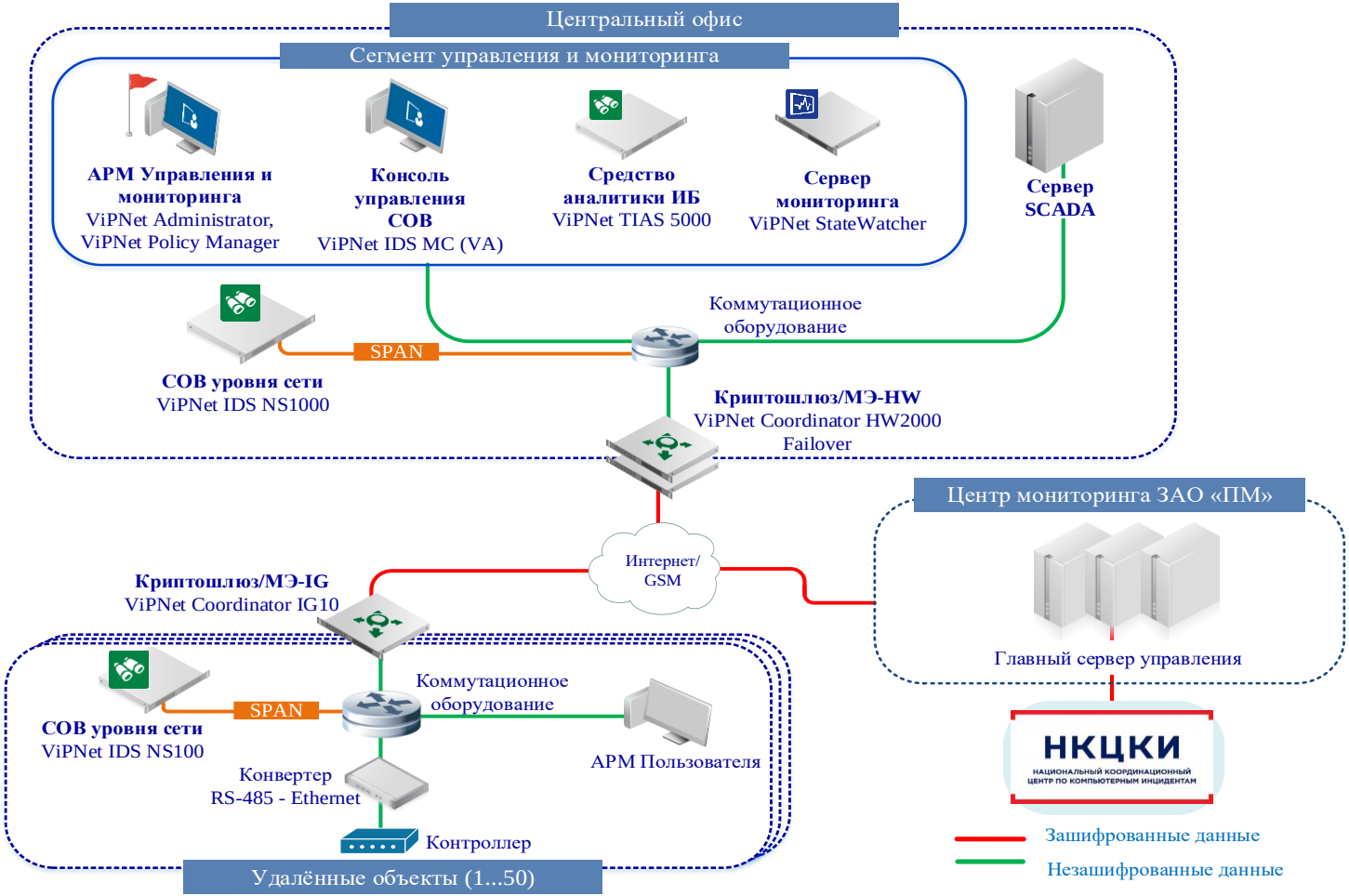
10 мая 2021

Реальность – массовое распространение АСУ ТП, тотальная автоматизация всех сфер промышленности и жизнедеятельности

Вызовы для производителей СЗИ:

- фильтрация трафика со специфическими тех. протоколами
- инспекция и выявление угроз в трафике с тех. протоколами
- работа в нештатных ситуациях – режим «пропускать всё»
- работа в особых климатических условиях
- шифрование специфических типов данных и трафика

Построение комплексной системы защиты



Выполнение требований КИИ

Группы мер обеспечения безопасности значимого объекта	ViPNet 4* Endpoint /Network	Coordinator HW Network	Coordinator IG Network	ViPNet IDS/TIAS Network	ViPNet Endpoint Endpoint
I. Идентификация и аутентификация (ИАФ)	+	+	+		+
II. Управление доступом (УПД)	+				+
III. Ограничение программной среды (ОПС)					+
IV. Защита машинных носителей информации (ЗНИ)					+
V. Аудит безопасности (АУД)	+	+	+	+	+
VI. Антивирусная защита (АВЗ)					
VII. Предотвращение вторжений (компьютерных атак) (СОВ)				+	
VIII. Обеспечение целостности (ОЦЛ)					+
IX. Обеспечение доступности (ОДТ)		+	+		+
XI. Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)	+	+	+		
XII. Реагирование на компьютерные инциденты (ИНЦ)	+			+	

ViPNet IG – шлюзы безопасности для АСУ ТП

VPN

- ViPNet VPN-шлюз сетевого уровня L3
- ViPNet VPN-шлюз сетевого уровня L2 (L2OverIP)
- VPN-сервер
- Аутентификация для каждого зашифрованного IP-пакета
- СКЗИ класса КС3 по требованиям ФСБ России

МЕЖСЕТЕВОЙ ЭКРАН

- NAT,
- Антиспуффинг
- Фильтрация по портам, адресам и типам протоколов
- Раздельные наборы фильтров для разных режимов работы
- DPI для Modbus TCP/RTU
- МЭ 4 класса защищенности по требованиям ФСБ России
- Сертификат ФСТЭК МЭ типа А.4 и Д.4

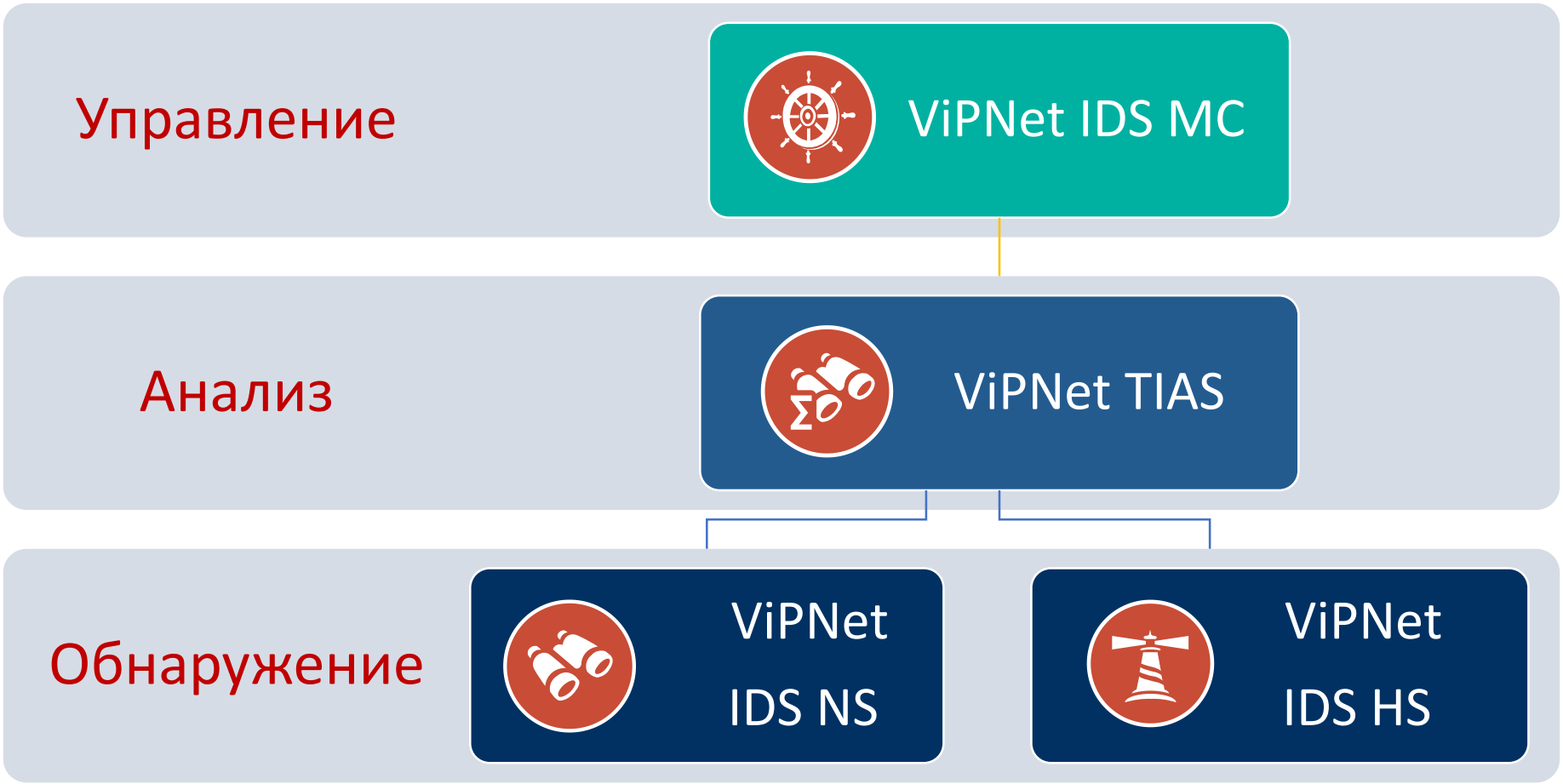
Новые технологии – новые угрозы …
2. Своевременное обнаружение компьютерных атак

Реальность – существенное снижение затрат для проведени компьютерных атак

Вызовы для производителей СЗИ:

- автоматизация своевременного обнаружения и предварительного анализа компьютерных атак
- автоматизация нейтрализации «типовых» атак
- доверие к базам решающих правил для СОВ и автоматизированных аналитических систем

Обнаружение, автоматизация анализа событий ИБ



Экспертиза. Создание баз решающих правил для СОВ

infotecs

Cisco

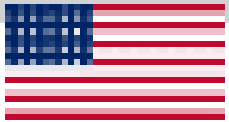
(VRT, Talos)

- 32665
- 250-300 новых сигнатур
- ZeroDay сигнатуры
- Страна происхождения: США

ET

(Emerging Threats Pro)

- 30034
- 300-400 новых сигнатур
- ZeroDay сигнатуры
- Страна происхождения: США

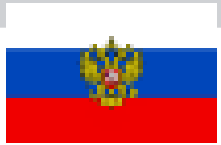


~~StoneSoft~~

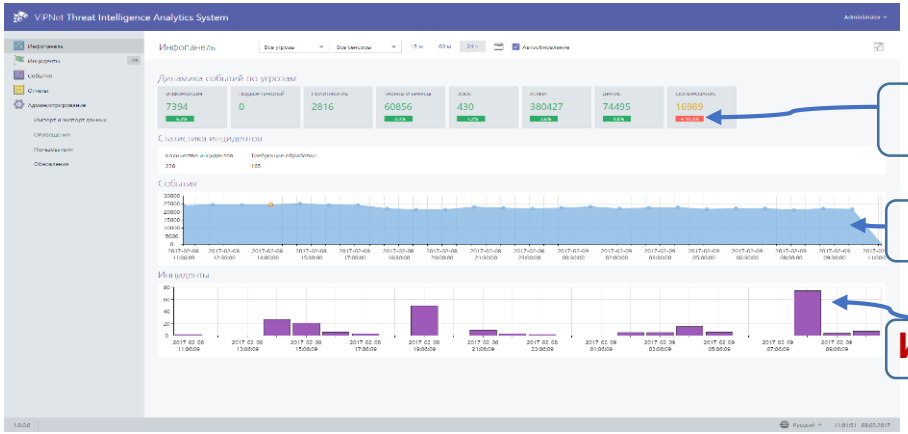
ИнфоТеКС

(AM Rules)

- 24866
- 300-400 новых сигнатур
- ZeroDay сигнатуры
- Страна происхождения: Россия



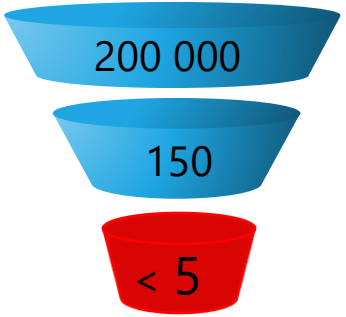
ViPNet TIAS. Автоматизация анализа событий ИБ



Динамика

События

Инциденты



- сбор и анализ событий от сенсоров
- автоматическое выявление инцидентов;
- оповещение об инцидентах;
- инструменты для проведения расследований;
- формирование отчетов

ViPNet xFirewall
Автоматизация нейтрализации угроз, работа модуля IPS

Новые технологии – новые угрозы …
3. Своевременное реагирование на компьютерные атаки

Спецназ США готовится к кибервойне с Россией

Интернет ИТ в госсекторе Техника

12.10.2020, Пн, 09:08, Мск , Текст: Эльяс Касми

В составе американского спецназа могут появиться кибервойска для возможной виртуальной войны с КНР и Россией. В нее войдут хакеры, специалисты по ИИ и машинному обучению, а также знатоки языков.

Реальность – дефицит специалистов по мониторингу, анализу и реагированию на компьютерные атаки

Вызовы для производителей СЗИ:

- доверие к базам решающих правил для СОВ и автоматизированных аналитических систем
- экспертиза - методы и способы выявления и реагирования на компьютерные атаки
- экспертиза по расследованию инцидентов

ГосСОПКА

Опыт сотрудничества по ГосСОПКА

- Наличие у Головной организации действующего SOC центра в момент внедрения системы
- Наличие у Заказчика настраиваемой SIEM системы

Экспертиза

Первая линия	Вторая линия	Третья линия
Взаимодействие с пользователями	Помощь в расследовании и установлении причин инцидентов	Подготовка и улучшение нормативной базы, описание сценариев выявленных инцидентов
Анализ событий и обнаружение компьютерных атак и инцидентов	Координация действий при реагировании на инциденты ИБ	Разработка сигнатурных правил и правил корреляции
Регистрация инцидентов ИБ и оповещение заинтересованных лиц	Анализ уязвимостей, анализ защищенности, тестирование на проникновение	Углубленный анализ Инцидентов ИБ, сбор доказательной базы

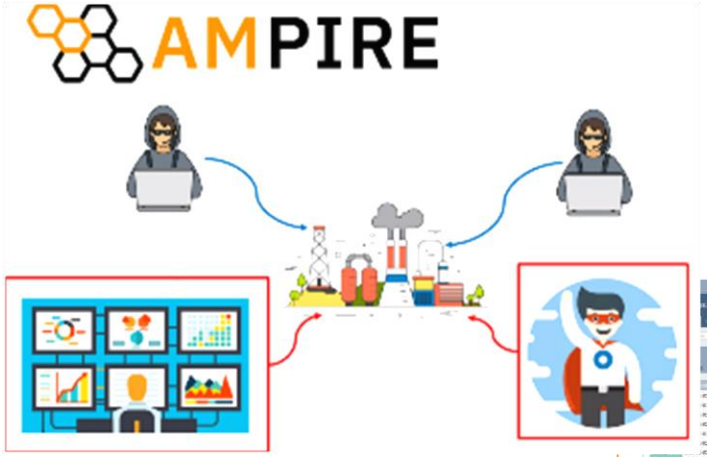
Новые технологии – новые угрозы …
4. Подготовка специалистов по защите информации

Реальность – дефицит специалистов по мониторингу, анали
и реагированию на компьютерные атаки

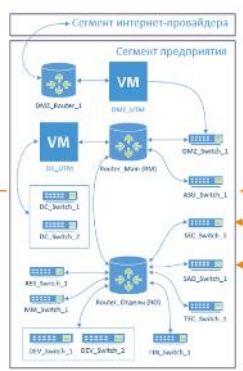
Вызовы для производителей СЗИ:

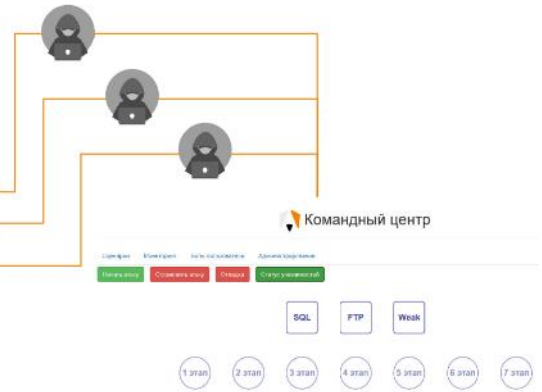
- автоматизация процесса обучения специалистов по ИБ
- создание средств имитации компьютерных атак и технических средств обучения реагирования на компьютерные атаки, приближенные к реальности

ViPNet AMPIRE– киберполигон, платформа для обучения



Технические средства





Силы реагирования

Контакты:

ОАО «ИнфоТеКС»

Макарова Ольга

olga.makarova@infotecs.ru

+7 (912) 62-918-58