Руководство по эксплуатации

программного обеспечения «Программный комплекс защиты и анализа информационных систем NeuroFortress»

ООО «Сивиэй Технолоджиес»

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

«Программный комплекс защиты и анализа информационных систем NeuroFortress»

РУКОВОДСТВО ПО ЭКСПЛУАТАЦИИ

На 23 листах

Ростов-на-Дону

2023

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Сокращения, которые используются в настоящем документе, приведены в таблице 1.

Таблица 1 – Сокращения и расшифровки

Сокращение	Расшифровка
ОС	Операционная система
ПК	Персональный компьютер
ПО	Программное обеспечение
ПО NeuroFortress	Программный комплекс защиты и анализа информационных систем NeuroFortress

1. Общие сведения. Назначение

Из-за остро необходимого процесса цифровизации предприятий торговли, промышленности, строительства и услуг, позволяющей расширяться и оптимизировать процессы и расходы компаний, они все чаще сталкиваются с угрозами киберпреступлений.

В последние годы в связи с экспоненциальным ростом возможных каналов утечки информации – из-за увеличения количества программных продуктов и широкого использований социальных взаимодействий посредством новейших средств личной и корпоративной связи, используемых в современном производстве и деятельности компаний – классические подходы к защите информации не дают полной изоляции информации.

NeuroFortress, являясь современным комплексом – базируется на архитектуре защиты информации от момента их рождения в инфраструктуре – следуя и контролируя весь жизненный цикл, используя контейнеры данных и сквозной контроль за ними на уровне ядра операционных систем, что полностью исключает утечку в результате несанкционированных действий или вредоносного доступа.

В настоящее время для противостояния более сложным угрозам, целенаправленным атакам - организациям необходимо уделять особое внимание не только уровню конечных точек, но и другим потенциальным точкам проникновения злоумышленника в инфраструктуру и, самое главное, на взаимосвязи между ними. Профессиональные киберпреступники сегодня предпочитают многовекторный подход к проникновению в корпоративную сеть, атакуют как можно больше элементов инфраструктуры и часто объединяют множество различных методов в одну запланированную атаку. Организации должны обладать пониманием того, что происходит у них в рамках всей инфраструктуры, контролировать ключевые точки проникновения и получать полную картину атаки, иметь возможность быстро анализировать первопричины, проводить глубокие расследование сложных инцидентов и реагирования на них в рамках всей инфраструктуры, а не отдельных элементов.

Благодаря NeuroFortress все подсистемы обретают единую среду обмена данными и получения единой картины происходящего в инфраструктуре. Единая консоль управления для удобства работы аналитика, предоставляемый высокий уровень автоматизации, усовершенствованный процесс приоритизации инцидентов, сокращение числа

ложноположительных срабатываний и времени, которое аналитики тратят на процесс расследования и реагирования на инциденты делает NeuroFortress самым оптимальным решением.

Рассмотрим корпоративную систему кибербезопасности NeuroFortress и Единую среду взаимодействий и реагирования XDR

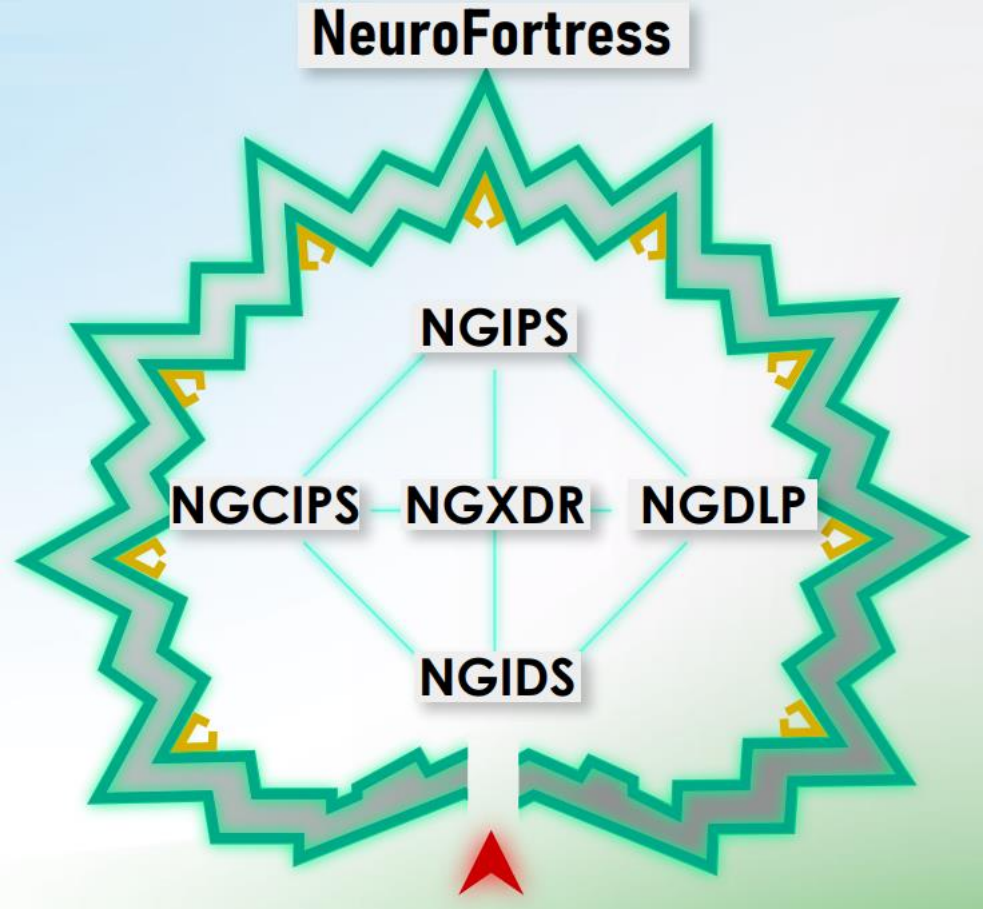

Рисунок 1 – Структурная схема ПО NeuroFortress

Архитектура системы базируется на интеллектуальном обнаружении и предотвращении. Реагирование на сложные угрозы и целевые атаки проводятся путем охвата большого количества источников данных, подсистем предотвращения в рамках конечных точек и сетевой шине обмена статистическими обезличенными данными. На конечных точках используемся программное обеспечение агента NeuroFortress для операционных систем, серверов и персональных компьютеров. Сделаем важное уточнение – система не собирает и не передает персональные сведения, однако защита информации в системе начинает работать с момента рождения таких данных, и подсистема предотвращения утечек прозрачно на уровне

ядра операционных систем контролирует весь жизненный цикл защищенных контейнеров не раскрывая внутреннего содержимого.

На следующем рисунке приведено сравнение с конкурентными решениями:

Сравнение с конкурентами

По данным:
www.vulnerability-lab.com
www.defcon.org
www.anti-malware.ru
securityweekly.com
www.owasp.org
www.aircrack-ng.org

В рамках требований ГосСОПКА наша система поддерживает и реализует функционал средств обнаружения, предупреждения, ликвидрации, обмена информацией, интегрируется в средства криптогразащиты каналов связи, и существенно опережает известные системы в идентификации неизвестных угроз, благодаря использованию инновационных алгоритмов машинного обучения.

Наименование IDS/IPS	Нейросетевой детектор	Беспроводные сети и IoT	Скорость обнаружения угрозы	Обнаружение неизвестных атак
Наш продукт IDS NeuroFortress	**+**	**+**	**Быстро**	**+**
Traffic Inspector Next Generation/ Suricata	-	-	Средне	-
FortiGate	-	Заявлено в перспективе	Быстро	+
Континент	-	-	Быстро	-
СОВ Континент	-	-	Быстро	-
Check Point Next Generation Firewalls	Заявлено в перспективе	-	Средне	-
Cisco Firepower NGFW	-	-	Быстро	+
ViPNet IDS	-	-	Быстро	+
Аргус	-	-	Медленно	-
Fortinet	-	Заявлено в перспективе	Быстро	-
Palo Alto Networks	-	-	Быстро	-
Usergate	-	-	Быстро	-

Рисунок 2 – сравнение с конкурентными решениями

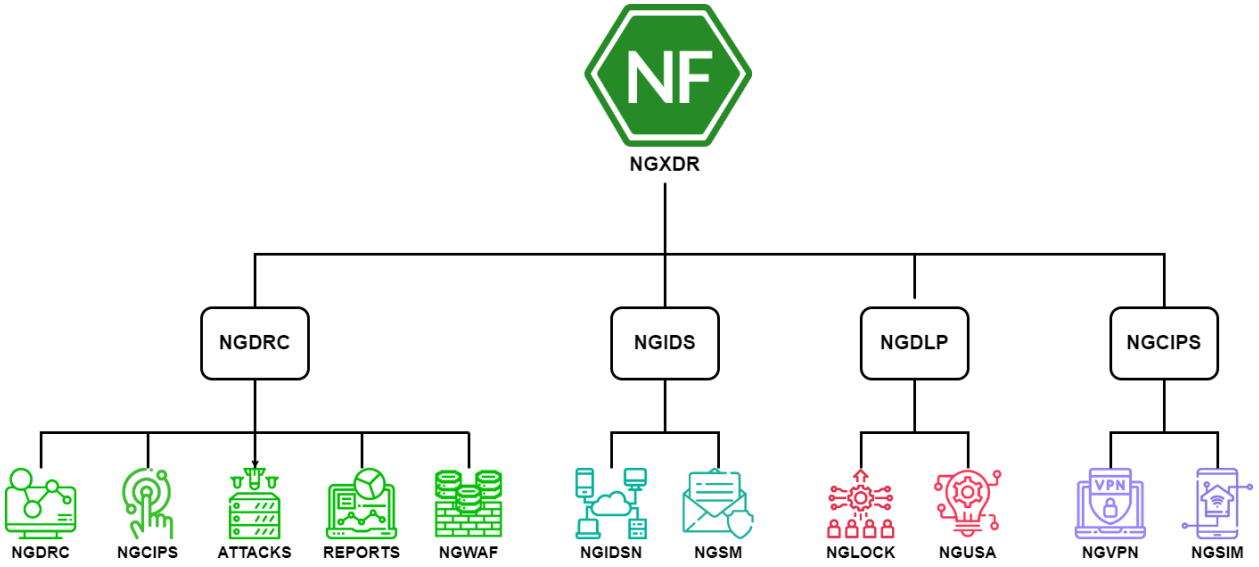

Рисунок 3 – схема инфраструктуры NeuroFortress

2. Системные требования

Операционная система Widows

Операционная система	Windows 10,11
Процессор	CPU 2 ядра и более
Оперативная память	Минимально – 2 ГБ Рекомендуется – 4 ГБ
Жесткий диск (свободное пространство)	SSD или HDD размером от 10 Гб

Операционная система Linux

Операционная система	Linux Ubuntu, Linux Ubuntu Server, Astra Linux, ALT Linux, OS Atlant
Процессор	CPU 2 ядра и более
Оперативная память	Минимально – 2 ГБ Рекомендуется – 4 ГБ
Жесткий диск (свободное пространство)	SSD или HDD размером от 10 Гб

3. Проверка работоспособности ПО NeuroFortress

Для начала работы с программным продуктом «Программный комплекс защиты и анализа информационных систем NeuroFortress» необходимо запустить приложение, подключиться к системе и авторизоваться в соответствии с данными, полученными от сотрудников ООО «Сивиэй Технолоджиес»

Выбрать информационную модель «NGDRC»:

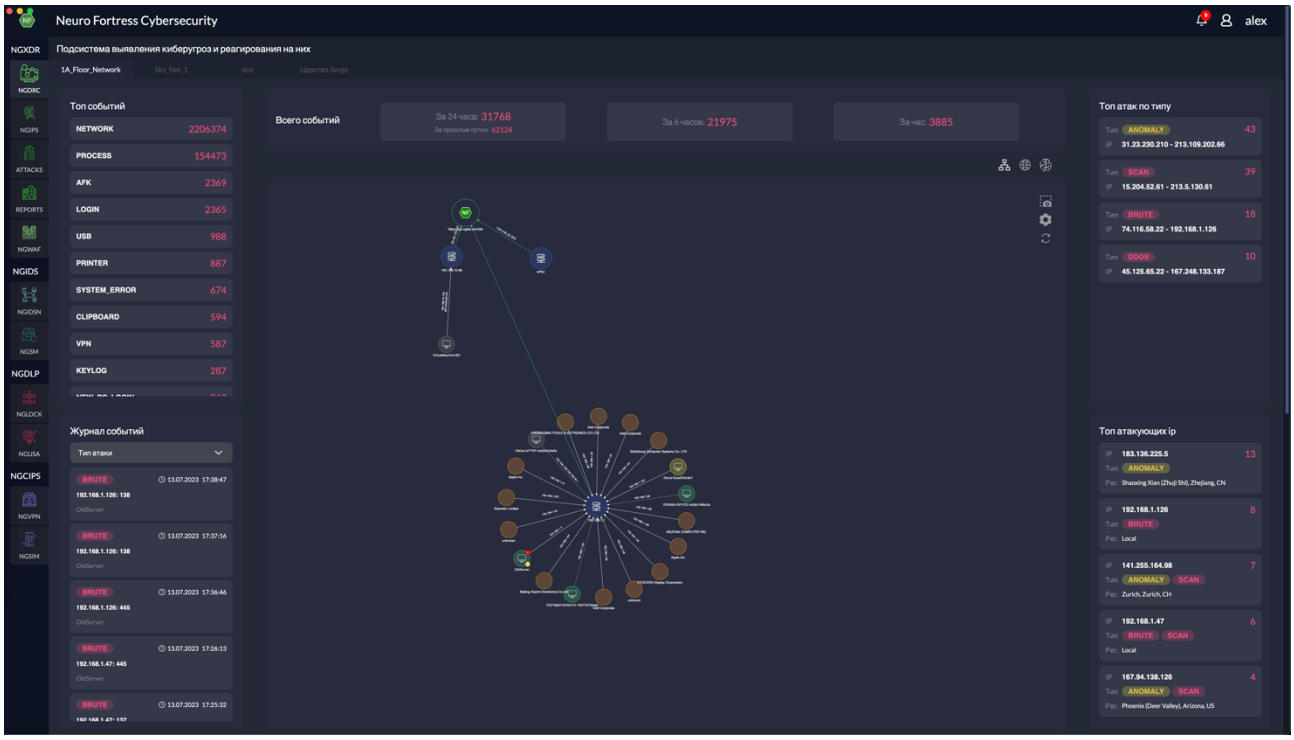

Рисунок 4 – Выбор информационной модели «NGDRC»

Путем контроля информационной модели «Топ событий» проверяют наличие полей «NETWORK» и «PROCESSES» более 2 полей.

Путем контроля информационной модели «Журнал событий» проверяют наличие полей событий с датой и временем до 48 часов более 2 шт.

Путем контроля информационной модели «Топ атак по типу» проверяют наличие полей «ANOMALY» и «SCAN» более 2 шт.

Путем контроля информационной модели «Топ атакующих ip» проверяют наличие полей с ip адресами.

Путем контроля информационной модели «Карта сети» проверяют наличие отображения «NF» и соседних хостов.

Положительных результат контроля данных информационных систем говорит о выполнении требований к качественным и количественным характеристикам функционала «NGDRC».

Выбрать информационную модель «NGIPS»:

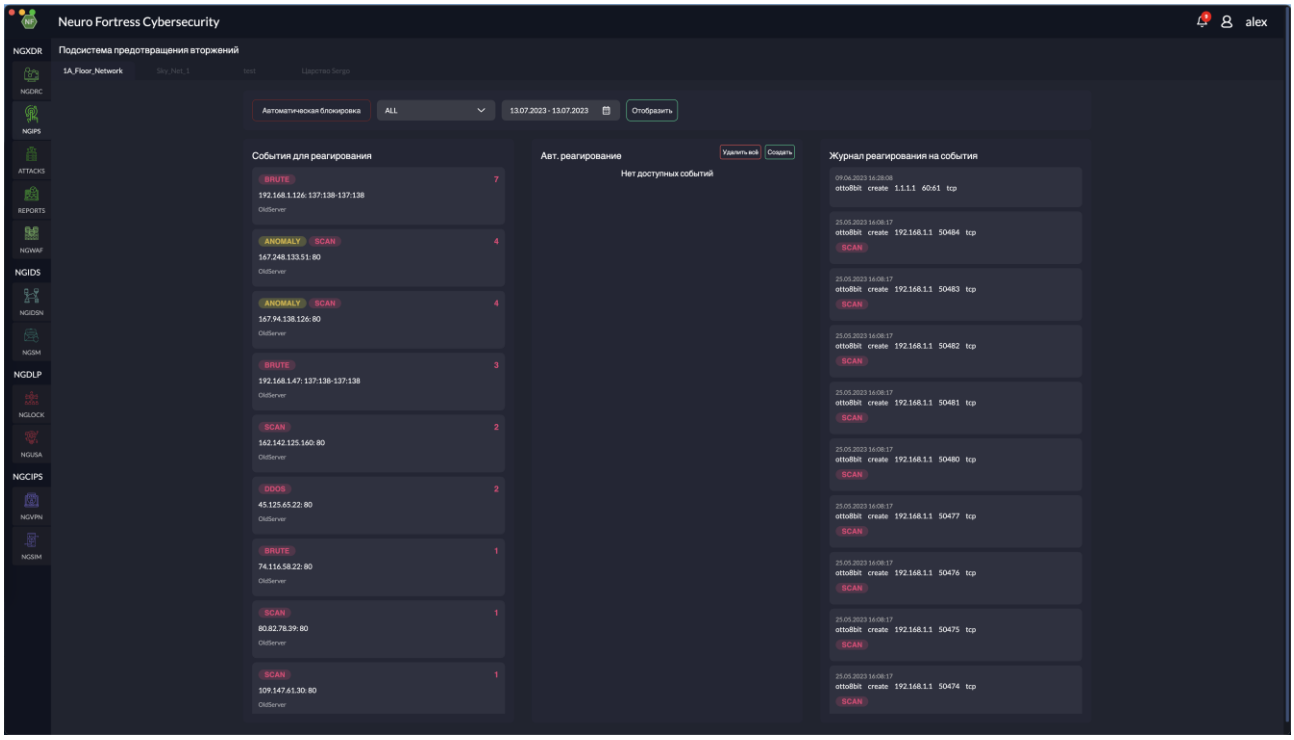

Рисунок 5 – Выбор информационной модели «NGIPS»

Путем контроля информационной модели «События для реагирования» проверяют наличие полей «ANOMALY» или «SCAN» более 2 полей.

Путем контроля информационной модели «Журнал реагирования на события» проверяют наличие полей событий с датой и временем до 60 дней более 2 шт.

Путем выбора в информационной модели «События для реагирования» и выбора первого поля контролируют создание правила в модели «Авт. Реагирование».

Положительных результат контроля данных информационных систем говорит о выполнении требований к качественным и количественным характеристикам функционала «NGIPS».

Выбрать информационную модель «ATTACKS»:

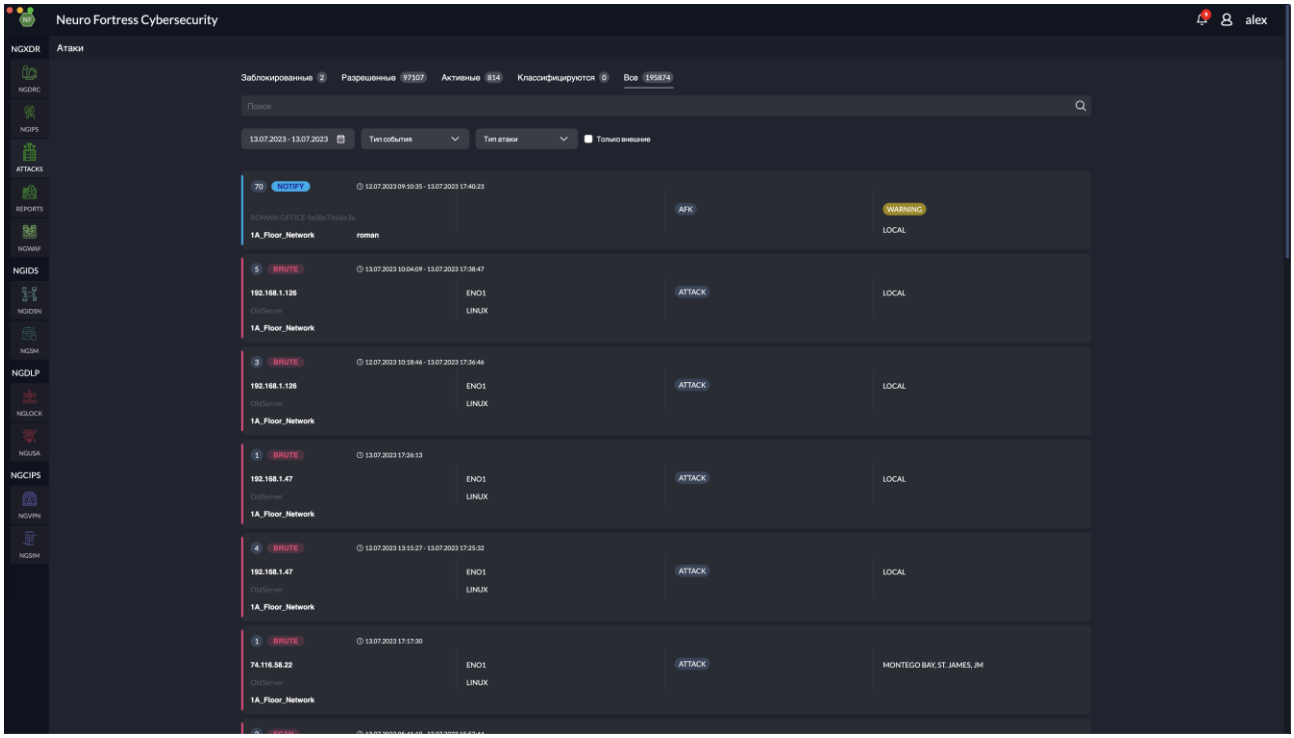

Рисунок 6 – Выбор информационной модели «ATTACKS»

Путем контроля информационной модели «Атаки» проверяют наличие полей – должно быть отображено более 2 полей и указан тип атаки в каждом из них.

Путем контроля фильтра «Тип события» проверяют наличие переключение типа событий.

Положительных результат контроля данных информационных систем говорит о выполнении требований к качественным и количественным характеристикам функционала «ATTACKS».

Выбрать информационную модель «REPORTS»:

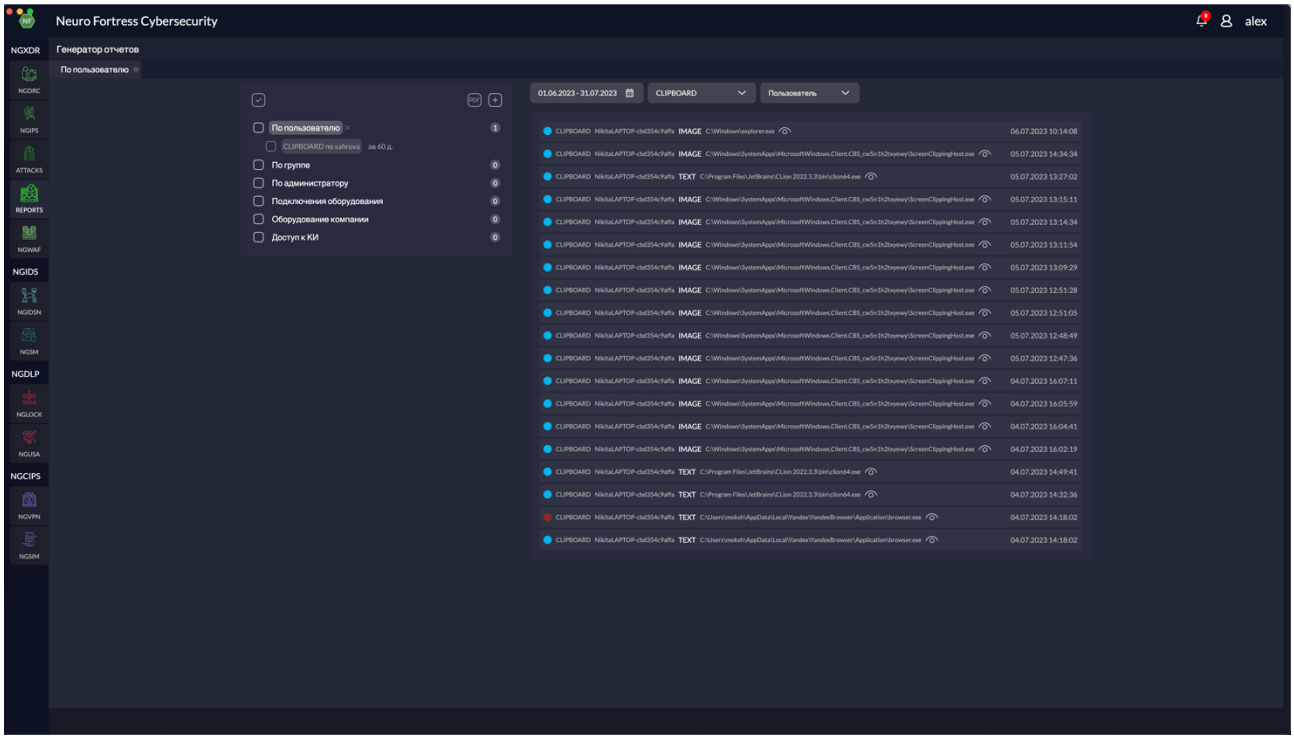

Рисунок 7 – Выбор информационной модели «REPORTS»

Путем контроля информационной модели «Генератор отчетов» проверяют наличие отчета по выбранному типу «CLIPBOARD».

Путем выбора другого фильтра – контролируют изменение вида отчета.

Положительных результат контроля данных информационных систем говорит о выполнении требований к качественным и количественным характеристикам функционала «REPORTS».

Выбрать информационную модель «NGWAF»:

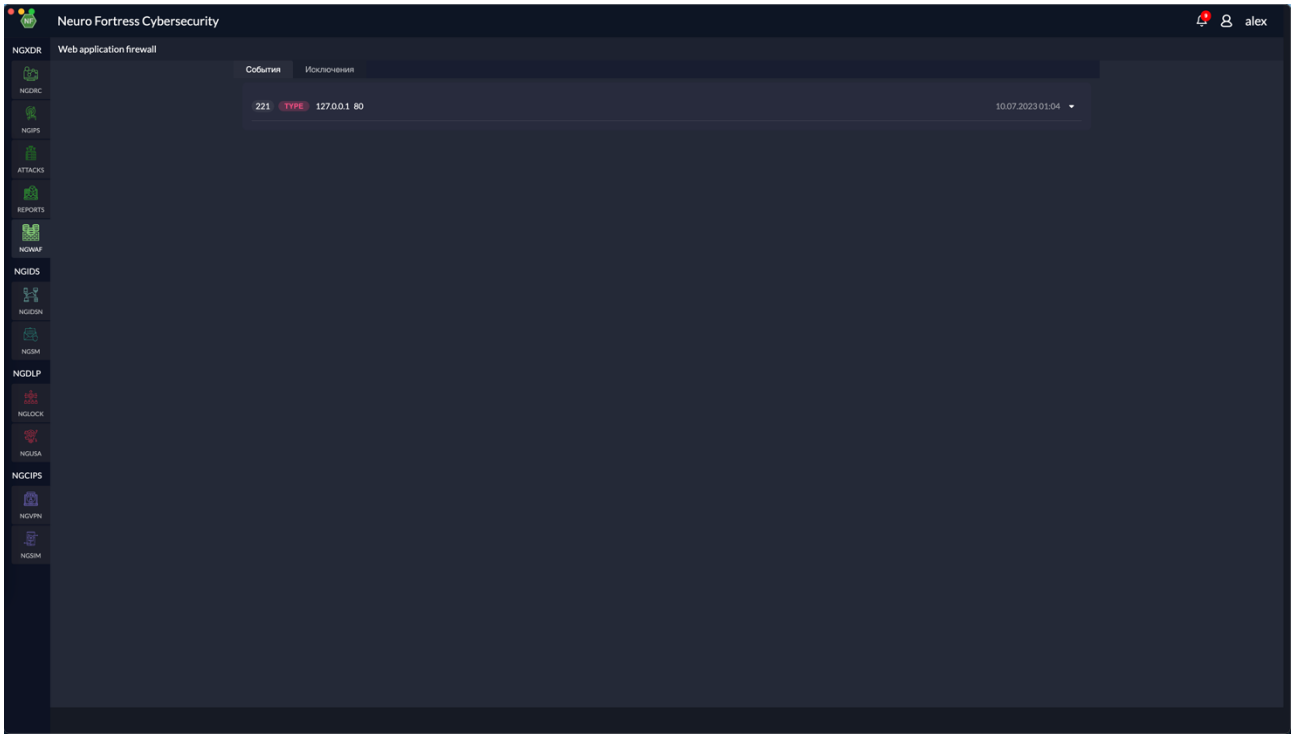

Рисунок 8 – Выбор информационной модели «NGWAF»

Путем контроля информационной модели «События» проверяют наличие как минимум одного поля событий брандмауэра.

Положительных результат контроля данных информационных систем говорит о выполнении требований к качественным и количественным характеристикам функционала «NGWAF».

Выбрать информационную модель «NGIDSN»:

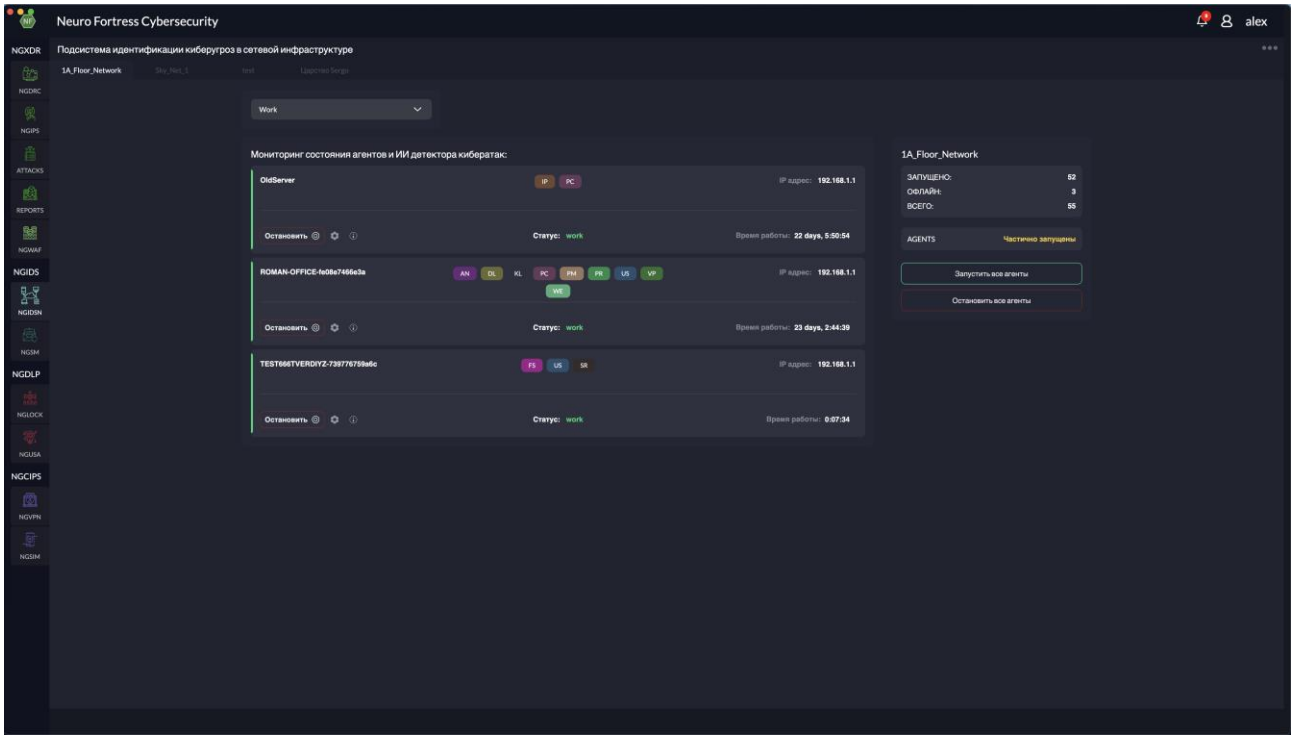

Рисунок 9 – Выбор информационной модели «NGIDSN»

Путем контроля информационной модели «Подсистема идентификации киберугроз сетевой инфраструктуры» проверяют наличие полей с данными мониторинга состояния агентов и ИИ детектора кибератак – должно быть не менее одного агента в «Статусе» «work».

Положительных результат контроля данных информационных систем говорит о выполнении требований к качественным и количественным характеристикам функционала «NGIDSN».

Выбрать информационную модель «NGSM»:

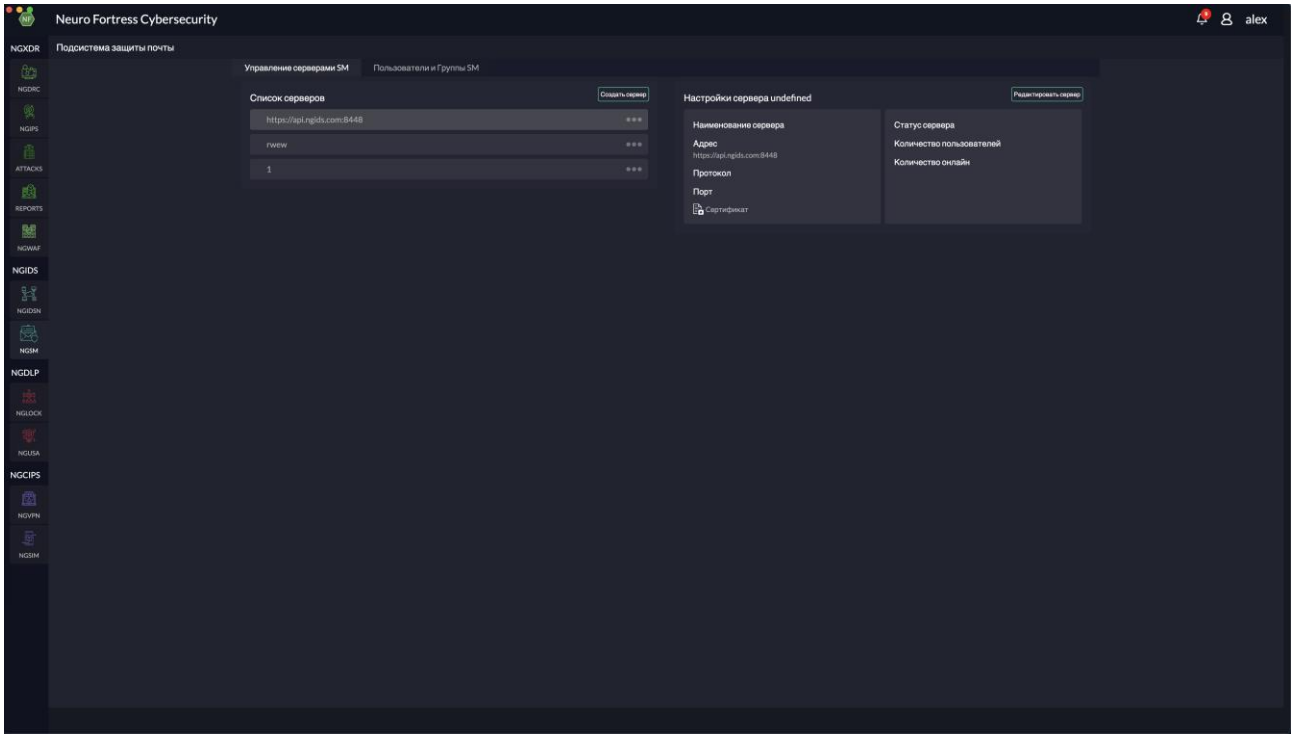

Рисунок 10 – Выбор информационной модели «NGSM»

Путем контроля информационной модели «Список серверов» проверяют наличие не менее 1 сервера почты.

Положительных результат контроля данных информационных систем говорит о выполнении требований к качественным и количественным характеристикам функционала «NGSM».

Выбрать информационную модель «NGLOCK»:

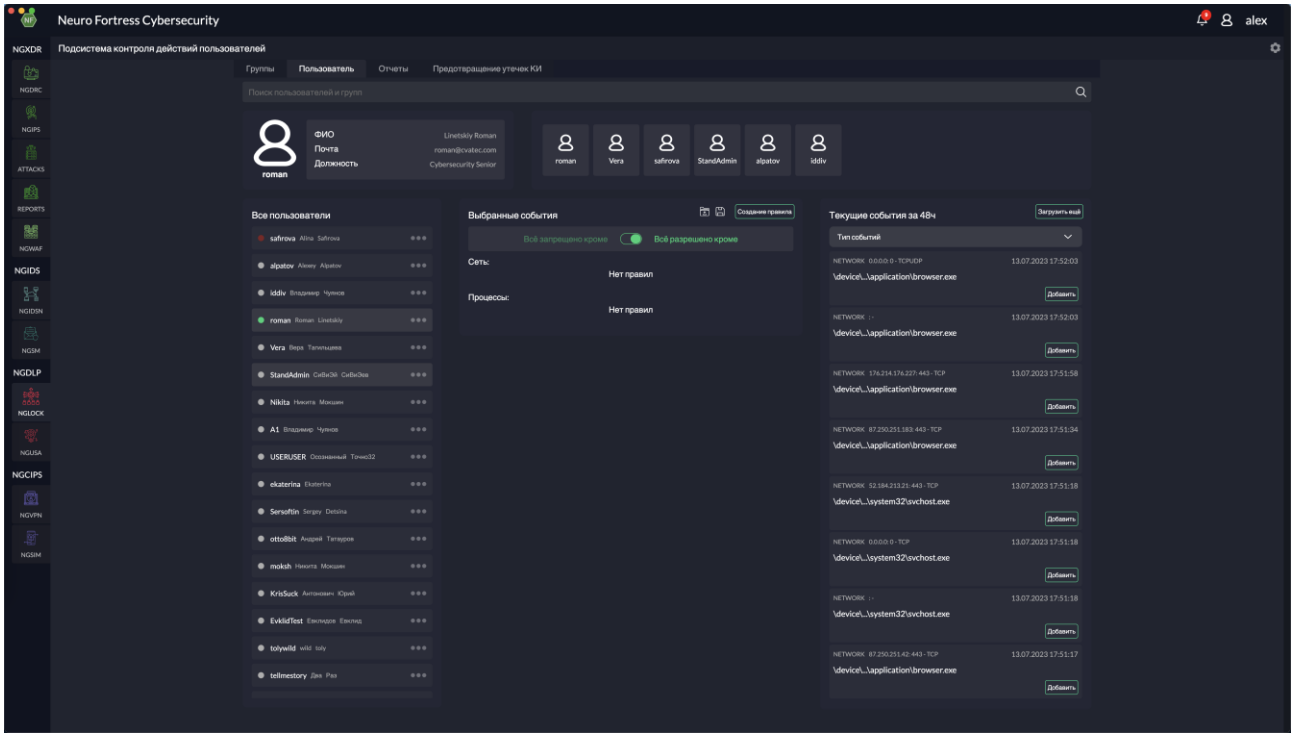

Рисунок 11 – Выбор информационной модели «NGLOCK»

Путем контроля информационной модели «Подсистема контроля действий пользователя» проверяют наличие информационных моделей «Группы» и «Пользователь» - контролируем отображение в них не менее 1 группы и не менее 1 пользователя.

Путем контроля информационной модели «Текущие события» убеждаются в наличии событий действий пользователя с датой и временем до 48 часов более 2 шт.

Положительных результат контроля данных информационных систем говорит о выполнении требований к качественным и количественным характеристикам функционала «NGLOCK».

Выбрать информационную модель «NGUSA»:

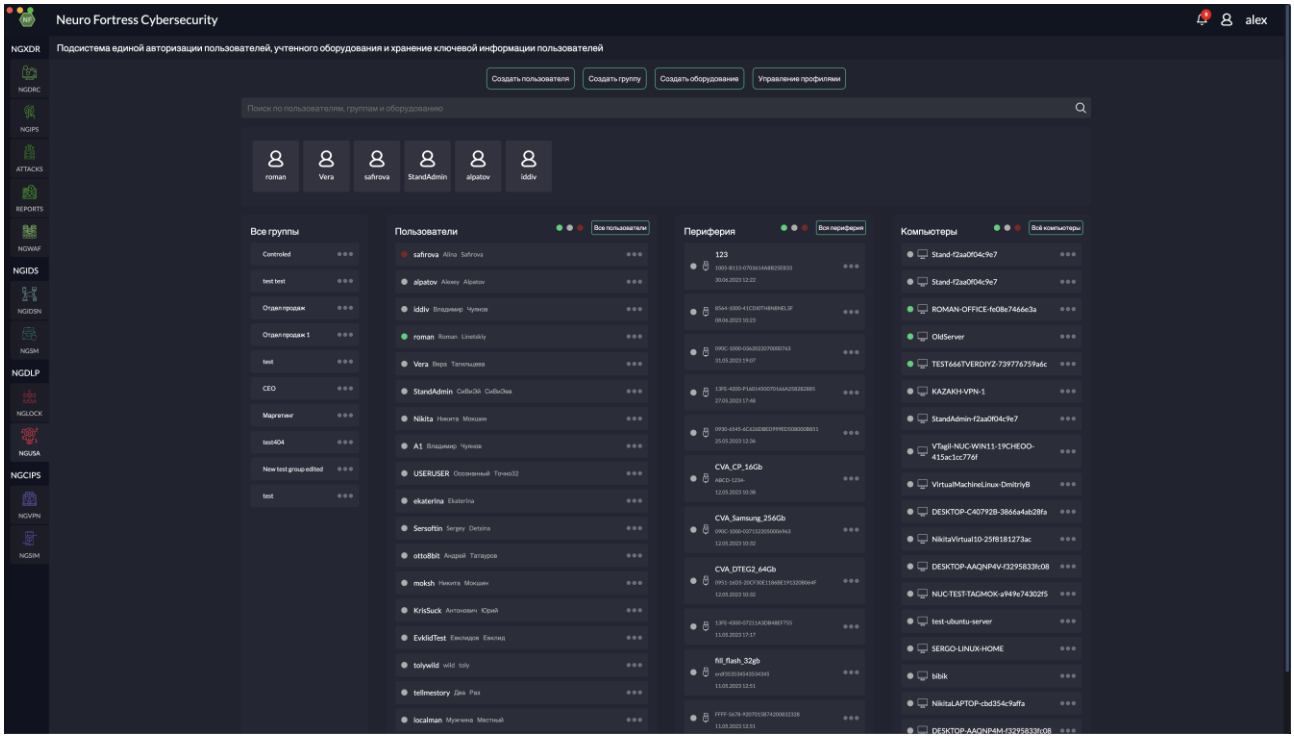

Рисунок 12 – Выбор информационной модели «NGUSA»

Путем контроля информационной модели «Подсистема единой авторизации пользователей, учтенного оборудования и хранения ключевой информации» проверяют наличие в информационной модели «Пользователи» не менее 1 пользователя.

Путем контроля информационных моделей «Периферия» и «Компьютеры» при выборе пользователя убеждаются в наличии более 2 полей с данными об учтенном оборудовании и компьютерах.

Положительных результат контроля данных информационных систем говорит о выполнении требований к качественным и количественным характеристикам функционала «NGUSA».

Выбрать информационную модель «NGVPN»:

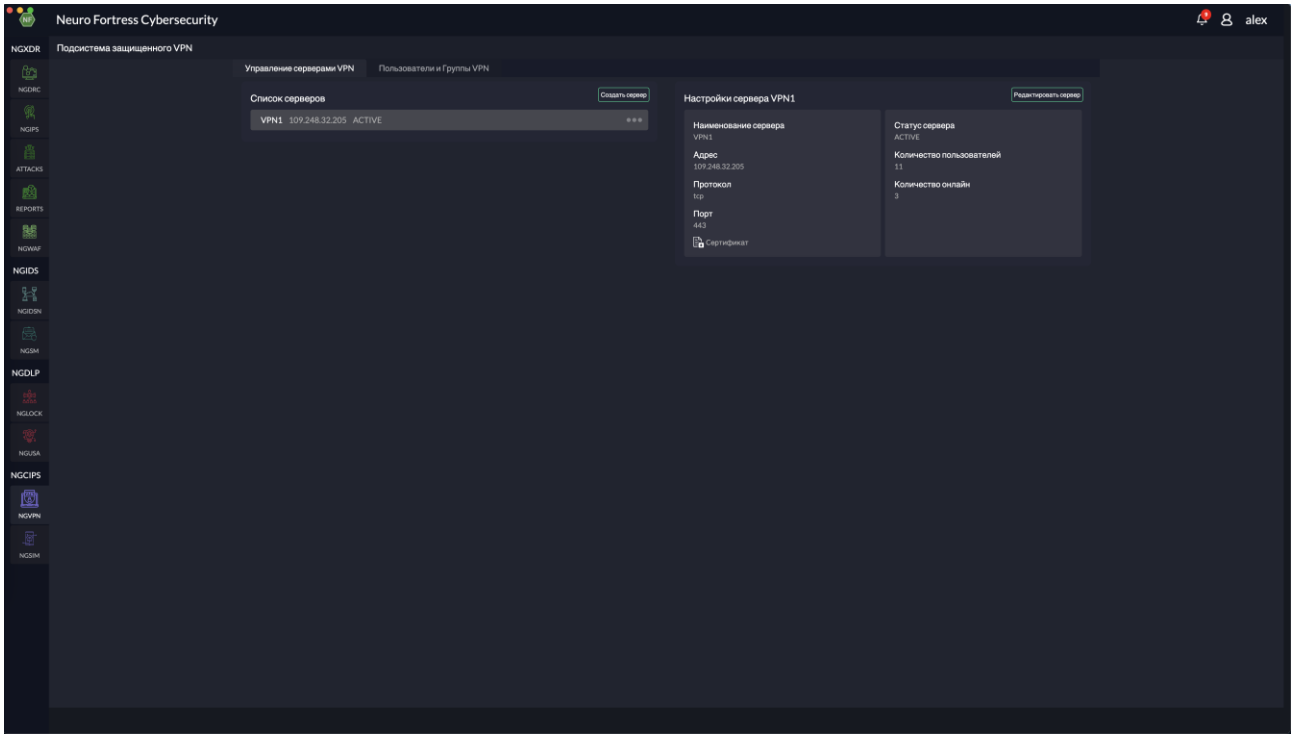

Рисунок 13 – Выбор информационной модели «NGVPN»

Путем контроля информационной модели «Подсистема защищенного VPN» проверяют наличие полей «Список серверов» и минимум 1 поля сервера.

Положительных результат контроля данных информационных систем говорит о выполнении требований к качественным и количественным характеристикам функционала «NGVPN».

4. Работа в ПО NeuroFortress

Рассмотрим кратко самые важные подсистемы кибербезопасности – которые объединяет в себе NeuroFortress XDR

На главном экране приложения XDR Neuro Fortress слева расположена вертикальная информационная модель с иконками выбора нужной подсистемы

NGXDR:

NGDRC;

В данной информационной модели представлен интерфейс подсистемы выявления киберугроз и реагирования на них. Подсистема DRC предоставляет интегральную картину атак на информационные системы, позволяет контролировать события реагирования и служит отправной точкой расследований инцидентов.

Выбор параметров мониторинга происходит относительно формализованных подсетей или контролируемых сущностей укрупненной информационной инфраструктуры.

В информационной модели «Карта сети» - отображаются взаимодействия между узлами сети, агентами конечных точек, пользователей единой системы авторизации, событий, каналов утечек, при идентификации новых или имеющихся узлов возможен контроль сервисов и протоколов, версий и возможных уязвимостей, конечные узлы идентифицируются относительно их окружения, используемой маршрутизации и информационных потоков, в том числе каналов утечек.

В информационной модели «Геокарты» инцидентов – показаны взаимодействия относительно геопривязки, характеризуемые интегральными и конформными параметрами.

В информационной модели «Карта нейросетевой идентификации» – контролируется идентификация сетевых атак и аномалий, формализация зон атак, аномалий и нормальных информационных потоков в реальном времени.

Информационная модель имеет фильтры и сортировки относительно видов атак и информационных взаимодействий.

В панели «Журнал событий» при выборе атаки в реальном времени можно выбрать вид реагирования – слежение.

NGIPS;

Подсистема предотвращения вторжений позволяет задать меры реагирования на атаки или вредоносные воздействия сетевой инфраструктуры – правила создаются на основе событий безопасности или вручную по собственным параметрам.

Информационная модель позволяет включить режим автоматического создания правил блокирования вторжения относительно событий кибербезопасности.

Подсистема включает в себя функционал «HoneyPots» предоставляющий ловушку для хакеров и систему расследования вредоносных действий.

ATTACKS;

Информационная модель Атак позволяет проводить мониторинг конкретных атак путем выбора режимов фильтрации, группировки и сортировки событий воздействий, акторов атакующих воздействий, блокировать те или иные атаки.

По каждому атакующему воздействия интеллектуальная система расследования строит граф вектора атаки и связей.

REPORTS;

Подсистема отчетов и журналов предназначена для оперативного и отложенного анализа событий кибербезопасности, информационная модель позволяет формировать практически любые выборки и аналитические отчеты по пользователям системы, атакам, векторам воздействия, источникам, типам каналов утечки, и так далее.

NGWAF.

Информационная модель веб приложений позволяет контролировать события блокировки и устанавливать исключения для сервисов, каталогов.

По событиям блокировки возможно создание постоянных правил блокирования относительно вектора атакующего воздействия – переходом в информационную модель NG IPS.

NGIDS:

NGIDSN;

Информационная модель позволяет проводить контроль состояния и жизненного цикла агентов конечных сетевых точек системы XDR NeuroFortress. Возможно выполнение операций включения и отключения модулей контроля, остановки или запуска конечных точек.

NGSM.

Подсистема почты позволяет выполнять контроль заголовков почтовых сообщений путем интеллектуальной нейросетевой оценки для предотвращения атак на подсистему почты – спам фишинг BEC атаки и тому подобные.

NGDLP:

NGLOCK;

Подсистема DLP NG LOCK объединяет мощь агентов конечных точек по контролю и блокировке информационных потоков, операций над файлами, запуском процессов на уровне ядра и драйверов операционных систем, а также политик разрешенных, контролируемых и блокируемых операций относительно групп и пользователей, система прозрачно встраивается в уже имеющуюся инфраструктуру при ее наличии – «Актив директори», «SMB сервис» или локальные учетные записи.

Осуществляется контроль запуска процессов, сетевые разрешения относительно протоколов, адресов и портов, режимы закрытого контура, режимов с отключением сетевой активности как для приложения, так и для системы, блокирование и контроль буферов обмена, интеллектуальные кейлоггеры, контроль звуковых устройств, интервальная запись, контейнеры информации.

Все данные операции выполняются на уровне ядра операционной системы, компоненты драйверов удостоверяются усиленными квалифицированными подписями, система снабжена отказоустойчивыми и резервируемыми сервисами.

Потребление ресурсов компьютера также сведено к минимуму благодаря исполнению идентификационных и блокируемых действий в нулевом кольце высокоэффективным машинным кодом.

NGUSA.

Подсистема единой авторизации пользователей позволяет полностью контролировать операции входов и выходов пользователей, гарантирует поддержку досье пользователя, блокировку пользователя одной кнопкой во всех информационных системах единовременно, сопоставление пользователю аппаратной конфигурации, контроль аппаратной конфигурации, защиту от социальной инженерии, использование учтенных носителей информации, блокирование флешек и файловых систем мобильных телефонов и переносных дисков. Система позволяет выполнять администрирование пользователей, добавление удаление пользователей. Создание групп, управление привилегиями, аппаратными мощностями, носителями информации.

NGCIPS:

NGVPN.

Подсистема защищенного ВПН является инфраструктурной подсистемой, которая объединяет гибкость централизованного подхода к частных корпоративным сетям и защищенность полностью контролируемого протокола связи между филиалами, сервисами компании, подразделениями.

В информационной модели возможно добавление ВПН серверов, учетных записей аутентификации.

Система кибербезопасности NeuroFortress объединяет в себе интеллектуальные средства идентификации воздействий на сетевую инфраструктуру (NG IDS/ NG IPS), идентификацию аномальных процессов нейросетевым контролем на конечных точках – все это не требует обновления сигнатурных баз и высокоэффективно для еще неизвестных атак и новых вредоносных систем шифраторов и майнеров. Система включает подсистему NG DLP с возможностью организации контейнеров информации, подсистема также включает интеллектуальные кейлоггер, средство записи, буфера обмена, контроль всех процессов на уровне ядра ОС. В состав NeuroFortress входит подсистема единой авторизации пользователей с возможностью задания политик и групп, контроля аппаратных средств и учтенных носителей информации, с возможностью блокирования пользователя во всех системах нажатием одной кнопки, подсистемой отчетов и журналов с умными аналитическими инструментами включая граф вектора атаки, карту нейросети, геокарту инцидентов. Подсистемы периметра кибербезопасности содержат защиту почты, ВПН сеть.

5. Техническая поддержка

Контактная информация службы технической поддержки ООО «СИВИЭЙ Технолоджиес» CVA Technologies в случае возникновения вопросов, неописанных в данном руководстве:

- Адрес электронной почты: vav@cvatec.com
- Телефон: 8-900-130-3-666.