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

ООО «Сивиэй Технолоджиес»

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ «Программный комплекс защиты и анализа информационных систем NeuroFortress»

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

На 7 листах

Ростов-на-Дону
2023

Все упомянутые в этом документе названия продуктов, логотипы, торговые маркии товарные знаки принадлежат их владельцам.

Товарные знаки «NeuroFortress», «NF», принадлежат ООО «Сивиэй Технолоджиес», «CVA Technologies».

Ни при каких обстоятельствах нельзя истолковывать любое содержимое настоящего документа как прямое или косвенное предоставление лицензии или права на использование товарных знаков, логотипов или знаков обслуживания, приведенных в нем.

Любое несанкционированное использование этих товарных знаков, логотипов или знаков обслуживания без письменного разрешения их правообладателя строго запрещено.

.

СОДЕРЖАНИЕ

1. Общая информация

Программный комплекс защиты и анализа информационных систем NeuroFortress — современное средство, базирующееся на архитектуре защиты информации от момента их рождения в инфраструктуре – следует и контролирует весь жизненный цикл, использует контейнеры данных и сквозной контроль за ними на уровне ядра операционных систем, что полностью исключает утечку в результате несанкционированных действий или вредоносного доступа.,

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.

Архитектура системы базируется на интеллектуальном обнаружении и предотвращении. Реагирование на сложные угрозы и целевые атаки проводится 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.

2. Функциональные характеристики NeuroFortress

- сбор и интеллектуальный анализ данных из множества подсистем и систем;

- обнаружение несанкционированных действий;

- сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения;

- реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти;

- мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них;

- защита информации о событиях безопасности;

- защита серверов и рабочих станций от несанкционированного доступа;

- автоматическое реагирование на атаки;

- идентификация целенаправленных и распределенных атак на сетевую инфраструктуру, сервера и персональные компьютеры пользователей;

- сбор данных для идентификации попыток похищения информации по сетевым каналам связи;

- сбор данных для расследования инцидентов сетевых вторжений, эксплойтов и попыток удаленного управления сетевой инфраструктурой;

- каталогизация и хранение событий безопасности сетевой инфраструктуры

- анализ проникновения в беспроводную инфраструктуру;

- сбор данных для расследования инцидентов в беспроводных средах и попыток удаленного управления беспроводными маршрутизаторами и терминалами;

- каталогизация и хранение событий безопасности беспроводной инфраструктуры;

- анализ почтовых отправлений на признаки спама, фрода, фишинг;

- контроль доступа устройств и портов относительно пользователей и групп пользователей;

- тревожные оповещения о инцидентах безопасности в реальном режиме времени;

- журналирование всех действий пользователей с устройствами и сетевыми протоколами по факту обращения к ним, передачи файлов и прочих данных;

- отчеты на основе данных, хранимых в базе данных, а также отчеты по текущим настройкам и по используемым на рабочих станциях устройствам, динамический граф связей для анализа коммуникаций;

- система контроля входа пользователей в систему.