Эшелон
комплексная безопасность

NTA eSensor

Интеллектуальная защита от сетевых киберугроз

NTA eSensor — система глубокого анализа сетевого трафика, которая позволяет обнаруживать сетевые угрозы, расследовать инциденты и контролировать соблюдение политик безопасности в инфраструктуре компании.

Преимущества NTA eSensor

Полная видимость сети
Контролирует трафик как на периметре, так и внутри сети — исключает «слепые зоны» и выявляет скрытую вредоносную активность, которую не видят обычные СОВ и межсетевые экраны

Экспертное обнаружение
Подключаемая экспертиза от «Перспективного мониторинга» позволяет выявлять сложные угрозы, своевременно реагировать на атаки и отсекать «шум»

Детальный контекст срабатываний
Регистрирует метаданные сетевых сессий, извлекает передаваемые файлы и сохраняет полную копию трафика (PCAP) — это позволяет восстановить картину любого события и ускорить расследование

Технические возможности

- глубокий анализ трафика (DPI): разбор протоколов до уровня L7 включительно, обработка VLAN, VXLAN, GRE, IP-in-IP и фрагментированного трафика, поддержка стека IPv4/IPv6;
- комплексное обнаружение атак: использование сигнатурного анализа (поддержка правил с синтаксисом Suricata), выявление индикаторов компрометации (IP-адреса, домены, URL, хэши файлов) и эвристический анализ для фиксации аномалий по пороговым значениям;
- гибкая масштабируемая архитектура: разделение на независимые сенсоры (сбор трафика через SPAN/TAP) и центральный сервер управления. Легкое подключение новых сенсоров при расширении сети;
- управление и автообновление правил: создание, редактирование и тонкая настройка пользовательских сигнатур, а также автоматическая загрузка и актуализация баз из фидов ET Open, TI-портала AM TIP («Перспективный мониторинг») и собственных серверов;
- развертывание и поддержка отечественной ОС: полноценное функционирование на базе сертифицированной ОС Astra Linux SE 1.8 и стандартном дистрибутиве Debian 12. Развертывание доступно как на физических серверах (Bare Metal), так и в средах виртуализации.

Функциональные возможности

- **Обнаружение и регистрация атак**
- **Регистрация сетевых взаимодействий**
- **Извлечение файлов, передаваемых по сети**
- **Запись и хранение полной копии трафика**
- **Централизованное управление сенсорами**
- **Дашборды и фильтры для анализа данных**
- **Блокировка угроз через NGFW «Рубикон Nova»**
- **Отправка событий в SIEM-системы**
- **Регистрация метаданных прикладных протоколов (HTTP, DNS +8) и TLS**
- **Обнаружение учётных данных в HTTP, FTP, NTLM, RDP, Kerberos**

Сертификаты и лицензии

Сертификация

Сертификат ФСТЭК России ожидается в I–II кв. 2027 г.

Входит в реестр российских программ для электронных вычислительных машин и баз данных (Реестр российского ПО)

Больше информации о NTA eSensor

npo-echelon.ru/esensor

NTA eSensor в Telegram

t.me/eSensorNTA

Запросите демонстрацию решения:

- 107023, г. Москва, ул. Электрозаводская, д. 24
- +7 (495) 223-23-92
- npo-echelon.ru
- sales@npo-echelon.ru