imperva
a Thales company

SOFTPROM

IMPERVA – ПРОДУКТОВЫЙ ПОРТФЕЛЬ КОРОТКО

Imperva — компания, занимающаяся программным обеспечением и услугами в области кибербезопасности, которая обеспечивает защиту корпоративных данных и приложений. Штаб-квартира компании находится в Сан-Матео, Калифорния. Imperva, по сути, работает в трех областях: безопасность данных, безопасность приложений и пограничная/сетевая безопасность, также имеется отдел профессиональных услуг. Миссия компании: «Защита данных и всех путей к ним».

Data Security:

В области безопасности данных речь идет о решениях, которые позволяют компаниям защитить свои данные. Одной из двух основных мотивирующих причин проектов по обеспечению безопасности данных является обеспечение соблюдения компанией нормативно-правовых актов. Вторая причина — повысить безопасность данных организации путем их непрерывного мониторинга и обнаружения аномалий.

Основные варианты использования:

- Классификация данных. Определение того, где хранятся данные и их актуальность. Классификационные работы внутри БД и других репозиториях, например, в файлах.

- Мониторинг активности данных (DAM). Проведите полный аудит доступа к любым данным, чтобы гарантировать соответствие нормативным требованиям и способность расследовать предполагаемые утечки данных.

- Управление правами пользователей. Применение принципа наименьших привилегий в отношении доступа к данным. Обеспечение того, чтобы у каждого был минимальный набор разрешений на доступ к ценным данным.

- Расширенная аналитика, изучающая использование данных в организации следующим образом:

    - Поведенческий анализ доступа к данным, то есть изучение обычного поведения пользователя и обнаружение аномалий на основе дефолтных и кастомных моделей.
    - Анализ на основе шаблонов, который представляет собой анализ использования данных в сравнении с данными, предоставленными поставщиком сигнатур, и обнаружение вредоносного поведения.
    - Анализ на основе пользовательских правил, то есть возможность применять собственные определения нежелательного поведения и генерировать инциденты, если таковые наблюдаются.

- Соответствие нормативным требованиям. В частности: GDPR, PCI DSS, HIPPA и т. д. Регулируемая обработка данных, как PII, которая требует контроля доступа к данным.

- Маскирование данных – безопасное использование продакшн данных в средах разработки без риска обработки исходных ценных данных в незащищенных средах.

- Реагирование на инциденты – поддержка реагирования на инциденты с данными посредством автоматизации и интеграции с другими системами безопасности (Runbooks, SOAR).

- Поддержка автоматизированных процессов, включая поддержку доступа к запросам субъектов данных в рамках данных, обрабатываемых организацией.

Ключевые особенности решения:

- Интеграция с базами данных с использованием агента или без агента (например, нативный аудит).
- Поддержка баз данных как в локальном дата-центре, так и в облаке (PaaS и IaaS).
- Поддержка данных как в базах данных, так и в файлах (неструктурированные данные).
- Решение доступно в виде оборудования, виртуальных машин и облачного сервиса.

Application Security:

Область безопасность приложений посвящена защите веб-приложений на различных уровнях. Главной и наиболее популярной функцией является WAF (брандмауэр веб-приложений), который представлен в виде услуги из облака, а также программное/аппаратное обеспечение, которое клиенты могут установить в свою инфраструктуру. Предложение дополняется RASP (Runtime Application Self-Protection), который обеспечивает защиту посредством прямой интеграции с веб-приложением.

Основные варианты использования:

- Защита веб-приложения от известных и неизвестных атак, которые обычно используются в контексте веб-приложений.

- Защита приложений от DoS и DDoS-атак на уровне приложений, целью которых является перегрузить сервер приложений.

- Content Delivery Network (CDN). Ускоряет производительность приложений за счет оптимизации контента сайта и кэширование контента в точках доступа по всему миру.

- Управление трафиком, генерируемым ботами (хорошими или плохими), в частности, предотвращение:
  - Веб-скрапинга — автоматическое считывание содержимого страницы, например, цен, продуктов и т.д.
  - Спама – размещения значительного количества бесполезных данных.
  - Кардинга и взлома карт – различные злоупотребления, связанные с кредитными картами.
  - Перегрузки сервера и отсутствия контроля за поведением клиентов.

- Защита идентификаторов клиентов компании, обнаружение и нейтрализация атак, направленных на захват учетных записей клиентов (Account Takeover attacks).

- Защита и контроль среды браузера, управление кодом, исполняемым на стороне браузера и снижение риска перехвата данных на стороне браузера (например, атак Magecert).

- Защита API от злоупотреблений, в частности:
  - API Discovery — сканирование (самообучающееся) API.
  - Обеспечение защиты посредством применения позитивной модели безопасности.
  - Сканирование самих интерфейсов на предмет выявления их слабых мест.
  - Видимость конфиденциальных данных, предоставляемых API.

Ключевые особенности решения:

- Защита приложений доступна на всех уровнях: в облаке, локально и на уровне приложения.
- Возможность применения позитивной и негативной модели безопасности.
- Для облачного сервиса сеть из более чем 60 точек доступа распространена по всему миру.
- Динамическое использование репутационной информации, собранной Imperva.
- Гибкое лицензирование всех компонентов.
- Решение, созданное с учетом низкой совокупной стоимости владения.
- Команда SOC работает 24/7/365.

imperva
a Thales company

SOFTPROM

Edge/Network Security:

Область Edge/Network Security сосредоточена вокруг проблемы DDoS-атак. Атаки могут осуществляться на разных сетевых уровнях и на разных протоколах приложений. Imperva предлагает четыре основных продукта в своем портфолио, которые защищают целые центры обработки данных (сетевая защита от DDoS), отдельные серверы (отдельная IP-защита от DDoS), веб-приложения (защита веб-приложений от DDoS) и DNS-серверы (DNS DDoS-защита).

Основные варианты использования:

- Защита сетей от DDoS-атак. Это объемные атаки, часто распределенные, направленные на перегрузку сетевой инфраструктуры и, как следствие, блокировку доступа к серверам приложений.

- Защита веб-приложений от DDoS-атак. Имеются в виду атаки на приложения, которые стремятся перегрузить сам сервер приложений, отправив чрезмерное количество запросов к приложениям. Последствием успешной такой атаки является блокировка доступа к серверам приложений.

Ключевые особенности решения:

- Сеть из более чем 60 центров очистки траффика разбросана по всему миру (https://www.imperva.com/products/global-network-map/).
- 3-секундный SLA для нейтрализации атаки.

- SLA соглашение об уровне обслуживания для 100% доступности сервисов при правильной настройке услуги.
- Команда SOC работает 24/7/365.

SOFTPROM — IT ДИСТРИБЬЮТОР С ДОБАВЛЕННОЙ ЦЕННОСТЬЮ

Софтпром — ведущий ИТ-дистрибьютор на рынках СНГ и Восточной Европы, которому доверяют более 1200 партнеров. Компания была основана в 1999 году и сегодня представлена более чем в 30 странах мира.

НАША МИССИЯ

Повышение эффективности работы клиентов за счет предоставления высококачественных ИТ-решений и услуг.