Корпоративные коммуникационные сети часто подвергаются атакам с использованием сложных и ранее неизвестных вредоносных программ или внутренних угроз, что делает необходимыми передовые защитные механизмы, такие как системы обнаружения вторжений на основе аномалий, для обнаружения, оповещения и реагирования на инциденты безопасности. Стратегии как на основе сигнатур, так и для обнаружения аномалий основаны на функциях, извлеченных из сетевого трафика, для чего необходимы безопасные и расширяемые стратегии сбора, использующие современные многоядерные архитектуры. Доступные решения написаны на низкоуровневых языках системного программирования, которые требуют ручного управления памятью и страдают от частых уязвимостей, которые позволяют удаленному злоумышленнику отключить или скомпрометировать монитор сети. Другие не были разработаны с целью исследования и нехватки с точки зрения гибкости и доступности данных. Чтобы решить эти проблемы и облегчить будущие эксперименты с методами обнаружения на основе аномалий, будет представлена ​​исследовательская структура для сбора функций трафика, реализованных на языке, безопасном для памяти. Он обеспечивает доступ к сетевому трафику в виде структурированных данных безопасного типа, для определенных протоколов или пользовательских абстракций, путем создания записей аудита в нейтральном формате платформы. Чтобы уменьшить объем памяти, вывод сжимается по умолчанию. Подход полностью реализован на языке программирования Go, имеет параллельный дизайн, легко расширяется и может использоваться для захвата в реальном времени с сетевого интерфейса или с дамп-файлами PCAP и PCAPNG. Кроме того, платформа предлагает функциональные возможности для создания маркированных наборов данных, ориентированных на приложения в контролируемом машинном обучении. Для демонстрации разработанного инструментария проводится серия экспериментов по классификации вредоносного поведения в наборе данных CIC-IDS-2017 с использованием Tensorflow и Deep Neural Network.