Программное обеспечение «Система анализа и контроля DNS-запросов [SL] DNS версии 1»

Программное обеспечение представляет собой специализированную систему для мониторинга, анализа и фильтрации DNS-трафика, предназначенную для обеспечения проактивной защиты корпоративной сети от киберугроз на уровне разрешения доменных имён.

Система осуществляет полный перехват и глубокий анализ всех поступающих DNS-запросов в реальном времени, что позволяет выявлять признаки вредоносной активности до момента установления сетевого соединения с потенциально опасными ресурсами.

Анализ трафика направлен на обнаружение обращений к доменам, ассоциированным с ботнетами, фишинговыми платформами, командно-контрольными серверами (C&C), эксплоит-китами и другими категориями киберугроз, актуальность которых поддерживается за счёт постоянной синхронизации с внешними репутационными базами данных и внутренними источниками угроз.

Динамическая категоризация доменных имён выполняется на основе комбинации сигнатурного анализа, репутационных оценок и поведенческих алгоритмов машинного обучения, что обеспечивает своевременное выявление как известных, так и ранее не встречавшихся угроз.

Система реализует превентивную блокировку доступа к опасным ресурсам на стадии DNS-запроса, предотвращая тем самым загрузку вредоносного контента и минимизируя поверхность атаки.

Для обнаружения сложных и скрытых угроз программное обеспечение включает механизмы выявления аномалий в паттернах DNS-активности, включая признаки туннелирования данных через DNS, использование доменных имён, генерируемых алгоритмически (DGA), аномально высокую частоту запросов к несуществующим доменам, а также другие техники, применяемые злоумышленниками для обхода традиционных средств защиты.

Все события, связанные с обработкой DNS-запросов, фиксируются в детализированных журналах с указанием временной метки, исходного IP-адреса, запрашиваемого домена, типа записи, статуса ответа, категории домена и принятого действия (разрешено, заблокировано, перенаправлено). Сформированные журналы служат основой для проведения аудита,

расследования инцидентов информационной безопасности и восстановления цепочки атаки.

Дополнительно система предоставляет средства визуализации на основе веб-интерфейса, позволяющие отслеживать динамику угроз, анализировать тенденции DNS-активности в разрезе пользователей и подразделений, а также оперативно реагировать на выявленные инциденты посредством гибких правил реагирования и интеграции с системами управления инцидентами безопасности.