Аракчеев Егор Алексеевич
студент, Факультет «Информатика и системы управления»
Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет), г. Москва
Горелова Ксения Игоревна
студент, Факультет «Информатика и системы управления»
Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет), г. Москва

СРАВНЕНИЕ OPEN SOURCE SIEM WAZUH И ALIENVAULT OSSIM

Аннотация. Цель работы — сравнительный анализ архитектуры и функциональных возможностей открытых SIEM-систем Wazuh и AlienVault OSSIM, а также оценка их применимости для мониторинга и реагирования на инциденты информационной безопасности в организациях разного масштаба. Обе платформы относятся к классу open source SIEM, но отличаются подходом к масштабируемости, интеграциям и уровню автоматизации процессов безопасности.

Ключевые слова: SIEM, Wazuh, AlienVault OSSIM, инциденты ИБ, журналирование, открытое ПО, корреляция событий.

Введение

Рост количества источников событий (облака, контейнеры, мобильные и IoT-устройства) делает централизованный сбор и корреляцию журналов критически важной задачей для служб информационной безопасности. Коммерческие SIEM-решения остаются дорогостоящими и часто избыточными для малого и среднего бизнеса, поэтому интерес к open source SIEM, таким как Wazuh и AlienVault OSSIM, стабильно высок.

Wazuh позиционируется как унифицированная платформа XDR и SIEM с акцентом на интеграцию с облачными средами и расширенные возможности мониторинга конечных точек. AlienVault OSSIM, в свою очередь, является

открытой редакцией коммерческого продукта AT&T USM и сочетает базовые функции SIEM с набором встроенных средств обнаружения атак.

Общая концепция и цели Wazuh и OSSIM

Wazuh ориентирован на построение масштабируемой платформы для мониторинга безопасности, соответствия требованиям и реагирования на инциденты, объединяя сбор логов, управление уязвимостями, контроль целостности и функции EDR. Ключевая задача Wazuh — предоставить гибкую, расширяемую и хорошо документированную экосистему, которая легко встраивается в существующую инфраструктуру и стек наблюдаемости (в том числе ELK).

AlienVault OSSIM преследует цель предоставить «всё-в-одном» решение для корреляции событий, расчёта риска и базового управления инцидентами на основе интеграции множества открытых средств, таких как Snort, OSSEC, Nagios и др. Проект фокусируется на упрощении развёртывания и предоставлении единичного окна для наблюдения за сетью, включая инвентаризацию активов и базовые средства оценки уязвимостей.

Архитектура и ключевые компоненты

Wazuh реализован как распределённая платформа с агентами на конечных точках, центральным сервером и бекендом, основанным на стеке Elasticsearch/OpenSearch и Kibana/Opensearch Dashboards для хранения и визуализации событий. Агенты Wazuh собирают журналы, данные об уязвимостях, сведения о целостности файлов и системной конфигурации, передавая их на сервер для корреляции и генерации оповещений в режиме, близком к реальному времени.

OSSIM строится вокруг центрального сервера, хранилища событий (SQL-база данных и логгер) и одного или нескольких сенсоров, отвечающих за сбор и нормализацию событий из сетевых и хостовых источников. Типичная инсталляция по профилю «all-in-one» сочетает в одном узле сенсор, сервер, фреймворк (веб-интерфейс) и базу данных, что упрощает пилотное

развёртывание, но ограничивает масштабируемость без дальнейшей сегментации ролей.

Функциональные возможности и сценарии применения

Основные функциональные блоки Wazuh включают: корреляцию событий и генерацию оповещений, управление уязвимостями, контроль целостности файлов, оценку конфигураций (SCA), средства соответствия стандартам (PCI-DSS, HIPAA, GDPR и др.), а также поддержку контейнерной и облачной безопасности. Благодаря агентской модели и широким интеграциям Wazuh подходит для гибридных и облачных инфраструктур, а также для организаций, которым критична детализация данных с конечных точек и возможность расширенной автоматизации.

Функциональность OSSIM фокусируется на корреляции событий, расчёте риска инцидентов с учётом ценности актива, приоритета и надёжности события, а также на использовании встроенных IDS/IPS, сканеров уязвимостей и средств мониторинга. OSSIM удобно применять в средах с преобладанием традиционной сетевой инфраструктуры, где важны интеграция с SNORT, syslog-источниками и наличие базовой панели управления активами и уязвимостями «из коробки».

Сравнение Wazuh и AlienVault OSSIM

Ниже приведена таблица, отражающая ключевые различия между Wazuh и AlienVault OSSIM.

Критерий	Wazuh	AlienVault OSSIM
Лицензия и стоимость	Открытое ПО, свободно распространяется; коммерческие услуги — опционально.	Открытое ПО как часть линейки AT&T, базовый функционал бесплатен.
Архитектура	Агентская модель, распределённый бекенд на Elasticsearch/OpenSearch.	Сервер, сенсоры, логгер и база данных, возможен профиль

Критерий	Wazuh	AlienVault OSSIM
Основной фокус	XDR + SIEM, глубинный мониторинг конечных точек и облаков.	Классический SIEM с акцентом на корреляцию и расчёт риска.
Интеграции и расширяемость	Широкий набор интеграций (облака, контейнеры, внешние TI, SIEM/ELK).	Встроенная интеграция с набором open source средств (Snort, OSSEC и др.).
Масштабируемость	Хорошо масштабируется за счёт горизонтального расширения кластера.	Масштабируемость возможна через разнесение ролей, но сложнее в больших инсталляциях.
Простота развёртывания	Настройка более сложна, требует планирования архитектуры и интеграций.	Относительно простая базовая установка, особенно all-in-one профиль.
Сообщество и поддержка	Активное сообщество, подробная документация, коммерческая поддержка партнёров.	Поддержка сообщества, документация; коммерческая поддержка — через продукты AT&T.
Типовые сценарии	Гибридные/облачные среды, DevSecOps, соответствие регуляторике.	Классические сети малого и среднего бизнеса, лабораторные стенды.

Преимущества, ограничения

К преимуществам Wazuh относят современную архитектуру, сильный акцент на мониторинге конечных точек, контейнерной и облачной безопасности, а также

развитую экосистему интеграций, что делает платформу привлекательной для организаций с гибридной инфраструктурой. Вместе с тем отмечаются повышенная сложность первоначальной настройки и необходимость наличия компетенций по работе со стеком Elasticsearch и системами автоматизации.

AlienVault OSSIM выигрывает за счёт сравнительно простой начальной установки, наличия набора уже встроенных средств обнаружения и привычной модели работы классического SIEM. Ограничениями выступают менее гибкая масштабируемость, зависимость от устоявшегося набора интегрированных инструментов и смещение акцента в сторону традиционной сетевой инфраструктуры, что делает OSSIM менее удобным в облачно-ориентированных сценариях.

С учётом отмеченных факторов Wazuh чаще выбирают для масштабируемых и сложных сред, где требуется высокая степень интеграции и автоматизации, тогда как AlienVault OSSIM остаётся актуальным вариантом для небольших инсталляций и учебно-лабораторных стендов, где важны простота запуска и наличие готового набора средств обнаружения.

Заключение

Wazuh и AlienVault OSSIM представляют собой две зрелые open source SIEM-платформы, каждая из которых ориентирована на разные сценарии применения в задачах мониторинга и реагирования на инциденты информационной безопасности. Wazuh выделяется современной агентской архитектурой, расширенными возможностями XDR, поддержкой облачных и контейнерных сред, что делает её предпочтительным выбором для масштабируемых гибридных инфраструктур. AlienVault OSSIM предлагает удобное «всё-в-одном» решение с встроенными инструментами обнаружения, подходящее для небольших сетей и лабораторных стендов, где важны простота развёртывания и базовая корреляция событий.statia-OP.

При наличии компетенций по администрированию Linux, контейнеризации и стека Elasticsearch Wazuh может стать эффективной основой для комплексной системы защиты, обеспечивая высокий уровень кастомизации и интеграций.

OSSIM, в свою очередь, рекомендуется для начальных внедрений или сред с ограниченными ресурсами, где требуется быстрая настройка без глубокого погружения в архитектуру.

Выбор между ними зависит от масштаба инфраструктуры, уровня автоматизации и приоритетов организации: Wazuh для роста и гибкости, OSSIM для оперативного старта.

СПИСОК ЛИТЕРАТУРЫ

Wazuh. Официальный сайт. URL: https://wazuh.com/ (дата обращения: 12.01.2026).

Security Information and Event Management (SIEM). Real-time threat detection. URL: https://wazuh.com/platform/siem/ (дата обращения: 12.01.2026).wazuh

Wazuh Documentation. Getting started. URL: https://documentation.wazuh.com/current/getting-started/index.html (дата обращения: 12.01.2026).

Wazuh GitHub Repository. URL: https://github.com/wazuh/wazuh (дата обращения: 12.01.2026).

AlienVault OSSIM Review - Open Source SIEM. URL: https://www.infosecinstitute.com/resources/network-security-101/alienvault-ossim-review-open-source-siem/ (дата обращения: 12.01.2026).

AlienVault OSSIM vs Wazuh. URL: https://www.peerspot.com/products/comparisons/alienvault-ossim_vs_wazuh (дата обращения: 12.01.2026).

Top 13 Open Source SIEM Tools in 2026. URL: https://aimultiple.com/open-source-siem (дата обращения: 12.01.2026).

What are the best free and open-source SIEM tools in 2026? URL: https://www.webasha.com/blog/what-are-the-best-free-and-open-source-siem-tools (дата обращения: 12.01.2026).

AlienVault OSSIM: SIEM Product overview. URL: https://www.techtarget.com/searchsecurity/feature/AlienVault-OSSIM-SIEM-Product-overview (дата обращения: 12.01.2026).