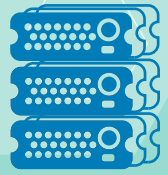
Любое количество сканируемых серверов от одного до сотен тысяч



Высокая периодичность проверок: благодаря горизонтальной масштабируемости системы

Предусмотрена возможность взаимодействия между экспертами по выявленным проблемам с целью их оперативного решения

Легко интегрируется с любыми развёрнутыми у пользователя системами мониторинга

Имеет непрерывный и независимый от работы одного сервера-сканера процесс мониторинга

Возможность эскалации событий в системах мониторинга функционального состояния ИС

Гибко реагирует на ложные срабатывания для исключения "лавины" алертов по уже проверенным событиям

COMPLAUD позволяет:

Поиск уязвимостей в программном обеспечении

Проверка на соответствие конфигурации требованиям безопасности

Кастомизация функционала проверок (исходя из потребностей клиентов) и их реализация на базе существующей платформы

Инвентаризация программного обеспечения

Аудит

Поиск уязвимостей в ПО

Compliance

Соответствие параметрам безопасной конфигурации ПО

Inventory

Информация по установленному ПО на проверяемых серверах за указанный временной срез, списку серверов с указанным ПО, изменениям состояния ПО, аналогично режимам Audit и Compliance

Управление false positives

Согласование с security officer исключения из результатов мониторинга уязвимости, определённой как ложная

Отслеживание изменений

Ticketing

Контакты

Адрес:
127018, Россия, город Москва
улица Полковая, дом 3
Телефоны:
+7 (495) 009 87 87
+7 (800) 302 87 87
Email: info@rcntec.com

rcntec.com/complaud

COMPLAUD

Эластичная распределённая система мониторинга состояния безопасности и аудита соответствия стандартам и настройкам ИТ-инфраструктуры

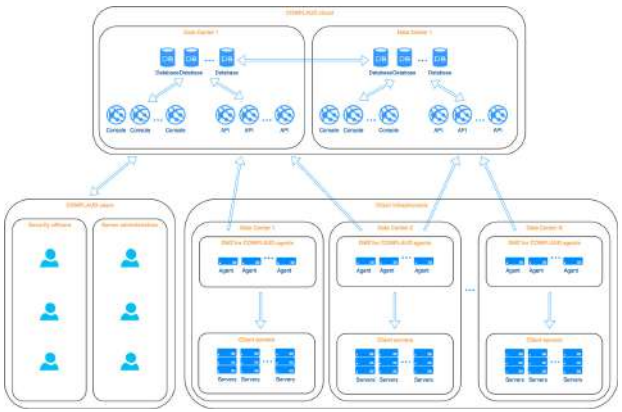
RCNTEC
Resilient Cloud and Network TEChnologies

COMPLAUD - мониторинг информационной безопасности и аудит соответствия стандартам и настройкам

COMPLAUD – это:

- Realtime информация по compliance и уязвимостям всей инфраструктуры
- Уверенность в прохождении аудитов
- Избавление от человеческого фактора при обеспечении информационной безопасности
- Единая консоль для ИТ и ИБ
- Непрерывный аудит установленного ПО

СХЕМА ОБЛАЧНОЙ ВЕРСИИ



НЕКОТОРЫЕ ТЕХНИЧЕСКИЕ ДЕТАЛИ РЕАЛИЗАЦИИ COMPLAUD

Горизонтальная масштабируемость и отказоустойчивость *

Доступный и документированный API позволяет автоматизировать процесс работы с интерфейсом системы

Открытый программный код агента и плагинов обеспечивает прозрачный и контролируемый для клиентов процесс аудита их серверов

Использование протокола HTTPS для взаимодействия агента с API позволяет кастомизировать код агента под конкретную инфраструктуру или клиента

Эскалация событий, генерируемых системой, через syslog и в корпоративный мессенджер Slack позволяет обеспечить мгновенную реакцию администраторов информационных систем на выявленные уязвимости или несоответствия требованиям

Интеграция с поисковым движком Elasticsearch обеспечивает хранение и поиск информации по всем выявленным уязвимостям или несоответствиям требованиям, а также логам действия пользователей системы

Кастомизация плагинов Compliance из web-интерфейса системы позволяет гибко изменять проверяемые на сканируемых хостах параметры

Управление доступом на основе ролей позволяет организовать взаимодействие между сотрудниками служб информационной безопасности и администраторами информационных систем с помощью функционала Ticketing

ГОРИЗОНТАЛЬНАЯ МАСШТАБИРУЕМОСТЬ И ОТКАЗОУСТОЙЧИВОСТЬ ОБЕСПЕЧИВАЕТСЯ ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИЙ И РЕШЕНИЙ:

Децентрализованная noSQL СУБД Cassandra обеспечивает линейную масштабируемость и репликацию между любым количеством нод кластеров, размещаемых в нескольких дата-центрах

DNS round-robin позволяет балансировать нагрузку между идентичными узлами API, обрабатывающими данные, отправляемые агентами

Ассинхронный web-сервер Nginx обрабатывает запросы агентов к API, количество которых также может увеличиваться практически без ограничений

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

Поиск уязвимостей (Audit) на основе более, чем 14 тысяч вендорных публикаций безопасности (Red Hat Enterprise Linux, CentOS, Ubuntu, Suse Linux Enterprise Server)

Проверки на соответствие требованиям безопасной конфигурации (Compliance) устройств (Linux, MS Windows)

Инвентаризация ПО

БЕЗОПАСНОСТЬ

Взаимодействие пользователей и агентов с интерфейсами системы осуществляется по протоколу HTTPS, обеспечивающему шифрование

Конфиденциальные пользовательские данные, сохраняемые в системе, шифруются алгоритмом AES с длиной ключа 256 бит

Интеграция со службой каталогов MS Active Directory по протоколу LDAP обеспечивает стандартизированный в корпоративных средах подход к процедурам аутентификации и авторизации