Release notes KOMRAD ENTERPRISE SIEM 4.5

KOMRAD Enterprise SIEM позволяет осуществлять централизованный сбор событий ИБ, выявлять инциденты ИБ и оперативно на них реагировать.

KOMRAD предназначен для работы в значимых объектах критической информационной инфраструктуры 1 категории, в государственных информационных системах 1 класса защищенности, в автоматизированных системах управления производственными и технологическими процессами 1 класса защищенности, в информационных системах персональных данных при необходимости обеспечения 1 уровня защищенности персональных данных, в информационных системах общего пользования 2 класса.

KOMRAD проводит сбор и регистрацию информации о событиях информационной безопасности, позволяет осуществлять мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них, выявляет потенциальные инциденты информационной безопасности в соответствии с заданными критериями фильтрации и корреляции событий, оповещает о выявлении потенциальных инцидентов информационной безопасности, формирует отчеты об инцидентах информационной безопасности.

KOMRAD поддерживает такие протоколы и механизмы сбора событий, как syslog, WMI, SQL, SNMP, xFlow, SFTP, локальная машина, HTTP, а также поддерживает формат событий информационной безопасности CEF (Common Event Format).

Что нового в версии 4.5

1) Пересмотрен подход к поиску по событиям, теперь KOMRAD позволяет проводить поиск по событиям с использованием «выражений поиска».
2) Добавлен новый механизм сбора событий с помощью eBPF коллектора, благодаря которому стал возможным сбор информации о событиях информационной безопасности, связанных с функционированием ядра Linux, сетевого взаимодействия и многого другого.
3) Добавлены новые плагины, а также функция эвристического анализа для них:

    a) eBPF parsing – плагин нормализации событий eBPF коллектора;

б) eBPF policies – набор политик сбора событий eBPF коллектора;

в) http-scraping – плагин активного сбора HTTP-событий;

г) sigma – проверяет соответствие события правилам Sigma;

д) Zeek JSON – нормализация событий логов Zeek в формате json;

е) ecs – нормализация событий ecs к внутренним событиям Komrad;

ж) evtx – XML события Windows event log;

з) агент Auditd – устанавливает подписку в ядре Linux для получения событий аудита по мере их возникновения, что позволяет реагировать быстрее);

и) syslog – позволяет извлекать и приводить к модели события Elastic Common Schema ECS события syslog в различных форматах, подобно коллектору syslog;

к) rename – переименовывает поля;

л) split – разбиение события на многие;

м) http-routes – добавление произвольных API в HTTP коллектор – имитация.

4) Добавлено семейство плагинов if, deny, assign использующие условия в виде регулярного выражения RE2, выражения grok, выражения на языке CEL (Common Expression Language)

а) deny – позволяет как не пропускать события подходящие под условия

б) if – позволяет создавать ветвление в правилах нормализации и обрабатывать нижеследующими правилами нормализации только событиями подходящими под условие if в виде regex RE2, grok или CEL

в) assign – позволяет выполнять произвольные трансформации над текстовыми полями, полями в виде JSON строк, множественными конкатенациями и обработками строк и массивов среди нескольких полей одного события, операции извлечения и трансформации поля события содержащего XML, поддержку XSD схем для XML в поле события

5) Добавлена имитация Elasticsearch API коллектором HTTP, которая позволяет за 1 минуту перевести сбор событий из Elastic в KOMRAD без перенастройки инфраструктуры и продолжать собирать логи средствами logstash, vector, beats, пока осуществляется переход на коллекторы KOMRAD.
6) KOMRAD теперь устанавливается на RedOS версии 8 и AltLinux версии 10, а также Astra Linux Special Edition 1.8.
7) Работать с пакетами экспертиз стало гораздо проще благодаря добавлению специального модуля управления ими.
8) Производительность подсистемы сбора событий увеличена в 2 раза за счёт оптимизаций кода, а скорость обработки событий на высоких EPS увеличена в десятки тысяч раз за счет улучшения алгоритма обработки и корреляции событий.
9) Осуществлен перенос функционала фильтрации событий на коллекторы, что позволяет балансировать нагрузку при горизонтальном масштабировании.
10) Добавлена возможность автоматической установки коллекторов на удаленных хостах.
11) Проработана возможность настройки иерархичной системы из нескольких работающих совместно систем, а также добавлены «внешние инциденты», т.е. подчиненный KOMRAD имеет возможность отправлять инциденты и принимать изменения, связанные с ними, при взаимодействии с вышестоящим.
12) Добавлена агрегация уведомлений, а также агрегация в корреляции. Агрегация в корелляции возможна в нескольких режимах - агрегация нескольких инцидентов в один, агрегация во временных окнах по ключам событий с возможностью схлопывания событий во временном окне в одно и расчётом минимальных, максимальных, средних, уникальных, первых либо последних значений каждого поля в событиях окна
13) Инциденты теперь можно импортировать в KOMRAD из файла формата «CSV».
14) Появились продвинутые виджеты: встроенные редактируемые, а также модуль Grafana без телеметрии со встроенными плагинами источников данных ClickHouse и HTTP/JSON/CSV/XML.
15) Обновлена СУБД, теперь используется собственный форк ClickHouse 24.8 LTS.
16) Матрицы атак перенесены в раздел «Справочники», теперь доступ к информационной базе есть у любого пользователя KOMRAD.

17) Добавлена возможность отправки уведомлений с использованием метода «webhook», в частности – появилась возможность отправки уведомлений через мессенджер telegram.

Что улучшено

1) Шаблоны SQL коллектора теперь явно привязаны к типу БД.
2) Для Windows агента оптимизировано регулярное выражение для парсинга деталей вызова команды при чтении журнала Powershell.
3) Для Syslog коллектора парсеры Syslog RFC5424, RFC3164 ускорены в 2-3 раза, а также добавлена возможность автоматического распознания парсера SYSLOG из CEF, RFC5424, RFC316.
4) Снижен средний размер события в базе данных на 10-20%, снижено потребление памяти при обработке событий на 5-10%, упрощение написания SQL запросов к таблице событий в ClickHouse, снижено время выполнения запросов и ресурсов, расходуемых на исполнение запроса в ClickHouse на 2-7%.
5) Оптимизирована вставка событий ИБ в БД ClickHouse в модуле «komrad-processor», теперь риск возникновения очередей из собранных коллекторами событий информационной безопасности минимален и может проявляться на экстраординарной нагрузке более 800 000 EPS.

Что исправлено

1) Добавлена ERROR_INVALID_PARAMETER к списку ошибок, при которых WMI агент может восстановиться, что снижает число рестартов агента при большой нагрузке.
2) Теперь все байтовые буферы получают новые образцы из одного пула, в результате чего оптимизируется работа с памятью агента, особенно при больших нагрузках.
3) Исправлена ранее некорректная таблица User Account Control Attributes для модуля security нормализатора журналов Windows.
4) Обработка Lua фильтров переведена на асинхронный режим, что помогает использовать все доступные ресурсы машины при большом потоке событий.