УДК 60

ОБЗОР SIEM-СИСТЕМ: ПРОПРИЕТАРНЫЕ ARCSIGHT И MAXPATROL ПРОТИВ OPEN-SOURCE РЕШЕНИЙ

Королев И.Д.,
доктор технических наук, профессор, профессор кафедры безопасности программного обеспечения систем и комплексов военного назначения,
Краснодарское высшее военное училище,
Краснодар, Россия
Попов В.И.,
Адъюнкт,
Краснодарское высшее военное училище,
Краснодар, Россия
Ларионов В.А.,
Курсант,
Краснодарское высшее военное училище,
Краснодар, Россия
Литвинов Е.С.,
Специалист по защите ИО,
Краснодарское высшее военное училище,
Краснодар, Россия

Аннотация: В статье рассмотрены вопросы современного состояния информационной сферы России и обеспечения бесперебойного функционирования критической информационной структуры, в частности – с помощью SIEM-систем. Дана краткая характеристика наиболее распространенных проприетарных решений, а также показана «open-source» альтернатива и приведено их сравнение.

Ключевые слова: информационная безопасность; анализ SIEM-систем; сравнение SIEM-систем; проприетарное и «open-source» программное обеспечение.

REVIEW SEEM SYSTEMS: PROPRIETARY ARCSIGHT AND MAXPATROL AGAINST OPEN-SOURCE OF SOLUTIONS

Korolev I.D.
Professor, Doctor of Technical Sciences, Professor of the Software Department of Military Systems and Complexes,
Krasnodar Territory Military School,
Krasnodar, Russia
Popov V.I.
Adjunct,
Krasnodar Higher Military School,
Krasnodar, Russia
Larionov V.A.
Cadet,
Krasnodar Higher Military School,
Krasnodar, Russia
Litvinov E.S.
Specialist in the protection of IO,
Krasnodar Higher Military School,
Krasnodar, Russia

Abstract: The article deals with the current state of the information sphere in Russia and ensuring the smooth functioning of the critical information structure, in particular with the help of SIEM-systems. A brief description of the most common

proprietary solutions is given, as well as an “open-source” alternative is shown and compared.
Keywords: information security; analysis of SIEM-systems; comparison of SIEM-systems; proprietary and open-source software.

Согласно Доктрине информационной безопасности Российской Федерации от 05.12.2006 г, одними из национальных интересов в информационной сфере являются бесперебойное функционирование критической информационной структуры и развитие в России отрасли ИТ и электронной промышленности – два направления, совместно формирующие проблему соблюдения баланса между защищенностью и инновациями в масштабах государства.

Россия в сфере информационных технологий не отстает от мирового сообщества. Во многих актуальных направлениях этой сферы реализуются проекты, составляющие достойную конкуренцию американским, европейским и азиатским компаниям. Виртуальная и дополненная реальность, технологии умного города, предоставление гражданам доступа к госуслугам в цифровом виде, 3D-печать, облачные технологии, интернет вещей – все это уже является частью повседневной жизни. Соответственно, значительно повышаются и требования к обеспечению информационной безопасности (ИБ).

Обращаясь к статистическим данным, ясно видно, что угрозы сетевой безопасности продолжают расти. Количество выявляемых вредоносных программ в мире за 10 лет увеличилось в 208,3 раза и превысило 300 тыс. в сутки, следует из выступления управляющего директора «Лаборатории Касперского» в России и СНГ Сергея Земкова.[1]. Количество уникальных киберинцидентов в I квартале 2018 года на 32% превысило показатели аналогичного периода в 2017 году. [2]

Итоги 2018 года показывают, что в общей сложности рынок ИБ в России вырос очень незначительно: общий прирост составил менее 10% по сравнению с показателями 2017 года. При этом позитивную динамику рынок получает за счет запуска отдельных проектов в области цифровизации федерального уровня (например, перевода городского хозяйства на новые технологии, появления умных городов, умного транспорта, государственных сервисов), а также за счет ряда крупнейших игроков отечественного рынка, выбравших для себя путь цифровой трансформации и понимающих необходимость некоей безопасности 2.0 – подхода, основанного не только на отражении атак, но и на проактивном выявлении угроз. [3]

Основными угрозами ИБ по итогам года стали:

– использование машинного обучения и искусственного интеллекта киберпреступниками;

– дальнейшее развитие вирусов-вымогателей;

– эксплуатация уязвимостей в устройствах класса IoT;

– рост атак на промышленные предприятия и атак на цепочки поставок;

– атаки на мобильные устройства;

– атаки на облачную инфраструктуру и хранилища;

– эксплуатация уязвимостей в мобильных сетях, а также протоколах Wi-Fi и Bluetooth;

– взломы криптовалютных кошельков и криптобирж;

– криптомайнеры в различных вариациях;

– рост мощности DDoS атак;

– крупные утечки данных. [4]

Исследования показывают, что только в 2018 году количество вредоносных программ выросло на 71%. Многие организации уязвимы для хакеров, вирусов, вредоносных программ, взлома данных и мошенничества с

идентификацией, а тем более организации с меньшими группами ИБ и меньшими бюджетами по ИБ. Хуже того, у этих фирм часто нет специальной группы по ИБ или большого опыта в этой области. С ростом угроз по ИБ требования нормативно-правовых актов также продолжают расти, и, тем не менее, численность персонала для борьбы с угрозами во многих организациях сокращается.

Автоматизация процесса сбора сведений о произошедших киберинцидентах, их корреляция, структурированное хранение и модификация системы безопасности с целью устранения обнаруженных уязвимостей – повседневная задача не только полноценных отделов ИБ в государственных корпорациях и банковских структурах, но и рядовых специалистов отделов IT в коммерческих организациях.

Сохранность информации ограниченного доступа, находящейся в системе, от коммерческой и служебной тайны до персональных данных, стала одним из камней преткновения 2018 года. На основании статистических данных видно, что киберпреступники на сегодняшний день находятся на высоком уровне компетенций, они скурпулезно выбирают цели своих атак, используют изощренные и мощные инструменты. При этом, в современном информатизированном обществе утечка уже упомянутых персональных данных может нести серьезные последствия для информационной и финансовой безопасности личности, предоставляя злоумышленнику доступ к сервисам управления гражданскими функциями или возможность регистрации финансовых операций от имени жертвы.

В свете вышесказанного понятно, что даже организации, которые не могут себе позволить полноценный отдел кибербезопасности, вынуждены внедрять SIEM-решения (Security Information and Event Management) [5], так как стандартного набора антивируса и межсетевого экрана недостаточно для полноценного функционирования системы защиты. Кратко рассмотрим

несколько наиболее популярных SIEM-решений: ArcSight от компании Hewlett-Packard и MaxPatrol SIEM от российского разработчика Positive Technologies.

Решение ArcSight ESM Security для управления информацией и событиями используется для защиты самых известных в мире компаний. ArcSight ESM отслеживает все события в масштабах всего предприятия и использует мощную корреляцию и анализ для выявления угроз для бизнеса и технологий. Созданный на гибкой расширяемой платформе, ESM обеспечивает переносимость контента с одной технологии на другую, как внутри организаций, так и между ними.

Инфраструктура сбора ESM предлагает расширенные возможности сбора для самой широкой библиотеки источников событий - собираются журналы с более чем 275 устройств и источников событий, включая ОС, сетевые устройства (маршрутизаторы, коммутаторы), сетевые анализаторы (сетевые мониторы и анализаторы трафика, NAC, NBA). Решения для обеспечения безопасности (IPS/IDS, брандмауэр, VPN, сканеры уязвимостей), а также журналы приложений, баз данных, решений для управления идентификацией и веб-серверов/веб-приложений. События от разных устройств в одном семействе (например, маршрутизаторы) нормализуются для облегчения мониторинга и анализа между устройствами. Дополнительные пакеты решений могут поддерживать и решать наиболее важные проблемы и инициативы, такие как SOX, PCI, HIPAA, GLBA, мониторинг пользователей и управление ИТ. [6]

ArcSight ESM предлагает ряд функций, которые обеспечивают быстрый, удобный и интуитивно понятный доступ к информации, он предоставляет исчерпывающие технические, эксплуатационные и трендовые отчеты, которые сообщают о состоянии безопасности и соответствуют требованиям нормативной отчетности. [7]

MaxPatrol SIEM от компании Positive Technologies, реализовавшей новые подходы для эффективного выявления инцидентов, основанные на глубоком понимании инфраструктуры и адаптации системы к её изменениям, на анализе не только событий, но и всей доступной информации. [8].

MaxPatrol SIEM предусматривает возможность передачи экспертизы заказчику, для этого используется база знаний Positive Technologies Knowledge Base (PTKB) – постоянно пополняемый набор данных, основанный на 15-ти летнем аудите защищенности информационных систем. Связка SIEM-системы с PTKB позволяет получать данные о новых сценариях атак и паттернах поведения хакеров, учитывать новые уязвимости и эксплойты, автоматически обновлять правила корреляции и применять их в инфраструктуре заказчика без ручной перенастройки [9].

Рассмотренные решения обладают широким спектром преимуществ, но существует критичный для организаций, не способных включить в бюджет средства на использование проприетарных решений, недостаток – их высокая стоимость. Может также сложиться ситуация, когда руководству организации перед тем, как принять решение о приобретении необходимых, казалось бы, программных продуктов, необходимо убедиться на живом примере в эффективности этого класса решений. В этих случаях помогут «open-source» («открытое программное обеспечение», англ.) решения, в качестве примера рассмотрим OSSIM:

OSSIM (Open Source Security Information Management) — система управления, контроля и обеспечения ИБ. OSSIM «из коробки» включает в себя такой функционал как:

- сбор, анализ и корреляция событий – SIEM;
- хостовая система обнаружения вторжений (HIDS) – OSSEC;
- сетевая система обнаружения вторжений (NIDS) – Suricata;
- беспроводная система обнаружения вторжений (WIDS) – Kismet;

– мониторинг узлов сети – Nagios;

– анализ сетевых аномалий – P0f, PADS, FProbe, Arpwatch и др.;

– сканер уязвимостей – OpenVAS;

– мощнейшая система обмена информацией об угрозах между пользователями OSSIM – OTX;

– более 200 плагинов для парсинга и корреляции логов со всевозможных внешних устройств и служб. [10]

Ресурс anti-malware.ru провел комплексное сравнение SIEM-систем [11-12], в том числе рассматриваемых выше, приведем выдержку наиболее важных пунктов:

Таблица 1 - Сравнение SIEM-систем

Критерии оценки	Micro Focus (HP) ArcSight	MaxPatrol SIEM	AlienVault OSSIM
Сертификаты ФСТЭК России	№ 3605 от 12.08.2016 (НДВ4, ТУ)	№ 3734 от 12.04.2017 (НДВ4, ТУ)	нет
Карточка инцидента	55 настраиваемых полей	19 настраиваемых полей	12 настраиваемых полей
Пути эскалации инцидента	выстраивание уровней и путей эскалации инцидента	автоматическая маршрутизация инцидента при наличии условий (сработавшего правила, критичности инцидента, критичности активов, свойств активов)	нет
Принятие решений в рамках процесса обработки инцидентов	ручное и автоматическое	ручное	нет
Возможность выделения ложных срабатываний	в ручном режиме	в ручном режиме	нет
Наличие предустановленных правил корреляции	около 350	более 150	82

Возможность увеличения мощности компонентов системы	расширением доступных аппаратных ресурсов	расширение лицензии или улучшение аппаратной платформы	нет
Возможности управления ИТ-активами	автоматическое и ручное создание.	возможность автоматического поиска и создания	да
Управление правилами корреляции	объектный конструктор	язык поисковых запросов	объектный конструктор
Агрегация событий по типу	да	да	нет
Возможность сбора данных о сетевом трафике	netflow/ J-flow/ IPFIX	отдельный модуль, использующий SPAN или NetFlow	да
Количество поддерживаемых источников событий	300+	200+ (по уточнению вендора)	без ограничений

Очевидно, что по многим параметрам OSSIM уступает проприетарным решениям, но выполняет основные функции, требуемые от подобных систем. Организациям, планирующим внедрить SIEM-систему, можно рекомендовать начать с «open-source» решений, с тем, чтобы понять, насколько серьезный комплекс защиты фактически требуется для их информационной среды, отработать навыки работы с SIEM у администраторов и взвешенно принять решение о внедрении проприетарной версии.

Альтернативным подходом может служить расширение функций SIEM-системы за счет внедрения «open-source» программ для реагирования на инциденты, обогащения данным по ним, создания распределенной структуры оповещения об инцидентах и превентивной защиты в структурных подразделениях. Такой подход потребует большего мастерства администратора информационной безопасности, но останется бесплатным для организации.

В качестве примера можно рассмотреть использование TheHive – платформы по реагированию на инциденты и Cortex – системы обогащения

данных по инцидентам, а также MISP – платформы распространения данных об инцидентах. В TheHive поступают данные, из любых систем, посредством API TheHive4Py, например, из SIEM, либо заносятся вручную. У каждого инцидента есть важная составляющая – индикаторы компрометации. Это ссылки, IP, домены, сэмплы вредоносных файлов, хэши, названия процессов и так далее. По сути то, что специалист посчитал угрозой. И вот тут появляется второй элемент стека – Cortex. Он, используя API десятков сервисов обогащает данные инцидента. Данные по закрытым подтверждённым инцидентам попадают в MISP и сразу отправляются в территориально удалённые подразделения компании, где происходит превентивная блокировка индикаторов компрометации в системах защиты информации[13]

Таким образом, с помощью 3-4 программных продуктов возможно создание совершенно бесплатного полноценного комплекса сбора, анализа, реагирования и превентивной защиты от инцидентов компьютерных атак, если не брать в расчёт затраты на аппаратное обеспечение и оплату работы штатного специалиста по ИБ.

Библиографический список

1. rns.online.ru: Вирусная статистика – [Электронный ресурс]. – Режим доступа: https://rns.online/it-and-media/Kolichestvo-viyavlyaemih-kompyuternih-virusov-v-mire-za-10-let-viroslo-v-200-raz--2017-04-18/ (Дата обращения 19.02.2019).

2. ptsecurity.com: Кибербезопасность и пространство киберугроз – [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2018-q1/ (Дата обращения 19.02.2019).

3. ptsecurity.com: Анализ кибербезопасности. – [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-2018-2019/ (Дата обращения 19.02.2019).

4. rvision.pro: Итоги информационной безопасности 2018 года – [Электронный ресурс]. – Режим доступа: https://rvision.pro/blog-posts/itogi-informatsionnoj-bezopasnosti-v-2018-godu/ (Дата обращения 19.02.2019).

5. Попов В.И., Королев И.Д. Анализ проблематики системы управления информацией и событиями безопасности в информационных системах //Инновации в науке. 2018. - № 12 (88)– С. 19-26.

6. g2crowd.com: SIEM-системы – [Электронный ресурс]. – Режим доступа: https://www.g2crowd.com/categories/security-information-and-event-management-siem (Дата обращения 19.02.2019).

7. cisco.com: – [Электронный ресурс]. – Режим доступа: https://www.cisco.com/c/dam/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Smart_Business_Architecture/February2012/SBA_Ent_BN_ArcSightSIEMPartnerGuide-February2012.pdf (Дата обращения 19.02.2019).

8. tadviser.ru: Обзор Продукта HPE_ArcSight_ESM – [Электронный ресурс]. – Режим доступа: http://www.tadviser.ru/index.php/Продукт:HPE_ArcSight_ESM_(Security_Information_and_Event_Management,_SIEM)#2016:_ArcSight_ESM_.D0.B7.D0.B0.D0.B2.D0.B5.D1.80.D1.88.D0.B8.D0.BB.D0.B0_.D1.81.D0.B5.D1.80.D1.82.D0.B8.D1.84.D0.B8.D0.BA.D0.B0.D1.86.D0.B8.D1.8E_.D0.A4.D0.A1.D0.A2.D0.AD.D0.9A (Дата обращения 19.02.2019).

9. ib.radiuscompany.ru – [Электронный ресурс]. – Режим доступа: https://ib.radiuscompany.ru/products/maxpatrol-siem/ (Дата обращения 19.02.2019).

10. habr.com – [Электронный ресурс]. – Режим доступа: https://habr.com/ru/post/255433/ (Дата обращения 19.02.2019).

11. anti-malware.ru: комплексное сравнение SIEM-систем – [Электронный ресурс]. – Режим доступа: https://www.anti-malware.ru/compare/SIEM-systems (Дата обращения 19.02.2019).

12. anti-malware.ru: комплексное сравнение SIEM-систем – [Электронный ресурс]. – Режим доступа: https://www.anti-malware.ru/compare/SIEM-systems-part2 (Дата обращения 19.02.2019).

13. habr.com: – [Электронный ресурс]. – Режим доступа: https://habr.com/ru/post/350392/ (Дата обращения 19.02.2019).

Оригинальность 96%