Внедрение киберполигона в образовательный процесс

Сергей Вячеславович Кривоногов
Старший преподаватель
Нижегородский государственный инженерно-экономический университет
Княгинино, Россия
ksvkn@mail.ru
ORCID 0000-0001-7502-8014

Поступила в редакцию 06.03.2024
Принята 26.04.2024
Опубликована 15.10.2024

УДК 004.946:37
DOI 10.25726/o3629-6381-3996-s
EDN QOZFUN
ВАК 5.8.1. Общая педагогика, история педагогики и образования (педагогические науки)
OECD 05.03.HA. EDUCATION & EDUCATIONAL RESEARCH

Аннотация

Данная статья посвящена детальному рассмотрению проблем, с которыми сталкиваются учебные заведения при подготовке студентов по направлениям, связанным с информационной безопасностью. В современном мире, где цифровые технологии проникли во все сферы жизни, защита информации стала одной из ключевых задач для организаций и государств. Обеспечение компетентной подготовки специалистов в этой области является критически важным, однако процесс обучения сопряжен с рядом трудностей. Часто программы обучения отстают от стремительного развития технологий, а преподаватели не всегда имеют доступ к современным инструментам и ресурсам. Студенты же, в свою очередь, нуждаются в практических навыках и реальном опыте работы с актуальными системами защиты, чтобы быть готовыми к вызовам профессиональной деятельности. Все это создает необходимость переосмысления подходов к образованию в сфере информационной безопасности. Важным аспектом современной информационной безопасности является использование SIEM-решений (Security Information and Event Management) в организациях. В статье подробно описывается актуальность внедрения таких систем в корпоративную среду. SIEM-системы позволяют собирать, анализировать и коррелировать данные о событиях безопасности из различных источников, что значительно повышает эффективность обнаружения и реагирования на инциденты. Проведен сравнительный анализ имеющихся решений, который показал, что готового решения для обучения студентов мониторингу безопасности не существует. Показаны результаты внедрения SIEM-системы в образовательный процесс подготовки бакалавров. Сделаны выводы.

Ключевые слова

информационная безопасность, киберполигон, киберпреступления, компетентностный подход, мониторинг, обучение студентов, сравнительный анализ, угрозы безопасности.

Введение

В настоящее время в мире ежедневно совершается более 100 тыс. киберпреступлений, все они направлены на взлом, хищение и распространение информации. Раскрытие коммерческой информации приводит к глобальной потере финансовых потоков, и, как следствие, снижается выручка, теряются партнеры, расторгаются договора. В связи с этим необходимо отметить, что обеспечение информационной безопасности занимает немаловажную роль в деятельности любых организаций. В Российской Федерации в настоящее время идет активный цикл развития разработки методов и мер по

обеспечению информационной безопасности. Это направление развития соответствует Указу Президента Российской Федерации № 250 от 01.05.2022 г. «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».

В этой связи отметим, что для разработки таких методов защиты информации необходимы специалисты, однако в данное время образовательные учреждения не подготавливают их в нужном количестве. В то же время в вузах, обучающих студентов обеспечению информационной безопасности, наблюдается острая нехватка необходимого для этих целей оборудования. Такие комплексы дорогостоящие, кроме того, должна проводиться модернизация материально-технической базы, так как готовые решения требуют больших вычислительных ресурсов и обладают высокой конечной стоимостью владения. В результате обучение студентов проводится на урезанной материальной базе, которая, в свою очередь, не подходит под запросы работодателей, и для трудоустройства на работу выпускникам приходится проходить дополнительное обучение на внешних образовательных площадках.

Еще одним важным аспектом в этой связи является актуальность используемых в процессе обучения образовательных лабораторий и программных продуктов, так как ежедневно появляются новые угрозы безопасности, а имеющиеся в наличии у вузов программные продукты не предоставляют возможность обучения по устранению новых угроз.

Материалы и методы исследования

В образовательных учреждениях, занимающихся подготовкой специалистов по информационной безопасности, лаборатории реализованы с использованием средств виртуализации. На виртуальном сервере развернута машина с угрозами, обучающиеся в рамках выполнения поставленных задач удаленно подключаются к ней и в соответствии с заданием устраняют возникшие угрозы, а также предотвращают появление новых путем установки обновлений безопасности программного обеспечения.

В крупных организациях имеется большое количество персональных компьютеров, и в производственных реалиях трудно отследить любые изменения и подозрительную активность. Поэтому организации используют SIEM-решения с определенным набором правил, которые своевременно сообщают о возникших угрозах. За работу такой системы отвечают специалисты по информационной безопасности, они отслеживают действия пользователей на компьютерах организации и в автоматическом режиме определяют любую подозрительную активность. Таких SIEM-систем становится все больше, но обучающиеся в процессе обучения не получают реальный опыт работы с ними, так как в образовательных организациях нет возможности развернуть такую систему из-за отсутствия образовательной версии, а коммерческие версии стоят дорого, что выходит за рамки бюджета вуза.

Существует большое количество готовых решений, позволяющих проводить обучение студентов, аналоги которых используются в реальных организациях. Все эти решения платные, но при этом не обладают достаточным функционалом и в целом не подходят для проведения обучения, так как имеют сложную структуру и не предоставляют собой реальной версии для обучения. Для оценки существующих решений проанализируем ряд решений, наиболее подходящих для обучения студентов.

Результаты и обсуждение

В процессе проведения сравнительного анализа существующих SIEM-систем были рассмотрены три наиболее часто использующихся решения. Наиболее распространена SIEM-система от компании IBM QRadar Security Intelligence, включающая в себя несколько интегрированных систем, тесно взаимосвязанных между собой. Такие системы в основном используются в промышленных организациях. Решение не требует комплексной настройки и готово к использованию после развертывания на сервере. QRadar Security Intelligence. Оно обладает функционалом по сбору данных с различных источников, в том числе с разноуровневых операционных систем (Windows, Linux), серверов баз данных, расположенных на разных иерархических уровнях, сбор обеспечивается и с баз данных, устройств безопасности, в том числе и серверов цифровой подписи. Отдельно сбор данных осуществляется с устройств локальной сети, приложений и иных пользовательских компонентов. Для

обеспечения сбора данных с устройств локальной сети и пользовательских компонентов необходима комплексная настройка программного обеспечения.

Ограничением в работе программного обеспечения является невозможность фильтрования данных, обрабатывающихся посредством электронной почты, так как почтовые провайдеры не представляют API, позволяющий интегрироваться с сервисом. Исключение составляет корпоративная почта, которая располагается непосредственно на серверах организации. В программном обеспечении имеется система, позволяющая в автоматическом режиме отслеживать вредоносные IP-адреса и блокировать их. При работе с программным обеспечением сотрудник в режиме 24/7 отслеживает работу корпоративной сети и получает отчеты о возможных вредоносных воздействиях, при этом критические уведомления приходят на корпоративную электронную почту. Типовые кибератаки определяются SIEM-системой IBM QRadar Security Intelligence быстро и автоматически применяют меры по их ликвидации и устранению вредных воздействий. При выявлении угроз безопасности программное обеспечение в автоматическом режиме расставляет приоритеты по обезвреживанию угроз. Рассматриваемое программное обеспечение предоставляется на коммерческой основе с лицензией сроком на один год, пробная версия не предусмотрена. Лицензия для образовательных учреждений не предусматривается.

MaxPatrol SIEM является программным обеспечением, на базе которого можно реализовать собственную SIEM систему, используя модульную сборку компонентов. Программное обеспечение может работать с широким спектром разнородного оборудования, обрабатывающего информацию. В частности, к разнородному оборудованию можно отнести мобильные телефоны, распределенные устройства, корпоративные сети, различные web-сервисы. Программное обеспечение может обработать такую информацию, как действия пользователей, хранящиеся во внутренних журналах оборудования, новые файлы, процессы, установку программного обеспечения, использование несанкционированных носителей. При возникновении угрозы системный администратор получает уведомление с уровнем тревоги как на мобильный телефон, так и на электронную почту. Для получения уведомлений на телефон необходимо установить программное обеспечение и привязать к нему свой номер телефона. Своевременное обновление инструкций позволяет избавляться от угроз в автоматическом режиме посредством блокировки угрозы и передачи информации системному администратору. Для удобства работы программное обеспечение MaxPatrol SIEM может быть интегрировано с внешними сервисами для повышения уровня защиты данных (Анацкая, 2016). MaxPatrol SIEM позволяет комплексно отслеживать запросы и распределять их по уровням безопасности.

Программное обеспечение обладает простым и удобным пользовательским интерфейсом, в котором можно просмотреть статистику по действиям пользователей и различным обработчикам событий оборудования, имеющегося в локальной сети организации. Важным преимуществом MaxPatrol SIEM является работа с большими массивами данных, поэтому его можно использовать в глобальных вычислительных сетях, которые действуют в рамках филиалов одной организации. Также в программном обеспечении можно корректно распределять нагрузку, вследствие этого вырастает производительность SIEM-системы (Гриншкун, 2013). MaxPatrol SIEM является масштабируемой системой – в случае необходимости пользователь может подключить любой из доступных модулей или заказать его разработку. Для развертывания SIEM-системы не нужно приобретать дополнительное оборудование – развертывание осуществляется на внешнем облачном сервере, доступ к которому предоставляется только системному администратору. MaxPatrol SIEM предоставляется строго на коммерческой основе и не предполагает версию для обучения. Пользователям SIEM-системы MaxPatrol предоставляется техническая поддержка и краткий обучающий курс по работе с системой.

Часто используется и российское решение RuSIEM, которое представляет собой облачную платформу, интегрирующуюся в корпоративную сеть организации. Преимуществом SIEM-системы является использование аналитики пользователей и контроль отклонения работы системы от эталонных показателей. Это позволяет определить инсайдерские угрозы и проводимые атаки, не взаимосвязанные с вредоносным воздействием на корпоративную сеть организации. Решение обладает собственными запатентованными решениями, которые, в свою очередь, на базе своего ядра системы позволяют противостоять возможным угрозам в корпоративной сети.

Отслеживание угроз безопасности выполняется в режиме реального времени путем сравнительного анализа с эталонным поведением системы. Распределение ресурсов на сервере позволяет обеспечить высокую производительность SIEM-системы. Собственный механизм безопасности позволяет в автоматическом режиме определять даже новые угрозы безопасности (Кирсанов, 2024). При определении SIEM-системой нештатной ситуации в корпоративной сети системному администратору либо IT-специалисту, ответственному за безопасность, приходит уведомление, при этом градация уведомлений распределяется в зависимости от уровня угрозы. RuSIEM обеспечивает поддержку индикаторов компрометации, что позволяет определять и отличать реальные атаки от тестовых. Архитектура RuSIEM обеспечивает равномерное распределение нагрузки между несколькими виртуальными машинами, тем самым снижается временная задержка на обработку атаки. Отдельно RuSIEM поддерживает ведение журналов обработки возникающих событий, при этом копия журнала хранится на удаленном носителе, эти данные используются при расследовании инцидентов.

RuSIEM не предоставляет образовательную версию, имеется только коммерческая версия, предоставляемая организациям. При этом необходимо отметить, что SIEM-система может устанавливаться по подписке, при этом также можно выбрать только необходимые компоненты. Кроме этого, система может быть масштабируема и использована в рамках филиалов одной организации.

Анализ поведения позволяет предотвратить умышленные нарушения безопасности устройств, имеющихся в корпоративной сети организации. В SIEM-систему заложены методики, позволяющие определить странное поведение пользователей сети, неспецифичные процессы, кроме этого, анализируются и другие устройства на предмет возникновения на них аналогичных нештатных ситуаций. Такие нештатные ситуации заложены во внутренние политики системы RuSIEM. Для удобства работы с полученной информацией система позволяет формировать визуальные отчеты с граничными распределениями данных. Использование системы RuSIEM позволяет выстроить надежную систему защиты данных организации либо модернизировать уже имеющуюся. Встроенный модуль отслеживания снижает число ложных срабатываний (Дудина, 2021).

Все рассматриваемые системы поддерживают интеграцию с ГосСОПКА и сертифицированы ФСТЭК России.

На основе изложенной информации можно сделать вывод, что все рассматриваемые SIEM-системы не имеют версий для обучения, которые могут использоваться в образовательных учреждениях. Кроме этого, не предоставляются и пробные версии программного обеспечения. Для работы с SIEM-системами необходимо приобретать либо реальное серверное оборудование, либо арендовать виртуальный сервер. Аренда сервера в MaxPatrol SIEM и RuSIEM включается в основную подписку. Также необходимо отметить, что для работы с рассматриваемыми SIEM-системами обучение во внешних организациях не предусмотрено, так как для этой цели нет сертифицированных инструкторов.

Для проведения сравнительного анализа необходимый функционал сведем в таблицу.

Таблица. Сравнительный анализ существующих решений

Критерий	IBM QRadar Security Intelligence	MaxPatrol SIEM	RuSIEM
Бесплатная лицензия	–	–	–
Возможность использования в образовательных целях	–	–	–
Возможность генерации вредоносных программ для обучения системы	–	–	–
Возможность доработки	–	+	–
Формирование отчётности	+	+	+
Рассылка уведомлений	+	+	+
Просмотр статистики	+	+	+

Необходимость комплексной настройки	–	+	+
Работа с большими массивами данных	–	+	–
Автоматическое блокирование угроз	+	+	+
Высокий уровень производительности	–	+	–
Использование облачного сервера	–	+	–
Просмотр логов и журналов	+	–	–
Фильтрование данных	+	–	–
Разграничение уровней пользователей	–	–	–
Интеграция с внешними сервисами	+	+	+
Проведение сравнительного анализа поведения с эталонным	+	–	–
Отслеживание угроз в режиме реального времени	+	+	+
Организация единого цифрового пространства	+	–	–

Анализируя данные таблицы, можно сделать вывод, что бесплатная лицензия, как и версия для образовательных учреждений, не предусматривается ни одним из рассматриваемых программных продуктов. Кроме этого, все существующие программные решения могут обучаться только вручную с использованием существующих баз вирусов, генерация вредоносных воздействий не поддерживается ни одним из анализируемых решений. Возможность доработки программного обеспечения реализовано в IBM QRadar Security Intelligence и RuSIEM, это в целом позволит пользователю в период поддержки предлагать различные варианты изменения системы, либо вносить изменения самостоятельно.

При этом формирование отчетности, рассылка уведомлений, просмотр статистики реализовано во всех анализируемых SIEM-решениях. Комплексная настройка необходима IBM QRadar Security Intelligence, остальные анализируемые решения могут работать непосредственно после установки, необходимо лишь добавить оборудование, которое будет мониториться.

Работу с большим объемом данных поддерживает программный продукт MaxPatrol SIEM. Автоматическое блокирование угроз поддерживается всеми рассматриваемыми решениями. Высокий уровень производительности и использование в своей работе облачного сервера реализовано в решении MaxPatrol SIEM. Просмотр логов и журналов и фильтрование данных поддерживает решение IBM QRadar Security Intelligence. Ни одно из рассматриваемых решений не поддерживает комплексное разграничение уровней пользователей. Интеграция с внешними сервисами и отслеживание угроз в режиме реального времени поддерживается всеми рассматриваемыми решениями. Сравнительный анализ поведения с эталонным и организация единого цифрового пространства реализованы в решении IBM QRadar Security Intelligence.

Таким образом, можно сказать, что в образовательных целях невозможно использовать рассматриваемые SIEM-системы, так как они не предоставляют образовательных лицензий и многие из них не обладают необходимым функционалом для обучения.

Для обеспечения необходимого уровня профессиональной подготовки обучающихся предлагается внедрить бесплатную SIEM-систему Wazuh, она является полноценной SIEM-системой,

позволяющей проводить комплексный менеджмент информации и событий безопасности. Важным преимуществом SIEM-системы Wazuh является низкое потребление ресурсов даже в режиме максимальной нагрузки. Основным функционалом Wazuh является сканирование процессов операционной системы, причем SIEM-система является мультиплатформенной и может сканировать процессы на любой операционной системе (Королев, 2018). Кроме этого, в функционал системы входит получение отчетов об инцидентах безопасности, осуществление проверки уязвимости операционной системы. Wazuh состоит из двух элементов – агента, который устанавливается на рабочей машине пользователя. Он работает в тихом режиме, и пользователь не замечает его присутствие. Вторая, основная, часть SIEM-системы размещается на сервере. В качестве сервера может использоваться высокопроизводительный компьютер, при этом Wazuh просто встраивается в контроллер домена и автоматически загружается у пользователей.

Важным преимуществом Wazuh является наличие готовых наборов политик для разных операционных систем – начинающему пользователю достаточно загрузить в Wazuh скрипт с политиками и настроить агент для работы с ними. Новые версии Wazuh поддерживают интеграцию с сервисами Telegram, уведомления об обнаруженных изменениях и нарушениях будут приходить в данный мессенджер. Для интеграции и настройки используется специальный бот, который взаимодействует только с отдельным сервисом, что позволяет не нарушать режим безопасности инфраструктуры предприятия. Все ошибки, обнаруженные агентом Wazuh, разделяются по нескольким уровням – критические ошибки (пятый уровень и выше) и не критические (ниже пятого уровня). По умолчанию отправляются лишь обнаруженные критические ошибки, на которые необходимо своевременно реагировать (Перекотий. 2024).

В SIEM-системе все события отображаются в отдельном лог-журнале, доступ к которому имеет только системный администратор. При этом если возникает стандартная ошибка, то решение этой ошибки предлагается автоматически из справочной системы. Кроме этого, в системе имеется и модуль блокировки вредных воздействий, его корректная настройка обеспечивает комплексную безопасность корпоративной сети. Такая система позволяет мониторить сервера как на базе операционной системы Windows Server всех редакций, так и на базе Ubuntu.

SIEM-систему Wazuh можно использовать для обучения студентов, так как ее можно развернуть в рамках одного компьютерного класса. Система не требует для работы глобальных вычислительных ресурсов – сервер можно развернуть на любом компьютере. Кроме этого, систему можно развернуть и внутри виртуальной машины и запускать ее только в рамках практических занятий по дисциплинам.

На базе института информационных технологий и систем связи по безопасности обучаются студенты по направлению подготовки 11.03.02 «Инфокоммуникационные технологии и системы связи» с профилем «Защищенные системы и сети связи». Киберполигон на базе SIEM-системы Wazuh предполагается использовать в рамках таких дисциплин, как «Программно-аппаратные средства обеспечения информационной безопасности», «Эксплуатация уязвимостей программного обеспечения», «Комплексное обеспечение информационной безопасности инфокоммуникационных сетей и систем». Кроме этого, киберполигон можно использовать в рамках практических занятий по дисциплине «Информационная безопасность» при подготовке бакалавров по направлению подготовки «Информационные системы и технологии».

Для отображения пользователей и доступного им функционала в рамках учебного процесса построим диаграмму вариантов использования. На диаграмме выделим актеров (пользователей) и для каждого из пользователей определим необходимый функционал. Диаграмма вариантов использования представлена на рисунке 1.

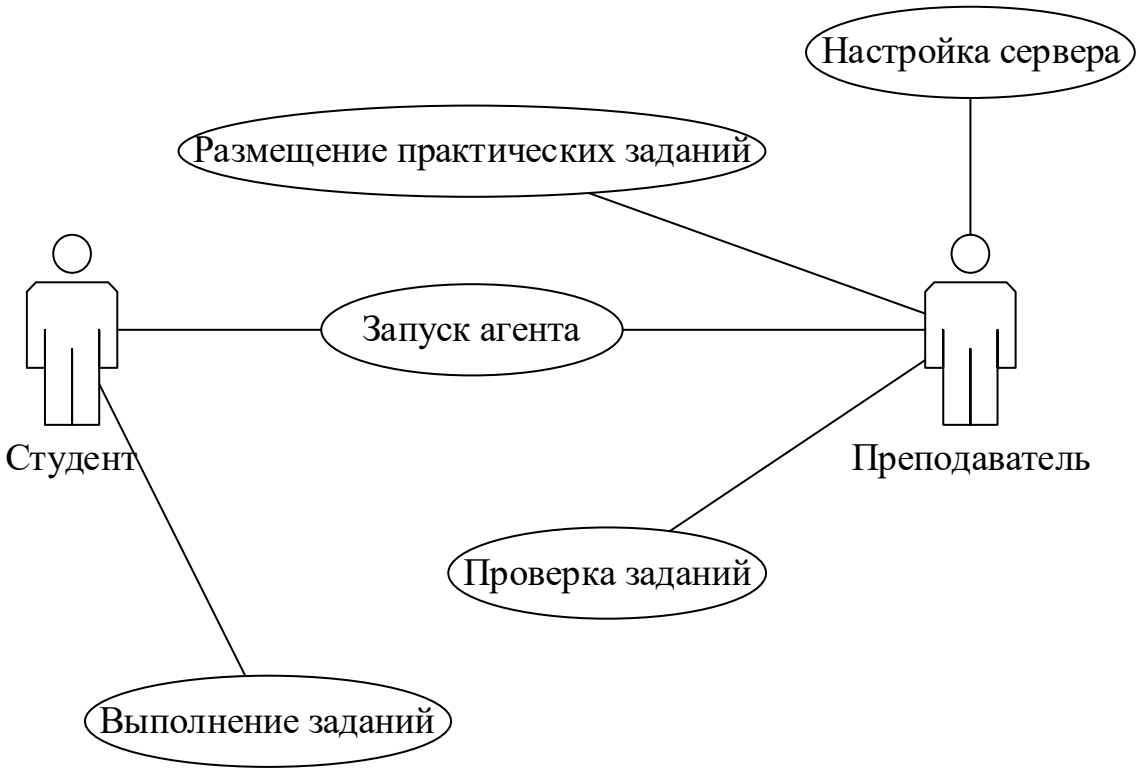

Рисунок 1. Диаграмма вариантов использования

Из диаграммы вариантов использования показанной на рисунке 1 видно, что с киберполигоном будут взаимодействовать два действующих лица – преподаватель и студент. Студенту предстоит выполнять задания, загруженные в систему преподавателем. Задание может включать выявление угрозы или нелегального копирования файлов, определение подозрительной активности. Преподаватель, в свою очередь, занимается подготовкой практических работ и размещением их на централизованном сервере, выполняет настройку сервера, активирует агента на компьютерах пользователей и проверяет выполненные студентами работы.

Киберполигон размещается в компьютерном классе на виртуальных машинах. Это необходимо для того, чтобы при выполнении практических работ не затрагивалась основная операционная система. Сервер размещается на виртуальной машине, установленной на главном компьютере, за которым работает преподаватель. При проведении практических работ преподаватель запускает сервер и поднимает на нем хосты, в типовом компьютерном классе 12 персональных компьютеров, на которых занимаются студенты, использование личных ноутбуков при работе с SIEM системой Wazuh не предусматривается, так как их нужно размещать как виртуальный хост в рамках одной локальной сети. Персональных компьютеров хватает на всех студентов, так как на практических занятиях они занимаются по подгруппам, количество реципиентов в которых не превышает 12 человек.

Для SIEM-системы Wazuh написано большое количество технической документации, которая размещена в свободном доступе в сети Интернет. Документация используется преподавателем как для настройки SIEM-системы, так и для разработки практических работ. Практические работы разрабатываются по вариантам таким образом, чтобы у студентов не было одинаковых вариантов. Кроме мониторинга вирусов студенты занимаются базовой настройкой SIEM-системы Wazuh путем удаленного подключения к серверу на виртуальной машине. Также они обучаются настраивать хосты для корректного взаимодействия с SIEM-системой, на встроенном синтаксическом языке учатся писать правила, позволяющие контролировать действия пользователей при работе в корпоративной сети и реагировать на подозрительные действия.

По каждой из изучаемых дисциплин, где предполагается использовать в качестве киберполигона SIEM-систему Wazuh, учебным планом предусмотрено 36 часов практических занятий, что

приравнивается к 18 практическим работам. В рамках дисциплины «Информационная безопасность» предполагается реализовать такие практические занятия, как:

1. установка и первоначальная настройка SIEM-системы Wazuh,
2. запуск агентов,
3. написание скриптов,
4. отслеживание активности пользователей,
5. нахождение подозрительных процессов,
6. проверка открытых портов,
7. написание правил.

Студентов, обучающихся по направлению подготовки 11.03.02 «Инфокоммуникационные технологии и системы связи» с профилем «Защищенные системы и сети связи» в рамках дисциплины «Комплексное обеспечение информационной безопасности инфокоммуникационных сетей и систем», предполагается обучить установке и настройке Wazuh как на локальном, так и на облачном серверах (в качестве облачного сервера будет использоваться сервер университета); установке и настройке агента и хостов Wazuh, а также корректному и безопасному запуску на компьютерах пользователей. Комплексно будет изучаться работа с менеджером Wazuh, который отвечает за анализ данных и рассылку оповещений.

В рамках дисциплины «Эксплуатация уязвимостей программного обеспечения» студенты будут изучать:

1. принципы централизованного сбора логов с конечных пользовательских устройств, приводить их к унифицированному формату;
2. визуализацию данных, обрабатываемых Wazuh, с разграничением по уровням опасности для корпоративной сети;
3. индексатор Wazuh, который является полнотекстовым поисковым и аналитическим движком в реальном времени для данных безопасности;
4. принципы работы с панелью Wazuh которая является центральным компонентом для анализа и визуализации данных безопасности.

В рамках дисциплины «Программно-аппаратные средства обеспечения информационной безопасности» предполагается обучать студентов написанию правил, которые позволяют реагировать на возникающие инциденты информационной безопасности, а в рамках дисциплины «Аналитика безопасности» – принципы работы с системой вторжений, принципы файлового мониторинга и обнаружения уязвимостей. Также будет изучаться интеграция SIEM-системы Wazuh с внешними сервисами, к примеру, VirusTotal, для автоматической загрузки и проверки подозрительного файла на наличие вредоносного кода. Отдельно будут изучаться принципы мониторинга целостности файлов при помощи специального предназначенного модуля.

В учебном плане вышеперечисленные дисциплины связаны и следуют друг за другом, что позволяет полноценно сформировать необходимые компетенции у обучающихся.

На рисунке 2 показан пример выполнения практической работы студентом по определению подозрительных активностей на рабочих машинах пользователей (активность генерируется преподавателем) и выведению активностей в удобное графическое представление. Активности отслеживаются благодаря агентам, размещенным на рабочих машинах пользователей. В рамках практической работы студент настраивает пользовательскую панель с результатами мониторинга, панель сохраняется в системе, и пользователь в любое время может просмотреть активности и определить, какие из них являются подозрительными.

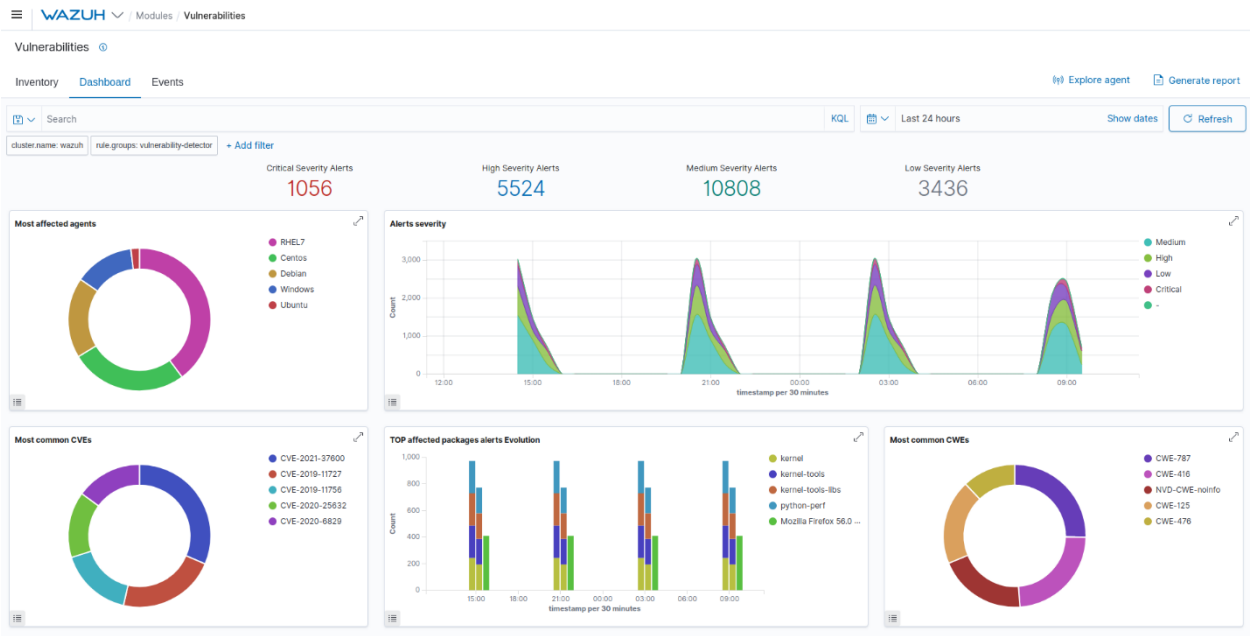

Рисунок 2. Настройка пользовательской панели Wazuh для выявления подозрительных активностей

В рамках данной практической работы студенты также занимаются написанием скриптов для корректного определения активностей, работают с библиотеками активностей.

Заключение

Применение SIEM-системы Wazuh в образовательном процессе позволит сформировать у обучающихся компетенции, которые в последующем реально используются в организациях, предоставляющих услуги по обеспечению информационной безопасности. Студенты получают практические навыки по настройке SIEM-системы, написанию правил, настройки системы оповещений, панелей управления. Кроме этого, студенты изучают синтаксис, который аналогичен другим системам мониторинга уязвимостей и активностей. Студенты обучаются нахождению угроз, уязвимостей в операционных системах и их последующему устранению.

Распространение опыта использования SIEM-системы Wazuh поможет другим ВУЗам занимающихся подготовкой специалистов по информационной безопасности обеспечить учебный процесс практическими работами. Лекционные занятия позволят изучить студентам понятия SIEM-систем и их основные цели и задачи, основные функции Wazuh. Практические занятия включающие групповые проекты, помогают развивать навыки командной работы, которые, несомненно, пригодятся в трудовом коллективе.

Практические сценарии, разработанные преподавателем, способствует пониманию студентами комплексного процессуального подхода к реагированию на киберугрозы возникающие в корпоративной локальной сети. В процессе обучения студенты получают доступ к различным ресурсам и сообществам, что способствует дальнейшему самостоятельному обучению и развитию интереса к кибербезопасности.

В ходе обучения студент правильно оценивает значение SIEM в современном мире, где ежедневно появляются новые угрозы безопасности, которые становятся всё более изощренными и опасными.

Сформированные знания и компетенции позволят студенту-бакалавру в последующем обеспечить себя работой и быстро акклиматизироваться при работе с SIEM-системами. Важным фактором при поиске работы является само обучаемость, которая также развивается в ходе прохождения обучения.

Список литературы

1. Анацкая А.Г. Формирование у студентов вуза компетенций в сфере управления информационной безопасностью в контексте профессиональных стандартов // Вестник СИБИТа. 2016. № 4(20). С. 120-127.
2. Гриншкун В.В., Димов Е.Д. Принципы фундаментального обучения студентов вузов технологиям защиты информации // Вестник МГПУ. Серия: Информатика и информатизация образования. 2013. №2 (26).
3. Джуракулов Т.Х., Петросян А.А., Логинова Л.Н. SIEM-системы управления событиями безопасности: обзор, анализ // Вестник науки и образования. 2022. № 8(128). С. 18-20.
4. Дудина Е.В., Колыванова Л.А., Чеканушкина Е.Н. Формирование профессиональных компетенций в области информационной безопасности как фактор успешной подготовки будущего специалиста // Известия Самарского научного центра Российской академии наук. Социальные, гуманитарные, медико-биологические науки. 2021. № 79-2. С. 194-201.
5. Кирсанов Д.Г., Айдинян А.Р. Эффективное обеспечение безопасности с помощью SIEM // Молодой исследователь Дона. 2024. № 3.
6. Королев И.Д., Попов В.И., Ларионов В.А. Анализ проблематики системы управления информацией и событиями безопасности в информационных системах // Инновации в науке. 2018. № 12(88). С. 19-26.
7. Перекотий З.А., Демкин Д.А. Роль SIEM-систем в информационной безопасности // Вестник науки. 2024. № 8(77). С. 166-169.
8. Цымбал Федор Алексеевич Управление инцидентами безопасности и событиями (SIEM) // Столыпинский вестник. 2022. № 4. С. 2121-2129.

The introduction of cyberpolygon into the educational process

Sergey V. Krivonogov
Senior Lecturer
Nizhny Novgorod State University of Engineering and Economics
Knyaginino, Russia
ksvkn@mail.ru
ORCID 0000-0001-7502-8014

Received 06.08.2024
Accepted 26.09.2024
Published 15.10.2024

UDC 004.946:37
DOI 10.25726/o3629-6381-3996-s
EDN QOZFUN
VAK 5.8.1. General pedagogy, history of pedagogy and education (pedagogical sciences)
OECD 05.03.HA. EDUCATION & EDUCATIONAL RESEARCH

Abstract

This article is dedicated to a detailed examination of the challenges faced by educational institutions in preparing students in areas related to information security. In today's world, where digital technologies have penetrated all spheres of life, information protection has become one of the key tasks for organizations and governments. Ensuring competent training of specialists in this field is critically important, but the training process is accompanied by a number of difficulties. Educational programs often lag behind the rapid development of technologies, and educators do not always have access to modern tools and resources. Students, in turn, need practical skills and real experience working with current security systems to be prepared

for professional challenges. All this creates the need to rethink approaches to education in the field of information security. An important aspect of modern information security is the use of SIEM (Security Information and Event Management) solutions in organizations. The article discusses in detail the relevance of implementing such systems in the corporate environment. SIEM systems allow for the collection, analysis, and correlation of security event data from various sources, significantly enhancing the efficiency of detecting and responding to incidents. A comparative analysis of existing solutions was conducted, showing that there is no ready-made solution for training students in security monitoring. The results of implementing a SIEM system into the educational process for bachelor's degree training are presented. Conclusions are drawn.

Keywords

information security, cyberpolygon, cybercrimes, competence approach, monitoring, student education, comparative analysis, security threats.

References

1. Anatskaya A.G. Formation of university students' competencies in the field of information security management in the context of professional standards // Bulletin of SIBITa. 2016. № 4(20). pp. 120-127.
2. Grinshkun V.V., Dimov E.D. Principles of fundamental education of university students in information security technologies // Bulletin of the Moscow State Pedagogical University. Series: Computer Science and Informatization of education. 2013. №2 (26).
3. Jurakulov T.H., Petrosyan A.A., Loginova L.N. SIEM-security event management systems: review, analysis // Bulletin of Science and Education. 2022. № 8(128). pp. 18-20.
4. Dudina E.V., Kolyvanova L.A., Chekanushkina E.N. Formation of professional competencies in the field of information security as a factor of successful training of a future specialist // Proceedings of the Samara Scientific Center of the Russian Academy of Sciences. Social, humanitarian, medical and biological sciences. 2021. № 79-2. pp. 194-201.
5. Kirsanov D.G., Aydinyan A.R. Effective security assurance using SIEM // Young researcher of the Don. 2024. № 3.
6. Korolev I.D., Popov V.I., Larionov V.A. Analysis of the problems of the information management system and security events in information systems // Innovations in science. 2018. No. 12(88). pp. 19-26.
7. Perekotiy Z.A., Demkin D.A. The role of SIEM systems in information security // Bulletin of Science. 2024. № 8(77). pp. 166-169.
8. Tsymbal Fedor Alekseevich Management of security incidents and events (SIEM) // Stolypin Bulletin. 2022. № 4. pp. 2121-2129.