МРНТИ 77.03.09 DOI 10.48501/2092.2023.14.10.004

[1]Асаубаев А.С., [1]Ахметова Ж.Ж.
[1]Евразийский национальный университет им. Л.Н.Гумилева
Казахстан, Астана
e-mail: zaure_nurgalieva@mail.ru

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И МАШИННОЕ ОБУЧЕНИЕ В SOAR

Аннотация
В статье рассмотрена необходимость автоматизирования и организации процессов, подключая различные инструменты с использованием API-интерфейсов конкретных поставщиков, чтобы дать аналитикам возможность исследовать и принимать решения, повышающие эффективность процессов реагирования на инциденты.
Ключевые слова: SOC, IDS, устройства SIEM, UTM, SOAR, API-интерфейс

[1]Асаубаев А.С., [1]Ахметова Ж.Ж.
[1]Л.Н.Гумилев атындағы Еуразия ұлттық университеті
Қазақстан, Астана
e-mail: zaure_nurgalieva@mail.ru

SOAR-да жасанды интеллект және машиналық оқыту

Аннотация
Мақалада талдаушыларға оқиғаға жауап беру процестерінің тиімділігін арттыратын зерттеуге және шешім қабылдауға мүмкіндік беру үшін нақты жеткізушілердің API интерфейстерін қолдана отырып, әртүрлі құралдарды қосу арқылы процестерді автоматтандыру және ұйымдастыру қажеттілігі қарастырылады.
Кілт сөздер: SOC, IDS, SIEM құрылғылары, UTM, SOAR, API-интерфейс

[1]Asaubaev A.S., [1]Akhmetova Zh.Zh
[1]L.N. Gumilyov Eurasian National University
Kazakhstan, Astana
e-mail: zaure_nurgalieva@mail.ru

Artificial Intelligence and Machine Learning in SOAR

Annotation
The article considers the need to automate and organize processes by connecting various tools using API-interfaces of specific suppliers in order to give analysts the opportunity to investigate and make decisions that increase the effectiveness of incident response processes.
Keywords: SOC, IDS, SIEM devices, UTM, SOAR, API interface

Введение.

Сегодня аналитикам SOC становится все труднее эффективно отслеживать и управлять текущими уровнями объема, скорости и разнообразия данных через брандмауэры, IDS и устройства SIEM. Это усугубляется тем фактом, что большинство средних и крупных организаций используют множество инструментов/продуктов безопасности для защиты своих данных, сети, конечных устройств и другой критически важной инфраструктуры. Кроме того, организациям не хватает единого инструмента безопасности, который мог бы удовлетворить все их потребности в обеспечении безопасности, и в конечном итоге они устанавливают несколько типов продуктов и инструментов от разных поставщиков, которые предоставляют различные услуги и решения для обеспечения безопасности.

Следовательно, необходимо автоматизировать и организовать процессы, подключая различные инструменты с использованием API-интерфейсов конкретных поставщиков, чтобы дать аналитикам возможность исследовать и принимать решения, повышающие эффективность процессов реагирования на

инциденты. SOAR является важнейшим компонентом смягчения угроз кибербезопасности, когда разрозненные инструменты интегрированы в общую платформу. Традиционно журналы безопасности отображаются на разных консолях с помощью разных устройств, таких как SIEM, UTM, решения Threat Intelligence (TI), решения Endpoint Detection and Response (EDR) и решения для песочницы, что утомительно и сложно для аналитиков SOC и экспертов по кибербезопасности отслеживать возникающие киберугрозы и атаки. Системы киберзащиты на основе ИИ/МО будут играть важную роль в реагировании на продолжающийся рост числа и сложности угроз, меняющийся характер угроз и потребность в быстром и в значительной степени автоматизированном реагировании на угрозы. Например, системы защиты на базе ИИ/МО способны анализировать большие наборы данных и мгновенно выявлять аномалии и подозрительные закономерности. Автоматические обновления существующего программного обеспечения на основе сложного анализа в реальном времени с помощью ИИ/МО могут предотвратить крупномасштабные кибератаки.

Реализация искусственного интеллекта и машинного обучения в SOAR решениях.

Были рассмотрены несколько лучших решений SOAR согласно Gartner [1] и другим источникам [3], такие как FireEye, IBM Resilient, Splunk, Demisto, DF Labs и т. д. Целью данной статьи было сравнить эти платформы на основе следующих возможностей SOAR: автоматизация, оркестровка, реагирование и то, как эти платформы используют ИИ/МО в процессах реагирования на инциденты. Существуют две структуры реагирования на инциденты, которые в основном используются в промышленности: структура NIST [4] и структура SANS [5]. Было принято решение сравнить уровни автоматизации, используя структуру реагирования на инциденты SANS PICERL (Планирование, идентификация, сдерживание, искоренение, восстановление и извлеченные уроки). В частности, мы сосредоточились на этапах выявления, сдерживания, искоренения и восстановления (ICER), поскольку в доступных источниках не обсуждалось, как эти платформы поддерживают этапы планирования и извлечения уроков.

Все решения безопасности SOAR включают внутреннюю и внешнюю TI в процессы реагирования на инциденты. Возможность автоматизации является основной функцией любой платформы безопасности SOAR, а автоматизация реализуется с помощью playbooks и runbooks [2]. Playbook — это линейный контрольный список шагов и действий (рабочих процессов), необходимых для успешного реагирования на определенные типы инцидентов и угроз. Схемы реагирования на инциденты представляют собой простой пошаговый нисходящий подход к оркестровке. Поскольку рабочие процессы являются ядром процессов автоматизации и оркестровки в решении SOAR, гибкость и простота использования одинаково важны. Напротив, модуль Runbook состоит из ряда условных шагов для выполнения действий, таких как обогащение индикатора, сдерживание угроз и отправка уведомлений, автоматически в рамках процесса реагирования на инциденты или операций безопасности. Runbook — это рабочие процессы, управляемые потоком, и они должны поддерживать различные типы механизмов управления потоком, в том числе те, которые позволяют аналитикам SOC принимать решения вручную, прежде чем рабочий процесс продолжится. Реализация этих рабочих процессов (playbook или runbook) должна быть достаточно гибкой, чтобы поддерживать практически любой процесс, который может потребоваться кодифицировать в рамках решения SOAR.

Мы рассмотрели уровни SOAR, приняв во внимание, какие этапы структуры ICER поддерживаются возможностью SOAR. Последнее важное соображение заключается в том, где и как ИИ/МО использовались этими платформами на этапах ICER структуры SANS. Все платформы SOAR поддерживают автоматизацию и управление на всех четырех этапах структуры SANS ICER. Основное различие, которое мы обнаружили, заключается в том, где и как ИИ/МО используется на платформах SOAR, как описано ниже.

Вендоры	TI	Идентификация	Сдерживание	Восстановление	ИИ/МО
FireEye	+	+	+	+	ICE
IBM Resilient	+	+	+	+	ICER
Splunk	+	+	+	+	ICER
Siemplify	+	+	+	+	ICER
D3 Security	+	+	+	+	ICER
DFLABS	+	+	+	+	ICER
Rapid7	+	+	+	+	ICER
ThreatConnect	+	+	+	+	ICE
Demisto	+	+	+	+	ICER
ATAR Labs	+	+	+	+	ICE
ServiceNOW	+	+	+	+	ICER

Таблица 1. ИИ/МО на платформах SOAR.

ИИ/МО по-разному используется на различных рассмотренных платформах SOAR. В FireEye реализован механизм обнаружения ML PowerShell для обнаружения атак PowerShell, и он способен успешно обнаруживать стандартные вредоносные программы, такие как Kovter и тесты на проникновение Red Team [2]. Кроме того, они разработали производственный сквозной конвейер машинного обучения, который постоянно развивается вместе с злоумышленниками путем перемаркировки и повторного обучения. Еще одним заметным применением ИИ/МО является MalwareGuard от FireEye, который использует модель ML для обнаружения и предотвращения вредоносных программ [1]. Платформа Siemplify SOAR использует машинное обучение, чтобы лучше расставлять приоритеты и исследовать предупреждения, а также назначать лучшего аналитика для решения проблемы. Во-вторых, машинное обучение постоянно анализирует и расставляет приоритеты в очереди дел аналитика, чтобы гарантировать, что аналитики будут решать критические дела в первую очередь. Он назначает более высокий приоритет случаям, которые напоминают те, которые исторически считались вредоносными, и назначает более низкий приоритет случаям, похожим на те, которые ранее были отмечены как ложные срабатывания. При назначении лучшего аналитика для дела алгоритмы машинного обучения используют показатели предыдущего аналитика, чтобы дать мгновенные рекомендации по назначению дела, чтобы максимизировать производительность и эффективность аналитика. Платформа Siemplify SOAR имеет возможность машинного обучения, которая также предоставляет список похожих случаев, которые аналитики могут использовать для помощи в их текущем расследовании на основе исторического контекста, чтобы сообщить ответные действия, которые они могут предпринять для своих расследований.

Заключение

Используя многие из ключевых функций внутри инструментов управления информационной безопасностью, автоматизации и реагирования, включая автоматизацию, интеграцию и сборники сценариев, организации могут решать и преодолевать все сложности, возникающие с ограниченным пулом специалистов по безопасности во всем мире. Наряду с тем, что SOAR помогает организациям получить большую отдачу от своей группы обработки инцидентов, SOAR сокращает время разрешения инцидентов с недель или месяцев до минут или часов после первоначального оповещения. В целом, инструменты SOAR помогают создавать наиболее эффективные и успешные группы реагирования на инциденты, доступные любой организации. Следующим большим шагом в усилиях по обнаружению, смягчению и предотвращению киберугроз является использование ИИ/МО на платформах SOAR. ИИ/МО будет действовать как множитель силы, расширяя возможности аналитиков SOC.

Литература

1. Gartner. (2017). “Cybersecurity scenario 2025: Outrageous intelligence,”.
2. A. Iyer. (2019). “Security orchestration for dummies,” Demisto Special Edition. Hoboken, NJ, USA: John Wiley & Sons, Inc.
3. R. Brewer. (2019). “Could SOAR save skills-short SOCs?,” Computer Fraud & Security, vol. 2019, no. 10, pp. 8–11.
4. NIST. (2012). “NIST SP 800-61, revision 2, Computer security incident handling guide,”.
5. SANS. (2011). “SANS incident handler’s handbook,”

References

1. Gartner. (2017). “Scenarij kiberbezopasnosti 2025: vozmutitel'nyj intellekt”.
2. A. Ajer. (2019). “Organizacija bezopasnosti dlja chajnikov”, special'noe izdanie Demisto. Hoboken, N'ju-Dzhersi, SShA: John Wiley & Sons, Inc.
3. R. Brjuer. (2019). “Mozhet li SOAR sohranit' navyki-korotkie SOC?”, Computer Fraud & Security, tom 2019, № 10, str. 8-11.
4. NIST. (2012). ”NIST SP 800-61, redakcija 2, Rukovodstvo po obrabotke incidentov komp'juternoj bezopasnosti".
5. BEZ. (2011). “Rukovodstvo dlja operatora BEZ incidentov”

Сведения об авторах

Ахметова Жанар Жумановна
Должность: PhD доктор, доцент кафедры «Информатика и информационная безопасность», ЕНУ им.Л.Н.Гумилева
Почтовый адрес: Республика Казахстан, г. Астана
E-mail: zaure_nurgalieva@mail.ru
Akhmetova Zhanar Zhumanovna
Position: PhD Doctor, Associate Professor of the Department of Informatics and Information Security, L.N.Gumilyov ENU
Postal address: Republic of Kazakhstan, Astana
E-mail: zaure_nurgalieva@mail.ru
Ахметова Жанар Жұманқызы
Лауазымы: PhD докторы, "Информатика және ақпараттық қауіпсіздік" кафедрасының доценті, ЕҰУ.Л. Н. Гумилева
Пошталық мекенжайы: Қазақстан Республикасы, Астана қ.
E-mail: zaure_nurgalieva@mail.ru

Асаубаев Аян
Должность: магистрант 2 курса ЕНУ им.Л.Н.Гумилева
Почтовый адрес: Республика Казахстан, г. Астана
E-mail: zaure_nurgalieva@mail.ru
Асаубаев Аян
Лауазымы: Л. Н. Гумилев атындағы ЕҰУ 2 курс магистранты.
Пошталық мекенжайы: Қазақстан Республикасы, Астана қ.
E-mail: zaure_nurgalieva@mail.ru
Asaubaev Ayan
Position: 2nd year master's student at L.N.Gumilyov ENU
Postal address: Republic of Kazakhstan, Astana
E-mail: zaure_nurgalieva@mail.ru