УДК 004.056.5

ШАБЛОНЫ ДЕТЕКТИРОВАНИЯ И КОРРЕЛЯЦИИ СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ ПРАКТИК MITRE ATT&CK

Солонович Т.И., студентка гр.961402

Белорусский государственный университет информатики и радиоэлектроники[1]

г. Минск, Республика Беларусь

Петров С.Н. – доцент кафедры ЗИ

Аннотация. Обеспечение информационной безопасности – одна из главных целей крупных организаций, осуществляющих хранение и обработку персональных данных. Для реализации перед сотрудниками стоят задачи проведения комплекса мероприятий по защите информации и IT-инфраструктуры предприятия. Существует большой спектр программных комплексов, которые предоставляют оптимальные инструменты для управления информационной безопасностью. Для корректного использования необходимо понимать принципы реализаций атак, пути их распространения, техники и тактики, используемые злоумышленниками. Методология MITRE ATT&CK содержит вышеперечисленную информацию, опираясь на которую, можно формировать и обрабатывать инциденты информационной безопасности. Их грамотная аналитика позволит снизить риски утечки информации, проникновения вредоносного программного обеспечения в корпоративную сеть или компрометации учетных данных сотрудников организации.

Ключевые слова. Информационная безопасность, SOC, риск, уязвимость, ERP, SGRC, IRP, SOAR, SIEM, ядро, коллектор, коррелятор, хранилище, инцидент, реагирование, анализ, правило корреляции, MITRE ATT&CK, тактика, техника, событие информационной безопасности, аутентификация.

В настоящее время наиболее актуальной практикой в сфере обеспечения информационной безопасности является организация Security Operation Center (далее SOC) [1].

SOC, или центр мониторинга информационной безопасности, – это команда квалифицированных специалистов в направлении кибербезопасности, которая занимается круглосуточным мониторингом состояния IT-инфраструктуры организации. Анализ событий и инцидентов позволяет снизить риски сбоев функционирования систем обеспечения безопасности, предотвратить угрозы и различного рода мошеннические действия (например, мошеннические действия в каналах дистанционного банковского обслуживания).

Для корректной аналитики нотификаций о потенциальных уязвимостях и фильтрации ложных инцидентов, а также реализации прочих задач, SOC должен включать множество программных решений.

Сюда можно отнести EDR (Endpoint Detection & Response) – класс решений для обнаружения и изучения вредоносной активности на оконечных устройствах: подключенных к сети рабочих станциях, серверах, устройствах Интернета вещей и так далее.

Системы SOAR (Security Orchestration, Automation and Response) предназначены для оркестровки систем безопасности, их координации и управления ими. Threat Intelligence предоставляет информацию об актуальных угрозах, что позволяет организациям изучить цели, тактики, векторы атак и инструменты злоумышленников для выстраивания эффективной стратегии защиты.

SGRC (Security Governance, Risk Management and Compliance) обеспечивает управление информационной безопасностью на основе рассмотрения вопроса информационной безопасности на высшем уровне руководства организации (Governance), управления рисками (Risk), а также в соответствии с требованиями различных нормативных документов (Compliance).

IRP (Incident Response Platform, «платформа реагирования на инциденты») является программным продуктом, предназначенным для автоматизации реагирования на киберинциденты. Данная функция реализуется посредством составления сценариев (плейбуков) с последовательностью стандартных действия при возникновении угрозы информационной безопасности для дальнейшего автоматического выполнения, что позволяет оптимизировать процесс реагирования.

Однако, одним из главных программных решений, используемых для построения SOC, является система обработки логов Security Information and Event Management (далее SIEM).

SIEM система [2] позволяет получать события из различных источников с помощью агентов, отправлять их в хранилище, обрабатывать через шаблоны детектирования и корреляции, также анализировать инциденты в режиме реального времени и обеспечивать оперативное реагирование.

Примерами таких решений являются системы MaxPatrol SIEM (Positive Technologies), Argsight SIEM (Micro Focus), Kaspersky Unified Monitoring and Analisys (Kaspersky).

Архитектурно программа имеет ядро (для управления настройками компонентов системы), коллекторы (для получения событий из источников, парсинг, нормализацию, фильтрацию, агрегацию), хранилище (для регистрации нормализованных событий и оповещений) и корреляторы (для анализа нормализованных событий и создания оповещений в соответствии с правилами корреляции). Архитектура SIEM системы представлена на рисунке 1.

Рисунок 1 – Архитектурное представление SIEM системы

SIEM система ежедневно генерирует большое количество уведомлений и чем больше организация, тем больше этот поток. В данном случае, колоссальный переизбыток информации может привести к тому, что многие из них могут игнорироваться. Во избежание этого информация должна корректно обработана и передана аналитикам для детального разбора.

Правила корреляции позволяют коррелировать события и формировать оповещения аналитикам SOC для анализа и оперативного принятия мер по предотвращению развития угрозы. Они составляются на основе методологий и тактик MITRE ATT&CK [3]. Данная база знаний содержит техники, которыми зачастую пользуются злоумышленники, описание и категоризацию их действий, а также ряд вредоносного инструментария, тем самым позволяя решать ряд задач информационной безопасности, в том числе расследовать киберинциденты.

Необходимо понимать, какие тактики и техники используются хакерами при выполнении атак и как они могут быть обнаружены. На основе базы знаний MITRE ATT&CK можно составить список типичных событий, которые могут указывать на наличие атаки или нарушения безопасности в системе. После того, как определены типичные события, необходимо определить, какие из них могут быть коррелированы друг с другом. Например, возможно, что событие блокировки учетной записи пользователя может быть связано с другим событием, указывающим на подозрительную активность в этой учетной записи.

Угрозы описаны принципом набора TTP, который расшифровывается как Tactics-Technique-Procedure (или Тактика-Техника-Процедура). Под тактикой понимается то, как злоумышленник действует на разных этапах своей операции, какая цель или задача злоумышленника на определенным шаге. Техника включает информацию о том, как злоумышленник достигает цели или поставленной задачи, какие использует инструменты, технологии, код, эксплоиты, утилиты. Процедура – действия, по выполнению этой техники выполняется и ее целевое назначение.

Каждая из матриц отражает техники определенного этапа атаки и ее нацеленность:

1 PRE-ATT&CK – TTP, отражённые в данной матрице, используются злоумышленниками непосредственно на стадии подготовки к атаке, например, сканирование, инвентаризация сети или социальная инженерия;

2 Enterprise – данная матрица отражает TTP, которые используются для атак на организации;

3 Mobile – TTP, связанные с переносными устройствами;

4 ATT&CK for ICS – включает в себя TTP, направленные на индустриальные системы.

Так, аномалии аутентификации можно отследить по правилам корреляции, опираясь на тактику TA0008 Lateral Movement. На основании техники T1078 Valid Accounts и анализа риска M1026 Privileged Account Management, можно составить правило реагирования на интерактивный вход под привилегированной учётной записью для операционной системы Windows, механизм которого позволит обнаружить вход как с использованием клавиатуры, так удаленные подключения по протоколу RDP. Для этого необходимо настроить фильтр на события типа 4624, со значениями типа входа Logon Type 2 (пользователь успешно вошел в систему на данном компьютере), 10 (пользователь выполнил вход в систему на этом компьютере через службы терминалов или удаленного рабочего стола.) и 11 (пользователь выполнил вход в систему на этом компьютере с сетевыми учетными данными, которые хранились локально на компьютере. Контроллер домена не использовался для проверки учетных данных.). Для корректной работы правила должен быть привязан список привилегированных учетных записей и признак, по которому их можно распознать. Одним из таких признаков может быть значения поля имени пользователя, которое содержит, например, символы “svc” (от “service”), “sa” (от “service account”), “adm” (от “admin”).

Таким образом, опираясь на конкретную тактику TA0008 Lateral Movement было смоделировано правило, которое генерирует оповещения в SIEM системе при наличии событий формата, отраженного на рисунке 2. Оперативный анализ оповещений и реагирование позволит предупредить намеренные вредоносные действия, произведенные под привилегированными учетными данными.

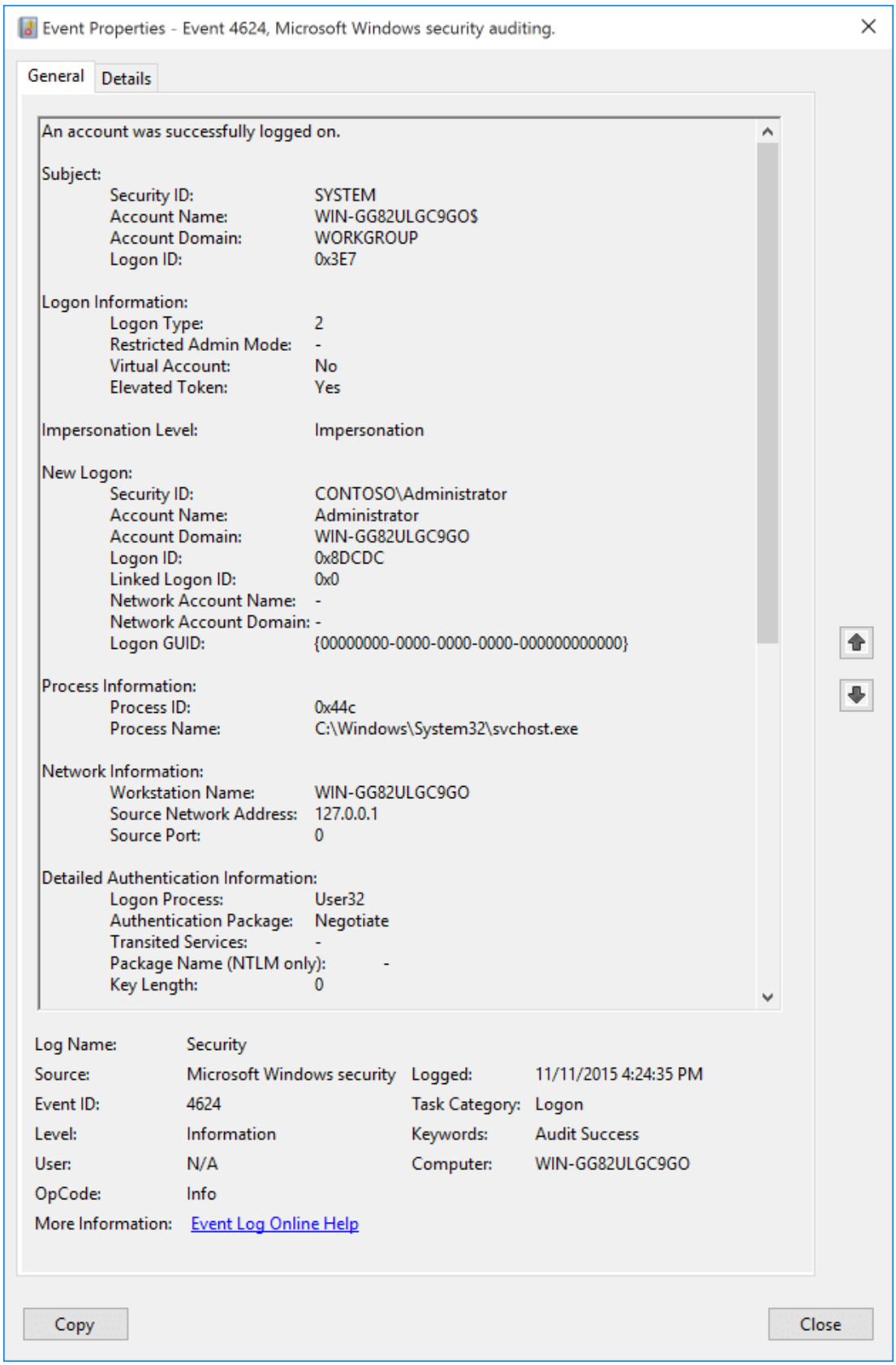

Рисунок 2 – Событие интерактивного входа под привилегированной учетной записью

Методология MITRE ATT&CK позволяет формировать пути реализации и вектор атаки, использовать наборы TTP при моделировании угроз и на основании этого формировать правила

обработки логов, связанных с доступом к учетным записям, обходом защитных мер, повышением привилегий, запуском исполняемых файлов и скриптов, сканированием и сбором данных сети.

Созданные шаблоны мониторинга на основе MITRE ATT&CK могут быть дополнены, тестированы и обновлены со временем, учитывая новые тактики, техники и IOC, появляющиеся в киберугрозах. Регулярное тестирование эффективности шаблонов и их обновление может помочь. Мониторинг реального времени может помочь определить, какие события коррелируются, и какие могут потенциально приводить к ложным срабатываниям.

Список использованных источников:

1. Security Operation Center [Электронный ресурс]. – https://www.securityvision.ru/blog/soc-chto-eto/. – Дата доступа: 0104.2023

2. SIEM система [Электронный ресурс]. – https://encyclopedia.kaspersky.ru/glossary/siem/. – Дата доступа: 01.04.2023

3. MITTRE ATT&CK [Электронный ресурс]. – https://attack.mitre.org/. – Дата доступа: 01.04.2023

UDC 004.056.5

PATTERNS OF DETECTION AND CORRELATION OF INFORMATION SECURITY EVENTS BASED ON MITRE ATT&CK PRACTICES

Solonovich T.I., student gr.961402

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Petrov S.N. – PhD, associate professor

Annotation. Ensuring information security is one of the main goals of large organizations that store and process personal data. For implementation, employees are faced with the task of carrying out a set of measures to protect information and IT infrastructure of the enterprise. There is a wide range of software systems that provide optimal tools for information security management. For correct use, it is necessary to understand the principles of attack implementations, ways of their distribution, techniques and tactics used by attackers. The MITRE ATT&CK methodology contains the above information, based on which it is possible to generate and process information security incidents. Their competent analytics will reduce the risks of information leakage, penetration of malicious software into the corporate network or compromising the credentials of employees of the organization.

Keywords. Information security, SOC, Risk, Vulnerability, ERP, SRC, IP, STAR, SIM, Core, Collector, Correlator, Storage, Incident, response, analysis, correlation rule, MITRE ATT&CK, Tactics, Technique, Information security event, authentication.