УДК 004.056
DOI: 10.31673/2409-7292.2021.041421

Рижков Д.О., Поляков Д.А., Рабчун Д.І.

СТРУКТУРА ЦЕНТРУ УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ НА БАЗІ РІШЕННЯ MICROFOCUS ARCSIGHT

Досліджено та удосконалено організаційні та технологічні підходи, що пов'язані із підготовкою до впровадження важливих інструментів та підготовкою фахівців. Дістало подальший розвиток і аргументацію необхідності постійної перевірки стану захищеності корпоративної інформаційної системи, рівень підготовки фахівців і проведення лікнепу та перевірку усвідомленості кінцевих користувачів.

Ключові слова: корпоративна інформаційна система, кібербезпека, центр управління кібербезпекою, SIEM система.

Вступ

Сучасні тенденції у сфері кібербезпеки демонструють, що кількість та рівень критичності загроз у всесвітній мережі безперервно зростає, а кількість атак постійно збільшується. Заходи із забезпечення інформаційної безпеки потребують запровадження суттєво нових рішень. Вже недостатньо використання одних лише налаштувань на мережевому обладнанні, IPS системах та файрволах та недостатньо використання антивірусів з їх не завжди актуальними базами сигнатур, що не виявляють загроз принципово нового покоління. Ситуація потребує свіжого погляду на вирішення проблеми [1].

Не дивлячись на високу актуальність питання забезпечення інформаційної безпеки, велика кількість підприємств досі не має власних підрозділів ІБ. Відповідними питаннями займаються недостатньо компетентні співробітники, що зазвичай не мають уяви про реальний стан речей у галузі. Заходи, які застосовувалися раніше, зараз є недостатніми і являють собою лише базовий підхід. Будь-які заходи застосовуються за фактом виявлених інцидентів та атак, що вже вразили цільову систему. Відсутність проактивних засобів не дає змогу забезпечити належний рівень безпеки, більше того, у персоналу немає уяви про те, як себе поводить внутрішня мережа та пристрої у ній [2].

Вирішуючи задачі із забезпечення необхідного рівня реактивних та проактивних методів захисту, організації приходять до розуміння необхідності появи власних центрів управління кібербезпекою, або ж звертаються до MSSP, які надають відповідні послуги [3]. Однак одного лише розуміння недостатньо, адже планування та впровадження відповідних заходів потребують дуже серйозної підготовки та побудови чіткої стратегії, яка має враховувати і оцінювати власні можливості, а також усвідомлення кінцевої мети у функцій, які виконуватиме майбутній кіберцентр. Успіх будь-якого кіберцентру полягає у чіткій злагодженій взаємодії досвіду та знань людей і переваг та можливостей технологій.

Аналіз проблеми побудови раціональної структури центру управління кібербезпекою

Зазвичай SOC складається с декількох окремих груп для розмежування обов'язків у середині команди [4]. Для пріоритезації подій існує окрема група аналітиків, які виконують відповідні задачі в режимі реального часу, а також розбирають телефоні дзвінки та звернення електронною поштою від користувачів та займаються іншими рутинними завданнями. Ця група часто згадується як Перша(1-а) Лінія. Якщо фахівець 1-ої лінії визначає, що подія досягла встановленої заздалегідь критичної межі, тоді створюється кейс (англ. case), який перекладається на Другу (2-у) Лінію. Цей поріг може бути визначений в залежності від різних типів потенційної «небезпеки» (типу інциденту, атакованого активу або інформації, порушеного процесу і т.д.). Як правило, період часу, протягом якого 1-а Лінія має опрацювати кожну подію, що представляє інтерес, триває від 1 до 15 хвилин. Його довжина залежить від політики ескалації SOC, кількості аналітиків, обсягу подій та розміру компанії, в якій знаходиться SOC або для якої надаються відповідні послуги. Співробітникам першої лінії не рекомендується виконувати поглиблений аналіз, оскільки вони не повинні

відволікатися від обробки подій, що надходять в режимі реального часу. Якщо для оцінки події потрібно більше кількох хвилин, воно буде переведено на Лінію 2 [5].

2-а Лінія отримує події від 1-й Лінії і виконує поглиблений аналіз, щоб визначити, що відбулося насправді (наскільки це можливо при наявних тимчасових ресурсах та інформації) і чи потрібні подальші дії. Для визначення масштабу і тяжкості події може знадобитися кілька тижнів для збору і перевірки всіх необхідних даних. Оскільки Лінія 2 не відповідає за моніторинг в режимі реального часу і складається з більш досвідчених аналітиків, її співробітники можуть витратити більше часу на повноцінний аналіз кожного набору дій, щоб отримати додаткову інформацію та затвердити варіанти вирішення. Зазвичай Лінія 2 (або вище) відповідає за підтвердження факту виникнення інциденту.

За усією цією «еталонною» схемою працюють далеко не всі центри кібербезпеки. Здебільшого вона застосовується у компаніях, в яких надання послуг із інформаційної безпеки та зокрема SOC-as-a-serice(SOCaaS) є основним бізнес процесом. Усі кроки із проведення моніторингу, виявлення, пріоритизації, ескалації та вирішення зазвичай окреслюються окремо серед фахівців окремого SOC. Все зазвичай залежить від розміру підприємства, кількості фахівців, наявних інструментів та досвіду фахівців. Не рідко, коли усі вище зазначені задачі можуть виконуватися одним й тим же аналітиком і, в залежності від ситуації, може залучатися більша кількість фахівців із різною специфікою. Деякі SOC виконують поглиблений аналіз і реагування в рамках 2-й Лінії. Інші передають деякі з цих функцій на третю лінію. На рисунку 1 представлені типові шляхи ескалації інциденту і ключові ролі в SOC [6].

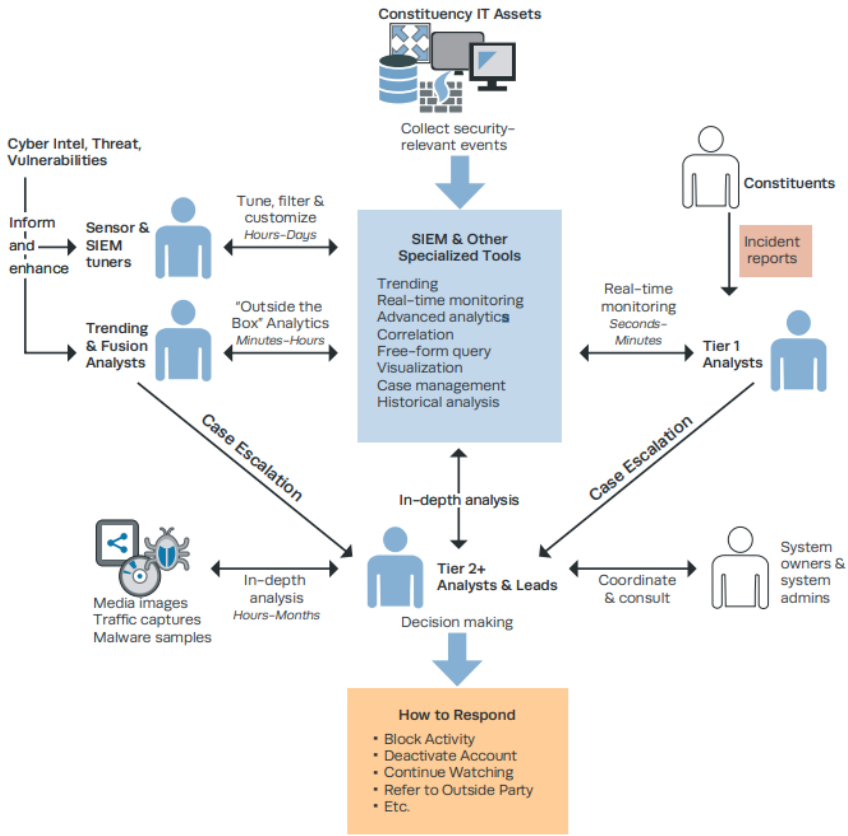

Рис. 1. Розподіл ролей та ескалація інцидентів в SOC

Мета роботи: розробити варіант технології побудови центру управління кібербезпекою на базі рішення Microfocus ArcSight та рекомендації по її застосуванню.

Технології та інструменти центру управління кібербезпекою

На будь-який центр управління кібербезпекою покладається низка специфічних задач із захисту мережі та інформаційних активів підприємства. Звісно, що проводити моніторинг та реагувати на загрози не можливо без спеціальних інструментів. У сфері інформаційної безпеки існує безліч різноманітних та вузькоспеціальних програмних та апаратних комплексів, що створені для покращення стану безпеки у різних аспектах.

Комерційний ринок представлений великим різноманіттям рішень із збору та аналізу даних. З точки зору саме SIEM систем серед найпоширеніших є Microfocus Arcsight ESM, IBM Qradar, Splunk Enterprise Security, LogRhythm SIEM, McAfee ESM та багато інших. Відомі також і open-source рішення такі як Elastic Search, у тандемі з інструментами LogStash та Kibana він стає доволі серйозним засобом моніторингу подій та пошуку інцидентів, однак, на відміну від багатьох комерційних систем, цей тандем ELK доволі довго та складно налаштовувати і він не зможе забезпечити вас достатнім початковим рівнем аналітики «з коробки». У даній роботі прикладом будуть системи платформи Arcsight від розробника Microfocus, а саме: ESM, Logger, Management center та Arcsight SmartConnector [7].

Аналіз можливостей платформи Arcsight

ArcSight Enterprise Security Management (ESM) – це комплексне програмне рішення, яке поєднує традиційний моніторинг подій безпеки з мережевою розвідкою, кореляцією подій, виявленням аномалій, інструментами аналізу та автоматичним виправленням. Це багаторівневе рішення, яке забезпечує інструментами аналітиків мережевої безпеки, системних адміністраторів та бізнес-користувачів. ESM включає в себе Корреляційний механізм оптимізованого зберігання та отримання (CORR), засіб зберігання та пошуку даних, який отримує та обробляє події з високою швидкістю та виконує високошвидкісний пошук.

Рисунок 2 ілюструє схему користувачів у ESM та ,залежно від його ролі, до якої документації він має звернутися для отримання інформації про свою діяльність [8].

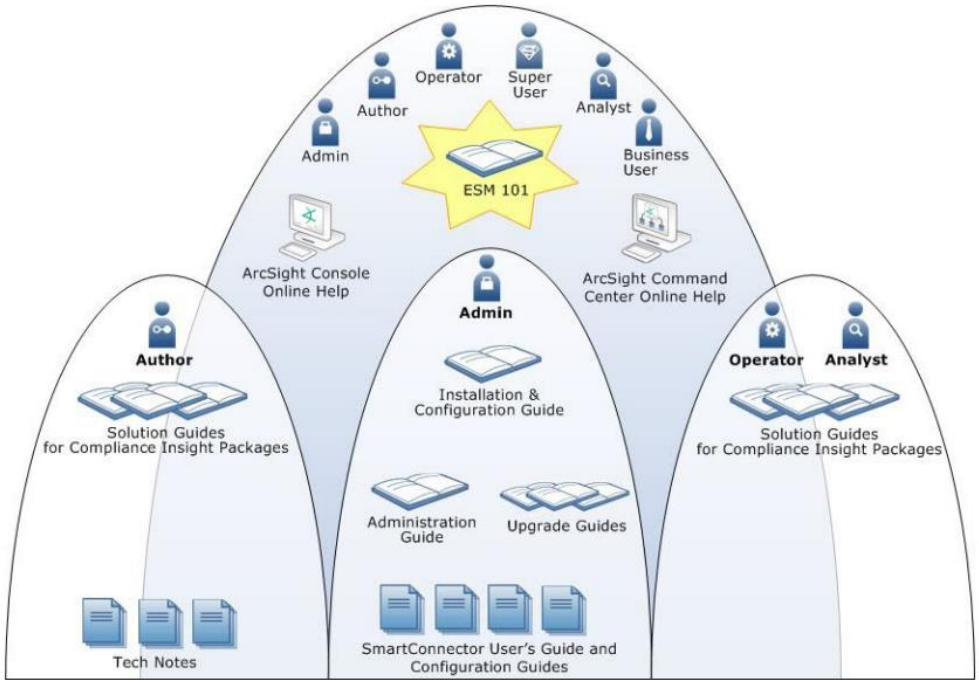

Рис. 2. Ролі користувачів ArcSight ESM

ESM збирає, нормалізує, агрегує та фільтрує мільйони подій з тисяч пристроїв у мережі в керований потік, який пріоритизований за ризиком, вразливостями та критичностю відповідних пристроїв. Потім ці події можуть бути скорельовані, досліджені, проаналізовані

та усунені за допомогою вбудованих інструментів ESM, надаючи ситуаційну обізнаність та час реагування на події в режимі реального часу. Ядром усього ESM є служба ArcSight Manager (рис. 3). Це сервер на основі Java, який керує аналізом, робочими потоками та іншими сервісами. Він також корелює дані із широкого спектру систем безпеки [9].

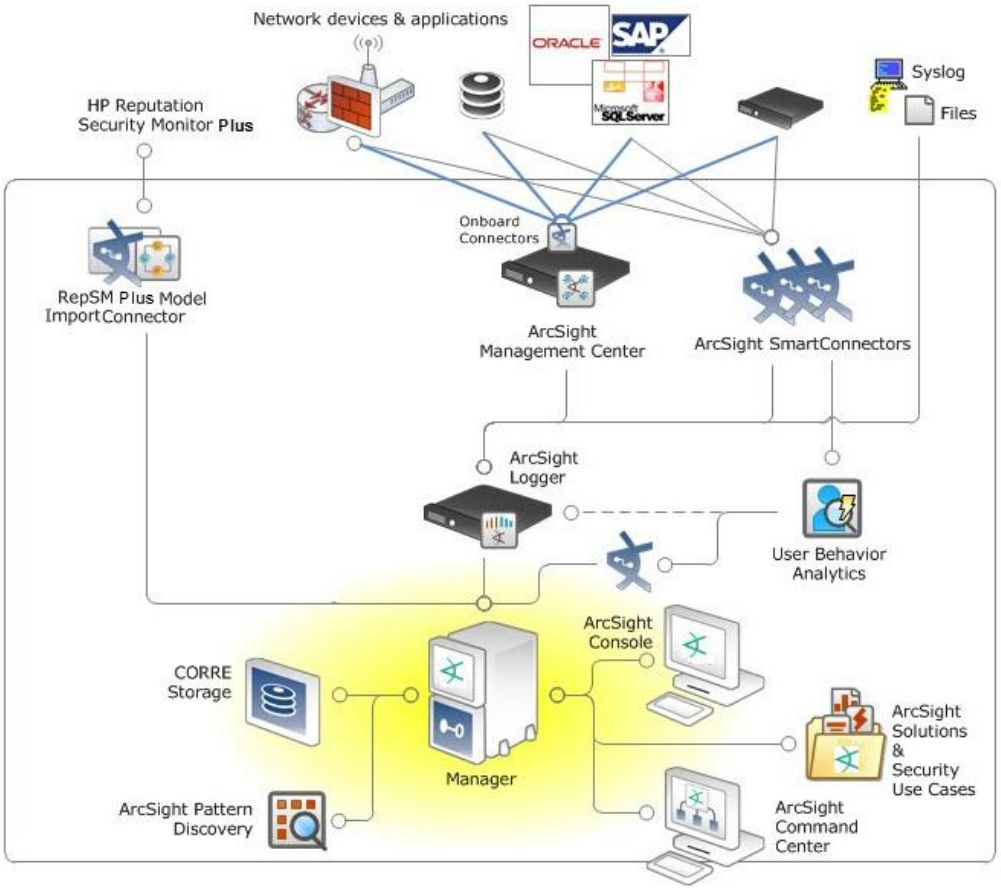

Рис. 3. Архітектура ArcSight

Життєвий цикл події у Arcsight ESM

ESM обробляє події поетапно, щоб ідентифікувати та реагувати на події, що представляють інтерес. На рисунку 4 нижче наведено огляд основних етапів життєвого циклу події. Джерела даних генерують тисячі подій. SmartConnectors, розміщені окремо або частково в ArcSight Management Center, розкладають для використання у схемі подій ESM. Кожен крок звужує кількість подій до тих, які викликатимуть інтерес [10].

Після звуження потоку подій ESM надає інструменти для моніторингу та дослідження подій, що представляють інтерес, відстеження та ескалації ситуацій, що розвиваються, а також аналізу та звітування про інциденти. Далі події зберігаються та архівуються відповідно до тих політик, що були встановлені встановлених під час налаштування.

Збір та обробка подій

Ця відповідна стадія є першим етапом життєвого циклу події, що здійснюється за допомогою SmartConnector. Це свого роду канал, по якому події надходять у ESM від пристроїв. Він визначає кінцеві точки, представлені в події в мережевій моделі, а також виконує перший рівень тегування подій. SmartConnectors також можуть застосовувати перший рівень фільтрації та агрегування подій, щоб зменшити обсяг потоку подій, щоб у свою чергу зробити обробку подій швидшою та ефективнішою (рис. 5) [11].

Джерело даних на у мережі генерує події, які збирає ArcSight SmartConnector. Конектор нормалізує дані у схему ESM, пов’язує із категоріями подій і шукає зони та атрибути користувача, налаштовані у мережевій моделі ESM. Можна налаштувати SmartConnector для фільтрації та агрегації подій, щоб зменшити обсяг потоку подій [12].

Збір подій – це процес збору інформації з пристроїв у інформаційній системі. Пристрої можуть бути основними (наприклад, брандмауер або IDS) або концентратором (наприклад, службою syslog, Symantec SESA або SiteProtector), який збирає дані з кількох подібних основних пристроїв. Потім з цих джерел збираються події за допомогою ArcSight SmartConnectors.

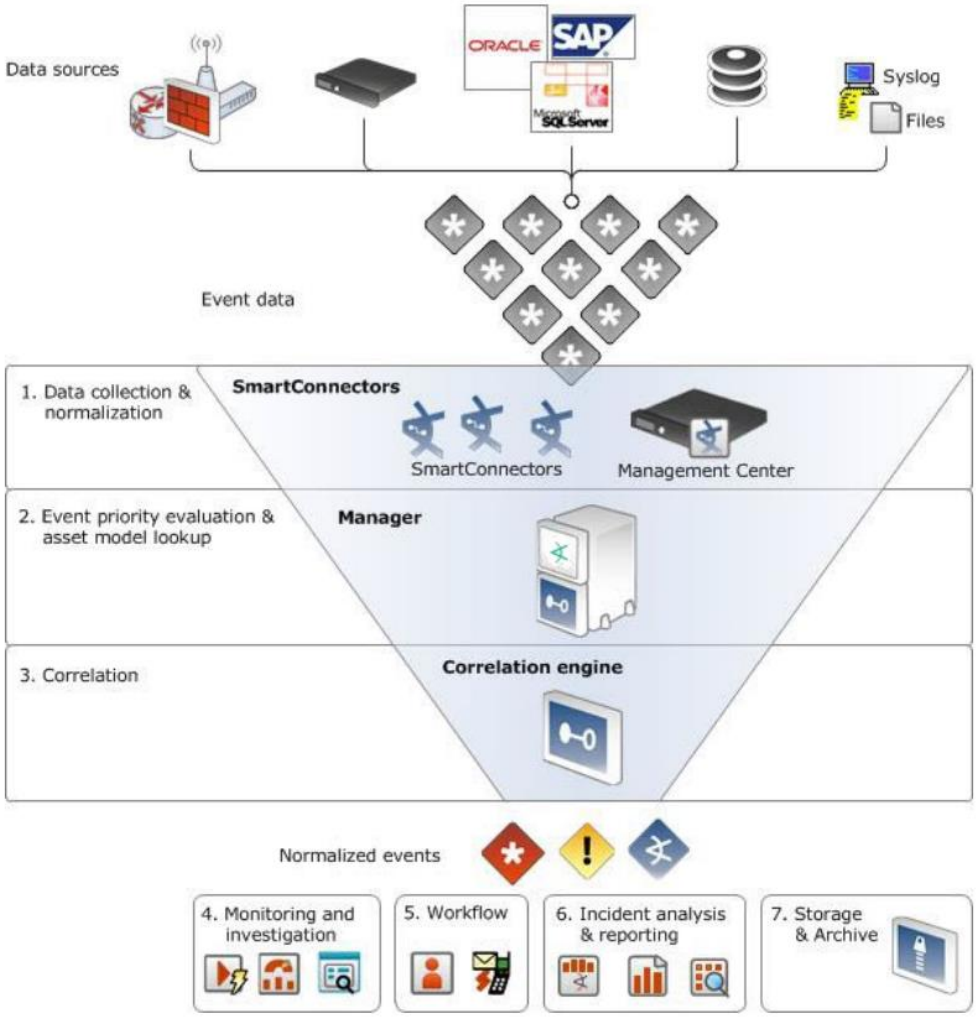

Рис. 4. Життєвий цикл події в ArcSight ESM

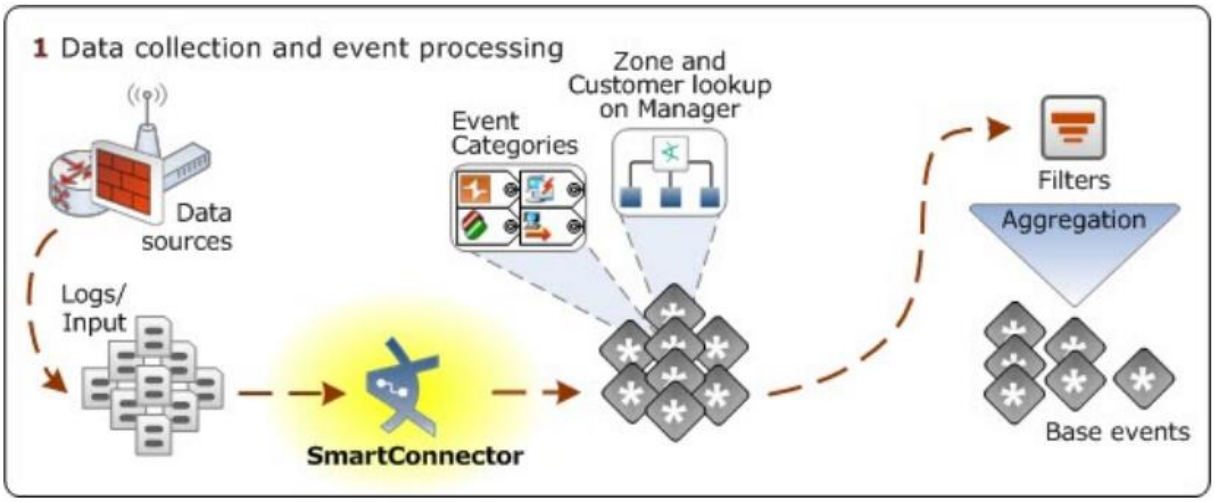

Рис. 5. Процес збору та обробки подій

Кореляція

Як тільки події проходять нормалізацію, визначаються за пріоритетами та визначаються їх кінцеві точки в мережевій моделі, вони обробляються механізмом кореляції, де відбувається оцінка загроз (рис. 6). Події з визначеними категоріями подій, пріоритетами та інформацією про мережеву модель, потім обробляються механізмом кореляції, де фільтри, правила та монітори даних з'єднують точки, знаходять необхідні події та можуть ініціювати негайну реакцію на них [13].

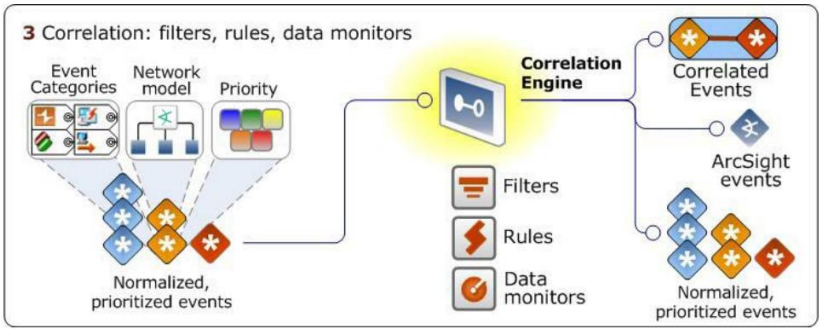

Рис. 6. Процеси кореляції у Arcsight ESM

Мережева активність, що може представляти інтерес, часто представлена кількома подіями. Кореляція – це процес, який виявляє взаємозв'язки між подіями, визначає значення цих відносин, визначає їх пріоритетність, а потім забезпечує основу для дій.

Контекст для кореляції забезпечує мережева модель. Фаза виявлення здійснюється за допомогою правил, кореляційних дата моніторів та детектора загроз. Висновки та дії здійснюються за правилами. Пріоритет визначається формулами пріоритетів ESM.

Кореляція – це чотиривимірний процес, який спирається на мережеву модель, пріоритизацію та детектор загроз, щоб виявити, вивести значення, визначити пріоритети та реагувати на події, які відповідають певним визначеним параметрам.

Моніторинг та аналіз

Процеси нормалізації та кореляції ESM дозволяють Центрам кібербезпеки отримувати інформацію про ситуацію в реальному часі, щойно подія відбулася. Засоби ESM для моніторингу та розслідування дозволяють відстежувати інциденти в процесі їх розвитку та детально аналізувати походження події, бачити інші задіяні системи та розуміти вплив на інші процеси у мережі. Можна відстежувати та досліджувати події за допомогою активних каналів, інформаційних панелей (дешбордів) та переглядачів запитів [14].

Інформаційні панелі – це ідеальний спосіб переглянути дані про події у мережі у різноманітних статистичних поданнях. Вони забезпечують безліч різних способів візуалізації, а також аналізу потоку подій (рис. 7).

У наведеному нижче прикладі показано стандартну інформаційну панель моніторингу міжмережевих екранів, яка відображає дані зразків мережевої активності. Він показує безліч моніторів даних, які разом надають дані про мережеву активність зсередини та зовні корпоративної мережі з різних ракурсів. Є можливість детально розглянути елементи, що відображаються на інформаційній панелі, щоб дослідити їх деталі.

Після того, як події обробляються Менеджером та зберігаються в базі даних, можна виконати ряд пакетно-орієнтованих функцій, які використовують модель подій ESM для аналізу інцидентів, пошуку нових моделей та формування звітів про діяльність системи [15].

Звіти – це захоплені подання або зведення даних, які можна роздрукувати або переглянути в консолі ArcSight або засобі перегляду ArcSight Command Center у різних форматах. Модульний підхід ESM до створення, запуску та ведення звітів спрощує створення більш складних багатоелементних звітів. Звіт пов'язує один або кілька запитів із шаблоном звіту. Запити можуть збирати дані з трендів, списків сеансів та активних списків.

На додаток до звітування про дані про події, звіти також можуть узагальнювати дані з кейсів, сповіщень та мережевих активів.

Рис. 7. Інструментальна панель моніторингу між мережевих екранів

Звіт пов'язує одне або кілька джерел даних із шаблоном звіту та встановлює вихідні атрибути, такі як формат файлу, розмір паперу, обмеження рядків та обмеження часового поясу. На вкладці звітів також можна застосувати фільтри та встановити графік формування звіту. Після створення звіту його можна запустити вручну, запланувати автоматичний запуск через рівні проміжки часу або запустити дельта-звіт, щоб порівняти результати одного звіту з іншим [16].

Кіберзагрози постійно розвиваються і з’являються нові та більш складні загрози. Для можливості протидії необхідне постійне поповнення новими технічними засобами, що забезпечить високий рівень виявлення та усунення загроз. Можливість інтеграції таких рішень із SIEM-системами із налаштуванням кореляційних правил забезпечить належний рівень проактивності..

Висновки

Проведено дослідження можливостей рішень Microfocus ArcSight у забезпеченні повноцінних процесів зі збору, аналізу та розслідування подій та інцидентів. Визначено цінність функцій ArcSight SmartConnector із можливості збору даних з різноманітних видів

систем джерел даних, а також їх здатність проведення повноцінного синтаксичного аналізу, який трансформує події у зрозумілий для людського ока формат. ArcSight ESM оснащено усіма необхідними засобами із проведення аналізу інцидентів, має в своєму складі механізм кореляції, завдяки якому можна обробляти великі масиви даних та виявляти з великої кількості подій саме ту, яка становить загрозу, при налаштуванні відповідних необхідних правил. Розроблено комплексні рекомендації із планування та впровадження процесів SOC. Визначено важливість розуміння цілей організації в цілом та SOC окремо, а також важливість їх взаємовигідної взаємодії.

Перелік посилань

1. М.П Войнаренко, О.М Кузьміна, Т.В. Янчук. Інформаційні системи і технології в управлінні організацією // Корпоративні інформаційні системи – Вінниця: ПП Едельвейс і К, 2015. – 496 с.
2. Carson Zimmerman. MITRE. “Ten Strategies of a World-Class Cybersecurity Operations Center”. The MITRE Corporation. 2014. – 346 с.
3. Committee on National Security Systems, “CNSS Instruction No. 4009,” Committee on National Security Systems, Ft. Meade, 2010
4. NIST, “Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, NIST SP 800-137,” September 2011. [Електронний ресурс] – Режим доступу: http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf.
5. Killcrece, Georgia; Kossakowski, Klaus-Peter; Ruegle, Robin; Zajicek, Mark, “Organizational Models for Computer Security Incident Response Teams,” December 2003. [Електронний ресурс] – Режим доступу: www.cert.org/archive/pdf/03hb001.pdf.
6. Joey Muniz, Gary McIntyre, Nadhem AlFardan. “Security Operations Center: Building, Operating and Maintaining your SOC”. Cisco Press. Release Date: November 2015
7. Jonathan Risto. “Vulnerability Management Maturity Model Part I”. SANS Institute. July 6, 2020. [Електронний ресурс] – Режим доступу: https://www.sans.org/blog/vulnerability-management-maturity-model/
8. Rob McMillan. “Definition: Threat Intelligence”. 16 May 2013. [Online]. Available: https://www.gartner.com/en/documents/2487216/definition-threat-intelligence
9. Brian Kime. “RSA Conference 2020: An Intelligence Nerd’s Shopping List”. 13 Feb 2020. [Електронний ресурс] – Режим доступу: https://go.forrester.com/blogs/rsa-conference-2020-an-intelligence-nerds-shopping-list/
10. Micro Focus Security. “ArcSight ESM. ESM 101”. July 2020. [Електронний ресурс] – Режим доступу: https://www.microfocus.com/documentation/arcsight/arcsight-esm-7.3/pdfdoc/ESM_101/ESM_101.pdf
11. Micro Focus Security. “ArcSight Connectors. SmartConnectorUserGuide. SoftwareVersion:8.1.0”. 2020. [Електронний ресурс] – Режим доступу: https://community.microfocus.com/t5/ArcSight-Connectors/ArcSight-SmartConnector-User-Guide-8-1-0/ta-p/1586784?nm=
12. Geoff Harmer. “Governance of Enterprise IT based on COBIT5”. IT Governance Publishing. February 2014. – 175 с.
13. Petr Hnevkovsky, Dmitriy Ryzhkov. “Microfocus Universe 2020. Next-Gen SOC and ArcSight customer story: Ukrenergo”. 18 March 2020. [Електронний ресурс] – Режим доступу: https://content.microfocus.com/virtual-universe-next-gen-soc/arcsight-success-krenergo?utm_campaign=vuod&_ga=2.229177500.1893095171.1599550486-1790801641.1579283751
14. Microfocus Security, Dmitriy Ryzhkov. “ArcSight ESM Case Study. NPC Ukrenergo”. May 2020. [Електронний ресурс] – Режим доступу: https://www.microfocus.com/media/case-study/npc-ukrenergo-cs.pdf
15. Microfocus Security. “Speed Up Security Operations with ArcSight SOAR”. September 2020. [Електронний ресурс] – Режим доступу: https://www.microfocus.com/media/flyer/speed-up-security-operations-with-arcsight-soar-flyer.pdf
16. Dmytro Ryzhkov. Security operations center: first steps to good performance / Рижков Д.О. // «Актуальні проблеми кібербезпеки» - 2020 -№3. – С.84-87.

Надійшла: 21.09.2021 Рецензент: д.т.н., професор Савченко В.А.