ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЯ ПОБУДОВИ ЦЕНТРУ УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ НА БАЗІ РІШЕННЯ MICROFOCUS ARCSIGHT»

Виконав: студент 6 курсу, групи БСДМ-61
Спеціальності 125 Кібербезпека
Освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Рижков Д.О.
(прізвище та ініціали)
Керівник Гахов С.О.
(прізвище та ініціали)
Рецензент _____
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.

КИЇВ – 2020

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Інститут ННІЗІ
Кафедра Інформаційної та кібенетичної безпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Г.І. Гайдур
"___" _____ 2020 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Рижкову Дмитру Олеговичу
(прізвище, ім'я, по батькові)

1. Тема магістерської роботи: «Технологія побудови центру управління кібербезпекою корпоративної інформаційної системи на базі рішення Microfocus ArcSight»
керівник магістерської роботи Гахов Сергій Олександрович, к.військ.н.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від «13» жовтня 2020 року № 230

2. Строк подання студентом магістерської роботи 15.12.2020р.

3.Вихідні дані до магістерської роботи
корпоративна інформаційна мережа;
центр управління кібербезпекою;
SIEM-система;
реагування на інциденти;
науково-технічна література, стандарти, рекомендації.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1. Аналіз сутності та концепції центрів управління кібербезпекою
2. Методи та засоби управління кібербезпекою, процеси і технології
3. Рекомендації з впровадження процесів центру управління кібербезпекою

5. Перелік графічного матеріалу

1. Тема.
2. Об’єкт, предмет дослідження, мета роботи, основні завдання
3. Актуальність центрів управління кібербезпекою
4. Концепція SOC
5. Ролі SOC та рівні ескалації інцидентів
6-9 Платформа Microfocus ArcSight
10-13. Процедура збору та аналізу подій. Конектор
14. Планування та стратегія
15. Розмежування обов’язків. Лінії SOC
16. Рекомендації
17. Висновки

6. Дата видачі завдання_____09.10.2020р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської роботи	Строк виконання етапів магістерської роботи	Примітка
1.	Аналіз науково-технічної літератури	09.11.2020р.	
2.	Аналіз концепції центрів управління кібербезпеки і забезпечення реактивних і проактивних заходів кібербезпеки	18.11.2020р.	
3.	Дослідження методів впровадження і розвитку процесів управління подіями та інцидентами	29.11.2020р.	
4.	Розробка рекомендацій із планування та впровадження центрів управління кібербезпеки	06.12.2020р.	
5.	Оформлення результатів роботи: Реферат, вступ, висновки.	08.12.2020р.	
6.	Підготовка доповіді та презентації до захисту	13.12.2020р.	

Студент _____ Рижков Д.О.
(підпис) (прізвище та ініціали)

Керівник магістерської роботи _____ Гахов С.О.
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Текстова частина магістерської роботи: 91 сторінка, 49 рисунків, 2 таблиці, 15 джерел.

Об'єкт дослідження – побудова та функціонування центрів управління кібербезпекою.

Предмет дослідження – технологія побудови центрів управління кібербезпекою на базі рішення Microfocus ArcSight.

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

Методи дослідження – опрацювання літератури за темою, аналіз найкращих практик та сучасних тенденцій, аналіз експлуатаційної документації, моделювання процесу впровадження технологій.

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.

Галузь використання – кібербезпека корпоративних інформаційних систем

КОРПОРАТИВНА ІНФОРМАЦІЙНА СИСТЕМА, КІБЕРБЕЗПЕКА, ЦЕНТР УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ, SIEM СИСТЕМА

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

Подія	–	будь-яка видима активність в системі або мережі
Інцидент	–	будь-яка подія, що негативно впливає на безпеку мережевих та інформаційних систем
Форензика	–	цифрова криміналістика та розслідування інцидентів
Парсинг	–	синтаксичний розбір
Комплаенс	–	відповідність будь-яким внутрішнім або зовнішнім вимогам або нормам
Лог	–	файли, що містять системну інформацію роботи сервера або комп'ютера, в які заносяться певні дії користувача або програми
Кореляція	–	статистичний взаємозв'язок двох або більше подій
SOC	–	Security operations center (Центр управління кібербезпекою)
SIEM	–	система управління подіями та інцидентами ІБ
Threat intelligence	–	розвідка кіберзагроз

ВСТУП

Актуальність теми: 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.

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.

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. 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.

Об'єкт дослідження: побудова та функціонування центрів управління кібербезпекою.

Предмет дослідження: технологія побудови центрів управління кібербезпекою на базі рішення Microfocus ArcSight.

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

Наукові завдання:

проаналізувати призначення та користь володіння SOC;

дослідити методи збору та аналізу подій у мережі, визначити практичні методи управління подіями та інцидентами;

дослідити можливості забезпечення повноцінної видимості та інформованості про події в мережі;

розробити рекомендації із планування, впровадження та розвитку процесів SOC.

Практичне значення одержаних результатів: Дана робота корисна для опанування функціоналу SIEM ArcSight ESM на достатньому початковому рівні, описані усі типи робіт такі як підключення джерел подій, проведення моніторингу аналітики засобами ESM, створення кореляційних правил, проведення роботи зі звітами та оформлення карток інцидентів (кейсів).

Надані в роботі рекомендації із побудови та розвитку SOC розбивають усі процеси на конкретні кроки із планування і впровадження процесів, поступове досягнення яких приводить до кінцевої цілі – побудови повноцінного централізованого SOC на базі організації.

Галузь застосування: кібербезпека корпоративних інформаційних систем

Апробація результатів: Dmytro Ryzhkov. Security operations center: first steps to good performance / Рижков Д.О. // «Актуальні проблеми кібербезпеки» - 2020 - №3. – С.84-87

1 АНАЛІЗ СУТНОСТІ ЦЕНТРУ УПРАВЛІННЯ ПОДІЯМИ КІБЕРБЕЗПЕКИ В КОРПОРАТИВНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ

1.1. Призначення, структура, функції та умови функціонування корпоративної інформаційної системи

Будь-яке сучасне підприємство, незалежно від розміру та виду діяльності, являє собою складну систему внутрішніх та зовнішніх інформаційних зв’язків. З часом, задля того, щоб належним чином зберігати, обробляти та передавати інформацію та поліпшувати виконання своїх бізнес-процесів, завдяки технічному прогресу, стало можливим автоматизувати свої процеси. У теперішній час починають розуміти всю важливість і необхідність комплексного підходу у забезпеченні таких рішень. Вже звичною є ідея побудови корпоративних інформаційних систем (КІС) стосовно не тільки великих, територіально розподілених інформаційних систем, але і будь-яких підприємств, незалежно від їх масштабу і форми власності. Організація, за наявності ресурсів, маючи одну невелику локальну мережу, через деякий час може розширитися і представляти із себе саморегулюючу систему, здатну гнучко і оперативно перебудовувати принципи свого функціонування, маючи в своєму активі інтеграцію великого числа програмних продуктів.

Корпоративна інформаційна система — це інформаційна система, яка підтримує взаємозв’язки між активами у мережі, автоматизацію усіх функцій на підприємстві (в корпорації) і поставляє інформацію для прийняття рішень. У ній реалізована ідеологія, яка об'єднує бізнес-стратегію підприємства і прогресивні інформаційні технології[1].

Сучасні КІС мають такі основні характеристики:

Масштабність. ІС повинна мати в своєму підпорядкуванні: сервери, операційні системи, системи комунікацій, системи управління базами даних та потребує значних зусиль спеціалістів з проектування і упровадження таких систем.

Робота в неоднорідному обчислювальному середовищі. Можливість роботи в мережах, до яких входять комп'ютери, сервери та інші пристрої, що працюють під управлінням різних операційних систем. При цьому має бути забезпечена взаємодія всіх операційних систем, які використовуються.

Розподілені обчислення. Це один із видів роботи в клієнт-серверній архітектурі, коли дані чи запити, які надходять з клієнтських машин розподіляються поміж кількома серверами, що збільшує пропускну здатність для користувача і дає можливість багатозадачної роботи. Це сприяє максимальному використанню обчислювальних ресурсів, зниженню витрат і підвищенню ефективності системи. Забезпечення розподіленої роботи — це обов'язкова вимога до інформаційних систем корпоративного рівня.

КІС повинна забезпечити інформаційну прозорість підприємства, формувати єдиний інформаційний простір який об'єднує інформаційні потоки, що існують у мережі.

Сьогодні, є звичним, що у мережі однієї установи використовуються робочі станції, сервери та інше обладнання одного типу, що були створені різними розробниками і мають абсолютно різні операційні системи та архітектуру. Поява кожного з пристроїв завжди зумовлюється його можливостями задовольнити конкретні потреби, наявністю потрібного функціоналу, під кожну задачу техніка, дуже часто, обирається окремо. Наприклад для користувачів, що працюватимуть переважно із офісними програмами та програмами обліку, зазвичай достатньо функціоналу, що може запропонувати ОС Windows, до того ж він є більш дешевим і максимально простим у використанні. Однак є категорія користувачів, що потребує більш складних, вузькоспеціалізованих програм та можливостей для виконання свої задач, як приклад: Mac OS підійде для графічних дизайнерів та ОС сімейства Linux для інженерів інформаційної безпеки. Це також трапляється із серверною частиною мережі, де домен-контролери часто встановлюються на сервери Windows, а інші сервіси благополучно функціонують на Linux-серверах або ж це зумовлено необхідністю підтримувати роботу ресурсів, що застаріли та не підтримуються розробником, а альтернативи досі не було знайдено.

З точки зору інформаційної безпеки, велика кількість пристроїв дорівнює кількості джерел інформації, що постійно циркулює у мережі. Кожен апарат реєструє та записує абсолютно усі свої дії у певному форматі, створюючи лог-файл, що може бути прочитаний для проведення аналітики. Ведення логів дає змогу ІТ-персоналу фіксувати усі дії того чи іншого пристрою, для того, щоб у випадку виникнення загрози прочитати дані про те, як себе поводила система, що з нею відбувалося, які були мережеві підключення та які служби або програми запускалися. Кожна така дія називається подією (англ. event). Кожна така подія, що несе загрозу інформаційній системі може бути перекваліфікована у інцидент.

Аби тій чи іншій події надати певної класифікації та визначити рівень її небезпечності необхідно зібрати усі дані, що до неї відносяться, з усіх пристроїв, які могли мати відношення до неї, після чого проводиться аналіз, оцінюється рівень загрози та проводяться заходи із усунення наслідків. Збирати інформацію з кожного пристрою окремо дуже складно і потребує часу, не менше часу знадобиться на проведення аналітичної роботи. З цієї причини згодом з’явились засоби, що збирають лог-файли із різних пристроїв-джерел та зберігають їх в одному місці для значного пришвидшення процедури збору даних. Однак, нажаль, на цьому не закінчуються усі складнощі, пов’язані із реагуванням на події та інциденти. Кількість даних і надалі залишається великою, а необхідність витрачення часу на їх сортування і аналіз все ще залишається актуальною. Автоматизація цих процесів можлива завдяки кореляції, що присутня у сучасних SIEM-системах.

Потоки інформації, що надходять від усіх пристроїв у корпоративній мережі збираються в одному місці, проводиться їх синтаксичний аналіз (парсинг) і виводиться зручну користувальницьку консоль для відповідно зручного аналізу даних, що надходять. Окрім того для SIEM-систем притаманна можливість кореляції події, тобто встановлення їх взаємозв’язку у результаті чого низка базових подій можуть сформувати одну скорельовану за тими чи іншими механізмами.

Окрім того наявні у мережі пристрої мають особливі ознаки – вразливості, які характеризуються нездатністю системи протистояти існуючим загрозам. Для вирішення питань захисту від вразливостей запроваджуються заходи із управління ними.

1.2. Концепція центрів управління кібербезпекою, їх задачі та діяльність

Центр управління кібербезпекою, більш відомий як SOC (англ. Security operations center) – централізований підрозділ установи, який вирішує питання з інформаційної та кібербезпеки на організаційному та технічному рівні. SOC — це об'єкт, де корпоративні інформаційні системи (веб-сайти, додатки, бази даних, центри обробки даних, сервери, активне мережеве обладнання, комп'ютери та інше кінцеве обладнання) контролюються, оцінюються та захищаються, а спеціалісти виконують відповідні задачі із захисту від несанкціонованої діяльності в комп'ютерних мережах, включаючи моніторинг, виявлення, аналіз (наприклад, аналіз трендів і патернів), реагування та відновлення.

Існує безліч варіацій назви таких центрів та команд спеціалістів, що займаються такою діяльністю. Окрім SOC можна зустріти абревіатури CIRT (англ. Computer Incident Response Team), CSIRT (англ. Computer Security Incident Response Team), CERT (англ. Computer Emergency Response Team) та ін.[2]. Від назви не змінюється головна суть – основна діяльність підрозділу полягає у реагуванні та попередженні кіберінцидентів. Однак, за деякими переконаннями поняття SOC та наприклад CSIRT розділяють у зв’язку із їх специфікою та деякою різницею у їх задачах. Наприклад існує думка, що підрозділам SOC притаманні задачі із інтеграції усіх безпекових систем моніторинг у системі SIEM та моніторинг подій з метою виявлення загроз, а CSIRT, у свою чергу реагують на загрози та усувають їх наслідки. У той же час, сучасні центри кібербезпеки прагнуть охоплювати все більше функцій і стають досить багатозадачними структурами і вдало поєднують у собі функції моніторингу і пошуку загроз та реагування на них із подальшим розслідуванням інциденту. Тому усі відповідні

структури можна позначати як SOC, тут і далі використовуватиметься саме ця назва.

Центри управління кібербезпекою можуть бути як невеликими і складатися із невеликої кількості спеціалістів так і можуть бути повноцінними галузевими або національними центрами і навіть можуть об’єднувати декілька, менших за розміром, центрів. Типовий SOC виконує такі задачі:

- Моніторинг, виявлення і аналіз потенційних загроз в режимі реального часу і через відстеження трендів із значущих джерел даних у галузі інформаційної безпеки.
- Запобігання інцидентів кібербезпеки, що включає в себе заходи:
  - Безперервний аналіз загроз;
  - Сканування мереж і пристроїв для пошуку вразливостей;
  - Координація заходів із протидії;
  - Розробка рекомендацій в області політики безпеки і безпеки систем.
- Реагування на підтверджені інциденти, координація ресурсів та контроль за використанням своєчасних захисних заходів, що відповідають виниклій ситуації.
- Надання відповідним організаціям актуальної інформації про поточну ситуацію, а також звітів про стан кібербезпеки, інциденти та тенденції в поведінці зловмисників.
- Розробка і управління засобами захисту комп'ютерних мереж, такими як системи виявлення та запобігання вторгнень (IDS/IPS) або системи управління подіями та інцидентами (SIEM-системи).
- Проведення внутрішніх аудитів стану кібербезпеки внутрішньої та зовнішньої мережі організації, так званих «тестів на проникнення» (англ. pentest).

Серед перерахованих обов'язків найбільш трудомісткими є обробка і аналіз великої кількості даних. Як правило, основним джерелом даних про стан безпеки, використовуваним SOC, є системи SIEM. Кожен аналітик постійно переглядає дані на інструментальних панелях(дешбордах) та проводить моніторинг потоків

подій у реальному часі з метою виявлення можливого інциденту. У свою чергу одним з найбільш пріоритетних наповнювачів даних для SIEM є системи IDS\IPS. Ці системи, розміщені на хості або в мережі, мають певні сигнатурні політики для виявлення потенційно зловмисної або небажаної активності, яка вимагає додаткової уваги аналітика SOC. У поєднанні з журналами аудиту безпеки і іншими каналами даних типовий SOC щодня збирає, аналізує і зберігає десятки або сотні мільйонів подій безпеки.

Сама подія (інформаційної безпеки) – це будь-яка видима подія в системі і/або мережі[3]. Іноді події вказують, на виникнення інциденту. Подія – це всього лише необроблені дані. Для встановлення та визначення подальших дій, потрібно провести додатковий аналіз – процес оцінки виділення значущої інформації з набору даних про стан безпеки, як правило, за допомогою спеціалізованих інструментів. Серед усіх потоків даних, що надходять, аналітик має визначити ті, що сповіщають про можливу небезпеку та визначити, на яку саме необхідно звернути увагу в першу чергу. Для цього існує поняття пріоритизації – процес сортування, категоризації та визначення пріоритетності вхідних даних і інших запитів на ресурси SOC.

Зазвичай SOC складається с декількох окремих груп для розмежування обов'язків у середині команди. 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.

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.

Деякі SOC також виділяють ресурси одного або декількох своїх відділів (іноді включаючи лінію 2) для пошуку всіх неструктурованих індикаторів інцидентів, що виходять за рамки обов'язків лінії 1. Дійсно, багато випадків пов'язані з нестандартними індикаторами і аналітикою, з якими не може працювати Лінія 1, але може працювати Лінія 2. У більших SOC ці команди працюють спільно, щоб знайти і оцінити розташування підозрілої або аномальної активності в мережі.

Для реагування на інцидент і подальшого відновлення SOC, як правило, використовують і внутрішні, і зовнішні ресурси. Важливо розуміти, що SOC не завжди розгортає заходи протидії при перших ознаках вторгнення. Для цього є як мінімум три причини:

- Аналітики SOC мають бути впевнені, що їх дії не призведуть до переривання звичних процесів.
- Відповідні дії можуть вплинути на інформаційну систему підприємства більше, ніж на сам інцидент.

- Розуміти масштаб і серйозність вторгнення, спостерігаючи за діями зловмисників, іноді це більш ефективно, ніж виконувати статичне експертне розслідування на вже скомпрометованих системах постфактум.

Щоб визначити характер атаки, SOC часто повинен застосовувати методи форензики та виконувати розширений експертний аналіз артефактів, зібраних в якості свідчень про інцидент, наприклад: образи жорстких дисків або файлів захоплення пакетів цілої сесії (pcap), реверс-інжиніринг шкідливого програмного забезпечення. Іноді дані для форензики повинні збиратися і аналізуватися юридично обґрунтованим методом. У таких випадках SOC повинен більш суворо дотримуватися визначених процедур, ніж при звичайних розслідуваннях.

Коли ознаки атаки досить добре зрозумілі, щоб окреслити сигнатурні дані у правилах SIEM, атака може бути легко виявлена, аналітик у свою чергу збирає усі вхідні дані та приймає рішення про ескалацію інциденту на наступну лінію, або ж, за необхідності приймається за його вирішення самостійно. Якщо, загрозу було усунуто безпосередньо на пристрої-джерелі подій, тоді у SIEM потрапить сповіщення про усунуту загрозу, наприклад на системах IPS, міжмережевих екранах, антивірусах тощо. Оскільки такі системи зазвичай використовуються для запобігання самих базових атак, ступінь, в якій вони можуть автоматизувати аналіз, обмежена. Для нейтралізації великих інцидентів завжди необхідна участь людини. Ряд технологій дозволяє SOC щодня обробляти мільйони подій з підтримкою повного життєвого циклу інциденту. Інструменти SIEM збирають, зберігають, зіставляють і відображають дані про стан безпеки з багатьох джерел, підтримуючи операції сортування, аналізу, ескалації та реагування. Системи виявлення (IDS) і запобігання (IPS) вторгнень є двома з безлічі систем, які поставляють дані в SIEM. Як показує досвід, технології IDS/IPS можуть бути необхідні, але не достатні для виявлення інцидентів. У сукупності уся різноманітність джерел інформації дозволяє використовувати для аналізу як розрізнені і непідтверджені, так і достовірні в контексті ситуації дані. Будь-яке джерело подій безпеки має низьку цінність окремо сама по собі.

SOC не обмежується отриманням інформації лише зі своїх корпоративних інформаційних систем. Він також збирає інформацію з різних зовнішніх джерел, які забезпечують розуміння загроз і вразливостей, а також тактик, технік і процедур зловмисників. Ця інформація є даними кіберрозвідки (англ. threat intelligence) і включає в себе фіди в сфері кібер-безпеки, оновлення сигнатур, звіти про інциденти, повідомлення про загрози і попередження про вразливість. Як захисник, SOC знаходиться в постійній гонці озброєнь, щоб підтримувати паритет зі змінним середовищем і ландшафтом загроз. Ключем до перемоги в цій гонці для SOC є постійний збір даних кіберрозвідки інструментами моніторингу. За тиждень SOC обробляє десятки фрагментів таких даних, які можуть дати сигнал до застосування різних захисних заходів, від оновлень сигнатур до термінової установки патчів. SOC повинен вміти відбирати розвіддані для використання – вони повинні бути своєчасними, актуальними, точними, конкретними і дієвими щодо інциденту, уразливості або загрози, яку описують.

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.

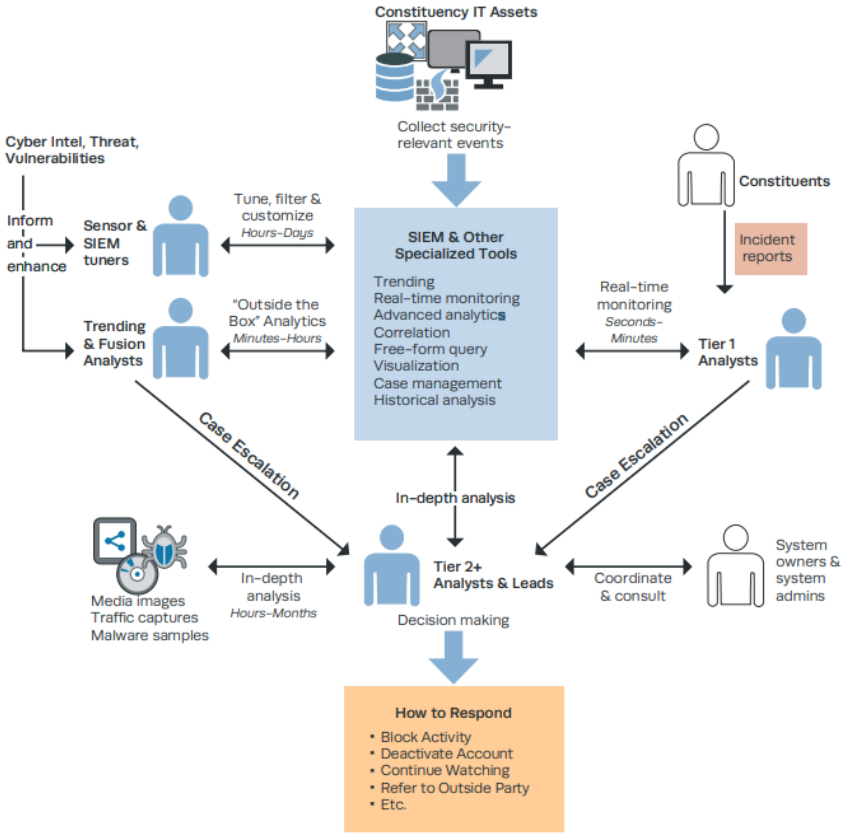


Рис. 1.1. Розподіл ролей та ескалація інцидентів в SOC

Дуже важливо розділяти структури аналогічні або схожі на SOC, але їх слід визнати окремими і самостійними. SOC абсолютно точно відрізняється від[2]:

- Центру управління мережею (англ. Network Operations Center, NOC), оскільки SOC в основному шукає кібератаки, тоді як NOC займається експлуатацією і обслуговуванням мережевого обладнання.
- IT-дирекції (CIO) або підрозділів інформаційної безпеки, оскільки SOC виконує функції в режимі реального часу, а його зусилля з моніторингу зазвичай не призначені для забезпечення стратегічного планування (хоча деякі SOC можуть безпосередньо підпорядковуватися CISO або CIO).
- Програми безперервного моніторингу інформаційної безпеки (ISCM)[4], оскільки SOC відповідає за виявлення і реагування на інциденти.
- ISSO або ISSM, тому що SOC відповідає за моніторинг і реагування на повномасштабну кібер-загрозу, тоді як ISSO зазвичай пов'язані з наглядом за IT і забезпечують безпеку конкретних систем.

- Команди експлуатації комп'ютерної мережі (CNE) або комп'ютерних мережевих атак (CNA), однак дуже часто трапляється, коли фахівці внутрішніх SOC на підприємстві проводять тести на проникнення своїх інформаційних ресурсів самостійно.
- Моніторингу фізичної безпеки (наприклад, «ворота, охоронці, озброєння»), оскільки SOC займається кібер-сферою, в той час як моніторинг фізичної безпеки в першу чергу стосується захисту фізичних активів і забезпечення безпеки персоналу.
- Правоохоронних органів, оскільки SOC зазвичай не є слідчими органами; вони можуть виявити вторгнення, які можуть призвести до правових наслідків, але їх основний обов'язок, як правило, не укладається в зборі, аналізі та поданні доказів, які будуть використовуватися в судових провадженнях.

Однак ці відмінності не виключають того, що деякі SOC можуть мати схожі із вище переліченими структурами функції та мати у своєму складі фахівців, що здатні виконувати вузькоспеціальні специфічні задачі. Окрім того, самі підрозділи SOC, у межах підприємства, галузі або держави повинні працювати з усіма перерахованими групами на регулярній основі і підтримувати навички в багатьох областях IT і кібербезпеки.

1.3. Характеристики центрів управління кібербезпекою

Оскільки SOC можуть значно відрізнятися за розміром і структурою, потрібно визначити ключові характеристики для опису цих відмінностей. Перш ніж докладно описувати різні можливості SOC, почнемо з трьох його характеристик:

- Відносини зі споживачами послуг SOC з організаційної точки зору.
- Розподіл ресурсів, які складають SOC (наприклад, його організаційна модель).
- Повноваження, якими він володіє по відношенню до споживачів своїх послуг.

Відносини: SOC є або частиною організації, яку вони обслуговують, або є зовнішньої структурою.

До SOC, які є зовнішніми по відношенню до своїх клієнтів, відносяться постачальники послуг безпеки (MSSP), якими керує сервіс-провайдер, що надає послуги клієнтам за оплату. До них також відносяться SOC, орієнтовані на конкретний продукт, наприклад, SOC компанії-розробника, якому необхідно оперативно реагувати на виявлені в їх продукті уразливості.

У більшості випадків SOC є частиною організації, яку він обслуговує, тому їх взаємини вважаються внутрішніми. Внутрішні споживачі SOC включають користувачів та IT-активи, що належать конкретній незалежної організації, наприклад, державному органу, університету або корпорації, частиною якої є SOC. У цих випадках зазвичай є генеральний директор (CEO) і IT-директор (CIO), що відповідають за всю організацію. Такі споживачі зазвичай поділяються на кілька бізнес-одиниць, кожна з яких може бути географічно розташована в одному або декількох місцях.

В цій роботі здебільшого будуть описані підходи із побудови внутрішніх SOC.

Що стосується внутрішніх SOC можна виділити такі п'ять організаційних моделей:

- **Команда безпеки.** В ній відсутня окрема структурна одиниця для виявлення або реагування на інциденти. У разі виникнення інциденту комп'ютерної безпеки, збираються ресурси для вирішення проблеми, відновлення систем, після чого команда припиняє свою роботу. Результати можуть сильно відрізнятися, оскільки немає центрального спостерігача або єдиної бази знань, а процеси обробки інцидентів зазвичай погано визначені. Цю модель, як правило, вибирають клієнти, що складаються з менше 1000 користувачів або IP-адрес.
- **Внутрішній розподілений SOC.** Постійний SOC існує, але в основному складається з осіб, що організаційно знаходяться за межами SOC, чия основна робота пов'язана з IT або безпекою, але не обов'язково пов'язана із

захистом комп'ютерних мереж. Одна людина або невелика група відповідає за координацію дій щодо забезпечення безпеки, але складні завдання виконуються особами, залученими з інших організацій. У цю категорію часто входять SOC, що обслуговують клієнтів малого та середнього розміру, від 500 до 5000 користувачів або IP-адрес.

- **Внутрішній централізований SOC.** Виділена команда фахівців в області інформаційних технологій і кібербезпеки. Забезпечує безперервний захист корпоративних інформаційних систем, виконуючи завдання на постійній основі. Ресурси і повноваження, необхідні для щоденної підтримки безпеки мереж, виділені в окрему офіційно визнану одиницю, зазвичай з власним бюджетом. Ця команда звітує перед керівником SOC, який контролює усі процеси. Більшість SOC відносяться до цієї категорії, зазвичай обслуговуючи клієнтів, що становлять від 5000 до 100 000 користувачів або IP-адрес.
- **Внутрішній комбінований розподілений і централізований SOC.** SOC складається як з центральної команди (як у випадку внутрішніх централізованих SOC), так і з відокремлених ресурсів, що належать організації(як у випадку внутрішніх розподілених SOC). Особи, що підтримують операції за межами основного SOC, не розглядаються як окрема частина SOC. Для більш великих підприємств ця модель підтримує баланс між наявністю узгодженої, синхронізованою команди і підтриманням обізнаності про віддалені IT-активи і структурні підрозділи. SOC, що обслуговують інфраструктуру, що складається в середньому з 25 000 – 500 000 IP адрес, можуть використовувати цей тип, особливо якщо їх споживачі географічно розподілені або вони обслуговують дуже неоднорідне середовище інформаційних систем.
- **Координаційний SOC.** SOC виступає посередником і полегшує діяльність між декількома підлеглими SOC, як правило, характерний для великого підприємтсва, яке може включати мільйони користувачів або IP-адрес. Координуючий SOC зазвичай надає консультаційні послуги підлеглим. Як

правило, у нього немає всієї повноти картини аж до кінцевого пристрою, а повноваження по відношенню до споживачів послуг - обмежені. Координаційні SOC часто служать розподільними центрами для проведення кіберрозвідки, формування кращих практик та навчання. Вони також можуть пропонувати послуги з аналізу та розслідування на прохання підлеглих їм SOC.

На практиці не усі SOC точно відповідають будь-якій з цих категорій - більшість з них потрапляють в область десь між суто розподіленою і суто централізованої моделлю. Крім того, координаційні SOC узгоджують діяльність підпорядкованих їм SOC, а також виконують свої власні прямі завдання з моніторингу та реагування. У будь-якому випадку, SOC повинен оптимально поєднувати глибоке розуміння принципів захисту мереж і знання всіх активів і задач системи. Разом вони утворюють «репутацію» SOC (тобто сприйняття цінності і можливостей SOC споживачами його послуг та іншими SOC).

Ключовим аспектом також є повноваження – ступінь свободи дій SOC по відношенню до активів користувачів послуг (внутрішніх або зовнішніх) – необхідність їх узгодження з іншими групами, отримання дозволу. Використовується схема описана американським CERT[5] з деякими змінами. SOC може володіти трьома рівнями повноважень:

- **Відсутність повноважень.** SOC може пропонувати або намагатися впливати на дії, які споживачі його послуг повинні виконати. Однак у SOC немає ні формальних засобів для чинення тиску, ні вищої організаційної одиниці, здатної це зробити. Тільки замовник вирішує, розглянути або ігнорувати рекомендації SOC.
- **Спільні повноваження.** SOC може давати рекомендації керівництву замовника (наприклад, IT-директорам, керівникам ІБ підрозділів (CISO), генеральним директорам, власникам систем), у якого є повноваження для реалізації запропонованих змін. Ці рекомендації порівнюються з пропозиціями інших зацікавлених сторін до прийняття рішення, даючи SOC можливість «висловитися».

- **Повні повноваження.** SOC може давати споживачам своїх послуг вказівки на певні дії, не чекаючи схвалення або підтримки з боку учасників вищого рівня. Здатність SOC диктувати зміни визнається на практиці. Відповідні положення також можна закріпити окремим внутрішнім документом про діяльність SOC або додавши змін до політик безпеки підприємства.

Повноваження SOC не є абсолютними, навіть якщо він має «повний авторитет» в рамках будь-якої сфери його діяльності. Офіційні повноваження SOC слід використовувати до певної межі, після якої SOC повинен використовувати скоріше вплив, ніж вимоги. Для агресивних контрзаходів або реагування, як наприклад, відключення критично важливого корпоративного сервера, потрібне розуміння і схвалення високого рівня. У той час як SOC може відключати систему від мережі, тому що щось негативне вже сталося, він не може вимагати зміни конфігурації для компанії, тому що щось негативне може статися. Часто повноваження SOC прописують таким чином, що SOC можуть використовувати їх частину тільки при виявленні серйозного інциденту. На практиці, всі SOC використовують як офіційні, так і неофіційні внутрішні повноваження, а також вплив і авторитет своїх експертів. Повноваження класифікують[5] за двома етапами життєвого циклу інциденту:

- **Реактивні.** Реактивні заходи, вжиті після вірогідного, або підтвердженого інциденту. Дії зазвичай більш тактичні за своєю суттю – вони тимчасові і впливають тільки на ті складові і системи, які безпосередньо порушені інцидентом. Наприклад, логічна або фізична ізоляція робочої станції або сервера, збір лог-файлів з сервера або збір артефактів по конкретній ситуації.
- **Проактивні.** Запобіжні заходи, вжиті до того, як будуть виявлені прямі докази інциденту. Ці дії носять більш стратегічний характер – вони, як правило, довготривалі і впливають на значну частину споживачів послуг SOC. Наприклад, термінова установка патчів на весь домен Windows, «чорні діри» в DNS або блокування IP для мереж, що належать зловмисникам, скидання пароля поза циклом для користувачів веб-порталу або зміна політики безпеки.

Незалежно від повноважень, покладених на SOC, нічого не відбувається без тісних робочих відносин з власниками систем, системними адміністраторами та IT-керівниками.

1.4. 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.

Моніторинг. З точки зору моніторингу перш за все перед фахівцями SOC стоїть задача визначити, які саме пристрої необхідно відслідковувати та яку категорію подій в них, потрібно отримати відповідні дані, перш ніж проводити будь-який аналіз. У контексті моніторингу безпеки дані з різних джерел та у різних форматах можуть збиратися з метою аналізу рівня захищеності, аудиту та комплаєнсу. Дані, що представляють особливий інтерес, включаючи журнали(логи) подій, мережеві пакети та мережеві потоки. Також може знадобитись можливість досліджувати або збирати такі дані, як статичний вміст веб-сторінки або хеш-сумму файлу.

Створення та збір журналів подій є критично важливою задачею для SOC. Події можуть прямо чи опосередковано сприяти виявленню інцидентів безпеки. Наприклад, високо пріоритетна подія, отримана з правильно налаштованої системи IDS, буде свідчити про спробу атаки. Однак подія про аномально високу завантаженість лінії зв'язку, що згенерована маршрутизатором, може не бути подією безпеки сама по собі, але може вказувати на інцидент безпеки, пов'язаний з іншими подіями, такими як атака на відмову в обслуговуванні (DoS) або на скомпрометований хост, який сканує мережу.

Точне розуміння середовища інформаційної системи та визначення елементів, з яких необхідно отримувати дані, є фундаментальним принципом у

процесі підготовки до збору даних. Концептуальні етапи, показані на рисунку 2, представляють цей процес. Дані можуть зберігатись у текстовому файлі, реляційній базі даних або в розподілених файлових системах, таких як розподілена файлова система Hadoop (HDFS). Аналіз може проводитись різними методами, такі як статистичне виявлення аномальної активності, за допомогою розгортання правил кореляції подій або застосовуючи техніку машинного навчання. Починаючи з фази проектування SOC, слід формалізувати та задокументувати всі процеси та процедури, включаючи вибір технології.

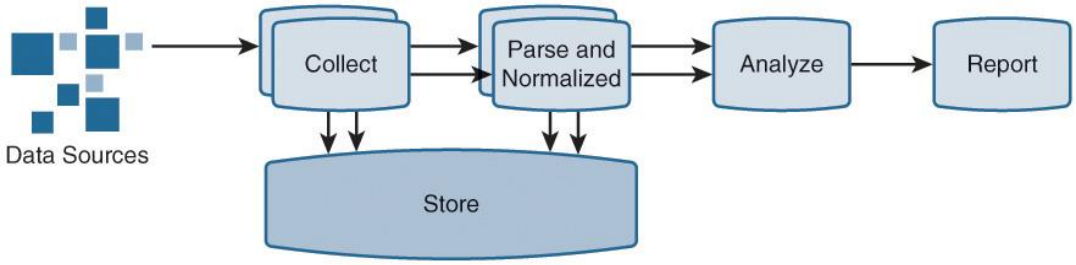


Рис. 1.2. Базова модель управління потоками даних

Після збору даних варто визначити чи зберігати їх, чи аналізувати або і те, і те. Хоча зберігання даних у оригінальному форматі може бути корисним для проведення цифрових розслідувань, ретроспективної аналітики та задоволення вимог комплаєнсу, важливо зазначити, що дані на цьому етапі розглядаються як неструктуровані, тобто точна структура досі невідома або не перевірена. Щоб зрозуміти структуру даних, необхідно провести синтаксичний розбір(парсинг) для вилучення різних полів події. Щоб дані несли якусь користь для організації, потрібно мати сховище, яке може їх зберігати, та інструменти, якими можна формувати запити, отримувати та аналізувати ці дані. Багато факторів можуть бути визначальними щодо того, які типи і яку кількість даних повинен зберігати SOC, наприклад, юридичні та регулятивні фактори, вартість зберігання даних тощо.

Розглянемо різні типи джерел даних. Логи(журнали) вважаються найбільш корисним типом даних для отримання. Логи є узагальненням дій, які мали місце в системі, що містять інформацію, пов’язану з конкретною подією. Залежно від

середовища, необхідно розглядати можливість збору логів з різних видів систем: системи безпеки, мережеві пристрої та додатки. Приклади фізичних та віртуальних засобів, які можуть надавати цінні дані:

- Засоби безпеки, такі як міжмережеві екрани, системи виявлення та запобігання вторгненню, антивірусні рішення, проксі-сервери та засоби аналізу шкідливих програм.
- Мережеві пристрої, такі як маршрутизатори, комутатори, бездротові точки доступу та контролери.
- Операційні системи, такі як різні версії Microsoft Windows, UNIX, Linux та OS X.
- Платформи для віртуалізації, такі як Virtual-Box, віртуальна машина на базі ядра (KVM), Microsoft Hyper-V та VMware ESX.
- Додатки, такі як веб-сервери, сервери системи доменних імен (DNS), шлюзи електронної пошти, програми виставлення рахунків, голосові шлюзи та інструменти управління мобільними пристроями (MDM)
- Бази даних.
- Елементи фізичної безпеки, такі як відео-камери, пристрої контролю доступу до дверей та системи відстеження.
- Системи, що використовуються в технологічних мережах, такі як системи контролю та збору даних (SCADA) та розподілені система управління (DCS).

Окрім вичитування логів існує потреба збирати, зберігати та, можливо, аналізувати інші форми даних. Як приклад це збір мережевих пакетів, NetFlow та вміст файлів, таких як файли конфігурації, хеш-суми та файли HTML. Кожне з цих джерел даних має унікальну цінність, але кожне має свої пов'язані з цим витрати, які слід врахувати перед тим, як інвестувати в методи збору та аналізу даних. Наприклад, зберігання мережевих пакетів, як правило, коштує найбільше, але може надавати детальнішу інформацію про події, ніж NetFlow. Деякі галузеві норми вимагають зберігання даних на рівні пакетів, що робить процес захоплення мережевих пакетів обов’язковим.

Аналіз безпеки відноситься до процесу дослідження даних з метою виявлення потенційних відомих та невідомих загроз. Складність завдання варіюється від відображення базових інцидентів до вдосконаленого математичного моделювання, що використовується для виявлення невідомих загроз. Виявлення взаємозв'язку між подіями в контексті досягається за допомогою методів машинного навчання або методів, заснованих на знаннях, таких як узгодження на основі правил та виявлення статистичних аномалій.

Кореляція подій – найвідоміша та найуживаніша форма аналізу даних. Кореляція подій безпеки відноситься до завдання створення контексту, в межах якого виявляються взаємозв'язки між різними подіями, отриманими з різних джерел, з метою виявлення та звітування про загрози. Контекст може бути пов'язаний часом, евристикою та вартістю активів[6].

Правила кореляції представлені функціоналом інструментів SIEM. Більшість з них має в собі низку вже готових корисних правил. Також постачальники таких систем зазвичай пропонують можливість регулярного оновлення наборів правил в рамках платної послуги підтримки. Ці правила можна налаштувати під себе або створити власні правила, однак, важливо визначитись із тим, на які саме події варто реагувати. Більшість правил кореляції, пропоновані постачальниками SIEM, базуються на досвіді, який вони отримують при розгортанні своїх рішень клієнтам та завдяки внутрішнім дослідницьким групам. Приклади стандартних правил кореляції включають позначення надмірної кількості невдалих спроб авторизації, зараження шкідливим програмним забезпеченням, несанкціоновані вихідні підключення та спроби DoS-атак.

Управління вразливістю відноситься до процесу виявлення, підтвердження, класифікації, пріоритизації, призначення, усунення та відстеження вразливостей. Однак варто розділяти процеси управління вразливістю зі скануванням вразливості, яке є частиною процесу управління вразливістю, з акцентом на фазі виявлення. Важливо також розуміти, що управління ризиками має відношення до усіх типів ризиків інформаційної безпеки

підприємства, в той час, коли управління вразливістю орієнтоване на технологічні процеси.

Вразливістю можна вважати слабкі сторони людей, процесів та технологій. Управління вразливістю в контексті SOC фокусується на відомих технічних недоліках, що виникають у програмному забезпеченні та прошивках. Варто підкреслити, що наявність технічної вразливості може бути наслідком слабких місць у людях та процесах, таких як відсутність належного процесу перевірки якості програмного забезпечення.

Організації зі зрілою структурою безпеки інтегрують тісно пов'язані практики управління уразливістю та управління ризиками. Іноді це можна зробити за допомогою інструментів, які можуть автоматизувати цю інтеграцію. Рисунок 1.3 показує початкові кроки, які робляться для визначення межі застосування та підготовки програми управління вразливістю.

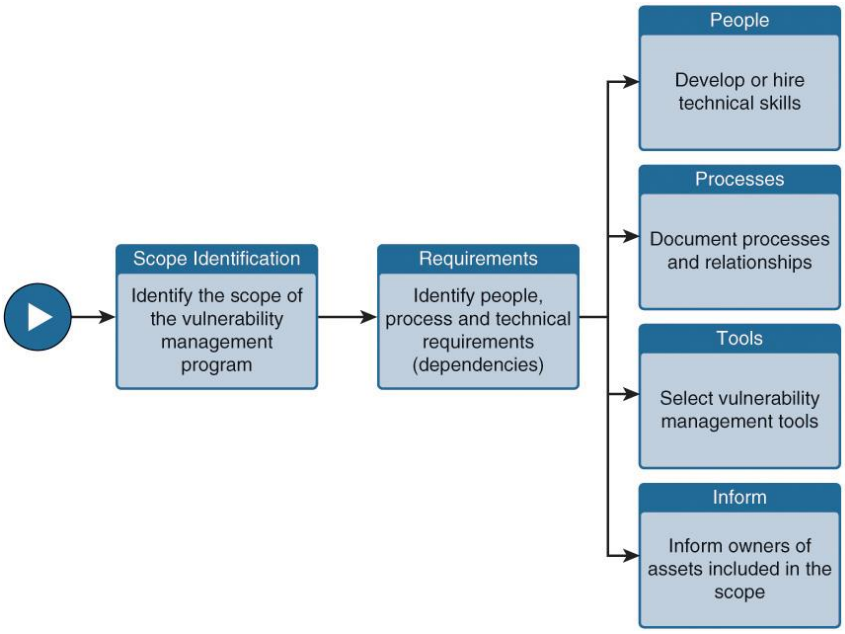


Рис. 1.3. Підготовка процесів із управління вразливостями

Найважливішим елементом управління вразливостями є швидший захист вразливих пристроїв до того, як їх слабка сторона буде використана. Так званий проактивний підхід. Це досягається низкою кроків із виявлення, оцінки та усунення ризику, пов'язаного з вразливістю. Хорошою еталонною моделлю, якою у цьому питанні є модель управління вразливістю від інституту SANS[7],

показана на рисунку 1.4. Одним із найпоширеніших методів виявлення вразливості системи є моніторинг опублікованих даних про виявлені нові вразливості у продуктах, які є частиною корпоративної інформаційної системи організації.

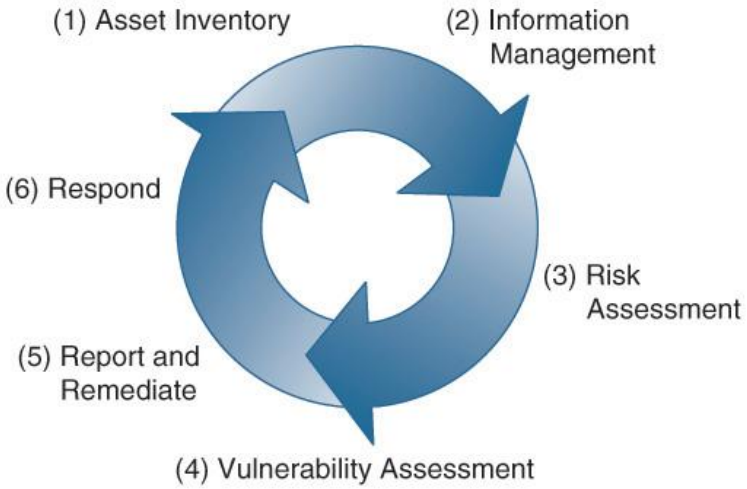


Рис. 1.4. Модель управління вразливостями від SANS

Кіберрозвідка(threat intelligence). Кіберрозвідка – це засновані на фактичних даних знання, включаючи контекст, механізми, індикатори, наслідки та дієві поради щодо існуючої або імовірної загрози чи небезпеки для активів, які ви можете використовувати для обґрунтування рішень щодо реакції на цю загрозу або небезпеку[8]. Або ж можна дати наступне визначення: «Детальна інформація про мотиви, наміри та можливості внутрішніх та зовнішніх суб’єктів загроз. Туди входять дані про специфіки тактик, технік та процедур зловмисників. Основною метою розвідки загроз є інформування щодо ризиків та наслідків, пов'язаних із загрозами».

Перекладаючи ці визначень на загальноприйняту мову – розвідка загроз є доказовим знанням можливостей внутрішніх та зовнішніх суб'єктів загроз. Ідея полягає в розширенні рівня обізнаності з питань безпеки за межами внутрішньої мережі шляхом використання інформації з інших джерел, що стосуються всієї мережі Інтернет, пов’язаної з можливими загрозами для організації. Наприклад, можна дізнатись про загрозу, яка вплинула на кілька організацій, завдяки чому

можна заздалегідь підготуватися, а не реагувати, як тільки загроза дійде до нашої інфраструктури. Забезпечення інформаційного каналу збагачення даними – це одна з функцій, яка зазвичай є у будь-якій сучасній платформи розвідки загроз.

Аналітичний центр Forrester визначає п'ятиступеневий цикл розвідки загроз, показаний на рисунку 1.5, для оцінки джерел розвідки загроз: планування, збір, обробка, аналіз, а також видобування та розповсюдження.

Рис.1.5. Цикл процесів із розвідки кіберзагроз

Усі вище перелічені класи інструментів наразі є в наявності у будь-якого сучасного SOC і є його невід’ємною частиною для забезпечення себе максимальною видимістю усіх інформаційних процесів в середині підприємства та кібербезпекової ситуації поза ним. Ринок рішень ІБ представлений великою низкою комерційних програмно-апаратних засобів, а також безкоштовних рішень із відкритим кодом (англ. Open-source). Безпосередній вибір кожного з них залежить індивідуально від кожного окремого SOC. На вибір здебільшого впливають такі фактори: вартість рішення, правила ліцензування, розмір компанії-замовника та специфіка виконуваних завдань, для яких планується придбати відповідне рішення.

Висновки до розділу 1

Розкрито сутність та значення корпоративної інформаційної системи та процесів, що циркулюють у ній. Визначено види активів, що працюють у типовій інформаційній системі та їх взаємозв’язок. Порушено проблему забезпечення інформаційної безпеки у мережі підприємства та розкрито необхідність володіння інформацією про процеси, що проходять у мережі та реєстрування усіх подій та керування ними з метою забезпечення реактивних підходів інформаційної безпеки.

З’ясовано концепцію центрів управління кібербезпекою(SOC), їх призначення функції, характеристие та їх необхідність у сучасних умовах, коли рівень загроз постійно зростає і для реагування на інциденти та для усунення загроз неможливо обійтись без проактивних заходів забезпечення інформаційної безпеки.

Типовий SOC виконує задачі, які потребують постійний збір, аналіз даних, що циркулюють у мережі підприємства, мають необхідність пріоритизувати ризики, щоб ефективно реагувати на загрози. Їм в цьому допомагають спеціальні інструменти, які, за умови коректного налаштування та за умови наявності необхідних спеціальних знань у фахівця, стають корисною зброєю у протистоянні із сучасними кіберзагрозами.

2 ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ НА ПРИКЛАДІ РІШЕНЬ MICROFOCUS ARCSIGHT

У попередньому розділі було з’ясовано які види задач має виконувати SOC та які інструменті для цього потрібні. 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 слугуватимуть системи платформи Arcsight від розробника Microfocus, а саме: ESM, Logger, Management center та Arcsight SmartConnector.

2.1 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.

Впровадження системи ESM в операційному центрі безпеки вимагає планування. Ролі користувачів допомагають особам, які приймають рішення, визначити, які навички та досвід необхідні для успішного розгортання, а також

сприяють чіткому розмежуванню доступу та розмежування обов’язків між фахівцями SOC.

ESM надає групи користувачів та списки контролю доступу (ACL) для управління доступом користувачів до певних функцій та ресурсів. Групи користувачів і ACL за замовчуванням забезпечують контроль доступу до певних ресурсів під час інсталяції. Є можливість створити власну групу користувачів, яка застосовуватиметься до ролей користувачів, яку можна визначити, виходячи зі своїх потреб. Вирізняють такі категорії користувачів[10]:

- Author(аналітик-адміністратор) – відповідає за розробку юз-кейсів(англ. use case)(правил), що стосуються потреб і цілей підприємства. Ця роль передбачає роботу над контентом(вмістом), який формує напрямок розслідування, проведення аналізу та шляхи усунення загроз, які визначені в самому SOC.
- Operator(оператор) – проводить щоденний моніторинг подій та розслідування інцидентів до рівня сортування. Оператори спостерігають події в реальному часі та відтворюють події за допомогою інструментів відтворення. Вони інтерпретують події за допомогою Інспектора подій та реагують на події заздалегідь визначеними шляхами. Вони формують звіти та працюють із Базами знань.
- Analyst(аналітик) – відповідає за спеціалізоване розслідування та усунення загроз, після безпосереднього сповіщення про інцидент від операторів. Аналітики також можуть бути операторами, або можуть бути фахівцями, які реагують лише на конкретні ситуації.
- Super user (Супер користувач) – має одночасно декілька ролей в SOC. Хоча обов'язки кожної ролі користувача можуть збігатися з іншими, супер користувач має високий рівень досвіду та займає вищу посаду, яка може охоплювати ролі автора, оператора та аналітиків

Рисунок 2.1 ілюструє схему користувачів у ESM та ,залежно від його ролі, до якої документації він має звернутися для отримання інформації про свою діяльність.

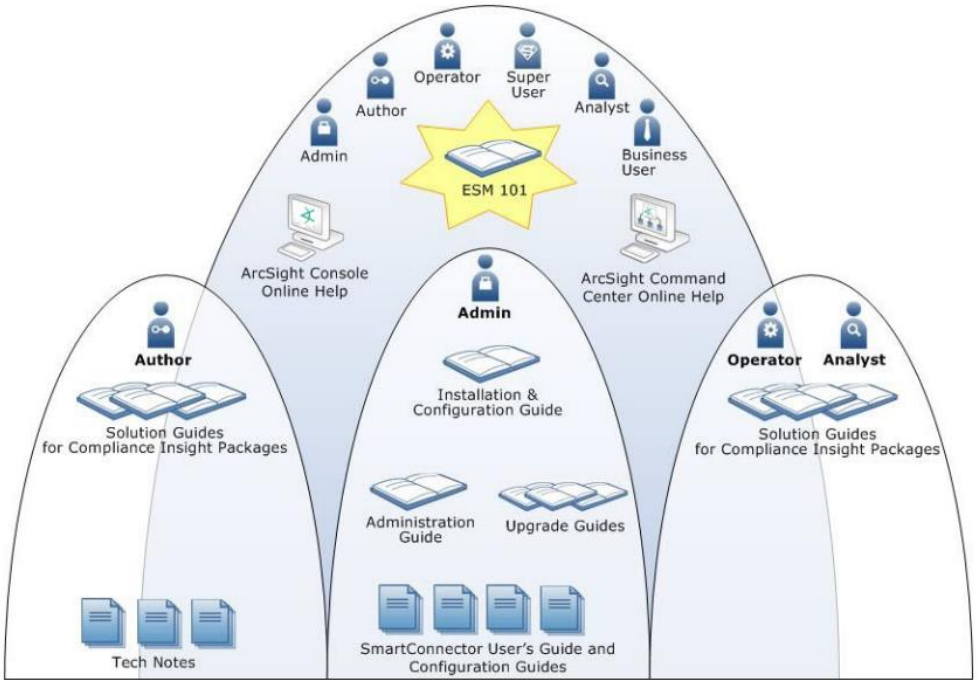


Рис. 2.1. Ролі користувачів ArcSight ESM

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.

Кореляція. Багато активностей часто представлені кількома подіями. Кореляція – це процес, який виявляє взаємозв'язок між подіями, визначає значення цих відносин, визначає їх пріоритетність, а потім забезпечує основу для дій.

Моніторинг. Після обробки та кореляції подій для визначення найбільш критичних або потенційно небезпечних з них. ESM надає різноманітні гнучкі інструменти моніторингу, які дозволяють дослідити та усунути потенційні загрози, перш ніж вони можуть завдати шкоди мережі.

Робочий процес – фреймворк, що забезпечує настроювану структуру рівнів ескалації, щоб забезпечити ескалацію подій, що цікавлять, до потрібних людей у потрібний проміжок часу. Це дозволяє фахівцям негайно проводити розслідування, приймати обґрунтовані рішення та вживати відповідних та своєчасних заходів.

Аналіз – Коли відбуваються події, які вимагають розслідування, ESM надає набір інструментів розслідування, які дозволяють фахівцям детально розглянути подію, виявити її деталі та зв'язки та виконати такі функції, як NSlookup, Ping, PortInfo, Traceroute, WebSearch та Whois.

Звіти – Інформування про стан безпеки вашої мережі є життєво важливим для всіх, хто бере участь в обслуговуванні та керуванні інформаційною системою, включаючи менеджерів з IT та безпеки, виконавчого управління та аудиторів регуляторних органів. Інструменти звітування ESM можуть бути використані для створення універсальних багатоелементних звітів, які можуть зосереджуватися на вузьких темах або повідомляти про загальний стан системи, вручну або автоматично, за регулярним розкладом.

Ядром усього ESM є служба ArcSight Manager. Це сервер на основі Java, який керує аналізом, робочими потоками та іншими сервісами. Він також корелює дані із широкого спектру систем безпеки.

Менеджер записує події в CORR-Engine, коли вони надходять у систему. Він одночасно обробляє їх за допомогою механізму кореляції, який оцінює кожну подію за допомогою мережевої моделі та інформації про вразливість для генерації результатів у реальному часі.

ESM постачається з конфігураціями за замовчуванням та стандартними use case, що складаються з фільтрів, правил, звітів, моніторів даних, інформаційних панелей та мережевих моделей, які роблять ESM готовим до використання після встановлення. Можна також розробляти самостійно всі процеси, якиими керує Менеджер, від виявлення, до кореляції та ескалації.

ESM збирає вихідні дані з таких джерел, як мережеві пристрої, системи виявлення та запобігання вторгнень, сканери вразливості, брандмауери,

антивіруси та анти-спам інструменти, засоби шифрування, журнали(логи) аудиту програм та логи систем фізичної безпеки. На рисунку 2.3 показано загальні джерела даних мережевої безпеки, які підтримує ESM та способи, якими можна проаналізувати їх результати.

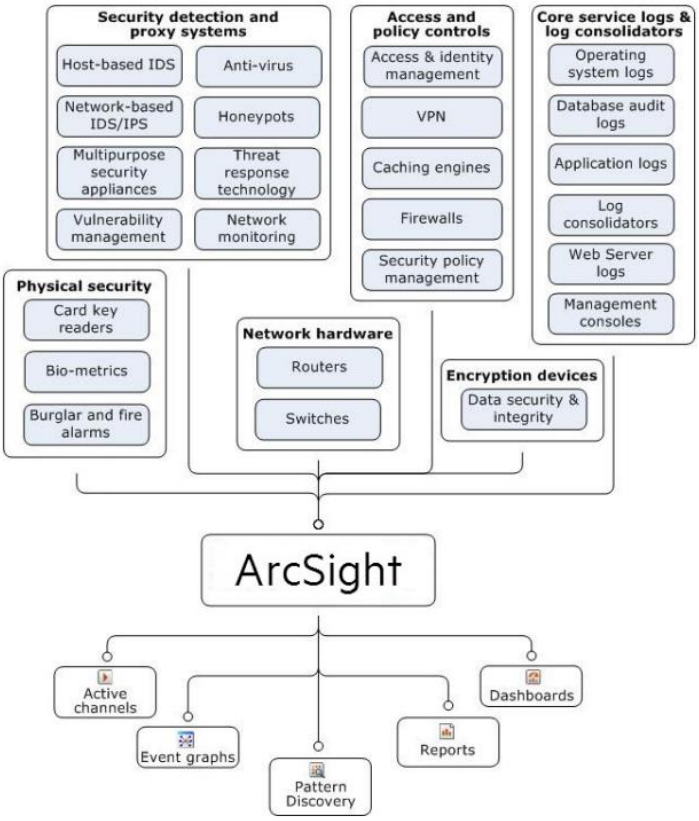


Рис.2.2. Типи джерел даних безпеки і способи їх аналізу в ESM

Усі події до ESM потрапляють через спеціальний засіб – **SmartConnector** – його задача полягає в тому, щоб збирати дані із усіх систем та відправляти їх у ESM або Logger у зрозумілому для них форматі[11]. SmartConnectors – це інтерфейс до об’єктів у мережі, які генерують події. Після збору подій вони нормалізують дані двома способами: нормалізуючи значення (такі як рівень загрози, пріоритет і часовий пояс) у загальний формат та переводячи структури даних у загальну схему. Конектори можуть фільтрувати та агрегувати події, щоб зменшити обсяг подій, що надсилається в ESM, що підвищує ефективність та точність його роботи та зменшує час обробки подій.

Смартконектори дозволяють виконувати команди на локальному хості, наприклад відправляти команди сканеру виконати сканування, додають інформацію до даних, що самі збирають, такі як пошук IP-адрес та/або хостнеймів, щоб визначити IP або ім'я хосту при пошуку у менеджері(ESM).

SmartConnectors виконують такі функції:

- Збирають усі необхідні дані, з пристрою-джерела, щоб не було необхідності працювати із самим пристроєм під час розслідування або аудиту.
- Зберігають пропускну здатність мережі та простір для зберігання, за допомогою фільтрації тих даних, про які ви знаєте, що вони не будуть використовуватись для аналізу.
- Проводить парсинг подій та впорядковує їх у загальну схему (формат) для використання в ESM.
- Агрегує події, щоб зменшити кількість подій, що надсилаються Менеджеру.
- Категоризує події, використовуючи загальноприйнятий для читання формат. Це рятує від необхідності бути експертом у зчитуванні логів з безлічі пристроїв від різних розробників та спрощує використання цих категорій подій для створення фільтрів, правил, звітів та інструментальних панелей.
- Передає події ESM після їх обробки.

В залежності від пристрою, деякі конектори також можуть налаштовані давати команди пристроям. Ці дії можна виконати вручну або через автоматизовані дії за допомогою правил та деяких моніторів даних.

SmartConnector можна встановлювати безпосередньо на пристрої-джерела або на окремі сервери. SmartConnector можна розміщувати на самому пристрої, якщо це пристрій загального призначення, такі як комп’ютер або сервер для роботи із програмним забезпеченням, таким як ISS RealSecure, Snort тощо. Для вбудованих джерел даних, таких як мережеві пристрої, брандмауери, то встановлення на пристрої не є можливим.

Під час конфігурації SmartConnector реєструється в ArcSight Manager, центральний серверний компонент рішення ESM і налаштований за характеристиками, унікальними для пристроїв, з яких він зчитує дані, та залежності від потреб конкретної мережі. За замовчуванням SmartConnectors перевіряють із Менеджером кожні 10 секунд. Менеджер надсилає назад усі команди або оновлення конфігурації, які він має для конектора. SmartConnector надсилає нові дані про події менеджеру пакетом в 100 подій або раз на секунду, залежно від того, що трапиться раніше. Час і інтервали кількості подій можна налаштувати.

У інфраструктурі Arcsight також існує можливість створення самописних конекторів, так званих **FlexConnector**. Фреймворк FlexConnector – це комплект для розробки програмного забезпечення (SDK), який дозволяє створити свій власний SmartConnector для специфічних пристроїв у свої мережі та для вичитування тих подій, що вони генерують. Типи FlexConnector включають конектори для читання файлів, програму для читання файлів із регулярними виразами, зчитувач баз даних за часовими параметрами, системний журнал(Syslog) та зчитувачі протоколу SNMP.

ArcSight Logger – це пристрій для зберігання подій, який оптимізовано для надзвичайно високої пропускної здатності. Він зберігає події безпеки в стиснутому вигляді, але завжди може отримати немодифіковані події на вимогу для ретроспективних аналізів даних .

Logger можна розгорнути самостійно для отримання Syslog-подій, файлів журналювання або для отримання подій у CEF-форматі (загальний формат подій) від SmartConnector’ів. Логгер може пересилати вибрані події як Syslog до ESM.

Кілька логерів можуть працювати разом, щоб збільшити масштаб, щоб витримувати високий рівень потоків даних, таким чином події розподіляються по одноранговій мережі між Logger`ами.

ArcSight Management Center (ArcMC) – це апаратне рішення, яке розміщує необхідні SmartConnectors на одному пристрої з веб-інтерфейсом для централізованого управління.

ArcMC може керувати конекторами на самому пристрої, на інших віддалених ArcMC та програмному SmartConnector, встановленому на віддалених хостах. Його функції:

- Підтримує масові операції на всіх SmartConnector і ідеально підходить для розгортання ArcSight з великою кількістю SmartConnector
- Забезпечує функцію управління SmartConnector в середовищах, що працюють лише з Logger
- Забезпечує єдиний інтерфейс, за допомогою якого можна налаштовувати, контролювати, налаштовувати та оновлювати SmartConnector

ArcMC не впливає на працюючі SmartConnectors, якщо він не використовується для зміни їх конфігурації. Він дуже корисний у середовищах з конекторами, що націлені на кілька різнорідних напрямків (наприклад, коли Logger розгортається разом із ESM), в середовищі, що працює лише для Logger, або коли задіяна велика кількість SmartConnectors, наприклад, при розгортанні MSSP. Рисунок 2.4 демонструє схему зв’язків усіх компонентів Arcsight та джерел подій.

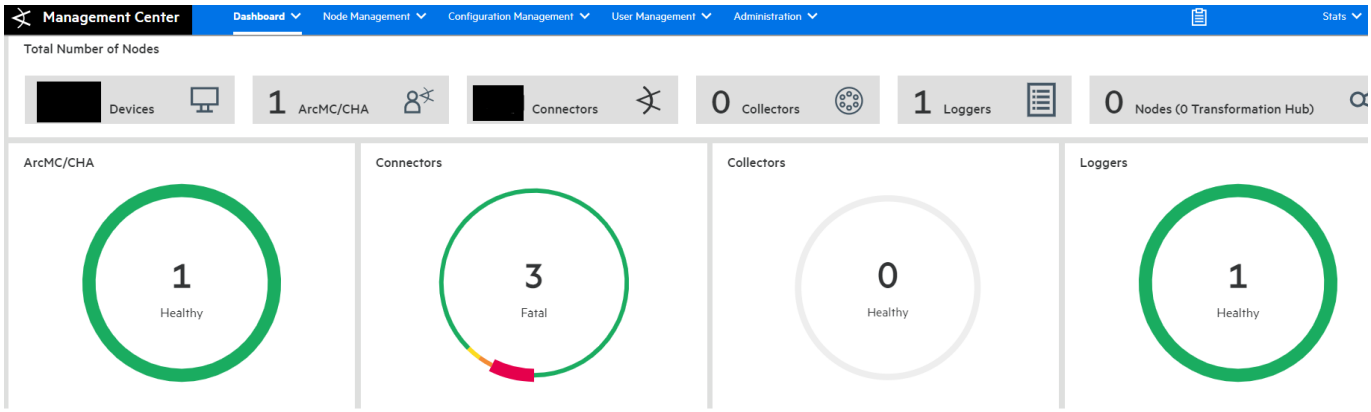


Рис.2.3 Інструментальна панель ArcMC

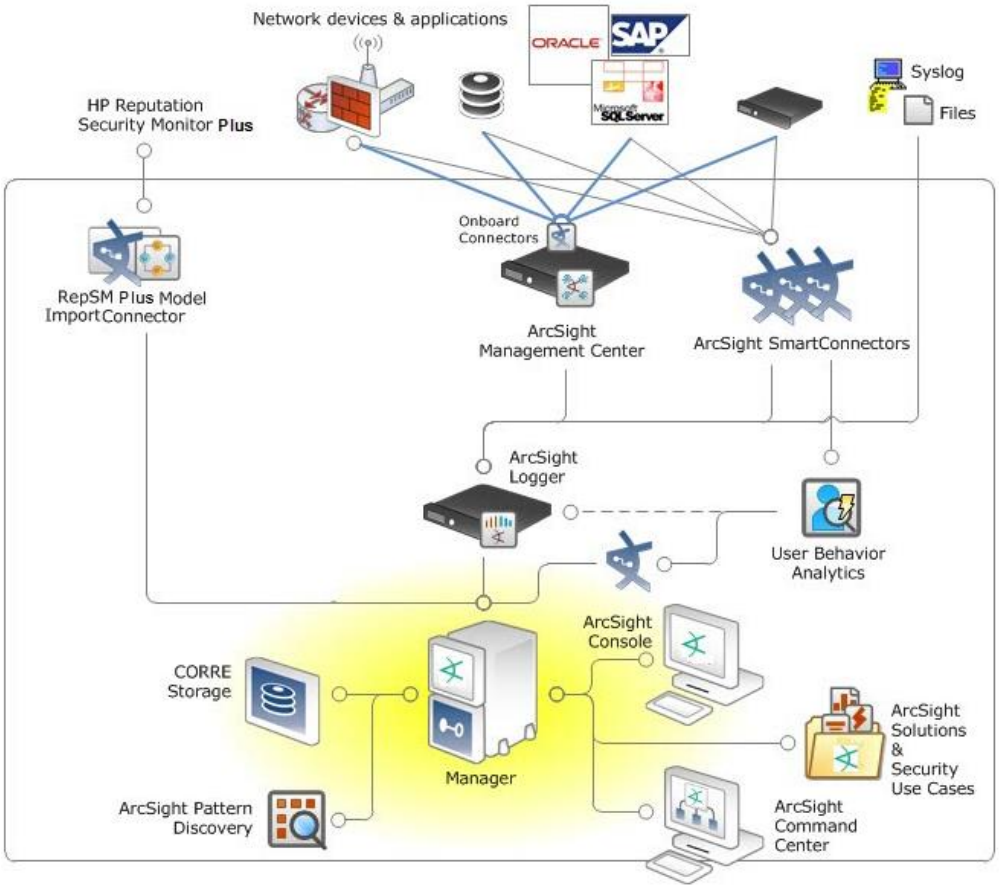
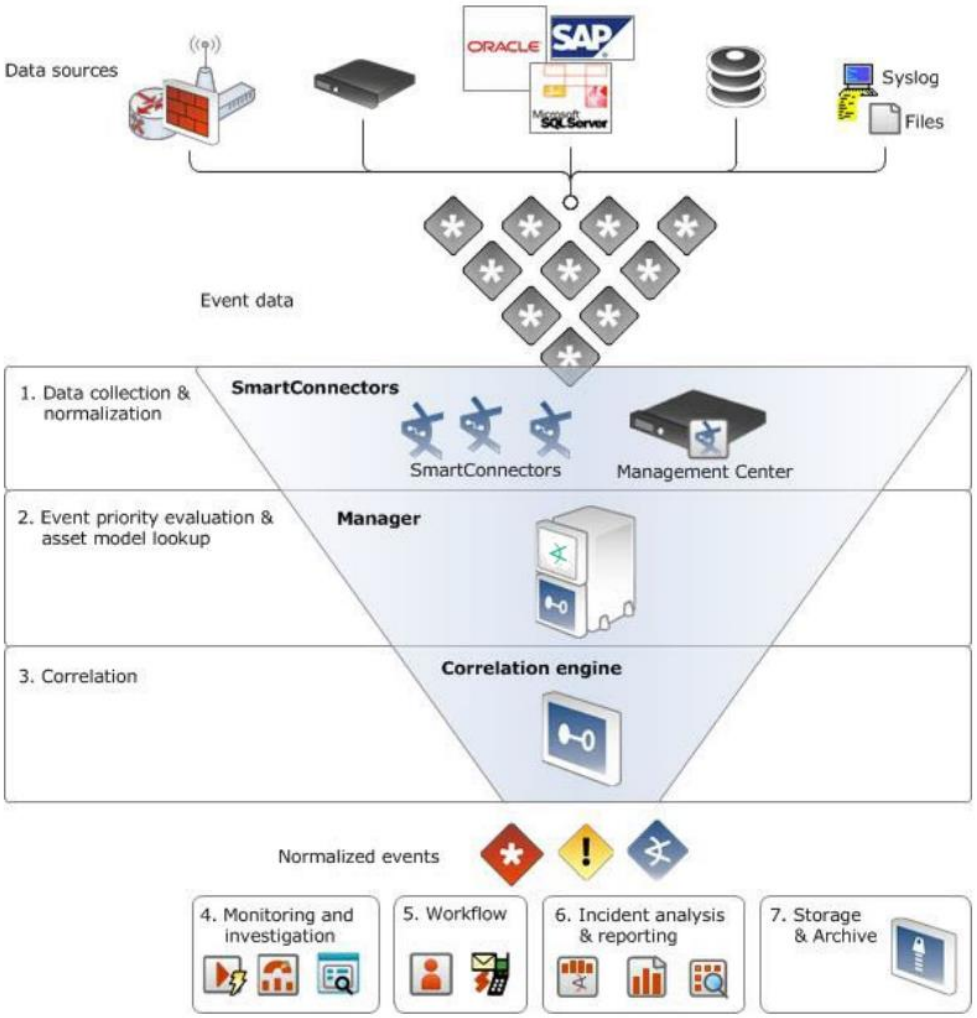


Рис. 2.4. Архітектура ArcSight

2.2 Життєвий цикл події у Arcsight ESM

ESM обробляє події поетапно, щоб ідентифікувати та реагувати на події, що представляють інтерес. На рисунку 2.5 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.

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.



2.5. Життєвий цикл події в ArcSight ESM

2.2.1 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.

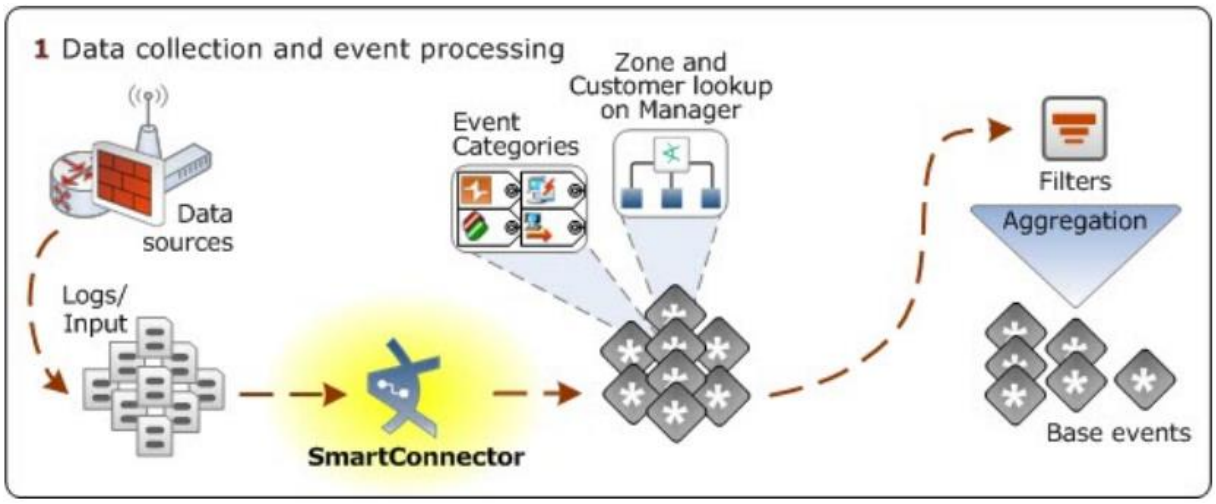


Рис.2.6. Процес збору та обробки подій

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.

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.

Зібрані дані є даними логів, генеровані різними типами джерел у мережі. Кожен елемент логу перекладається в одну подію. Те, як дані надходять до конектора, залежить від джерела, яке записує логи.

Наприклад, дані про події можуть бути отримані з баз даних, таких як MS SQL, або надіслані як потік подій через мережу, такі як syslog або SNMP. У деяких випадках дані зчитуються з файлів журналів, а в інших випадках вони витягуються конектором за допомогою приватних протоколів, таких як OPSEC (Check Point) або RDEP (Cisco IDS).

Однією із задач конектора є нормалізація (впорядкування) подій. Нормалізація означає відповідність прийнятим стандартам або нормам. Оскільки

мережі є неоднорідними середовищами, кожен пристрій має різний формат ведення логів та механізми звітування. Можна також отримувати логи з віддалених місць, де політики та процедури безпеки можуть відрізнятись, з різними типами мережевих пристроїв, засобами безпеки, операційними системами та журналами програм. Оскільки всі формати різні, важко отримати інформацію для запитів, спершу не нормалізувавши події.

Розглянемо приклад: в нас є маршрутизатор CISCO, він налаштований, щоб надсилати Syslog на SmartConnector, у «сирому» вигляді подія, яку отримуватиме конектор виглядатиме так:

```
Nov 21 15:10:27: %SEC-6-IPACCESSLOGP: list 102 permitted tcp 192.0.2.0(1355) -> 192.0.2.1(80), 1
packet Cisco PIX: Nov 21 2016 12:10:28: %PIX-6-302001: Built inbound TCP connection 125891 for faddr
192.0.2.0/1355 gaddr 192.0.2.1/80 laddr 10.0.111.22/80
```

Хоча і теоретично можна розібрати що саме записано в цей лог, все ж необхідно розуміти як записується цей конкретний формат логу і як його інтерпретувати.

Для продуктивного зберігання цих різноманітних даних у загальному сховищі даних, SmartConnectors оцінюють, які поля є релевантними, та розміщують їх у загальній схемі. Вибір полів залежить від вмісту, а не на основі синтаксичних відмінностей між тим, що саме може називати адресою призначення та тим, що, наприклад, Juniper називає адресою призначення.

Для нормалізації SmartConnector використовує синтаксичний аналізатор (парсер), щоб витягти значення з події та заповнити відповідні поля в схемі. Ось дуже простий приклад тих самих попереджень після їх нормалізації.

Date	Time	Event_Name	Src_IP	Src_Port	Tgt_IP	Tgt_Port	Device_Type
21-Nov-16	12:10:27	List 102 permitted tcp	192.0.2.0	1355	192.0.2.1	80	Cisco Router

Рис. 2.7. Нормалізована подія, отримана з логу маршрутизатора CISCO

ArcSight посилається на подію, яка була оброблена SmartConnector або компонентом ESM, який пройшов цю схему нормалізації, як нормалізована подія.

Події, які були оброблені SmartConnector і готові до надсилання менеджеру, також називаються *базовими* подіями. З упорядкованими даними можна витягувати всі записи, що містить саме те значення, яке цікавить, або сортувати за будь-яким полем.

Іншим фактором нормалізації є перетворення позначок часу (англ. timestamp) в загальний формат. Оскільки всі пристрої можуть використовувати різні часові пояси, нормалізація ESM перетворює мітки часу в UTC (GMT).

Процес нормалізації ESM фіксує та доставляє до механізму кореляції всю відповідну інформацію про безпеку, зібрану усіма пристроями, які надсилають дані в конектори.

Розглянемо процеси збору, відправки та аналізу події на конкретному прикладі. Виконуємо усі етапи від встановлення SmartConnector до безпосереднього аналізу подій у консолі користувача.

Уявимо, що в нас є критично важливий хост, з встановленим ОС Windows на ньому. Перегляд журналів на самому комп’ютері або сервері доволі не зручний, крім того, через деякий час, дані перезаписуються та втрачаються. Перед фахівцями SOC стоїть задача налаштувати відправку подій на Arcsight ESM для проведення моніторингу та аналізу. Виконання відповідної задачі починається із встановлення та налаштування конектору. Його можна встановити як безпосередньо на сервері так і на іншому хості, для віддаленого читання даних. Запускається засіб інсталяції конектора, специфікується шлях встановлення.

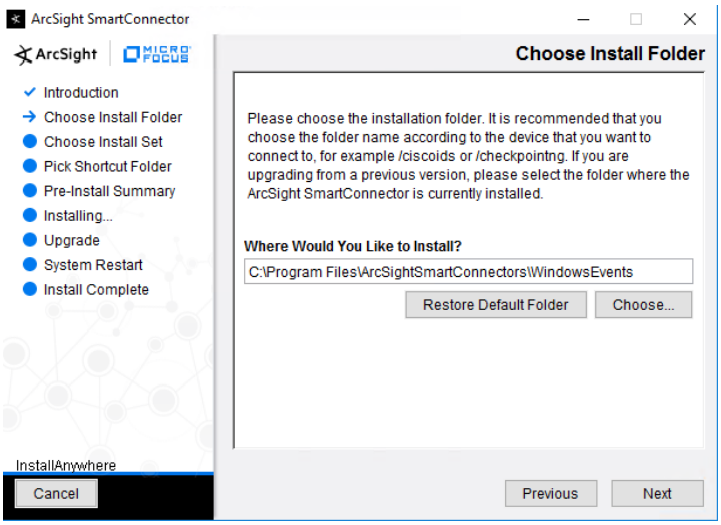
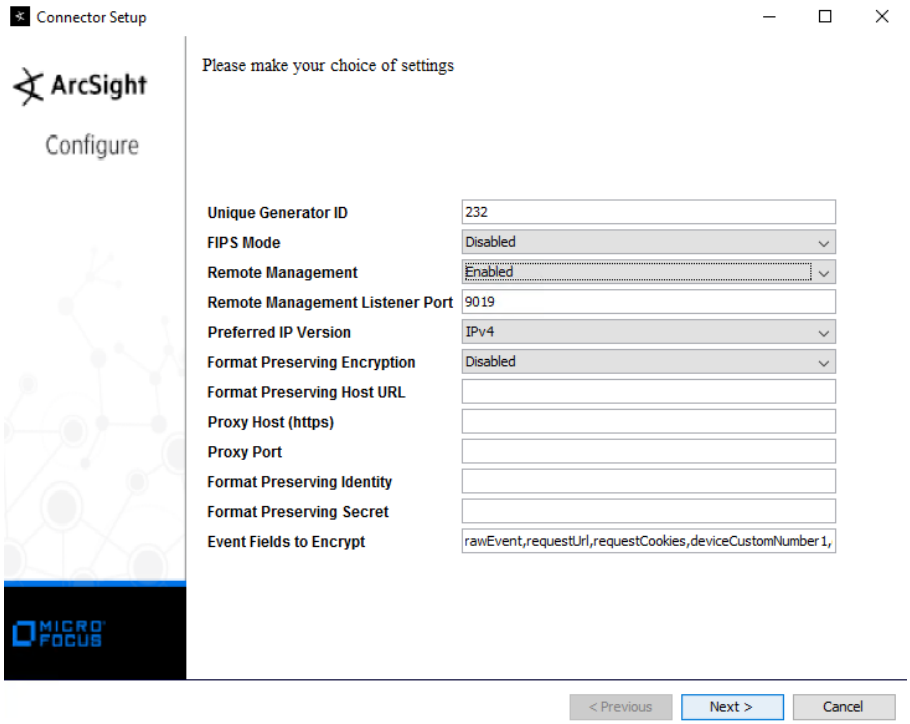


Рис.2.8. Початок установки SmartConnector

Задаються параметри конектора, такі як: Унікальний ідентифікатор, порт для віддаленого керування засобом ArcMC, версія IP, налаштування шифрування, налаштування проксі, рисунок 2.9.



2.9. Налаштування глобальних параметрів SmartConnector

Обирається тип конектора, нас відповідно цікавить необхідність читати події із пристрою Windows і чітко відомо, що пристрій має версію ОС новішу за

Windows XP та Server 2008, тому обирається тип “Microsoft Windows Event Log – Native”, рисунок 2.10.

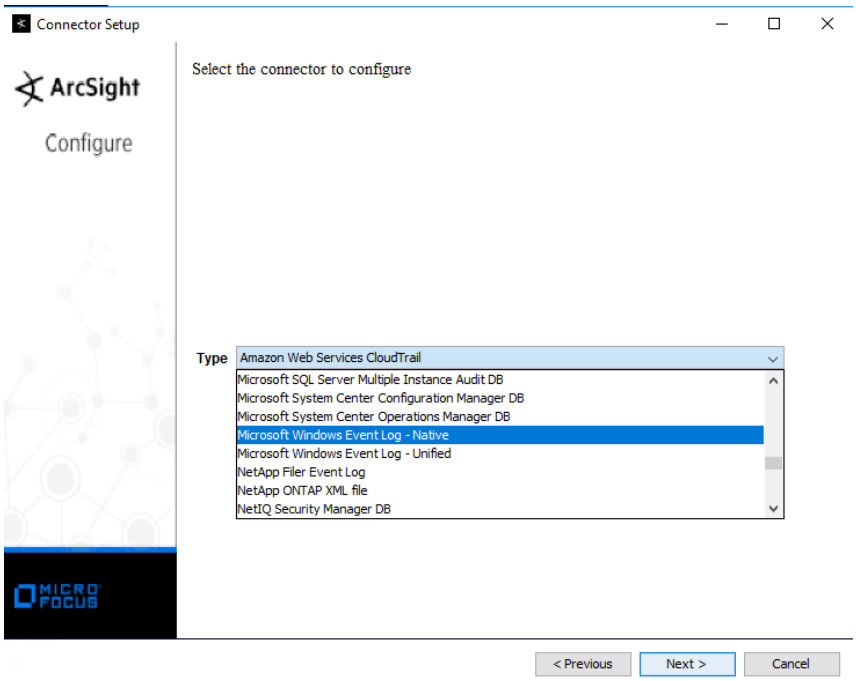


Рис.2.10. Вибір типу джерела даних для зчитування

Далі необхідно специфікувати облікові дані, з якими буде здійснюватись доступ на віддалену систему, з якої збиратимуться події. Для цього заздалегідь мають бути проведені такі налаштування: налаштовано обліковий запис, що має доступ на читання логів на пристрої (доданий локально або в домені у групу Event Log Readers), відкрито мережевий доступ до хосту-джерела подій, включені правила Windows Firewall на Віддалене управління журналами. Дані про те, як саме налаштовувати зчитування містяться окремо у посібниках із налаштування різнихи типів конекторів. Якщо відповідні налаштування проведено, то необхідно вписати дані у відповідні поля, що зображені на рисунку:

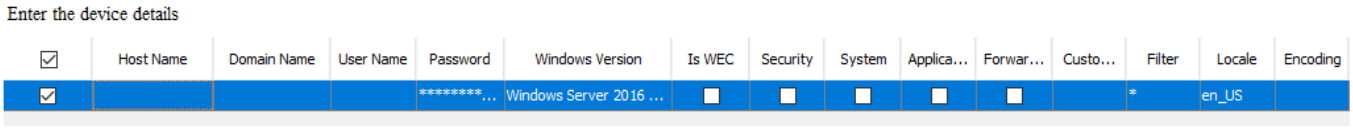


Рис.2.11 Налаштування параметрів зчитування подій з системи ОС Windows

Ім’я хосту, доменне ім’я, користувач, пароль, версія ОС Windows та обрати категорію подій, яку необхідно збирати, можна відфільтрувати які саме ID Windows-подій збирати.

Далі має бути специфіковано куди саме відправляти вже оброблені у конекторі події. Для відправки у ESM необхідно зазначити доменне ім’я серверу з

встановленим ESM, порт на якому працює Manager, та користувача у системі ESM, який буде реєструвати конектор і ініціюватиме обмін сертифікатами між SmartConnector та ESM, рисунок. Відповідно у процесі додатково потрібно задати ім’я конекторові, обрати тип інсталяції: служба або додаток. За необхідності можна додавати більшу кількість різноманітних хостів як з платформи ArcSight та інших для прийому оброблених подій.

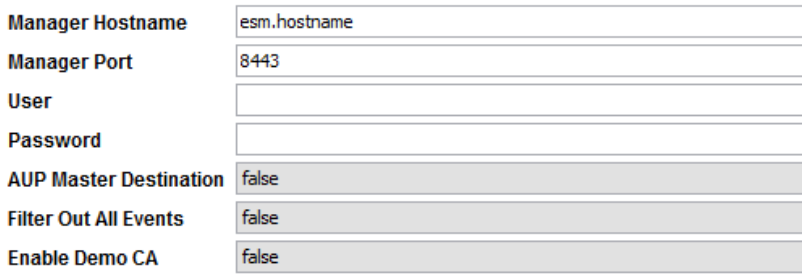


Рис.2.12. Налаштування відправки нормалізованих подій у ESM

У засобі Arcsight Console необхідно пересвідчитись, що конвектор встановлено, для цього необхідно перейти на вкладку “Connectors” та перевірити його наявність у папці “Site connectors”. Конектор із назвою Windows успішно додано до ESM, рисунок.

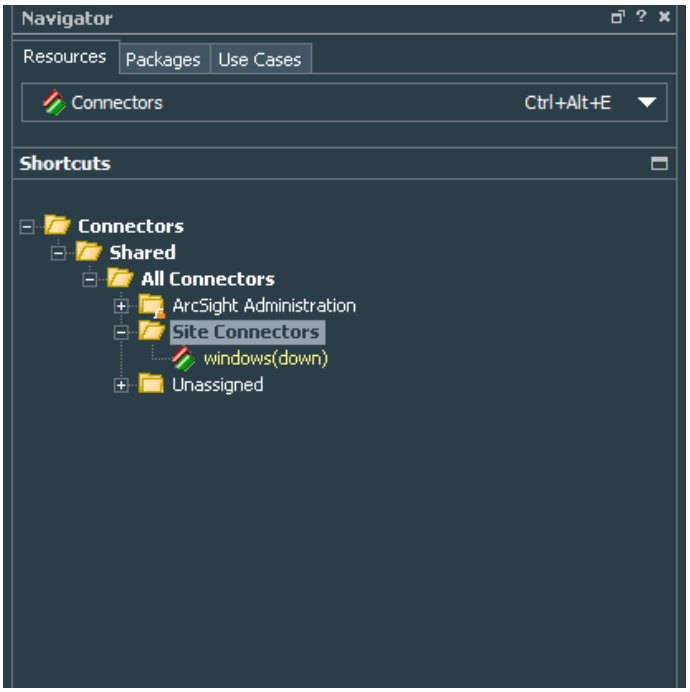


Рис.2.13 Панель управління конекторами в ESM Console

Проводимо перевірку наявності потоків подій із пристрою, що нас цікавить, для цього формується Активний канал (англ. Active channel) для збору подій лише з цього пристрою, рисунок (усі критичні дані приховано).

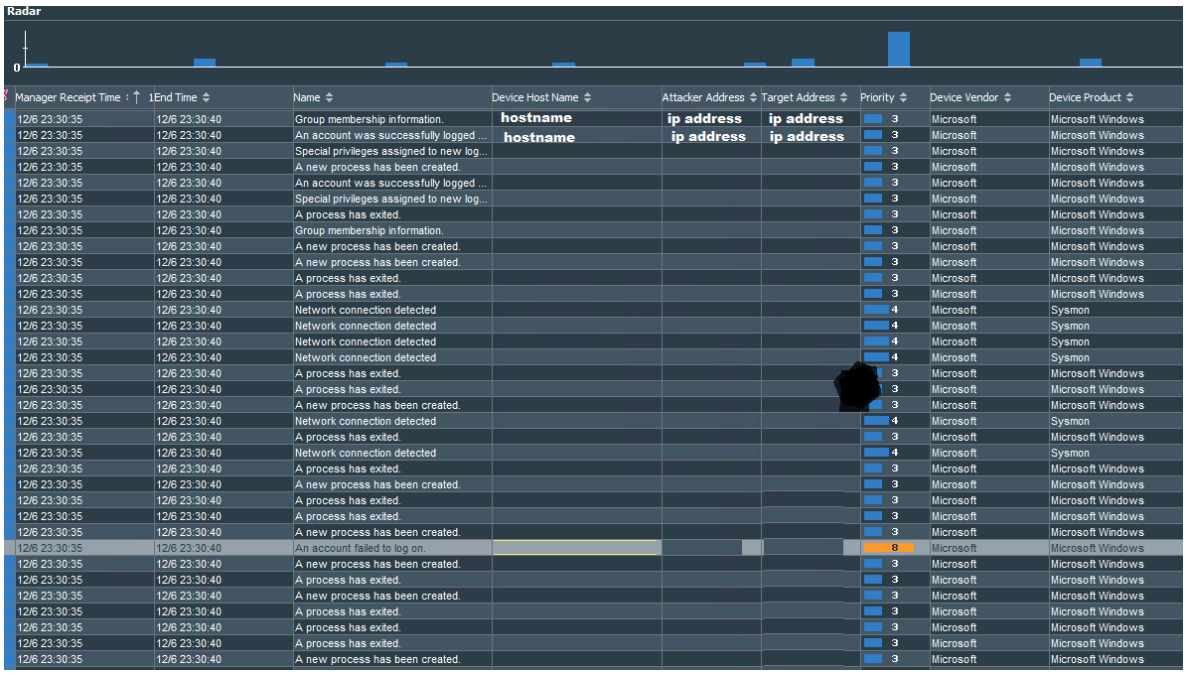


Рис.2.14 Активний канал у ArcSight Console

У каналі видно події, а отже це означає, що конектор було налаштовано правильно і пристрій було підключено на відправку подій до ESM. Таким чином виглядає Активний канал у веб-інтерфейсі Arcsight ESM Command Center:

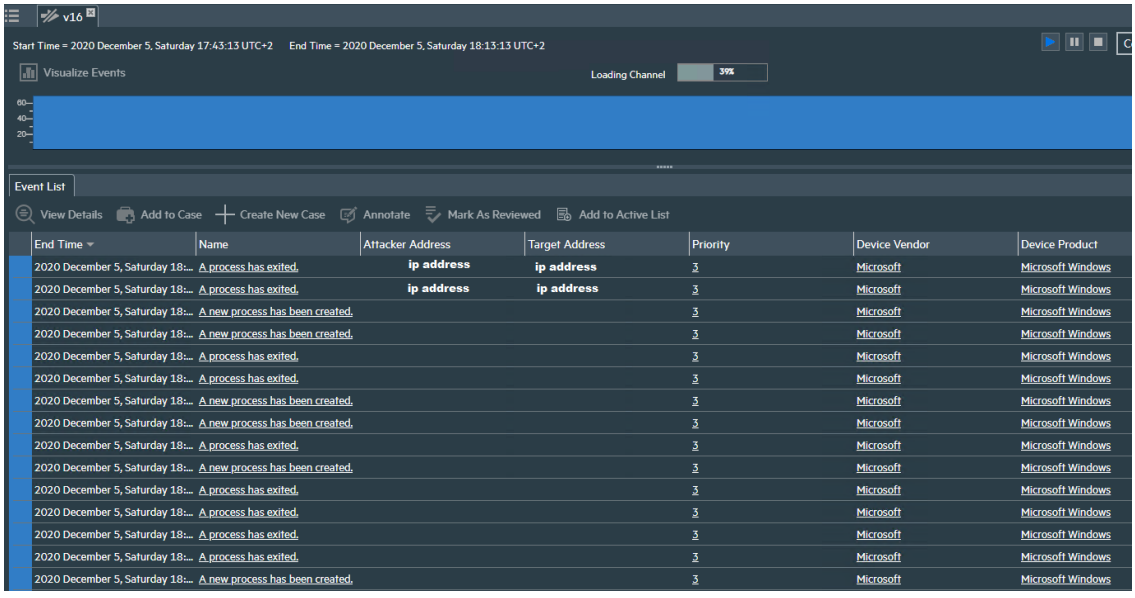


Рис.2.15 Активний канал у ArcSight Command Center

На попередньому серед усього переліку подій низького пріоритету можна знайти подію із пріоритетом 8 із назвою An account failed to log on, щоб дізнатися більше деталей необхідно її відкрити і продивитись значення усіх полів. Стосовнно конкретно цієї категорії подій, фахівця має зацікавити те, який на який саме обліковий запис була спроба авторизації, і якої IP-адреси та хосту, також приблизну геолокацію, в якій зареєстровано IP-адреси. Відповідні дані можна визначити, переглянувши значення полів Attacker Hostname та Attacker Address для імені хосту та адреси відповідно, які ініціюють запит на авторизацію на нашому сервері. Також з’ясовано, що цільовим обліковим записом є “target user” і всі адреси, що фігурують, локально знаходяться у Києві.

Attacker Host Name	**attacker hostname**
Attacker Address	**attacker IP**
Attacker Zone	<Resource URI="/All Zones/Site ABABCVyn8f4hndkw==/>
Attacker Zone ID	M2eB0V3ABABCVyn8f4hndkw==
Attacker Zone URI	/All Zones/Site Zone
Attacker Zone Resou...	(
Attacker Zone Name	(
Attacker Port	60361
Attacker Process Na...	0x0
Attacker Geo Countr...	UA
Attacker Geo Locatio...	Kyiv
Attacker Geo Longitu...	30° 30' 0" E
Attacker Geo Latitude	50° 25' 0" N
Attacker Geo Countr...	Ukraine
Attacker Geo Countr...	/arcsight/web/images/flags/ua.gif
Target	
Target Host Name	**target host**
Target Address	**target IP**
Target Zone	<Resource URI="/All Zones/Site Zone 3CVv7M05mwCmw==/>
Target Zone ID	M2eB0V:
Target Zone URI	/All Zones/Site Zon
Target Zone Resource	
Target Zone Name	
Target Nt Domain	**Domain**
Target Asset ID	4nStY6XEBABC0HizmLS4I1Q==
Target Asset Local ID	17179878741
Target Asset Resour...	
Target Asset Name	**target host**
Target User Name	**target user**
Target Process Name	-
Target Geo Country ...	UA
Target Geo Location I...	Kyiv
Target Geo Longitude	30° 30' 0" E
Target Geo Latitude	50° 25' 0" N
Target Geo Country ...	Ukraine

Рис.2.16 Детальні дані про подію у Console

Важливо розуміти та знати імена та адресацію хостів, що є мережі та їх функції, щоб знати яка саме подія може бути дійсно небезпечною, а яка ні. У цьому випадку було зареєстровано звичайну активність між хостами у

корпоративній мережі, та їх поведінка відома фахівцям, то ж інциденту в цій події немає. Той саме, аналіз, але у веб-інтерфейсі на рисунку 2.17.

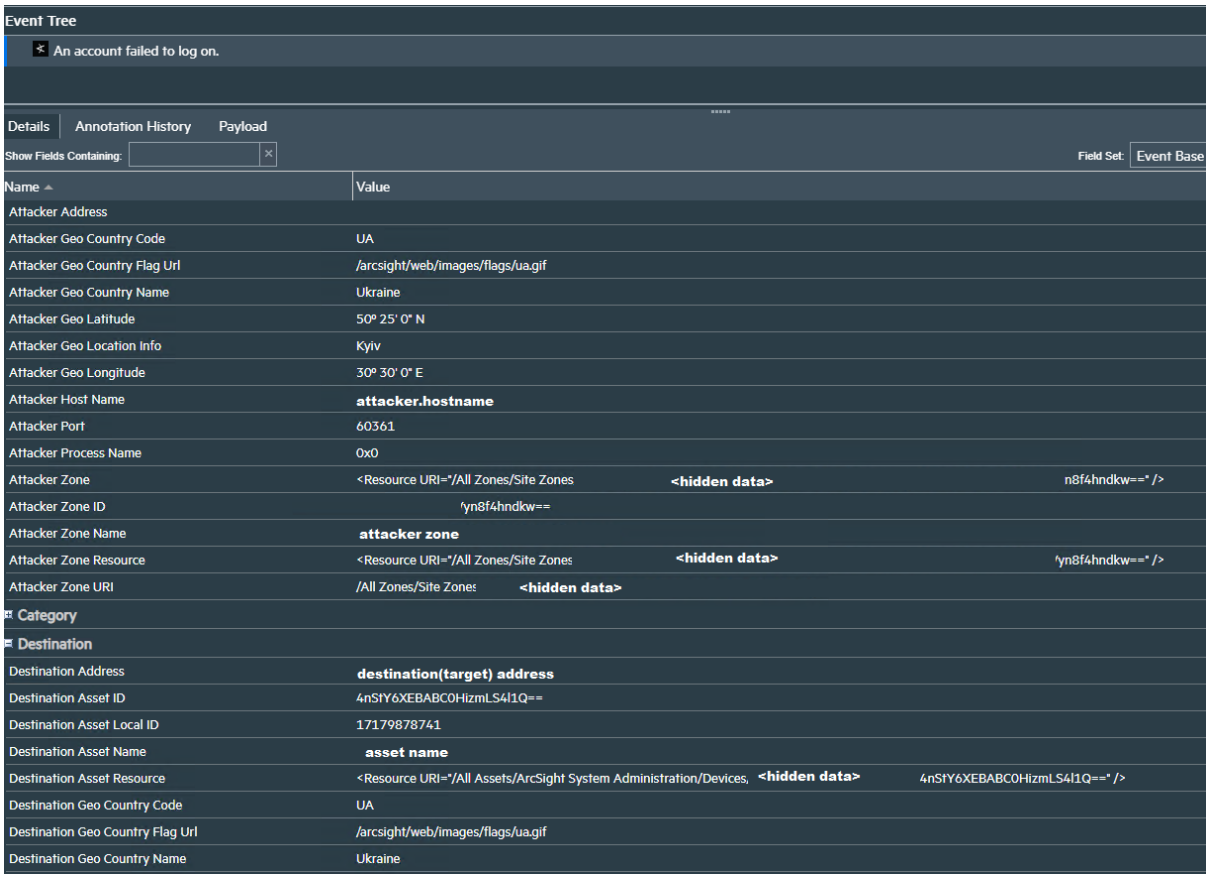


Рис.2.17 Детальні дані про подію у Command Center

Для порівняння варто розглянути як така ж сама подія, виглядає на самій Windows машині.

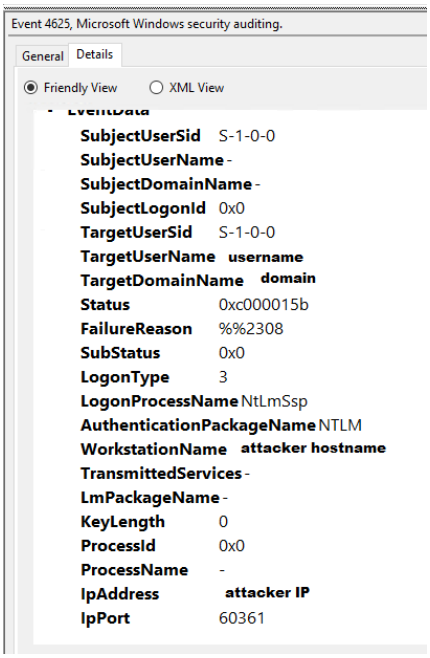


Рис.2.18 Дані про подію у Windows Event Viewer

А ось в такому вигляді вона потрапляє в SmartConnector:

{"System":{"EventId":"4625","Version":"0","Channel":"Security","ProviderName":"Microsoft-Windows-Security Auditing","Computer":"<hostname>","EventRecordID":"2475637","Keywords":"Audit Failure","Level":"Information","Opcode":"Info","Task":"Logon","ProcessID":"936","ThreadID":"976","TimeCreated":"1607290113406","UserId":""},"EventData":{"SubjectUserSid":"NULL SID","SubjectUserName":"-","SubjectDomainName":"-","SubjectLogonId":"0x0","TargetUserSid":"NULL SID","TargetUserName":"<username>","TargetDomainName":"<Domain Name>","Status":"0xc000015b","FailureReason":"The user has not been granted the requested logon type at this machine.","SubStatus":"0x0","LogonType":"3","LogonProcessName":"NtLmSsp ","AuthenticationPackageName":"NTLM","WorkstationName":"<hostname>","TransmittedServices":"-","LmPackageName":"-","KeyLength":"0","ProcessId":"0x0","ProcessName":"-","IpAddress":"<ip.address>","IpPort":"60361"}}

Як видно з прикладу, такий лог суттєво складніше розібрати, адже відсутне сортування за полями, що до того ж унеможливлюватиме будь-який пошук подій за параметрами, що нас цікавлять.

2.2.2 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. 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.

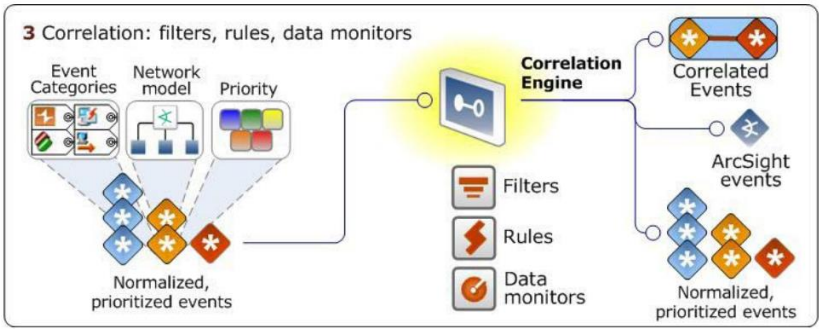


Рис.2.19 Процеси кореляції у Arcsight ESM

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.

Наприклад, різні системи в мережі можуть генерувати такі події:

- Операційна система UNIX: кілька невдалих входів
- IDS: Спроба брутфорс-атаки
- Операційні системи Windows: кілька невдалих входів

Правило кореляції об'єднує ці показники і виявляє п'ять або більше невдалих входів протягом однієї хвилини, націлених на одну й ту ж цільову систему. Виходячи з цих фактів, це поєднання подій означає спробу проведення брутфорс-атаки.

Далі операційна система Windows повідомляє про успішний вхід із того самого пристрою. Спроба брутфорс-атаки з подальшою успішною авторизацією на тій же системі підвищує ризик того, що атака була успішною.

Щоб перевірити, чи була атака успішною, можна проаналізувати обсяг трафіку, спрямований на цільову Windows машину. У цьому випадку раптовий стрибок трафіку до цієї машини може підтвердити, що брутфорс-атака була успішною.

Інструменти кореляції ESM використовують статистичний аналіз, Булеву логіку та агрегацію для пошуку подій із специфікованими характеристиками[10]. Спеціальні налаштовані правила можуть виконувати автоматичні дії для захисту мережі.

Фільтри подій. Вони є набором умов(англ. conditions), що фокусуються на певних атрибутах події. Цей фокус також зменшує кількість подій, які обробляє система. Фільтри застосовуються в багатьох частинах життєвого циклу події SmartConnector'ом, Менеджером та механізмом кореляції. Фільтри також використовуються у моніторингу, аналізу та звітах.

Фільтри, застосовані на SmartConnector, вибирають лише ті події, які відповідають заданим параметрам, і саме ці події передаватимуться менеджеру для обробки. Події, що не відповідають цим параметрам не пересилаються менеджеру. Фільтри, застосовані в Менеджері, вибирають, які події він буде обробляти, виходячи із заданих параметрів. Події, які не відповідають цим умовам, не беруться до уваги, але вони зберігаються в сховищі даних. Усі умови, побудовані в ESM, є виразами, які складаються із певного значення або змінної, оператора (наприклад NOT(!=), AND(&), OR(||)) та другого значення або змінної, за допомогою яких обчислюється перше значення.

Правила. Запрограмований процес, який оцінює вхідні події за конкретними умовами та паттернами, і, знаходячи збіги, може ініціювати дії у відповідь. Правила є центральним елементом ESM Correlation Engine і виявляє конкретне значення з постійного потоку подій.

Кореляційні правила подібні до правил системи виявлення вторгнень (IDS), за винятком того, що вони працюють з потоками подій замість потоку бітів. Вони побудовані за принципом порівняння агрегації та булевих патернів для оцінки об'єктів, таких як поля подій, моделі мережі та активні списки.

Правила виражають параметри, за якими оцінюється весь потік подій. Ці параметри можуть посилатися на:

- Мережеву модель
- Модель активів
- Формула пріоритету
- Активні списки
- Сеансові списки

Правила можуть бути побудовані модульно для використання блоків інших умов, виражених у:

- Фільтри
- Інші правила
- Кореляційні дата-монітори

Правила повинні бути активовані, щоб працювати з даними у режимі реального часу. При активації, правила проводять оцінку кожної події за визначеними параметрами.

Правила, параметри яких були дотримані, генерують подію ESM, яка називається скорельованою подією, яка повертається до життєвого циклу події у Менеджері і сама оцінюється Менеджером та процесами кореляції. Стандартні правила спрацьовують, коли події відповідають одній або кільком умовам, наприклад, події, виявлені на критично важливому пристрої і класифікуються як злоякісна активність.

Можна налаштувати правило для агрегації подій із атрибутами відповідності, які відбуваються протягом певного встановленого інтервалу часу. Наприклад, якщо правило налаштовано на агрегацію трьох подібних подій, то правило спрацьовує, коли ці три події відбуваються у визначений проміжок часу.

Стандартні правила можуть мати об’єднання (англ. joins). Об’єднання подій з різних пристроїв за атрибутами, які можуть бути спільними для всіх пристроїв. Правила приєднання розпізнають шаблони, що включають більше одного типу подій. Правила приєднання ініціюються подіями, які відповідають двом або більше наборам умов, але не береться часовий інтервал, крім часового інтервалу, представленого кількістю даних про події, які у вас є для порівняння.

Наприклад, правило приєднання може бути запущено, якщо є подія з вашої системи виявлення вторгнень та відповідна подія дозволу з брандмауера, і обидва націлені на один і той же актив на одному порту від того самого зловмисника. Якщо правило об’єднання налаштовано на агрегування, правило спрацьовує, якщо зазначена кількість відповідних подій відбувається протягом зазначеного періоду часу.

Наведемо приклад простого правила у Arcsight ESM. Розглянемо активне правило, що працює зараз у режимі реального часу – “Account Locked Out” – відповідно до назви, це правило знаходить облікові записи, які з якої-небудь причини були заблоковані.

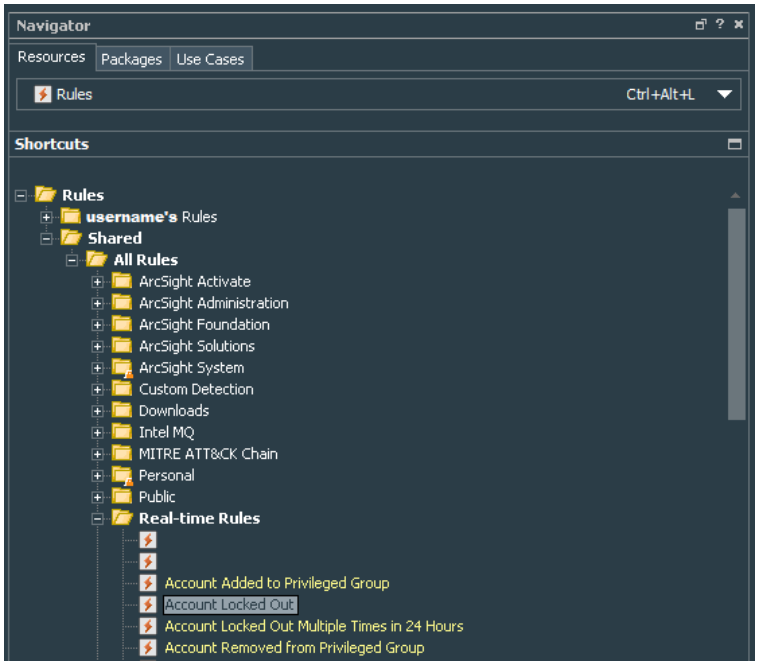
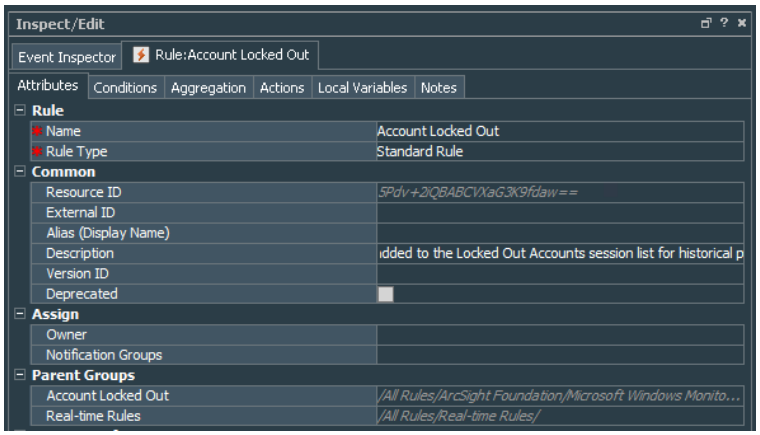


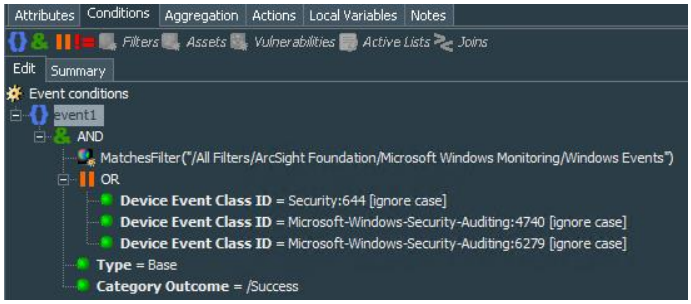
Рис.2.20 Панель управління правилами в Console

Атрибути правила: назва та тип правила, опис та додаткові, за необхідності, додаються вручну для зручності роботи фахівців. Опис відповідно містить такі дані: «Це правило виконує пошук подій із блокування облікових записів користувачів Microsoft Windows. Після кожної події обліковий запис користувача додається до сеансового списку – «Accounts Locked Out Multiple Times in 24 Hours» – облікових записів заблокованих кілька разів за 24 години, значення критичності пристрою та агента встановлюються на Середній рівень, а команда операторів SOC отримує повідомлення. За замовчуванням сповіщення вимкнено. Якщо обліковий запис користувача вже є у списку сеансів, кількість заблокувань просто додається. Обліковий запис також додається до списку сеансів " Locked Out Accounts ".»



2.21.Атрибути правила

І так, судячи із опису, з'ясовуємо, що це правило нам допоможе знаходити правила лише від пристроїв із ОС Windows, необхідно зрозуміти за яким саме принципом це працюватиме, розглянемо вкладку "Conditions", рисунок 2.22.



2.22 Умови спрацювання правила

І так, судячи із налаштованих умов правило спрацьовує за наступним алгоритмом, рисунок: 1) пошук подій, що стосуються саме систем із операційною системою Windows (визначено фільтром Windows Events); 2) подія Windows категорії Security із ID 644 – "User Account Locked Out" (для систем Windows XP\2003 та старші), або Security подія із ID 4740 – "A user account was locked out" (для систем Windows 7\2008 R2 і новіші), або Security подія із ID 6279 – "Network Policy Server locked the user account due to repeated failed authentication attempts" (для систем Windows 7\2008 R2 і новіші); 3) подія має бути базова, не скорельована; 4) лише успішна подія – категорія подій "Success", тобто "Attempt"(спроба) та "Failure"(невдача) правило не розглядатиме.

Агрегація, відповідно до рисунку 2.23, у цієї події доволі проста, окрім фільтрів, правило спрацьовуватиме на кожне одне правило у межах однієї секунди, що означає, що до уваги будуть братися абсолютно усі події, а також додаватимуться лише ті події, що мають ті ж самі показники у полях, такі як назва облікового запису, IP-адреса, домен тощо.

Вкладка Actions, рисунок 2.24, демонструє які додаткові дії виконуватиме спрацювання правила. Відповідно до рисунка, кожна подія матиме чітко визначений набір полів із налаштованими значеннями вручну або взятими із оригінальної базової події(позначені символом $ на початку). Записи про заблоковані облікові записи будуть вестись у сеансові списки, для кожного з них чітко визначено шлях та набір полів для запису. Є можливість налаштувати сповіщення про скорельовану подію для різних груп користувачів із різним заголовком.

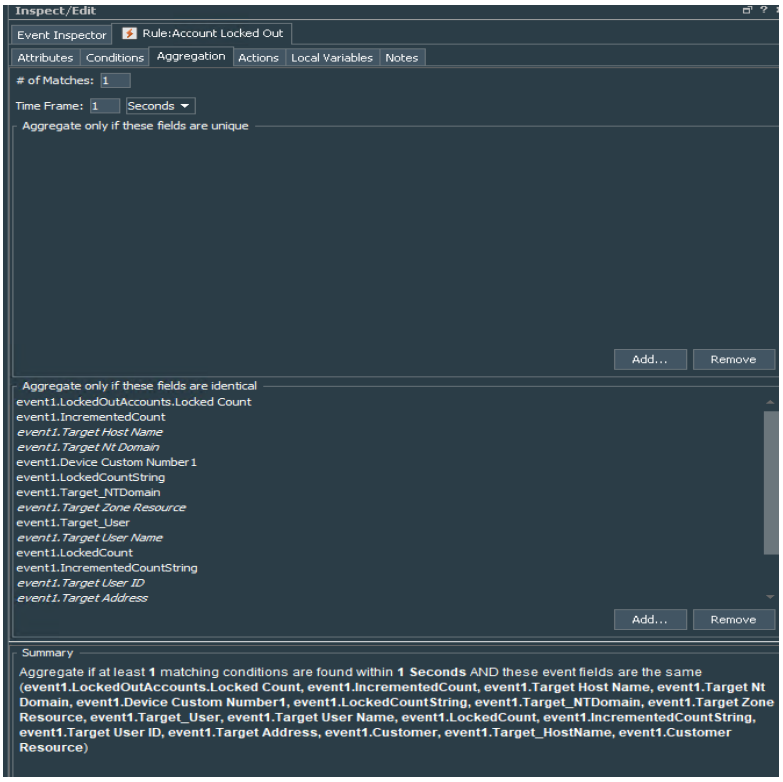


Рис.2.23 Параметри агрегації події

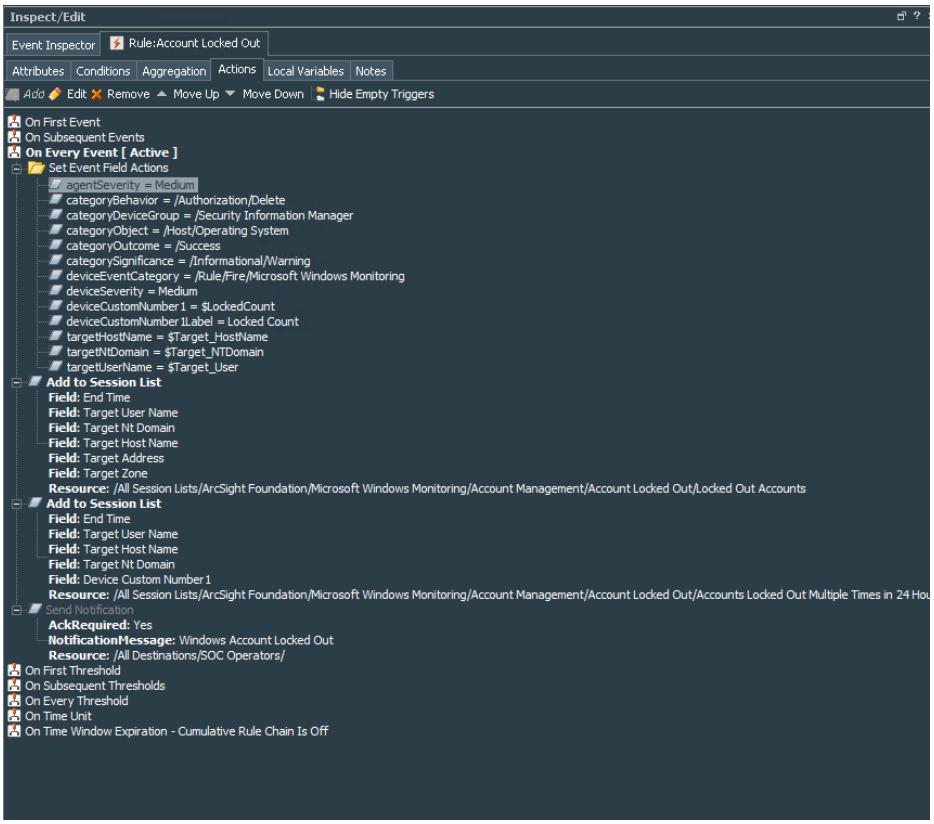


Рис.2.24. Дії, які ініціюватиме спрацювання правила

2.2.3 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.

Активний канал відображає потік інформації, визначений параметрами, встановленими в редакторі активного каналу. Канал може транслювати події або відображати статус деяких ресурсів. Канал можна додатково налаштувати за допомогою вбудованих фільтрів.

Існує три типи активних каналів, які відображають різні типи даних:

- Live (живі) канали відображають постійно оновлювані дані про події у реальному часі;

- Rule канали відображають події відтворення для тестування правил;
- Канали ресурсів відображають статус певних ресурсів, таких як активи у мережевій моделі та відкриті кейси.

Типовим видом будь-якого активного каналу є таблична сітка, але активні канали також можна переглядати як діаграми різних форматів, як географічну карту чи граф подій.

Подібно до панелі приладів автомобіля, на інформаційних панелях (дешбордах) відображаються індикатори, що повідомляють про стан мережі всього підприємства. Дешборди складаються з окремих моніторів даних (англ. data monitors) та/або переглядачів запитів у різноманітних графічних та табличних форматах, які узагальнюють потік подій та повідомляють про вплив трафіку подій на конкретні системи в мережі або відображають стан компонентів ESM. ESM забезпечує безліч стандартних інформаційних панелей, а також можна створювати свої власні.

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.

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.

Рис.2.25 Інструментальна панель моніторингу між мережевих екранів

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.

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.

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.

Перейдемо до прикладу. У минулому підрозділі було розпочато розбір того, як побудовано правило Account Locked Out для систем Windows. Тепер спробуємо застосувати це правило. Проведемо ретроспективний пошук подій, що підпадають під відповідне правило, щоб переконатися, що воно спрацьовує, для цього можна налаштувати Активний канал, що виявлятиме події, визначені у вкладці “Conditions” правила. Рисунок 2.26 демонструє дані, зібрані у каналі про відповідні події, що сталися за поточну добу, у проміжку від 0 годин і до зараз(21:40). У корпоративній мережі, за цей час сталося понад 38 подій із блокування облікових записів користувачів на системах Windows. Усі скорельовані події в Arcsight ESM позначаються символом блискавки.

Розглянемо одну з подій для прикладу, рисунок 2.27. О 8:09:48 сталася одна з багатьох подій із блокування користувача, ознайомлюємося із деталями, також вивчаємо дані з базової події, що є основою для даної скорельованої події. Дані висвітлені із однаковим набором полів, можна провести порівняльний аналіз.

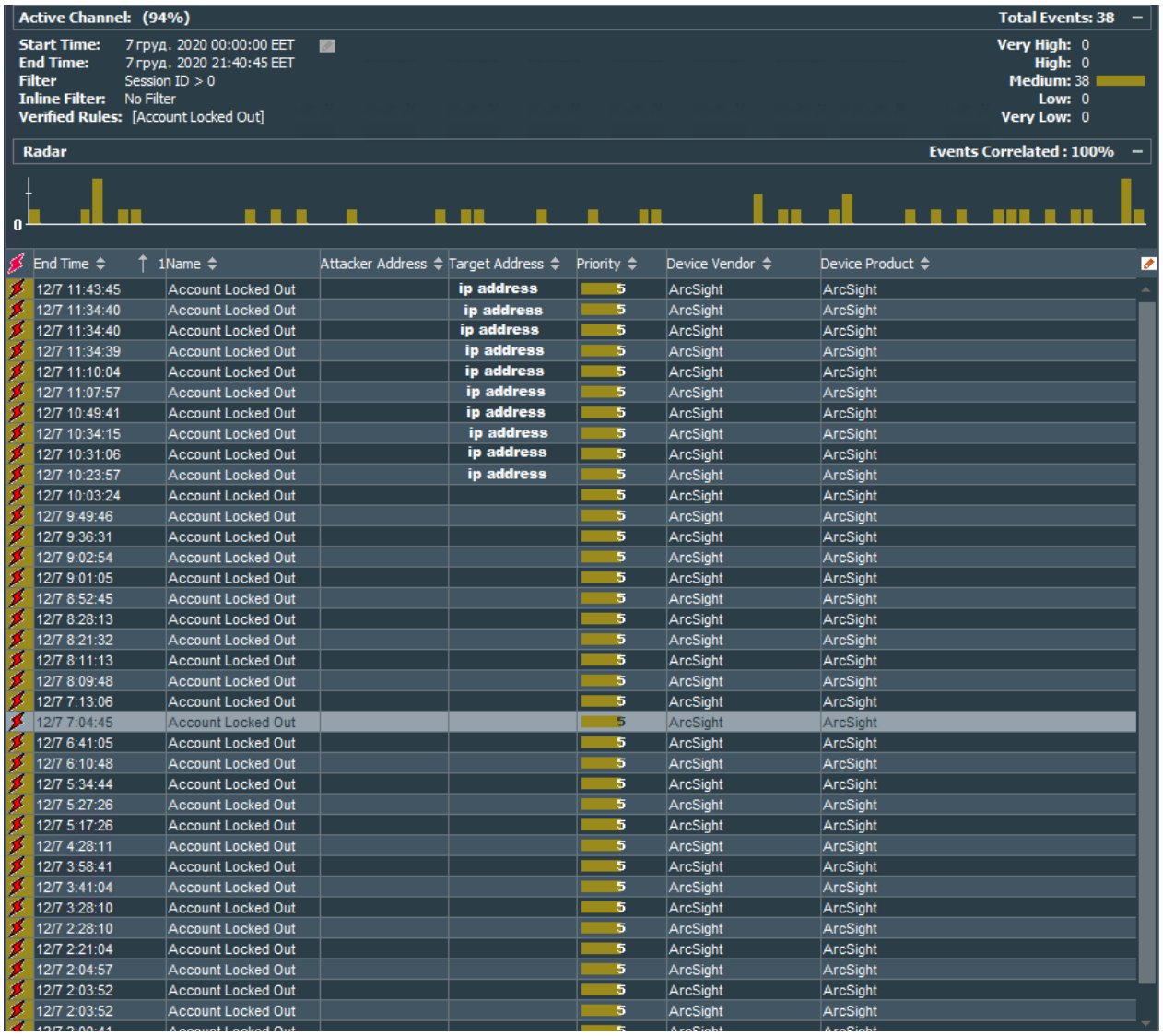


Рис.2.26 Активний канал на базі правила

Рис.2.27 Деталі подій, скорельоване (зліва) та базове (справа)

Судячи з рисунку, помітним є те, значення для низки різних полів відрізняються, дещо різні назви подій: у скорельованій події вона визначена вручну, у базовій при синтаксичному розборі. Різні записи у полях типу “Category”, різні оцінки рівня загрози та пріоритетів – Medium та Low. Значення полів Agent Host Name та Device Host Name також відрізняються – причина

полягає в тому, що для скорельованої події джерелом базової події є подія, що вже потрапила у ESM, і механізм кореляції також знаходиться на хості із ESM; для базової події агентом буде конектор, тобто у даному випадку параметр Agent Host Name відповідає імені серверу конекторів, Device Host Name – ім'я хосту на якому було виявлено подію із самого початку (робоча станція, сервер, домен-контролер). Дані про цільову систему цілком співпадають, значення target user, target username, target IP однакові. Варто звернути увагу на те, що у скорельованій події відсутня інформація про систему-джерело, та її користувача, яке могло ініціювати блокування облікового запису – це могло статися на автоматично на робочій станції, на домен контролері, на проксі-сервері. Базова подія у свою чергу містить відповідне значення та реєструє блокування користувача на домен-контролері.

Звичайному оператору доволі складно відбирати та аналізувати дані по активних каналах, адже правил дуже багато, вони довго збираються у канал, проглядати їх доволі не зручно, до того ж це створює додаткове навантаження на Manager і негативно впливає на роботу всього ESM. Для задоволення потреб у моніторингу, аби не пропустити важливі події, можна користуватись дешбордами, які самостійно відбирають події після спрацювання правила і роблять їх доступними протягом тривалого часу, можна перемикатись між цими дешбордами відслідковувати появи можливих інцидентів таким чином, до того ж це не створює такого суттєвого навантаження на систему.

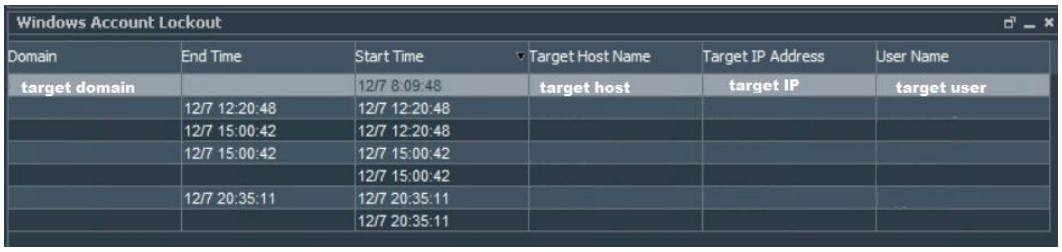


Рис.2.28 Дешборд Windows Account Lockout

Також є можливість реалізувати сповіщення про виникнення події як безпосередньо у консолі так і отримувати їх електронною поштою, що позбавить

проблеми неінформованості про можливі інциденти у не робочі часи, коли немає доступу до консолі.

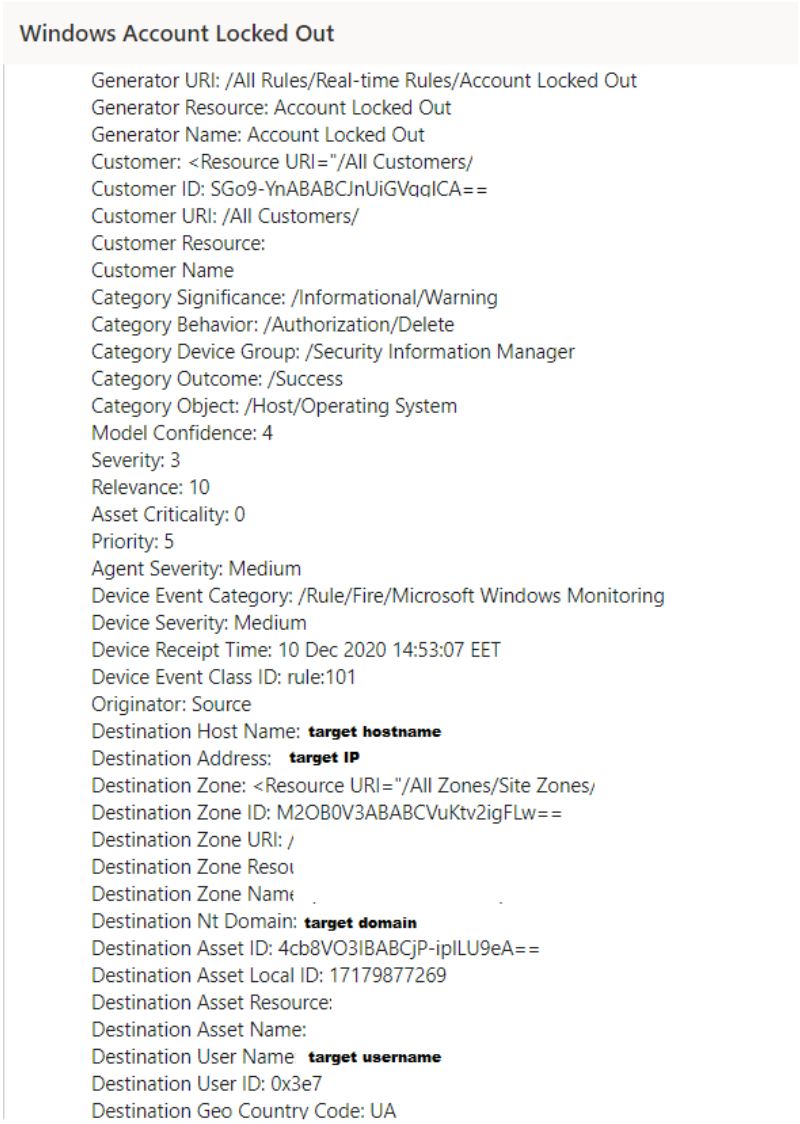


Рис.2.29 Сповіщення на пошту про спрацювання правила

Для отримання статистичних даних про події із блокування облікових записів користувачів Windows можна сформувати відповідний звіт. Для цього у консолі необхідно перейти до вкладки Reports, і у відповідному шляху знайти шаблон для формування звітів за необхідною категорією подій, задати необхідні параметри, такі як розмір, часовий проміжок збору даних, формат тощо.

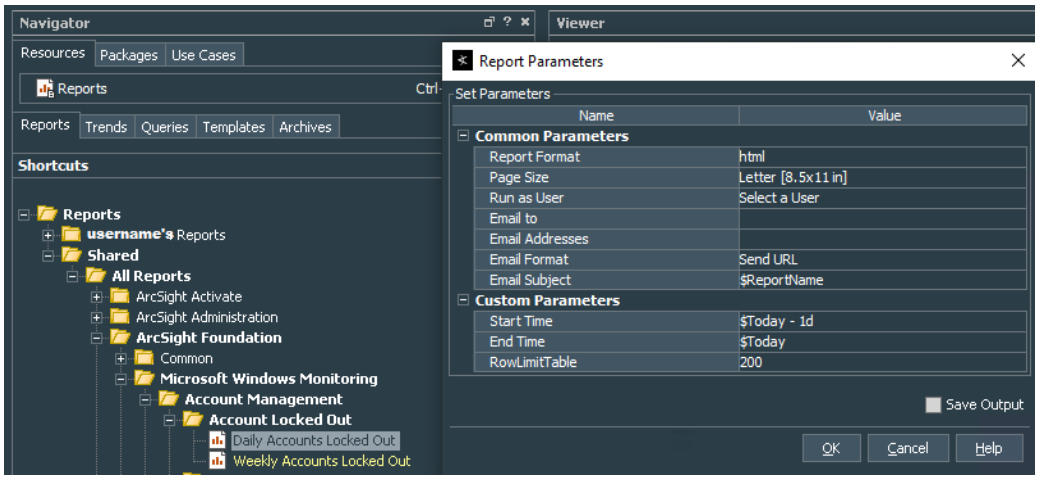


Рис.2.30 Налаштування параметрів звіту

Daily Accounts Locked Out

Domain	Target Zone Name	Target IP Address	Target Host Name	User Name	Time
domain	Coprorate Network Zone (1.0.0.0 - 1.0.255.255)	1.0.10.10	target.dc	petro	Dec 9, 2020 11:11:15 AM
					Dec 9, 2020 12:40:54 PM
					Dec 9, 2020 2:11:10 PM
					Dec 9, 2020 3:41:00 PM
					Dec 9, 2020 5:13:08 PM
					Dec 9, 2020 6:41:18 PM
					Dec 9, 2020 8:10:58 PM
					Dec 9, 2020 9:41:07 PM
					Dec 9, 2020 10:53:36 PM
				serhiy	Dec 9, 2020 1:37:58 AM
					Dec 9, 2020 3:17:59 AM
					Dec 9, 2020 5:42:45 AM
					Dec 9, 2020 7:11:45 AM
					Dec 9, 2020 8:39:00 AM
					Dec 9, 2020 10:21:01 AM
				olga	Dec 9, 2020 2:51:39 AM
					Dec 9, 2020 4:31:39 AM
					Dec 9, 2020 7:27:34 AM
					Dec 9, 2020 8:31:41 AM
					Dec 9, 2020 9:42:57 AM
					Dec 9, 2020 11:27:30 AM
					Dec 9, 2020 1:54:57 PM

Рис.2.31 Звіт про заблоковані облікові записи протягом доби

Рисунок 2.31 демонструє приклад простого звіту із інформацією про користувачів, облікові записи яких було заблоковано протягом доби.

Cases(кейс, справа, випадок) – це вбудована система ESM-заявок, призначена для відстеження окремих або декількох пов'язаних подій та експортування даних про події до сторонніх продуктів. Кейси розроблені окремо в рамках ESM або інтегровані із сторонніми системами управління кейсами

Кейс слугує контейнером для інформації про конкретний інцидент, як правило, з однією або кількома подіями, що використовується для відстеження, розслідування та усунення інцидентів. Коли виникають з'являються підозрілі події, то можна створювати кейс та призначати їх аналітикам, які потім можуть досліджувати та вирішувати їх, користуючись інструкціями та вимога політик безпеки підприємства. Існує можливість автоматичного відкриття або оновлення справи за певних умов.

За допомогою системи управління кейсами ESM можна створювати нові кейси та призначати їх певним групам користувачів, які отримують повідомлення з доступом до нього та пов'язані із ним дані. Відповідні користувачі можуть вжити заходів самостійно або визначити конкретні дії, які необхідно виконати, та призначити кейс іншому користувачеві.

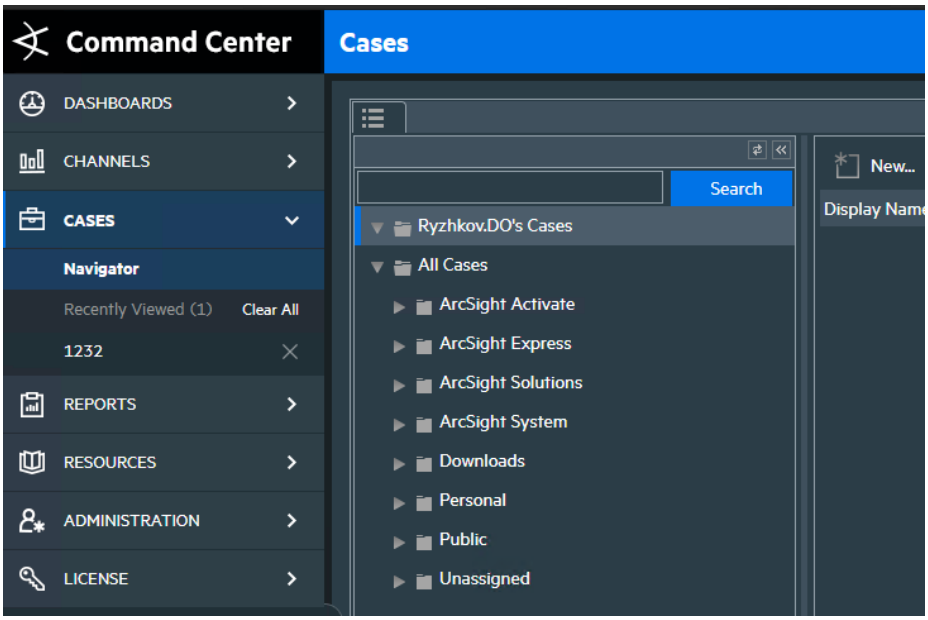


Рис.2.32 Вкладка Cases у Arcsight Command center

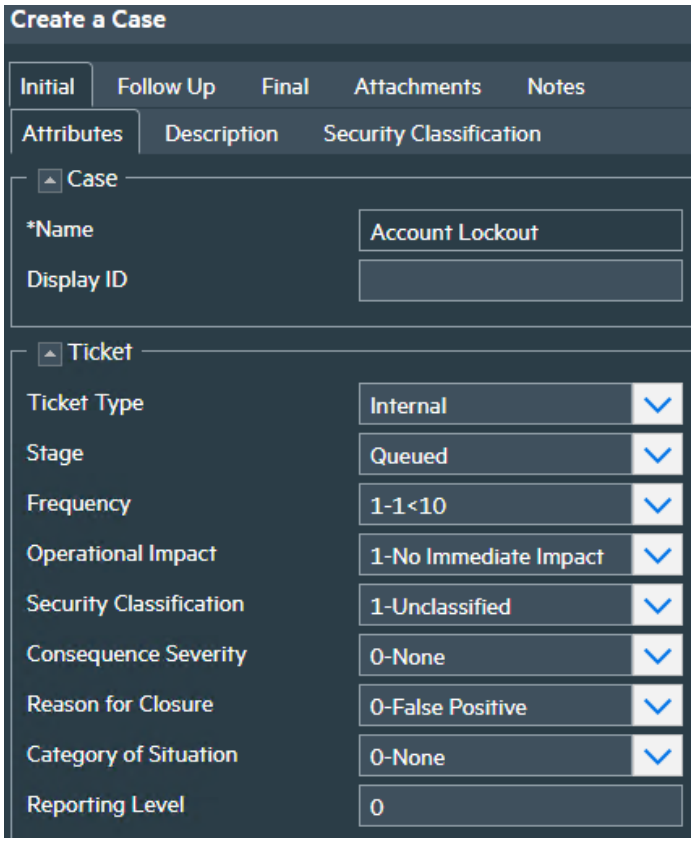


Рис.2.33 Атрибути кейсу

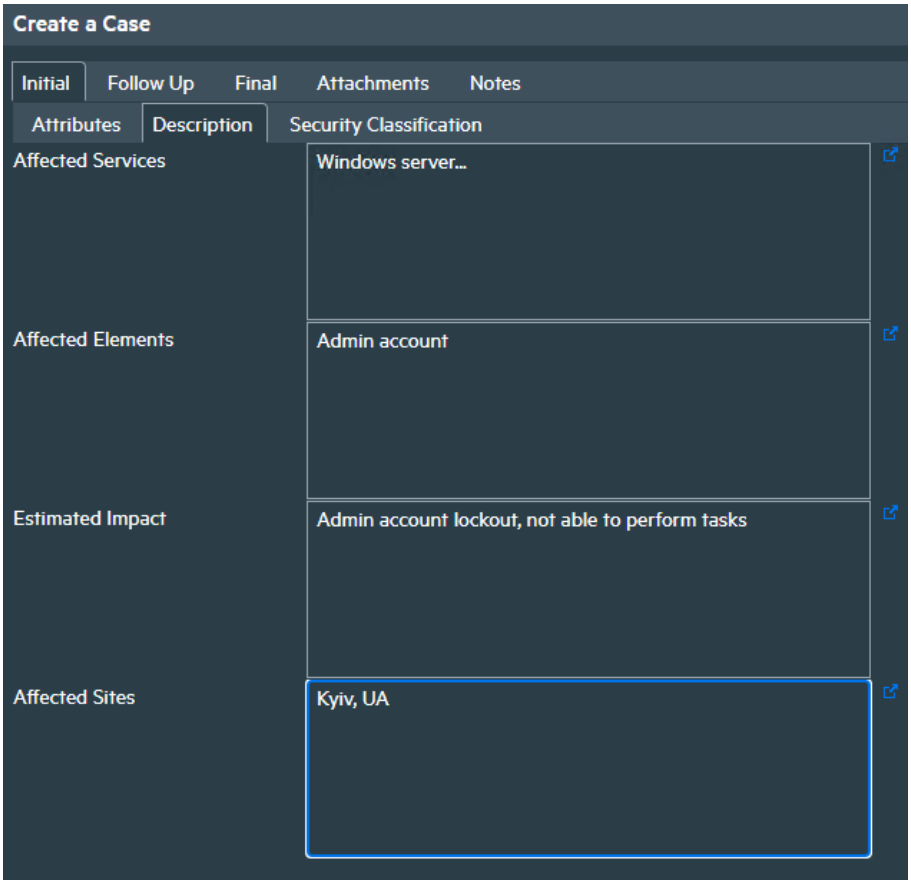


Рис.2.34 Опис інциденту у кейсі

Висновки до розділу 2

Система Microfocus Arcsight ESM є однією за найпоширеніших із SIEM систем. Вона необхідна для роботи будь-якого SOC і задовольняє потреби у процесах збору та обробки даних. Вбудовані засоби моніторингу та аналізу подій дозволяють виявляти та реагувати на інциденти, зокрема завдяки вбудованим механізмам кореляції подій.

У розділі описано життєвий цикл події від моменту його виникнення до його безпосереднього аналізу та формування звіту. Компоненти платформи ArcSight забезпечують повноцінне управління усіма процесами життєвого циклу подій, що пов’язані з інтеграцією із іншими інформаційними ресурсам, збір даних, синтаксичний розбір та потрапляння у Менеджер подій із подальшою обробкою механізмом кореляції, проведення аналізу та проведення робіт після інциденту.

Було визначено як теоретичні відомості із можливостей Arcsight ESM та SmartConnector, так і розглянуто як відповідні процеси виконуються безпосередньо фахівцем SOC кожного дня.

3 РОЗРОБЛЕННЯ ТЕХНОЛОГІЇ ПОБУДОВИ ЦЕНТРУ УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ НА БАЗІ РІШЕНЬ MICROFOCUS ARCSIGHT

Процеси із побудови SOC дуже трудомісткі, потребують достатньо багато часу на впровадження стратегії із побудови та визначення того, якого кінцевого результату необхідно досягти, а також подальші дії із пошуку та придбання необхідних інструментів, пошук фахівців та самі внутрішні процеси із налагоджування роботи стають взагалі нескінченними і продовжуватимуться протягом усього часу існування SOC. Далі у розділі розглядатимуться усі етапи побудови центру управління кібербезпекою на базі внутрішньої корпоративної інформаційної системи підприємства (англ. on-premise SOC) від самого етапу планування і до становлення повноцінного SOC, будуть надані відповідні рекомендації на основі найкращих світових практик та власного досвіду автора цієї магістерської роботи.

3.1 Підготовка та планування

Етап планування допомагає визначитися і формалізувати цілі, що виправдовують наявність SOC, а також розробити дорожню карту, яку можна використовувати для відстеження свого прогресу на шляху до цих заздалегідь визначених цілей. Перш, ніж будь-що планувати, слід оцінити існуючі на даний момент можливості тих компонентів, які стануть основою майбутнього SOC, щоб зрозуміти поточні можливості людей, процесів та технологій. Необхідно порівняти реальне положення із цілями побудови SOC, щоб встановити рівень зусиль, необхідних для досягнення цих майбутніх цілей.

3.1.1 Оцінка можливостей та зрілості SOC

Оцінка можливостей є першим кроком до розуміння того, як розробити новий або вдосконалити існуючий SOC. Результати цієї оцінки використовуються як основа, на якій будуються подальші процеси із побудови. Методологія оцінки вимог та можливостей SOC повинна бути актуальною, задокументованою, повторювана, посилатися на найкращі практики, має контролюватися та постійно вдосконалюватися. Важливо ставитись до цього як до безперервної роботи, щоб SOC міг адаптуватися до змін у бізнесі, технологіях та ландшафті загроз.

Методологія оцінки SOC, показана на рисунку 3.1, включає наступні етапи:

- Визначення цілей SOC
- Визначення можливостей, які слід оцінити на основі цілей SOC.
- Збір інформацію про можливості людей, процесів та технологій.
- Аналіз зібраної інформації та призначення рівнів зрілості оціненим можливостям.
- Представити, обговорити та формалізувати висновки.

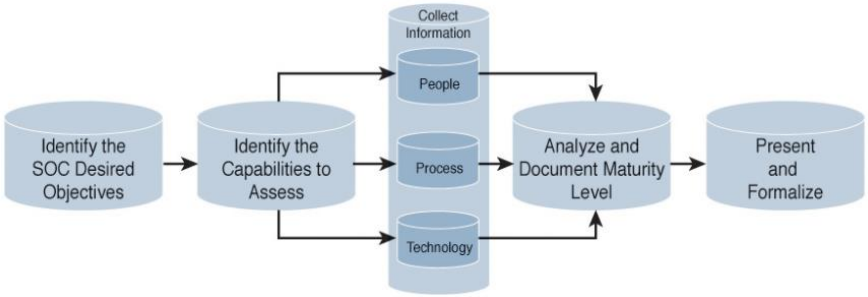


Рис. 3.1 Методологія оцінки SOC

Перш ніж заглибитися в розрахунки рівня зрілості SOC, спочатку потрібно визначити бізнес-цілі організації. Це основа, за якою буде проводитись оцінка і таким чином рівень зрілості може бути обґрунтовано. Наприклад, SOC може мати дуже талановитих пентестерів, але якщо цей набір навичок не узгоджується з бізнес-стратегією, ці навички можуть не мати великої цінності для організації або, можливо, навіть відбирати від іншої важливої посади, якою нехтують.

Багато організацій можуть бути не в змозі чітко визначити свої бізнес-цілі щодо технологій. Найкраще спочатку визначити внутрішніх зацікавлених сторін, які мають повноваження представляти організацію. Важливо зібрати відгуки від керівників різного рангу та підрозділів організації, щоб визначити, як організація бачить бізнес-цілі ІТ. Оцінка може показати, як ІТ-процеси збігаються із баченням керівництва та наскільки воно саме орієнтується в тому, які задачі виконує ІТ та які має виконувати. Звичайно ж, що оцінювати необхідно як із точки зору бізнес-процесів та із точки зору ІТ, а саме: доступності, цілісності, конфіденційності та ІТ-ризиків.

Вимоги для досягнення бізнес-мети перекладаються на ІТ-цілі. Це означає, що ІТ-цілі – це дії, які необхідно досягти для досягнення бізнес-мети, і таким чином створення SOC допомагає бізнесу бути успішним. Отже, щоб зрозуміти, як досягти бізнес-цілей, їх необхідно на ІТ-цілі. У таблиці 3.1 наведено перелік ІТ-цілей, запропонованих COBIT-5[12], ліва сторона представляє ІТ-цілі бізнесу.

Після того, як цілі бізнесу та ІТ будуть визначені, наступним кроком є оцінка ІТ-процесів, пов’язаних з кожною ціллю ІТ. Як і бізнес-цілі, цілі ІТ, як правило, складаються з безлічі ІТ-процесів. Важливо розуміти, що ІТ-процеси можна оцінювати з точки зору зрілості. Середнє значення оцінки всіх ІТ-процесів використовується для демонстрації ефективності ІТ-цілі.

ІТ-процес може складатися з конкретних вимог до людей, процесів та технологій. Ці компоненти повинні працювати як єдине ціле для сформування ІТ-процесів, узгоджених із ІТ-цілями. Оцінюючи рівні зрілості ІТ-процесів, можна кількісно оцінити ефективність ІТ-процесів, що означає, що для вдосконалення ІТ-процесу може знадобитись додаткова підготовка.

Необхідно враховувати можливості, які мають відношення до моделі функціонування SOC на додаток до послуг SOC. Прогалини у можливостях SOC можуть означати необхідність навчання, набору нових фахівців або отримання технологій.

Таблиця 3.1

IT-цілі бізнесу

Фінансові	IT комплаенс та підтримка бізнес-комплаенсу; управління бізнес ризиками, пов’язаними із IT; прозорість IT витрат, вигоди та ризиків; реалізована вигода від IT інвестування в IT послуги; прихильність керівництва за прийняті рішення щодо IT.
Користувачі	Надання IT послуг, що відповідають бізнес потребам; адекватне використання програм, інформації та технічних рішень.
Внутрішні	Гнучкість; захист інформації, обслуговування інформаційної інфраструктури та програм; оптимізація IT активів, ресурсів та можливостей; забезпечення можливостей та підтрики бізнес процесів шляхом інтеграції технологій; доступність до достовірної та корисної інформації для прийняття рішень; дотримання відповідності IT до вимог внутрішніх політик.
Навчання та зріст	Компетентний та мотивований персонал; знання, досвід та ініціативи для бізнес-іновацій.

Скласти перелік можливостей для оцінки SOC складно, оскільки кожна організація матиме різні технології та по-різному кваліфікованих людей. На рисунку 3.2 наведено загальну схему різних можливостей SOC, вони поширені в більшості середовищ SOC. Формат цього підходу розбиває можливості на такі категорії як: люди, процеси та технології.

Розпочнемо з людей. Вони ключовим компонентом будь-якого успішного SOC. Оцінюючи здібності, пов'язані з людьми, слід враховувати сфери, що стосуються управління, структури, досвіду, навчання та сертифікації. Ось

декілька областей, які слід враховувати при опитуванні людей щодо можливостей IT-процесів.

З точки зору управління важливо розуміти, як управляється SOC. Важливо також розуміти, як організація розглядає та керує SOC.

З точки зору структури необхідно знати структурні підрозділи організації, щоб визначити тих осіб, хто має належні повноваження відповідати на ваші запитання та для розуміння від хто саме за які функції відповідає та який рівень повноважень та відповідальності має. Це також стосується і внутрішньої структури самого SOC – мають бути чітко визначені ролі кожного із фахівців (аналітик, пентестер, адміністратор).

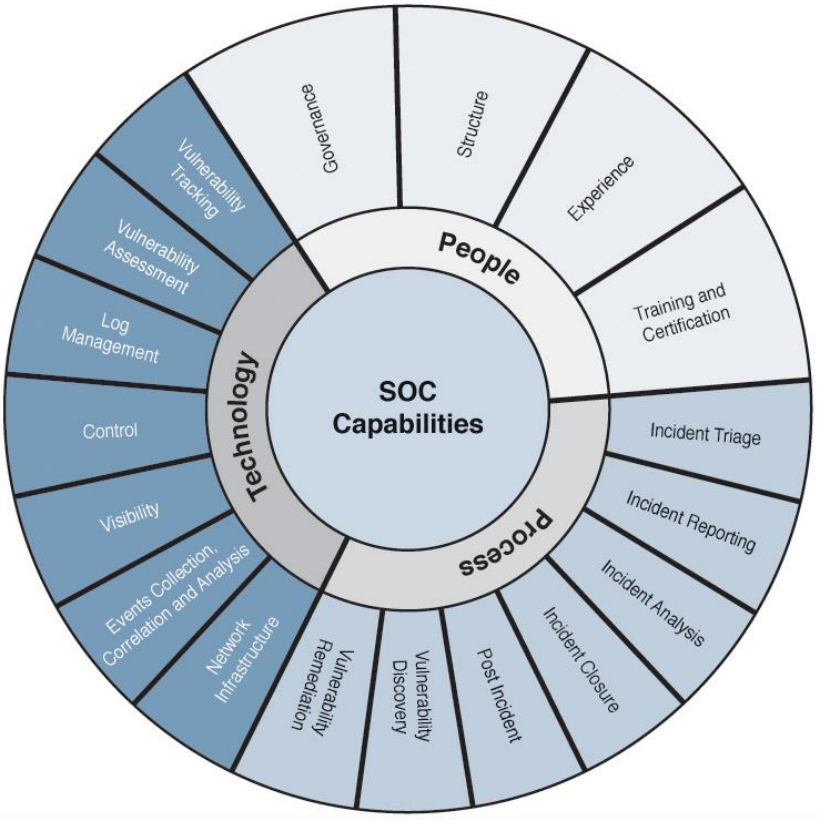


Рис. 3.2 Можливості SOC

З точки зору досвіду організації, як правило, мають ресурси, як внутрішні, так і аутсорсингові, які можуть розробляти та управляти безпекою систем та мережі. Хоча це цінні ресурси, якими захочеться скористатися у своїй програмі побудови SOC, є й інші критичні та спеціалізовані галузі SOC, які необхідно оцінити, включаючи наступні:

- Реагування на інциденти
- Цифрові розслідування
- Оцінка вразливостей
- Управління логами
- Робота з інструментами SIEM
- Розвідка загроз
- Технології Big data
- Управління людьми
- Аналіз даних

Інші аспекти досвіду SOC, які слід оцінити, включають здатність працювати під тиском, особливо під час великих інцидентів безпеки, та набори навичок. Більшість ролей мають конкретні вимоги до навичок; наприклад, люди, відповідальні за цифрові розслідування, повинні відповідний досвід та знання спеціальних інструментів.

З точки зору знань – навчання та сертифікація. Розуміння необхідності навчатись є важливим для визначення того, чи здатен SOC адаптуватися до змін та задовольняти робочі потреби працівників, підвищуючи їх кваліфікацію. Багато людей хочуть мати можливість рости в межах своєї ролі, і це, як правило, вимагає навчання та отримання сертифікатів для підтвердження нових досягнень.

Процеси. Процеси забезпечують взаємодію між людьми та технологіями. Процеси безпеки, які потрібно оцінити, пов’язані з тим, як обробляються інциденти та вразливості в системі безпеки. Розуміння та документування поточного стану процесів SOC є важливим для розробки відповідної та реалістичної дорожньої карти розвитку SOC. Процеси SOC можна класифікувати за сортуванням інцидентів, повідомленням про інциденти, аналізом інцидентів, закриттям інцидентів, дії після інциденту, виявленням вразливостей, їх усуненням та відстеження.

Подібно до людей та процесів, використання правильно підібраних та налаштованих технології є критичним для успіху SOC. Категорії технологій, які слід оцінювати, пов’язані з готовністю інфраструктури, збором та обробкою

журналів, моніторингом системи, контролем безпеки та управлінням уразливостями до цього також можна віднести взаємодію з питань реагування на інциденти та обслуговування систем із іншими структурними підрозділами як всередині, так і поза організацією.

Після визначення вищевказаних бізнес та IT-цілей та визначення поточних можливостей SOC, пов'язані з IT-процесами необхідно зібрати всю цю інформацію для подальшого аналізу. Далі ми розглянемо, як правильно збирати інформацію в процесі оцінювання.

Під час процесу оцінювання буде необхідність зустрічатися та спілкуватися з представниками різних ролей в організації. Починаючи з керівника організації, як правило, з генерального директора або з подібної ролі, і аж до системних операторів. Необов'язково бути експертом з абсолютно усіх аспектів SOC, а це означає, що ви можете не розуміти деякі зібрані дані, можливо, неправильно трактувати спосіб запису результатів. Щоб уникнути спотворення даних, необхідно підходити до даного процесу з точки зору консультанта, який є частиною команди, яка пропонує різні погляди на кожен предмет, який перевіряється (мають бути уповноважені особи, які підтверджують результати).

Наявність експертів або кількох людей, які сприяють досягненню результатів, збільшить потенціал для успіху підсумкового звіту. Залучаючи таких фахівців як: керівники проектів, інженерів ІБ, фахівців із управління ІБ, мережевих інженерів та спеціалістів із технічної підтримки, - можна отримати додаткову підтримку у подальших процесах, адже вони відчуватимуть свою участь у процесах проектування. До того ж розширить розуміння середовища дозволить отримати більше корисної інформації, якою може володіти лише конкретна група працівників, а також допоможе уникнути непорозуміння з приводу результатів оцінювання. У деяких випадках фізичні або юридичні особи можуть спробувати вплинути на оцінку на свою користь. Тому збереження неупередженості та вимагання підтверджуючих доказів є вирішальним для точності результатів оцінки.

Окрім людей, звичайно ж, має також цікавити інформація про процеси та технології. Зазвичай це фіксується за допомогою різних документів. Іноді ці дані можна отримати із згенерованих звітів із наявною на даний момент технологією, або з документів, які ведуться вручну. Важливо перевірити точність цих даних, оскільки багато звітів можуть містити застарілі результати, наприклад стару карту мережі, що містить системи, що не використовуються. Необхідно враховувати наступні документи про процеси та технології: список IT активів, реєстр ризиків, список наявних інструментів моніторингу безпеки, список наявних інструментів управління безпекою, карта мережі, файли конфігурацій, стандарти та шаблони, політика безпеки, система заявок внутрішньої технічної підтримки та нормативні документи із процесів контролю змін (ITSM). Після того, як будуть зібрані всі дані про організацію, потрібно розрахувати ефективність людей, процесів та технологій. Ці розрахунки проводяться на етапі аналізу процесу оцінювання.

Після того, як будуть зібрані дані, що охоплюють бізнес та IT-цілі, наступним кроком є визначення їх ефективності. Це можна зробити, обчисливши рівень зрілості IT-процесу та взявши середнє значення всіх IT-процесів, які безпосередньо відносяться до певної IT-цілі. Рейтинг IT-процесу може змінюватись за ступенем оцінювання та зважування важливості процесу для IT-цілі. Діаграми рівня зрілості повинні бути налаштовані для організації, що оцінюється. У таблиці 3.2 наведено шестирівневу систему оцінювання[12] яка включає варіанти оцінки рівня зрілості.

Таблиця 3.2.

Модель оцінки зрілості COBIT

Рівень зрілості	Критерій
0- Неіснуючий	Абсолютна відсутність виявлення процесів. Організація не здатна визначити проблеми, які необхідно вирішувати.

Рівень зрілості	Критерій
1- Початковий	Є доказ того, що організація виявила наявну проблему, однак не має стандартизованих процесів і замість цього застосовує заготовлені підходи на конкретний кейс. Загалом підходи із управління дезорганізовані.
2- Повторюваний	Процеси розвинуті до рівня, коли різні люди виконують ті ж слідуючи тим же процедурам. Немає формального тренування та зв'язку стандартних процедур, покладена індивідуальна відповідальність. Високий рівень надії на індивідуальні знання, доволі високий рівень помилок.
3- Визначені процеси	Процедури стандартизовані, задокументовані та донесені протягом тренування. Однак досі існує індивідуальна відповідальність за їх дотримання, відхілення маловірогідні. Процедури не досконалі, а є формалізацією існуючих практик.
4- Керований та оцінюваний	Є можливість моніторингу та оцінки відповідності процедур і прийняття заходів на випадок сбою роботи одного з процесів. Процеси постійно вдосконалюються і забезпечуються хорошими практиками. Автоматизація та інструменти застосовуються у обмеженому обсязі.

Рівень зрілості	Критерій
5- Оптимізований	Процеси досягли рівня найкращих практик, що засновані постійному покращенні та моделюванні зрілості із іншими організаціями. IT використовується у автоматизації робочих процесів, забезпечує інструменти для покращення якості та ефективності, прискорює адаптацію до нових технологій.

Розрахунок оцінки зрілості є дуже корисним, але його потрібно задокументувати у зручному форматі, щоб інформацією можна було ділитися та була зрозумілою.

Останнє завдання процесу оцінки можливостей – це розробка остаточного звіту. Остаточний звіт повинен починатися з переліку всіх визначених бізнес-цілей та відзначати, як вони відносяться до IT-процесів, за які відповідає SOC. IT-процеси повинні містити рейтинг зрілості, щоб можна було чітко визначити їх ефективність та зрозуміти поточний стан SOC. Звіт має містити такі дані: погляди та стратегії організації; погляди та стратегії департаменту, який керує SOC безпосередньо; вимоги внутрішнього та зовнішнього комплаєнсу; ландшафт загроз організації (специфічні для окремої галузі та типу підприємства); історія попередніх інцидентів інформаційної безпеки; бюджет побудови та розвитку SOC; результат поведених заходів із оцінки рівня відповідності та зрілості. На сам кінець, звіт повинен містити посилання на використані джерела, наприклад, інформація про людей, в котрих брали інтерв'ю, які інструменти використовувались для створення звітів тощо. Крім того, варто включити деякий меседж, певну заяву, яку хотілося б донести усім, разом із звітом про оцінку можливостей.

3.1.2 Стратегія побудови та розвитку SOC

Формалізація стратегії SOC та відстеження його прогресу є ключовими аспектами для досягнення належного рівня управління процесами. Стратегія SOC базується на результатах оцінки можливостей, викладених у попередньому підрозлі, і має на меті формалізувати наступні аспекти:

- Затвердження (статуту) місії SOC.
- Стратегічні цілі SOC.
- Область застосування SOC.
- Базування SOC.
- Сервіси SOC.

Місія має узгоджуватися із баченням та стратегією бізнесу, а також із департаментом, якому підзвітний SOC. Визначаючи заяву про місію, ви повинні чітко визначити наступне:

- Область застосування SOC
- Ролі SOC
- Відділ, відповідальний за побудову, експлуатацію та підтримку програми SOC

Нижче наведено приклад місії SOC:

SOC контролює загальний стан безпеки IT-мережі, реагує та відстежує інциденти інформаційної безпеки з метою підтримання належного рівня захищеності безпеки. Функції виконуються цілодобово підтримуючи діяльність організації.

Документування **області застосування** SOC допомагає організації чітко визначити, що саме доручено виконувати SOC. Область застосування повинна передбачати рівень зусиль та ресурсів, необхідних для завершення проекту. Це критично важливо, оскільки загальноприйнятою помилкою є фінансування попередніх витрат, не включаючи додаткові витрати на встановлення, технічне обслуговування, модернізацію, підтримку, налаштування та супутні витрати на зміну або скасування угоди про рівень обслуговування. При цьому мають бути враховані такі аспекти:

- Часовий проміжок: Стратегія повинна бути обмежена періодом часу, протягом якого мають бути реалізовані стратегічні цілі SOC та досягнуто відповідного рівня зрілості. Досягнення цих цілей оцінюється під час і після періоду стратегії.
- Локації: фізичні локації, що містять елементи, що контролюються SOC (наприклад, штаб-квартира, регіональні відділення та віддалені офіси підприємства).
- Мережі: це мережі, які контролює SOC. Типові приклади включають мережі центрів обробки даних, широкосмугові мережі, локальні мережі, екстранет та точки доступу до Інтернету. В залежності від середовища можуть існувати інші мережі.
- Власність: Власність систем та інформації впливає на сферу діяльності SOC, з точки зору того, які активи будуть контролюватися та захищатися. Наприклад, мережі, які розміщують промислові системи управління, як правило, не керуються IT, і, отже, моніторинг цих активів може не входити до сфери управління SOC, яким керує IT. Залежно від інформації, яку зібрано під час оцінки SOC, ці мережі можуть охоплюватися або не охоплюватися.
- Стратегія організації: Бізнес-цілі організації та стратегії інших підрозділів повинні враховуватися в загальній стратегії SOC. Це допоможе іншим бізнес-підрозділам співпрацювати з SOC та допоможе SOC краще зрозуміти вимоги щодо захисту кожного відділу.
- Вибір технологій: Залежно від елементів, які планується контролювати, та активів, які потрібно захистити, вибір технологій буде відрізнятися в залежності від типу, розміру та дизайну:
    - Тип: Сфера застосування диктує необхідність нових технологій. Ті елементи, над якими здійснюється моніторинг, можуть вимагати впровадження певних технологій. Наприклад, може знадобитися впровадження можливості захоплення пакетів та виявлення вторгнень у кількох місцях та мережах.

  - Розмір: розгорнуті служби повинні мати можливість збирати та обробляти весь обсяг даних із усього середовища, визначеного областю застосування, що в свою чергу формує певні вимоги до апаратних потужностей та кількості і розповсюдженості пристроїв.
  - Дизайн: Розподілене або централізоване розгортання таких процесів, як управління журналами та інструменти оцінки вразливості.
- Ресурси та досвід: Деякі технології можуть бути більш складними, ніж інші, і, можливо, вимагатимуть спеціалізованих знань. Крім того, чим більший обсяг, тим більше ресурсів знадобиться для проектування, побудови та врешті-решт експлуатації SOC.
- Термін: Область застосування впливає на термін проектування та впровадження послуг SOC.
- Базування: аутсорсинг проти внутрішнього SOC
- Комплаенс: внутрішні та зовнішні вимоги комплаенсу.
- Бюджет: Звичайно, чим більший масштаб, тим вищі витрати на проектування, будівництво та врешті-решт експлуатацію SOC.

Одним із важливих питань, яке необхідно враховувати на етапі планування, полягає в тому, розвивати власні можливості SOC, можливості аутсорсингу або використовувати гібридний підхід. Це рішення повинно базуватися на ряді факторів, включаючи наступне:

- Вартість внутрішньої розробки, експлуатації та підтримання прийнятного рівня можливостей SOC порівняно з аутсорсингом. Особливо враховуючи, що можна розподілити витрати на аутсорсинг протягом певного періоду порівняно з початковими витратами на розробку власного SOC.
- Наявність надійного постачальника послуг SOC, який може відповідати або навіть виходити за рамки угоди про рівень обслуговування (SLA).
- Наявні ресурси та вартість аутсорсингу порівняно з витратами на внутрішнє обслуговування.

- Нормативи, які можуть забороняти передачу всіх або деяких задач SOC стороннім організаціям.
- Час, необхідний для створення власної документації та процесів SOC.

Традиційна внутрішня модель функціонування SOC передбачає, що всі технології, процеси та людські ресурси розробляються та надаються в рамках установи, що будує SOC для власних потреб. Організація відповідає за розробку, експлуатацію та обслуговування інструментів та процесів, а також за те, щоб ресурси SOC зберігалися вміло. Люди можуть бути співробітниками або підрядниками, а технології можуть бути локальними або хмарними, але обов'язки щодо технології налаштовуються та управляються внутрішньо.

Віртуальний SOC – це реалізація концепції “SOC як послуга”, в рамках якої організації передають свої послуги SOC на аутсорсинг. Деякими перевагами цього підходу є пришвидшення створення SOC, мінімізація зусиль із розвитку процесів і технологій та набуття необхідного досвіду в SOC. Віртуальний SOC розробляється таким чином, що дані збираються локально та управляються спеціалізованим постачальником послуг, що займається кореляцією подій, управлінням вразливостями та розслідуванням інцидентів безпеки. Цей постачальник послуг SOC, як правило, постачає інструменти управління, такі як веб-панель інструментів, щоб місцева команда могла переглядати та відстежувати інциденти безпеки, переглядати стан вразливостей та спілкуватися з аналітиками SOC, які базуються віддалено. У цій моделі замовник, як правило, керує невеликою групою, відповідальною за вживання заходів щодо загроз, які ідентифікує віртуальний SOC.

Розробка стратегії SOC повинна закінчуватися офіційним документом, в якому зазначаються послуги, які надаватиме SOC. На цьому етапі не треба вказувати технічні деталі, послуг які надаються, а навпаки, висвітлити самі послуги та цінність, яку вони приносять організації. Деякі послуги, які може запропонувати SOC, включають наступне:

- Виявлення, аналіз та управління інцидентами інформаційної безпеки. Основна мета – здатність швидко реагувати та усувати інцидент, мінімізуючи можливий вплив.
- Виконання моніторинг комплаєнсу, щоб відповідати внутрішнім і зовнішнім вимогам або стандартам. Це включає правову, регуляторну та внутрішню політику.
- Проведення процесів управління вразливістю або налагодження тісної співпраці із системними адміністраторами, які несуть відповідальність за управління вразливостями.
- Збір, аналіз та зберігання подій з відповідних джерел даних з метою покращення видимості та виявлення можливих інцидентів та проведення розслідування інцидентів.
- Проведення заходів із інформування користувачів про важливість виявлення та повідомлення про інциденти інформаційної безпеки.
- Проведення цифрових розслідувань, детальний та глибокий аналіз систем.

При розгляді питання із передачі послуг SOC на аутсорсинг важливо мати чітко визначену угоду про рівень обслуговування до прийняття угоди. Це означає наявність задокументованих процесів та періодів часу, необхідних для реагування на інцидент безпеки. SLA має вказувати кроки, які вживаються щодо виявленого інциденту безпеки, включаючи процедури захисту від тієї самої атаки, що впливатиме на мережу в майбутньому. Також має існувати певна форма страхування для відшкодування збитків, якщо постачальник не надає узгоджені послуги.

3.2 Процеси впровадження

Розробивши необхідний план та стратегію необхідно переходити до безпосереднього впровадження нових технологій та процесів, зайнятися підбором нових фахівців або зайнятися навчанням вже наявних. Будь-який центр управління кібербезпекою будується на базі якоїсь спеціальної технології, що

допомагає проводити моніторинг мережі, виявляти загрози і реагувати на них. Як вже і було визначено у розділі 1, у переважній кількості, ядром для SOC виступає SIEM-система, відповідно більшість процесів як на початкових етапах так і у подальшому вибудовуються навколо неї, включаючи і навчання фахівців, що працюватимуть із нею. Очевидно, що все це дуже трудомісткіий процеси, який вимагає великої кількості часу. Розіб'ємо ці процеси на три умовні стадії, кожна з яких передбачатиме виконання різного типу завдань: стадія SIEM, Pre-SOC і, нарешті, SOC.

3.2.1 Стадія SIEM

І так, у ході планування було визначено, які саме задачі виконуватиме майбутній SOC, визначено які технології у підприємства, яка кількість подій циркулює у мережі. В залежності від цих вхідних даних необхідно обирати систему SIEM на якій і буде базуватися робота усього центру кібербезпеки. Дуже корисним у цьому питані буде можливість проведення пілотного проекту аби зрозуміти для самих себе які функціональні можливості необхідні, які переваги та недоліки і взагалі, просто отримати розуміння про те, що саме нашому кіберцентру потрібно від SIEM, щоб як слід розробити ТЗ для постачальника. Проводити пілотні проекти варто до самого моменту придбання та інтеграції рішення, яке задовольнило потреби майбутнього SOC та було поставлено із урахуванням всіх вимог, описаних в ТЗ.

Відповідна рекомендація повністю будується на підходах із побудови і розвитку SOC на базі SIEM Arcsight ESM, тому уникнемо згадку про інші рішення, що існують та перейдемо до кроків, що мають бути виконані після придбання. До того ж усі подальші кроки розглядатимуться з точки зору побудови внутрішнього SOC, який повністю обслуговуватиметься силами власних фахівців.

Безумовно, що у ТЗ із придбання необхідно закладати навчання для фахівців, які не мають досвіду роботи із SIEM взагалі, або мають досвід роботи із іншим рішенням цього класу. Окрім того, необхідно правильно визначати якого

типу навчання має бути, адже якщо перед фахівцями стоїть задача не тільки проводити моніторинг та аналітику подій, а ще й буде необхідність підключення нових джерел даних та розробка правил, тоді варто це враховувати і закладати у вартість послуги із придбання рішення.

Процеси навчання та здобуття нових навичок з цього моменту мають стати постійним для всіх фахівців і бути невід'ємною частиною всього життєвого циклу SOC. Доволі значна частина навичок здобувається дослідним шляхом та шляхом постійних спроб та помилок. Необхідно максимально глибоко вивчати функціонал системи. Це доволі довгий процес, він займатиме значну частину часу на початкових етапах, але саме це дозволить якнайшвидше отримувати користь від системи. Розібравшись як працюють правила із стандартного набору та визначивши, чого саме не вистачає, щоб отримати більше видимості можна поступово розробляти власні правила, дешборди та фільтри для відслідковування тих категорій подій, що цікавлять команду зараз.

На перших етапах, зазвичай, інсталяція та початкова інтеграція SIEM проводиться постачальником послуг, тому дуже важливо знати які саме кроки та яким чином виконувались інженерами постачальника, переймати досвід та знання від них. Задля зручності налагодити особисті формальні або неформальні зв'язки із ними для можливості подальшого звернення по незначних питаннях, що стосуються експлуатації системи, це дещо пришвидшить та полегшить виконання деяких завдань[13].

Не варто забувати про існування документації до усіх компонентів системи. Можна уникнути дуже велику кількість помилок, якщо просто декілька разів вдумливо ознайомлюватись із інструкціями та рекомендаціями, що описані в них. До того ж, у будь-якого постачальника рішень SIEM є власних електронний ресурс для користувачів, де можна знайти готове рішення для деяких проблем, що з якоїсь причини не визначені у документації, або ж безпосередньо звернутись по допомогу або за порадою до інших, більш досвідчених користувачів. Однак, якщо проблема потребує особливих знань, тоді рекомендовано звернутись по допомогу до фахівців компанії-інтегратора або компанії-постачальника SIEM, для цього у

організації, що будує SOC має бути відповідна активна ліцензія на отримання технічної підтримки та для отримання оновлень до наявних систем.

З точки зору людського фактору, у SOC має бути досягнуто певний рівень взаємодії із іншими підрозділами Департаменту IT. Зазвичай, сам центр кібербезпеки будується на базі тих можливостей і потужностей, якими володіє підрозділ ІБ, у свою чергу адміністратори IT забезпечують роботу технічних рішень, якими користуються спеціалісти ІБ. Фахівці SOC та інші фахівці IT мають розуміти завдання один одного, бачення один одного там максимально близько взаємодіяти у питаннях налаштування системних та мережевих ресурсів та покращення їх безпеки. У всіх процесах взаємодії мають приймати участь керівництво IT і керівники структурних підрозділів та сприяти налагодженню зв'язків і підвищенню ефективності. Відповідних речей варто досягати ще на етапі планування та постійно їх розвивати, що було описано у попередніх підрозділах.

SIEM не має бути єдиним інструментом із яким працює SOC, адже є необхідність у наявності інших спеціальних можливостей, якими не володіє SIEM, як-от, наприклад, системи управління вразливостями. Вони дуже важливі для проведення сканувань внутрішніх та зовнішніх ресурсів аби розуміти яка ситуація є наразі у мережі, які є вразливі сторони та розробляти процедури із усунення вразливостей. Доволі значна частина робіт буде неможлива без допомоги підрозділів IT, що повинні будуть постійно оновлювати ОС та програми на робочих станціях і сервера та проводити інші налагоджувальні роботи для усунення вразливих сторін.

Однак система SIEM може стати в нагоді в цих процесах, якщо налагодити відправлення даних про проведені сканування у консоль системи. У консолі ArcSight можна відслідковувати дані про пристрої у мережі та їх атрибути, зокрема їх домені ім'я, IP-адреса, авторизований користувач, а також і увесь перелік виявлених вразливостей. Маючи на руках дані про наявні критичні для організації пристрої та маючи результати проведених сканувань, можна виконати задання із пріоритизації IT-активів та налаштувати правила або інструментальні

панелі із від слідкування атак на найбільш вразливі із критичних пристроїв. Це дасть можливість розподілити проведення заходів із реагування на інциденти в залежності від пріоритету системи, спочатку усунувши проблему на більш критичному активі та перейшовши до іншого.

В свою чергу налагодження відправки стосується не тільки для сканерів, а взагалі для всіх систем у мережі, які дійсно необхідно моніторити. Процеси із підключення джерел подій є постійними протягом усього життєвого циклу SOC, однак початкові етапи вирізняються необхідністю підключення систем у великій кількості за порівняно невеликий термін. Відповідні процеси потребуватимуть певних додаткових знань із принципів роботи для ведення лог-журналів тієї системи, яку підключатимуть. Це пов’язано із необхідністю пошуку та вивчення великої кількості документації із налаштування ArcSight SmartConnector та документації до цільової системи. Розпочинати підключення варто із систем, які або є найбільш критичними або ті, які найлегше інтегрувати. Серед найбільш легких є мережеві пристрої, на них достатньо налаштувати відправку подій категорії Syslog та Netflow на конектор, що збиратиме ці дані пасивно, варто лише налаштувати прийом на заздалегідь відкритий порт. А окремо, серед цих систем, найбільш корисними на перших етапах будуть події з між мережевих екранів як у внутрішній мережі, так і мережевих екранів і маршрутизаторів, що налаштовані на роботу у просторі між внутрішньою та зовнішньою мережею.

Рекомендовано, щоб задачами із встановлення, налаштування та обслуговування компонентів SIEM-системи займалися якнайменш двоє осіб, або більше, в залежності від розміру штату SOC, а також варто досягти того, щоб кожен з них одночасно робив різні завдання, що прискорить виконання робіт із налаштування компонентів системи. Відповідними обов’язками займаються адміністратори SOC, вони здебільшого працюють над підключенням нових джерел подій, працюють над усуненням несправностей систем та програм, якими користується SOC, проводять оновлення систем, лише за умови гострої необхідності приймають участь у аналізі та усуненні інцидентів, однак і це можливо здебільшого у малих та середніх SOC. Критично важливим завданням

для будь-якого адміністратора полягає у проведенні резервного копіювання усіх компонентів системи, а також наявність знань про те, як встановити та налаштувати усі компоненти із самого початку. Відповідні навички мою відточувати на тестовому середовищі, наявність якого дуже важливе для будь-якого SOC. Тестування нових конекторів, оновлень до всіх компонентів, а також додавання нового функціоналу на тестовому середовищі дозволить уникнути наслідків у разі допущення помилок. Крім того, це додаткова платформа для нових співробітників для навчання функціоналу SIEM та для відточення наявних і вивчення нових навичок для всіх фахівців.

3.2.2 Pre-SOC

Після того, як буде досягнуто успіхів у попередній стадії, здобуто нові знання та закріплено їх, з’явиться можливість рухатись далі виконувати більш складні завдання. Без сумніву, що фахівці потребуватимуть більше видимості та більше функціоналу для виконання задач, адже за цей час усі зрозуміли те, як працює система, визначено проблеми та недоліки і кожен розуміє чого не вистачає.

Забезпечивши себе базовим рівнем безпеки та моніторингу SOC потребуватиме перевірки своїх навичок та знань, перевірити рівень захищеності інформаційної системи та уважність кінцевих працівників організації. Задля цього необхідно проводити внутрішній аудит та тести на проникнення.

Під час аудиту необхідно перевірити обізнаність кінцевих користувачів та пояснювати, кому вони повинні повідомити у випадку, якщо з ними або їх колегами трапився інцидент інформаційної безпеки, було виявлено підозрілу поведінку пристроїв або отримано підозрілого листа на електронну пошту.

Також потрібно звертати увагу на права та привілеї, які користувачі мають на своїх робочих станціях. Кінцеві користувачі не повинні мати локальний доступ рівня адміністратора. Якщо вони насправді потребують і будуть використовувати його дуже часто, тоді вони повинні мати додатковий обліковий запис для використання програм “від імені адміністратора”. Але для “одноразових”

операцій вони можуть звернутися за допомогою до служби підтримки. Наприклад, для встановлення чогось. Але в той же час, підрозділ ІБ або SOC повинен перевірити, що саме вони збираються встановити, навіщо їм потрібен такий інструмент, перевірити інформацію про ліцензію та переконатися, що він не є шкідливим. Йдеться також про спілкування з людьми, адміністратори IT та технічна підтримка повинні інформувати про встановлене нове програмне забезпечення або про їх заявки на встановлення чого-небудь на конкретний комп'ютер.

Корисним є перевірка операційних системи за допомогою шаблонів STIG або за критеріями CIS Benchmark, що дозволяють автоматично перевіряти точність налаштувань системи та отримувати повний звіт про конфігурацію та політику безпеки.

Варто перевіряти як налаштовані системи моніторингу та захисту, що працюють на кінцевих точках (антивіруси, хостові IDS тощо).

Перевірка того, як налаштовані ваші між мережеві екрани, які політики застосовуються та чи є в ньому вразливі місця, які можуть скомпрометувати мережу. Вартий уваги підхід, що передбачає постійну перевірку периметру, щоб зрозуміти, що, наприклад, експлойт, який знаходиться у вільному доступі, не спричинить жодних проблем, це одна з ключових речей, яку потрібно перевіряти на постійній основі. Важливо розуміти, що факт наявності між мережевого екрану не врятує від усього; правильні налаштування політики та виправлення пристроїв відіграють важливу роль.

Тестування користувачів на фішинг – це також одне з головних речей, яке слід проводити на постійній основі з подальшим вивченням уроків з цього та коригуванням політики.

Протягом усього аудиту кожен із операторів і аналітиків має брати участь як той, хто відловлюватиме спроби зламу від інших фахівців, що проводять тести на проникнення. Такі речі також входять в програму підготовки фахівців. Керівництво IT має бути інформованим про ці процедури і, за можливості, заохочувати їх проведення. Корисним також може бути можливість залучати для

проведення тестів на проникнення і сторонні організації, про дії яких, SOC не має знати нічого і має виявляти активні спроби сканування і зламу.

Завжди необхідно враховувати той факт, що інформаційна безпека не є основною справою організації, тому керівництво не захоче витрачати багато коштів на інформаційну безпеку. Але робота SOC досі полягає в тому, щоб захистити мережу і програмні та апаратні засоби корпоративної інформаційної системи, особливо якщо це якийсь конкретний інструмент для промислових систем управління, для банківської справи тощо. Необхідно розуміти, які системи та засоби у вас є у внутрішньому інформаційному середовищі. Сидіти і чекати, поки компанія не придбає якийсь конкретний інструмент, не можна. Необхідно знайти якесь альтернативне тимчасове рішення.

Тут OpenSource рішення можуть допомогти забезпечити захист на хорошому рівні, але очевидно, лише якщо правильно їх налаштували і витратити на це суттєву кількість часу.

Для сбору індикаторів компрометацій (англ. IoC) використовують платформу розвідки загроз MISP[misp] та різноманітні безкоштовні канали (англ. feed), щоб отримувати актуальну інформацію про нові виявлені хеш-суми шкідливого програмного забезпечення, зловмисників, що розсилають фішинг, адреси центрів управління ботнетами (C&C) тощо.

Для проведення пентесту необов’язково купувати метасплойт і дорогі сканери, можна використовувати просто стандартний набір засобів Kali Linux від Offensive Security[kali]. Але для вивчення всіх функцій потрібен певний час.

Sysmon[sysmon] – при правильній конфігурації цей інструмент дуже корисний для виявлення загроз на кінцевих пристроях на базі Windows. Він має досить хороші конфігурації, засновані на техніці MITRE Attack[Mitre]. Він легко встановлюється на будь-яких серверах та робочих станціях. У поєднанні з відправкою подій Windows (Windows Event Forwarding)[WEF] забезпечує більшу видимість процесів, що відбуваються локально на кожному с пристроїв.

3.2.3 Стадія SOC

В решті решт, після виконаних задач на двох попередніх стадіях, а також відточення здобутих навичок і їх неодноразове повторення, можна свідчити про здобуття певних необхідних навичок та знань. Однак, аби вважатись повноцінним SOC необхідно виконати ще низку умов.

Однією з таких є розмежування обов'язків. Якщо, з будь-якої причини на попередніх етапах усі фахівці виконували різний набір завдань із моніторингу, аналітики, реагування, адміністрування та тестування на проникнення разом, не доручаючи обов'язки чітко за конкретні задачі конкретному фахівцеві, тоді саме час про це потурбуватись. До цього часу кожен з фахівців має відчути який з аспектів роботи SOC йому вдається найбільше, відповідно керівник має розуміти слабкі і сильні сторони своїх підлеглих і чітко визначити якою саме роботою у подальшому, кожен з фахівців займається.

В залежності від специфіки SOC, наявних інструментів, розміру команди та розміру організації можуть існувати різноманітні схеми розподілу обов'язків між членами команди. Їх можна розробляти самостійно під себе і розмежовувати обов'язки як зручно, так і вдаватись до рекомендованих найкращими практиками схем. Прикладами таких схем є, описані у посібнику і від центру MITRE[2]. На рисунку 3.3 зображена еталона модель архітектури SOC, що включає в себе усі необхідні функції. Тут чітко розмежовані задачі між командами у середині SOC на 5 умовних «ліній».

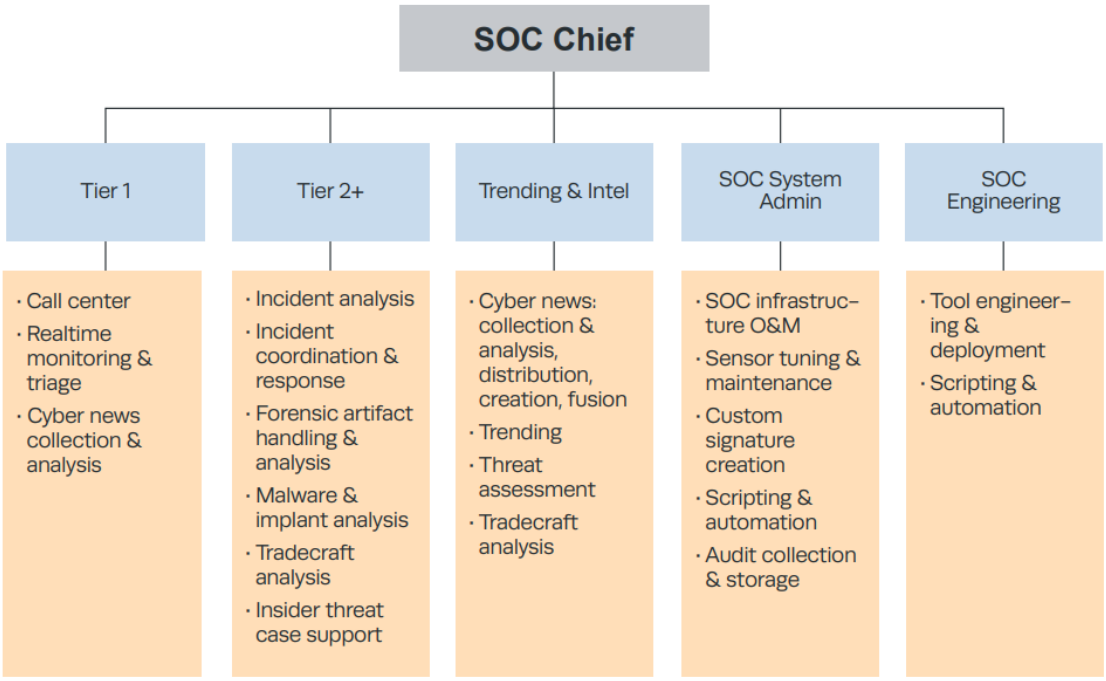


Рис. 3.3 Усі функції SOC, еталонна модель

Відповідно перша лінія складається із операторів, що займаються постійним моніторингу та сортуванням подій, реагують для сповіщення про інциденти від користувачів та працівників IT, що надходять поштою, телефоном, системою заявок тощо, вивчають та аналізують новини у сфер кібербезпеки та кіберзагроз.

На другу лінію приходяться більш специфічні задачі із реагування на інциденти та їх аналіз; проведення цифрового розслідування; аналіз шкідливого ПЗ; реагування на загрози інсайдерів; проведення аудиту[14].

Важливою частиною SOC є наявність у ньому функцій із збору та аналізу новин, трендів у сфері кіберзагроз, оцінка загроз, збір розвідувальних даних у сфері кібербезпеки, в тому числі на спеціалізованих ресурсах, якими користуються хакери.

Адміністратори проводять заходи із: обслуговування засобів SOC; встановлення та налаштування конекторів; розробка скриптів і автоматизація процесів; збір та зберігання логів. Деякі з цих функцій виділяють в окрему категорію розробки, до якої можна додати процеси із розробки та впровадження власних програм.

У рамках одного підприємства можна побудувати SOC різного розміру та рівня розгалуженості. Найбільш розповсюдженим типом внутрішнього SOC є малий внутрішній централізований тип, розглядатимемо саме його. Рисунок 3.4 демонструє його вигляд за версією MITRE[2].

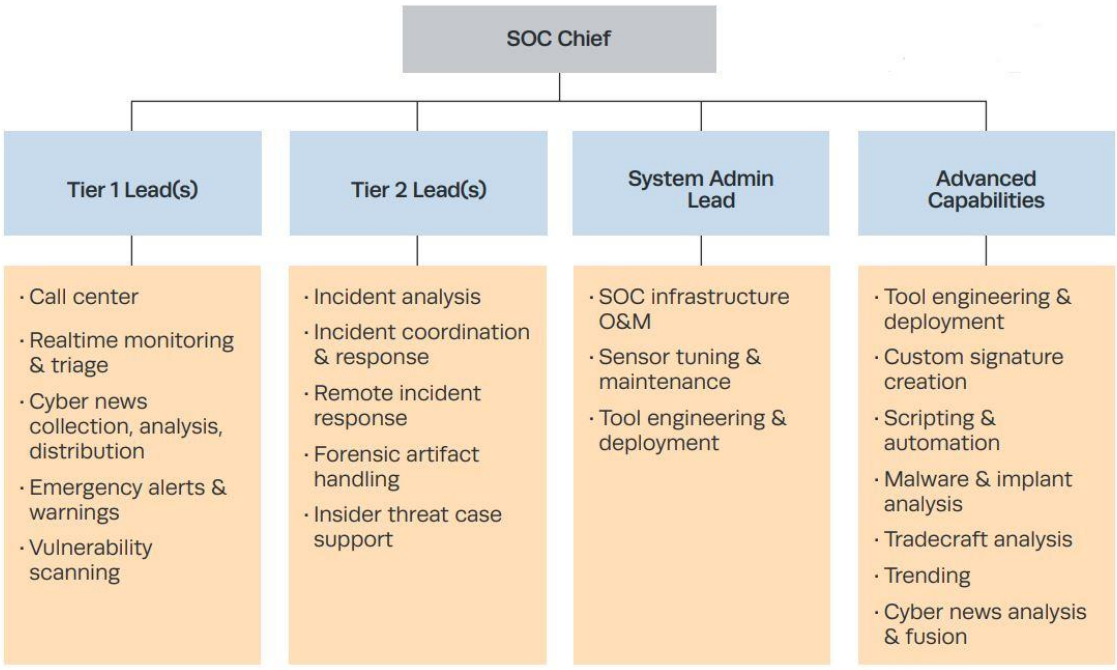


Рис. 3.4 Малий внутрішній централізований SOC

Є чітко визначені 2 лінії аналітики, група системних адміністраторів та перелік додаткових функцій, які в свою чергу можуть бути розподіленими між цими лініями, або висунуті для виконання окремою групою фахівців. Як видно на цьому рисунку, усі функції описані в еталонній моделі функцій чітко розподілені у межах цієї архітектури.

Як було зазначено у попередньому підрозділі, одного лише SIEM не достатньо аби бути повноцінним SOC. Вже визначено яке високе значення має наявність процесів управління вразливостями та OpenSource рішення, але і інші інструменти, що необхідні сучасним центрам управління кібербезпекою для покращення своєї видимості та можливості автоматизації своєї роботи.

Зокрема, з точки зору аналітики та виявлення загроз індустрія рухається до того аби впроваджувати рішення класу UEBA (User and entity behavior analytics). Рішення цього класу здатні проводити аналітику дій користувачів та пристроїв у системі, виявляючи аномальну поведінку. Переважна кількість сучасних систем

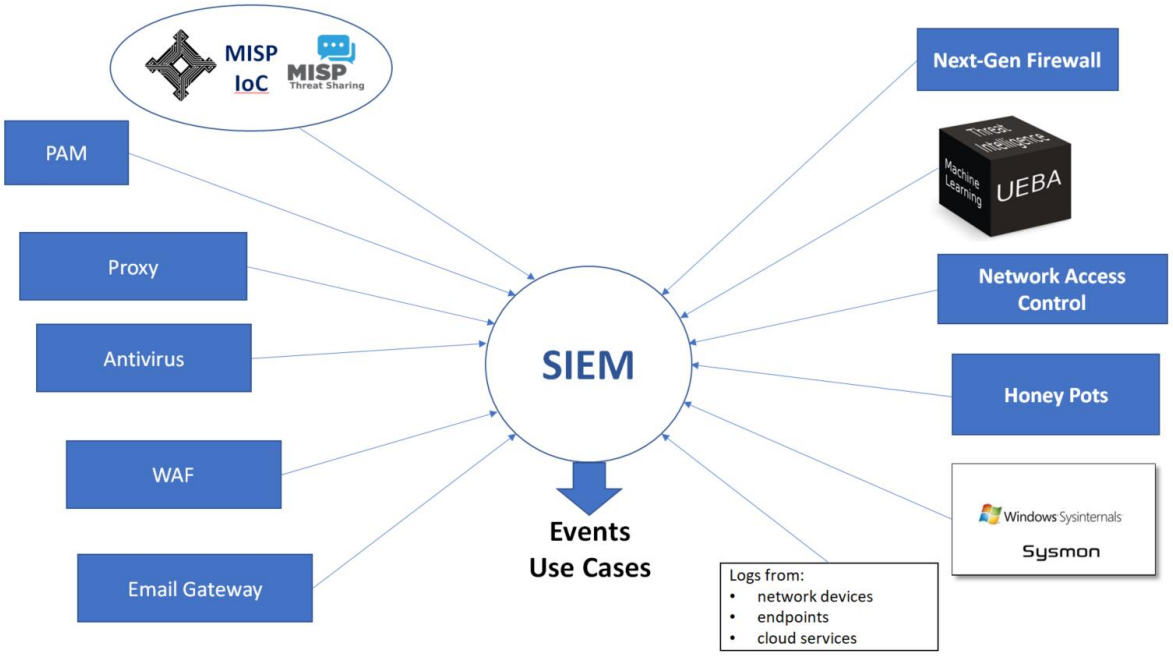
цього класу оснащена модулем машинного навчання або, навіть, штучним інтелектом, в той час, як системи SIEM побудовані на кореляційних правилах, що мають бути визначені вручну. Зрозуміло, що за допомогою SIEM досить важко досягти 100 відсоткової аналітики та доволі складно виявляти, наприклад, Zero-day (англ. нульового дня) загрози, завдяки здатності проведення поведінкового аналізу, системи UEBA здатні виявляти аномальні активності, як-от вивантаження даних користувачем на сторонній ресурс у неробочий час, фіксуючи високу активність його комп'ютера у мережі, та облікового запису, що взаємодіє із проксі-сервером організації.

З точки зору мережі доволі широкого розповсюдження досягли рішення класу Next-Generation Firewall (Міжмережеві екрани наступного покоління). Повністю керовані пристрої, що мають власні інструментальні панелі, що мають більш просунуті, в порівнянні із звичайними фаерволлами функції. Маючі правильно налаштовані політики та правила, виконують функції фаерволла, системи виявлення та запобігання вторгнень, системи DLP, можуть комплектуватися модулями машинного навчання для проведення поведінкового аналізу подій у мережі внутрішній та зовнішній.

З точки зору автоматизації рекомендовано забезпечитись засобами класу SOAR (Security Orchestration, Automation and Response). Це порівняно новий клас рішень, задача якого забезпечувати SOC можливістю автоматизації низки рутинних завдань, пов'язаних із обслуговуванням компонентів SIEM та інших інструментів[15]. Надає можливість блокування скомпрометованих користувачів або пристроїв без необхідності звертатись до інших інструментів. Виступає системою реєстрації інцидентів, формує звіти та здійснює моніторинг активності працівників усього SOC, реєструючи їх дії, затрачений час та зусилля.

Звичайно, що усі відповідні засоби можна інтегрувати із системою SIEM для розробки додаткових правил реагування або ж для відправки сповіщень про виявлені загрози для подальшого реагування аналітиками. Окрім вище згаданих, у сучасному ринку засобів кібербезпеки існує низка інших специфічних рішень, які підвищують видимість та захищеність у мережі. Пошук нових засобів безпеки,

проведення пілотних проектів, їх придбання та інтеграція у існуючу інфраструктуру SOC є частиною його життєвого циклу і відбувається постійно, адже середовище кіберзагроз постійно поповнюється новими різновидам загроз і викликають необхідність впровадження нових контрзаходів. Рисунок 3.5 демонструє тип схеми інтегрованих джерел у типовому сучасному повноцінному SOC.



3.5 Схема підключених джерел подій до SIEM

3.3 Розробка рекомендацій щодо побудови та функціонування SOC

Будь-які процеси із побудови необхідно розпочинати із проведення стратегічного планування із урахуванням усіх аспектів бізнес-процесів організації, на базі якої будується SOC. Оцінка можливостей організації та самого центру управління кібербезпекою є ключовою, як на етапі планування і початковому етапі впровадження так і протягом усього життєвого циклу SOC. Стратегія, що закладена на початкових етапах впливатиме у подальших процесах планування і всі перебудови відбуватимуться із урахуванням усіх попередніх здобутків. Тому очевидно, що найбільшої уваги варто приділити саме процесам планування та оцінки можливостей і зрілості на самому початку.

Враховуючи дані, здобуті при проведених оцінюваннях та виходячи з потреб і можливостей організації необхідно ретельно обирати технології, на

основі яких будуватиметься робота усього SOC. Так як функціонально процеси із забезпечення реактивних та проактивних заходів найкраще реалізовані в системах класу SIEM, варто будувати технологічні процеси на основі цих рішень.

Процеси із впровадження мають формуватись із урахуванням знань до досвіду фахівців та можливостей технологічних засобів, які також впливають один на одного. Важливо приділяти увагу постійному розвитку та навчанню фахівців задля отримання ефективного розвитку технологічних процесів, якості та швидкості реагування на інциденти та їх вирішення.

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 до розділу 3

Було надано рекомендацій із планування процесів побудови та розвитку центру управління кібербезпекою. Зокрема визначено критерії та аспекти за якими необхідно оцінювати можливості та зрілість SOC. Дуже важливо розуміти цілі та цінності організації, в якій функціонуватиме SOC, на основі яких має бути вибудовано його цілі та процеси. Фахівці майбутнього SOC мають розуміти яке місце вони займають у діяльності організації та вибудовувати свої функції, які сприятимуть роботі підприємства.

Має бути чітко вибудована стратегія розвитку, що враховує аспекти досвіду, технологій, параметри часу та місця, ресурси, область застосування тощо.

Безпосереднє впровадження процесів побудови і подальшого розвитку SOC умовно поділені на стадії, кожна з яких передбачає досягнення мети із інтеграції інструментів у мережу, вивчення функціоналу, постійне забезпечення самих себе вищим рівнем видимості та аналітики, впровадження нових функцій та засобів та орієнтація на постійний, безперервний розвиток усього SOC як структурної одинці так і кожного фахівця окремо.

ВИСНОВКИ

Проведено аналіз центрів управління кібербезпекою як явища, визначено їх задачі та цілі, визначено їх характеристики з різних точок зору та їх значення у протидії сучасним кіберзагрозам.

Досліджено, що наявність власного SOC здатна забезпечити організацію необхідним рівнем реактивного та проактивного захисту інформаційної інфраструктури. Це можливо завдяки правильно побудованим процесам, вдало підібраним фахівцям та технологіям, які разом є основою будь-якого SOC.

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. Важливо опрацьовувати ретельну стратегію перш, ніж переходити до безпосереднього впровадження. Розроблено чіткі практичні рекомендації із впровадження процесів SOC від моменту початкової інтеграції технології та їх опанування і до самого становлення повноцінного центру управління кібербезпекою, який постійно розвивається.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

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

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)

Державний університет телекомунікацій
Навчально-науковий інститут Захисту інформації
Кафедра інформаційної та кібернетичної безпеки

Магістерська робота

на тему:

ТЕХНОЛОГІЯ ПОБУДОВИ ЦЕНТРУ УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ НА БАЗІ РІШЕННЯ MICROFOCUS ARCSIGHT

Виконав: Рижков Д.О.

Науковий керівник: Гахов С.О.

Київ 2020

Об’єкт дослідження: Процеси побудови та розвитку центрів управління кібербезпекою

Предмет дослідження: Технології планування та впровадження процесів на базі рішень ArcSight

Мета роботи: Розробка ефективних рекомендацій із побудови повноцінного центру управління кібербезпекою із перспективою розвитку.

Основні завдання:

- Проаналізувати призначення та користь володіння SOC.
- Дослідити методи збору та аналізу подій у мережі, визначити практичні методи управління подіями та інцидентами.
- Дослідити можливості забезпечення повноцінної видимості та інформованості про події в мережі.
- Розробити рекомендації із планування, впровадження та розвитку процесів SOC.

Актуальність центрів управління кібербезпекою

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. Відсутність проактивних засобів не дає змогу забезпечити належний рівень безпеки, а у більшості IT підрозділів недостатня видимість того, як себе поводить внутрішня мережа та пристрої у ній.

Організації приходять до розуміння необхідності появи власних центрів управління кібербезпекою, або ж звертаються до MSSP, які надають відповідні послуги. 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.

Концепція SOC

SOC – централізований підрозділ установи, який вирішує питання з інформаційної та кібербезпеки на організаційному та технічному рівні; Об'єкт, де корпоративні інформаційні системи контролюються, оцінюються та захищаються, а спеціалісти виконують відповідні задачі із захисту від несанкціонованої діяльності в комп'ютерних мережах, включаючи моніторинг, виявлення, аналіз реагування та відновлення.

Основні завдання SOC:

- проактивний нагляд за IT-системами та постійний аналіз поточного стану загроз;
- розпізнання слабких місць у IT-безпеці та їхнє усунення;
- централізоване управління безпеки різноманітними пристоями у системі;
- інформування про випадки розпізнання нападів та загроз;
- безпосередні заходи щодо захисту та/або мінізації шкоди під час кібератак;
- проведення оцінки стану систем IT-безпеки;
- технічна підтримка в усіх пов'язаних з IT-безпекою питаннях;
- звітування щодо роботи SOC та усіх пов'язаних з IT-безпекою систем.

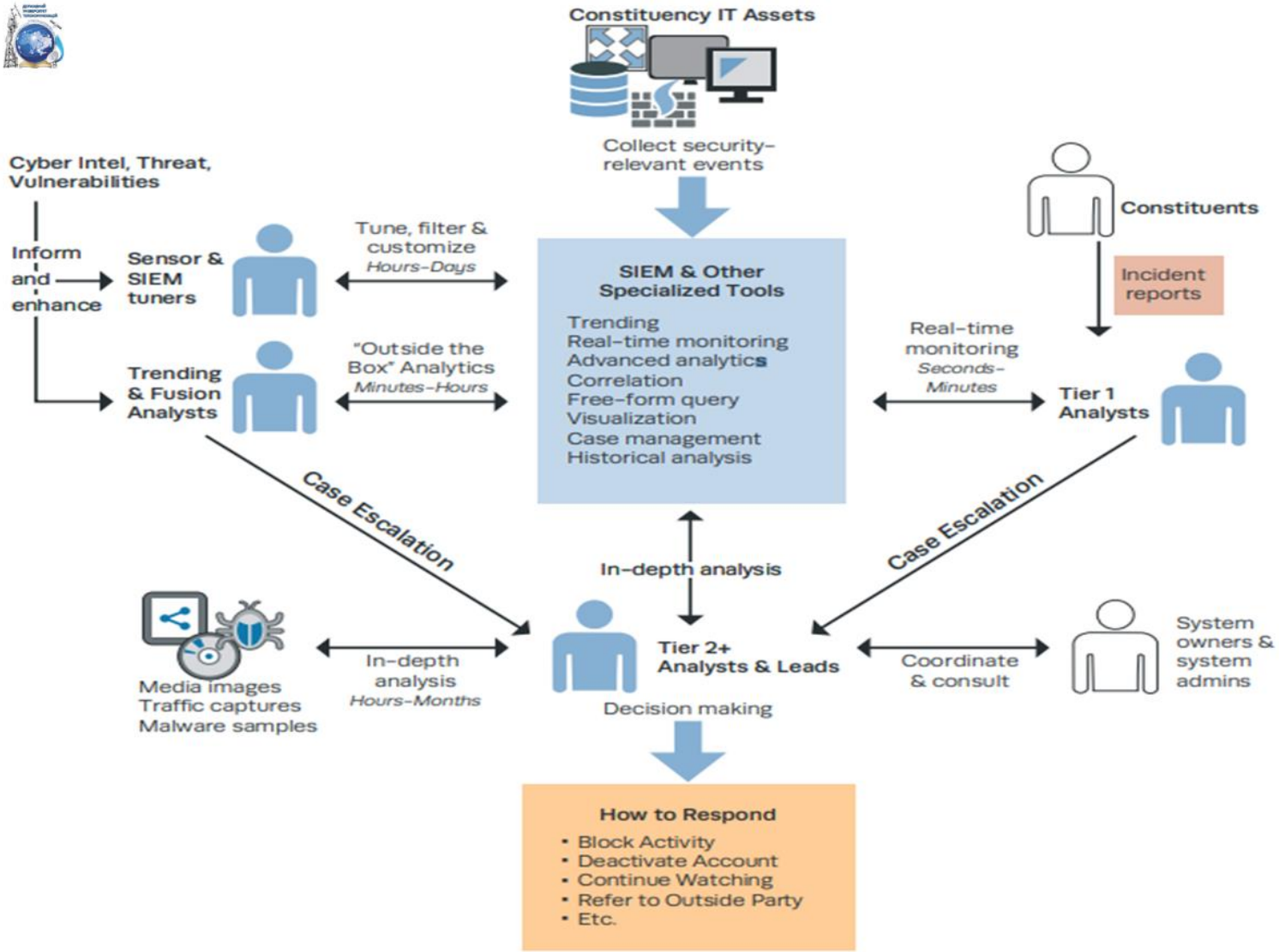


Figure 1. SOC Roles and Incident Escalation. Carson Zimmerman. MITRE. "Ten Strategies of a World-Class Cybersecurity Operations Center". The MITRE Corporation.

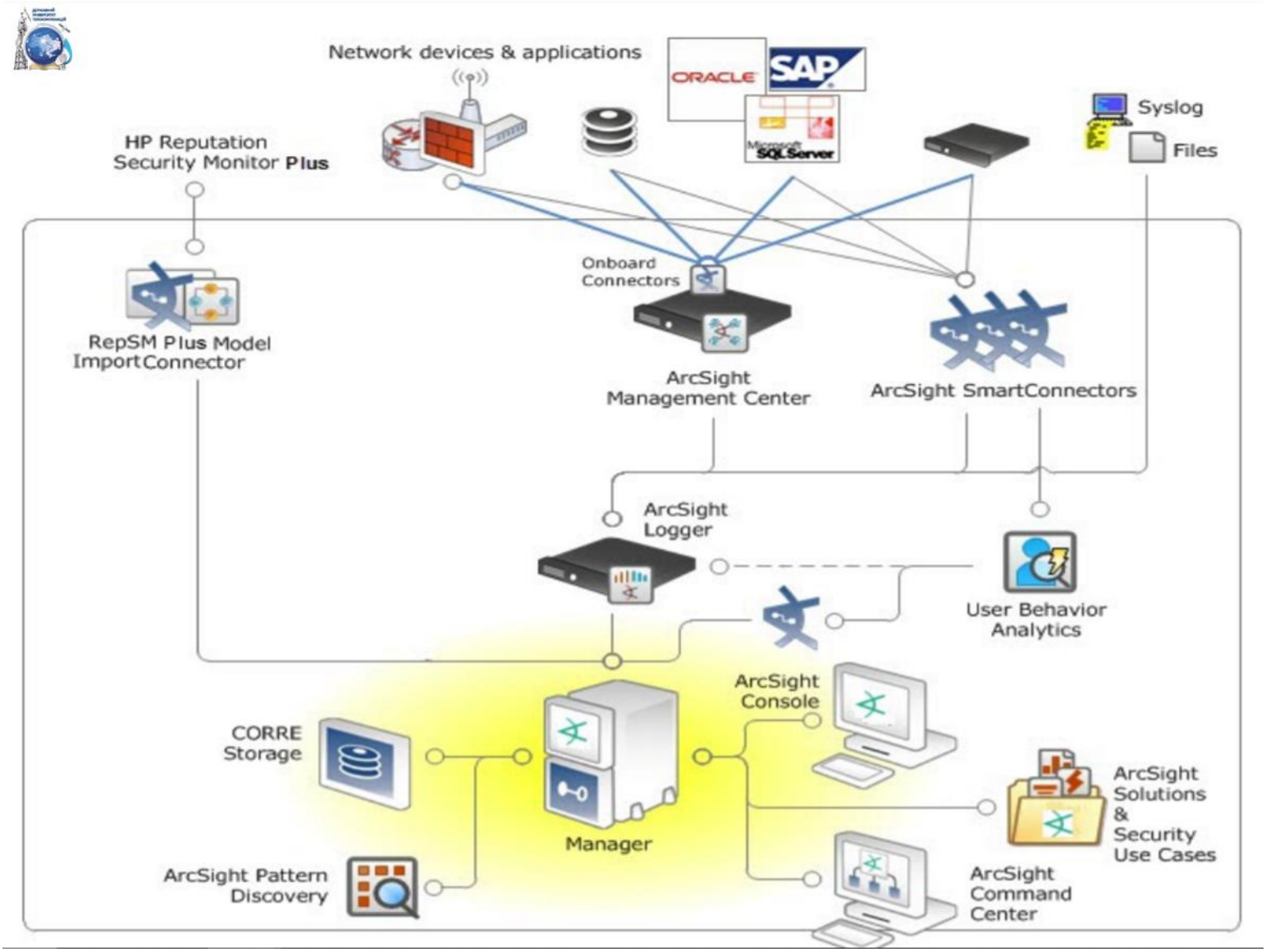
Платформа Microfocus ArcSight

Єдина платформа технічних засобів для налагодження процесів SOC. Має наявний набір компонентів для збору, нормалізації, аналізу та кореляції подій інформаційної безпеки.

Складається з програмних комплексів ArcSight ESM, Logger, Management Center та SmartConnector.

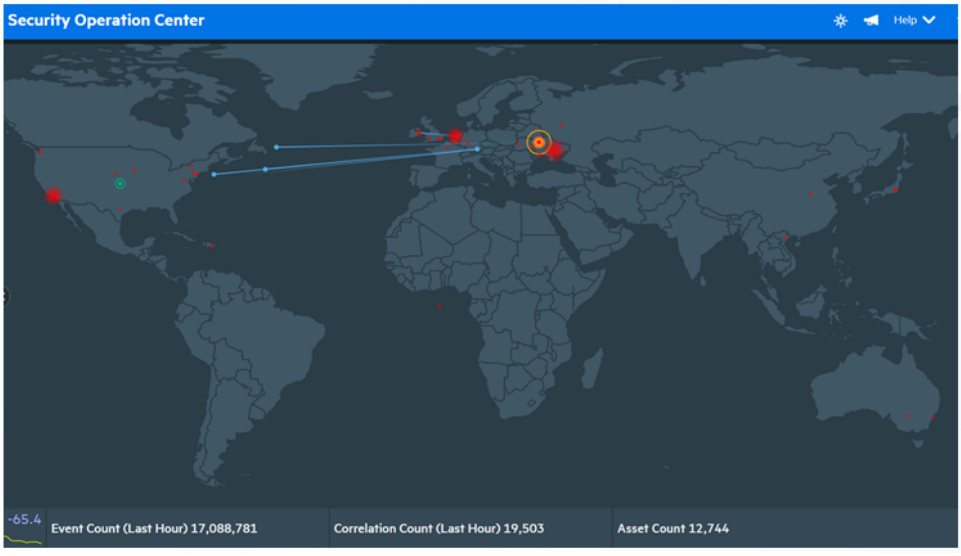
ArcSight™

MICRO FOCUS®


Network devices & applications
ORACLE
SAP
Microsoft SQL Server
Syslog
Files
HP Reputation Security Monitor Plus
RepSM Plus Model Import Connector
Onboard Connectors
ArcSight Management Center
ArcSight SmartConnectors
ArcSight Logger
User Behavior Analytics
ArcSight Console
CORRE Storage
Manager
ArcSight Solutions & Security Use Cases
ArcSight Pattern Discovery
ArcSight Command Center

ArcSight ESM

Комплексне програмне рішення моніторингу подій безпеки, мережевої розвідки, кореляції подій, виявлення аномалій з наявними інструментами аналізу. Багаторівневе рішення, яке забезпечує інструментами аналітиків мережевої безпеки, системних адміністраторів та бізнес-користувачів. ESM включає в себе Корреляційний механізм оптимізованого зберігання та обробки даних CORR-Engine – засіб зберігання та пошуку даних, який отримує та обробляє події з високою швидкістю та виконує високошвидкісний пошук.

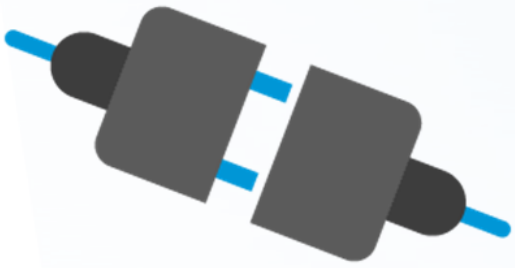


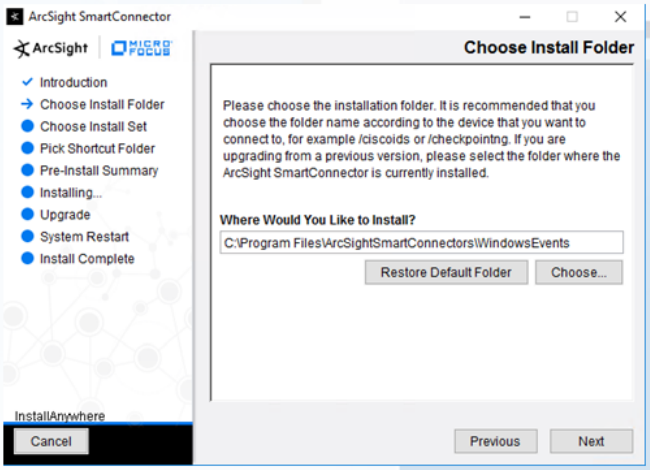
ArcSight SmartConnector

Зв’язуюча ланка між пристроями-джерелами подій та між іншими компонентами платформи ArcSight.

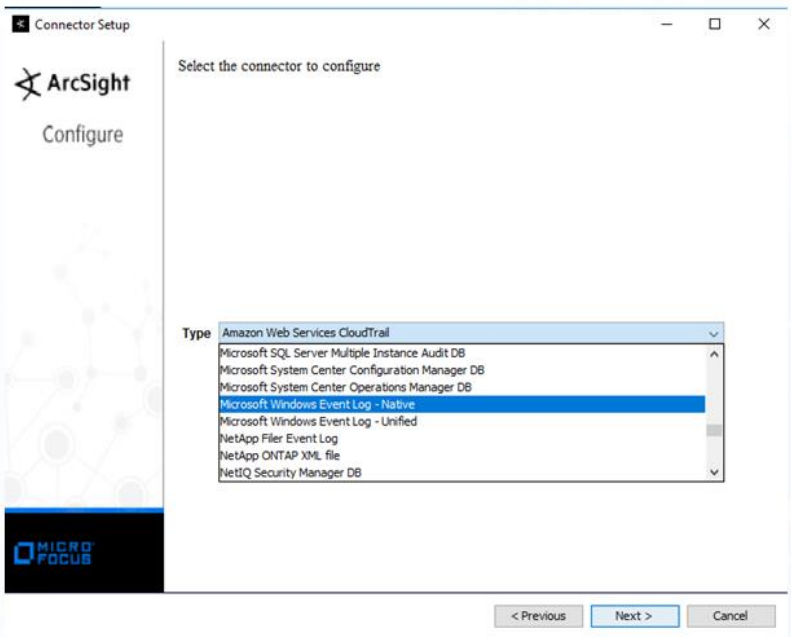
SmartConnectors виконують такі функції:

- Збирають усі необхідні дані, з пристрою-джерела.
- Зберігають пропускну здатність мережі та простір для зберігання.
- Проводить парсинг подій та впорядковує їх у загальну схему (формат) для використання в ESM.
- Агрегує події, щоб зменшити кількість подій, що надсилаються Менеджеру.
- Категоризує події, використовуючи загальноприйнятий для читання формат.
- Передає події ESM після їх обробки.





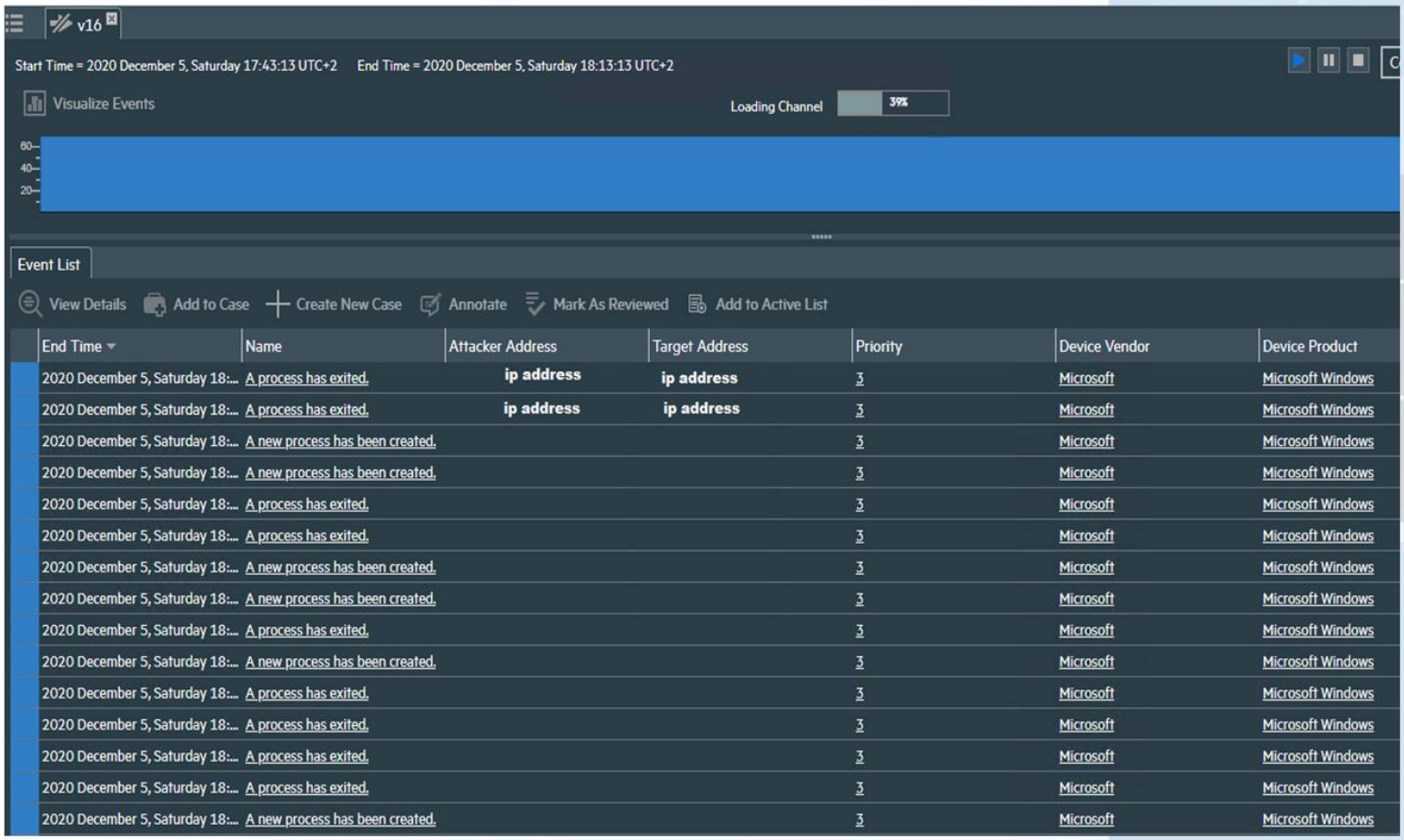
Процедура збору та аналізу подій



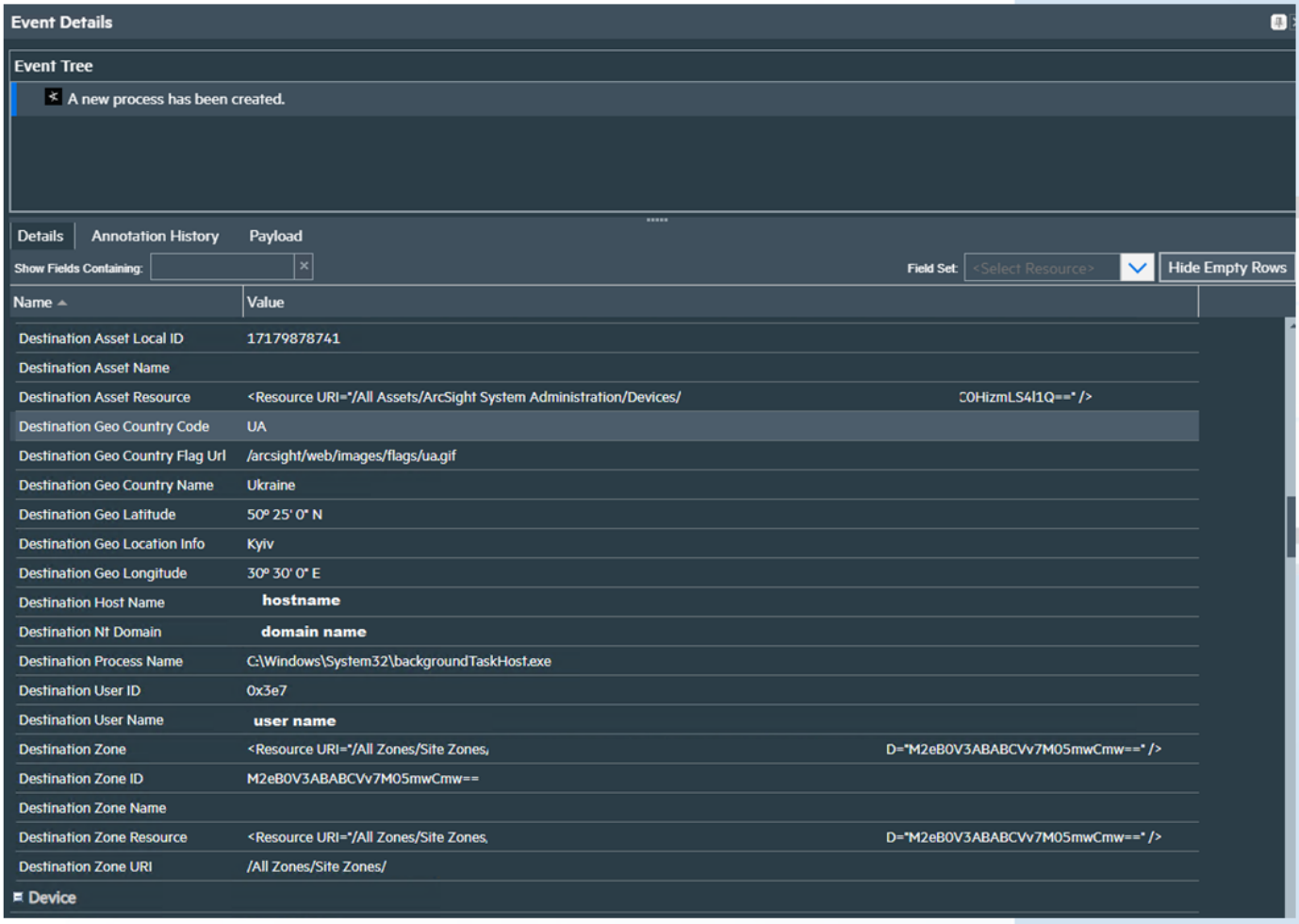
Enter the device details

	Host Name	Domain Name	User Name	Password	Windows Version	Is WEC	Security	System	Applica...	Forwar...	Custo...	Filter	Locale	Encoding
☑				******** ...	Windows Server 2016 ...	☐	☐	☐	☐	☐		*	en_US	

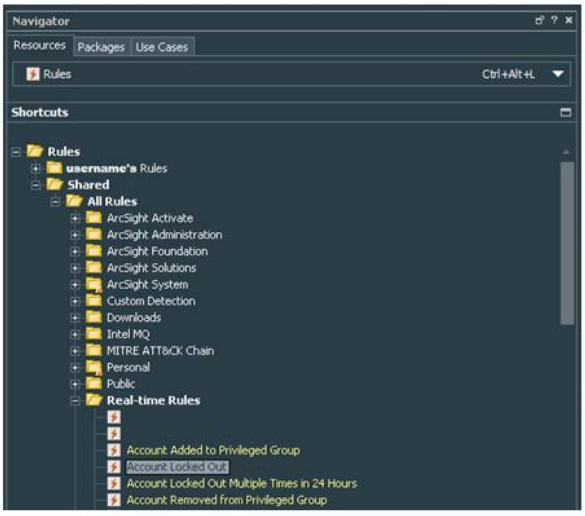
Процедура збору та аналізу подій

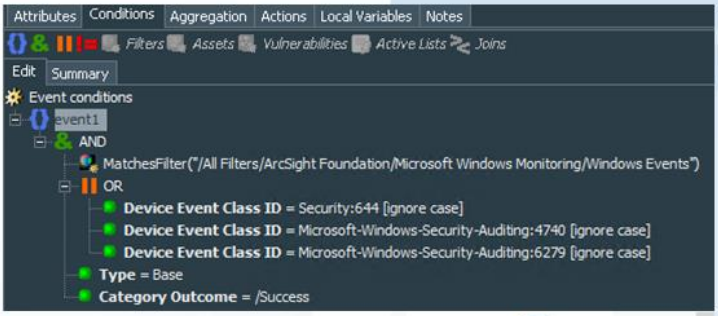


Процедура збору та аналізу подій

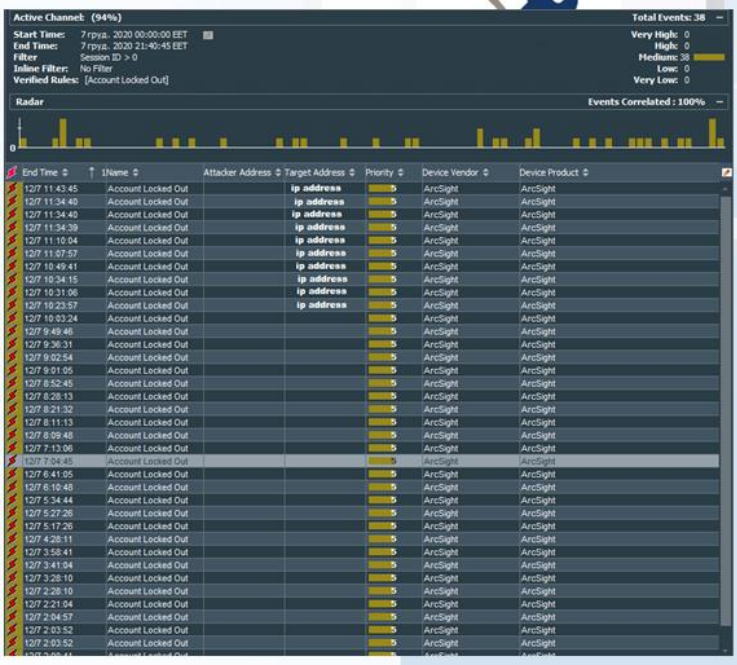


Кореляція

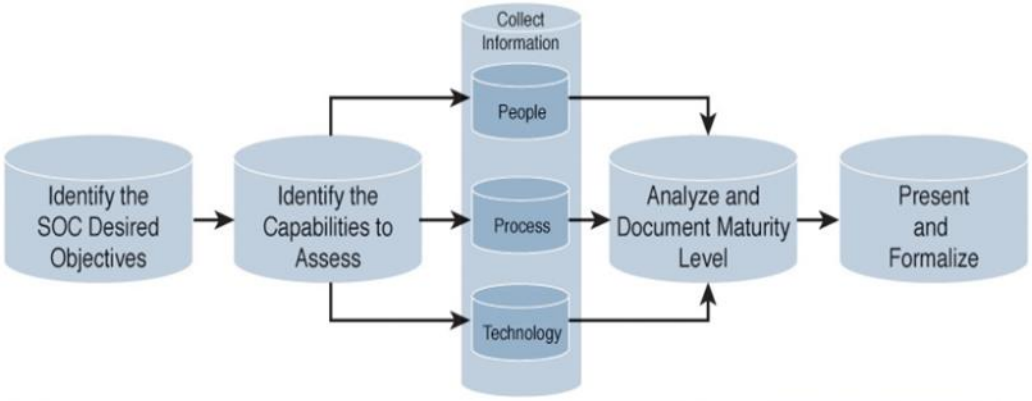




MITRE ATT&CK™



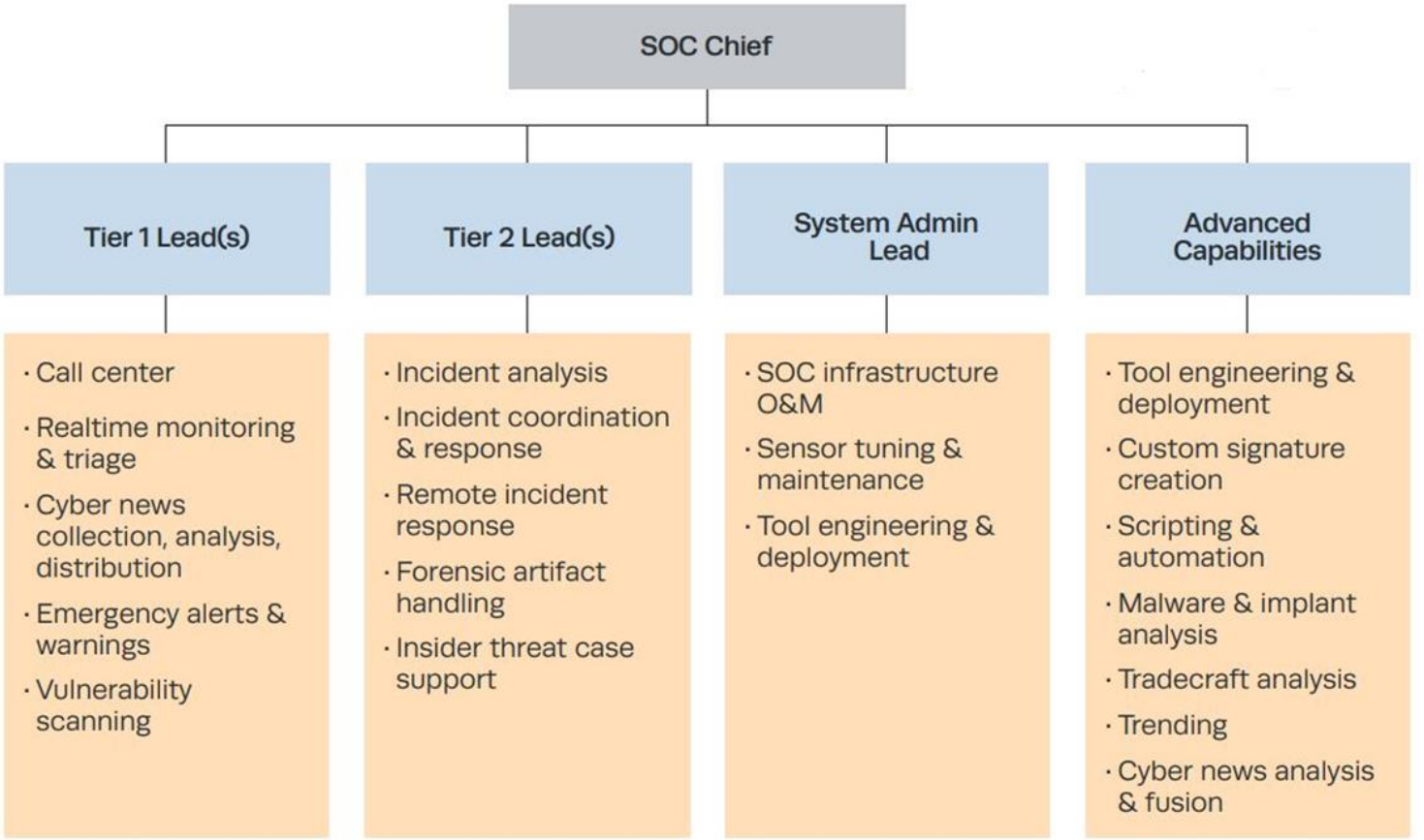
Планування та стратегія



Дуже важливо розуміти цілі та цінності організації, в якій функціонуватиме SOC, на основі яких має бути вибудовано його цілі та процеси. Фахівці майбутнього SOC мають розуміти яке місце вони займають у діяльності організації та вибудовувати свої функції, які сприятимуть роботі підприємства.

Має бути чітко вибудована стратегія розвитку, що враховує аспекти досвіду, технологій, параметри часу та місця, ресурси, область застосування тощо.

Розмежування обов'язків



Alternative Arrangement for a Small SOC. "Ten Strategies of a World-Class Cybersecurity Operations Center". Carson Zimmerman, The MITRE Corporation

Рекомендації

- Для забезпечення належного рівня захисту необхідно впроваджувати проактивні заходи, зокрема вибудовувати процеси управління кібербезпекою за концепцією SOC
- Інформаційна безпека та IT мають знати наявні у мережі активи, їх поведінку та поведінку користувачів, мають бути наявні засоби моніторингу мережі та засоби зберігання лог-файлів
- З метою автоматизації процесів пошуку, збору та аналізу даних та засобів із реагування на інциденти мають бути наявні інструменти управління подіями та інцидентами з налаштованими кореляційними правилами
- Необхідно проводити процеси планування та формування стратегії за принципами та цілями, що збігаються із цілями всієї організації
- Проведення заходів оцінки можливостей та зрілості повинна стати частиною основних процесів роботи SOC
- Розмежування обов'язків важлива складова роботи SOC, кожен з фахівців має розуміти свою роль та виконувати задачі в межах своєї відповідальності
- Необхідно постійно проводити роботу із вдосконалення процесів управління кібербезпекою, впроваджувати нові технології, навчати фахівців.

Висновки

У даній роботі викладені результати дослідження питання побудови та розвитку у корпоративній інформаційній системі, а саме:

- розглянуто концепцію сучасних корпоративних інформаційних систем та порушено питання забезпечення їх кібербезпеки;
- Досліджено, що наявність власного SOC здатна забезпечити організацію необхідним рівнем реактивного та проактивного захисту інформаційної інфраструктури;
- досліджено концепцію управління подіями та інцидентами як складової процесів управління кібербезпекою;
- Проведено дослідження можливостей рішень Microfocus ArcSight у забезпеченні повноцінних процесів зі збору, аналізу та розслідування подій та інцидентів;
- наведено приклад практичного застосування процесів збору та аналізу подій у засобі ArcSight ESM ;
- Розроблено чіткі практичні рекомендації із впровадження процесів SOC від моменту початкової інтеграції технології та їх опанування і до самого становлення повноцінного центру управління кібербезпекою, який постійно розвивається.

Отримані результати роботи можуть бути застосовані як методична рекомендація та інструкція із впровадження процесів забезпечення захисту мережі та систем корпоративної інформаційної системи із використанням аспектів реактивного і проактивного реагування на кіберзагрози.