МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Навчально-науковий інститут захисту інформації

На рецензію	До захисту
Завідувач кафедри УІКБ	Завідувач кафедри УІКБ
доктор економічних наук, професор	доктор економічних наук, професор
_____ С.В. Легомінова	_____ С.В. Легомінова
«___»_____ 2022 р.	«___»_____ 2022 р.

КВАЛІФІКАЦІЙНА РОБОТА

другого магістерського рівня вищої освіти

на тему:

ЦЕНТР ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ (SOC): НАПРЯМКИ І ТЕХНОЛОГІЇ

СТУДЕНТКА: Киричук Анна Олександрівна _____
(підпис)

КЕРІВНИК: к.держ.упр., доц. Мужанова Тетяна Михайлівна _____
(підпис)

НОРМОКОНТРОЛЕР: к.в.н., доц. Якименко Юрій Михайлович _____
(підпис)

Київ – 2022

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Навчально-науковий інститут захисту інформації

Кафедра управління інформаційною та кібернетичною безпекою
Спеціальність «Кібербезпека»
Спеціалізація «Управління інформаційною безпекою»
Другого магістерського рівня вищої освіти

«ЗАТВЕРДЖУЮ»
Завідувач кафедри УІКБ
_____ С.В. Легомінова
(підпис)

«___» _____ 2023 р.

ЗАВДАННЯ
на кваліфікаційну роботу
студенту Киричук Анні Олександрівні

Тема роботи «ЦЕНТР ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ (SOC): НАПРЯМКИ І ТЕХНОЛОГІЇ», затверджена наказом по університету № 122 від «12» жовтня 2022 р.

1. **Термін здачі** студентом оформленої роботи «04» грудня 2022 р.
2. **Об'єкт дослідження:** центр забезпечення безпеки (SOC).
3. **Предмет дослідження:** напрямки і технології центру забезпечення безпеки.
4. **Мета дослідження:** дослідження напрямків і технологій центру забезпечення безпеки (SOC).
5. **Перелік питань, які мають бути розроблені:**

5.1.Проаналізувати сутність і структуру SOC.

5.2.Дослідити компоненти й технології SOC.

5.3.Сформувати рекомендації щодо розробки і впровадження SOC.

7. Дата видачі завдання «15» вересня 2022 р.

Науковий керівник _____ Т.М. Мужанова
Підпис

Завдання прийнято до виконання _____ А.О. Киричук
Підпис

КАЛЕНДАРНИЙ ПЛАН

Дата видачі завдання: «15» _вересня_ 2022 р.

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	23.09.2022	
2.	Збір та аналіз літератури.	30.09.2022	
3.	Аналіз сутності і структури SOC	17.10.2022	
4.	Дослідження компонентів і технологій SOC	01.11.2022	
5.	Формування рекомендацій щодо розробки і впровадження SOC	15.11.2022	
6.	Формулювання висновків за результатами дослідження.	22.11.2022	
7.	Оформлення роботи.	04.12.2022	
8.	Оформлення презентації.	21.12.2022	
9.	Отримання рецензії на роботу.	24.12.2022	
10.	Захист в ДЕК.	__.01.2023	

Студентка А.О. Киричук
(підпис)

Науковий керівник Т.М. Мужанова
(підпис)

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню напрямків і технологій центру забезпечення безпеки (SOC) та розробці рекомендацій щодо його розробки і впровадження. Робота складається зі вступу, трьох розділів, що містять 14 рисунків, висновків та списку використаних джерел, що містить 104 найменування. Загальний обсяг роботи становить 101 аркуша, з яких 12 аркушів займають перелік умовних позначень і скорочень, список використаних джерел.

Об'єктом дослідження є центр забезпечення безпеки (SOC).

Предмет дослідження – напрямки і технології центру забезпечення безпеки.

Метою роботи є дослідження напрямків і технологій центру забезпечення безпеки (SOC).

Як результат у роботі проаналізовано сутність і структуру SOC; досліджено компоненти й технології SOC; сформовано рекомендації щодо розробки і впровадження SOC.

Галузь застосування. Розроблені рекомендації щодо напрямків, технологій та етапів впровадження центрів забезпечення безпеки (SOC) можуть бути використані при плануванні та реалізації SOC на підприємствах різних типів.

Ключові слова: ЦЕНТР ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ, SECURITY OPERATION CENTER (SOC), НАПРЯМКИ І ТЕХНОЛОГІЇ SOC, ЕТАПИ РОЗРОБКИ І ВПРОВАДЖЕННЯ SOC.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

CSIRT	Computer Security Incident Response Team
DCS	Distributed Control System
DDoS	Distributed Denial-of-Service
DNS	Domain Name System
DoS	Denial-of-Service
DSOC	Distributed SOC
GRC	Governance, Risk, and Compliance
GSOC	Grid SOC
IDS	Intrusion Detection System
IPFIX	The IP Flow Information eXport (IPFIX) protocol
IPS	Intrusion Prevention System
MDM	Mobile Device Management
MPLS	Multiprotocol Label Switching
NOC	Network Operations Center
NTP	Network Time Protocol
PPT	People, Processes, and Technologies
PPTGC	People, Processes, Technologies, Governance, Compliance
SCADA	Supervisory Control and Data Acquisition
SEM	Security Event Management
SIC	Security Intelligence Center
SIEM	Security Information & Event Management
SIM	Security Information Management
SLMS	Security Log Management Service
SNMP	Simple Network Management Protocol
SOC	Security Operation Center
UEBA	User & Entity Behavior Analytics

ВСТУП

Актуальність теми. З моменту запровадження центрів забезпечення безпеки (SOC) близько 15 років тому, їх значення постійно зростає, особливо за останній час. Це головним чином пов'язано з першочерговою необхідністю запобігання великим кіберінцидентам і, як наслідок, впровадженням централізованих операцій з безпеки на підприємствах.

Незважаючи на свою популярність, існуючі наукові роботи з питань комплексного захисту інформації підприємства не мають загальноприйнятого погляду і зосереджуються переважно на фрагментах, а не розглядають проблему цілісно. Ці недоліки перешкоджають подальшим інноваціям. Помітним недоліком академічних досліджень є їх зосередженість на людських і технологічних аспектах SOC, нехтуючи при цьому зв'язками між цими двома сферами через конкретні, найчастіше нетехнічні процеси.

З огляду на зазначене дослідження напрямів і технологій SOC, а також розробка рекомендацій щодо етапів їх розробки і впровадження є актуальним науковим завданням

Мета і завдання дослідження. **Мета роботи** полягає у дослідженні напрямків і технологій центру забезпечення безпеки (SOC).

Для досягнення цієї мети в роботі необхідно виконати наступні **завдання**:

1. Проаналізувати сутність і структуру SOC.
2. Дослідити компоненти й технології SOC.
3. Сформувати рекомендації щодо розробки і впровадження SOC.

Об’єкт дослідження - центр забезпечення безпеки (SOC).

Предмет дослідження – напрямки і технології центру забезпечення безпеки.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу та синтезу, узагальнення, порівняння, моделювання; історичний і абстрактно-логічний методи; методи системного аналізу і комплексного підходу.

Наукова новизна одержаних результатів. Розроблені рекомендації щодо напрямків діяльності та технологій у межах SOC допоможуть підприємствам спланувати і впровадити такий центр відповідно до встановлених цілей, ресурсів і бізнес-можливостей.

Практичне значення одержаних результатів. Застосування напрацювань дадуть змогу створити SOC, здійснивши обґрунтований вибір методів і технологій захисту інформації, інфраструктури та персоналу для конкретного типу підприємства.

Розділ 1 СУТНІСТЬ І СТРУКТУРА SOC

1.1 Визначення SOC та його архітектура

1.1.1 Що таке SOC?

Згідно з нещодавнім звітом The Cost of Cybercrime, середня кількість порушень безпеки, про які повідомляють організації, зросла на 11% з 130 у 2017 році до 145 інцидентів у 2018 році у всьому світі. За останні п'ять років ця кількість зросла загалом на 5%. Загальна річна вартість на відновлення після будь-якого виду кібератаки також зростає стійкими темпами.

Варто відзначити, що цей звіт охоплює лише виявлені та повідомлені інциденти, а кількість неповідомлених інцидентів вірогідно є значно більшою, і багато з них залишаються невиявленими упродовж довгого часу. Так, у 2018 році середній час виявлення інциденту склав 196 днів, а на локалізацію порушення в середньому пішло ще 69 днів [1]. Такий час виявлення демонструє, наскільки неефективно компанії виявляли та протидіяли кібератакам.

Причини такого неефективного виявлення та реагування на кібератаки включають, але не обмежуються тим, що компанії:

– не здійснюють огляду своїх пристроїв, систем, додатків та мереж;

– не знають, які активи захищати;

– не знають, які інструменти використовувати та як інтегрувати їх з існуючою інфраструктурою;

– не встигають за швидкісними технологіями та ландшафтом загроз, що постійно змінюється.

Центр забезпечення безпеки (Security Operation Center, SOC) – це організаційна одиниця, що діє в центрі всіх операцій з безпеки. Зазвичай він не розглядається як окремий підрозділ або система, а скоріше як складна структура для управління та посилення загальної системи безпеки організації.

Його функція полягає у виявленні, аналізі та реагуванні на загрози та інциденти кібербезпеки з використанням людей, процесів та технологій.

Хоча широко визнається, що SOC є надзвичайно важливим для безпеки компанії, він все ще вважається пасивним і реактивним захисним механізмом. Дослідження часто описують операції в рамках SOC відповідно до концепції «Персонал, Процеси і Технології» (People, Processes, and Technologies, PPT) [2]. Ця структура використовується для різних тем IT, таких як управління знаннями або управління взаємовідносинами з клієнтами. Крім того, серед постачальників SOC ця структура популярна для узагальнення і структурування свого продукту.

Хоча аспект управління та відповідності часто підпорядкований процесам, його вважають самостійною категорією через високу важливість у SOC. Він пропонує рамки, в яких працюють фахівці й відповідно до яких будуються процеси та технології. Розширивши оригінальну структуру PPT, отримуємо структуру Персонал, Процеси, Технології, Управління та Відповідність (People, Processes, Technologies, Governance, Compliance PPTGC), яка показана на рисунку 1.1.

Рис 1.1 Структура PPTGC

При впровадженні разом з системою PPTGC SOC може покращити стан безпеки компанії. Однак, не існує чіткої термінології, що описує SOC. Наступні пункти розмежовують SOC від різних інших термінів:

Команда реагування на інциденти комп'ютерної безпеки (Computer Security Incident Response Team, CSIRT). Цей термін часто використовується як взаємозамінний для SOC, хоча він в основному фокусується на частині реагування після того, як атака сталася. CSIRT - це організаційний підрозділ, відповідальний за координацію та підтримку реагування на інцидент комп'ютерної безпеки. CSIRT класифікується або як незалежна команда або як частина SOC.

Центр мережевих операцій (Network Operations Center, NOC). NOC здійснює нагляд за виявленням, розслідуванням, визначенням пріоритетів, ескалацією та вирішенням проблем. Однак, NOC фокусується на інцидентах, що впливають на продуктивність та доступність мережі організації. Оскільки інциденти можуть виникати у всіх системах, а не тільки в мережах, організаціям вигідно, коли команди NOC і SOC працюють разом.

Центр розвідки безпеки (Security Intelligence Center, SIC). SIC був вперше використаний в 2017 році для опису наступника SOC. Він може повністю візуалізувати та управляти розвідданими з питань безпеки в одному місці. Таким чином об'єднуються кілька технологій (наприклад, управління знаннями з інформаційної безпеки, обробка великих даних).

Управління інформацією та подіями безпеки (Security Information and Event Management, SIEM). Система SIEM є невід'ємною частиною багатьох SOC для покриття значної частини технологічних вимог. Вона відповідає за централізований збір даних, що мають відношення до безпеки. Таким чином, вона забезпечує можливості аналізу безпеки шляхом кореляції журналів подій. Інші функціональні можливості дозволяють збагачення контекстними даними, нормалізацію різнорідних даних, звітність та оповіщення. Для забезпечення обміну інформацією про загрози SIEM

забезпечує підключення до платформ обміну розвідданими про кіберзагрози, і залучає аналітиків з питань безпеки, пропонуючи можливості візуальної аналітики безпеки. Вона включає в себе можливості ведення журналів та управління шляхом тривалого зберігання даних про події.

Центр забезпечення безпеки (Security Operation Center, SOC) забезпечує виконання організаційного аспекту стратегії безпеки підприємства. Він об'єднує процеси, технології та людей для управління та посилення загальної системи безпеки організації. Ця мета, як правило, не може бути досягнута окремим підрозділом або системою, а скоріше складною структурою. Вона створює ситуаційну обізнаність, зменшує ризики й допомагає дотримуватися регуляторних вимог. Крім того, SOC забезпечує управління та дотримання вимог як рамки, в яких працюють люди і до яких пристосовані процеси та технології.

1.1.2 Архітектура SOC

Проведемо огляд підходів до архітектурного проектування SOC.

ЗАГАЛЬНА АРХІТЕКТУРА.

На високому й абстрактному рівні SOC можуть бути структуровані як централізовані, розподілені або децентралізовані структури. У випадку SOC, централізована архітектура описує підхід, коли всі дані надсилаються з різних місць або дочірніх компаній до одного центрального SOC для подальшої обробки.

Розподілений SOC, з іншого боку, нагадує одну єдину систему, що працює в декількох дочірніх компаніях. А користувачам здається, що вони мають справу з одним суб'єктом господарювання. Розподілена система дозволяє всім суб'єктам отримувати, обробляти, об'єднувати та надавати інформацію та послуги з безпеки іншим суб'єктам. Це дозволяє рівномірно розподілити робоче навантаження і дані.

Третім загальним архітектурним рішенням для SOC є децентралізована система, яка є поєднанням двох вищезгаданих системних рішень.

Децентралізований SOC складається з декількох SOC з можливо обмеженими можливостями, які підпорядковуються одному або декільком центральним SOC. Зрушення від наявності одного центрального SOC до більш децентралізованої архітектури спостерігається при порівнянні більш ранніх досліджень з більш пізніми публікаціями. Основною причиною цього, як визначається, є уникнення єдиної точки відмови.

ТЕХНОЛОГІЧНІ АРХІТЕКТУРИ ТА ПРОЕКТИ.

SOC - це організаційна одиниця, що охоплює різні функціональні можливості, а не лише одну єдину систему. Однією з перших архітектурних моделей для SOC є SOCBox, яка була запропонована Р. Біду та ін. [18] і оцінена А. Ганаме та ін. [8]. SOCBox визначає SOC як систему, що складається з п'яти основних модулів: генераторів подій, збирачів подій, баз даних повідомлень, механізмів аналізу та програмного забезпечення для управління реакцією.

Хоча архітектура SOCBox все ще залишається актуальною щодо її основних компонентів, вона має певні обмеження, оскільки була запропонована майже 15 років тому, а технології значно розвинулись. SOCBox в першу чергу фокусується на зборі даних та управлінні інцидентами, але не включає цифрову криміналістику та можливості реагування для запобігання атакам. Крім того, запропонована архітектура описує централізовану систему з численними єдиними точками відмови. Через складність сучасних IT-ландшафтів та технологічних розробок, розподілені архітектури часто вважаються більш доцільними. Тому архітектура SOCBox пройшла кілька ітерацій і вдосконалювалася протягом багатьох років. Її прямим спадкоємцем є Distributed SOC (DSOC), запропонована тією ж групою авторів [22].

Архітектура DSOC закладає основу для розподіленої архітектури Grid SOC (GSOC) для критичних інфраструктур, яка знову ж таки розробляється дослідницькими групами, що починали роботу над оригінальним SOCBox. Ці три архітектури підкреслюють перехід від централізованого до розподіленого налаштування SOC з плином часу. Оригінальна архітектура SOCBox також

була використана Н. Милославською [16] для проектування сучасної SOC для обробки великих даних.

С. Раду [2] стверджує, що архітектура SOC складається з рівня генерації, рівня збору, рівня маніпулювання даними та рівня виведення або представлення. Цей більш абстрактний підхід до визначення технологічної архітектури SOC з використанням лише декількох будівельних блоків можна знайти в декількох роботах [3, 24–26].

У цих публікаціях робиться висновок, що SOC складається з подібних архітектурних блоків: блок, який узагальнює джерела даних, за яким слідує блок, призначений для збору даних з джерел і передачі їх третьому блоку, що відповідає за аналіз даних. Останній блок описує представлення результатів аналізу даних. Жоден з цих блоків не робить жодних припущень, незалежно від того, робиться це вручну чи автоматично.

Визначимо подальші пропозиції архітектур SOC у відповідній літературі, зосередившись на SOC для конкретних варіантів використання. Дж. Сеттані та ін. [27] описують реалізацію архітектури SOC для постачальників критичної інфраструктури. Т. Тафаззолі та Х.Г. Гракані [28] пропонують архітектуру для обробки подій в середовищі OpenStack для виявлення атак в хмарі на дуже поверхневому рівні. Існує широкий спектр інших, дуже специфічних та орієнтованих на конкретні домени SOC архітектур.

ОПЕРАЦІЙНІ МОДЕЛІ ТА ФАКТОРИ ВПЛИВУ.

Існує багато способів управління SOC. У широкому розумінні, операторська діяльність може здійснюватися як на внутрішньому, так і на зовнішньому ринках. Однак існують різні інші та більш специфічні класифікації.

С. Шинагл та ін. [47] пропонують класифікувати різні операційні моделі на основі організаційного розміщення та функціональності SOC на інтегральний, технологічно орієнтований, частково аутсорсинговий та спеціалізований SOC.

Інший підхід до класифікації операційних моделей SOC застосовують К. Зіммерман та ін. [48] та адаптований С. Раду та ін. [2]. Вони використовують комбінацію розміру, повноважень, організаційної моделі та пропонують розділити SOC на п'ять різних операційних моделей: віртуальний SOC, малий SOC, великий SOC, багаторівневий SOC та національний SOC.

Інша класифікація операційних моделей SOC застосовує чотири основні категорії: виділені, віртуальні, аутсорсингові та гібридні SOC.

Незалежно від операційної моделі SOC, він повинен бути захищеним. Несправний SOC залишає всю решту компанії вразливою, оскільки атаки можуть поширюватися непоміченими. Тому безпеці SOC необхідно приділяти особливу увагу. Кожна операційна модель має певні переваги та недоліки, і важливо прийняти рішення заздалегідь.

Зміна структури SOC після його створення потребуватиме значної кількості часу та ресурсів. Однак, вибір між моделями функціонування SOC не є тривіальним завданням, і наслідки цього вибору повинні бути ретельно розглянуті. В літературі виділяють різні фактори, які впливають на цей вибір:

- **Стратегія компанії:** Необхідно узгодити рішення із загальною бізнес-стратегією та IT-стратегією компанії, щоб визначити, яка операційна модель підходить найкраще. Стратегія SOC повинна бути визначена до вибору відповідної операційної моделі.

- **Галузь:** Галузь, в якій компанія в основному працює, значною мірою впливає на обсяг необхідного SOC.

- **Розмір:** Розмір компанії також має вплив на рішення, оскільки невелика компанія може бути не в змозі створити та керувати SOC самостійно або може навіть не потребувати чітко визначеного SOC.

- **Витрати:** Витрати на внутрішнє впровадження та підтримку SOC необхідно порівнювати з витратами на аутсорсинг операцій з безпеки. На початковому етапі розгортання власної SOC може бути дорожчим, але такий варіант може виявитися більш економічно ефективним у довгостроковій перспективі. Витрати на пошук, наймання та навчання персоналу SOC є

значним фактором, особливо з огляду на те, що вони можуть зростати через дефіцит кваліфікованих кадрів і збільшення ринкового попиту.

- **Час:** створення SOC займає значний проміжок часу. Тому узгодження з організаційними планами та часовими рамками є необхідним. Крім того, час на створення SOC слід порівнювати з часом, необхідним для його аутсорсингу.

- **Нормативно-правове забезпечення:** Залежно від галузі, необхідно враховувати різні нормативні акти. Деякі з них можуть вимагати впровадження операційного SOC, інші можуть забороняти аутсорсинг операцій SOC взагалі, або, принаймні, конкретним постачальникам, які не дотримуються відповідних правил.

- **Конфіденційність:** Недоторканність приватного життя також підпадає під регулювання і має бути дотримана при роботі SOC з персональними даними .

- **Доступність:** Необхідно враховувати вимоги щодо доступності. Здебільшого мета полягає в тому, щоб мати SOC 24/7, 365 днів на рік.

- **Підтримка з боку топ-менеджменту:** Підтримка керівництва має вирішальне значення при створенні спеціалізованого SOC. Якщо керівництво не зацікавлене, а переваги SOC не будуть доведені до його відома, команда може не отримати необхідних ресурсів.

- **Інтеграція:** Можливості внутрішнього SOC повинні бути інтегровані з іншими IT-підрозділами, в той час як у зовнішньому SOC необхідно інтегрувати провайдера, щоб отримати всі необхідні дані.

- **Проблеми втрати даних:** SOC найчастіше є центральним місцем, де обробляється значна кількість конфіденційних даних. Внутрішні SOC повинні бути високо захищеними, в той час як для зовнішніх SOC повинен бути обраний надійний провайдер, який може забезпечити захист даних від крадіжки інтелектуальної власності, а також від випадкової втрати.

- **Експертиза:** Для накопичення досвіду потрібен час і гроші. Необхідні навички для управління SOC не легко знайти. Набір і утримання персоналу є вирішальним фактором для внутрішніх SOC. Однак, необхідні навички вже

наявні є у зовнішніх провайдерів послуг SOC. Однак компанії повинні усвідомлювати, що аутсорсинг зменшує внутрішні знання.

1.2 Концепція PPT

Концепція PPT (People, Process. Technology) передбачає визначення процесів для оптимізації операцій, впровадження правильної технології для підвищення ефективності роботи і наймання фахівців з потрібними навичками для управління цими процесами. Таким чином, структура дозволяє нам узгоджено визначити SOC та його компоненти.

1.2.1 Персонал

Дотримуючись структури PPT, спочатку розглянемо персонал, який бере участь у роботі SOC. Наукова література дозволяє визначити різні ролі й обов'язки, пов'язані з управлінням SOC. Іншим важливим аспектом, який обговорюється у відповідній літературі, є підбір персоналу та різні методи його утримання. Також, підкреслюється важливість програм навчання й підвищення обізнаності і, визначаються процедури співпраці та комунікації в рамках SOC.

РОЛІ ТА ОБОВ'ЯЗКИ.

Як і в будь-якій іншій організаційній одиниці, в рамках SOC існує декілька різних ролей та обов'язків. Залежно від сфери діяльності та розміру, різні команди потрібні в різній кількості. Типовими основними ролями в SOC є аналітики різних рівнів, а також спеціалізовані менеджери. На основі проведеної роботи виділимо три ролі з відповідними обов'язками [34]:

Рівень 1 (спеціаліст з обробки даних): Аналітики рівня 1 в основному відповідають за збір первинних даних, а також аналіз тривог і попереджень. Вони повинні підтвердити, визначити або скоригувати критичність тривог та збагатити їх відповідними даними. Для кожної тривоги фахівець із сортування повинен визначити, чи є вона обґрунтованою або хибнопозитивною. Додатковим обов'язком на цьому рівні є виявлення інших подій високого

ризику та потенційних інцидентів. Всі вони повинні бути пріоритезовані відповідно до їхньої критичності. Якщо проблеми, що виникають, не можуть бути вирішені на цьому рівні, вони передаються на розгляд до аналітиків 2-го рівня. Крім того, фахівці з обробки даних часто керують і налаштовують інструменти моніторингу.

Рівень 2 (фахівець з реагування на інциденти): На рівні 2 аналітики розглядають більш критичні інциденти безпеки, які були передані від фахівців з обробки даних, і проводять більш поглиблену оцінку, використовуючи розвіддані про загрози (індикатори компрометації, оновлені правила, тощо). Вони повинні розуміти масштаби атаки і знати про уражені системи. На рівні 2 необроблені дані телеметрії атаки, зібрані на рівні 1, перетворюються в дієву інформацію про загрози. Фахівці з реагування на інциденти відповідають за розробку й реалізацію стратегій для локалізації та відновлення після інциденту. Якщо аналітик рівня 2 стикається з серйозними проблемами з ідентифікацією або пом'якшенням наслідків атаки, залучаються додаткові аналітики рівня 2, або інцидент передається на розгляд на рівень 3.

Рівень 3 (мисливець за загрозами або Threat Hunter): Аналітики рівня 3 є найбільш досвідченими працівниками SOC. Вони займаються великими інцидентами, які їм передають оперативні служби реагування на інциденти. Вони також виконують або, принаймні, контролюють оцінку вразливостей і тести на проникнення для виявлення можливих векторів атаки. Їх найважливішим обов'язком є активне виявлення можливих загроз, прогалин у безпеці та вразливостей, які можуть бути невідомими. Отримавши обґрунтовані знання про можливу загрозу для систем, вони також повинні рекомендувати шляхи оптимізації розгорнутих інструментів моніторингу безпеки. Крім того, будь-які критичні попередження, розвіддані про загрози й інші дані про безпеку, надані аналітиками рівнів 1 та 2, розглядаються на цьому рівні.

SOC-менеджер: Менеджери SOC здійснюють нагляд за командою оперативного управління безпекою. Вони надають технічні рекомендації за необхідності, але найголовніше – вони відповідають за належне управління

командою. Це включає в себе наймання, навчання й оцінку членів команди, створення процесів, оцінку звітів про інциденти, а також розробку та впровадження необхідних планів кризових комунікацій. Вони також здійснюють нагляд за фінансовими аспектами діяльності SOC, підтримують проведення аудитів безпеки та звітують перед керівником служби інформаційної безпеки (КСІБ) (Chief Information Security Officer, CISO) або відповідною посадовою особою вищого рівня управління.

Ці ключові ролі можна знайти у всіх SOC незалежно від їхнього розміру. Однак, у менших SOC обов'язки кожної ролі є ширшими, і вони звужуються, щоб бути більш конкретними, коли SOC зростає. Наприклад, у невеликому SOC, де працює лише кілька аналітиків, кожен з них повинен володіти кількома навичками, оскільки кілька співробітників повинні виконувати всі завдання, що виникають.

У більшому SOC ролі можуть бути більш специфічними, оскільки, наприклад, деякі аналітики можуть бути зосереджені на моніторингу мережі, в той час як інші є експертами з особливостей Windows або Linux. Це дає багато переваг: краща і швидша реакція на загрози або кращий розподіл завдань.

Окрім чотирьох вже описаних основних ролей, визначимо додаткові ролі, які принаймні певною мірою задіяні у повсякденній діяльності у повсякденній діяльності SOC , спробуємо їх структурувати і встановити можливі взаємозв'язки між ними. На рисунку 1.2 зображено ті з них, що базуються на підході, розробленому С. Олт [63].

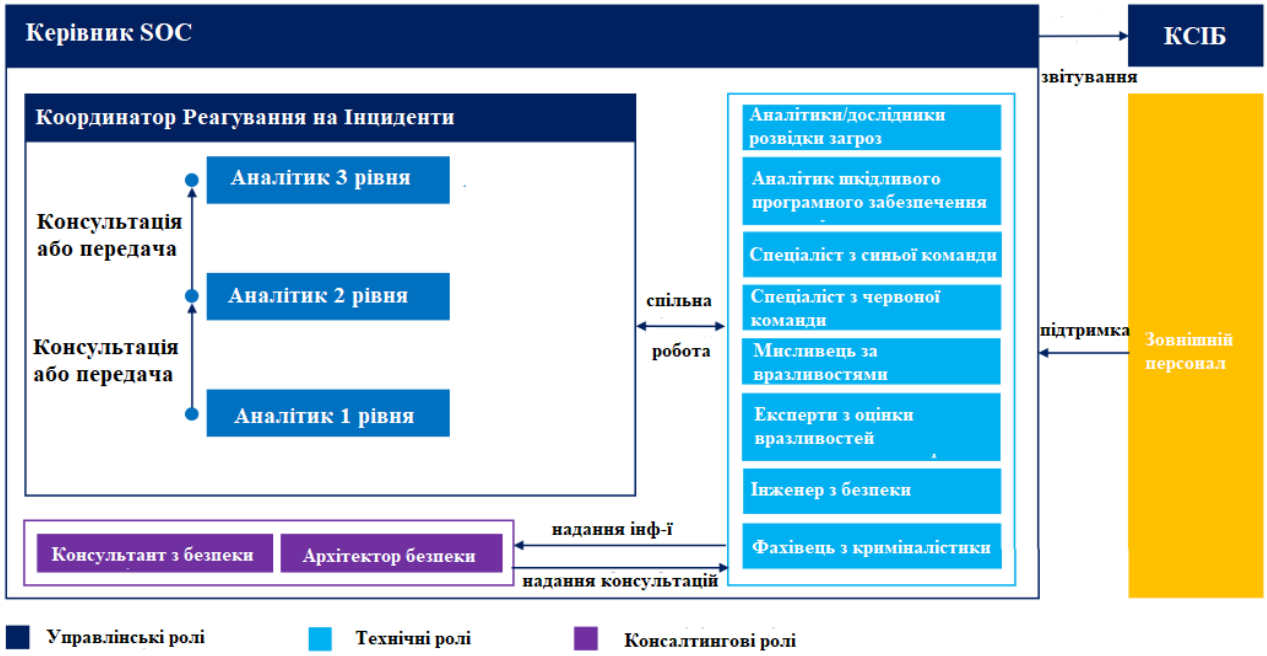

Рис 1.2 Взаємодія різних ролей в рамках SOC

Виконавці цих додаткових ролей повинні очолювати, працювати разом або співпрацювати з раніше описаними носіями основних повноважень SOC, які також враховані на рисунку 1.2. Однак, при управлінні конкретним SOC може відбуватися значне перекриття між основними й додатковими ролями. Саме тому ролі згруповано в п'ять основних груп, які позначені різними кольорами. Ці групи за потреби можуть бути адаптовані або розширені додатковими ролями:

– **Управлінські ролі:** У контексті SOC виділимо три критично важливі управлінські ролі. Перш за все, керівник служби інформаційної безпеки (КСІБ), який визначає стратегії, цілі та завдання загальних операцій з безпеки організації. Друга позиція це керівник SOC, який власне і керує SOC. Третьою важливою позицією в SOC є координатор реагування на інциденти, який координує всю діяльність, пов'язану з реагуванням на інциденти.

– **Технічні ролі:** Існує широкий перелік додаткових фахівців з безпеки, які можуть співпрацювати з аналітиками SOC для забезпечення його ефективної та результативної роботи.

Аналітики шкідливого програмного забезпечення допомагають реагувати на складні загрози, виконуючи зворотну розробку шкідливого коду і

створюючи важливі результати для заходів з реагування на інциденти. Щоб бути в курсі можливих поточних атак, мисливці за загрозами активно шукають загрози всередині організації, наприклад, переглядаючи журнали, або за межами організації, аналізуючи наявні дані розвідки загроз. Ці дані розвідки загроз також безпосередньо обробляються аналітиками або дослідниками розвідки загроз, які аналізують розвіддані про загрози з різних джерел і надають інформацію команді SOC. Якщо частина атаки була успішною, фахівці з криміналістики проводять її детальне розслідування. Вони збирають і аналізують судові докази юридично обґрунтованим чином.

Червоні та Сині команди активно намагаються атакувати або відповідно захищати системи організації для виявлення вразливостей, і обидві команди тестують, а також підвищують ефективність і стійкість механізмів безпеки. Нарешті, експерти з оцінки вразливостей проводять дослідження для виявлення нових, раніше невідомих вразливостей та управляють відомими вразливостями з урахуванням бізнес-ризиків. Ці експерти створюють детальні технічні звіти зі своїми висновками та надають підтримку SOC аналітикам або командам реагування на інциденти у виявленні вразливостей.

Ще однією важливою роллю цієї групи є інженер з безпеки (Security Engineer, SE), який розробляє, інтегрує і підтримує інструменти SOC. Інженери з безпеки також визначають вимоги до нових інструментів. Вони забезпечують відповідний доступ до інструментів і систем. Додатковими завданнями є конфігурація та встановлення міжмережевих екранів і систем виявлення або запобігання вторгненням. Крім того, вони допомагають у написанні й оновленні правил виявлення для SIEM.

– **Консалтингові функції:** Дві найважливіші ролі в цій групі - це архітектор безпеки (Security Architector, SA) та консультант з безпеки (Security Consultant, SC). Архітектори безпеки планують, досліджують і розробляють надійну інфраструктуру безпеки в компанії, проводять регулярне тестування

системи та її вразливостей, контролюють впровадження або вдосконалення системи. Вони також відповідають за створення процедур відновлення.

Консультанти з безпеки часто досліджують стандарти безпеки, кращі практики і системи безпеки. Вони можуть надати огляд галузі для організації і порівняти поточні можливості SOC з конкурентами. Вони можуть допомогти у плануванні, дослідженні та розробці надійної архітектури безпеки.

На рисунку 1.3 показано, як організації з різних куточків світу зацікавлені в розгортанні SOC. Вони постійно наймають фахівців SOC, таких як керівники SOC (Security Managers) та аналітики SOC (Security Analysts), щоб забезпечити безпеку своєї інфраструктури.

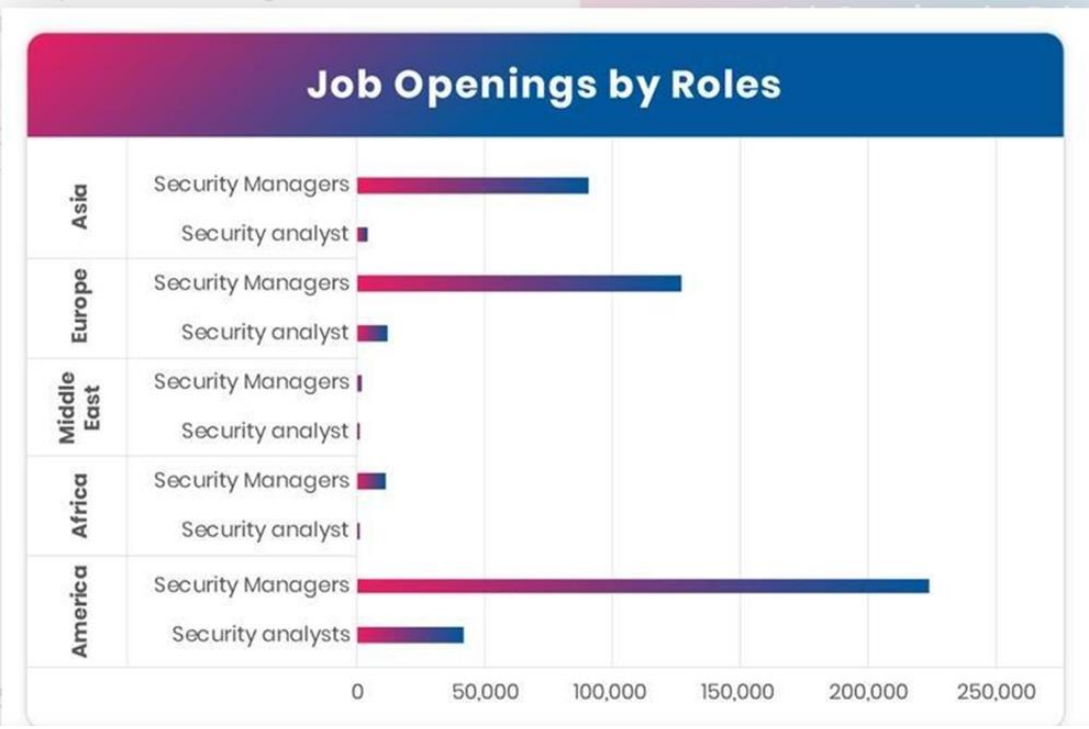

Рис 1.3 Графік відкритих вакансій в різних частинах світу за 2022 рік

Професіонали, які працюють в SOC, є останньою лінією оборони і відповідають за виявлення та успішне пом'якшення наслідків атак. Таким чином, наявність кваліфікованих людських ресурсів у достатній кількості є обов'язковою умовою для успіху SOC. Однак знайти й утримати потрібний персонал є непростим завданням.

Міжнародний консорціум з сертифікації безпеки інформаційних систем (ISC) оцінює поточний дефіцит кадрів у сфері кібербезпеки приблизно в 4 млн

осіб у світовому масштабі, і він продовжує зростати [64]. Тому набирати новий кваліфікований персонал для SOC стає все складніше. Літератури про те, як саме обирати персонал для SOC, практично не існує. Більшість відповідних документів зосереджені на утриманні персоналу SOC та закритті прогалин у навичках за допомогою автоматизації.

Перспективною тенденцією є оперативне використання платформ візуалізації з функціями спільної роботи. Наприклад, платформа 3D CyberCOP [70] розрізняє явну спільну роботу через платформу та неявну співпрацю через усне спілкування і протоколювання дій кожного користувача.

Для успіху команди SOC вкрай важливо мати постійну взаємодію та комунікацію з іншими бізнес-підрозділами, зокрема службою підтримки, мережевими адміністраторами або навіть юридичною командою. Для цього необхідно сформувати розуміння працівників інших підрозділів, що фахівці SOC працюють не для того, щоб стежити за кожним їхнім кроком, а щоб допомогти.

1.2.2 Процеси

Відповідно до моделі PPT наступним елементом SOC є процеси. Оскільки метою SOC є реагування на інциденти або підготовка до них, одним із способів структурування основних процесів є життєвий цикл реагування на інциденти або подібні структури, такі як представлені в ISO/IEC 27035:2016 [77]. Відповідно до Керівництва NIST з обробки інцидентів комп'ютерної безпеки [78], життєвий цикл реагування на інциденти складається з чотирьох етапів: "підготовка", "виявлення та аналіз", "локалізація, усунення та відновлення" та "діяльність після інциденту".

Література дає лише неповне уявлення про процеси. Наприклад, технічні процеси розглядаються дуже інтенсивно, в той час як більшість супутніх процесів розглядаються лише поверхнево. Ці аспекти слід розглядати як прогалини в дослідженнях, відповідно вони представлені в наступній главі неповно.

1) ПІДГОТОВКА

Проаналізована література в основному зосереджена на зборі даних в рамках теми підготовки, однак вона не дає єдиного уявлення про те, з яких етапів складається процес збору даних. Як показано на рисунку 1.4, етапи нормалізації з синхронізацією часу, фільтрації, скорочення, агрегування, та визначення пріоритетів або оцінка ризиків згадувалися найчастіше. Порядок етапів процесу в наукових джерелах не є однаковим, оскільки він може змінюватися в залежності від використовуваного додатку. Однак, здебільшого він описується у представленій послідовності.

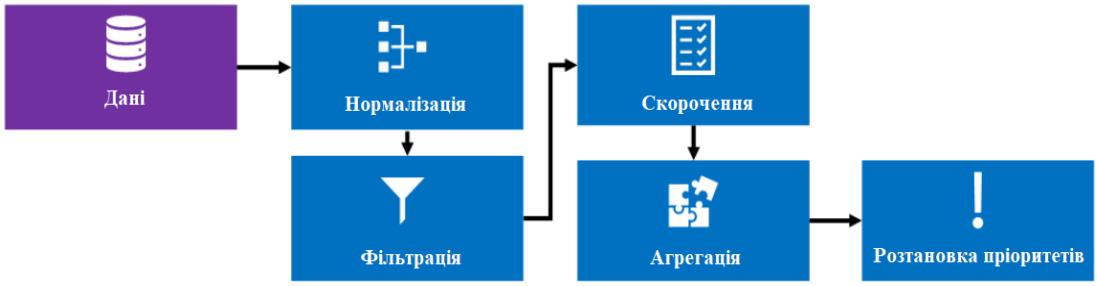

Рис 1.4 Процес збору даних

Виділені етапи процесу пояснюються більш детально для забезпечення загального розуміння:

Нормалізація: Життєво важливо перевести різнорідні формати даних в єдине представлення для проведення подальшої обробки. Також важливо привести всі часові дані до одного стандартного часового поясу й формату. Синхронізація допомагає уникнути плутанини в часовій шкалі подій безпеки і знижує ймовірність помилкових висновків на основі непослідовно виміряної мережевої активності. У літературі нормалізацію часто називають синтаксичним аналізом журналу або попередньою обробкою.

Фільтрація: Оскільки системи зазвичай генерують величезні обсяги даних, важливо фільтрувати елементи даних, які можуть містити важливу інформацію з точки зору безпеки.

Скорочення: Скорочення схоже на фільтрацію, з тією різницею, що окремі, неважливі поля даних сортуються для зменшення обсягу даних.

Агрегація: Подібні події об'єднуються в один єдиний елемент даних. Наприклад, три записи журналу, які вказують на спробу входу на хост, можуть бути об'єднані в один єдиний журнал, де зазначається тип і кількість спроб входу.

Розстановка пріоритетів: Кожні дані журналу повинні бути класифіковані відповідно до важливості для полегшення подальшої обробки. Наприклад, щоб вирішити, як реагувати на події або як довго зберігати журнали, корисно розставити пріоритети для вхідних даних.

2) ВИЯВЛЕННЯ ТА АНАЛІЗ

Велика кількість даних, зібраних на попередніх етапах, може бути непосильною для опрацювання навіть досвідченими практиками й дослідниками у сфері безпеки. Перетворення цих даних на корисну інформацію здійснюється за допомогою аналізу даних і, по суті, є засобом осмислення зібраної інформації. Однак лише кілька робіт розглядають предметну область з абстрактної, процесно-орієнтованої точки зору. Наступні кроки процесу були визначені шляхом об'єднання наявних процесів та шляхом послідовності індивідуально названих кроків у зазначеній літературі. В результаті отримано процес, який складається з етапів виявлення, аналізу та пріоритизації оповіщень/послідовність.

Виявлення: Інциденти виявляються за участю фахівців або з допомогою автоматичних процедур. Таким чином, необхідно вирішити, чи свідчать зібрані дані про інцидент безпеки.

Аналіз: Щодо методів, які використовуються для аналізу, можна виділити кореляцію джерела та цілі, структурний аналіз, функціональний аналіз і аналіз поведінки. Таким чином, автори описують мету кореляції як забезпечення можливості аналізу складних послідовностей шляхом отримання простих, синтезованих і точних подій.

Пріоритизація оповіщень/послідовність: Пріоритетність оповіщення, також відома як сортування, може розглядатися як зв'язок між локалізацією, ліквідацією і відновленням. Вона служить двом основним цілям. По-перше, для

забезпечення того, щоб найбільш серйозні інциденти розглядаються в першу чергу, а по-друге, для забезпечення того, щоб інциденти розподілялися для подальшої обробки відповідно до наявних ресурсів.

3) ЛОКАЛІЗАЦІЯ, ЛІКВІДАЦІЯ ТА ВІДНОВЛЕННЯ

Діяльність з локалізації, ліквідації та відновлення на високому рівні описана С. Бхаттом та ін [88]. Цей етап спрямований на прийняття рішення про те, чи є інцидент нешкідливою подією (наприклад, під час тестування на проникнення) або шкідливою подією. У випадку шкідливого інциденту він передається відповідним зацікавленим сторонам для вжиття подальших заходів.

У цьому контексті велике значення мають системи захисту управління, автоматизації та реагування на інциденти безпеки (Security Orchestration, Automation, and Response, SOAR), які становлять дуже активний напрямок досліджень останніх двох років. За даними Ч. Іслам та ін. [89] ключовою метою SOAR є автоматизація процесів за допомогою управління. Функціональні можливості SOAR в основному поділяються на інтеграцію, управління й автоматизацію. Захист управління є передумовою автоматизації безпеки, яка є процесом автоматичного виявлення. Таким чином, SOAR інтегрує наявну інформацію про інциденти безпеки (Cyber Threat Intelligence), щоб якомога швидше автоматично вживати належних заходів для обмеження шкоди.

Простою структурою для боротьби з інцидентами є цикл "Спостерігай, орієнтуйся, вирішуй, дій" (Observe, Orient, Decide, Act, OODA), який є відомою аналітичною структурою для прийняття рішень, розробленою Дж. Бойдом [92]. Вона може бути застосована до управління інцидентами в контексті SOC, як показано в дослідженнях [58, 93] (або аналогічно до циклу "Плануй, впроваджуй, перевіряй, дій" (ПВПД) [76]).

У літературі про SOC управління інцидентами здебільшого згадується у зв'язку з життєвим циклом обробки інцидентів. Так, процес управління оповіщеннями й інцидентами (Alert and Incident Management), показаний на рисунку 1.5, складається з етапів процесу, визначених двома основними стандартами з управління інцидентами інформаційної безпеки [77, 78].

Рис 1.5 Процес аналізу, виявлення й управління інцидентами SOC

Більш детального опису цих етапів процесу стосовно SOC в проаналізованій літературі не представлено, з огляду на що за необхідності слід звертатися до згаданих вище стандартів. Причиною цього може бути те, що працівники знають, які завдання вони мають виконувати, але це не було чітко визначено, що може спричинити проблеми, наприклад, при зміні персоналу.

1.2.3 Технології

Третім елементом, який розглядається у рамках SOC, є технології. Він охоплює етапи процесу з технічної точки зору. Спочатку розглянемо технології збору даних, які підтримують процес підготовки. Кожна організація повинна визначити, які пристрої слід контролювати, які дані необхідно збирати та в якому форматі вони повинні зберігатися. Крім того, в залежності від даних, необхідно встановити термін зберігання даних. Далі буде розглянута методологія та підходи, що застосовуються для аналізу даних, виявлення загроз і представлення результатів, які можна зіставити з процесом виявлення й аналізу. Як інтерфейс між людьми і машинами, представлення даних і результатів аналізу представляє особливий інтерес в контексті SOC.

1) ЗБІР ДАНИХ

Існують різні методи збору даних, які загалом можна розділити на чотири категорії: виштовхування/витягування, розподілений/централізований, збір у реальному часі/історичний та частковий/повний збір. Дані можуть або витягуватися збирачем даних, або надходити до збирача даних із самого джерела даних. Крім того, вони можуть збиратися в централізованому колекторі журналів або в розподіленій топології на різних вузлах. Таким чином, дані можуть бути зібрані повністю або частково. Збір даних в основному пов'язаний з визначенням джерел даних, які фіксують відповідну інформацію, пов'язану з безпекою. Хоча нові джерела даних постійно створюються, наведені найбільш поширені джерела, їх класифікація та відповідні приклади:

– **Захисне програмне забезпечення:** SIEM-системи, системи виявлення/запобігання вторгнення, міжмережеві екрани, антивірусне програмне забезпечення, сканери вразливостей, управління ідентифікацією та доступом.

– **Мережеве обладнання:** Комутатори, маршрутизатори, сервери, хости, проксі-сервери.

– **Середовища віртуалізації:** Гіпервізор, самоаналіз віртуальних машин, хмарні середовища.

– **Операційні технології:** Датчики, виконавчі механізми.

– **Інше програмне забезпечення:** Аналітика великих даних з відкритим кодом, бази даних, управління ідентифікацією та доступом, поштовий сервер, операційні системи.

– **Фізичні засоби безпеки:** Камери спостереження, засоби контролю доступу.

– **Зовнішня розвідка (загроз):** Геолокація та DNS пошук, розвідка з відкритих джерел (OSINT), розвіддані з платформ обміну загрозами або інших організацій.

– **Люди:** Співробітники (Human-as-a-Security-Sensor), зовнішні користувачі.

Кожне з цих джерел даних може надавати величезну кількість інформації, з якої не вся є релевантною. Збір усієї наявної інформації може допомогти у

виявленні зловмисної діяльності, але це також може негативно вплинути на продуктивність системи. І навпаки, якщо для збору даних використовується менше джерел, атака може залишитися непоміченою. Таким чином, пошук правильного балансу між надмірним і недостатнім збиранням даних має важливе значення при проектуванні технологічних можливостей SOC. Однак, як правило, краще збирати дані з якомога більшої кількості джерел, наскільки це можливо (в умовах обмежень продуктивності), а потім покладатися на добре відпрацьовані механізми нормалізації, кореляції й аналізу даних.

Залежно від джерела даних, тип зібраних даних може відрізнятися. Всі зібрані дані можна умовно поділити на дані журналів або розвідувальні дані. Журнали документують поточний стан системи і, як правило, фіксують всі зміни, що відбуваються в системі. Журнали, як правило, поділяються на журнали операційної системи/додатків і журнали програмного забезпечення безпеки. Можна додати мережеві журнали, запропоновані Дж. Джигуо та ін. [94], оскільки вони мають унікальні особливості й не можуть бути ідеально класифіковані за категоріями журналів.

Операційні системи та додатки також часто фіксують дані у вигляді журналів. Ці журнали надають користувачеві інформацію про системні події, такі як вимкнення або запуск служби, записи аудиту, запити клієнта й відповіді сервера, інформацію про обліковий запис, інформацію про використання тощо. Журнали безпеки натомість відображають підозрілі дії, результати перевірки на віруси тощо. Розвідка надає додатковий контекст для аналізу загроз.

2) АНАЛІЗ ТА ВИЯВЛЕННЯ

Виявлення атак здійснюється або автоматично, або вручну. Ручне виявлення - це виявлення інциденту через внутрішню або зовнішню особу. Тобто виявлення може здійснюватися експертами з безпеки, такими як аналітики в рамках SOC, або новачками в сфері безпеки. Прикладом ручного виявлення за допомогою новачків у сфері безпеки може бути ситуація, коли працівник отримує фішинговий лист, а потім повідомляє про це, щоб команда безпеки могла вжити відповідних заходів. Концепція інтеграції співробітників в

процес виявлення була введена як "людина як датчик безпеки" (Human-as-a-Security-Sensor) [95] і означає, що співробітники мають можливість виявляти і повідомляти про інциденти безпеки. Таким чином, навчання з підвищення обізнаності відіграє вирішальну роль. Загалом, ручне виявлення є необхідним, оскільки не всі атаки можуть бути виявлені за допомогою технологій, особливо коли мова йде про просунуті атаки.

Загалом література з питань автоматичного аналізу та виявлення загроз переважно зосереджена на конкретних методах і технологіях. Методології, що базуються на аномаліях або на поведінці, використовують нормальну поведінку системи як основу і намагаються виявити відхилення. Методи, засновані на сигнатурах або на знаннях, використовують накопичені знання про атаки і є дуже корисними для виявлення відомих атак або експлуатації відомих вразливостей. Методології, засновані на специфікаціях, зосереджені на виявленні інцидентів на основі заздалегідь визначених профілів або протоколів. Гібридні методології використовують суміш трьох описаних методологій виявлення.

Що стосується підходів до виявлення, то одним із найстаріших методів є виявлення на основі статистики, що використовує статистичні властивості і тести, такі як середнє значення, медіана або дисперсія, для виявлення відхилення між нормальною поведінкою і поведінкою, що спостерігається. Порогові метрики, приховані марковські моделі та багатовимірні моделі є прикладами статистичних підходів до виявлення вторгнень.

Підходи на основі шаблонів і правил використовують заздалегідь визначені шаблони, вивчені шаблони або правила для виявлення. Прикладом виявлення на основі правил є машини опорних векторів. Евристичні підходи, які народились від біологічних концепцій, як, наприклад, штучні нейронні мережі.

На противагу цьому, кожному класу підходів до виявлення інцидентів можна поставити у відповідність описаний в літературі підхід, при якому помітна орієнтація на підходи, засновані на статистиці та правилах. Для

покращення виявлення інцидентів незалежно від використовуваного підходу Л. Карачай та ін. [96] пропонують принцип, який дозволяє виявляти вторгнення навіть тоді, коли було використано наскрізне шифрування. М. Сміт [97] пропонує більш інтенсивно використовувати аналіз поведінки користувачів (АПК), оскільки зловживання обліковими даними є великою загрозою.

Висновки до розділу 1

У розділі 1 встановлено, що Центр забезпечення безпеки (SOC) – це організаційна одиниця, яка діє в центрі всіх операцій з безпеки і виконує функції виявлення, аналізу й реагування на загрози та інциденти кібербезпеки з використанням людей, процесів та технологій.

Огляд підходів до архітектурного проектування SOC показав, що на високому й абстрактному рівні SOC можуть бути структуровані як централізовані, розподілені або децентралізовані структури.

Зрушення від наявності одного центрального SOC до більш децентралізованої архітектури спостерігається при порівнянні більш ранніх досліджень з більш пізніми публікаціями. Основною причиною цього, як визначається, є уникнення єдиної точки відмови.

Проаналізовано концепцію PPT, яка передбачає визначення процесів для оптимізації операцій, впровадження правильної технології для підвищення ефективності роботи і наймання фахівців з потрібними навичками для управління цими процесами.

Зроблено висновок, що незалежно від операційної моделі, SOC повинен бути захищеним. Несправний SOC залишає всю решту компанії вразливою, оскільки атаки можуть поширюватися непоміченими. Тому безпеці SOC необхідно приділяти особливу увагу. Кожна операційна модель має певні переваги та недоліки, і важливо прийняти рішення заздалегідь.

Розділ 2
КОМПОНЕНТИ Й ТЕХНОЛОГІЇ SOC

2.1 Покоління SOC та його компоненти

Розуміння компонентів SOC та очікуваних послуг з часом змінилося. Це є відображенням коригування сприйняття критичності операцій із забезпечення інформаційної безпеки та захисту інформації. Ця трансформація відбувається у відповідь на мінливий ландшафт загроз безпеці, на додаток до того, що все частіше приймаються офіційні стандарти інформаційної безпеки, які вимагають створення й управління офіційною моделлю операцій з безпеки і процесами перевірки.

Шлях SOC за останні 15 років можна розбити на чотири послідовних покоління, як показано на рисунку 2.1 [41]. В ідеалі, організація, яка використовує технології четвертого покоління, такі як аналітика безпеки великих даних, повинна була б прийняти більшість послуг SOC від попередніх поколінь. Однак на практиці це не завжди так.

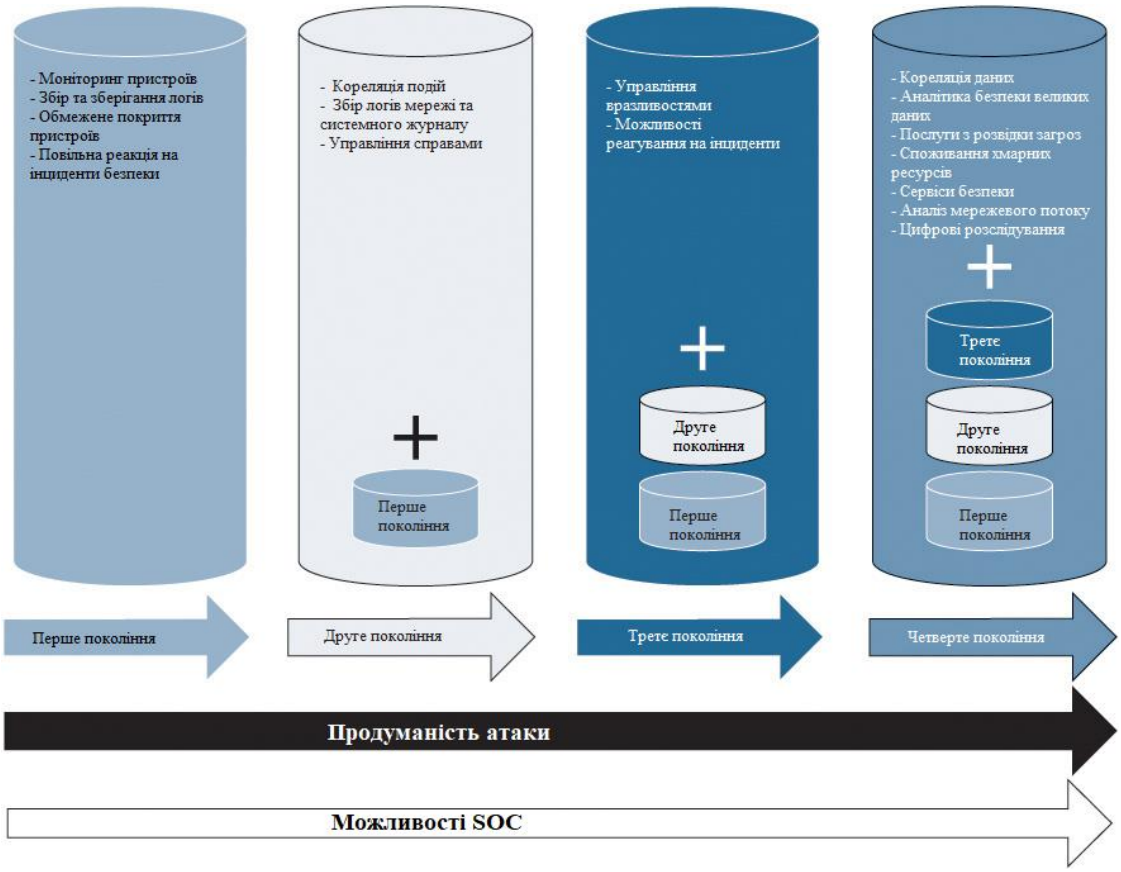

Рис 2.1 Чотири покоління SOC

Чотири покоління відображають зміни у функціональних можливостях SOC у відповідь на все більш продумані атаки. Розглянемо деталі послуг, що пропонуються в SOC кожного з поколінь.

Перше покоління SOC

У цьому поколінні більш широка команда IT-операцій надавала те, що можна вважати функціями та послугами SOC. Ця команда не обов'язково була кваліфікованою або підготовленою для роботи з подіями та інцидентами інформаційної безпеки. Операції з безпеки здійснювалися не шляхом створення формальної SOC, а в багатьох випадках окремими IT-операторами або командами, які зосереджувалися на виконанні різних завдань: моніторинг стану пристроїв та мережі, управління антивірусною безпекою в організації та збір журналів.

Збір журналів для SOC першого покоління був обмежений кількістю джерел і типів пристроїв, здатних створювати журнали, таких як брандмауери. У багатьох випадках зберігання повідомлень журналів здійснювалося локально.

В інших випадках для отримання інформації журналів, в основному у вигляді незашифрованих повідомлень syslog або простого мережевого протоколу управління (SNMP), було передбачено центральний засіб ведення журналів.

У цьому поколінні повідомлення журналів рідко аналізувалися проактивно, зазвичай до них зверталися, якщо повідомлялося про інцидент або вимагалося усунення певних несправностей. Крім того, концепція реагування на інциденти безпеки не була офіційно встановлена або оцінена. Процес виявлення, інформування й реагування на потенційні інциденти інформаційної безпеки загалом був повільним (і в багатьох випадках ситуативним).

SOC другого покоління

Це покоління, в якому почали з'являтися інструменти SIEM. Перші покоління постачальників SIEM, такі як netForensics, Network Intelligence (пізніше придбана EMC) і Cisco Security Monitoring, Analysis and Response System (MARS), обіцяли виявляти мережеві загрози, звільняючи адміністраторів від складного і в багатьох випадках нездійсненного завдання ручного аналізу величезних обсягів журнальної інформації.

Основна ідея SEM полягає в тому, щоб спочатку агрегувати лог-інформацію у вигляді подій з різних джерел, таких як операційні системи, пристрої безпеки та додатки. Потім події корелюються таким чином, щоб виявити можливі взаємозв'язки між ними, які вказують на потенційне виникнення інцидентів. Потім про інциденти повідомляється у вигляді попередження на інформаційній панелі оператору для подальшого розслідування.

Функція SEM в кінцевому підсумку була об'єднана з функцією управління інформацією про безпеку (SIM), щоб створити те, що сьогодні відомо як SIEM. Інструменти SIM були зосереджені на пошуку у великих обсягах отриманих даних журналів. Ці історичні дані можна було потім аналізувати для різних цілей, таких як проведення цифрових розслідувань або виконання низки вимог щодо відповідності, пов'язаних зі збереженням журналів та створенням звітів про відповідність.

Іншим важливим операційним аспектом, представленим в SOC другого покоління, стало управління інцидентами безпеки. Оператори SIEM можуть створювати і призначати справи для інцидентів безпеки, про які повідомляють інструменти.

SOC третього покоління

У міру того, як інструменти SIEM ставали все більш важливими, інші служби безпеки почали знаходити свій шлях до SOC. У цьому поколінні команда SOC займається завданнями, пов'язаними з управлінням вразливостями, на додаток до активної участі в формалізації та виконанні завдань, пов'язаних з реагуванням на інциденти.

Управління вразливостями відноситься до практики, в якій вразливості виявляються і підтверджуються, оцінюється їх вплив, визначаються і виконуються коригувальні заходи, а їх статус відстежується і повідомляється до моменту закриття. Це визначення подібне до того, що використовується в стандарті NIST SP 800-40 [98].

Дуже важливо, щоб етап оцінки впливу виявлених вразливостей був пов'язаний із практикою оцінки ризиків в організації. Це означає, що мова йде про весь процес управління вразливостями, а не про запуск інструментів сканування вразливостей лише проти IT-активів.

Сканування вразливостей - це діяльність, яка є частиною управління вразливостями і зазвичай виконується на етапах виявлення, підтвердження та відстеження вразливостей. Деякі комерційні продукти, такі як Qualys, nCircle та Rapid, Nexpose, еволюціонували переважно зі сканерів вразливостей до засобів автоматизації процесу управління вразливостями. Команда SOC при цьому керує процесом управління вразливостями, працюючи з іншими підрозділами, або їй доручають деякі із таких завдань.

SOC четвертого покоління

Це покоління SOC представляє ряд удосконалених служб безпеки, які намагаються протистояти новим загрозам безпеки. Першою новою концепцією є розширення обмеженої кореляції подій, яка спостерігалася в попередніх

поколіннях SIEM, до безпеки великих даних. Аналітика безпеки великих даних може бути визначена як "здатність аналізувати великі обсяги даних протягом тривалих періодів часу для виявлення загроз, а потім представляти і візуалізувати результати". Платформи великих даних зараз розгортаються для споживання даних з будь-якого джерела на високій швидкості і у великому обсязі, при цьому вони здатні виконувати складну аналітику безпеки в режимі реального часу або в автономному режимі.

Прикладом використання великих даних є поглинання обширних потоків розвідданих про атаки, які спостерігаються в усьому світі, замість того, щоб обмежувати кореляцію подій внутрішніми загрозами. Дані про атаки можуть бути даними про репутацію веб-сайтів, шкідливі джерела, об'ємні тренди для виявлення розподілених атак на відмову в обслуговуванні (DDoS) тощо.

Ще однією новою концепцією SOC четвертого покоління є збагачення даних за рахунок використання таких джерел, як геодані, дані системи доменних імен (DNS), інтеграція контролю доступу до мережі, а також служби репутації IP і доменів. Інформація мережевої телеметрії також використовується для складного моніторингу мережі і безпеки, по суті перетворюючи звичайне мережеве обладнання на порти датчиків безпеки.

Нові технології використовуються SOC для криміналістики і виявлення мережевих порушень, також відомих як рішення для виявлення порушень. Інтеграція між продуктами використовується для автоматизації усунення порушень, наприклад, продукт для виявлення вторгнень визначає загрозу і використовує технологію контролю доступу до мережі для автоматичного усунення порушень.

Таким чином, SOC четвертого покоління розширює джерела даних про загрози, виконує різні функції безпеки для боротьби з більш сучасними загрозами і автоматизує безпеку для покращення часу реагування на інциденти. Це покоління SOC також включає в себе політики для оцінки своїх можливостей як безперервного процесу з метою оптимізації та вдосконалення. Щоб краще

зрозуміти останнє покоління SOC, розглянемо характеристики ефективного SOC.

SOC відстежує дані про безпеку, що генеруються в усій IT-інфраструктурі організації, від хост-систем і додатків до мережевих і захисних пристроїв, таких як брандмауери та антивірусні рішення. Поєднуючи ряд передових інструментів і навички досвідчених фахівців з кібербезпеки, SOC виконує наступні життєво важливі функції:

– Моніторинг подій безпеки, виявлення, розслідування й сортування оповіщень.

– Управління реагуванням на інциденти безпеки, включаючи аналіз шкідливого програмного забезпечення та криміналістичні розслідування.

– Управління розвідданими про загрози.

– Управління вразливостями на основі оцінки ризиків (зокрема, визначення пріоритетності виправлень).

– Розвідка загроз.

– Управління й обслуговування пристроїв безпеки.

– Розробка даних і метрик для звітності.

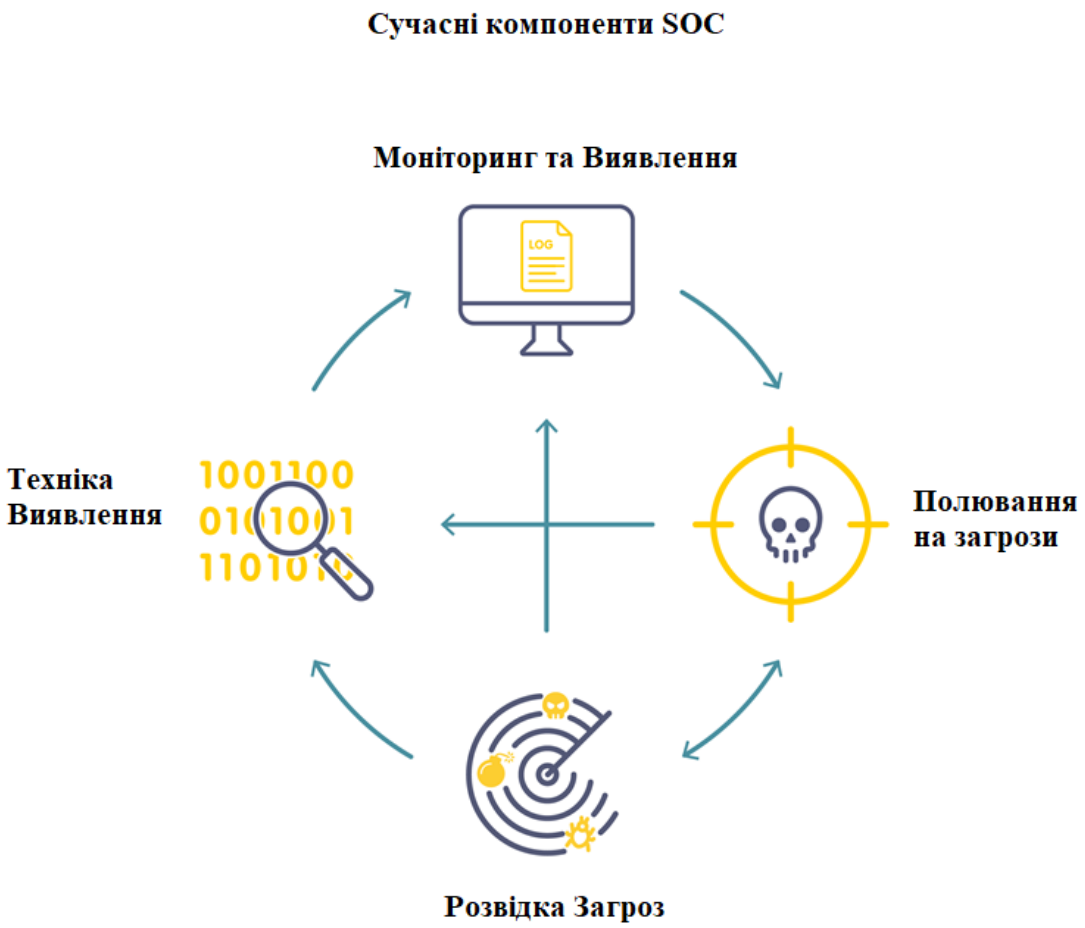

Рис 2.2 Компоненти сучасного SOC

У SOC типу hub-and-spoke передають дані до SIEM, що зазвичай складається з таких компонентів:

– **Брандмауер:** запобігає зловмисному проникненню в мережу через Інтернет шляхом блокування несанкціонованого доступу.

– **Система виявлення вторгнень (IDS) / Система запобігання вторгненням (IPS):** система виявлення вторгнень (IDS) здійснює моніторинг заданої мережі та надсилає оповіщення при виявленні зловмисної активності в мережі/системі та порушень політик. Система запобігання вторгненням (IPS) пропонує такі ж можливості моніторингу та виявлення, але може також запобігати вторгненням, коли вони відбуваються.

– **Інструмент управління, ризиків, відповідності (GRC):** забезпечує відповідність діяльності організації чинним правилам і нормам, таким як GDPR, CPAA, HIPAA, PCI DSS і т.д.

– **Інструмент виявлення та реагування на кінцеві точки (EDR):** EDR забезпечує безпеку кінцевих точок для пристроїв, підключених до мережі.

– **Система управління журналами (LMS):** централізує дані з різних кінцевих точок мережі, збираючи і зберігаючи файли журналів в одному місці.

– **Сканер вразливостей:** допомагає в управлінні вразливостями, перевіряючи мережі, комп'ютери та програми на наявність відомих вразливостей, а також виявляючи нові вразливості.

– **Тестування на проникнення:** виявляє існуючі вразливості системи, мережі й додатків, а також методи, за допомогою яких зловмисник може їх використати.

– **Інструмент безпеки додатків:** забезпечує програмні додатки повним захистом від зовнішніх загроз протягом усього життєвого циклу.

– **Інструмент виявлення активів:** здійснює моніторинг активних і неактивних мережевих активів для виявлення будь-яких невідомих вразливостей.

– **Інструмент моніторингу даних:** відстежує й аналізує дані в мережах, системах і додатках для забезпечення дотримання стандартів безпеки даних.

– **Інструмент оркестрування, автоматизації та реагування на загрози безпеці (SOAR):** використовує автоматизацію і цифрові робочі процеси для оптимізації аналізу інцидентів і процедур реагування.

– **Аналіз поведінки користувачів та організацій (UEBA):** визначає регулярні тенденції використання мережі для встановлення моделі очікуваної поведінки і виявляє аномальну поведінку, щоб виділити підозрілу активність, особливо внутрішні загрози. UEBA також використовується для зменшення кількості помилкових спрацьовувань, які виявляються.

– **Платформа розвідки загроз (TIP):** збирає й організовує дані розвідки загроз з різних джерел та форматів.

2.2 Технології SOC

Розглянемо технології, які використовуються для розробки концептуальної архітектури, що інтегрує різні технології та послуги SOC. Почнемо з представлення найбільш фундаментальної функції SOC: збору й аналізу даних.

2.2.1 Збір та аналіз даних

Перш ніж виконувати будь-який корисний аналіз, необхідно спочатку отримати відповідні дані. У контексті моніторингу безпеки, дані з різних джерел і в різних форматах можуть бути зібрані для цілей аналізу, аудиту та дотримання вимог безпеки. Дані, що представляють особливий інтерес, включають журнали подій, мережеві пакети і мережеві потоки. Іноді також може знадобитися активно досліджувати або збирати такий вміст як статичний вміст веб-сторінки або хеш-значення файлу.

Створення та захоплення журналів подій має вирішальне значення для забезпечення безпеки. Події можуть прямо чи опосередковано сприяти виявленню інцидентів безпеки. Наприклад, високопріоритетна подія, згенерована правильно налаштованою системою виявлення вторгнень, вкаже на спробу атаки. Однак, подія з високим рівнем використання каналів зв'язку, що генерується маршрутизатором, може не бути подією безпеки за визначенням, але може вказувати на інцидент безпеки, якщо співвідноситься з іншими подіями, такими як атака типу "відмова в обслуговуванні" (DoS) або сканування мережі скомпрометованим хостом.

Кожна організація використовує свій власний унікальний перелік послуг і систем, що постійно розвивається.

Основна ідея полягає не в тому, щоб моніторити все заради моніторингу, а в тому, щоб спроектувати можливості зі збору даних таким чином, щоб технічні цілі та цілі відповідності були досягнуті в тих межах, в яких застосовується моніторинг. Наприклад, залежно від топології мережі та

елементів, з яких потрібно збирати дані, можна розподілити колектори даних і централізувати інформаційну панель моніторингу таким чином, щоб було кілька точок видимості, які подаються в одне місце для моніторингу всіх подій. Іншим прикладом є порівняння вартості і віддачі від інвестицій у збір і зберігання пакетів у порівнянні з використанням NetFlow в існуючих мережевих активах для судової експертизи безпеки.

Незалежно від обраної технології і дизайну, ключовим моментом є те, що кінцевий продукт не повинен надавати занадто багато або занадто мало даних. Вважається, що багато збоїв, з якими стикається SOC, є результатом поганих практик збору даних. Це може бути викликано багатьма факторами, від "сліпих зон", заснованих на способах збору даних, до кореляції неправильних даних, таких як виявлення вразливих систем, які не існують в мережі. Іноді відповідні інструменти увімкнені, але їхні годинники не синхронізовані належним чином, що спричиняє плутанину під час пошуку й усунення несправностей.

У принципі, тип даних, які потрібно зібрати, і джерело даних, визначають механізм збору, який потрібно розгорнути. Наприклад, більшість мережевих пристроїв корпоративного рівня за замовчуванням підтримують протокол syslog з метою віддаленої реєстрації подій, тоді як інші системи вимагають встановлення агента для виконання аналогічної функції.

Розуміння середовища та визначення елементів, з яких отримуються корисні дані, є початковими кроками в процесі створення потенціалу для збору даних. На рисунку 2.3 показані концептуальні кроки, які представляють цей процес. Дані можуть зберігатися у плоскому файлі, реляційній базі даних або в розподіленій файловій системі, такій як Hadoop Distributed File System (HDFS). На етапі аналізу можуть використовуватися різні методи, такі як виявлення аномалій на основі статистики, розгортання правил кореляції подій або застосування машинного навчання на даних. Починаючи з етапу проектування SOC, слід формалізувати та задокументувати всі процеси та процедури, включаючи вибір технології.

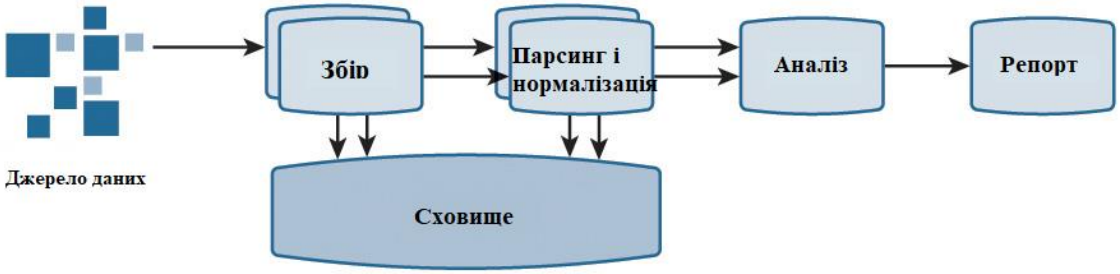

Рис 2.3 Базовий робочий процес управління даними

Після того, як дані зібрані, доцільно вирішити, чи зберігати їх, чи аналізувати, чи робити і те, і інше. Хоча зберігання даних в оригінальному форматі може бути корисним для цілей цифрових розслідувань, позасмугової аналітики безпеки і виконання вимог відповідності, важливо відзначити, що дані на цьому етапі вважаються неструктурованими, тобто точна структура все ще невідома або не була підтверджена.

Щоб зрозуміти структуру даних, необхідний синтаксичний аналіз для вилучення різних полів події. Для того, щоб дані могли бути корисними для організації, потрібно при зберіганні оригінальних даних, незалежно від форми, мати сховище, яке може їх прийняти, та інструменти, які можуть пізніше запитувати, отримувати й аналізувати їх. Розглянемо різні типи джерел даних.

Джерела даних

Повідомлення журналів вважаються найбільш корисним типом даних для отримання, оскільки вони підсумовують дію або діяльність, яка відбулася в системі, і містять інформацію, пов'язану з відповідною подією. Залежно від середовища, розглядають можливість збору повідомлень журналів з різних форм продуктів безпеки, мережевих і прикладних продуктів. Приклади фізичних і віртуальних пристроїв, які можуть надавати цінні повідомлення журналювання, включають:

– елементи безпеки, такі як брандмауери, системи виявлення та запобігання вторгненням, антивірусні рішення, веб-проксі-сервери та інструменти аналізу шкідливого програмного забезпечення;

– мережеві елементи, такі як маршрутизатори, комутатори, бездротові точки доступу та контролери;

– операційні системи, такі як різні випуски Microsoft Windows, UNIX, Linux і OS X;

– платформи віртуалізації, такі як Virtual-Box, віртуальна машина на основі ядра (KVM), Microsoft Hyper-V і VMware ESX;

– додатки, такі як веб-сервери, сервери системи доменних імен (DNS), шлюзи електронної пошти, білінгові програми, голосові шлюзи та інструменти управління мобільними пристроями (MDM) ;

– бази даних;

– елементи фізичної безпеки, такі як камери спостереження, пристрої контролю доступу до дверей і системи відстеження;

– системи, що використовуються в технологічних і керуючих мережах, такі як диспетчерський контроль і збір даних (SCADA) і розподілені системи управління (DCS).

На додаток до реєстрації повідомлень, може знадобитися збирати, зберігати і, можливо, аналізувати інші форми даних. Приклади включають збір мережевих пакетів, NetFlow і вміст файлів, таких як конфігураційні файли, хеш-значення і HTML-файли. Кожне з цих джерел даних має унікальну цінність, однак має свої власні супутні витрати, які слід враховувати, перш ніж інвестувати в методи збору та аналізу даних.

Наприклад, зберігання мережевих пакетів зазвичай має більш високу вартість збору і зберігання, але може забезпечити більш детальну інформацію про події, ніж NetFlow. Деякі галузеві норми вимагають зберігання даних на рівні пакетів, що робить захоплення пакетів обов'язковою функцією. Для клієнтів, які шукають аналогічні криміналістичні дані за нижчою ціною, збір NetFlow може бути менш витратною альтернативою, в залежності від таких факторів, як існуюче обладнання, дизайн мережі тощо.

Збір даних

Щоб краще зрозуміти вартість і цінність збору даних, розглянемо докладніше, як можна збирати дані. Після того, як прийняте рішення про те, які

дані необхідно зібрати, треба обрати спосіб їх збору. Для збору даних з різних джерел використовують різні протоколи та механізми. Залежно від того, що підтримує джерело даних, дані можуть бути витягнуті з джерела до колектора або підштовхнуті джерелом до колектора.

Важливо підкреслити необхідність синхронізації часу при зборі даних. Збирання логів без належного позначення часу може спричинити плутанину при оцінці подій і спотворити результати. Найбільш поширеним способом забезпечення синхронізації часу в мережі є використання центрального сервера синхронізації з використанням протоколу мережевого часу (NTP). Найкраща практика полягає в тому, щоб всі служби і системи, включаючи ті, які генерують, збирають і аналізують дані, синхронізували свій годинник з довіреним центральним сервером часу.

Протокол Syslog

Протокол syslog, як визначено в IETF RFC 5424 [99], забезпечує формат повідомлень, який дозволяє надавати специфічні для постачальника розширення в структурованому вигляді, на додаток до передачі повідомлень про події від клієнта syslog (оригінатора) до одержувача syslog (реле або колектора). Протокол syslog підтримує три ролі:

1. Оригінатор: генерує вміст syslog для передачі в повідомленні.

2. Колектор: збирає повідомлення syslog.

3. Реле: пересилає повідомлення, приймаючи їх від оригінаторів або інших ретрансляторів і відправляючи колекторам або іншим ретрансляторам.

На рисунку 2.4 показані різні шляхи зв'язку між трьома ролями syslog, відзначаючи, що клієнт syslog може бути сконфігурований з декількома реле syslog і колекторами.

Реалізації syslog використовують для пересилання подій протокол User Datagram Protocol (UDP) з номером порту 514. Також можлива реалізація протоколу через надійний транспортний протокол, наприклад, протокол управління передачею (TCP), відповідно до IETF RFC 3195 [100].

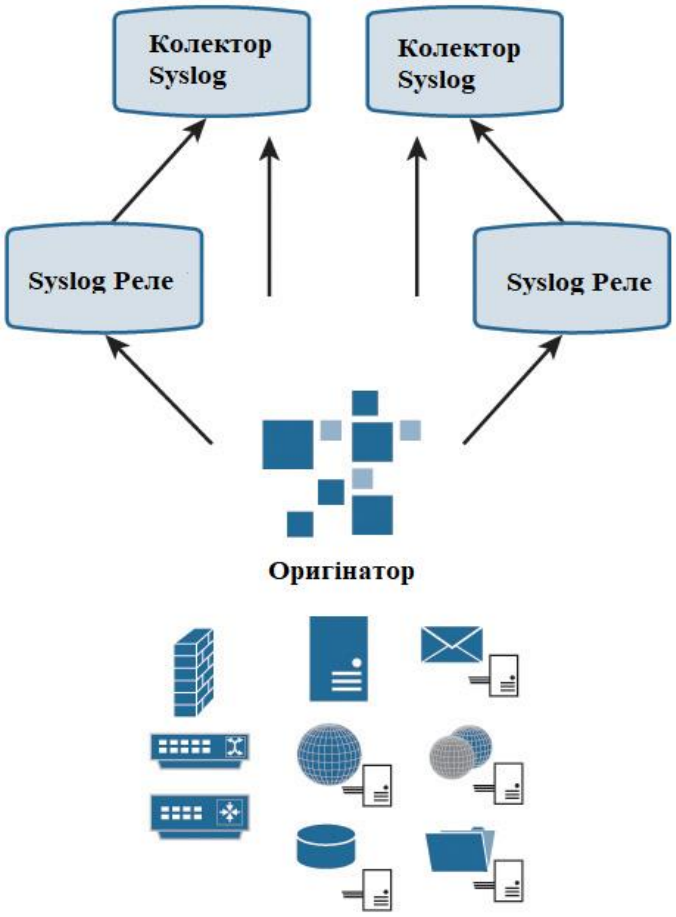

Рис 2.4 Дизайн збірки Syslog

Syslog за замовчуванням не забезпечує захист безпеки з точки зору конфіденційності, цілісності та автентичності. Однак ці функції безпеки можуть бути надані шляхом запуску syslog через захищений мережевий протокол, такий як Transport Layer Security (TLS) і Datagram Transport Layer Security (DTLS), як описано в RFC 5425 і 6012, відповідно.

Ці підходи можуть бути більш безпечними, але, як правило, за рахунок додаткових накладних витрат і ризику того, що деякі системи можуть не підтримувати ці протоколи. Рекомендується переглянути посібник з конфігурації продукту для перевірки можливого впливу на продуктивність і можливості перед впровадженням певних функцій.

2.2.2 Управління вразливостями

Управління вразливостями - це процес виявлення, підтвердження, класифікації, визначення пріоритетів, призначення, усунення та відстеження

вразливостей. Управління вразливостями не варто плутати зі скануванням вразливостей, оскільки останнє є частиною процесу управління вразливостями, з акцентом на етапі виявлення. Також важливо розуміти, що управління ризиками має справу з усіма пов'язаними з ними ризиками, в той час як управління вразливостями спрямоване на технології.

Вразливості можуть сприйматися як слабкі місця в роботі з персоналом, процесах і технологіях. Управління вразливостями в контексті SOC фокусується на відомих технічних слабкостях, закладених у програмному та апаратному забезпеченні. Варто підкреслити, що існування технічної вразливості може бути результатом слабких місць в персоналі та процесах, таких як відсутність належного процесу забезпечення якості програмного забезпечення.

Організації з розвиненою програмою безпеки інтегрують тісно пов'язані практики управління вразливостями та управління ризиками. Іноді цього можна досягти за допомогою інструментів, які можуть автоматизувати цю інтеграцію.

Найбільш важливим елементом управління вразливостями є більш швидкий захист вразливого активу до того, як вразливість буде використана. Це досягається шляхом постійного застосування низки кроків для виявлення, оцінки та усунення ризику, пов'язаного з вразливістю.

Оголошення про вразливості

Одним з найпоширеніших методів виявлення вразливості системи є моніторинг оголошень про вразливості в продуктах, що використовуються в компанії. Розглянемо докладніше, як ця інформація публікується.

Вразливості у відкритому та закритому коді оголошуються щодня. Ідентифікатори пов'язані з оголошеннями про вразливості, щоб на них можна було посилатися в глобальному масштабі, забезпечуючи інтероперабельність. Одним із загальновживаних стандартів для посилання на вразливості є Common Vulnerabilities and Exposures (CVE), який є словником загальновідомих вразливостей та загроз інформаційній безпеці, що знаходяться у відкритому доступі. Загальні ідентифікатори CVE полегшують обмін даними між окремими

базами даних та інструментами мережевої безпеки. Якщо звіт одного з ваших інструментів безпеки містить ідентифікатори CVE, адміністратор може швидко і точно отримати доступ і виправити інформацію в одній або декількох окремих CVE-сумісних базах даних для усунення проблеми. Кожен CVE ідентифікатор містить наступне:

– номер CVE ідентифікатора (CVE-ID) у вигляді префікса CVE + рік + довільні цифри;

– короткий опис уразливості або вразливості в системі безпеки;

– інші супутні матеріали.

Список продуктів, що використовують CVE для позначення вразливостей, підтримується MITRE [102].

Ідентифікатор CVE не надає контекст вразливості, такий як складність експлуатації та потенційний вплив на конфіденційність, цілісність і доступність. Ці дані надаються системою оцінки вразливостей (CVSS), яка підтримується NIST. Згідно з NIST, CVSS визначає вразливість як помилку, недолік, слабкість або вразливість програми, системного пристрою або служби, яка може призвести до порушення конфіденційності, цілісності або доступності [41].

CVSS - це кількісна модель, яка забезпечує повторюваність точних вимірювань, дозволяючи користувачам бачити основні характеристики вразливості, які були використані для отримання балів. Таким чином, CVSS добре підходить як стандартна система вимірювання для галузей, організацій та урядів, які потребують точних і послідовних оцінок впливу вразливостей.

2.2.3 Розвідка загроз

Розуміння ринком поняття "розвідка загроз" еволюціонує. За визначенням Гартнер, "розвідка загроз - це засновані на фактах знання, включаючи контекст, механізми, індикатори, наслідки та практичні поради, про існуючу або нову

загрозу або небезпеку для активів, які можна використовувати для прийняття рішень щодо реагування суб'єкта на цю загрозу або небезпеку".

Forrester визначає розвідку загроз як "детальну інформацію про мотивацію, наміри і можливості внутрішніх і зовнішніх суб'єктів загроз. Розвідка загроз включає конкретні відомості про тактику, методи і процедури цих суб’єктів. Основною метою розвідки загроз є надання інформації для прийняття бізнес-рішень щодо ризиків та наслідків, пов'язаних із загрозами" [41].

Перекладаючи ці визначення на загальну мову, можна сказати, що розвідка загроз - це засновані на фактах знання про можливості внутрішніх і зовнішніх суб'єктів загроз. Використання такого типу даних може принести користь SOC шляхом розширення обізнаності про безпеку за межами внутрішньої мережі, споживання розвідданих з інших джерел в Інтернеті, пов'язаних з можливими загрозами для організації. Так, отримавши інформацію про загрозу, яка вплинула на кілька організацій, компанія може заздалегідь до неї підготуватися, а не тільки реагувати, коли ця загроза буде виявлена в корпоративній мережі.

Forrester визначає п'ятиступеневий цикл розвідки загроз для оцінки джерел розвідки загроз: планування і керівництво, збір, обробка, аналіз і виробництво, розповсюдження.

У багатьох випадках клієнт будете споживачем одного або декількох каналів розвідки. Серед платформ розвідки загроз, які слід розглянути, можна назвати наступні:

– **Cyber Squad ThreatConnect:** Локальне, приватне або загальнодоступне хмарне рішення, що пропонує збір даних про загрози, аналіз, співпрацю та експертизу на одній платформі.

– **BAE Detica CyberReveal:** Продукт для моніторингу, аналітики, розслідування й реагування на різноманітні загрози. CyberReveal об'єднує надбання BAE Systems Detica в галузі мережевої розвідки, аналізу великих

даних і досліджень кіберзагроз. CyberReveal складається з трьох основних компонентів: платформа, аналітика і дослідник.

– **Lockheed Martin Palisade:** Підтримує комплексний збір, аналіз, співпрацю та експертизу загроз на єдиній платформі.

– **MITRE CRITs:** Спільні дослідження загроз (CRITs) - це джерело даних про загрози з відкритим вихідним кодом.

Крім того, розробляється низка стандартів схем розповсюдження розвідувальної інформації про загрози, серед яких:

– **Structured Threat Information eXpression (STIX):** Експрес-мова, призначена для обміну інформацією про кібератаки. Деталі STIX можуть містити такі дані, як IP-адреси командно-контрольних серверів (CnC), хеші шкідливого програмного забезпечення тощо.

– **Open Indicators Of Compromise (OpenIOC):** Відкрита платформа для обміну розвідданими про загрози в машинозчитуваному форматі.

– **Cyber Observable eXpression (CybOX):** Безкоштовна стандартизована схема для специфікації, захоплення, опису та передачі подій, що мають властивості стану, які можна спостерігати в оперативній області.

Транспортні механізми, такі як Trusted Automated eXchange of Indicator Information (TAXII), використовуються для обміну інформацією про кіберзагрози, представленою раніше розглянутими схемами.

Кожна компанія повинна визначити, яка розвідувальна інформація про загрози найкраще підходить для саме для її операцій із забезпечення безпеки. Критерії оцінки можуть включати переваги, які вона приносить, плани компанії та можливості інтеграції розвідки загроз з іншими технологіями і процесами SOC, включаючи автоматизацію цієї інтеграції. Крім того, важливо зазначити, що існує багато джерел з відкритим вихідним кодом і джерел, не пов'язаних з безпекою, які також можуть бути використані для розвідки загроз. Деякі приклади - джерела соціальних мереж, форуми, блоги, веб-сайти постачальників тощо.

Забезпечення відповідності

Моніторинг відповідності корпоративних систем еталонним шаблонам конфігурації або стандартним збіркам систем дає можливість виявити зміни та існуючі проблеми конфігурації, які можуть призвести до можливого порушення. Іноді ці проблеми не можуть бути помічені звичайними інструментами безпеки, такими як сканери вразливостей, до тих пір, поки проблема конфігурації не буде використана, а це не найкращий час для виявлення проблеми. Існують також випадки, коли у вас може бути політика, яка змушує вас слідувати деяким належним практикам безпеки, таким як безперервна оцінка за критеріями, встановленими Центром інтернет-безпеки (CIS) або відповідність стандарту PCI DSS 2.0 [42].

Багато сучасних інструментів для сканування вразливостей, таких як Qualys, Nessus і Nexpose, включають в себе модуль відповідності, який дозволяє їм віддалено входити в систему, збирати її конфігурацію, а потім аналізувати її в порівнянні з еталонними показниками. Можливо розробити власні програми або скрипти, які можуть виконувати ту саму функцію.

Автоматизація процесу відповідності системи вимогам, а потім його зв'язок з практиками управління ризиками та реагування на інциденти є ключовими кроками в будь-якій успішній операції з забезпечення безпеки. Прикладом включення цього в практику є включення відповідності системи як частини етапів оцінки ризиків і оцінки вразливостей моделі управління вразливостями SANS, представленої вище.

Реєстрація заявок та управління кейсами

Очікується, що команда SOC буде відстежувати потенційні інциденти, про які повідомляють інструменти або люди. Для забезпечення належного управління інцидентом необхідно створити, призначити та відстежувати його до закриття. Ця діяльність повинна бути підкріплена відповідними інструментами, повноваженнями й інтеграцією з процесами реагування на інциденти та управління кейсами.

Ключовим моментом, який слід враховувати, є те, що для усунення деяких подій можуть знадобитися ресурси поза межами аналітиків SOC для бізнес або іншої технічної підтримки. Ось чому розподіл обов'язків, які підтримуються відповідним органом, є критично важливим для успіху управління інцидентами.

Матриця "Відповідальність, підзвітність, консультації та інформованість" (RACI) може бути використана як модель для визначення ролей та обов'язків. На рисунку 2.5 наведено приклад матриці RACI, де R = відповідальний, A = підзвітний, C = консультувати, I = інформувати.

Функція	Сронсор проекту	Бізнес аналітик	Проет менеджер	Розробник програмного забезпечення
Ініціювати проект	C		AR	
Скласти план проекту	I	C	AR	C
Зібрати вимоги до користувачів	I	R	A	I
Розробити технічні вимоги	I	R	A	I
Розробка програмних засобів	I	C	A	R
Тестове програмне забезпечення	I	R	A	C
Розгортання програмного забезпечення	C	R	A	C

Рис 2.5 Приклад матриці RACI

Типові кроки для побудови матриці RACI є наступними:

1. Визначити всі процеси або види діяльності, відомі як функції, у лівій частині матриці.

2. Перерахувати всі ролі у верхній частині матриці.

3. Створити значення для посилань, такі як AR, C, I та R, які будуть призначені.

4. Переконатися, що кожен процес має R і що є тільки один R, щоб уникнути конфліктів. Якщо має бути більше одного R, розбийте функцію на частини, поки на кожну функцію не залишиться тільки один R.

Коли залучено кілька команд, як, наприклад, у випадку з матрицею RACI, співпраця між командами стає критично важливою для виконання місії.

Висновки до розділу 2

У розділі 2 проаналізовано чотири покоління SOC, які відображають зміни у функціональних можливостях SOC у відповідь на все більш продумані атаки. Встановлено, що сучасний SOC останнього покоління представляє ряд удосконалених служб безпеки, які виконують широкий перелік важливих функцій: моніторинг подій безпеки; управління реагуванням на інциденти безпеки; управління розвідданими про загрози; управління вразливостями; розвідка загроз; розробка даних і метрик для звітності тощо.

Розглянуто технології, які використовуються для розробки концептуальної архітектури SOC: збору й аналізу даних, управління вразливостями, розвідки загроз. У результаті аналізу технологій збору й аналізу даних зроблено висновок, що повідомлення журналів вважаються найбільш корисним типом даних, оскільки вони підсумовують дію або діяльність, яка відбулася в системі, і містять інформацію, пов'язану з відповідною подією. Також розглянуто протокол syslog та проаналізовано його структуру.

Виявлено, що технології з управління вразливостями забезпечують виконання завдань із виявлення, підтвердження, класифікації, визначення пріоритетів, призначення, усунення та відстеження вразливостей. Технології розвідки загроз розроблені для збору інформації про можливості внутрішніх і зовнішніх суб'єктів загроз. До найбільш затребуваних платформ розвідки загроз відносять Cyber Squad ThreatConnect, BAE Detica CyberReveal, Lockheed Martin Palisade, MITRE CRITs, Structured Threat Information eXpression (STIX) та інші.

Розділ 3
РЕКОМЕНДАЦІЇ ЩОДО РОЗРОБКИ І ВПРОВАДЖЕННЯ SOC

3.1 Етап планування

Створення можливостей SOC вимагає ретельного планування. Етап планування допомагає визначити та формалізувати цілі, які виправдовують наявність SOC, а також розробити карту можливостей, яку можна використовувати для відстеження прогресу у досягненні цих заздалегідь визначених цілей. Перш ніж приступити до планування, необхідно оцінити існуючу SOC або все, що буде використовуватися для SOC, щоб зрозуміти поточні можливості персоналу, процесів і технологій. Можна порівняти цю існуючу базову лінію середовища з цілями для бажаної SOC, щоб встановити рівень зусиль, необхідних для досягнення цих майбутніх цілей.

Розглянемо методологію визначення вимог до SOC та оцінки операційних можливостей безпеки відповідно до цих вимог. Результати оцінки допоможуть визначити стратегію SOC і сформулювати допоміжну карту можливостей.

Методологія оцінки

Оцінка можливостей – це перший крок до розуміння того, як розробити нову або вдосконалити існуючу операцію SOC. Результати цієї оцінки використовуються як фундамент, на якому будуються інші розділи, незалежно від того, чи розробляється новий або модифікується існуючий SOC. Методологія оцінки вимог та можливостей SOC повинна бути актуальною, задокументованою, посилатися на джерела, повторюватися, контролюватися та постійно вдосконалюватися відповідно до моделей зрілості. Важливо розглядати це як безперервну програму, щоб SOC могла адаптуватися до змін у бізнесі, технологіях та загрозах.

Методологія оцінки включає наступні кроки:

– Крок 1. Визначення бізнес-цілей та IT-цілей SOC.

– Крок 2. Визначення спроможностей, які оцінюють на основі цілей SOC.

– Крок 3. Збір інформації, пов'язаної з людьми, процесами та технологічними можливостями.

– Крок 4. Аналіз зібраної інформації та присвоєння рівнів зрілості оцінюваним можливостям.

– Крок 5. Представлення, обговорення та формалізація результатів.

Основна ідея полягає в тому, щоб дотримуватися процесу, в якому збирається, документується, перевіряється та оновлюється інформація з метою отримання результату, який використовується для розуміння поточного стану SOC. Методологія оцінювання SOC розглядає заходи, які необхідно здійснити, та сфери, які необхідно оцінити, не нехтуючи при цьому важливістю використання інструментів, які можуть автоматизувати завдання зі збору, зберігання та відстеження інформації.

Перші два кроки методології оцінки спрямовані на розуміння того, що є важливим для бізнесу. Це необхідно перед тим, як аудитор зможе зібрати інформацію, що має відношення до організації. Крок 3 розпочинає загальний збір інформації, яка буде використана разом з інформацією, отриманою на попередніх кроках, для аналізу рівня зрілості процесів SOC. Заключним кроком є звітування про результати оцінки, які потім використовуються як основа для майбутніх розробок SOC.

Багато кроків передбачають збір інформації, яка може бути отримана шляхом проведення інтерв'ю, запиту документів або простого спостереження за тим, як здійснюється діяльність. Зібрана інформація може мати різне представлення, що пов'язано з рівнем її достовірності. Важливо, щоб відокремлювали особисті думки від фактів, запитуючи підтверджуючі докази, коли це можливо. Також потрібно перевіряти інформацію, отриману з різних джерел. Відповіді на деякі з питань оцінювання можуть бути недоступними, тому в деяких випадках доведеться сприяти обговоренню між членами команди для досягнення поступок. Загалом, найкраща практика полягає в тому, щоб

зібрати якомога більше даних, які допоможуть підтвердити результати, що потрапляють до остаточного звіту.

Стратегія SOC

Результати оцінки SOC, повинні дати чітке уявлення про цілі корпоративного центру безпеки та поточні можливості компанії у сфері безпеки.

Першим кроком у розробці SOC є формалізація стратегії.

Елементи стратегії

Формалізація стратегії SOC та відстеження її прогресу є ключовими практиками для досягнення або розширення програми належного врядування. Стратегія SOC ґрунтується на результатах оцінки спроможностей, і спрямована на формалізацію таких аспектів SOC:

- формулювання місії;
- стратегічні цілі;
- сфера діяльності;
- модель функціонування;
- послуги;
- план розвитку можливостей;
- ключові показники ефективності (KPI) та метрики.

У документі про стратегію SOC з посиланням на звіт про оцінку SOC та інші документи мають бути зафіксовані такі теми як: стратегія організації, стратегія IT-відділу та, можливо, різні політики безпеки високого рівня.

Як правило, розробкою стратегії SOC керує старший архітектор безпеки або еквівалентна посадова особа. Розробка стратегії SOC - це колективна і спільна робота, в якій беруть участь кілька осіб, що приймають рішення, з різних команд, кожна з яких має свої власні вимоги, очікування і рівень впливу.

Зазвичай участь у формуванні стратегічного документа беруть такі посадові особи:

Керівник стратегії SOC: Це керівник, який очолює зусилля з розробки стратегії і здійснює координацію з іншими учасниками для збору інформації та забезпечення зв'язку під час обговорень. У деяких випадках ця роль передається зовнішньому досвідченому консультанту з питань SOC, якщо внутрішні ресурси з відповідним набором навичок не доступні.

Керівники, відповідальні за прийняття рішень щодо стратегії SOC: Цю роль, зазвичай, виконують IT-директор, директор з інформаційної безпеки та виконавчий спонсор SOC. Залежно від організації, генеральний директор може брати активну участь у визначенні стратегії SOC, однак часто виконавчий спонсор SOC відіграє головну роль у формуванні стратегії SOC.

Посадові особи, що впливають на стратегію SOC: Це, зазвичай, керівники IT-підрозділів, бізнес-підрозділів, відділу навчання, відділу кадрів та інших підрозділів, на які впливає SOC. Типові IT-підрозділи, які впливають на стратегію SOC, включають відділи, які займаються інформаційною безпекою (infosec); плануванням та інжинірингом безпеки, мереж і систем; операціями безпеки, мереж і систем; управлінням ризиками безпеки; управлінням проектами.

Місія SOC. Формулювання місії має узгоджуватися з бізнес-баченням та стратегією організації, а також з департаментом, якому в кінцевому підсумку буде підпорядковуватися SOC. Визначаючи місію, необхідно чітко визначити: сферу діяльності та ролі SOC; підрозділ, відповідальний за створення, функціонування та підтримку програми SOC; виконавчого спонсора SOC, який затверджує і підписує заяву про місію.

Наведемо приклад формулювання місії SOC: SOC контролює загальний стан безпеки IT-мережі, реагує та відстежує інциденти інформаційної безпеки з метою підтримання загального стану безпеки. Функції виконуються цілодобово для підтримки операційної моделі організації.

3.2 Етап проектування

3.2.1 Інфраструктура SOC

Доступ до послуг SOC повинен бути безпечним і надійним. Багато систем, що використовуються SOC, містять конфіденційну інформацію, яка може негативно вплинути на організацію, якщо вона стане відомою. Наприклад, інструменти моніторингу мережі та управління вразливостями можуть виявити слабкі місця, які зловмисник може використати для проникнення в організацію і, можливо, навіть для того, щоб уникнути виявлення. Захист даних також є вимогою багатьох нормативних документів, які включають процеси забезпечення безпеки послуг, пов'язаних з SOC. Невиконання таких вимог може мати негативні юридичні та фінансові наслідки для бізнесу.

Розглянемо фактори, які впливають на проектування інфраструктури SOC. Важливими моментами, які слід враховувати, є сфера застосування SOC, модель роботи, графік створення SOC та послуги, що надаються SOC. Деякі сфери інфраструктури, які повинні бути розглянуті, включають тип об'єкта, мережу, безпеку, обчислювальне сховище, спільну роботу, тікетування та вимоги до управління справами.

Міркування щодо проектування

Під час проектування інфраструктури SOC архітектор SOC приймає рішення, які підтримують дорожню карту SOC та узгоджуються з іншими пов'язаними програмами та проектами. Першим кроком після визначення критеріїв для SOC може бути розмова з постачальниками для кращого розуміння наявних технологій та з'ясування очікуваних витрат, необхідних для досягнення цілей SOC. Рекомендується провести розмови з постачальниками, які вже надають обладнання для організації. Це допоможе організації скористатися перевагами тієї ж моделі підтримки, а в деяких випадках і того ж контракту на підтримку.

Перш ніж оцінювати технологію, необхідно перевірити всі вимоги до обладнання та підключення. У деяких випадках продукти можуть включати запатентовані компоненти або вимагати спеціальної конфігурації мережі або

живлення, які можуть бути недоступні або важкодоступні. Варто впевнитися, що планування потужностей виконано та задокументовано на основі придбання нової технології. Планування потужностей не повинно призводити до надмірного збільшення вимог, а скоріше узгоджувати вибір дизайну та технології з дорожньою картою SOC. Планування потужностей має також враховувати очікуване зростання, працюючи в рамках виділеного бюджету. Важливо пам'ятати, що технології постійно розвиваються, тому обов'язковими є консультації з постачальниками, особливо в тих сферах, які мають безпосередній вплив на рішення щодо проектування інфраструктури SOC.

Варто переконатися, що команди SOC залучають інші бізнес-підрозділи, програми та проектні команди на ранніх етапах циклу планування й оцінки, коли це можливо. Наприклад, архітектор SOC має співпрацювати з мережевими, системними командами та командами центрів обробки даних, щоб приймати кращі проектні рішення щодо того, де і як підключати компоненти інфраструктури SOC.

На багато з цих технологічних проектних рішень буде впливати той факт, чи компанія розробляє власний SOC, чи використовує віртуальні послуги SOC. Далі ми розглянемо, як модель роботи SOC може вплинути на його дизайн.

Модель роботи

Модель роботи значно впливає на інфраструктуру, необхідну для надання послуг SOC. Наприклад, аутсорсинг послуг SOC, як правило, мінімізує капітальні інвестиції, скорочує час розгортання послуг і потенційно дозволяє досягти більш високого рівня зрілості надання послуг за більш короткий період часу. Більшість розгортань, які передають послуги SOC на аутсорсинг, вимагають мінімального обладнання та програмного забезпечення на місці, яке зазвичай використовується для збору даних та оцінки вразливостей. Решта сервісів аналітичного порталу, як правило, знаходяться в офісі постачальника послуг. Ось деякі питання, на які слід відповісти, що стосуються проектування інфраструктури SOC при розгляді віртуальних послуг SOC:

– Яку пропускну здатність необхідно забезпечити для зв'язку між компанією та постачальником послуг SOC?

– Скільки фізичних або віртуальних каналів зв'язку слід забезпечити для підключення до постачальника послуг SOC, і які засоби захисту даних слід впровадити для захисту даних під час передачі?

– Де слід розмістити пристрої, що надаються постачальником послуг SOC, та які привілеї віддаленого доступу вони повинні мати?

– Як організація повинна інтегрувати пропозицію керованих послуг з внутрішніми системами продажу квитків?

– Де будуть встановлені компоненти постачальника керованих послуг?

– Чи потрібно буде надавати послуги віддаленого доступу, щоб дозволити постачальнику послуг керувати компонентами на місці?

Внутрішній макет SOC

Типове планування SOC складається з таких зон:

– **Перший поверх SOC (також відомий як операційний зал):** Це зона, яку займають аналітики SOC для виконання своїх повсякденних завдань, включаючи моніторинг інформаційних панелей SOC, роботу з вхідними випадками інцидентів, аналіз та розслідування інцидентів безпеки, а також виконання інших адміністративних завдань. Планування приміщення має забезпечувати всім аналітикам SOC безперешкодний огляд відеостіни SOC, на яку проектуються або виводяться різні інформаційні панелі. Кількість аналітичних консолей, а також тип і розташування відеостіни визначають розмір і габарити підлоги. Важливо не допустити переповненості поверху, що може негативно вплинути на робочу атмосферу в SOC та ускладнити комунікацію між аналітиками.

– **Оперативний штаб (або ситуаційна кімната):** Кімната, яка зазвичай обладнана засобами для проведення конференцій і, можливо, відеоконференцій, що дозволяє залучати віддалених учасників. Кімната використовується

командою SOC для проведення регулярних зустрічей, а також управління ситуацією під час великих або серйозних інцидентів безпеки.

– **Кабінети керівника та супервайзерів SOC:** Керівник і супервайзери SOC здійснюють нагляд за його роботою та загальним процесом управління інцидентами. Рекомендується, щоб їхні кабінети були розташовані в приміщенні SOC і були відокремлені скляними вікнами, щоб вони могли бачити підлогу SOC та відеостіну.

– **Комп'ютерна кімната:** Може виникнути потреба у виділенні комп'ютерної кімнати для розміщення обладнання SOC, якщо воно не може бути безпечно розміщене в інших місцях, таких як центр обробки даних або близька комп'ютерна/комунікаційна кімната. Якщо необхідна комп'ютерна кімната для SOC, слід розглянути питання контролю навколишнього середовища, щоб гарантувати, що опалення, електропостачання, кондиціонування повітря та інші вимоги належним чином забезпечені відповідно до стандартів організації.

На етапі проектування потрібно тісно співпрацювати з відділом експлуатації приміщень або із зовнішнім проектувальником приміщень SOC для розробки схем розташування SOC. Ці схеми повинні формалізувати різні особливості планування SOC, про які йшлося вище, а також інші деталі, такі як розетки, мережеві та телефонні точки тощо.

Активна інфраструктура

Активна інфраструктура відноситься до базового IT обладнання та програмного забезпечення, яке забезпечує роботу операційної системи, мережі, безпеку, обчислення, зберігання, співпрацю й управління справами, необхідними для розміщення додатків SOC, таких як збір та аналіз даних, управління вразливостями тощо.

Основною перевагою відокремлення інфраструктури SOC є захист систем та інформації SOC від інцидентів, що впливають на різні елементи, які контролюються SOC. Рівень ізоляції базується на критичності SOC для

організації та ризиками, пов'язаними з її невиконанням. Наприклад, розглянемо організацію, яка розміщує додатки SOC у віртуальній локальній мережі (VLAN), що знаходиться на мережевому комутаторі, який також з'єднує користувачів і загальні сервери. Ризик такого підходу може полягати в тому, що мережевий адміністратор допустить помилку в конфігурації комутатора, яка дозволить неконтрольований доступ до додатків SOC. Це може зробити ці додатки вразливими до джерел загроз, яких можна було б уникнути, якби послуги SOC надавалися їх власними комутаторами.

Важливо не тільки правильно спланувати сегментацію мережевих компонентів SOC, а й визначити рівень ізоляції. У деяких випадках повна ізоляція SOC від решти мережі може бути недоцільною або навіть неможливою. Найкращою практикою є повторне використання існуючих інфраструктурних послуг для ситуацій, пов'язаних з низьким рівнем безпеки, одночасно інвестуючи в сегментацію послуг, які не повинні переглядатися учасниками за межами SOC.

Доступ до систем

Анклав SOC буде підключений до внутрішньосмугової або позасмугової мережі з прямим або опосередкованим доступом до систем, що контролюються SOC. Рекомендується здійснювати моніторинг пристроїв за допомогою позасмугової мережі, що забезпечує безпечний доступ, на який не впливає внутрішньосмуговий трафік, особливо в разі атаки. Сьогодні більшість пристроїв корпоративного рівня забезпечені одним або декількома портами управління, які можуть бути підключені до логічної або фізичної позасмугової мережі управління. Доступ до цієї мережі управління повинен бути доступний тільки авторизованим суб'єктам, таким як члени і пристрої NOC і SOC.

Доступ до мережевих компонентів повинен бути авторизованим, бажано через централізовану службу автентифікації, авторизації та обліку (AAA) та з використанням мережевих протоколів, таких як Remote Authentication Dial-In User Service (RADIUS) або Terminal Access Controller Access Controller Access Control System (TACACS). Використання сервера AAA гарантує, що всі спроби

доступу реєструються за допомогою журналу аудиту, який можна отримати під час розслідування інциденту.

Найкращою практикою є використання щонайменше двох факторів для автентифікації користувачів. Рішення для багатофакторної автентифікації, як правило, є поєднанням "того, що ви знаєте" (пароль), "того, що у вас є" (картки доступу, тверді або м'які токени), і "того, ким ви є" (сканер відбитків пальців). Зв'язок між пристроями, наприклад, від робочого столу користувача до пристрою SOC, повинен використовувати певну форму шифрування, таку як Secure Shell (SSH), Secure Sockets Layer (SSL) або Transport Layer Security (TLS).

Безпека

Захист мережі SOC, хостів і додатків має найвищий пріоритет. Компрометація мережі та систем SOC підриває мету створення SOC і негативно впливає на можливості виявлення, довіру до організації та виправдання майбутніх інвестицій. Розвиток анклаву SOC з використанням сегментації мережі та засобів контролю безпеки може запобігти порушенню.

Розробка анклаву SOC починається з сегментації трафіку різних рівнів довіри з використанням фізичного поділу або різних варіацій віртуальної сегментації мережі, таких як VLAN, списки доступу або групові теги безпеки (SGT). Вхідні та вихідні з'єднання з та до сегментів мережі SOC повинні відслідковуватися та контролюватися на підтримку принципу найменших привілеїв, при якому доступ обмежується лише тим, що потрібно для роботи служби або користувача.

При використанні брандмауерів правила їх сегментації мають забезпечувати стандартний контроль доступу на основі мережі, який застосовується до вхідного, вихідного та внутрішнього трафіку SOC. Правила управляються і підтримуються командою SOC і слідують стандартному процесу контролю управління змінами. Підтримка бази правил брандмауера включає регулярний перегляд та оновлення. Наприклад, правила, термін дії яких закінчився, вручну або автоматично відключаються або видаляються. Всі правила також належним чином задокументовуються. Кожне правило має бути

пов'язане з описом, який включає інформацію про: суб’єкта, що робить запит; мету звернення; дату створення та закінчення терміну дії; реєстраційний номер затвердження управління змінами.

Контроль запобігання вторгненням повинен бути інтегрований з дизайном анклаву SOC таким чином, щоб трафік перевірявся в потоці, де це можливо. Система запобігання вторгненням (IPS) може бути реалізована як окреме рішення або може бути інтегрована з брандмауером. Режим роботи IPS може бути налаштований на відмову-закриття або відмову-відкриття. При налаштуванні на відмову-відкриття, відмова IPS призведе до того, що IPS буде діяти як мережевий обхід, пропускаючи трафік без перевірки. Корпоративна політика безпеки повинна визначати прийнятний режим роботи на основі розуміння ризиків, пов'язаних з обома варіантами.

Підписи та правила IPS повинні бути налаштовані таким чином, щоб несуттєві підписи були відключені, в той час як відповідні підписи були вручну або автоматично включені та налаштовані. Також вкрай важливо враховувати вплив на продуктивність, що виникає в результаті включення занадто великої кількості правил і роботи функцій IPS і брандмауера в одній і тій же системі. Обов'язковими є консультації з постачальником щодо впливу на продуктивність перед ввімненням кількох функцій безпеки.

Управління квитками

Управління квитками безпосередньо пов'язане з програмою реагування на інциденти безпеки, де створюються, оновлюються і закриваються запити на обслуговування інцидентів відповідно до процесу обробки інцидентів. В ідеалі, компанії прагнуть використовувати наявні в них платформи запитів на обслуговування для відстеження інцидентів безпеки. Щоб відокремити квитки, пов'язані з SOC, система має призначити певний тег SOC для кожного квитка, а необхідні поля інцидентів безпеки повинні бути включені в тег запиту на обслуговування. Це спростить роботу сторони, відповідальної за обробку квитка.

Інтеграція між інструментами SOC і платформою запитів на обслуговування може бути реалізована в ряді областей, включаючи зв'язок SIEM та інструментів управління вразливостями з платформою запитів на обслуговування. Аналітик SOC повинен мати можливість відкрити і заповнити запит на обслуговування інциденту безпеки з інструменту SIEM, усуваючи або, можливо, мінімізуючи ручні зусилля, необхідні для створення і заповнення нового запиту. Поля запитів на обслуговування повинні бути узгоджені з планом обробки інцидентів таким чином, щоб важлива інформація була належним чином зафіксована і щоб статус інциденту можна було безперервно відстежувати.

3.2.2 Формування та збір подій безпеки

Слід розглянути способи збору даних з різних джерел, щоб їх можна було перетворити в корисний формат для SOC. Для кожного джерела, що генерує дані, описані кроки щодо експорту даних до централізованої утиліти кореляції.

Абсолютно важливо, щоб усі аспекти збору й аналізу даних були розроблені належним чином, щоб уникнути прогалин в тому, як SOC відстежує навколишнє середовище. Невелика сліпа пляма може стати дверима для майбутньої атаки. З цієї причини найкращою практикою є розміщення точок моніторингу безпеки по всій мережі і моніторинг всіх подій за допомогою централізованого рішення для збору даних. Це дає SOC швидку видимість багатьох систем і можливість відстежувати більш складні загрози, використовуючи кореляцію даних між тим, що бачать кілька продуктів або через відгалужувачі для збору трафіку.

Найкращою практикою є використання централізованого рішення для збору даних, яке діє як перша точка контакту SOC при розслідуванні подій.

3.2.3 Управління вразливостями

Зловмисникам достатньо використати лише одну вразливу систему, щоб отримати доступ до корпоравтиної мережі. Потрапивши всередину, вони можуть створити кілька виходів назовні, що надзвичайно ускладнює повне усунення прориву. Це називається створенням плацдарму відповідно до життєвого циклу цільової атаки Mandiant. Звідти зловмисник може переміщатися по мережі, створюючи хаос за допомогою внутрішніх кампаній атак, викрадаючи дані.

Багато виявлених порушень спричинені тим, що система має відому вразливість, яка була використана до того, як вона була належним чином виправлена. Звіт Verizon Breach Investigation Report (VBIR) [104] показав, що 99,9% використаних вразливостей були скомпрометовані більш ніж через рік після публікації CVE (метод виправлення). Саме так, 99,9% компрометацій систем з використанням вразливостей можна було б запобігти, якби було забезпечене належне управління вразливостями.

Це дослідження показує, що організації не встигають за управлінням виправленнями або, швидше за все, просто зосереджуються на останніх загрозах. Однак, організації повинні постійно проводити аудит на наявність нових і старих вразливостей, оскільки будь-яка вразливість є актуальною. Для більшості організацій, як правило, неможливо досягти 100%-го рівня управління виправленнями, оскільки нові вразливості, які виявляють щодня, роблять цю мету рухомою мішенню.

Завданням SOC є виявлення та усунення вразливостей до того, як зловмисник ними скористається. VBRI 2015 показав, що половина опитаних організацій виявили подію зловмисного програмного забезпечення протягом 35 днів (або менше). Ось чому належне управління вразливостями може підвищити або знизити ефективність SOC у боротьбі із загрозами.

Виявлення вразливостей

Вразливість означає потенційну можливість атаки, але це не означає, що система була використана. Так, можуть існувати системи, які вважаються вразливими до певного типу атак, таких як використання веб-сервісів; однак,

якщо ці системи не підключені до Інтернету, ризик їх використання є потенційно низьким. Важливим завданням SOC є кваліфікація вразливостей та визначення того, які з них становлять найбільший ризик для організації, щоб їх можна було визначити як пріоритетні перед іншими завданнями з усунення недоліків.

У міру зростання і розширення використання мереж з'являється все більше нових вразливостей. Вразливості можуть бути будь-якими з перерахованих нижче, плюс багато інших можливостей:

– Неправильна конфігурація програмного забезпечення або помилка в архітектурі мережі.

– Слабкі політики безпеки, наприклад, використання коротких, передбачуваних паролів.

– Виробничий брак в апаратному або програмному забезпеченні.

– Недостатня обізнаність про можливі загрози.

– Слабкість портів або протоколів, що використовуються.

Перелік можливих вразливостей нескінченний, а діапазон цілей може бути будь-яким: від обчислювальних систем до персоналу. Практично неможливо не мати вразливостей у корпоративній мережі, тому дуже важливо розуміти, як SOC управляє вразливостями, а також мати підтримку керівництва для забезпечення дотримання відповідних політик.

У загальних рисах, управління вразливостями - це циклічна практика виявлення, класифікації, усунення та зменшення вразливостей. Управління вразливостями є безперервним процесом, який адаптується до змін і масштабується до всіх областей мережі і до будь-яких бізнес-зв’язків.

Це є ключовим моментом, оскільки нерідко навіть захищені компанії ставали вразливими через вразливості у бізнес-зв’язках, таких як постачальники, з якими вони ведуть бізнес. Прикладом може бути компанія, яка купує системи автентифікації у зовнішнього постачальника, який виявляється вразливим під час циклу доставки, від складу, де створюється

обладнання, до компанії, яка продає продукцію. Зловмисник може перехопити вантаж і встановити шкідливе програмне забезпечення на продукцію з метою отримати доступ до мережі будь-якої компанії, яка встановлює рішення. Ось чому управління вразливостями повинно поширюватися на всі аспекти бізнесу, мати кілька рівнів контрольних точок і постійно відстежувати можливі слабкі місця.

Послуги безпеки

Багато організацій і постачальників використовують такі рішення як аудит, тестування на проникнення або оцінка для опису подібних послуг, які виявляють вразливості. Це може викликати плутанину щодо вимог до рівня зусиль та очікуваних результатів при укладанні зовнішніх контрактів або навчанні організації SOC для виконання таких обов'язків. Загалом, галузь використовує такі послуги для виявлення вразливостей:

– **Відповідність та аудит:** Відповідність та аудит можуть бути зосереджені на оцінці рівня ризику системи або програми, ризиків проектування мережевої архітектури або оцінці існуючих засобів контролю відповідно до набору стандартів або базових показників. Стандарти і базові показники можуть бути вимогами безпеки або мінімально прийнятним рівнем безпеки, який компанія перевіряє на відповідність, опублікованими всередині компанії або такими, що відповідають зовнішнім рекомендованим архітектурам (тобто, опублікованим політикам та архітектурам). Наприклад, деякі аудити безпеки перевіряють відповідність необхідним нормам, таким як відповідність стандарту безпеки даних індустрії платіжних карток (PCI DSS) або сертифікації обладнання Об'єднаною командою з тестування на сумісність (JITC). Іноді вони ґрунтуються на перевірці ефективності контролю або виявленні недоліків дизайну. Прикладом може бути система запобігання вторгненням (IPS), яка не має видимості в деяких сегментах мережі, що робить їх більш вразливими до атак через відсутність захисту. Причини надання послуги аудиту високого рівня варіюються від юридичного зобов'язання щодо дотримання вимог

законодавства до простого проходження політики безпеки співробітництва. З цієї причини аудит може створити хибне відчуття безпеки, засноване на тому, що багато галузевих нормативних актів або спільних політик вимагають певного часу для публікації вимог. Тактика кібератак швидко змінюється, випереджаючи багато галузевих нормативних актів щодо мінімальних стандартів безпеки. Найкращою практикою є використання аудиту для доведення відповідності конкретним засобам контролю або правилам; однак, для захисту мережі доцільно використовувати суворіші базові показники і поглиблені практики сканування вразливостей.

– **Оцінка вразливостей:** Ця послуга зосереджена на скануванні пристроїв, операційних систем і додатків на наявність відомих і потенційно невідомих вразливостей. Як правило, це досягається за допомогою інструменту або набору інструментів, які автоматизують процес сканування. Оцінка вразливостей припиняється після того, як вразливість знайдена або не підтверджена. Виявлені вразливості є потенційною слабкістю системи безпеки; однак не всі виявлені вразливості можуть бути використані. Оцінки вразливостей чудово підходять для створення списку нових вразливостей, які можуть бути використані для розрахунку ризику для бізнесу й перевірки існуючих засобів контролю безпеки; вони також можуть бути позиціоновані як цільовий список для більш глибокого аналізу, наприклад, з використанням тестування на проникнення.

– **Оцінка конфігурації:** Як і оцінка вразливостей, оцінка конфігурації фокусується на скануванні пристроїв, операційних систем і додатків; однак, оцінка конфігурації може оцінювати архітектуру і конфігурацію в порівнянні з кращими галузевими практиками або політиками і стандартами організації. Приклади включають виявлення використання функцій, не рекомендованих для належного налаштування безпеки (таких як Telnet або SNMP (Simple Network Management Protocol) Version 1), недоліків у конфігурації систем, відсутність увімкнених функцій і так далі. Оцінка вразливостей може виявити проблеми з

конфігурацією; однак, результати цієї послуги надаються з точки зору чистої вразливості, а не визначення проблеми з конфігурацією, що спричиняє небажаний ризик. Аудит та оцінка вразливостей можуть включати завдання з оцінки конфігурації як частину обсягу послуг.

– **Тестування на проникнення:** Тестування на проникнення додатково оцінює виявлені вразливості, намагаючись використати вразливість аналогічним методом реального зловмисника. Це означає, що виявлені вразливості перевіряються до того, як вони будуть включені до звіту, надаючи коротший, але більш точний список вразливостей, які SOC повинен розглянути. Тестування на проникнення, як правило, є більш цілеспрямованим і включає в себе більше послуг і більш високу вартість, ніж оцінка вразливостей, призначена для перевірки міцності існуючої системи безпеки. Це означає, що тестування на проникнення не призначене для того, щоб зробити корпоративну мережу більш безпечною. Найкраще використовувати тестування на проникнення, коли вичерпані інвестиції в поліпшення безпеки і компанії потрібно перевірити, чи є достатній захист від очікуваних загроз, або додатково оцінити відомі загрози, такі як слабкі місця, виявлені під час оцінки вразливостей.

Кожна послуга пропонує різні форми переваг і витрат, які слід враховувати. Аудит може не надати достатньо даних для захисту мережі, але допомагає обґрунтувати відповідність встановленим нормам. Аудит також може допомогти обґрунтувати бюджет для майбутніх проектів, оскільки недотримання багатьох вимог має юридичні наслідки. Важливо включити стратегію для отримання даних аудиту, коли необхідна валідація.

Оцінювання вразливостей і конфігурації є чудовим інструментом для моніторингу вразливостей та отримання загального уявлення про поточний стан ризиків безпеки у корпоративному середовищі. Оцінювання має бути безперервним процесом, оскільки ландшафт загроз для середовища SOC зміниться, як тільки буде завершено оцінювання. Оцінювання повинно

охоплювати всю мережу та враховувати всі аспекти бізнесу. Це повинно бути поєднано з цілями SOC щодо забезпечення інформаційної безпеки та підтримано керівництвом, щоб надати йому повноваження.

Тестування на проникнення використовують для перевірки будь-якої потенційно вразливої ділянки з високим рівнем ризику, але необхідно чітко визначити усі аспекти, щоб уникнути виснаження бюджету та часу. Хорошим варіантом є використання тестування на проникнення для перевірки результатів оцінки вразливостей або тестування можливостей захисту конкретних критично важливих систем. Недоцільним є використання тестування на проникнення для проникнення в мережу будь-яким можливим способом. Причина полягає в тому, що тестувальник може витратити багато часу на дослідження областей, які більшість SOC не вважають критично важливими для бізнесу.

Іншим поганим результатом є порушення мережі за допомогою тактики, яка не покращить практику SOC. Прикладом може бути наймання консультантів для проведення тестування на проникнення і виявлення того, що вони пройшли процес найму, витратили два тижні на крадіжку даних як нові співробітники, а потім передали вкрадені дані, і все це в той час, коли вони працювали і виставляли компанії рахунки за послуги з тестування на проникнення. Про цю слабкість було б корисно знати; однак, більшість SOC, ймовірно, могли б знайти більше користі, інвестуючи в інші методи виявлення вразливостей.

Так, основною метою тестування на проникнення має бути використання нестандартних тактик, до яких SOC не готовий, для оцінки реагування на інцидент; однак, реальність цієї послуги полягає в тому, що бюджет може обмежувати обсяг в залежності від бажаних результатів. Краща практика полягає в тому, щоб переконатися, що затверджуючий ресурс чітко визначає, чи є тестування на проникнення "чорною скринькою" (абсолютно невідоме середовище, яке атакується без будь-яких знань про цілі), "білою скринькою" (дуже специфічне середовище з конкретними цілями) або "сірою скринькою" (деякі знання про середовище і цілі, але нічого конкретного і, можливо,

обмежена область атаки), перш ніж залучати ресурси для тестування на проникнення, щоб отримати кращі результати.

3.3 Етап впровадження

3.3.1 Технологія

Розглянемо технології, що використовуються командами центрів забезпечення безпеки (SOC) по всьому світу. Перш ніж оцінювати технології, спочатку розглянемо різні середовища SOC.

Внутрішній та віртуальний SOC

Внутрішня SOC передбачає, що технологія, процеси та людські ресурси розробляються та надаються в межах об'єкта, на якому розміщується команда та послуги SOC, незалежно від місця розташування, розміру та особливостей об'єкта. Перевагою такого підходу є знайомство з середовищем SOC, притаманне використанню місцевого персоналу та технологій. Віртуальний SOC передає частину або всі послуги SOC на аутсорсинг зовнішньому провайдеру. Це допомагає прискорити створення SOC та пропонує додаткові можливості, які можуть бути недоступні на місцевому рівні.

У деяких ситуаціях компанія може використовувати варіації власного та віртуального SOC у гібридному форматі. Одним із гібридних варіантів використання є моніторинг внутрішньої мережі за допомогою штатного SOC, а віртуальний SOC використовується для масштабування на віддалених об'єктах. Інший варіант використання полягає в тому, щоб спочатку використовувати віртуальний SOC для створення служб SOC, а потім повільно переходити на новий власний SOC в міру того, як він буде запущений в експлуатацію.

Кожна модель SOC впливатиме на технології, які будуть використовуватися в ході щоденної роботи. Внутрішній SOC має вищу вартість, що базується на відповідальності за придбання та підтримку всіх продуктів. Аутсорсинг послуг SOC також означає аутсорсинг деяких

інструментів. Однак, навіть повністю віртуальне середовище SOC матиме певні місцеві технології, які повинні бути розроблені та керовані належним чином.

Почнемо з огляду більш широких технологічних тем, зокрема з високорівневих концепцій проектування для категорій мережі, безпеки, систем, зберігання і спільної роботи, слідуючи загальним технологічним рекомендаціям з оглядом загальних технологій, які використовуються в зрілих SOC. Спочатку розглянемо міркування щодо проектування мережі.

Мережа

Основою будь-якого SOC є мережа, на якій він працює. Деталі проектування і зона відповідальності будуть відрізнятися для кожного середовища, але деякі загальні концепції є спільними для більшості мереж. Мережа, яку захищає SOC, вважається внутрішньою, а все, що не є частиною мережі організації, вважається зовнішнім. Як би просто це не звучало, дуже важливо визначити, що таке внутрішня мережа, щоб інструменти моніторингу могли розпізнати, коли у внутрішній мережі з'являється невідома або зовнішня IP-адреса.

Як правило, внутрішня мережа розбивається на різні сегменти, яким присвоюються різні рівні довіри. Найпоширенішою сегментацією є наявність трьох зон, де зовнішня не має довіри, демілітаризована зона (DMZ) має певну довіру, а внутрішня повністю довіряється. Ідея цієї базової архітектури полягає в тому, щоб розмістити системи, які потребують зв'язку як ззовні, так і зсередини, такі як веб-сервери, в демілітаризованій зоні, надавши їм певну довіру, але на тому ж рівні, що і системам всередині мережі. На рисунку 3.1 показана ця базова архітектура. Зверніть увагу, що це базова модель довіри. Швидше за все, будуть існувати різні рівні внутрішньої довіри для захисту від різних варіацій внутрішніх загроз.

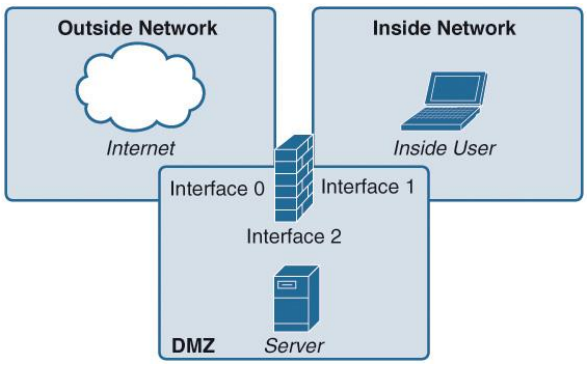

Рис. 3.1 Базова архітектура мережі

Найкращою практикою є більш детальний рівень довіри шляхом подальшого сегментування внутрішньої мережі на різні зони безпеки, наприклад, відокремлення центру обробки даних від загального трафіку внутрішньої мережі. Також важливо впровадити контроль трафіку в межах внутрішніх зон безпеки з використанням різних форм віртуальних локальних мереж (VLAN), списків контролю доступу (ACL) і групових тегів безпеки (SGT). Засоби контролю можуть бути вбудовані в сегментацію мережі або застосовуватися після того, як доступ до сегмента мережі був дозволений.

VPN

Можуть існувати проектні вимоги щодо безпечного з'єднання двох або більше окремих сегментів мережі або віддалених користувачів. Прикладом може бути організація з декількома філіями, розташованими по всьому світу, яким необхідно спільно використовувати внутрішні ресурси. Це може бути досягнуто шляхом з'єднання місць розташування за допомогою VPN на основі хоста або надання VPN на основі хоста віддаленим системам.

Фундаментальною концепцією міжсайтової VPN є створення зашифрованого тунелю між двома або більше місцями і забезпечення доступності мережі через тунелі. Це дозволяє співробітникам в одному місці діяти так, ніби вони знаходяться у віддаленому місці, без необхідності вносити будь-які зміни в те, як вони використовують мережу. Cisco пропонує безліч варіантів технології VPN, таких як GET-VPN, динамічна багатоточкова VPN (DMVPN), VPN на основі загальної інкапсуляції маршрутизації (GRE), Easy VPN і стандартний IPsec.

VPN на основі хоста розширює безпечний тунель між певним пристроєм і внутрішньою мережею, надаючи користувачеві такий же досвід, як якщо б цей пристрій був локально підключений до внутрішньої мережі. Найбільш поширеними формами цієї технології є використання клієнта, який встановлюється на хості або надання тунелю за допомогою сервісів на основі веб-браузера.

Клієнтська технологія VPN від Cisco пропонує безліч функцій, таких як автоматичне підключення, коли пристрій використовує не внутрішню IP-адресу, багатофакторна автентифікація, оцінка кінцевих точок на відповідність вимогам політики, наприклад, наявність встановленого антивірусу, і так далі. На рисунку 3.4 показано активний агент AnyConnect, обведений колом, і екран версії, що представляє AnyConnect 4.0.0048. Коли мережеве з'єднання цього пристрою втрачається, зображення блокування AnyConnect буде циклічно змінюватися, доки не з'явиться нове мережеве з'єднання. Якщо це з'єднання не є внутрішньою мережею, Cisco AnyConnect автоматично перепідключає тунель VPN.

Рис. 3.2 Клієнт Cisco AnyConnect

Безклієнтська VPN працює за допомогою інтернет-браузера для доступу до певного веб-сайту, який оцінює пристрій і надає доступ до розміщених послуг в залежності від постачальника та увімкнених функцій. Cisco Secure Sockets Layer (SSL) може забезпечити персоналізований веб-портал, який містить або ізолює активність в межах порталу. Доступ до певних служб, таких як віддалений робочий стіл, електронна пошта тощо, може бути включений і

контролюватися в середовищі порталу. Коли веб-сторінка закривається або сеанс завершується, кеш веб-браузера може бути очищений, щоб видалити сліди сеансу з локальної системи. Це ідеально підходить для надання довірених послуг ненадійним пристроям, таким як гостьовий комп'ютер в готелі.

Аутентифікація

Контроль мережевого доступу (NAC), на додаток до багатьох інших технологій безпеки, використовує фактори автентифікації для перевірки людей і систем. Найбільш поширеними факторами, що використовуються для автентифікації, є один або кілька з "того, що ви знаєте, того, що у вас є, і того, ким ви є". Багато нормативних актів адаптують мінімальні вимоги до двофакторної автентифікації, але компанії, які вимагають більш високого рівня безпеки, можуть мати кілька факторів в залежності від чутливості даних в мережевому сегменті.

Ще однією важливою функцією централізованої системи автентифікації є підзвітність. Багато мережевих і захисних рішень можуть отримувати дані користувачів з централізованого сховища і прив'язувати їх до того, як вони використовують мережеві ресурси. Підзвітність може поширюватися на адміністративні права та підзвітність, наприклад, надання конкретній особі Н. дозволу на вхід до маршрутизатора та запис усіх змін конфігурації, які вона вносить, перебуваючи в системі. Це може виявитися корисним, якщо виникла мережева проблема і системному адміністратору необхідно визначити, хто здійснив небажані зміни конфігурації. Прикладом може бути виявлення того, що саме Н. неправильно налаштував шлюз за замовчуванням філії, вносячи зміни в несанкціонований час (тобто, не під час авторизованого вікна технічного обслуговування), що призвело до відключення філії на 30 хвилин.

Безпека в мережі

Після впровадження технологій сегментації мережі та контролю доступу, наступним питанням безпеки є моніторинг та захист людей і пристроїв в

кожному сегменті мережі. Компанія може досягти цього, використовуючи різні форми сигнатур і технологій поведінки (розглянуті далі в цьому розділі), такі як системи запобігання вторгнень (IPS), виявлення порушень і аналіз мережевої поведінки. Найкраща практика полягає в тому, щоб забезпечити багаторівневе виявлення в масштабах всієї мережі і перегляд усіх типів трафіку. Це включає в себе розгляд вимог до пропускної здатності в кожній точці виявлення, щоб безпека не впливала на продуктивність мережі понад допустимі пороги.

Найбільш поширеним розміщенням рішення для мережевого моніторингу є включення функцій в брандмауері мережевого шлюзу або розміщення рішення безпосередньо за брандмауером шлюзу. Поширеними функціями безпеки, включеними в цій точці мережі, є IPS, фільтрація контенту, контроль додатків, сканування на наявність шкідливого програмного забезпечення та певні форми запобігання втраті даних. Прикладом пристрою безпеки, що забезпечує ці функції, є пропозиція Cisco FirePOWER, яка може працювати в складі брандмауера серії Adaptive Security Appliance (ASA) або як окремий пристрій, що знаходиться за брандмауером шлюзу. Пристрої мережевої безпеки можуть підключатися до інших частин мережі, наприклад, в центрі обробки даних або по всій мережі, в залежності від того, де розроблено мережеве виявлення.

Мережевий моніторинг не повинен обмежуватися мережевим шлюзом або випадковими прослуховуваннями всередині мережі. Мережева телеметрія може бути зібрана з загальних мережевих пристроїв для моніторингу незвичайної поведінки між контрольними точками безпеки, такими як пристрої IPS. NetFlow може бути включений на більшості поширених мережевих пристроїв і відправлений в інструмент, який може перетравити і проаналізувати його на предмет подій безпеки. Важливо знати, що всі інструменти збору NetFlow не створені однаково, як описано в обговоренні NetFlow далі в цій главі. Технологія захоплення пакетів також може бути розміщена в певних частинах мережі для збору і аналізу трафіку на предмет загроз. Як NetFlow, так і технології перехоплення пакетів можуть ідентифікувати загрози на основі

поведінки, але для належного впровадження технології можуть знадобитися додаткові інвестиції в сховище і модернізацію мережі.

Безпека неминуче зазнає збоїв, і важливо мати заходи безпеки, які дозволять виявити, коли стався збій. Технологія виявлення порушень використовує методи оцінки, спрямовані на визначення того, коли організація була скомпрометована, такі як карантин підозрілих додатків в пісочниці для моніторингу їх поведінки, моніторинг незвичайної поведінки, сканування портів, маніпуляції з файлами або виявлення зв'язків з відомими зовнішніми загрозами. Продукти для виявлення порушень, як правило, побудовані так само, як і інші технології мережевої безпеки, які повинні мати можливість бачити трафік для виконання аналітики. Найкращою практикою є виявлення порушень як у мережі, так і на всіх кінцевих точках для повної видимості. Прикладами таких технологій є FireEye, Cisco Advanced Malware Detection (AMP) та Bit9.

Однією з проблем для багатьох технологій мережевого виявлення є розширення видимості рішення. Ці технології можуть досліджувати тільки те, що вони можуть аналізувати, а це означає, що трафік, який недоступний або прихований шифруванням, не може бути оцінений. Якщо мережа належним чином сегментована, це може означати або вимогу до точок доступу або "відводів" для технології моніторингу, щоб переглядати кожен сегмент, або придбання виділених пристроїв для кожного сегмента мережі, що може стати дорогим задоволенням. Крім того, трансляція мережевого доступу (NAT) може заплутати технологію моніторингу, приховуючи ідентичність пристроїв, прихованих за точкою NAT. Наприклад, 20 пристроїв можуть відображатися в мережі як одна IP-адреса, якщо інструмент моніторингу бачить тільки внутрішній трафік. Деякі варіанти подолання приховування NAT полягають в інтеграції технології контролю доступу, щоб об'єднати те, які пристрої проходять аутентифікацію за NAT, з тим трафіком, який бачить інструмент моніторингу, або розмістити відгалужувачі для інструменту моніторингу перед точкою NAT.

3.3.2 Остаточна архітектура SOC

Вище розглянуто багато різних технологій і концепцій проектування. Кожна з них стосувалася конкретного випадку використання. Тепер нам потрібно об'єднати ці концепції разом, щоб побачити, як технологія буде виглядати в зрілій архітектурі SOC. Почнемо з розгляду рисунка 3.3, на якому показаний SOC, що використовує більшість концепцій, пристроїв і технологій, розглянутих у роботі. Кожна мережа буде відрізнятися, але цей приклад дає загальне уявлення про технології безпеки, які зазвичай використовуються в організації.

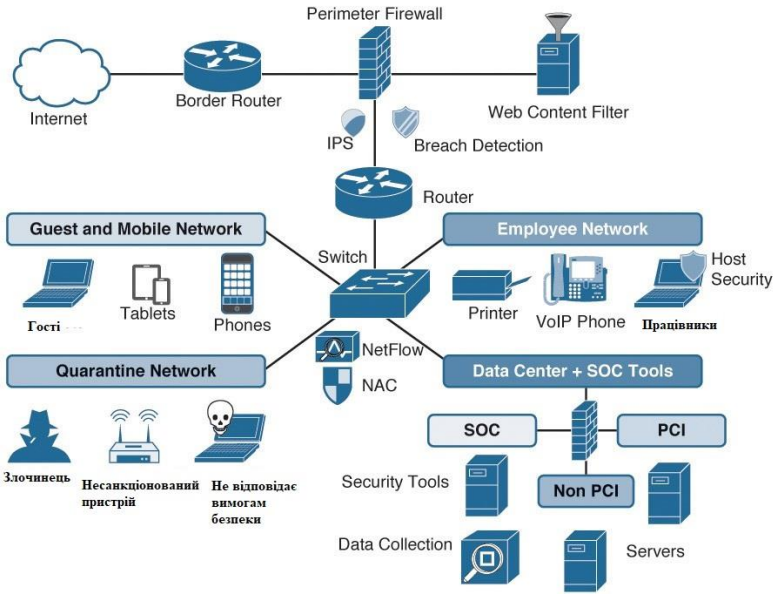

Рис. 3.3 Приклад зрілої архітектури SOC

Перша технологія, яку розглянемо на рисунку 3.3, – це рішення безпеки шлюзу. Потім перейдемо до внутрішніх мереж. Ця компанія використовує пристрій безпеки, який діє як брандмауер (з підтримкою стану і прикладного рівня), IPS і рішення для виявлення порушень, подібне до пропозиції Cisco FirePOWER з ліцензією IPS і AMP. Виділений проксі-сервер виконує фільтрацію веб-контенту, перенаправляючи трафік за допомогою WCCP на проксі-сервер з міжмережевого екрану шлюзу, коли трафік входить і виходить з мережі. Веб-проксі є продуктом компаній Cisco (WSA), BlueCoat, Websense тощо.

Внутрішня мережа сегментується на чотири мережі з використанням комбінації VLAN та ACL. Авторизовані пристрої та комп'ютери компанії

розміщені в мережі співробітників. Всі гості й особисті пристрої, такі як планшети і телефони, розміщені в гостьовій мережі.

Для контролю доступу до мережі використовується Cisco ISE для забезпечення дотримання цих політик. Якщо пристрій не відповідає політикам NAC, наприклад, не має останніх оновлень або встановленого антивірусу, він розміщується в мережі карантину. Крім того, будь-які несанкціоновані бездротові точки доступу або концентратори, виявлені Cisco ISE, поміщаються в карантин. Моніторинг всієї мережі здійснюється за допомогою обладнання з підтримкою NetFlow, яке контролюється SOC. Інструмент NetFlow інтегрований з ISE і виступає в якості рішення для контролю після доступу з можливістю помістити в карантин все, що вважається високим ризиком іншими інструментами мережевої безпеки.

Центр обробки даних сегментований за допомогою спеціального брандмауера, що розділяє системи PCI і не PCI. SOC має власну мережу, в якій розміщена система Splunk SIEM, а також різні інструменти безпеки, що використовуються для моніторингу мережі та хостів. Якщо будь-який інструмент виявляє загрозу високого рівня в мережі, він може використовувати Splunk для запуску Cisco ISE, щоб відправити пристрій в карантинну мережу. Інші інструменти, такі як рішення NetFlow, StealthWatch, можуть відправляти пристрої високого рівня небезпеки в карантинну мережу, використовуючи Cisco ISE в якості мережевого контролера.

Багато інших технологій безпеки присутні, але не представлені в цьому прикладі мережі. Існують продукти безпеки на основі хостів, які можуть представляти антивірус, засоби виявлення порушень на кінцевих точках та інші рішення безпеки на основі хостів. Швидше за все, інструменти управління робочими столами можуть мати події, що надсилаються в Splunk, щоб допомогти SOC у забезпеченні відповідності вимогам безпеки. Віддалений доступ не розглядається, але доступний як опція VPN, налаштована на периметральному брандмауері Cisco ASAx.

Підсумовуючи технології, показані на рисунку 3.3, нижче наведено перелік потенційних матеріалів лише для технології безпеки. У цьому прикладі не розглядаються міркування проектування для забезпечення високої доступності, фізичної безпеки, послуг по установці.

– ASA5555X з SSD: Брандмауер по периметру;

– Ліцензія FirePOWER для IPS та AMP: IPS та виявлення порушень;

– Cisco WSA S380: Проксі-сервер веб-безпеки з ліцензією на антивірус McAfee та фільтрацію спалахів;

– Cisco ISE VM сервер: NAC менеджер;

– Ліцензії на базі Cisco ISE та Apex на 500 користувачів: Ліцензування користувачів ISE;

– Lancope StealthWatch SMC: менеджер NetFlow;

– Lancope StealthWatch Collector: Колектор NetFlow;

– Lancope StealthWatch Sensor: Конвертер даних в NetFlow, розміщений в дата-центрі;

– Splunk: SIEM для збору даних.

Тепер розглянемо, як влаштована можлива віртуальна SOC. На рисунку 3.4 показаний приклад віртуального середовища SOC, де Cisco надає послуги віртуального SOC клієнту. Мережеві пристрої в місці розташування клієнта налаштовані на відправку журналів подій та інших даних в системи, які контролюються зовнішнім SOC. Оскільки Cisco надає послуги віртуального SOC, всі інструменти SOC розміщуються в центрі обробки даних Cisco. Зв'язок між сайтом замовника, SOC та дата-центром Cisco, де розміщені різні інструменти, здійснюється за допомогою зашифрованих веб-каналів. Клієнт має доступ до даних, що відстежуються віртуальною командою SOC, через портал, а також через систему продажу квитків, яка дозволяє визначити, які саме події розглядаються.

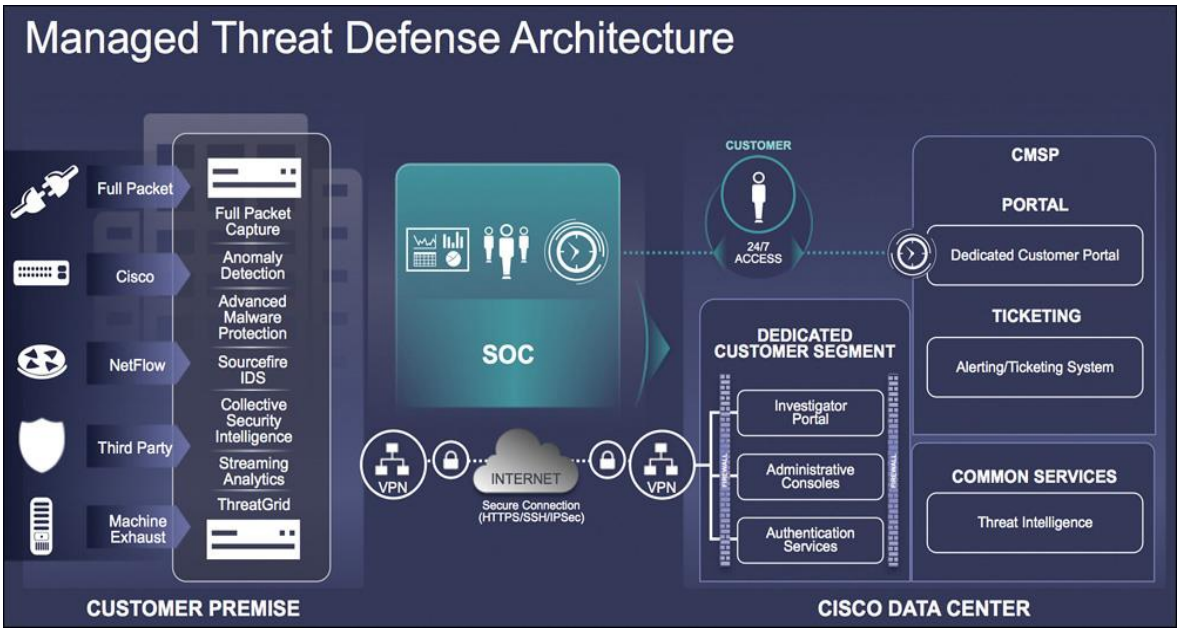

Рис. 3.4 Приклад середовища віртуального SOC

Ціноутворення віртуального SOC може базуватися на багатьох факторах, таких як кількість пристроїв, за якими ведеться моніторинг, тип запитуваних послуг SOC, робота служби підтримки, розташування офісів замовника тощо.

Гібридна SOC може виглядати як поєднання рисунків 3.3 і 3.4, де деякі технології належать і управляються SOC, а інші можуть відправляти трафік в центр обробки даних Cisco для моніторингу віртуальною командою SOC. Обидва приклади дуже високого рівня, але вони представляють загальні способи, якими середовища SOC використовують вище розглянуті технології.

3.3.3 Підготовка до експлуатації

Зробимо огляд типових кроків, які необхідно виконати для того, щоб SOC почав повноцінно функціонувати. Це означає розробку чіткого плану переходу або трансформації SOC та забезпечення наявності всіх основних компонентів, необхідних для ефективної роботи. Це також означає управління очікуваннями керівництва, як правило, до раніше узгоджених термінів. Таким чином, підготовка SOC до роботи зводиться до управління мінливими цілями, і все це за допомогою виконавчих спонсорів.

Ключові виклики

Необхідно вирішити ряд ключових проблем для успішного переходу нової SOC до того моменту, коли він стане ефективним способом виявлення та усунення інцидентів кібербезпеки в середовищі. Сюди входять виклики по всьому спектру, від персоналу до процесів і технологій.

Виклики, пов'язані з персоналом

Проблеми з людьми починаються на самому верху: керівники, які спонсорували розробку SOC. Запит на створення SOC часто виникає після серйозного інциденту з кібербезпеки, коли пристрасті і бажання вкласти гроші в вирішення проблеми досягають свого апогею. Зопалу керівники, які прагнуть усунути ризик, можуть бути готові інвестувати значні кошти, навіть якщо ці інвестиції можуть бути величезними, як у вигляді авансових капітальних вкладень, так і у вигляді поточних операційних витрат.

На початку, керівник, який виступає спонсором, наприклад, директор з IT, може відчувати, що SOC є ініціативою, яка отримує широку підтримку не тільки з боку топ-менеджменту (наприклад, ради директорів, фінансового директора, генерального директора), але і з боку колег в організації.

Розумний керівник SOC повинен бути готовим до певної перебудови, оскільки SOC наближається до того, щоб стати реально функціонуючим підрозділом організації. Тісна співпраця з керівником-спонсором є ключем до демонстрації того, що інвестиції в SOC залишаються обґрунтованими, а також допомагають гарантувати, що неминучі компроміси не вплинуть на успіх SOC.

Технологічні виклики

Типовий SOC вимагає значних інвестицій в технології, щоб бути навіть помірно ефективним, і вкрай малоймовірно, що компанія зможе розгорнути всю бажану технологічну базу до того, як потрібно буде перейти до експлуатації. При переході від SOC до виробництва, як правило, можна зіткнутися з проблемами, пов'язаними з більш тривалими, ніж очікувалося, термінами розгортання ключових технологій, затримкою або відсутністю важливих даних про події або збагачення, відсутністю інтеграції між

ключовими системами або тим, що кошти на новий канал розвідданих можуть просто вичерпатися. Розумний керівник SOC повинен ретельно управляти очікуваннями (в тому числі, очікуваннями своїх спонсорів, членів команди і споживачів послуг). Багато в чому це зводиться до постійного моніторингу розгортання технологічної бази і вирішення проблем так швидко, як тільки вони з'являються.

Подолання викликів за допомогою керованого переходу

Хоча це може здатися очевидним, розгортання SOC - це проект з багатьма рухомими частинами і пов'язаними ризиками. У найскладніших розгортаннях SOC він може навіть приймати форму декількох проектів, що перетинаються або паралельних проектів, якими доведеться керувати в рамках загальної програми. Незалежно від того, чи управляється розгортання SOC як єдиний проект або як кілька проектів в рамках однієї програми, воно потребує сильного, послідовного управління. Також знадобиться сильний і здібний керівник проекту/програми.

Керівник SOC, як правило, не є керівником проекту/програми (керівником програми), але забезпечує повсякденне керівництво цією особою від імені виконавчого спонсора. Керівник проекту може навіть не мати попереднього досвіду роботи з проектами у сфері безпеки, але повинен мати значний досвід реалізації складних проектів за участю багатьох партнерів, постачальників і служб. Вони забезпечують структуру й управління зусиллями, від управління окремими ресурсами, залученими до розгортання, до витрат, пов'язаних з ними. Вони управлятимуть проблемами і ризиками. Вони працюватимуть з керівником SOC над розробкою відповідного плану проекту/програми і відстежуватимуть досягнення етапів цього плану з тим, щоб очікувані послуги SOC були розгорнуті вчасно і в рамках бюджету.

Таким чином, план переходу буде залежати від ресурсів і часу, наявних для переходу послуг SOC на проектний рівень до певної узгодженої дати (яку часто називають "введенням в експлуатацію"). Окрім звичайних діаграм Ганта, які полюбляють керівники проектів у всьому світі, часто використовується

документ про перехід на обслуговування, який фіксує те, що має бути виконано, та перевірки, які будуть виконуватися під час переходу до нормальної роботи на етапі введення в експлуатацію. Він також документує залежності та передумови, які повинні бути в наявності перед кожною перевіркою, на додаток до ризиків та пов'язаних з ними стратегій пом'якшення, включаючи потенційний вплив на існуючі послуги, персонал та кінцевих користувачів послуг. Під час переходу також важливо вести реєстр ризиків та проблем для управління будь-якими питаннями, які можуть виникнути, що загрожують успішному переходу та поточним операціям.

Крім таких питань, пов'язаних з керівництвом, необхідно подбати про нову команду SOC. Навіть якщо компанії вдалося набрати міцну команду SOC, вона буде крихкою, коли вперше буде розгорнуто SOC, і учасники почнуть відчувати тягар високих очікувань. Команда може бути недосвідченою або неповною. Вони можуть мати великий досвід роботи в організації, але ще не мати досвіду роботи один з одним, особливо в кризових умовах. Крім того, в команді SOC можуть бути сторонні підрядники й постачальники, які відіграють ключову роль, і налагодження безперебійної роботи між внутрішніми та зовнішніми членами команди може зайняти певний час.

Проблеми процесу

Недосвідчені керівники SOC схильні вважати, що надійні, зрілі процеси та процедури вирішать багато проблем людей. Зрештою, консультанти та їхні власні колеги, ймовірно, говорили їм, що чітко визначений, ретельний процес є ліками від недосвідченості або відсутності навичок. Однак, так рідко буває; процеси та процедури супроводжуються власними проблемами.

Як обговорювалося вище, процеси і процедури мають обмежену ефективність в середовищі SOC. Процеси часто описують ідеальні способи взаємодії різних сторін (як всередині команди SOC, так і з іншими командами за межами SOC) для прийняття рішень та виконання завдань. Вони майже завжди добре виглядають на папері, але часто негативно впливають на те, як SOC виконує свою основну місію: виявлення та швидке реагування на

потенційні інциденти безпеки. Це стає особливо очевидним, коли для прийняття ключових рішень необхідно залучити кілька сторін. Процедури також можуть виглядати добре, але можуть бути настільки обмеженими (або обмеженими в дуже вузькому діапазоні умов), що аналітики SOC не можуть ефективно виконувати свою роботу. В особливо обмежених умовах це, як правило, має майже негайний вплив на моральний дух команди SOC та її утримання. Майже всі SOC починають з надлишку процесів і процедур.

Розгортання з урахуванням досяжних рівнів обслуговування

При розробці послуг SOC в попередніх розділах було проведено чітке розмежування між метриками, рівнями обслуговування, ключовими показниками ефективності та ключовими показниками ризику. При розгортанні SOC, увага має бути зосереджена на початкових рівнях обслуговування, при цьому необхідно переконатися, що очікувані показники дійсно можуть бути виміряні. Ключове слово "початковий", оскільки рівні обслуговування, які, ймовірно, можна забезпечити в перші дні роботи SOC, будуть значно відрізнятися від тих, які будуть надаватися з розвитком SOC. Можливо, навіть знадобиться період "вигорання" протягом декількох місяців, щоб визначити, який рівень обслуговування компанія може собі дозволити.

Кожна послуга повинна мати чітко визначені рівні обслуговування, які можна кількісно виміряти та відстежити в часі. Вони визначають, чи є ця конкретна послуга успішною в певний момент часу або протягом останнього звітного періоду, і призначені для відображення пріоритетів і вимог спонсорів SOC та ключових споживачів послуг. Рівні обслуговування також визначають інвестиції в автоматизацію та операційні потужності, а також можуть впливати на те, хто буде надавати послуги. Досягнення рівня обслуговування зазвичай фіксується на щомісячній основі та включається до звичайної операційної звітності. Він ретельно відстежується, особливо протягом перших 3 місяців після введення послуги в експлуатацію, і вирівнюється відповідно до фактичних показників.

Наприклад, розглянемо деякі загальні типи рівнів обслуговування, які більшість служб моніторингу SOC мають виконувати з моменту запуску: час реагування, доцільність ескалації, тобто передавання повноважень щодо інцидента на вищий рівень, відставання в черзі та дотримання процедур:

Середній час реагування на інцидент - це середній час, який аналітик SOC витрачає на завершення аналізу події безпеки, ідентифікацію/класифікацію інциденту, прийняття рішення про те, чи потребує інцидент ескалації або виправлення, а також ескалацію на основі визначених параметрів. Нерідкі випадки, коли нова служба моніторингу може досягти досить агресивного рівня обслуговування за часом реагування (наприклад, менше 15 або 30 хвилин з моменту потрапляння в чергу), навіть з молодшими аналітиками. Однак, без рівня точності обслуговування, описаного нижче, аналітики схильні до ескалації будь-чого, що наближається до рівня обслуговування.

Середня точність ескалації, яку іноді також називають точністю реагування, вимірює, чи були дії з ескалації, вжиті аналітиком, що здійснює моніторинг, доречними. Зазвичай це відображає низку факторів. На основі аналізу першопричин після інциденту, нижчий, ніж очікувалося, рівень точності може вказувати на:

– прогалини в індивідуальних навичках/знаннях аналітика і, таким чином, вимагати додаткового досвіду або навчання;

– поширеність помилкових спрацьовувань в автоматизованих системах і, таким чином, вимагати їх налаштування;

– невідповідні або неточні процедури і, таким чином, вимагати оновлення.

Загалом, цей рівень обслуговування використовується для пом'якшення рівня обслуговування часу реагування, заохочуючи аналітиків бути впевненими в тому, що вони збільшують фактичні інциденти, але також часто трапляється,

що нові аналітики помиляються у великому відсотку часу на початку роботи, хоча вони мають тенденцію швидко вдосконалюватися.

Відповідність процедурам управління інцидентами - це рівень обслуговування, який часто використовується для відстеження відповідності конкретним задокументованим процедурам. Однак процедури першого покоління, як правило, є неточними або неправильними і можуть бути фактором невідповідності. В ідеалі, однак, рівень обслуговування повинен швидко зростати до 100%.

Можна помітити що, для кожного з цих рівнів обслуговування часто існує початкова мета з можливістю встановити чітко визначене покращення з часом. Це може підійти для організацій, які будують SOC, використовуючи внутрішні ресурси з відносно невеликим попереднім досвідом SOC; однак, якщо більш бажані вищі рівні обслуговування, це вимагатиме або більш активного залучення висококваліфікованих ресурсів з ринку, або використання аутсорсингу або керованих постачальників послуг, готових підписатися на рівні обслуговування (і пов'язаних з цим штрафних санкцій).

Для початкового розгортання SOC часто краще зосередитися на відносно невеликій кількості варіантів використання, узгоджених зі спонсорами і споживачами послуг, і бути готовим розширити кількість варіантів використання, які SOC може підтримувати протягом першого року. Варто проаналізувати, з якими інцидентами кібербезпеки організація зіткнулася за останні кілька років, які сценарії зустрічаються частіше, взяти до уваги результати останнього аудиту та рекомендації, які могли б сприяти більш ефективному виявленню та реагуванню на конкретні загрози для конкретних активів. Також доцільно оцінити SIEM організації, зосередитися на рішеннях, які можна відносно легко розгорнути, використовуючи легко інтегровані джерела подій і даних з готовими правилами кореляції в SIEM.

Висновки до розділу 3

У розділі 3 представлено рекомендації щодо процесу створення SOC, який складається із трьох етапів: планування, проектування, впровадження.

Етап планування допомагає визначити і формалізувати цілі SOC, а також розробити карту можливостей для відстеження прогресу їх досягненні. У рамках планування необхідно окреслити вимоги до SOC і на їх основі оцінити операційні можливості безпеки організації; розробити стратегію SOC, яка визначає місію, стратегічні цілі, модель функціонування, перелік послуг, план розвитку можливостей, ключові показники ефективності та метрики.

На етапі проектування визначають сферу застосування SOC, модель роботи, графік створення, макет розташування об’єктів, умови безпечного функціонування SOC та послуги, що надаються SOC, зокрема формування та збір подій безпеки, управління вразливостями, аудит безпеки тощо.

У межах етапу впровадження SOC потрібно підготуватися до експлуатації й оцінити ключові виклики, пов’язані з його відкриттям, забезпечити розгортання архітектури SOC з урахуванням досяжних рівнів обслуговування, здійснити проектування і сегментацію мережі, впровадити необхідні інструменти.

ВИСНОВКИ

У результаті дослідження встановлено, що Центр забезпечення безпеки (SOC) – це організаційна одиниця, яка діє в центрі всіх операцій з безпеки і виконує функції виявлення, аналізу й реагування на загрози та інциденти кібербезпеки з використанням людей, процесів та технологій. SOC можуть бути структуровані як централізовані, розподілені або децентралізовані структури.

Проаналізовано концепцію PPT (People, Process. Technology), яка передбачає визначення процесів для оптимізації операцій, впровадження правильної технології для підвищення ефективності роботи і наймання фахівців з потрібними навичками для управління цими процесами.

Зроблено висновок, що незалежно від операційної моделі, SOC повинен бути захищеним. Несправний SOC залишає всю решту компанії вразливою, оскільки атаки можуть поширюватися непоміченими. Тому безпеці SOC необхідно приділяти особливу увагу. Кожна операційна модель має певні переваги та недоліки, і важливо прийняти рішення заздалегідь.

Аналіз SOC чотирьох поколінь показав, що зміни у функціональних можливостях SOC пов’язані з необхідністю реагувати на загрози, які постійно вдосконалюються. Встановлено, що сучасний SOC поєднує ряд удосконалених служб безпеки з широким переліком важливих функцій: моніторинг подій безпеки; управління розвідданими про загрози; розвідка загроз; управління вразливостями; управління інцидентами; розробка даних і метрик для звітності тощо.

Розглянуто технології, які використовуються для розробки концептуальної архітектури SOC: збору й аналізу даних, управління вразливостями, розвідки загроз. У результаті аналізу технологій збору й аналізу даних зроблено висновок, що повідомлення журналів вважаються найбільш корисним типом даних, оскільки вони підсумовують дію або діяльність, яка відбулася в системі, і містять інформацію, пов'язану з відповідною подією. Також розглянуто протокол syslog та проаналізовано його структуру.

Виявлено, що технології з управління вразливостями забезпечують виконання завдань із виявлення, підтвердження, класифікації, визначення пріоритетів, призначення, усунення та відстеження вразливостей. Технології розвідки загроз розроблені для збору інформації про можливості внутрішніх і зовнішніх суб'єктів загроз. До найбільш затребуваних платформ розвідки загроз відносять Cyber Squad ThreatConnect, BAE Detica CyberReveal, Lockheed Martin Palisade, MITRE CRITs, Structured Threat Information eXpression (STIX) та інші.

За результатами дослідження представлено рекомендації щодо процесу створення SOC, який складається із трьох етапів: планування, проектування, впровадження.

Етап планування допомагає визначити і формалізувати цілі SOC, а також розробити карту можливостей для відстеження прогресу їх досягненні. У рамках планування необхідно окреслити вимоги до SOC і на їх основі оцінити операційні можливості безпеки організації; розробити стратегію SOC, яка визначає місію, стратегічні цілі, модель функціонування, перелік послуг, план розвитку можливостей, ключові показники ефективності та метрики.

На етапі проектування визначають сферу застосування SOC, модель роботи, графік створення, макет розташування об’єктів, умови безпечного функціонування SOC та послуги, що надаються SOC, зокрема формування та збір подій безпеки, управління вразливостями, аудит безпеки тощо.

У межах етапу впровадження SOC потрібно підготуватися до експлуатації й оцінити ключові виклики, пов’язані з його відкриттям, забезпечити розгортання архітектури SOC з урахуванням досяжних рівнів обслуговування, здійснити проектування і сегментацію мережі, впровадити необхідні інструменти.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. The Cost of Cybercrime, Accenture and Ponemon Institute, New York, NY, USA, 2018.

2. S. Radu, "Comparative analysis of security operations centre architectures; Proposals and architectural considerations for frameworks and operating models," in Innovative Security Solutions for Information Technology and Communications (Lecture Notes in Computer Science), vol. 10006. Cham, Switzerland: Springer, 2016, pp. 248–260.

3. C. Onwubiko, "Cyber security operations centre: Security monitoring for protecting business and supporting cyber defense strategy," in Proc. Int. Conf. Cyber Situational Awareness, Data Analytics Assessment (CyberSA), London, U.K., Jun. 2015, pp. 1–10.

4. C. Onwubiko and K. Ouazzane, "Cyber onboarding is Broken," in Proc. Int. Conf. Cyber Secur. Protection Digit. Services, Oxford, U.K., Jun. 2019, pp. 1–13.

5. S. Mansfield-Devine, "Creating security operations centres that work," Netw. Secur., vol. 2016, no. 5, pp. 15–18, May 2016.

6. M. Majid and K. Ariffi, "Success factors for cyber security operation center (SOC) establishment," in Proc. 1st Int. Conf. Informat., Eng., Sci. Technol., Bandung, IN, USA, May 2019, pp. 1–11.

7. G. D. Bhatt, "Knowledge management in organizations: Examining the interaction between technologies, techniques, and people," J. Knowl. Manage., vol. 5, no. 1, pp. 68–75, Mar. 2001.

8. J. Bourgeois, A. Ganame, I. Kotenko, and A. Ulanov, "Software environment for simulation and evaluation of a security operation center," in Information Fusion and Geographic Information Systems (Lecture Notes in Geoinformation and Cartography). Berlin, Germany: Springer, 2007, pp. 111–127.

9. D. Kelley and R. Moritz, "Best practices for building a security operations center," Inf. Syst. Secur., vol. 14, no. 6, pp. 27–32, Jan. 2006.

10. R. Ruefle, "Defining computer security incident response teams," Carnegie Mellon Univ., Pittsburgh, PA, USA, Tech. Rep., 2007.

11. L. Aijaz, B. Aslam, and U. Khalid, "Security operations center—A need for an academic environment," in Proc. World Symp. Comput. Netw. Inf. Secur. (WSCNIS), Hammamet, Tunisia, Sep. 2015, pp. 1–7.

12. J. M. Brown, S. Greenspan, and R. Biddle, "Incident response teams in IT operations centers: The T-TOCs model of team functionality," Cognition, Technol. Work, vol. 18, no. 4, pp. 695–716, Nov. 2016.

13. O. Podzins and A. Romanovs, "Why SIEM is irreplaceable in a secure it environment?" in Proc. Open Conf. Electr., Electron. Inf. Sci., Vilnius, Lithuania, May 2019, pp. 1–5.

14. D. Robb, "How to manage a security operations center," eSecurity Planet, Nashville, TN, USA, Tech. Rep., 2019.

15. N. Miloslavskaya, "Analysis of SIEM systems and their usage in security operations and security intelligence centers," in Biologically Inspired Cognitive Architectures (BICA) for Young Scientists, vol. 636. Cham, Switzerland: Springer, 2018, pp. 282–288.

16. N. Miloslavskaya, "Security intelligence centers for big data processing," in Proc. 5th Int. Conf. Future Internet Things Cloud Workshops (FiCloudW), Prague, Czech Republic, Aug. 2017, pp. 7–13.

17. M. Vielberth and G. Pernul, "A security information and event management pattern," in Proc. 12th Latin Amer. Conf. Pattern Lang. Prog. (SLPLoP). 2018, pp. 1–5.

18. R. Bidou, J. Bourgeois, and F. Spies, "Towards a global security architecture for intrusion detection and reaction management," in Information Security Applications (Lecture Notes in Computer Science), vol. 2908. Berlin, Germany: Springer, 2004, pp. 111–123.

19. R. H. Syed, J. Pazardzievska, and J. Bourgeois, "Fast attack detection using correlation and summarizing of security alerts in grid computing networks," J. Supercomput., vol. 62, no. 2, pp. 804–827, Nov. 2012.

20. R. H. Syed, M. Syrame, and J. Bourgeois, "Protecting grids from crossdomain attacks using security alert sharing mechanisms," Future Gener. Comput. Syst., vol. 29, no. 2, pp. 536–547, Feb. 2013.

21. J. Webster and R. T. Watson, "Analyzing the past to prepare for the future: Writing a literature review," MIS Quart., vol. 26, no. 2, pp. 13–23, 2002.

22. A. Karim Ganame, J. Bourgeois, R. Bidou, and F. Spies, "A global security architecture for intrusion detection on computer networks," Comput. Secur., vol. 27, nos. 1–2, pp. 30–47, Mar. 2008.

23. J. Bourgeois and R. Syed, "Managing security of grid architecture with a grid security operation center," in Proc. Int. Conf. Secur. Cryptogr., Milan, Italy, 2009, pp. 403–408.

24. X. Hu and C. Xie, "Security operation center design based on D-S evidence theory," in Proc. Int. Conf. Mechatronics Autom., Luoyang, China, Jun. 2006, pp. 2302–2306.

25. S. Yuan and C. Zou, "The security operations center based on correlation analysis," in Proc. IEEE 3rd Int. Conf. Commun. Softw. Netw., Xi'an, China, May 2011, pp. 334–337.

26. E. G. Amoroso, "Cyber attacks: Awareness," Netw. Secur., vol. 2011, no. 1, pp. 10–16, Jan. 2011.

27. G. Settanni, F. Skopik, Y. Shovgenya, R. Fiedler, M. Carolan, D. Conroy, K. Boettinger, M. Gall, G. Brost, C. Ponchel, M. Haustein, H. Kaufmann, K. Theuerkauf, and P. Olli, "A collaborative cyber incident management system for European interconnected critical infrastructures," J. Inf. Secur. Appl., vol. 34, pp. 166–182, Jun. 2017.

28. T. Tafazzoli and H. Gharaee Garakani, "Security operation center implementation on OpenStack," in Proc. 8th Int. Symp. Telecommun. (IST), Tehran, Iran, Sep. 2016, pp. 766–770.

29. J.-S. Li, C.-J. Hsieh, and H.-Y. Lin, "A hierarchical mobile-agentbased security operation center," Int. J. Commun. Syst., vol. 26, no. 12, pp. 1503–1519, Dec. 2013.

30. J.-S. Li and C.-J. Hsieh, "Implementation of the distributed hierarchical security operation center using mobile agent group," in Proc. Int. Symp. Comput., Commun., Control Autom. (3CA), Tainan, Taiwan, May 2010, pp. 79–82.

31. G. Chamiekara, M. Cooray, L. Wickramasinghe, Y. Koshila, K. Abeywardhana, and A. Senarathna, "AutoSOC: A low budget flexible security operations platform for enterprises and organizations," in Proc. Nat. Inf. Technol. Conf. (NITC), Colombo, Sri Lanka, 2017, pp. 100–105.

32. E. Falk, S. Repcek, B. Fiz, S. Hommes, R. State, and R. Sasnauskas, "VSOC–A virtual security operating center," in Proc. IEEE Global Commun. Conf., Singapore, Dec. 2017, pp. 1–8.

33. U. Glasser, P. Jackson, A. Araghi, and H. Shahir, "Intelligent decision support for marine safety and security operations," in Proc. IEEE Int. Conf. Intell. Secur. Inform., Vancouver, BC, Canada, May 2010, pp. 101–107.

34. B. AlSabbagh and S. Kowalski, "A framework and prototype for a socio-technical security information and event management system (STSIEM)," in Proc. Eur. Intell. Secur. Informat. Conf. (EISIC), Uppsala, Sweden, Aug. 2016, pp. 192–195.

35. F. Sailhan and J. Bourgeois, "Log-based distributed intrusion detection for hybrid networks," in Proc. 4th Annu. workshop Cyber Secur. informaiton Intell. Res., New York, NY, USA, 2008, pp. 1–6.

36. P. Bienias, G. Kolaczek, and A. Warzynski, "Architecture of anomaly detection module for the security operations center," in Proc. IEEE 28th Int. Conf. Enabling Technologies: Infrastruct. Collaborative Enterprises (WETICE), Naples, Italy, Jun. 2019, pp. 126–131.

37. A. Chowdhary, D. Huang, G.-J. Ahn, M. Kang, A. Kim, and A. Velazquez, "SDNSOC: Object oriented SDN framework," in Proc. ACM Int. Workshop Secur. Softw. Defined Netw. Netw. Function Virtualization, New York, NY, USA, 2019, pp. 7–12.

38. D. Crooks and L. Valsan, "wlcg security operations centre working group," Proc. Sci., vol. 1, no. 1, pp. 1–25, 2017.

39. D. Crooks, L. Vâlsan, K. Mohammad, S. McKee, P. Clark, A. Boutcher, A. Padée, M. Wójcik, H. Giemza, and B. Kreukniet, "Operational security, threat intelligence & distributed computing: The WLCG security operations center working group," EPJ Web Conferences, vol. 214, p. 15, May 2019.

40. D. Crooks and L. Válsan, "Building a minimum viable security operations centre for the modern grid environment," in Proc. Int. Symp. Grids Clouds, Trieste, Italy, Nov. 2019, p. 10.

41. P. Danquah, "Security operations center: A framework for automated triage, containment and escalation," J. Inf. Secur., vol. 11, no. 4, pp. 225–240, 2020.

42. F. Alruwaili and T. Gulliver, "Socaas: Security operations center as a service for cloud computing environments," Int. J. Cloud Comput. Services Sci., vol. 3, no. 2, pp. 87–96, 2014.

43. F. B. Kokulu, A. Soneji, T. Bao, Y. Shoshitaishvili, Z. Zhao, A. Doupé, and G.-J. Ahn, "Matched and mismatched SOCs," in Proc. ACM SIGSAC Conf. Comput. Commun. Secur., New York, NY, USA, Nov. 2019, pp. 1955–1970.

44. N. Miloslavskaya, A. Tolstoy, and S. Zapechnikov, "Taxonomy for unsecure big data processing in security operations centers," in Proc. IEEE 4th Int. Conf. Future Internet Things Cloud Workshops (FiCloudW), Vienna, Austria, Aug. 2016, pp. 154–159.

45. D. Forte, "An inside look at security operation centres," Netw. Secur., vol. 2003, no. 5, pp. 11–12, 2003.

46. P. Jacobs, A. Arnab, and B. Irwin, "Classification of security operation centers," in Proc. Inf. Secur. South Afr., Johannesburg, South Africa, Aug. 2013, pp. 1–7.

47. S. Schinagl, K. Schoon, and R. Paans, "A framework for designing a security operations centre (SOC)," in Proc. 48th Hawaii Int. Conf. Syst. Sci., Kauai, HI, USA, Jan. 2015, pp. 2253–2262.

48. C. Zimmerman, "Ten strategies of a world-class cybersecurity operations center," MITRE Corp., Bedford, MA, USA, Tech. Rep., 2014.

49. H. Security, "Choosing a SOC service model: The key considerations," Huntsman Secur., London, U.K., Tech. Rep., 2018.

50. N. Miloslavskaya, "Security operations centers for information security incident management," in Proc. IEEE 4th Int. Conf. Future Internet Things Cloud (FiCloud), Vienna, Austria, Aug. 2016, pp. 131–136.

51. F. David Janos and N. Huu Phuoc Dai, "Security concerns towards security operations centers," in Proc. IEEE 12th Int. Symp. Appl. Comput. Intell. Informat. (SACI), Timisoara, Romania, May 2018, pp. 000273–000278.

52. D. Forte, "State of the art security management," Comput. Fraud Secur., vol. 2009, no. 10, pp. 17–18, Oct. 2009.

53. J. Muniz, G. McIntyre, and N. AlFardan, "Security operations center: Building, operating, and maintaining your SOC," Indianapolis, IN, USA: Cisco Press, 2015.

54. Outsourced Soc Vs. Internal Soc: How to Choose, Linkbynet, Montreal, QC, Canada, 2018.

55. A. Shah, R. Ganesan, and S. Jajodia, "A methodology for ensuring fair allocation of CSOC effort for alert investigation," Int. J. Inf. Secur., vol. 18, no. 2, pp. 199–218, Apr. 2019.

56. M. Khalili, M. Zhang, D. Borbor, L. Wang, N. Scarabeo, and M.-A. Zamor, "Monitoring and improving managed security services inside a security operation center," ICST Trans. Secur. Saf., vol. 5, no. 18, Apr. 2019, Art. no. 157413.

57. B. Hámornik and C. Krasznay, "A team-level perspective of human factors in cyber security: Security operations centers," in Advances in Human Factors in Cybersecurity, vol. 593 D. Nicholson, Ed. Cham, Switzerland: Springer, 2018, pp. 224–236.

58. C. DeCusatis, R. Cannistra, A. Labouseur, and M. Johnson, "Design and implementation of a research and education cybersecurity operations center," in Cybersecurity and Secure Information Systems (Advanced Sciences and Technologies for Security Applications), vol. 33. Cham, Switzerland: Springer, 2019, pp. 287–310.

59. R. Ganesan, A. Shah, S. Jajodia, and H. Cam, "Optimizing alert data management processes at a cyber security operations center," in Adversarial and Uncertain Reasoning for Adaptive Cyber Defense (Lecture Note in Computer Science), vol. 11830. Cham, Switzerland: Springer, 2019, pp. 206–231.

60. A. Vault, "How to build a security operations center," Alien Vault, San Mateo, CA, USA, Tech. Rep., 2017.

61. O. Cassetto, "Security operations center roles and responsibilities," Exabeam, Foster City, CA, USA, Tech. Rep., 2019.

62. S. C. Sundaramurthy, J. Case, T. Truong, L. Zomlot, and M. Hoffmann, "A tale of three security operation centers," in Proc. ACM Workshop Secur. Inf. Workers, New York, NY, USA, 2014, pp. 43–50.

63. C. Olt, "Establishing security operation centers for connected cars," ATZelectronics worldwide, vol. 14, no. 5, pp. 40–43, May 2019.

64. Strategies for Building and Growing Strong Cybersecurity Teams: Cybersecurity Workforce Study, International Information System Security Certification Consortium, Clearwater, FL, USA, 2019.

65. S. C. Sundaramurthy, M. Wesch, X. Ou, J. McHugh, S. R. Rajagopalan, and A. G. Bardas, "Humans are dynamic–our tools should be too," IEEE Internet Comput., vol. 21, no. 3, pp. 40–46, May 2017.

66. S. Sundaramurthy, "An anthropological study of security operations centers to improve operational efficiency," Ph.D. dissertation, Dept. Comput. Sci. Eng., Univ. South Florida, Tampa, FL, USA, 2017.

67. C. Zhong, J. Yen, P. Liu, and R. F. Erbacher, "Learning from Experts' experience: Toward automated cyber security data triage," IEEE Syst. J., vol. 13, no. 1, pp. 603–614, Mar. 2019.

68. C. Islam, M. Babar, and S. Nepal, "Automated interpretation and integration of security tools using semantic knowledge," in Advanced Information Systems Engineering (Lecture Notes in Computer Science), vol. 11483. Cham, Switzerland: Springer, 2019, pp. 513–528.

69. Y. Kanemoto, K. Aoki, M. Iwamura, J. Miyoshi, D. Kotani, H. Takakura, and Y. Okabe, "Detecting successful attacks from IDS alerts based on emulation of remote shellcodes," in Proc. IEEE 43rd Annu. Comput. Softw. Appl. Conf. (COMPSAC), Milwaukee, WA, USA, Jul. 2019, pp. 471–476.

70. A. Kabil, T. Duval, N. Cuppens, G. Le Comte, Y. Halgand, and C. Ponchel, "3D cybercop: A collaborative platform for cybersecurity data analysis and training," in Cooperative Design, Visualization, and Engineering (Lecture Notes in Computer Science), vol. 11151, Y. Luo, Ed. pp. 176–183. Cham, Switzerland: Springer, 2018, pp. 176–183.

71. A. Kabil, T. Duval, N. Cuppens, G. Le Comte, Y. Halgand, and C. Ponchel, "From cyber security activities to collaborative virtual environments practices through the 3D cybercop platform," in Information Systems Security (Lecture Notes in Computer Science), vol. 11281. Cham, Switzerland: Springer, 2018, pp. 272–287.

72. M. Mutemwa, J. Mtsweni, and L. Zimba, "Integrating a security operations centre with an Organization's existing procedures, policies and information technology systems," in Proc. Int. Conf. Intell. Innov. Comput. Appl. (ICONIC), Plaine Magnien, Mauritius, Dec. 2018, pp. 1–6.

73. A. Chin-Ching Lin, H.-K. Wong, and T.-C. Wu, "Enhancing interoperability of security operation center to heterogeneous intrusion detection systems," in Proc. 39th Annu. Int. Carnahan Conf. Secur. Technol., Las Palmas, Spain, 2005, pp. 216–221.

74. M. Nabil, S. Soukainat, A. Lakbabi, and O. Ghizlane, "SIEM selection criteria for an efficient contextual security," in Proc. Int. Symp. Netw., Comput. Commun. (ISNCC), Marrakech, Morocco, May 2017, pp. 1–6.

75. S. Y. Cho, J. Happa, and S. Creese, "Capturing tacit knowledge in security operation centers," IEEE Access, vol. 8, pp. 42021–42041, 2020.

76. M. H. Khyavi, "ISMS role in the improvement of digital forensics related process in SOC's," 2015, arXiv:2006.08255. [Online]. Available: https://arxiv.org/abs/2006.08255.

77. Information Technology - Security Techniques—Information Security Incident Management—Part 1: Principles of Incident Management, Standard ISO/IEC 27035-1:2016, 2016.

78. P. Cichonski, T. Millar, T. Grance, and K. Scarfone, "Computer security incident handling guide: Special publication 800-61 revision 2," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. 800-61, 2012.

79. A. Madani, S. Rezayi, and H. Gharaee, "Log management comprehensive architecture in security operation center (SOC)," in Proc. Int. Conf. Comput. Aspects Social Netw. (CASoN), Salamanca, Spain, Oct. 2011, pp. 284–289.

80. D. Zhang and D. Zhang, "The analysis of event correlation in security operations center," in Proc. 4th Int. Conf. Intell. Comput. Technol. Autom., Guangdong, Shenzhen, Mar. 2011, pp. 1214–1216.

81. Z. Qu and L. Wang, "The design of a correlation analysis engine model based on Carma_VE algorithm," in Proc. IEEE Int. Symp. Med. Edu., Jinan, China, Aug. 2009, pp. 1267–1270.

82. M. E. Verma and R. A. Bridges, "Defining a metric space of host logs and operational use cases," in Proc. IEEE Int. Conf. Big Data (Big Data), Seattle, WA, USA, Dec. 2018, pp. 5068–5077.

83. M. Alam, S.-U.-R. Malik, Q. Javed, A. Khan, S. B. Khan, A. Anjum, N. Javed, A. Akhunzada, and M. K. Khan, "Formal modeling and verification of security controls for multimedia systems in the cloud," Multimedia Tools Appl., vol. 76, no. 21, pp. 22845–22870, Nov. 2017.

84. K. Kent and M. Souppaya, "Guide to computer security log management: Recommendations of the National Institute of Standards and Technology," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. 800-92, 2006.

85. Y.-C. Cheng, C.-H. Chen, C.-C. Chiang, J.-W. Wang, and C.-S. Laih, "Generating attack scenarios with causal relationship," in Proc. IEEE Int. Conf. Granular Comput., Fremont, CA, USA, Nov. 2007, p. 368.

86. G. Gonzalez Granadillo, M. El-Barbori, and H. Debar, "New types of alert correlation for security information and event management systems," in Proc. 8th

IFIP Int. Conf. New Technol., Mobility Secur. (NTMS), Larnaca, Cyprus, Nov. 2016, pp. 1–7.

87. D. Tranfield, D. Denyer, and P. Smart, "Towards a methodology for developing evidence-informed management knowledge by means of systematic review," Brit. J. Manage., vol. 14, no. 3, pp. 207–222, Sep. 2003.

88. S. Bhatt, P. K. Manadhata, and L. Zomlot, "The operational role of security information and event management systems," IEEE Secur. Privacy, vol. 12, no. 5, pp. 35–41, Sep. 2014.

89. C. Islam, M. A. Babar, and S. Nepal, "Architecture-centric support for integrating security tools in a security orchestration platform," in Software Architecture (Lecture Notes in Computer Science), vol. 12292, A. Jansen, I. Malavolta, H. Muccini, I. Ozkaya, O. Zimmermann, Eds. Cham, Switzerland: Springer, 2020, pp. 165–181.

90. C. Islam, M. A. Babar, and S. Nepal, "A multi-vocal review of security orchestration," ACM Comput. Surv., vol. 52, no. 2, pp. 1–45, May 2019.

91. W. Yang and K.-Y. Lam, "Automated cyber threat intelligence reports classification for early warning of cyber attacks in next generation SOC," in Information and Communications Security, vol. 11999, J. Zhou, X. Luo, Q. Shen, and Z. Xu, Eds. Cham, Switzerland: Springer, 2020, pp. 145–164.

92. F. Osinga, Science, Strategy and War: The Strategic Theory of John Boyd. London, U.K.: Routledge, 2007.

93. C. Zhong, A. Alnusair, B. Sayger, A. Troxell, and J. Yao, "AOH-map: A mind mapping system for supporting collaborative cyber security analysis," in Proc. IEEE Conf. Cognit. Comput. Aspects Situation Manage. (CogSIMA), Las Vegas, NV, USA, Apr. 2019, pp. 74–80.

94. G. Zhiguo, X. Luo, J. Chen, F. L. Wang, and J. Lei, Eds., Emerging Research in Web Information Systems and Mining (Communications in Computer and Information Science). Berlin, Germany: Springer, 2011.

95. M. Vielberth, F. Menges, and G. Pernul, "Human-as-a-security-sensor for harvesting threat intelligence," Cybersecurity, vol. 2, no. 1, p. 35, Dec. 2019.

96. L. Karaçay, E. Savaä, and H. Alptekin, "Intrusion detection over encrypted network data," Comput. J., vol. 63, no. 4, pp. 604–619, Apr. 2020.

97. M. Smith, "The SOC is dead, long live the SOC!" Itnow, vol. 62, no. 1, pp. 34–35, 2020.

98. NIST SP 800-40 Version 2.0 Creating a Patch and Vulnerability Management Program, http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf.

99. The syslog protocol, http://tools.ietf.org/html/rfc542.

100. Reliable delivery for syslog, https://www.ietf.org/rfc/rfc3195.txt.

101. Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information, http://tools.ietf.org/html/rfc7011.

102. CVE-IDs - Products & Services by Product Category, https://cve.mitre.org/compatible/product_type.html.

103. CVSS Implementation Guidance, https://www.nist.gov/publications/cvss-implementation-guidance.

104. Verizon Breach Investigation Report, http://www.verizonenterprise.com/DBIR/2015/.